DISEÑO DE CONTROLES DE SEGURIDAD PARA LOS ACTIVOS INFORMÁTICOS EN LA EMPRESA TRANSPORTES TIERRA GRATA Y COMPAÑÍA LTDA. DE FUSAGASUGÁ

YON IVAN MARQUEZ BUITRAGO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

FUSAGASUGÁ - CUNDINAMARCA

2018

DISEÑO DE CONTROLES DE SEGURIDAD PARA LOS ACTIVOS INFORMÁTICOS EN LA EMPRESA TRANSPORTES TIERRA GRATA Y COMPAÑÍA LTDA. DE FUSAGASUGÁ

YON IVAN MARQUEZ BUITRAGO

Propuesta de proyecto aplicado como opción de grado para optar al título de Especialista en Seguridad Informática

Asesores: Ing. Luis Fernando Zambrano Hernández (Proyecto I) e Ing. Juan José Cruz (Proyecto II), Director de Proyecto Ing. Helena Clara Isabel Alemán Novoa

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

FUSAGASUGÁ - CUNDINAMARCA

2018

Nota de Aceptación:

_____
_____
_____
_____
_____
_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Fusagasugá, 06 de noviembre de 2018

DEDICATORIA

Al Todopoderoso.

Por permitirme llegar hasta este nuevo logro, por darme salud para así lograr mis objetivos, y además por brindarme su infinita bondad y amor.

A mis madres Flor y Esperanza.

Por apoyarme en todo instante, por sus consejos, sus valores, por la motivación constante que me han permitido ser una persona de bien, pero más que nada, por su constante amor.

A mi padre Gonzalo.

Por sus ejemplos de perseverancia y constancia que lo caracterizan y que me ha infundado siempre, por el valor mostrado para salir adelante y por su amor.

A mis amigos.

Que me apoyan en mi formación profesional y personal: Hernando Santos, Javier García, Francisco Benítez, Fidel Franco, Armando Barón, Cristina Mora, Rafael Pitta.

Todos aquellos familiares y amigos que no recordé al momento de escribir esto. Ustedes saben quiénes son.

AGRADECIMIENTOS

Le agradezco a Dios por haberme acompañado y guiado a lo largo de mis estudios profesionales, por ser mi fortaleza en los momentos de debilidad y por brindarme una vida llena de aprendizajes, experiencias y sobre todo de alegrías.

Agradezco a mis padres y hermanos por apoyarme en todo momento, por los valores que me han inculcado.

Les agradezco la confianza, apoyo y dedicación de tiempo a mis profesores y tutores: Ing. Luis Fernando Zambrano Hernández, Ing. Juan José Cruz, Ing. Helena Clara Isabel Alemán Novoa e Ing. Jorge Enrique Ramírez M

Gracias doctor Jorge Humberto Pulido Pardo, Gerente Empresa Transportes Tierra Grata y Cía. Ltda., y a todo el equipo de la empresa por permitirme trabajar con ustedes en el desarrollo de este proyecto.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

RESUMEN

El presente trabajo da los lineamientos para diseñar los controles de seguridad que salvaguarden los activos de información, describiendo las nociones relacionadas con el tema de seguridad de la información en las organizaciones, tratando un enfoque global mostrando los modelos, técnicas e instrumentos que suministran las guías necesarias para disminuir el nivel de fragilidad que tienen los activos ante una amenaza. Dichos lineamientos se hacen siguiendo la metodología MAGERIT alineado con la norma ISO/IEC 27001 para una empresa de transporte de pasajeros. Se define la situación actual de la empresa, se identifican los activos con sus pertinentes amenazas, se realiza la comprobación de riesgos efectivos y se sugieren las protecciones necesarias que podría formar parte del plan de implantación.

Palabras Clave: SGSI, Activos, Información, Riesgo, Amenaza, Control de seguridad, Activo, Gestión de Riesgos, Norma ISO, PSI

ABSTRAC

This paper gives the guidelines for designing security controls that safeguard information assets, describing the notions related to the topic of information security in organizations, trying a global approach showing the models, techniques and instruments provided by the guides necessary to reduce the level of fragility that assets have when faced with a threat. These guidelines are made following the MAGERIT methodology aligned with the ISO / IEC 27001 standard for a passenger transport company. The current situation of the company is defined, the assets are identified with their relevant threats, the actual risks are verified and the necessary protections that could be part of the implementation plan are suggested

Keywords: SGSI, Assets, Information, Risk, Threat, Security control, Asset, Risk Management, ISO Standard, PSI.

INTRODUCCION

Hoy en día los activos informáticos, con sus ventajas para el uso, transporte y acopio de la información, se convierten en elementos cada vez más valiosos para la empresa. Esto ha llevado a la modernización de los activos informáticos en la búsqueda de la eficiencia. En todo ámbito laboral se está expuesto a los riesgos, los cuales pueden llegar a provocar pérdidas al interior de las empresas, estos riesgos deben ser controlados oportunamente y de una manera procedente. Para ello se realiza la gestión de los riesgos tecnológicos cuyo fin es salvaguardar la información, este proceso busca conocer las fortalezas y falencias que puedan llegar a afectar durante todo el ciclo de vida del servicio. Las organizaciones se ven en la obligación de cumplir con regulaciones específicas y deben garantizar que llevan a cabo prácticas acerca del uso adecuado de las tecnologías de la información y de la protección de lo que procesan y almacenan.

Diseñar los controles de seguridad que salvaguarden los activos de información es una práctica que se puede realizar para validar la situación actual en cuanto a protección, control y medidas de seguridad; además es necesaria ya que permite validar que los controles de seguridad encargados de reducir los riesgos, se encuentren correctamente implementados. Lo anterior ayuda a garantizar que las empresas se encuentran al día en cuanto a prácticas de seguridad y cumplimiento de regulaciones específicas o normas vigentes. Es muy importante que una empresa, que se dedica a ofrecer servicios de transporte y que debe administrar información personal de manera segura, se cerciore de tener un plan de gestión de riesgos que garantice la normal continuidad de los procesos de negocio. Lo anterior hace que surja la necesidad del desarrollo de un estudio de riesgo tecnológico cualitativo aplicado en la sede principal que administra y ofrece los servicios de red y de sistemas de la Empresa, siguiendo la metodología MAGERIT.

El aporte de este estudio es la identificación del nivel de riesgo en que se ubican los activos mediante el nivel de madurez de la seguridad a implementarse y el lograr motivar a los empleados a seguir las consiguientes normas y procedimientos pertinentes a la seguridad de la información y de recursos con la Declaración de Aplicabilidad (SoA) que permite conservar el control y registro de las medidas de seguridad que se aplican socializándolos con la alta dirección de la empresa. Se espera con este proyecto aplicado poder entregar a la organización el diseño de los controles para poder salvaguardar o por lo menos aminorar los riesgos de los activos de la información de la empresa. En el Anexo B se encuentra la carta de aprobación por parte de la empresa.

1. TITULO

DISEÑO DE CONTROLES DE SEGURIDAD PARA LOS ACTIVOS INFORMÁTICOS EN LA EMPRESA TRANSPORTES TIERRA GRATA Y COMPAÑÍA LTDA. DE FUSAGASUGÁ.

2. DEFINICION DEL PROBLEMA

2.1. ANTECEDENTES DEL PROBLEMA

A diario se observa en las noticias y en las redes sociales que el número de atacantes de las redes y de los SI de las empresas y organizaciones es cada vez mayor, ya es casi que normal observar titulares como “grave fallo de seguridad en las redes *WiFi* de todo el mundo”, “*hackers* roban información de importante organización”, “un poderoso Ciberataque afecta a grandes empresas de todo el mundo”, “Fuga de datos” “Estamos a merced de los ataques informáticos”[1] , y un largo etc.; por momentos se siente que es algo lejano, pero ya se sufren estos maliciosos ataques, y muchos ya los han experimentado, Colombia se vio inmiscuido en el episodio de “*ramsomware*” del año 2017, donde el activo más expuesto de las organizaciones es la información.

Como les sucede a muchas organizaciones de la región el gran problema dentro de la empresa Transportes Tierra Grata y Compañía Ltda. de Fusagasugá es que se está presentando fuga y alteración de la información debido a que no existen controles de seguridad para los activos al interior de la empresa. Otro factor influyente para casos de inseguridad informática es la falta de cultura de prevención de ataques informáticos y el desconocimiento en las organizaciones por invertir en medidas preventivas que avalen la protección de la información y los datos.

La situación actual en la que se encuentra la empresa Transportes Tierra Grata y Compañía Ltda., es crítica ya que al interior de sus procesos no se implementan medidas de seguridad apropiadas, lo cual provoca un déficit elevado de seguridad a nivel general. El software que actualmente se maneja, se encuentra en un alto nivel de deterioro, debido a la falta de mantenimientos programados, así como la falta de restricción de acceso a los equipos de telecomunicaciones, servidores y demás equipos auxiliares.

Los *hosts* que actualmente maneja esta empresa no cuentan con la implementación de una topología de red, por lo tanto, no existe un dominio o grupo de trabajo estable con el cual trabajar y que permita implementar una adecuada seguridad. Esto permite que la información no se encuentre centralizada y que cualquiera de los usuarios puede disponer de ella para bien o para mal; la falta de centralización

[1] MENDIOLA ZURIARRAIN,José, et al. Ataques Informáticos. En: El País. Bogotá D.C. 16, octubre, 2017. sec. 1. p. 1. col 1.. {En línea}. {08 de septiembre de 2017} disponible en: (https://elpais.com/tag/ataques_informaticos/a).

provoca no tener un correcto *backup* de la información clave e importante de la empresa.

2.2. FORMULACIÓN DEL PROBLEMA

¿El diseño de Controles de Seguridad a partir de la norma ISO 27001 será un procedimiento efectivo para reducir los riesgos asociados con los activos informáticos de la empresa Transportes Tierra Grata y Compañía Ltda., de Fusagasugá?

2.3. DESCRIPCIÓN

Teniendo en cuenta lo anteriormente mencionado, se indica que no tiene un cableado estructurado y el sistema eléctrico no es el óptimo, no cuenta con una adecuada canalización, estructura y redundancia, hay déficit en la asignación de puntos de red y tomacorrientes y no hay aplicación de seguridad a través de un *Router* o *Firewall*. Con la creciente evolución de los activos informáticos es muy difícil cuidar todas sus configuraciones de seguridad, lo cual puede llevar a que datos e información queden comprometidos ante personas no autorizadas, es por ello que se hace necesario realizar revisiones periódicas para verificar controles de seguridad y sus configuraciones. Estas revisiones periódicas implican dificultad para la organización que tiene que recurrir a personal especializado para hacer la respectiva verificación de los controles de seguridad. La complejidad y costo de realizar revisiones manuales sobre activos informáticos y el incremento en la periodicidad de las revisiones debido al creciente avance tecnológico y los cambios en las arquitecturas de los sistemas llevan a no poder realizar la revisión de controles de seguridad como una actividad cotidiana[2].

Esto se evidencia en que, al interior de la empresa, no se da respuesta a lo referente a seguridad informática, para ello se realizaron la entrevista aplicada que se puede observar en el Anexo C, el Cuestionario de Estado de la Seguridad de la Información del Anexo D, así mismo como el Cuestionario Evaluación de Procesos Vitales que se Soportan en Servicios de TI que aparece en el Anexo E.

[2] ARAGON ALVAREZ, Alejandro. Implementación de Controles de Seguridad en Activos Informáticos. Trabajo de Grado Maestro en Ciencias en Informática. Instituto Politécnico Nacional, Unidad Profesional Interdisciplinaria de Ingeniería y Ciencias Sociales y Administrativas, Sección de Estudios de Posgrado e Investigación, México D.F. enero 2016

3. JUSTIFICACIÓN

El mundo se vio atacado durante el mes de mayo de 2017 por un *malware* "tipo '*Ransomware'* (modalidad que encripta los archivos y exige un rescate a cambio) que pide a las víctimas afectadas un pago de aproximadamente 300 dólares en *bitcoins*"[3] , importante fue lo que comunicó la petrolera Rosneft: "Un potente ataque informático tiene como objetivo los servidores del grupo"[4] , sus activos informáticos, pero gracias a su eficiente sistema de seguridad no tuvo consecuencias.

Este mismo ataque evidenció que varias empresas colombianas incluyendo una entidad pública se vieran expuestas ya que no se tiene un sistema de seguridad informática que los proteja de estos ataques.

En el informe "Impacto de los incidentes de seguridad digital en Colombia 2017"[5] presentado por el MinTIC, la OEA y el BID, el cual se basa en las organizaciones del sector público y privado, se demuestra que muchas de las empresas evidencian no poseer habilidades para identificar los riesgos a los que están expuestas en lo concerniente a la seguridad informática[6].

Los resultados del informe evidencian que la gran mayoría de las empresas y entidades estatales no realizan una evaluación de riesgo de la seguridad digital, y cuando se les preguntó bajo qué departamento se manejaba la seguridad digital, la gran mayoría respondió que era manejada por el departamento de tecnología y no por un departamento específico de seguridad[7].

El Grupo de Delitos Informáticos de la Dirección de Investigación Criminal de la Policía Nacional de Colombia es el ente encargado de apoyar a las víctimas, en este caso se les solicitó en primera instancia no pagar, todo esto nos lleva a, que a pesar de que existe la Ley No. 1273 enero 2009 "De la protección de la información y de

---

3 TECNÓSFERA CON INFORMACIÓN DE AGENCIAS. Un nuevo ataque cibernético mundial afecta a varias multinacionales En: El Tiempo, Bogotá D.C. 27 de junio 2017. sec. 1. p. 1. col 1{En línea}. 27 de junio de 2017 {consultado el 08 de Octubre de 2017} disponible en: (http://www.eltiempo.com/tecnosfera/novedades-tecnologia/nuevo-ataque-cibernetico-afecta-a-empresas-en-el-mundo-103092)

4 Ibid.

5 ORGANIZACIÓN DE LOS ESTADOS AMERICANOS OEA, Impacto de los incidentes de seguridad digital en Colombia 2017. {En línea}. {consultado el 08 de Octubre de 2017} disponible en: https://publications.iadb.org/bitstream/handle/11319/8552/Impacto_de_los_incidentes_de_seguridad_digital.pdf?sequence=1&isAllowed=y

6 Ibid, p. 119

7 Ibid, p. 29

los datos”[8], Colombia es uno de los países latinoamericanos que más ciberataques genera y de igual manera se ve atacado, y es que no hay una debida instrumentalización de la ley. Ante esto, se hace evidente que las empresas se blinden diseñando los controles para salvaguardar los activos de información. “En Colombia, por ejemplo, ha habido un crecimiento en la utilización de *smartphones* para transacciones financieras, y eso hace que aumente el interés de los criminales”[9].

Desde el año 2015 hasta la fecha se recibieron 15.565 incidentes informáticos a través de las plataformas dispuestas por Centro Cibernético Policial[10].

En Fusagasugá, es constante el llamado de atención por parte de entidades como la Policía Nacional, la Cámara de Comercio de Bogotá y la Secretaría de TIC de la alcaldía de Fusagasugá a que las organizaciones tomen medidas de seguridad que los protejan de los criminales físicos y virtuales.

Un incidente de seguridad se define como el acontecimiento de un suceso inesperado que pretende obtener, dañar, destruir, o realizar cualquier tipo de modificación a un bien o activo de una organización, siendo éste exitoso o no, para la obtención de un beneficio de manera ilícita; así como cualquier violación a las políticas de seguridad establecidas[11].

Existe una creciente demanda por garantizar la confidencialidad, disponibilidad e integridad de la información en los servicios informáticos debido al surgimiento de regulaciones para su protección.

Al revisar los controles de seguridad utilizando las herramientas adecuadas se puede reducir el tiempo dedicado a identificar anomalías, se puede identificar puntos importantes en la configuración de los activos informáticos para evitar comprometer

---

8 CONGRESO DE COLOMBIA, Ley 1273(5 de enero de 2009). De la protección de la información y de los datos. El Departamento. Bogotá D.C. {En línea}. {consultado el 08 de octubre de 2017} disponible en: (http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf)

9 VELÁSQUEZ DURÁN, Ana María. Colombia, entre los países con más ciberataques. En: El Tiempo. Bogotá D.C. 18, septiembre, 2017. sec. 1. p. 1. col 1. {En línea}. {consultado el 10 de noviembre de 2017} disponible en: (http://redyseguridad.fi-p.unam.mx/proyectos/politicas/desc/formato_reporte.pdf)

10 CENTRO CIBERNETICO POLICIAL, Informe: Amenazas del Cibercrimen en Colombia 2016-2017. {En línea}. Marzo 2017{consultado el 28 de octubre de 2017} disponible en: (https://caivirtual.policia.gov.co/contenido/informe-amenazas-del-cibercrimen-en-colombia-2016-2017)

11 UNAM, Reporte de incidente de seguridad informática. {En línea}. {consultado el 18 de octubre de 2017} disponible en: (http://redyseguridad.fi-p.unam.mx/proyectos/politicas/desc/formato_reporte.pdf)

la confidencialidad, integridad y disponibilidad de lo que éstos protegen, así como cuidar el cumplimiento de normas regulatorias.

Con la ejecución de este informe es posible responder adecuadamente en el procedimiento y corrección de cualquier tipo de suceso que se presente y así evitar que se vuelva recurrente, de esta manera se logrará menguar la ocurrencia de eventualidades que interrumpan los servicios, los trabajos y las actividades que se desempeñan en la empresa de Transportes Tierra Grata y Compañía Ltda. Así mismo se busca dar un seguimiento y un manejo apropiado a los diversos incidentes que se presenten.

La aplicación de este proyecto permitirá aplicar los conocimientos adquiridos en esta especialización

4. OBJETIVOS

4.1. OBJETIVO GENERAL

Diseñar los Controles de Seguridad para los Activos Informáticos en la empresa Transportes Tierra Grata y Compañía Ltda., de Fusagasugá haciendo uso de metodologías para análisis y control del riesgo, basados en la norma ISO 27001:2013.

4.2. OBJETIVOS ESPECÍFICOS

4.2.1. Identificar los riesgos, las vulnerabilidades e impactos que puedan tener los activos de información de la empresa Transportes Tierra Grata y Compañía Ltda.

4.2.2. Instaurar índices idóneos de gestión para el control de seguridad de activos informáticos que permitan una pronta detección y de respuesta a incidentes de seguridad

4.2.3. Definir controles de seguridad que posibiliten asegurar la disponibilidad, confiabilidad y continuidad de los activos, ofreciendo unos adecuados niveles de servicio

4.2.4. Realizar la Declaración de Aplicabilidad (SoA) que permite conservar el registro y control de las medidas de seguridad que se aplican socializándolos con la alta dirección de la empresa Transportes Tierra Grata y Compañía Ltda.

5. MARCO REFERENCIAL

5.1. MARCO TEÓRICO

La comunicación de las redes de una empresa y la unión de éstas a la WWW (*World Wide Web*: red informática mundial) han facilitado la realización de operaciones desde cualquier parte del mundo hacia una fuente de información común, logrando proporcionar información en tiempo real de las operaciones realizadas. Sin embargo, aunque facilitan la comunicación y son un excelente medio para compartir información; exponen la información a posibles ataques informáticos.

El reporte "*Internet Security Threat Report*, (*Symantec Corporation*, 2014)[12]"contiene un estudio anual sobre la actividad de las amenazas de todo el mundo. Entre los puntos que destaca se encuentran los siguientes:

- En 2013, las fugas de datos se acrecentaron en un 62%.
- Se expusieron más de 552 millones de identidades de clientes como resultado de las fugas de datos en 2013.
- El 38% de los usuarios de dispositivos móviles fueron víctimas de ataques informáticos en 2013.
- El volumen de spam disminuyó y representó el 66% de todo el correo electrónico.
- Los ataques basados en la web crecieron un 23%.
- 1 de cada 8 sitios web legítimos tiene vulnerabilidades críticas[13].

[12] SYMANTEC CORPORATION, Internet Security Threat Report 2014 :: Volume 19. . {En línea}. Abril de 2014 {08 de septiembre de 2017} disponible en: (http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf)

[13] AMÉRICAECONOMÍA.COM. La fuga de información es una de las razones por las que las empresas pierden más dinero. {En línea}. Julio 2016{28 de septiembre de 2017} disponible en:(https://mba.americaeconomia.com/articulos/notas/la-fuga-de-informacion-es-una-de-las-razones-por-las-que-las-empresas-pierden-mas-di)

Deloitte presentó los resultados del Estudio 2016 sobre Tendencias en Gestión de Ciber-Riesgos y Seguridad de la Información en Latinoamérica[14] donde se demuestra que las empresas Latinoamericanas se encuentran inmersas en un contexto de fuerte desarrollo de negocios digitales y de mayor exposición a las ciberamenazas inherentes a este nuevo contexto de negocios.

Allí se revela que, si bien hay un afianzamiento de la función de gestión de ciberriesgos y seguridad de la información, los encargados de administrar la seguridad de la información creen que aún no cuentan con recursos suficientes y son conscientes que tienen un largo camino por recorrer.

La implementación de capacidades de monitoreo de riesgos y de respuesta ante incidentes, y brechas de seguridad de la información son los mayores desafíos para las empresas en Latinoamérica. Esto es muy relevante teniendo en cuenta que el 40% de las empresas han sufrido una brecha de seguridad entre julio de 2014 y julio de 2016.

Para el año 2017 el *ESET Security Report* Latinoamérica 2017[15] muestra sus más altas preocupaciones al examinar cuáles son los escenarios y riesgos que más inquietan a las organizaciones de Latinoamérica, pues de aquí se parte para comenzar el diagnóstico del estado de la seguridad general de la zona. Esto es lo que arroja dicho análisis (Ver Figura 1):

- El *malware* está en el primer lugar con un 56%
- El *ransomware* alcanzó un 32%.
- La de-negación de servicios aparece con un 23% y esto debido a que muchos de estos casos son producidos por redes del tipo *botnet*[16]
- La amenaza que en 2015 estuvo en el primer lugar fue la explotación de vulnerabilidades que alcanzó un 52%.

---

14 DELOITTE, La Evolución de la Gestión de Ciber-Riesgos y Seguridad de la Información. Encuesta 2016 sobre Tendencias de Ciber-Riesgos y Seguridad de la Información en Latinoamérica. {En línea}. Julio 2016{08 de septiembre de 2017} disponible en: (https://www2.deloitte.com/content/dam/Deloitte/co/Documents/risk/Deloitte 2016 Cyber Risk Information Security Study - Latinoamérica - Resultados Generales vf.pdf)

15 ESET, Eset security report Latinoamerica 2017 {En línea}. {consultado el 28 de octubre de 2017} disponible en: (https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf)

16 Grandes redes de ordenadores infectados con una variedad de malware. KASPERSKY, Qué es un botnet?. {En línea}. {08 de septiembre de 2017} disponible en: . https://www.kaspersky.es/blog/que-es-un-botnet/755/

- El robo de información es considerado en un 43% de las organizaciones como una gran inquietud[17].

Figura 1 Comparativa de preocupaciones de acuerdo al tamaño de empresa

Empresas	Año	Malware	Fraude	Vulnerabilidad de software y sistemas	Ataque de denegación de servicio	Phishing	Acceso indebido a la información
Grandes	2015	52%	38%	60%	37%	34%	46%
	2016	55%	29%	53%	28%	28%	36%
Medianas	2015	60%	35%	60%	32%	34%	50%
	2016	56%	25%	49%	21%	27%	38%
Pequeñas	2015	55%	39%	58%	26%	28%	45%
	2016	57%	32%	51%	15%	22%	30%

Fuente: https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf

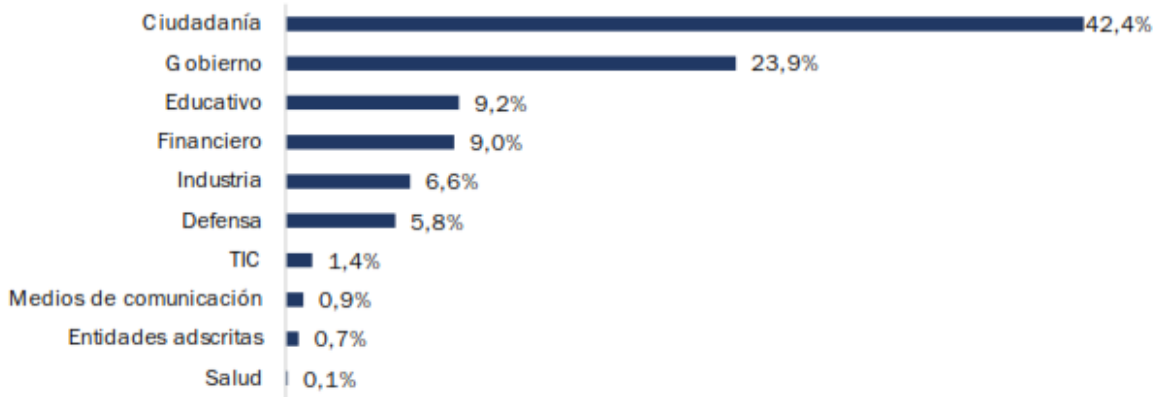
5.1.1. Riesgos en seguridad informática en Colombia. Con el uso del entorno digital también se promueven las amenazas cibernéticas, las vulnerabilidades y los incidentes digitales[18]. Situación que afecta la seguridad de los ciudadanos, de las públicas y privadas, e incluso de infraestructuras que hacen parte de los intereses de la nación. Durante los últimos años, Colombia ha sido foco de interés para distintos ataques cibernéticos, los cuales se han sofisticado trayendo consigo el incremento de la efectividad de los mismos y una mayor dificultad para su oportuna detección. Escenario que preocupa al Gobierno nacional toda vez que las condiciones para desarrollar actividades socioeconómicas en el país cada día se apoyan más en el uso de las TIC, y los incidentes digitales en Colombia afectan a varios agentes y sectores, siendo la ciudadanía la mayor afectada (Figura 2)[19].

17 Ibid, p. 4-6

18 Indicador propuesto por Katz (2015) que mide las condiciones de un país o región en cuanto a la asequibilidad, confiabilidad, accesibilidad, capacidad, utilización y capital humano de las TIC.

19 CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL CONPES, Política Nacional de Seguridad Digital. {En línea}. 11 de abril de 2016 {08 de septiembre de 2017} disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Figura 2 Sectores afectados en Colombia por incidentes digitales, 2015



Fuente: colCERT, 2015.

Durante el año 2016, la actividad maliciosa en Latinoamérica se mostró continuamente. Nicaragua se mostró con un 53%, seguido de Panamá con el 50,3% y Colombia con 46,7%.

Las *botnets* también infectaron equipos en Latinoamérica, como el caso Bondat , un código malicioso orientado al control de dispositivos de entorno Windows; la cual se popularizó principalmente a través de pendrives, aquejando a Perú, México, Colombia y Ecuador entre otros

Surgieron otros códigos maliciosos, como el *criptoransomware Locky*. El cual mostró su presencia en México, Perú, Colombia, Chile, Argentina y Guatemala.

Los sucesos por *Pishing* colocan a Colombia en el puesto 16 con un 12.6%, esto demuestra una notable protección contra campañas enfocadas en obtener contraseñas, datos bancarios e información confidencial de los usuarios a través de la suplantación de entidades reconocidas en los países donde se desarrollan estas amenazas.

5.1.2. Controles de seguridad. Los controles de seguridad más implementados en los países Latinoamericanos son el antivirus (83%), el firewall (75%) y las copias de seguridad de la información (67%).Estas tres herramientas conservan los primeros lugares en la clasificación de tecnologías de seguridad más usados.

5.1.3. Gestión de la seguridad. Las prácticas más usadas fueron el mantenimiento de políticas de seguridad (74%), las auditorías internas y/o externas (38%) y la codificación de la información (31%) (Ver Figura 3).

Figura 3 Prácticas de gestión de la seguridad más implementadas en 2016 en Latinoamérica

Fuente: https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf

Se observa que el 17% de las empresas pequeñas, el 10% de las medianas y el 6% de las grandes no adoptan estas prácticas. Esto es muy preocupante, sobre todo cuando tenemos en cuenta las consecuencias que puede conllevar para la protección del negocio. No obstante, estas cifras han disminuido en los últimos años, planteando un panorama esperanzador para el futuro.[20]

La inserción de controles tecnológicos, buenas prácticas de gestión y capacitación constante en seguridad son muy importantes al momento de salvaguardar la información crítica y, así, asegurar la continuidad del negocio.

5.1.4. Tendencias de amenazas de seguridad digital. De todas las tendencias de 2016, lo que más preocupa es la disposición de algunas personas a participar de las siguientes tres actividades a escala: secuestrar sistemas informáticos y archivos de datos (mediante ataques de *ransomware*); denegar el acceso a datos y sistemas

[20] ESET, Óp. Cit, p. 13-15

(con ataques de Denegación de Servicio Distribuido o DDoS); e infectar dispositivos que forman parte de la Internet de las Cosas (IoT, del inglés).[21]

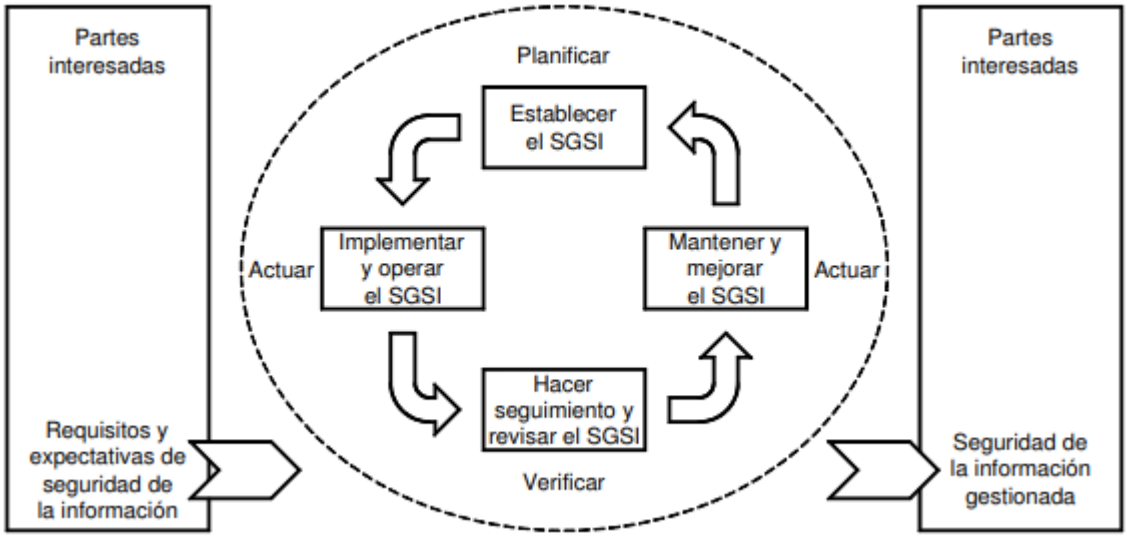
5.1.5. Norma Técnica Colombiana NTC-ISO/IEC 27001. Esta pauta fue elaborada para brindar un modelo que establezca, implemente, opere, siga, revise, mantenga y mejore un SGSI. El aplicar un SGSI al interior de las empresas debe ser una prioridad.

Es por medio de un enfoque basado en procesos para la gestión de la seguridad de la información que se estimula a sus usuarios a hacer énfasis en la importancia de comprender los requisitos de seguridad de la información del negocio implementar y operar controles para manejar los riesgos de seguridad de la información, hacer el seguimiento y revisión del desempeño y eficacia del SGSI, y establecer la mejora continua basada en la medición de objetivos.

Se adopta el modelo de procesos (PHVA), que se aplica para estructurar todos los procesos del SGSI. La Figura 4 ilustra cómo el SGSI toma como elementos de entrada los requisitos de seguridad de la información y las expectativas de las partes interesadas, y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que cumplen estos requisitos y expectativas.

[21] ESET, Eset Tendencias Latinoamérica 2017 {En línea}. {consultado el 28 de octubre de 2017} disponible en: (https://www.welivesecurity.com/wp-content/uploads/2016/12/Tendencias-2017-eset.pdf)

Figura 4 Modelo PHVA (“Planificar-Hacer-Verificar-Actuar”) aplicado a los procesos de SGSI



Fuente: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

“Planificar-Hacer-Verificar-Actuar” (PHVA)

- Planificar (establecer el SGSI) Establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización.
- Hacer (implementar y operar el SGSI) Implementar y operar la política, los controles, procesos y procedimientos del SGSI.
- Verificar (hacer seguimiento y revisar el SGSI) Evaluar, y, en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión.
- Actuar (mantener y mejorar el SGSI) Emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna del SGSI y la revisión por la dirección, para lograr la mejora continua del SGSI.[22]

[22] COLOMBIA. ICONTEC. NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. Norma Técnica Colombiana, 2006.

5.2. MARCO CONCEPTUAL

La información es el activo más importante de cualquier entidad y, para ella, deben preexistir protocolos que aseguren su acceso tanto de forma física como a su almacenamiento. Este acceso a ésta debe estar definido dentro de barreras y procedimientos que la resguarde, acceso que solo debe ser permitido única y exclusivamente a personal autorizado.

Hoy en día debido a la gran cantidad de puertas y ventanas que se abren con los diferentes dispositivos que se conectan a las redes, la información se convierte en un blanco de ataques y búsquedas de debilidades tales como fraude electrónico, robo de identidad, denegación de servicios, etc.

Por ende, la organización debe plantear una buena gestión de seguridad tanto lógica como física a través de planes de contingencia, políticas de seguridad y aplicación de normativas.

5.2.1 Características de un Sistema Seguro. Las características de un sistema seguro son las siguientes

- Confidencialidad: Los componentes del sistema serán accesibles sólo por aquellos usuarios autorizados.
- Integridad: Los componentes del sistema sólo pueden ser creados y modificados por los usuarios autorizados.
- Disponibilidad: Los usuarios deben tener disponibles todos los componentes del sistema cuando los necesiten. También se entiende como la capacidad de un sistema para recuperarse rápidamente en caso de ocurrencia de algún problema.[23]

Además, se relacionan, por su composición teórica a este proyecto los siguientes conceptos:

[23] AGUIRRE, Jorge Ramió Libro Electrónico de Seguridad Informática y Criptografía v4.1. Capítulo 3: Introducción a la Seguridad Informática. Madrid - España. Universidad Politécnica de Madrid, p. 75 {En línea}. {consultado el 30 de octubre de 2017} disponible en: (http://deic.uab.es/material/26118-03IntroSegInfo.pdf)

Control de acceso a los recursos: Regulación de quién utiliza el sistema o cualquiera de los recursos que ofrece y cómo lo hace.

Metodología Magerit: METODOLOGIA MAGERIT: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los SI Libro III - Guía de Técnicas. MAGERIT es la metodología propuesta en el caso de estudio realizado, para conocer las amenazas a los cuales se encuentran expuestos los activos que forman parte de la empresa Transportes Tierra Grata y Compañía Ltda., mediante un análisis de riesgos de orden cualitativo se busca conocer el nivel de madurez en la seguridad aplicada en la empresa para finalmente sugerir las salvaguardas necesarias para reducir los niveles de riesgo e impacto.[24]

Metodología y guía de referencia para realizar procesos de análisis de riesgos al igual que lineamientos para la gestión de riesgos en sistemas informáticos y todos los aspectos que giran alrededor de ellos en las empresas para lograr las metas planteadas al interior de las mismas y buscando cumplir las políticas de buen gobierno. En esta metodología se puede efectuar el proceso de análisis de riesgos identificando los activos, las amenazas, se determinan los riesgos como los impactos potenciales y se recomienda como proceder a elegir las salvaguardas o contra medidas para minimizar los riesgos.

Los pasos a seguir en la Metodología

- Definición de los Activos: Inventariar equipos de cómputo, de red, software y mobiliario, y así determinar cuál es la información crítica que se tiene que resguardar, además inventariar los servicios de cómputo, telecomunicaciones, internet, etc., que son requeridos para que los usuarios puedan llevar a cabo sus actividades normales.

- Determinación de Amenazas: Cuando se determina una amenaza que afecta a un activo, se debe valorar su dominio en el valor del activo, por un lado, por degradación (conocer cuán perjudicado resultaría el activo) y por otro lado la probabilidad (cuán probable o improbable es que se plasme la amenaza). La probabilidad de ocurrencia se modela de forma cualitativa y cuantitativa.

[24] MOLINA MIRANDA, María Fernanda. Propuesta de un Plan de Gestión de Riesgos de Tecnología aplicado en la Escuela Superior Politécnica del Litoral. Trabajo de Grado Máster Universitario en Ingeniería de Redes y Servicios Telemáticos. Madrid - España. Universidad Politécnica de Madrid - Escuela Técnica Superior de Ingenieros de Telecomunicación, 2015, p. 25-26 {En línea}. {consultado el 28 de octubre de 2017} disponible en: (http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Maria_Fernanda_Molina_Miranda_2015.pdf)

- Determinación de las Salvaguardas: Son los procedimientos o mecanismos tecnológicos que reducen el riesgo. Se hace revisión de la seguridad, controles físicos y ambientales existentes, evaluando si son adecuados respecto a las posibles amenazas. Se debe estar preparado para cualquier percance, verificando que dentro de la organización se cuente con los elementos necesarios para salvaguardar sus activos.

- Calcular el Impacto Residual: El impacto residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores. El sistema queda en una situación de posible impacto cuando en su proceso de gestión existe un conjunto de salvaguardas desplegadas y una medida de madurez.

- Calcular el Riesgo Residual: El sistema queda en una situación de posible riesgo cuando en su proceso de gestión existe un conjunto de salvaguardas desplegadas y una medida de madurez. [25]

Técnica de recolección y procesamiento de datos

- Se iniciará con un proceso de Observación, de esta forma se extrae y se valida la información obtenida, haciendo aclimatación con los componentes físicos de las diferentes áreas de la empresa, calculando el tiempo de ejecución de cada proceso, anotando lo observado evitando generalizaciones, siendo especifico y sobre todo validando las reglas de seguridad del área. Luego vendrán las Entrevistas, estas permitirán conocer datos que no están disponibles de ninguna otra forma, el preguntar específicamente conlleva a respuestas cuantitativas, evitando divagaciones y comentarios al margen de la investigación, se escucha atentamente lo que se dice y evitando anticiparse a las respuestas recibidas, con todo esto aplicado la consecuencia será la recolección y documentación de los resultados obtenidos y el archivo como referencia y para análisis posteriores.

SGSI[26]: Sistema de gestión de la seguridad de la información, es un sistema que se encarga de proveer una cantidad de mecanismos y herramientas basados en la

[25] Ibid, p. 36-37

[26] COLOMBIA. ICONTEC. Compendio: Sistema de gestión de la seguridad de la información (SGSI) Norma Técnica Colombiana, 2009.

norma ISO 27001 y tiene por objetivo conocer al interior de la Empresa a los que puede estar expuesta la información, define como se deben gestionar los riesgos y debe ser un marco de referencia para la Empresa el cual debe ser conocido por todo el personal y debe estar sometido a una revisión y a un proceso de mejora constante.

La información. Uno de los elementos esenciales dentro de una empresa. La seguridad de la información debe ser administrada según los criterios establecidos por los administradores y personal capacitado, previendo que usuarios externos y no autorizados puedan acceder a ella sin autorización.

La infraestructura computacional. Parte esencial para gestionar, administrar y almacenar la información indispensable dentro del normal funcionamiento de la Empresa. El papel que desempeña la seguridad informática en este punto es velar que el hardware (parte física) tengan un óptimo funcionamiento y logre evitar problemas relacionados con robo, incendios, desastres naturales, bloqueos, fallas en el suministro eléctrico, vandalismo, entre otros que lleguen a afectar directamente la infraestructura informática.

Los usuarios. Son las personas que están directamente involucradas con la infraestructura tecnológica, comunicaciones y administradores de la información. La seguridad informática debe establecer normas que minimicen los riesgos tanto de información como de su infraestructura, dentro de dichas normas de debe contemplar, horarios de acceso, restricciones físicas y lógicas, permisos, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo esto debe estar regido por estándares y normas que minimicen los riesgos y el impacto en caso de llegar a presentar un siniestro[27]

5.3 MARCO LEGAL

Con el fin reducir los riesgos de amenazas y ataques a los que se encuentra expuesta la empresa de Transportes Tierra Grata y Compañía Ltda. se propone hacer el diseño de Controles de Seguridad en los Activos Informáticos y así cumplir la normatividad establecida en la ley 1581: de Protección de Datos Personales de

[27] PERAFÁN RUIZ, John Jairo. CAICEDO CUCHIMBA, Mildred, Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca. Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas Tecnología e Ingeniería. Especialización en Seguridad Informática. Popayán. 2014 {En línea}. {consultado el 09 de octubre de 2017} disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/2655/3/76327474.pdf

2012[28], la ley 527: acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales[29], el decreto 886 de 2014: donde se reglamentó el Registro Nacional de Bases de Datos (RNBD) ante la Superintendencia de Industria y Comercio (SIC)[30] y la Ley 1273 de 2009 de la Protección de la información y de los datos. Además de proteger los activos informáticos e información crítica y sensitiva, establecer un Diseño de Controles de Seguridad en Activos Informáticos basados en la norma ISO 27001:2013[31], lo cual permitirá que la empresa de Transportes Tierra Grata y Compañía Ltda. utilice prácticas adecuadas de seguridad de la información, haciendo que sus empleados se concienticen sobre los riesgos y amenazas presentes a través de prácticas, procedimientos, guías y lineamientos documentados y liderados por las directivas.

5.4 MARCO CONTEXTUAL

El proyecto se aplica en la empresa Transportes Tierra Grata y Compañía Ltda. que tiene como sede principal la oficina en la Ciudad de Fusagasugá donde se concentra la planta administrativa, además cuenta con una oficina y una taquilla en el Terminal de Transportes de Fusagasugá, Una taquilla en la Terminal de Transportes del Salitre en Bogotá y otra taquilla en el Terminal del Sur de Bogotá.

El proyecto tiene una duración de 4 meses comprendidos en el primer semestre del año 2018

5.4.1 Transportes Tierra Grata y Cia Ltda

5.4.1.1 Imagen Corporativa

---

28 COLOMBIA. MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO, Decreto 1377 (27 de junio de 2013) Protección de Datos Personales. Presidencia. Bogotá D.C. {En línea}. {consultado el 09 de octubre de 2017} disponible en: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

29 CONGRESO DE COLOMBIA, Ley 527 (21 de agosto de 1999) Acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales. El Departamento. Bogotá D.C {En línea}. {consultado el 08 de octubre de 2017} disponible en: http://www.mintic.gov.co/portal/604/articles-3679_documento.pdf

30 COLOMBIA. MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO, Decreto 886 (13 de mayo de 2014) Protección de la información y de los datos. Presidencia. Bogotá D.C. {En línea}. {consultado el 08 de octubre de 2017} disponible en: http://wsp.presidencia.gov.co/Normativa/Decretos/2014/Documents/MAYO/13/DECRETO%20886%20DEL%2013%20DE%20MAYO%20DE%202014.pdf

31 EL PORTAL DE ISO 27001 EN ESPAÑOL, ISO 27000 Sistemas de gestión de seguridad de la información. {En línea}. {08 de septiembre de 2017} disponible en: (http://www.iso27000.es/iso27000.html)

Figura 5 Logo de la Empresa.

Fuente: Archivo de Transportes Tierra Grata y Compañía Ltda.

5.4.1.2 Misión. Ser líderes en la prestación del servicio de transporte público terrestre urbano e intermunicipal de pasajeros, contando con excelente equipo e instalaciones físicas adecuadas y un servicio de mantenimiento integral que garantice el normal funcionamiento del parque automotor y con un grupo humano comprometido con su labor, en beneficio de la comunidad.

5.4.1.3 Visión. Poseer un parque automotor que cumpla las necesidades del servicio de transporte terrestre de pasajeros aunado a la calidad de prestación del servicio con eficiencia y responsabilidad, siendo esta una empresa que permita dar solución a la problemática en el servicio terrestre de pasajeros urbano e intermunicipal.

5.4.1.4 Actividad Económica. La actividad económica de TRANSPORTES TIERRA GRATA S.A. Y CÍA. LTDA. , es la administración de transporte terrestre urbano e intermunicipal de pasajeros, por medio de vehículos automotores como microbuses y taxis. Constituye igualmente, objeto de la empresa, la compra de combustible, lubricantes, accesorios y demás artículos para vehículos automotores.

5.4.1.5 Recuento Histórico. La empresa TRANSPORTES TIERRA GRATA S.A. Y CÍA. LTDA. es una empresa que fue creada en 1983, con la unión de 12 personas propietarios de automotores, quienes decidieron establecerse como organización que prestaría un servicio de transporte terrestre urbano de personas en el municipio de Fusagasugá.

Se continuó trabajando hasta 1988, tan solo con el permiso de la oficina de transporte del municipio de Fusagasugá, año en el cual se crea la sociedad y se inscribe como sociedad LTDA, ante la cámara de comercio de Bogotá, bajo el número de registro mercantil 00342648.

En los años de 1992 y 1993 la empresa alcanza un crecimiento influenciado por tres factores específicos:

- El gran aumento de demanda en el servicio de transporte terrestre de la principal ruta Cementerio – Centro – Siboney.
- La creación del servicio de transporte terrestre intermunicipal entre la ciudad de Fusagasugá - Santa Fe De Bogotá - Fusagasugá.
- La autorización de la licencia de funcionamiento de la empresa Transporte Tierra Grata y CIA LTDA, por medio de la resolución Nº. 04419 del 21 de septiembre de 1993, expedida por el Instituto Nacional De Transporte.

La empresa inició con los doce dueños de vehículos, quienes tenían a cargo cada uno el mantenimiento de su carro, entre ellos estaban divididos los cargos administrativos teniendo como gerente el señor HECTOR EMILIO LOPEZ, quien luego se desempeñó como tesorero de la organización.

Ante el vertiginoso crecimiento de la empresa se realizó una reestructuración administrativa que fortaleció el desarrollo de la organización en la ciudad de Fusagasugá.

Las estrategias que implementó la empresa de TRANSPORTE TIERRA GRATA LTDA, en la prestación del servicio de transporte urbano en la ciudad de Fusagasugá se destacaron por:

La prestación de un servicio amable y eficiente en las diferentes rutas cubiertas por la empresa mediante el confort que se prestaba con unos automotores en buen estado, con exactitud y cumplimiento con los horarios preestablecidos que hacían que el cliente utilizara el servicio.

En cuanto a la prestación del servicio, en su comienzo fue con taxis y con el tiempo los socios afiliaron microbuses para satisfacer la demanda con mayor eficiencia, mayor cubrimiento, aumentar el nivel de ingresos de los socios, lograr un mayor

posicionamiento en el mercado, mediante la política de contar con un parque automotor con una antigüedad no mayor a 5 años.

En los vehículos no se admite sobre cupo de pasajeros, y los horarios de salida establecidos se deben cumplir con exactitud para cada ruta. Además, se mejoraron las condiciones de vida y en especial de salud de todos los pasajeros.

La empresa tierra grata ha aumentado su parque automotor en los últimos años, pero no han tenido grandes manifestaciones tecnológicas en lo referente a los procesos administrativos ni al servicio de transporte en sí, la mayoría de procesos se hacen manualmente como llevar las planillas, venta de tiquetes, control de horarios y rutas.

5.4.1.6 Ubicación: La Gerencia de la empresa Transportes Tierra Grata S.A. y Cía. Ltda., se encuentra situada en el departamento de CUNDINAMARCA, en el municipio de Fusagasugá y su dirección postal es Calle 19 # 10-12, teléfono (1)8717185. En el Terminal de Transportes de Fusagasugá en la Taquilla 7 , Tel.8671841. Y en Bogotá en el Terminal de Transportes - Módulo Amarillo , en la Taquilla No. 128 A , Tel. 5708880

5.4.1.7 Entorno físico. Transportes Tierra Grata S.A. y Cia Ltda, es una empresa PYME, su estructura física está compuesta de la siguiente forma:

- 1 oficina ubicada en el centro de Fusagasugá (10 pcs, sistema de cámaras)
- 1 oficina en el Terminal de Transportes de Fusagasugá (1 pc con internet)
- 1 oficina en el Terminal de Transportes de Bogotá, (1 pc con internet)
- 1 oficina en el Terminal del Sur de Bogotá, (1 pc con internet)
- 1 ruta Fusagasugá - Bogotá y viceversa
- 40 rutas de busetas y microbuses y 3 rutas de taxis Colectivos

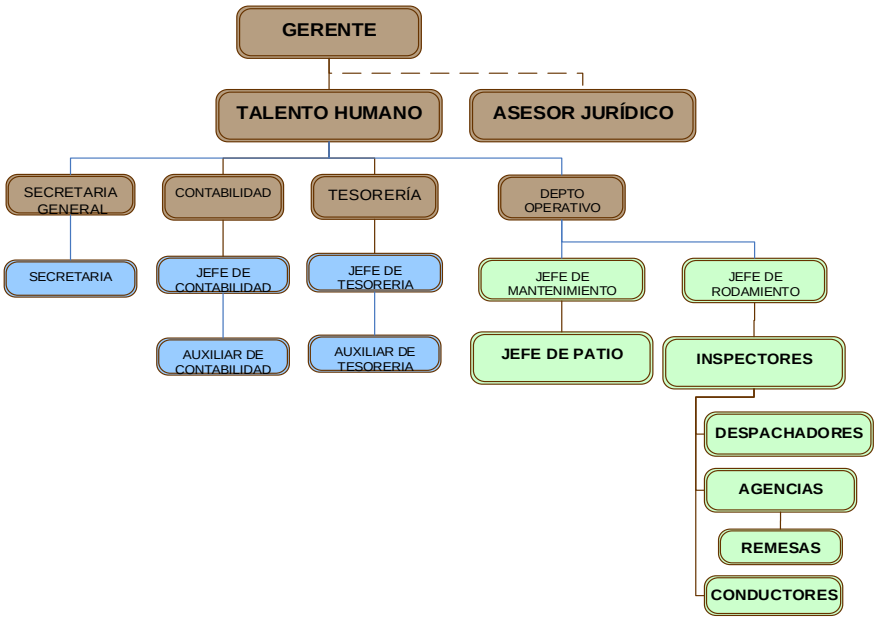
En cada una de las oficinas hay equipos de cómputo, pero solo en la oficina del centro de Fusagasugá hay una LAN compuesta por 10 PC´s que no ha tenido renovación en unos 5 años y tienen bastantes problemas de conectividad, alterno hay un servicio de cámaras de conexión IP conectadas a un pc, pero no se pueden verificar por Internet.

En el Anexo F se encuentra descrita la captura de requisitos de la empresa Transportes Tierra Grata S.A. y Cía. Ltda.

5.4.1.8 Organigrama. En la Figura 6 se presenta la estructura orgánica para el cumplimiento de los objetivos y funciones establecidas en los estatutos que rigen la empresa.

Transportes Tierra Grata S.A. y Cía. Ltda., se compone por 1 sede principal ubicada en el perímetro urbano de la ciudad de Fusagasugá, una oficina y una taquilla ubicadas en el Terminal de Transportes de Fusagasugá, una taquilla ubicada en el Terminal de Transportes de Bogotá y una taquilla ubicada en el Terminal satélite del Sur de Bogotá; siendo la sede principal donde se están ubicados la mayor parte departamentos que conforman la empresa.

Figura 6 Organigrama Organizacional de Transportes Tierra Grata S.A. y Cía. Ltda.



Fuente: El Autor

Sus Departamentos son: Gerencia, Recursos Humanos, Contabilidad, Pagaduría, Operatividad. Son más o menos 20 empleados afiliados a la empresa, los demás

son personas asignadas por los dueños de los carros ya que estos no son de propiedad de la empresa.

La empresa opera con 15 Vehículos intermunicipales (Ruta Fusagasugá - Bogotá y viceversa) y 74 vehículos urbanos distribuidos en 40 Rutas de busetas y microbuses y 3 rutas de taxis Colectivos. Solo los vehículos intermunicipales tienen servicio de GPS. Para los vehículos urbanos hay puestos de control distribuidos por toda la ciudad donde hay un operador que controla. La comunicación entre oficinas se hace por celular, ya que no hay una red que comunique las estructuras, todo se centraliza en las Oficinas del Centro de Fusagasugá, pero no hay un buen sistema de seguridad para la información ya que se comparte el servicio de internet con empresas vecinas. No hay radioperador entre vehículos

5.4.1.9. Estado de la seguridad de la información. Se utiliza el software contable Helisa sobre DOS, el cual ya es obsoleto y genera muchas demoras en la entrega de los informes. Para el control de personal todo se lleva en papel. La venta de tiquetes se hace a mano. En estos momentos se está haciendo la migración al software contable SIIGO.

Con el fin de conocer los aspectos generales en cuanto al tema de seguridad de la información en la empresa Transportes Tierra Grata S.A. y Cía. Ltda. y conocer las percepciones frente al tema de algunos de los miembros de la organización, se aplicó el cuestionario desarrollado por la Asociación Colombiana de Ingenieros de Sistemas (Acis): Encuesta Nacional de Seguridad Informática 2017[32]. El formato del cuestionario se encuentra en el Anexo D del presente documento.

Los datos recopilados en el 2017 afirman que el 73% de las empresas considera que es necesario que sus juntas directivas se actualicen en temas como la seguridad de la información. De esta manera, puede hacer mejor comprensión acerca de los desafíos de las compañías al enfrentarse en caso de ataques electrónicos.

En la encuesta realizada el año pasado se encontraron cifras como que el 42% de las empresas colombianas no cuentan con un grupo de trabajo específico o un centro de operaciones de ciberseguridad que monitoree el comportamiento, amenazas y ataques a sus sistemas de información. Además, el 56% de las

[32] ALMANZA JUNCO, Andres Ricardo. Encuesta nacional de seguridad informática 2017. En: Revista Sistemas [en línea]. [consultado 2 abr. 2018]. Disponible en: < http://acis.org.co/revista143/content/encuesta-nacional-de-seguridad-inform%C3%A1tica-2017>

compañías encuestadas a nivel global están preocupadas por el creciente impacto de las ciberammenazas para sus estrategias y planes de negocio.[33]

5.4.1.10. Aplicación del cuestionario. El cuestionario se aplicó a personal de los siguientes grupos:

La dirección y el departamento responsable por la gestión del riesgo operativo de la compañía:

El cuestionario permite proceder a un examen informal de la situación en cuanto a la seguridad de sus sistemas de información. Esta aproximación de alto nivel permite obtener una primera visión de los objetivos concretos y las opciones que tendrían que subyacer a la elaboración del proyecto.

Área de informática:

El cuestionario permite obtener una panorámica técnica para la elaboración del proyecto. Teniendo en cuenta lo anterior se aplicó el cuestionario a las siguientes personas que hacen parte de los grupos anteriormente mencionados:

- Jorge Humberto Pulido Pardo (Gerente) Responsable de la Dirección
- Francisco Alberto Benítez Manjarrez (Jefe de Contabilidad) –
- Fabio Penagos Moreno (Jefe Operativo Intermunicipal)
- José Arnulfo Beltrán Sánchez (Jefe Operativo Urbano)
- Ingeniero Yon Iván Márquez Buitrago (Jefe de Sistemas) – Responsable del área de informática

Se pidió a las personas entrevistadas que respondieran a las preguntas del cuestionario de acuerdo a su opinión y conocimiento de la organización, y que en caso de no conocer la respuesta a alguna de las preguntas sencillamente colocaran las palabras: “no sé”.

[33] Encuesta anual sobre el estado de la seguridad de la información 2017, un estudio mundial de la organización EY. En: www.enter.com [en línea]. [consultado 2 abr. 2018]. Disponible en: < http://www.enter.co/especiales/empresas/encuesta-global-de-ciberseguridad/>

5.4.1.11. Resultados de la aplicación del cuestionario. El cuestionario aplicado se encuentra dividido en las siguientes secciones:

- Sección I: Información General
- Sección II: Las implicaciones de la depresión del mercado actual en la función de seguridad.
- Sección III: Arquitectura y tecnología de seguridad
- Sección IV: incidentes relacionados con la seguridad durante el año pasado
- Sección V: Planeación, políticas y procedimientos de seguridad

De las respuestas al cuestionario y de las entrevistas mantenidas con los responsables anteriores, se obtiene una primera aproximación sobre las funciones, los servicios y los productos implicados en cuestiones de seguridad.

A. Sección I: Información General

Lo primero que hay que destacar de los resultados obtenidos del cuestionario es que quienes lo contestaron consideran que la privacidad y la continuidad del negocio hacen parte de la responsabilidad de la organización. Por otra parte, aunque existe un esfuerzo por adaptar el presupuesto al mercado cambiante, la seguridad de información es aún una prioridad, muestra de ello es que comparado con el año 2017 se estima que el gasto en seguridad de la empresa aumentará hasta un máximo de 8% para el 2018, tal como se muestra en la Tabla 1, donde se observa la planeación del gasto en seguridad de la información de la empresa Transportes Tierra Grata S.A. y Cía. Ltda. frente a la Empresa Colombiana.

Tabla 1. Planeación del gasto en seguridad de la información de la empresa

Comparado con el año 2017, para el 2018 el gasto en seguridad	**Empresa Colombiana**	**Transportes Tierra Grata S.A. y Cía. Ltda.**
Aumentará	6%	SI (hasta un máximo de 8%)
Permanecerá	80%	NO
Disminuirá	14%	NO
Fuente: El Autor		

B. Sección II: Las implicaciones de la depresión del mercado actual en la función de seguridad

Frente a la crisis de los mercados que se vive actualmente, hay que destacar que en materia de seguridad de la información el ambiente normativo se ha hecho más complejo y gravoso para la empresa Transportes Tierra Grata S.A. y Cía. Ltda. y aunque según los entrevistados las amenazas a la seguridad de los recursos no han aumentado y los riesgos debido al debilitamiento de proveedores y socios comerciales tampoco presentan un incremento, la función de seguridad cada vez tiene un papel más importante en la empresa.

Para cumplir con los objetivos de seguridad de la compañía en el contexto de una realidad económica más difícil, las siguientes estrategias se destacan por considerarse las más importantes para los entrevistados:

- Incrementar la protección de la información
- Mejorar la administración de privilegios
- Asignar prioridades a inversiones de seguridad con base en el riesgo
- Adoptar un marco de trabajo de seguridad reconocido, como medio para preparar requerimientos regulatorios futuros.
- Enfocarse en el núcleo de la estrategia de seguridad de la información existente.
- Reducir, mitigar o transferir riesgos mayores

C. Sección III: Arquitectura y tecnologías de seguridad

En esta sección del cuestionario se identificaron algunos elementos que pueden tener un impacto en el perfil de seguridad de la organización; esta información se complementó con una revisión de la documentación de la empresa, del software, los diagramas de red, así como de los procedimientos que actualmente operan en ella:

Hallazgos:

Evaluación de riesgos:

- En de la empresa Transportes Tierra Grata S.A. y Cía. Ltda., los riesgos empresariales no se habían evaluado antes y por ello no existe una medición específica de los riesgos referentes a la seguridad de la información.

Salvaguardas para la privacidad de la información:

- No se ofrece una capacitación sobre políticas y prácticas de privacidad.
- No existe un inventario preciso de donde se recogen, transmiten y almacenan los datos de los empleados y clientes.
- No existe un contrato de confidencialidad que se hace firmar a los terceros con el fin de proteger la información de clientes y de la compañía, así como la propiedad intelectual de esta.
- Los siguientes son algunos de los controles que no existen en la compañía para proteger la privacidad:

  Dispositivos externos bloqueados (Por ejemplo, USB, CD, DVD entre otros)
  Controles de acceso actualizados
  Transmisiones de datos cifrados

Salvaguardas de seguridad de la información relacionadas con personas:

- La compañía no emplea guardias de seguridad, así como otras medidas de seguridad físicas para la infraestructura de información
- Los antecedentes del personal son verificados.
- La compañía tiene gente dedicada ofrecer programas de concientización del empleado en las políticas, procedimientos y estándares técnicos internos.

Salvaguardas de proceso de seguridad de la información:

- No existen lineamientos básicos de seguridad establecidos para socios, clientes y proveedores.
- No existen estándares ni procedimientos establecidos para el despliegue de la infraestructura.
- No existe una estrategia implementada de gestión de identidades, sin embargo, esta es una prioridad para la empresa para los próximos 12 meses.
- La compañía no cuenta con un plan de recuperación de desastres empresariales documentado.

Salvaguardas de tecnología, en la Tabla 2 podemos observar las salvaguardas de tecnología de la empresa Transportes Tierra Grata S.A. y Cía. Ltda

Tabla 2. Salvaguardas de tecnología de la empresa

Actualmente la compañía implementa	**No implementa pero es una prioridad para los próximos 12 meses**
Firewall de redes	Firewall de aplicaciones
Herramientas de monitoreo de actividad de los usuarios	Restablecimiento de contraseñas automatizado
Cifrado en: base de datos, cintas de respaldo, computadoras portátiles y medios extraíbles.	Servidores seguros
Herramientas de detección de código malicioso (*spyware*, *adware*)	Acceso remoto seguro
Herramientas para detectar dispositivos no autorizados	
Herramientas de detección de intrusiones	
Herramientas de escaneo de vulnerabilidad	
Herramientas de administración de actualizaciones a las aplicaciones	
Herramientas de prevención de intrusiones	
Tecnologías de seguridad compatibles con intercambios de web 2.0.	
Software de control de acceso a la PC	
Seguridad de VoIP (voz sobre IP)	
Fuente: El Autor	

D. Sección IV: Incidentes relacionados con la seguridad durante el año 2017

Esta sección se enfoca en los incidentes de seguridad de la información que afectaron la organización durante los últimos 12 meses.

En la empresa Transportes Tierra Grata S.A. y Cía. Ltda., no se lleva un registro de los incidentes relacionados con seguridad, por lo tanto, la empresa no conoce que incidentes ocurrieron ni la fuente probable de los mismos. Al revisar el escenario de incidentes en la realidad nacional, encontramos: El 29% de los encuestados manifiesta no saber si la organización maneja sus incidentes o cómo los maneja. Y el porcentaje significativamente superior, 71%, está relacionado con la presencia de

incidentes de seguridad dentro de las organizaciones. El 20% de la misma población manifiesta haber manejado entre 1 y 3 incidentes, y el 17%, más de 7.[34]

E. Sección V: Planeación, políticas y procedimientos de seguridad

En la empresa Transportes Tierra Grata S.A. y Cía. Ltda., se destaca la carencia de una estrategia global de seguridad de la información con un proceso de administración centralizado; esto se refleja en la divergencia de las respuestas de los entrevistados frente a lo que cada uno de ellos considera como los elementos con los que cuenta la empresa en su perfil de seguridad.

Puntos de referencia de seguridad de la información seleccionados, a los cuales se evidencia una total ignorancia al respecto:

- Tiene una estrategia global de seguridad de la información
- Tiene un proceso de administración de la seguridad de la información centralizado
- Involucra tanto a los ejecutivos de negocios a los de tecnología de la información en abordar la seguridad.
- Integra los planes de cumplimiento y privacidad

Hallazgos:

Debido a las diferencias encontradas en las respuestas ofrecidas por los entrevistados en esta sección, se llevó a cabo un estudio más detallado al interior de la organización, sobre los puntos divergentes. Para este estudio se revisó la documentación de procesos y políticas de la compañía, y se complementó con las respuestas de los entrevistados para determinar los siguientes hallazgos:

- Los asuntos de seguridad de la información no son tratados ni por los encargados del área de negocios ni los del área de tecnología.
- La compañía no mide ni revisa la eficacia de sus políticas y procedimientos de seguridad de la información ya que no las posee.

[34] Encuesta anual sobre el estado de la seguridad de la información 2017, un estudio mundial de la organización EY. En: www.enter.com [en línea]. [consultado 2 abr. 2018]. Disponible en: < http://www.enter.co/especiales/empresas/encuesta-global-de-ciberseguridad/>

- No existe una política de seguridad de la información escrita, pero se propone una política de sistemas, con los siguientes elementos, los cuales se muestran en la Tabla 3 como Elementos de la Propuesta a Política de Sistemas de empresa Transportes Tierra Grata S.A. y Cía. Ltda.

Tabla 3. Elementos de la Propuesta a Política de Sistemas de empresa

Elementos contemplados dentro de la política de sistemas	**Elementos no contemplados dentro de la política de sistemas**
Continuidad del negocio	Segregación de tareas
Administración de usuarios	Administración de cambios
Control de accesos	Seguridad en desarrollo de sistemas
Seguridad física	Clasificación del valor comercial de los datos
Administración de seguridad de redes	Inventario de activos de información
Estándares técnicos de configuración de seguridad	Protección, divulgación y destrucción de datos
Procedimientos destinados a proteger la propiedad intelectual.	Respuesta a incidentes
	Evaluación de riesgos de seguridad
	Uso apropiado de la tecnología (internet, correo electrónico, entre otros)
	Capacitación de concientización de seguridad y comunicaciones del usuario final.
	Administración de parches
	Reportes de recolección y administración de criterios de seguridad.
	Uso de tecnologías Web 2.0 y acceso y publicación en redes de socialización
	Mecanismo de cumplimiento de normas
	Monitoreo de contenidos
Fuente: El Autor	

- La empresa no clasifica los activos de datos e información
- Los principales factores que impulsan el gasto en seguridad de la información son:
    - Los planes de continuidad para asegurar la recuperación de desastres empresariales
    - El cumplimiento regulatorio
- No existe una forma de medir la eficiencia del gasto en seguridad de la información de la compañía.

Resultados Consolidados del Diagnóstico

Después de ubicar a la empresa Transportes Tierra Grata S.A. y Cía. Ltda., dentro de su contexto corporativo, económico y legislativo, y de evaluar con conocedores del negocio su situación frente a la seguridad de la información se consolidó un diagnóstico inicial de la compañía mediante el siguiente análisis DOFA, que se muestra en la Tabla 4:

Tabla 4. Análisis DOFA de la Seguridad de la información en empresa

Debilidades	**Fortalezas**
• Carencia de una estrategia global de seguridad de la información con un proceso de administración centralizado • No existe una política de seguridad de la información escrita • Desconocimiento de los activos de datos e información y no clasificación de estos • No existe una medición específica de los riesgos referentes a la seguridad de la información. • Desconocimiento de los incidentes relacionados con seguridad de la información. • Pobre despliegue de salvaguardas de procesos y personas • No existen procedimientos establecidos para el despliegue de la infraestructura • La compañía no mide ni revisa la eficacia de sus políticas y procedimientos de seguridad de la información. • No existe una forma de medir la eficiencia del gasto en seguridad de la información de la compañía. • No hay despliegue de salvaguardas de tecnología • No existen programas de capacitación sobre políticas y prácticas de seguridad de la información • Los asuntos de seguridad de la información no son tratados ni por los encargados del área de negocios ni los del área de tecnología.	• La privacidad y continuidad del negocio es considerada una parte importante de la responsabilidad de la empresa • La empresa evalúa sus riesgos empresariales • Existen lineamientos básicos de seguridad establecidos para socios, clientes y proveedores • Existencia de un plan de continuidad del negocio en caso de desastres empresariales. •

Tabla 4. (Continuación)

Oportunidades	Amenazas
• La empresa cuenta con un nivel alto de capital debido al crecimiento registrado en los últimos años. • La empresa cuenta con una buena posición en el mercado. • Fuertes alianzas estratégicas con proveedores • Los márgenes de ganancia de la compañía son altos. • Los avances en el tema de seguridad de la información cada vez son más accesibles. • El gobierno nacional se encuentra desarrollando nuevos programas y políticas orientados a promover el uso de las tecnologías de la información y la seguridad de la información en la nación.	• El ambiente normativo y legislativo se ha hecho más complejo y gravoso para la empresa. Se han introducido nuevas exigencias regulatorias en cuanto a seguridad de la información. • La reforma financiera trae cambios para el sector que aumentarán la competencia. • Existe una crisis financiera a nivel mundial que afecta la capacidad de pago de los clientes. (aumenta la posibilidad de fraude, se hace necesario contar con información fiable de ubicación de los clientes) • El mercado objetivo de Transportes Tierra Grata S.A. y Cía. Ltda. tiene un nivel alto de riesgo • Baja capacidad de retención del personal clave (se pueden generar fugas de información y pérdida de *know how*)
Fuente: El Autor	

A partir de diagnóstico se detectan las siguientes necesidades frente a la seguridad de la información por parte de empresa Transportes Tierra Grata S.A. y Cía. Ltda:

- Adoptar una estrategia global de seguridad de la información
- Prepararse para enfrentar el ambiente normativo que viene desarrollándose en torno a la seguridad de la información
- Administrar de una forma más eficaz las salvaguardas tecnológicas existentes

Un Sistema de Gestión de Seguridad de la Información brinda las herramientas necesarias para afrontar estas necesidades, después de conocer las características de la empresa se establece como alcance inicial del sistema de gestión la información manejada en los procesos misionales del negocio, específicamente en el proceso de Colocación, y los sistemas informáticos donde esta es depositada y manejada. Es preciso señalar que la empresa efectúa operaciones en Bogotá y Fusagasugá; sin embargo, el proyecto se centrará en las operaciones realizadas en Fusagasugá debido a que allí se encuentra una mayor concentración de la

infraestructura tecnológica y de procesos, tal que al ser analizada cubre los aspectos más relevantes de otras sucursales.

Finalmente se debe hacer un análisis de riesgos sobre los activos de información del alcance, para determinar junto con la información ya recopilada los requisitos de seguridad información de la compañía, que en última instancia servirán de guía para todo el sistema.

Adicionalmente el análisis de riesgos es un paso indispensable para gestionar los procesos de seguridad de la información, de manera que las acciones encaminadas a proteger a la organización y a los interesados ante contingencias se sustenten en datos contrastables (no en impresiones, intuiciones o conocimientos parciales). Y este es el camino para que la alta dirección pueda decidir, a través de los órganos pertinentes, qué riesgos identificados de seguridad debe evitar, reducir, transferir o asumir.

6. DISEÑO METODOLÓGICO

6.1. TIPO DE INVESTIGACIÓN

El tipo de investigación que se lleva a cabo es de proyecto aplicado. Ya que se hará un análisis inicial de la situación actual de la seguridad de los activos informáticos de la Empresa de Transportes Tierra Grata S.A. y Cía. Ltda., lo cual permitirá reconocer la cantidad de activos informáticos, controles existentes, riesgos a los que se está expuestos y grado de conocimiento de los empleados con respecto al manejo adecuado de los activos informáticos.

6.2. POBLACIÓN Y MUESTRA

6.2.1. Población. Dirección, administrativos y operativos de la Empresa de Transportes Tierra Grata S.A. y Cía. Ltda., ubicada en la ciudad de Fusagasugá, departamento de Cundinamarca; la cual se compone por 1 sede principal ubicada en el perímetro urbano de la ciudad de Fusagasugá donde está el área administrativa, una oficina y una taquilla ubicadas en el Terminal de Transportes de Fusagasugá, una taquilla ubicada en el Terminal de Transportes de Bogotá y una taquilla ubicada en el Terminal satélite del Sur de Bogotá; siendo la sede principal donde se están ubicados la mayor parte departamentos que conforman la empresa.

La empresa opera con 15 Vehículos intermunicipales (Ruta Fusagasugá - Bogotá y viceversa) y 74 vehículos urbanos distribuidos en 40 Rutas de busetas y microbuses y 3 rutas de taxis Colectivos. Solo los vehículos intermunicipales tienen servicio de GPS. Para los vehículos urbanos hay puestos de control distribuidos por toda la ciudad donde hay un operador que controla. La comunicación entre oficinas se hace por celular, ya que no hay una red que comunique las estructuras, todo se centraliza en las Oficinas del Centro de Fusagasugá, pero no hay un buen sistema de seguridad para la información ya que se comparte el servicio de internet con empresas vecinas. No hay radioperador entre vehículos

6.2.2. Muestra. En la Sede Principal de la Empresa de Transportes Tierra Grata S.A. y Cía. Ltda., todo el personal tiene acceso a los activos informáticos, por tal razón para la aplicación de entrevistas y encuestas se tendrán en cuenta todo el personal administrativo.

Sus Departamentos son: Gerencia, Recursos Humanos, Contabilidad, Pagaduría, Operatividad. Son 10 empleados.

6.3. LINEA DE INVESTIGACION

La línea de investigación del proyecto está orientada de acuerdo a los controles del Anexo A del estándar ISO/IEC 27001:2013 (ver Anexo A de este documento), el cual nos ayuda con el propósito de conseguir los objetivos de seguridad del Sistema de Gestión de la Seguridad de la Información

6.4. INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

Se hace un proceso de Observación, de esta forma se extrae y se valida la información obtenida, haciendo aclimatación con los componentes físicos de las diferentes áreas de la empresa.

Se realizan entrevistas, estas permitirán conocer datos que no están disponibles de ninguna otra forma, el preguntar específicamente conlleva a respuestas cuantitativas, evitando divagaciones y comentarios al margen de la investigación.

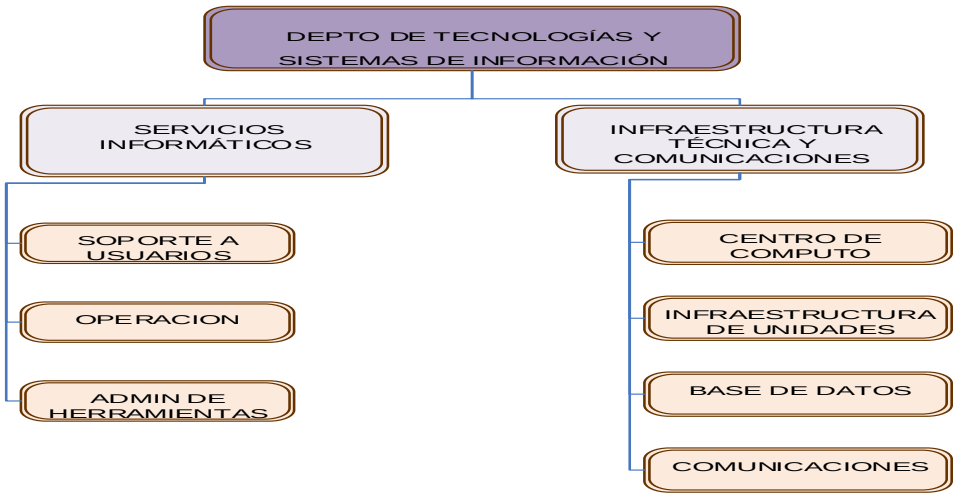
Se usan otras fuentes de información, tales como tesis, libros y escritos en medios físicos, electrónicos o publicados en Internet; referentes a temas de: SGSI, Norma ISO 27001 y 27002, metodología de MAGERIT e información que contribuya como guía y referencia para este proyecto.

7. ESQUEMA TEMATICO

7.1. ESTRUCTURA ORGANIZACIONAL DEL ÁREA INFORMÁTICA

La Figura 7 muestra la Estructura Organizacional del área Informática, en ella existen diferentes Cargos y Funciones del Área Informática de empresa Transportes Tierra Grata y Compañía Ltda., tal y como se muestra en el Anexo G de este documento.

Figura 7 Estructura Organizacional del área Informática.



Fuente: El Autor

7.1.1. Servicios que Ofrece la Empresa. Atención al Usuario. De manera permanente se efectúan los controles pertinentes para evaluar los ingresos por venta de servicios. Para nuestra Empresa es muy importante que el inversionista logre la rentabilidad que llene las expectativas con las que llegó. Que se centren en la prestación de un excelente servicio teniendo como eje central la satisfacción del Usuario, pues, utilizando la máxima “NOSOTROS NECESITAMOS DEL USUARIO, NO EL USUARIO DE NOSOTROS” y aplicando de buena forma nuestro eslogan “SERVICIO CON EFICIENCIA Y RESPONSABILIDAD” hemos logrado hasta la fecha mantener la imagen corporativa en un alto nombre siendo la mira de algunas empresas de la competencia dedicadas a poner en marcha estrategias que imiten las establecidas por la Administración.

En el sitio de despacho. Presentación personal del Vendedor. - El vendedor es la imagen de la Empresa en el sitio de Despacho, es por esto que debe estar

adecuadamente presentado, luciendo un uniforme con los emblemas de la Empresa, limpio, bien puesto. Su aspecto personal implica estar bien peinado, aseado, afeitado, luciendo su carné de identificación.

Al abordar el vehículo. Atención del Conductor - El conductor es la Imagen de la Empresa en el Vehículo. Apersonarse de recibir al Usuario ayudándolo con su equipaje y guiándolo al vehículo en forma cordial y educada, es lo más grato para que él sea una persona agradecida y quede satisfecha con el servicio.

En la vía.

- Conducción preventiva: - El Conductor es consiente que el mejor procedimiento para evitar accidentes es el manejo defensivo. No exceder límites de velocidad: - Tener presente que el pasajero desea llegar a su destino tranquilo, sin sobresaltos y en forma oportuna.
- Sobrecupo: - Concientizar al Conductor lo molesto e incómodo que resulta el sobrecupo para el pasajero.
- Cumplimiento de la ruta establecida: - Se tienen instrucciones específicas que a pesar de circunstancias molestas se debe cumplir con los recorridos establecidos salvo orientación de las autoridades competentes.

En la llegada.

- Al Descenso del Usuario. - El Usuario debe ser despedido por el conductor con un cordial saludo y una sonrisa, infundirle confianza y agradecerle por el haber utilizado el servicio de la Empresa.

7.2. IDENTIFICACIÓN DE ACTIVOS

Esta actividad se basa en recolectar la información necesaria para identificar los activos, mediante entrevistas al personal, solicitando diagramas de proceso y de flujos de datos. De esta manera, se puede medir el alcance del proyecto y obtener las relaciones entre los activos. En esta identificación no van todos los activos de la empresa, sino aquellos que nos competen al área de estudio. Para el desarrollo de esta fase se utilizó el software PILAR.

7.2.1 Activos Informáticos de la Empresa. Los activos de la empresa están definidos en las Tablas 5 y 6. Allí se evidencian los resultados de la investigación al interior de la empresa para poder definir dichos activos informáticos.

Tabla 5. Activos informáticos de la empresa

Equipamiento - Hardware	Computador de Personal	Computadoras de escritorio
	Equipos de Comunicaciones	Antenas
		Cableado
		Internet
		Lan
		Radios
		Router
		Sistema de vigilancia
		Telefonía ip
		Wifi
	Respaldos	Cd y discos duros
		Medios de impresión
	Servidores	Servidor de base de datos
Equipamiento - Software	Almacenamiento - Bases de Datos	Virtualización
	Correo Electrónico	Correo electrónico
	Internet	Internet
	Sistemas Financieros (contables) y Administrativos	Antivirus
		Ofimática
		Otros software
		Sistema operativo
	Virtualización	Virtualización
Equipamiento Auxiliar	Cableado eléctrico	Sistema de alimentación ininterrumpida
	Equipos de Climatización	Equipos de climatización
	Generadores Eléctricos	Sistema de alimentación ininterrumpida
	UPS	Sistema de alimentación ininterrumpida
Instalaciones	Centro de Datos	
	Cuartos de Red	
Personal	Administradores	
	Equipo de Desarrollo	
	Equipo Técnico	
Fuente. El Autor		

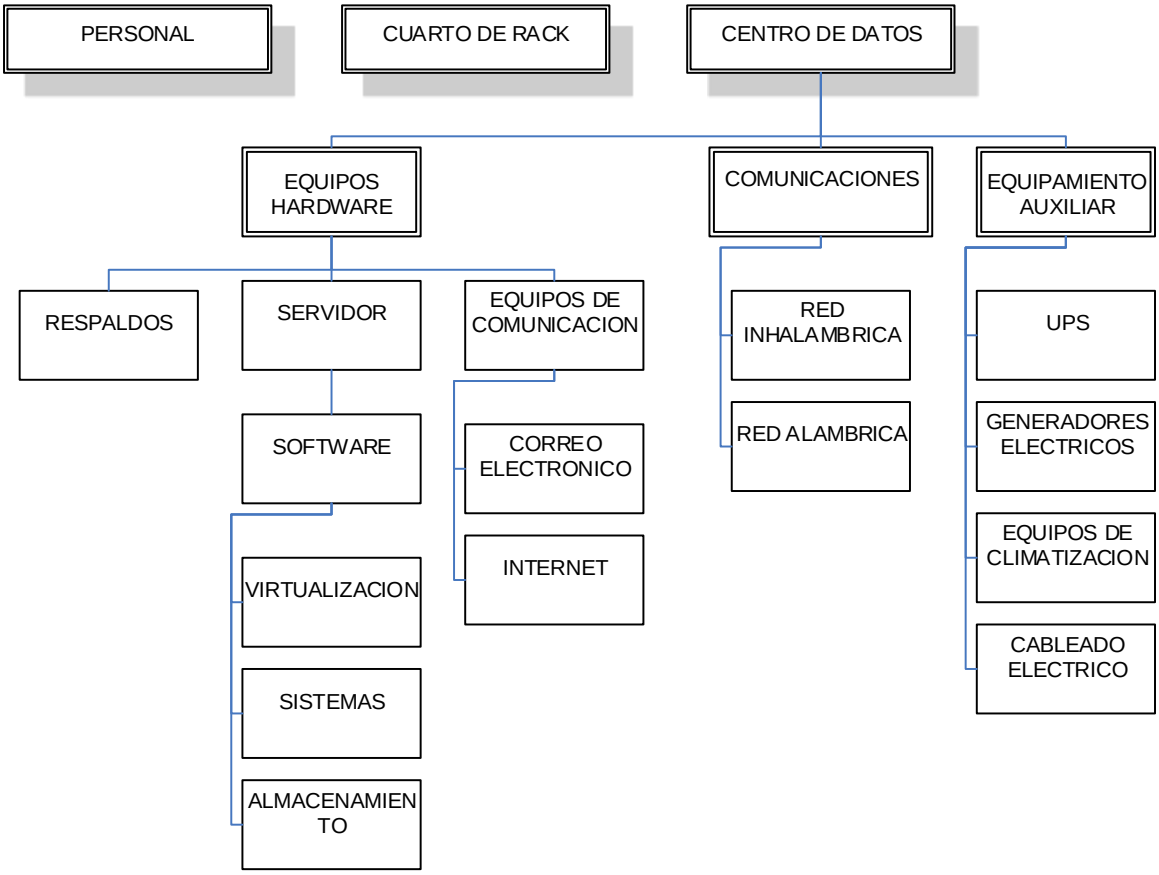
Tabla 6. Activos de la empresa según Magerit

[B] Activos esenciales		
[IS] Servicios internos		
[E] Equipamiento	[SW] Aplicaciones	A [cod005] sistemas
		A [cod006] almacenamiento
		A [cod007] correo electronico
		A [cod008] virtualizacion
	[HW] Equipos	I [cod001] servidores
		I [cod002] equipos_de_comunicacion
		A [cod003] respaldos
		A [cod004] computador_personal
	[COM] Comunicaciones	A [cod009] internet
		A [cod010] red_alambrica
		A [cod011] red_inalambrica
	[AUX] Elementos auxiliares	A [cod012] UPS
		A [cod013] generador_electrico
		A [cod014] equipos_climatizacion
[SS] Servicios subcontratados		
[L] Instalaciones		A [cod015] centro_datos
[P] Personal		A [cod016] equipo_desarrollo
		A [cod015] equipo_tecnico
		A [cod015] administrador
Fuente. El Autor		

7.2.2 Dependencias entre activos. El objetivo de esta tarea es identificar y valorar las dependencias entre activos, es decir, conocer la medida en que un activo de orden superior se puede ver perjudicado por una amenaza sobre un activo de orden inferior; resultando diagramas de dependencia.

En el mapa de dependencias de la Figura 8 se encuentran desplegados de forma jerárquica los activos de acuerdo al nivel de la dependencia que existe entre estos. En el primer nivel se han considerado al centro de datos, que es el lugar donde se concentran los servidores y equipos de comunicación, estos se encuentran en el segundo nivel al igual que el equipamiento auxiliar. En el tercer nivel se encuentran los servicios y aplicaciones que corren sobre los equipos de hardware. También, se han considerado a los equipos que generan electricidad y la climatización en el centro de datos que son de suma importancia para el normal funcionamiento de los equipos.

Figura 8 Mapa de dependencia de activos de la empresa



Fuente: El Autor

7.3. VALORACIÓN DE LOS ACTIVOS

El objetivo es identificar en qué dimensión es valioso el activo, para lo cual a la organización significara una pérdida en caso de que fuese afectado.

El resultado de esta actividad es el informe denominado “modelo de valor”. En la Tabla 7 se puede observar el resultado de la Valoración de activos para la empresa.

Tabla 7: Valoración de activos para la empresa

Tipo de activo	Nombre de activo	Bajo	Medio	Alto
Equipamiento - hardware	Computadoras de escritorio			
	Antenas			
	Cableado			
	Internet			
	Lan			
	Radios			
	Router			
	Sistema de vigilancia			
	Telefonía ip			
	Wifi			
	Cd y discos duros			
	Medios de impresión			
	Servidor de base de datos			
Equipamiento - software	Virtualización			
	Correo electrónico			
	Internet			
	Antivirus			
	Ofimática			
	Otros software			
	Sistema operativo			
Equipamiento auxiliar	Sistema de alimentación ininterrumpida			
	Equipos de climatización			
Instalaciones	Centro de datos			
	Cuartos de red			
Personal	Administradores			
	Equipo de desarrollo			
	Equipo técnico			
Fuente: el autor				

Para cada valoración conviene tomar en consideración la siguiente información:

- Dimensiones en las que el activo es relevante
- Estimación de la valoración en cada dimensión (Ver Tabla 8)

Tabla 8. Criterios de la valoración

Nivel	Valor	Criterio
10	Nivel 10 (Extremo)	Daño extremadamente grave
9	Nivel 9 (Muy Alto)	Daño muy grave
8	Nivel 8(+)	Daño grave
7	Alto	
6	Alto(-)	
5	Medio(+)	Daño importante
4	Medio	
3	Medio(-)	
2	Bajo(+)	Daño menor
1	Bajo	
0	Depreciable	Irrelevante a efectos prácticos

Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1793-magerit-libro-iii-tecnicas/file.html

En la Figura 9 se ha representado la valoración propia y acumulada de cada uno de los activos, en la cual se ha considerado la relación de dependencia de la Tabla 7; de esta forma sobresalen a simple vista los activos, tales como: las instalaciones, equipamiento auxiliar y entre los principales servicios ofrecidos están internet, almacenamiento de información, entre otros, este análisis se hace con las amenazas más comunes.

Figura 9. Dimensiones

	Equipamiento - Hardware																				Equipamiento - Software																					
	Servidores					Equipos de Comunicaciones					Respaldos					Computador de Personal					Sistemas Financieros (contables) y Administrativos					Almacenamiento - Bases de Datos					Correo Electronico					Virtualización					Internet				
Amenaza / Dimensi	[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
Incendio	10					10					10					10					8					8					10					10					10				
Terremoto	10					10					10					10					8					8					10					10					10				
Sobrecarga Electrica																					8					8																				
Falla de generador electrico	8					8					8					8					8					8					8					8					8				
Falla de equipos de climatizació	6					6					6					6					6					6					6					6					6				
Errores de configuración		5					6															6										6													
Desconexión física o lógica	8					8				8						2										9					8					8					10				
Agotamiento de recursos	6																									8																			
Spyware		8															5																												
Malware	8	8														5	5																												
Phishing																																	6												
Spam																																	6												
Flooding						6																																							
Acceso no autorizado			9					9						5				8					8	8					9	8							8								
Robo	10					10					10					8																													
Fuga de Información																																													

	Instalaciones										Equipamiento Auxiliar																Personal																					
	Centro de Datos					Cuartos de Red					UPS					Generadores Electricos					Equipos de Climatización					Cableado electrico					Administradores					Equipos Tecnico					Equipo de Desarrollo				
Amenaza / Dimensi	[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]	[D]	[I]	[C]	[A]	[T]
Incendio	10					10					10					10					10					10					10					10					10				
Terremoto	10					10					10					10					10					10					10					10					10				
Sobrecarga Electrica	9					9					8					8					8					8																				
Falla de generador electrico	8					8										10																													
Falla de equipos de climatizació	8					8															10																								
Errores de configuración																																													
Desconexión física o lógica	10					10																				10																		
Agotamiento de recursos	5					5																																							
Spyware																																													
Malware																																													
Phishing																																													
Spam																																													
Flooding																																													
Acceso no autorizado	8					8																										10	10				10	10				10	10			
Robo											10					10					10					5																				
Fuga de Información																																10	10				10	10				10	10			

Fuente: El Autor

[D] Disponibilidad [I] Integridad de los datos [C] Confidencialidad de los datos
[A] Autenticidad de los usuarios y de la información [T] Trazabilidad del servicio y de los datos

7.4. AMENAZAS

Se buscó por medio de la metodología aplicada, qué amenazas por activos eran las más recurrentes al interior de la empresa, llegando a definir que la exposición es alta ya que los riesgos siempre dieron medidas entre Medio y Alto además de que se encontraron amenazas en todas las clasificaciones de la caracterización de las Amenazas. Es preocupante que el Acceso no autorizado es una constante amenaza al interior de la empresa lo cual la convierte en una presa fácil a ser atacada por parte de cibercriminales. Al observar la valorización de las amenazas se hallan comprometidos muchos activos donde consecutivamente la Degradación del Valor y la Probabilidad de Ocurrencia dan niveles de Alta y Muy Alta, lo cual debe ser considerado a fondo por parte de las directivas para que se dé solución a tanta exposición.

En el Anexo H de este trabajo se encuentra lo correspondiente a las Amenazas definiendo los siguientes ítems:

- Mapa de Riesgos
- Caracterización de las Amenazas
- Identificación de las Amenazas
- Valoración de Amenazas por Activos
- Valoración de las Amenazas

7.5 CARACTERIZACIÓN DE LAS SALVAGUARDAS.

Teniéndose en cuenta que la seguridad de la organización en estudio es bastante vulnerable, se llegó a definir que hay varias salvaguardas muy importantes que son inexistentes al interior de la empresa ya que al revisar los niveles de madurez no hay un desarrollo de plan de contingencia ante desastres, así como no se realizan simulacros de forma periódica en lo que tiene que ver con los riesgos de incendio y terremoto. Ante el agotamiento de recursos no hay una revisión de directiva de copias de seguridad de forma regular. Ante un eventual robo no se encuentran el uso de cables de seguridad para computadores de personal y portátiles. Frente a los malware no hay la más mínima protección, así como tampoco se hacen pruebas periódicas del cortafuego. Frente al acceso no autorizado la situación es crítica ya que no se implementa un sistema de detección de intrusos, no se utiliza autenticación multifactor para conexión remota ni se implementa control de cuarentena en VPN. Frente a el riesgo de fuga de información se debe contratar personal responsable de la seguridad. Pero se avala también el hecho de

que la empresa ha iniciado procesos de seguridad que poco a poco van a ir ayudándole a redimir y corregir los errores y procesos faltantes.

En el Anexo I Caracterización De Las Salvaguardas, se realizan la Identificación de las Salvaguardas y la Valoración de las Salvaguardas.

7.6. IMPACTO

Los activos con mayor riesgo actualmente son los siguientes

- Servidores debido al acceso no autorizado y las fallas del servicio eléctrico.
- Los equipos de comunicación debido al acceso no autorizado
- Los computadores personales debido a los ataques de malware no controlados
- Los Sistemas financieros y administrativos debido al acceso no autorizado
- El Almacenamiento – bases de datos debido al acceso no autorizado y al agotamiento de recursos
- El correo electrónico y la virtualización debido al acceso no autorizado y a la desconexión física o lógica
- El internet y el Cableado eléctrico debido a la desconexión física o lógica
- Las UPS y los Equipos de climatización debido a la constante falla de equipos de climatización
- El Equipo de desarrollo, el Equipo técnico y Administradores debido a la Fuga de información

En el Anexo J, se evidencia el Impacto el cual viene definidos por el Impacto Potencial, el Impacto Residual Acumulado y la Estimación del Riesgo, lo cual nos lleva a determinar el estado de riesgo actual de la empresa y se les da a las directivas un direccionamiento de cuáles deben ser los riesgos objetivos par que se mejore la condición de riesgo y así el impacto negativo se disminuya.

Posteriormente se hacer una descripción del área informática o departamento de sistemas identificando los activos informáticos, los procesos que se realiza dentro del área y los servicios que presta a las demás áreas de la organización.

Finalmente se determinan las vulnerabilidades, amenazas y riesgos de seguridad del área informática o departamento de sistemas en cada uno de los activos informáticos categorizados de acuerdo al activo donde se presentan (talento humano, hardware, seguridad física, redes de datos, sistemas operativos, bases de datos, seguridad lógica, entre otros) y se debe entregar un cuadro con las categorías de los activos, las vulnerabilidades, amenazas de seguridad encontrados en dicha organización

7.7. TOTALIDAD DE LAS VULNERABILIDADES Y AMENAZAS ENCONTRADAS

Al revisar la totalidad de vulnerabilidades y amenazas encontradas, se observa que algunas de las constantes son el acceso no autorizado y el abuso de privilegios de acceso a diferentes activos, lo cual desencadena una serie de vulnerabilidades a todo el sistema de información de la empresa, tal como se describe en la Tabla 9 correspondiente a las amenazas y vulnerabilidades encontradas

Tabla 9. Totalidad de las vulnerabilidades y amenazas encontradas

ACTIVOS	**AMENAZAS**	FRECUENCIA	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**
[D] DATOS/INFORMACIÓN							
Códigos fuentes, contratos, Copias de Seguridad de los SI, historia laboral, historias clínicas, registros de actividad.	[A.11] Acceso no autorizado	5	100%	100%	100%	0%	0%
	[A.15] Modificación deliberada de la información	5	0%	100%	0%	100%	0%
	[A.18] Destrucción de información	5	100%	0%	0%	0%	0%
	[A.19] Divulgación de información	5	0%	0%	100%	0%	0%
	[A.3] Manipulación de los registros de actividad (log)	5	0%	100%	0%	0%	100%
	[A.5] Suplantación de la identidad del usuario	5	75%	75%	75%	0%	0%
	[A.6] Abuso de privilegios de acceso	5	100%	100%	100%	0%	0%
	[E.1] Errores de los usuarios	50	0%	50%	0%	0%	0%
	[E.14] Escapes de información	10	0%	50%	50%	0%	0%
	[E.15] Alteración accidental de la información	5	0%	50%	0%	0%	0%
	[E.18] Destrucción de información	5	100%	0%	0%	0%	0%
	[E.19] Fugas de información	5	0%	0%	100%	0%	0%
	[E.2] Errores del administrador	5	50%	50%	75%	0%	0%
	[E.3] Errores de monitorización (log)	5	100%	0%	0%	0%	100%
	[E.4] Errores de configuración	10	20%	0%	0%	0%	0%
[S] SERVICIOS							
Correo electrónico, gestión de identidades, servicios internos,	[A.10] Alteración de secuencia	5	0%	100%	0%	100%	0%
	[A.13] Repudio	5	0%	0%	0%	50%	0%
	[A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
	[E.24] Caída del sistema por agotamiento de recursos2	50	100%	0%	0%	0%	0%
[SW] SOFTWARE							
Bases de datos, ofimática, sistemas operativos, antivirus, software de la empresa, software estandar.	[I.5] Avería de origen físico o lógico	5	75%	75%	75%	0%	75%
	[A.22] Manipulación de programas	5	0%	50%	50%	0%	0%
	[A.7] Uso no previsto	5	75%	75%	75%	75%	0%
	[A.8] Difusión de software dañino	5	5%	5%	5%	0%	0%
	[A.9] [Re-]encaminamiento de mensajes	5	50%	0%	0%	0%	0%
	[E.1] Errores de los usuarios	10	5%	5%	5%	0%	0%

Tabla 9. (Continuación)

ACTIVOS	AMENAZAS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
	[E.2] Errores del administrador	10	50%	50%	50%	0%	0%
	[E.20] Vulnerabilidades de los programas (software)	10	50%	75%	75%	0%	0%
	[E.8] Difusión de software dañino	5	5%	5%	5%	0%	0%
[HW] HARDWARE							
Computadoras de escritorio que utilizan en la empresa, computadoras portátiles que utilizan en la empresa, dispositivos de respaldo, escáner, firewall, impresoras, puntos de acceso inalámbricos, routers, servidores, switch.	[I.1] Fuego	5	100%	0%	0%	0%	0%
	[A.23] Manipulación de los equipos	5	0%	75%	0%	0%	20%
	[A.25] Robo	5	100%	0%	0%	0%	0%
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	75%	0%	0%	0%	0%
	[E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
	[I.2] Daños por agua	5	100%	0%	0%	0%	0%
	[I.6] Corte del suministro eléctrico	50	100%	0%	0%	0%	0%
	[I.7] Condiciones inadecuadas de temperatura o humedad	10	75%	0%	0%	0%	0%
[COM] COMUNICACIONES							
Conectividad inalámbrica, internet, red de área local.	[E.9] Errores de [re-]encaminamiento	5	0%	20%	0%	0%	0%
	[A.12] Análisis de tráfico	5	0%	50%	50%	0%	0%
	[A.14] Interceptación de información (escucha)	5	0%	0%	100%	0%	0%
[AUX] EQUIPO AUXILIAR							
Cableado eléctrico, fibra óptica, fuente de alimentación, rack, sistema de alimentación ininterrumpida.	[A.26] Ataque destructivo	5	100%	0%	0%	0%	0%
[L] INSTALACIONES							
Oficinas	[I.11] Emanaciones electromagnéticas	5	20%	0%	0%	0%	0%
[P] PERSONAL							
Área administrativa, area de coordinaciona, area de sistema.	[E.28] Indisponibilidad del personal	10	50%	0%	0%	0%	0%
	[E.7] Deficiencias en la organización	5	75%	0%	0%	0%	0%
Fuente: El Autor							

7.7.1 Riesgo Inherente. Tal como se muestra en la Tabla 10, el riesgo inherente de acuerdo a la categoría del riesgo, la probabilidad de que suceda y el impacto muestran resultados bastantes críticos al interior de la empresa ya que afecta directamente al activo más importante: la información, ya que como se puede deducir, el hecho de que no haya la suficiente conservación de la fidelidad de dicha información podría generar una catástrofe que podría llegar a reducir a la mínima expresión la continuidad del negocio.

Tabla 10. Riesgo Inherente de acuerdo a la categoría del riesgo, la probabilidad de que suceda y el impacto

No. Riesgo	Riesgo del Proceso	Categoría del Riesgo	Probabilidad	Impacto	Riesgo Inherente
❶	[A.10] Alteración de secuencia	Estratégico	Posible	Mayor	Alto
❷	[A.11] Acceso no autorizado	Administrativo	Ocasional	Crítica	Moderado
❸	[A.12] Análisis de tráfico	Administrativo	Posible	Menor	Bajo
❹	[A.13] Repudio	Administrativo	Improbable	Menor	Bajo
❺	[A.14] Interceptación de información (escucha)	Estratégico	Posible	Mayor	Alto
❻	[A.15] Modificación deliberada de la información	Operativo	Constante	Crítica	Alto
❼	[A.18] Destrucción de información	Operativo	Ocasional	Catastrófico	Crítica
❽	[A.19] Divulgación de información	Estratégico	Ocasional	Crítica	Moderado
❾	[A.22] Manipulación de programas	Administrativo	Moderado	Menor	Moderado
❿	[A.23] Manipulación de los equipos	Operativo	Moderado	Menor	Moderado
⓫	[A.24] Denegación de servicio	Operativo	Posible	Crítica	Moderado
⓬	[A.25] Robo	Estratégico	Ocasional	Mayor	Alto
⓭	[A.26] Ataque destructivo	Operativo	Posible	Catastrófico	Crítica
⓮	[A.3] Manipulación de los registros de actividad (log)	Operativo	Moderado	Crítica	Alto
⓯	[A.5] Suplantación de la identidad del usuario	Operativo	Posible	Crítica	Moderado
⓰	[A.6] Abuso de privilegios de acceso	Administrativo	Ocasional	Crítica	Moderado
⓱	[A.7] Uso no previsto	Estratégico	Constante	Menor	Moderado
⓲	[A.8] Difusión de software dañino	Operativo	Ocasional	Mayor	Alto
⓳	[A.9] [Re-]encaminamiento de mensajes	Estratégico	Posible	Insignificante	Bajo
⓴	[E.1] Errores de los usuarios	Operativo	Constante	Crítica	Alto
❷❶	[E.14] Escapes de información	Financiero	Posible	Mayor	Alto
❷❷	[E.15] Alteración accidental de la información	Operativo	Moderado	Crítica	Alto
❷❸	[E.19] Fugas de información	Estratégico	Ocasional	Catastrófico	Crítica
❷❹	[E.2] Errores del administrador	Estratégico	Ocasional	Crítica	Moderado

Tabla10. (Continuación)

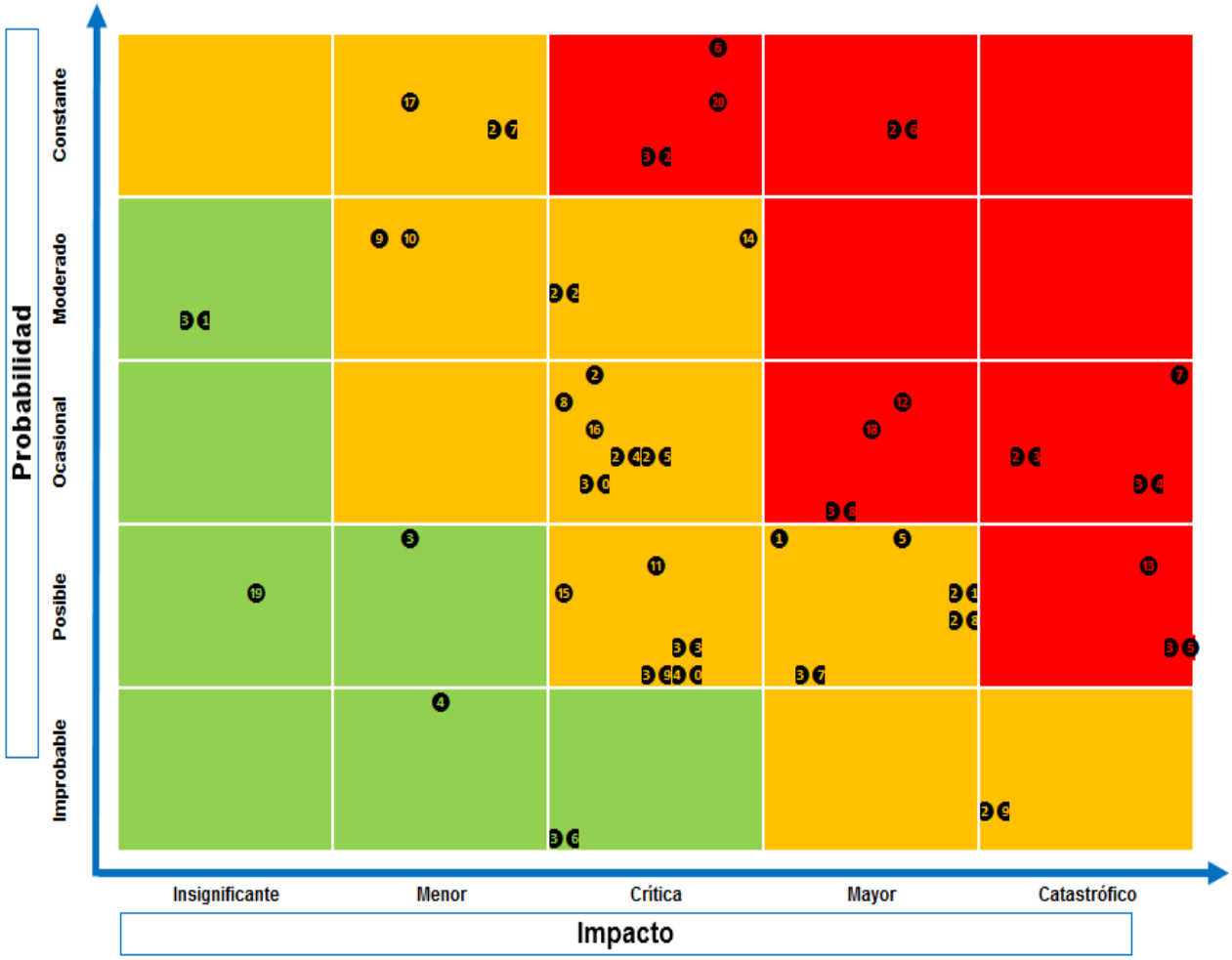
No. Riesgo	Riesgo del Proceso	Categoría del Riesgo	Probabilidad	Impacto	Riesgo Inherente
❷❺	[E.20] Vulnerabilidades de los programas (software)	Administrativo	Ocasional	Crítica	Moderado
❷❻	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Estrategico	Constante	Mayor	Crítica
❷❼	[E.24] Caída del sistema por agotamiento de recursos2	Administrativo	Constante	Menor	Moderado
❷❽	[E.25] Pérdida de equipos	Financiero	Posible	Mayor	Alto
❷❾	[E.28] Indisponibilidad del personal	Financiero	Improbable	Catastrófico	Crítica
❸❿	[E.3] Errores de monitorización (log)	Administrativo	Ocasional	Crítica	Moderado
❸❶	[E.4] Errores de configuración	Administrativo	Moderado	Insignificante	Bajo
❸❷	[E.7] Deficiencias en la organización	Operativo	Constante	Crítica	Alto
❸❸	[E.8] Difusión de software dañino	Administrativo	Posible	Crítica	Moderado
❸❹	[E.9] Errores de [re-]encaminamiento	Estrategico	Ocasional	Catastrófico	Crítica
❸❺	[I.1] Fuego	Operativo	Posible	Catastrófico	Crítica
❸❻	[I.11] Emanaciones electromagnéticas	Financiero	Improbable	Crítica	Moderado
❸❼	[I.2] Daños por agua	Operativo	Posible	Mayor	Alto
❸❽	[I.5] Avería de origen físico o lógico	Financiero	Ocasional	Mayor	Alto
❸❾	[I.6] Corte del suministro eléctrico	Financiero	Posible	Crítica	Moderado
❹❿	[I.7] Condiciones inadecuadas de temperatura o humedad	Financiero	Posible	Crítica	Moderado

Fuente. El Autor

7.7.2. Mapa de Calor de Riesgo Inherente

En el mapa de calor que se muestra en la Figura 10, se observa la distribución de las amenazas, las vulnerabilidades y sobre todo los riesgos que corre la empresa de acuerdo a la probabilidad que sucedan durante el tiempo y el impacto que se tiene por su ocurrencia, de esta manera se puede ver que en este estudio, las zonas rojas nos dan a entender que hay eventualidades que van de altas a críticas, las cuales se deben evaluar teniendo en cuenta que algunos eventos de riesgo se producen y duran sólo un período corto, quizás una cuestión de días. Otros tienen colas largas y duran muchos años. Algunos riesgos de larga duración pueden tener gran importancia estratégica, este mapa de riesgo puede trazar correlaciones entre riesgos.

Figura 10. Mapa de Calor de Riesgo Inherente



Fuente. El Autor

De la Figura 10 y de la Tabla 10 extracto los puntos más críticos que se ven reflejados en la Tabla 11, donde se extrapola que efectivamente la empresa de nuestro caso tiene niveles críticos en cuanto la protección de la información ya que está expuesta constantemente tanto a factores externos como internos. El hecho de que tengamos como riesgo inherente critico la destrucción de la información da a pensar que no se han tenido en cuenta ninguna de las normas de seguridad informática.

Tabla 11. Puntos críticos del Riesgo Inherente

No. Riesgo	Riesgo del Proceso	Categoría del Riesgo	Probabilidad	Impacto	Riesgo Inherente
❻	[A.15] Modificación deliberada de la información	Operativo	Constante	Crítica	Alto
❼	[A.18] Destrucción de información	Operativo	Ocasional	Catastrófico	Crítica
⓬	[A.25] Robo	Estratégico	Ocasional	Mayor	Alto
⓭	[A.26] Ataque destructivo	Operativo	Posible	Catastrófico	Crítica
⓲	[A.8] Difusión de software dañino	Operativo	Ocasional	Mayor	Alto
⓴	[E.1] Errores de los usuarios	Operativo	Constante	Crítica	Alto
❷❸	[E.19] Fugas de información	Estratégico	Ocasional	Catastrófico	Crítica
❷❻	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Estratégico	Constante	Mayor	Crítica
❸❷	[E.7] Deficiencias en la organización	Operativo	Constante	Crítica	Alto
❸❹	[E.9] Errores de [re-]encaminamiento	Estratégico	Ocasional	Catastrófico	Crítica
❸❺	[I.1] Fuego	Operativo	Posible	Catastrófico	Crítica
❸❽	[I.5] Avería de origen físico o lógico	Financiero	Ocasional	Mayor	Alto

Fuente. El Autor

En términos generales la empresa tiene bastante probabilidad de que sucedan eventos riesgosos que pueden poner en peligro la continuidad del negocio, se debe optar por implementar el sistema de gestión de seguridad informática de forma urgente. En la Tabla 12 se observa la identificación de los riesgos informáticos, categoría, vulnerabilidades, amenazas, recursos afectados, causas, controles internos, tratamiento de los riesgos de la empresa TRANSPORTES TIERRA GRATA Y COMPANIA LTDA, con el fin de darle un mejor manejo en la valoración de los activos informáticos.

Tabla 12: Identificación de los riesgos informáticos

RIESGOS	CATEGORIA	VULNERABILIDAD	AMENAZAS	RECURSOS AFECTADOS	CAUSAS	CONTROLES INTERNOS	TRATAMIENTO DE LOS RIESGOS	ACCIONES
Manipulación de terceros a información confidencial y privilegiada	Software	Fallas en los Sistemas Operativo	Perdida de programas e información valiosa, que afectan al software de facturación y contable	Imagen Institucional	Mal manejo de los permisos de acceso	Privacidad y protección de Información Personal Identificable.	Realizar capacitaciones para la reducción de riesgos en cuanto a las políticas de seguridad	Capacitaciones a funcionarios de las políticas
Hurto de información	Personal	Suplantación de usuarios.	Utilización de información privilegiada para fines inadecuado	Imagen Institucional	Desconocimiento de políticas de seguridad	Seguridad de Recursos Humanos	Practica de seguridad de la información	Capacitar al personal que efectúe el tratamiento de datos personales.
Acceso no autorizado a información	Hardware	Acceso no autorizado	Manipulación de información de reserva	SI	Privilegio no adecuado en accesos	Política de control de accesos.	Practica de seguridad de la información	Capacitar al personal que efectúe el tratamiento de datos personales.
Errores de Usuarios	Servidor de Correo	Contraseñas fáciles	El poco cambio de contraseñas y la utilización de algunas sin seguridad que se conviertan en fáciles de adivinar	SI	Usurpación de Usuario para el acceso a información	Política de uso de los controles criptográficos.	Protección mediante medios criptográficos e impedir el acceso a usuarios no autorizados	Técnicas y recomendaciones para el manejo de contraseñas
Mantenimiento de Software	Equipos Activos	Configuración de Servidores	Penetración a los sistemas desde cualquier ventana abierta	Desastre por la alteración de la información	Manipulación de contenidos confidenciales por terceros	Adquisición, desarrollo y mantenimiento de Sistemas.	Actualizar las medidas de seguridad y garantizar los SI	Mantenimiento continuo y actualizaciones de software autorizados

RIESGOS	CATEGORIA	VULNERABILIDAD	AMENAZAS	RECURSOS AFECTADOS	CAUSAS	CONTROLES INTERNOS	TRATAMIENTO DE LOS RIESGOS	ACCIONES
Desconocimiento de las políticas de Seguridad	Control de Información	Políticas de seguridad	Difusión de la información confidencial o hurto de la misma con fines diferentes a los establecidos	SI	Manipulación de contenidos confidenciales por terceros	PSI.	Practica de seguridad de la información	Capacitar al personal que efectúe el tratamiento de datos personales.

Tabla 12. (Continuación)

RIESGOS	CATEGORIA	VULNERABILIDAD	AMENAZAS	RECURSOS AFECTADOS	CAUSAS	CONTROLES INTERNOS	TRATAMIENTO DE LOS RIESGOS	ACCIONES
Destrucción de la información	Seguridad Lógica	Backup	Perdida de la información por falta de respaldo	Imagen institucional y toma de decisiones	Perdida de la Información	Copias de seguridad de la información.	Actividades para la ejecución de respaldos de información para prevenir la pérdida de información.	Respaldo de información
Adecuación y mantenimiento	Hardware	Instalación de UPS	Perdida de la información sin respaldo y daño a los equipos.	Retraso en los procesos	Falta de plan de mantenimiento	Perímetro de seguridad física.	Realizar un registro de los medios de almacenamiento de los datos personales	planes de recuperación de información inmediata y cubrimiento de equipos
Virus	Servicios	Privilegio de Instalación de Programas a todos los usuarios	Exponen el ingreso de software dañinos	Daño de la información y conectividad	Ataque a los sistemas por falta de actualización de antivirus	Controles contra el código malicioso.	Constante actualización de antivirus	Instalación de antivirus

Fuente : El Autor

8. CUADRO DE TRATAMIENTO DE LOS RIESGOS Y CONTROLES PROPUESTOS PARA MITIGAR LOS RIESGOS ENCONTRADOS

A continuación, se presenta la Tabla 13, que nos presenta el cuadro de tratamientos de los riesgos y controles propuestos, los cuales salen del análisis definido gracias al presente trabajo, donde se le muestra a la empresa opciones para que tenga en cuenta de cómo debe tratar los riesgos actuales a través de controles internos definidos, en la Tabla 14 se define como debe funcionar el sistema de control de acuerdo al riesgo que se asume.

Tabla 13. Control Interno y Tratamiento

Tipo de activo	Riesgos	Controles internos	Tratamiento
Hardware	R1. Robo de equipos de cómputo	Política de control de accesos.	Practica de seguridad de la información
	R2. Mal funcionamiento de los equipos y servicios.		
Software	R3. Intrusión no autorizada en los equipos.	Privacidad y protección de Información Personal Identificable.	Realizar capacitaciones para la reducción de riesgos en cuanto a las PSI
	R4. Modificación, borrado o robo de información.		
	R5. Ataques de DoS.		
	R6. Modificación y robo de identidades.		
	R7. Suplantación de Ip, dominio, páginas web.		
Redes	R8. Disponibilidad de los servicios.	Autenticación de firmas digitales	Realizar auditorías con personal capacitado profesionalmente para ello
Seguridad Física	R9. Perdida de información, equipos o partes asociadas a su gestión.	Perímetro de seguridad física.	Realizar un registro de los medios de almacenamiento de los datos personales
Seguridad Lógica	R10. Borrado, o eliminación de archivos, destrucción del S.O, robo de información personal.	Copias de seguridad de la información.	Actividades para la ejecución de respaldos de información para prevenir la pérdida de información.
Personal Del Área	R11. Robo de información personal.	PSI.	Practica de seguridad de la información
	R12. Sustracción, divulgación, venta o modificación de la información propia de la compañía.		
	R13. Alteración de archivos y registros.		
	R14. Robo o destrucción de información.		
	R15. Robo o destrucción de equipos de cómputo.		
	R16. Fuga de información.		
	R17. Ataque con ingeniería social		

Fuente: El Autor

Tabla 14. Sistema de Control

Tipo de activo	Riesgos	Sistema de control
Hardware	R1. Robo de equipos de cómputo	• Restringir el acceso al personal fuera de la dependencia. • Instalar cámaras de seguridad, para identificar y disminuir los robos. • Contratar vigilancia a la organización. • Establecer política de seguridad, al ingreso de la oficina. • Implementar o redefinir la matriz de control de acceso.
	R2. Mal funcionamiento de los equipos y servicios.	• Definir un plan semestral de mantenimiento preventivo
	R3. Interface e Información	• Procedimiento formal de alta y baja de usuarios con objeto de garantizar y cancelar los accesos a todos los sistemas y servicios de información. • restringir y controlar la asignación y uso de los privilegios. • controlar la asignación de contraseñas mediante un proceso de gestión • revisar con regularidad los derechos de acceso de los usuarios, siguiendo un procedimiento formal.
Software	R4. Intrusión no autorizada en los equipos.	• Cifrar la base de datos y la información transferida. • Realizar una buena configuración del servidor web. • Realizar copias de seguridad de la base de datos. • Validar la asignación de claves robustas. • Capacitación del usuario al responder un correo no deseado. • Requerir SSL para todas las páginas sensibles • Crear atributo (*secure*) en todas las cookies sensibles. • Configuración en forma adecuada los *Routers* y el *Firewalls* • Realizar filtros de IP a paquetes procedentes de IP's autorizadas. • Configuración adecuada de puertos y deshabilitar los que no se utilicen. • Realizar la securización de la red de datos Configurar el servidor SSL para que acepte únicamente algoritmos considerados fuertes. • Implementar o redefinir la matriz de control de acceso. • Control permanente y verificación a las actualizaciones y parches de seguridad. • Configurar archivos logs de transacciones para las diferentes aplicaciones • Solicitar periódicamente auditoria a las diferentes áreas (Bases de Datos, Comunicaciones, Seguridad, etc.) • Restringir el acceso con rango de IP
	R5. Modificación, borrado o robo de información privilegiada	
	R6. Ataques de DoS, Malware y procesamiento	
	R7. Modificación y robo de identidades.	
	R8. Suplantación de Ip, dominio, páginas web.	
	R.9. Adecuación y mantenimiento	

Tabla 14. (Continuación)

Redes	R10. Disponibilidad de los servicios.	• Monitoreo continuo a las actividades propias de la red. • Configuraciones seguras para dispositivos de red. • Establecer mecanismos de defensa perimetral como Proxy, redes DMZ, sistemas de prevención de intrusos (IPS), firewalls. • Monitorización y análisis de registros de auditoría. • Acceso controlado a los recursos de red.
Seguridad física	R11. Perdida de información, equipos o partes asociadas a su gestión. R12. Fallo eléctrico - corto circuito R13. Incursión a instalaciones	• Realizar copia de seguridad de los datos guardados en el PC, en un lugar diferente a este. • Establecer políticas para la copia de seguridad. • Prohibir el acceso de personal ajeno a la oficina. • Definir el personal encargado de las copias de seguridad
Seguridad Lógica	R14. Borrado, o eliminación de archivos, destrucción del S.O, robo de información personal. R15. Virus	• Encriptar la base de datos y la información contenida en ella. • Cifrar los datos transmitidos. • Generar claves robustas para el proceso de encriptado. • Instalación de antivirus y actualización permanente
Personal Del Área	R16. Errores de Usuarios R17. Sustracción, divulgación, venta o modificación de la información propia de la compañía. R18. Alteración de archivos y registros. R19. Robo o destrucción de información. R20. Robo o destrucción de equipos de cómputo. R21. Fuga de información. R22. Ataque con ingeniería social R23. Desconocimiento de las PSI R24. Relación e Integridad R25. Ingeniería social	• Capacitar a los funcionarios sobre la seguridad e inseguridad informática. • Dar a conocer los últimos tipos de ataque realizados a empresas. • Eliminar y/o deshabilitar las claves asignadas a los funcionarios que ya no están vinculados con la empresa. • Establecer y dar a conocer un conjunto de buenas prácticas sobre el uso de las tics. • Hacer que los funcionarios firmen un documento de confidencialidad. • Evaluar las condiciones laborales de los trabajadores para identificar el inconformismo. • Dar a conocer las técnicas utilizadas por personas mal intencionadas para obtener información privada de la organización.
Desastre natural - calamidad	R26. Terremoto, inundación, tormenta, etc	• Instalar UPS con buena capacidad • Instalar polos a tierra o para rayos

Fuente: El Autor

9. POLÍTICAS DE SEGURIDAD DE LOS ACTIVOS DE LA INFORMACIÓN Y ALCANCES DEL SGSI PARA LA EMPRESA TRANSPORTES TIERRA GRATA Y COMPANIA LTDA.

Se elabora el Manual de Políticas y Procedimientos de Seguridad de la Información (PSI) definidas por la Empresa de Transportes Tierra Grata Compañía Ltda., para la elaboración del mismo, se toman como base las leyes y demás regulaciones aplicables, el capítulo décimo segundo del título primero de la Circular Básica Jurídica de la Superintendencia Financiera de Colombia, la norma ISO 27001:2013 y las recomendaciones del estándar ISO 27002:2013. Las políticas incluidas en este manual se constituyen como parte fundamental del sistema de gestión de seguridad de la información de la Empresa de Transportes Tierra Grata Compañía Ltda., y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos. Las PSI cubren todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios y terceros que laboren o tengan relación con la Empresa de Transportes Tierra Grata Compañía Ltda., para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada, tal como se define en el Anexo K

Se desarrollan también las Políticas de Seguridad de los Activos de la Información y Alcances del SGSI para la Empresa, en estas políticas todos los directivos y funcionarios se obligarán a conservar la información lo más segura posible. Se prohíbe la reproducción total o parcial de los documentos clasificados como confidenciales, sin la correspondida autorización o aprobación del ente competente, así como el deterioro adrede de los mecanismos informáticos, software, cableado de datos, suministro eléctrico, o cualquier activo de la empresa. Se utilizarán políticas y lineamientos de seguridad que obliguen a mantener la información de en un entorno seguro. Estas políticas estarán enviadas a conservar los principios de la Seguridad Informática como lo son la Confidencialidad, Integridad y Disponibilidad, así como los Planes de Continuidad del Negocio y Recuperación de Desastres. Esto lo encontramos en el Anexo L de este documento.

8.1. DOMINIOS Y CONTROLES APLICABLES

Con el propósito de conseguir los objetivos de seguridad del Sistema de Gestión de la Seguridad de la Información, se establecen los siguientes controles de seguridad establecidos en la metodología de análisis y evaluación de riesgos MAGERIT y los controles del Anexo A del estándar ISO/IEC 27001:2013 (ver Anexo A de este documento)

Objeto y campo de aplicación: Seleccionar los controles dentro del proceso de implementación del Sistema de Gestión de Seguridad de la Información – SGSI

Referencias normativas: La ISO/IEC 27000, es referenciada parcial o totalmente en el documento y es indispensable para su aplicación.

Términos y definiciones: Para los propósitos de este documento se aplican los términos y definiciones presentados en la norma ISO/IEC 27000.

Estructura de la norma: La norma ISO/IEC 27000, contiene 14 numérales de control de seguridad de la información que en su conjunto contienen más de 35 categorías de seguridad principales y 114 controles, de los cuales se van a trabajar los que aparecen en verde en la columna de Aplica.

En Anexo M se describen los Dominios y controles de acuerdo a los activos informáticos existentes en la empresa

La norma o estándar ISO/IEC 27001:2013 solicita el cumplimiento de verdaderos criterios para crear, realizar, conservar y mejorar continuamente el Sistema de Gestión de la Seguridad de la Información (SGSI) en el contexto de una empresa.

Para comprobar el estado actual del cumplimiento del estándar ISO/IEC 27001:2013 de la oficina de Sistemas y Telecomunicaciones de la Empresa de Transportes Tierra Grata y Compañía Ltda, se realizará un Análisis Diferencial de los numerales obligatorios 4 al 10 (Requisitos de la Norma ISO/IEC 27001:2013) y del Anexo A (Dominios, Objetivos de Control y Controles de Seguridad). Este análisis consiente confrontar las condiciones actuales con el fin de encontrar las deficiencias efectivas y el nivel de cumplimiento en base al estándar y desarrollar un plan de mejoramiento de acuerdo a los objetivos de seguridad deseados.

Requisitos de la Norma ISO/IEC 27001:2013. Para que una empresa esté acorde al estándar ISO/IEC 27001:2013, no se deben descartar ninguno de los requisitos especificados en los numerales 4 al 10.

En el Anexo N: Requisitos de la Norma ISO/IEC 27001:2013 se exponen los resultados del nivel de conformidad y cumplimiento de estos requisitos.

8.2. LISTAS DE CHEQUEO

Se diseñan las listas de chequeo para verificación del cumplimiento de los controles de acuerdo a la norma ISO/IEC 27002 para determinar el nivel de madurez o grado de cumplimiento en porcentaje (%).

8.2.1 Formatos de Chequeo Propuesto.

Formato diseñado que permite auditar o verificar aspectos que de acuerdo a la norma se deben revisar en cada uno de los documentos de la gestión documental exigidos en el SGSI en relación a la norma ISO/IEC 27001:2013

Para realizar el nivel de cumplimiento del proceso de auditoría interna con base en la norma ISO/IEC 27001:2013, se deberá tener en cuenta los siguientes aspectos y anotaciones:

- Control: Número interno del control.
- Nombre del control: Nombre de identificación del control.
- Descripción del control: Se describirá el control.
- Aplica (SI-NO): Indica si la implementación del control tiene aplicabilidad a nivel de la función de la organización.
- Justificación: Se deberá justificar la aplicabilidad del control.
- Cumplimiento actualización: Indica el grado de implementación del control en porcentaje (0-100)
- Observaciones: Se realizarán anotaciones relacionados con el control, y otras que considere pertinentes mencionar.

Los Formatos de chequeo propuestos se definen de acuerdo a los controles a ejecutar en este proyecto donde se muestra la aplicación de dichos controles, así como la justificación y el porcentaje de su cumplimiento, tal y como se muestra en el Anexo O. También se hace la observación por parte de quien aplica estos formatos.

8.3 NIVEL DE MADUREZ O GRADO DE CUMPLIMIENTO

ANÁLISIS DE LA SITUACION ACTUAL Y RECOMENDACIÓN DE APLICABILIDAD ISO/IEC 27001:2013

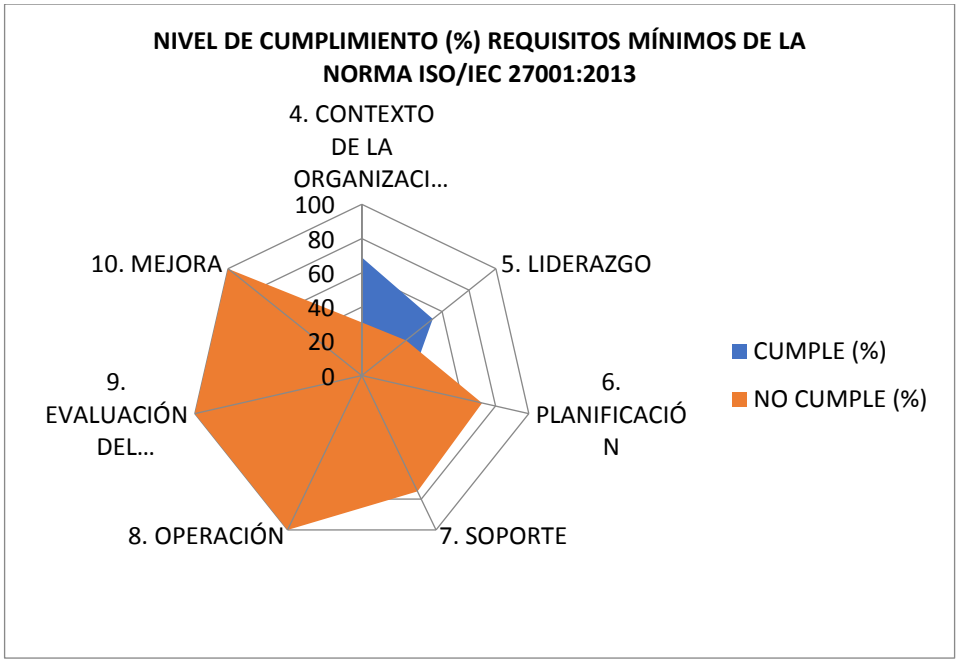
El Anexo A es un documento que enlista los controles de seguridad establecidos en el Anexo A del estándar ISO/IEC 27001:2013 que contiene un conjunto de 114 controles agrupados en 35 objetivos de control. (Se encuentra en el Anexo A de este documento) El Anexo A es usualmente utilizado como un informe para la implementación de medidas de protección de la información, así como para evidenciar que no se están dejando de lado medidas de seguridad necesarias que no habían tenido en cuenta dentro de una organización.

Los controles de Seguridad, dominios, Objetivos de Control, se realiza a su vez un Análisis Diferencial referente al Anexo A del estándar ISO/IEC 27001:2013 con el fin de determinar el nivel de cumplimiento de los Dominios, Objetivos de Control y Controles de Seguridad conformes al estándar ISO/IEC 27002:2013. Estos corresponden a los numerales 5 al 18. De esta forma, el nivel de cumplimiento para cada uno de los requisitos mínimos de la norma ISO/IEC 27001:2013 se resume de la siguiente manera en la Tabla 15:

Tabla 15. Nivel de Cumplimiento de los Requisitos de la Norma ISO/IEC 27001:2013.

NUMERAL/REQUISITO	CUMPLE (%)	NO CUMPLE (%)
4. CONTEXTO DE LA ORGANIZACIÓN	69	31
5. LIDERAZGO	53	33
6. PLANIFICACIÓN	28	72
7. SOPORTE	25	75
8. OPERACIÓN	0	100
9. EVALUACIÓN DEL DESEMPEÑO	0	100
10. MEJORA	0	100
Fuente: El Autor.		

Figura 11 Nivel de Cumplimiento de los Requisitos Mínimos de la Norma ISO/IEC 27001:2013.



Fuente: El Autor

Mediante este Análisis Diferencial, que se muestra en la Figura 11, es factible establecer que la oficina de Sistemas y Telecomunicaciones de la Empresa de Transportes Tierra Grata y Compañía Ltda., percibe la importancia y beneficios de un SGSI, también contienen e el liderazgo necesario para ejecutarlo; sin embargo aún no se ha establecido formalmente una metodología de análisis y evaluación de riesgos informáticos y su procedimiento, también ningún documento requerido por el estándar ISO/IEC 27001:2013. Por otra parte, se comprende la necesidad de ordenar el SGSI con el proceso de desarrollo tecnológico llevado a cabo en la empresa.

8.4. DECLARACIÓN DE APLICABILIDAD SOA

La Declaración de Aplicabilidad, (*Statement of Applicability (SoA)*, es un componente fundamental para la implementación del Modelo de Seguridad y Privacidad de la Información.

Se debe realizar en seguida del tratamiento de riesgos, y a su vez es la actividad posterior a la evaluación de riesgos. Debe revelar si los objetivos de control y los controles se hallan implementados y en operación, de igual manera se debe justificar por qué algunas medidas han sido excluidas. Después de la selección de los controles de seguridad, se procede a crear el plan de tratamiento de riesgos, esto con la finalidad de definir las actividades necesarias para la aplicación de los controles de seguridad.

En el Anexo P definido como Declaración De Aplicabilidad SOA presenta la declaración los controles que son relevantes para el SGSI de la Empresa de Transportes Tierra Grata Compañía Ltda y aplicables a la misma.

10. PARTICIPANTES EN EL PROYECTO

9.1 PROPONENTE PRIMARIO

YON IVÁN MÁRQUEZ BUITRAGO, Ingeniero de Sistemas egresado de la Universidad Nacional Abierta y a Distancia UNAD, desarrollador del proyecto, y responsable desde hace diez años del área de sistemas de empresa Transportes Tierra Grata y Compañía Ltda., ejecutando funciones como: administrador del Sistema de Información, redes de comunicaciones, Seguridad Perimetral, soporte a usuarios y supervisión de mantenimiento preventivos y correctivos.

9.2 PROPONENTES SECUNDARIOS

9.2.1 Transportes Tierra Grata y Compañía Ltda. Durante el desarrollo del proyecto fue necesario la participación de directivos y empleados de la empresa de la Sede Principal donde fue aplicado el proyecto. A continuación, se mencionan con detalle:

Funcionarios. Para el levantamiento de información fue importante la colaboración de los funcionarios de la empresa, tanto directivos como operativos, para conocer sus percepciones sobre el estado actual de la seguridad de la información. Las áreas que participaron en el proyecto fueron (Ver Tabla 16):

Tabla 16. Empleados Administrativos Transportes Tierra Grata Y Cía. Limitada

NOMBRES	CARGO QUE DESEMPEÑA
Jorge Humberto Pulido Pardo	Representante Legal
Martha Lucia Vargas Ávila	Asesora Jurídica
Francisco Alberto Benítez Manjarrez	Jefe de Contabilidad
Carlos Arturo Fula Pérez	Asistente Contable
Jhonatan Camilo Páez Cañón	Tesorero
Amanda Páez	Contadora
Fabio Penagos Moreno	Jefe Operativo Intermunicipal
José Arnulfo Beltrán Sánchez	Jefe Operativo Urbano
Mónica Yarledy Padilla Rodríguez	Jefe de Talento Humano
Lina María Acosta Moreno	Asistente de Gerencia
Ana Delia Galindo	Asistente Contable
Karen Lizeth Contreras Landinez	Aprendiz SENA
Fuente: Lina María Acosta Moreno, Asistente de Gerencia Empresa Transportes Tierra Grata y Cía. Ltda.	

9.2.2 Asesores del Proyecto. En las distintas fases del proyecto, la Universidad Nacional Abierta a Distancia UNAD, dispuso a docentes como asesores metodológicos, los cuales fueron de mucho apoyo para la construcción de este.

Docente del curso Proyecto de Seguridad I: LUIS FERNANDO ZAMBRANO HERNANDEZ, Ingeniero de Sistemas egresado de la Fundación Universitaria San Martín, Especialista en Seguridad Física y de la Informática de la ESCOM, Administrador de redes y sistemas CCNA de la FUNDACOMPUSESCO

Docente del curso Proyecto de Seguridad II: JUAN JOSÉ CRUZ. Ingeniero de Sistemas de la Universidad Cooperativa de Colombia. Especialista en Seguridad Informática de la Universidad Piloto de Colombia. Candidato a Magíster en Seguridad Informática de la Universidad Internacional de la Rioja y candidato a Magíster en Docencia Universitaria de la Universidad Broward International.

Director de Proyecto de grado: HELENA CLARA ISABEL ALEMÁN NOVOA. Ingeniera de Sistemas de la Universidad de Boyacá. Especialista en Pedagogía para el Desarrollo del Aprendizaje Autónomo y Magister en Seguridad Informática.

11. RESULTADOS E IMPACTOS ESPERADOS

La Propuesta del Diseño de Controles de Seguridad para los Activos Informáticos en la Empresa Transportes Tierra Grata y Compañía Ltda. de Fusagasugá, contendrá los siguientes aspectos (ver Tabla 17):

1. Diagnostico actual de la seguridad de la Información de empresa Transportes Tierra Grata y Compañía Ltda. de Fusagasugá

2. Desarrollo de la fase de Planeación del ciclo PHVA como producto del Sistema de Gestión de Seguridad de la Información.

3. Política general de seguridad de la empresa que incluyan controles para:

- Aspectos Organizativos de la seguridad de la información.
- Gestión de Activos.
- Seguridad relacionada a cada activo.
- Control de Acceso.
- Adquisición, desarrollo, mantenimiento de sistemas informáticos.
- Gestión de los Incidentes de Seguridad.

4. Compromiso firmado por parte de los directivos de la empresa Transportes Tierra Grata y Compañía Ltda. de Fusagasugá, de apoyar decididamente al diseño del SGSI.

5. Enfoque de evaluación de riesgos cuya metodología debe contemplar inventario de activos, identificación de amenazas y vulnerabilidades, identificación de impactos, análisis y evaluación de riesgos, y tratamiento de riesgos.

6. Estrategias para Formación y concientización.

7. Planes de acción correctiva/preventiva.

8. Planes de monitoreo y revisión.

Tabla 17. Resultados e Impactos esperados

RESULTADO/PRODUCTO ESPERADO	INDICADOR	BENEFICIARIO
Entrega del Plan de seguridad que se constituye de una política de seguridad y un plan de ejecución que conlleva la participación del personal de varias áreas a la futura ejecución y mejora de procesos aplicando medidas preventivas y correctoras para reducir los niveles de riesgo existentes, este resultado ayuda a reconocer el nivel de riesgo residual al cual aún se encuentran expuestos los sistemas y procesos de la empresa.	1	Empresa Transportes Tierra Grata y Compañía Ltda.
Declaración de Aplicabilidad (SoA) que permite mantener el registro y control de las medidas de seguridad que se aplican	1	Empresa Transportes Tierra Grata y Compañía Ltda.
Fuente: El Autor		

Se espera que la documentación generada del proyecto del diseño del Sistema de Gestión de Seguridad de la Información para Transportes Tierra Grata y Compañía Ltda. de Fusagasugá, sirva como bases para la implementación de un sistema sólido que garantice establecer lineamientos y controles para mitigar las amenazas que puedan presentarse y afectar los activos informáticos. Además, se espera concientizar a los empleados sobre la importancia de la seguridad informática con el apoyo de la Gerencia de Transportes Tierra Grata y Compañía Ltda. de Fusagasugá a través de la capacitación.

12. SOCIALIZACIÓN DE LOS RESULTADOS

En el siguiente link se encuentran algunos apartes de la socialización realizada ante las directivas y administrativos de la empresa:

https://youtu.be/NVTpZl0_tlg

La carta de aprobación de la socialización y la asistencia se encuentran en el Anexo B

Como se puede apreciar en la presentación se tomó un ejemplo de solución que se podría implementar para el problema de seguridad de redes, el cual fue la implementación de un *Small IT Solution*, el cual es una solución a nivel entrada dentro del cómputo basado en servidor para empresas pequeñas que buscan una funcionalidad de informática central de alto valor que sea asequible, segura, confiable y fácil de usar. Esta solución es para organizaciones con hasta 50 PCs

De esta socialización, se puede extractar que en general, los trabajadores de la empresa quedaron muy preocupados debido a la crisis de seguridad informática que tiene la empresa actualmente, son conscientes de que se debe hacer algo para mitigar esta inseguridad.

Algunos de los empleados después de la exposición se acercaron a mí con gran preocupación ya que sospechan que tengan un ataque al interior de la empresa debido a que el sistema actual es muy precario. Aun así, aseguran que han tenido modificaciones en la información de forma intencional. También se notan bastante reacios a creer que las directivas y propietarios vayan a invertir pronto en la soluciona los problemas de seguridad informática.

Por parte de las directivas, quedaron con la expectativa de analizar las Políticas de Seguridad Informática que se les propuso en el documento que se puede observar en los Anexos K y L los cuales son compendio del trabajo aquí realizado. Saben que deben hacer una alta inversión para mejorar, pero también saben y se dieron cuenta de que, si no se hace algo, en cualquier momento pueden llegar pérdidas de información que exponen la continuidad de negocio de la empresa Transportes Tierra Grata y Compañía Ltda.

13. CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. En este proyecto aplicado se describe la importancia de todo lo concerniente a la gestión del riesgo presente en la seguridad de la información que debe ser administrada por medio de equipos, servicios y personal del área de las Tecnologías de la Información, esto unido al respectivo conocimiento de estándares, metodologías y herramientas que hacen posible el desarrollo del análisis de riesgos en una empresa.

2. Al ser MAGERIT la metodología implementada en este caso, se lograron conocer las amenazas a las cuales está expuesta la infraestructura de los activos informáticos de la empresa Transportes Tierra Grata y Compañía Ltda. de Fusagasugá, esto se hizo mediante un análisis de riesgos cualitativo, el cual permitió conocer el nivel de madurez en la seguridad que tenía la empresa para finalmente sugerir cuales seria las salvaguardas apropiadas para reducir los niveles de riesgo e impacto.

3. Se ha desarrollado el plan de seguridad que consta de las políticas de seguridad de la información (PSI) y un plan de ejecución que radica en la participación de personal de todas las áreas para proyectar la implementación y mejora de procesos aplicando medidas preventivas y correctivas y así reducir los niveles de riesgo detectados, además de esto, reconocer el nivel de riesgo residual al cual se encuentran expuestos los sistemas y procesos de la empresa.

4. Al interior de la empresa se logró la concientización por medio de la socialización del presente proyecto, haciendo caer en cuenta al personal de la importancia de valorar la información a proteger y los costos que implicaría la perdida, modificación o borrado de ésta, y en este sentido planificar las acciones que permitan proteger tal información.

5. Los resultados obtenidos le dan la mano a la empresa para reconocer la necesidad inminente de implementar un plan de gestión de riesgos que mitigue los riesgos más críticos hallados en este proyecto, saben que deben considerar la contratación de personal especializado en seguridad, así como la compra de dispositivos apropiados que coadyuven a la protección eficaz de la información.

RECOMENDACIONES

1. Es indispensable el compromiso que debe asumir la dirección de la empresa Transportes Tierra Grata y Compañía Ltda. de Fusagasugá, para proyectarlo a sus empleados. Reconociendo la necesidad, aprobando y participando activamente en la implementación del Sistema de Gestión de Seguridad Informática.

2. Una de las falencias graves de la empresa Transportes Tierra Grata y Compañía Ltda. de Fusagasugá, es su infraestructura física que pone en riesgo todos los activos informáticos. Es recomendable realizar una estimación para la adecuación de las instalaciones y priorizarlo. Además, debe disponerse un espacio para la construcción de un cuarto de equipos con las normas necesarias de seguridad, para que los activos críticos que soportan la operación del negocio no queden expuestos a factores que puedan afectarlos.

3. Programar jornadas de sensibilización a los usuarios para aplicar buenas prácticas de las políticas de seguridad y crear hábitos de seguridad, como bloquear sesiones en periodos de inactividad laboral, cambiar periódicamente sus contraseñas.

4. Se invita a socializar y presentar mediante un informe a las directivas de la empresa, cada una de las sugerencias suministradas en el informe Declaración de aplicabilidad para mejorar circunstancialmente el nivel de seguridad la empresa.

5. Con los resultados obtenidos en el presente trabajo se invita a la empresa a que lleve a cabo la fase de implementación del plan de gestión de riesgos reduciendo la aparición de puntos críticos presentes en el análisis de la información, a través del uso de herramientas tecnológicas que faciliten su identificación para generar correctivos.

6. Es necesario generar cultura en la evaluación de las políticas de seguridad en los funcionarios, y mantener actualizados los controles de protección, ajustando constantemente las necesidades de la seguridad de los sistemas de información, a través de auditorías internas.

7. Mantener la estricta inspección en el personal, en la ejecución y control de políticas, dando consecución al mismo y garantizando aplicabilidad a las recomendaciones entregadas.

BIBLIOGRAFÍA.

AGUIRRE, Jorge Ramió Libro Electrónico de Seguridad Informática y Criptografía v4.1. Capítulo 3: Introducción a la Seguridad Informática. Madrid - España. Universidad Politécnica de Madrid, p. 75 {En línea}. {consultado el 30 de octubre de 2017} disponible en: (http://deic.uab.es/material/26118-03IntroSegInfo.pdf)

AMÉRICAECONOMÍA.COM. La fuga de información es una de las razones por las que las empresas pierden más dinero. {En línea}. Julio 2016{28 de septiembre de 2017} disponible en:(https://mba.americaeconomia.com/articulos/notas/la-fuga-de-informacion-es-una-de-las-razones-por-las-que-las-empresas-pierden-mas-di)

ARAGON ALVAREZ, Alejandro. Implementación de Controles de Seguridad en Activos Informáticos. Trabajo de Grado Maestro en Ciencias en Informática. Instituto Politécnico Nacional, Unidad Profesional Interdisciplinaria de Ingeniería y Ciencias Sociales y Administrativas, Sección de Estudios de Posgrado e Investigación, México D.F. enero 2016

CENTRO CIBERNETICO POLICIAL, Informe: Amenazas del Cibercrimen en Colombia 2016-2017. {En línea}. Marzo 2017{consultado el 28 de octubre de 2017} disponible en: (https://caivirtual.policia.gov.co/contenido/informe-amenazas-del-cibercrimen-en-colombia-2016-2017)

COLOMBIA. MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO, Decreto 1377 (27 de junio de 2013) Protección de Datos Personales. Presidencia. Bogotá D.C. {En línea}. {consultado el 09 de octubre de 2017} disponible en: https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

COLOMBIA. MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO, Decreto 886 (13 de mayo de 2014) Protección de la información y de los datos. Presidencia. Bogotá D.C. {En línea}. {consultado el 08 de octubre de 2017} disponible en: http://wsp.presidencia.gov.co/Normativa/Decretos/2014/Documents/MAYO/13/DECRETO%20886%20DEL%2013%20DE%20MAYO%20DE%202014.pdf

COLOMBIA. MINISTERIO DE DEFENSA. Análisis y gestión de riesgos. Herramienta Pilar. {En línea}. {consultado el 18 de octubre de 2017} disponible en: (https://www.aec.es/c/document_library/get_file?uuid=b3945e58-17f2-4dc0-88ac-863ae9f998cb&groupId=10128)

CONGRESO DE COLOMBIA, Ley 1273(5 de enero de 2009). De la protección de la información y de los datos. El Departamento. Bogotá D.C. {En línea}. {consultado

el 08 de octubre de 2017} disponible en: (http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf)

CONGRESO DE COLOMBIA, Ley 527 (21 de agosto de 1999) Acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales. El Departamento. Bogotá D.C {En línea}. {consultado el 08 de octubre de 2017} disponible en: http://www.mintic.gov.co/portal/604/articles-3679_documento.pdf

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL CONPES, Política Nacional de Seguridad Digital. {En línea}. 11 de abril de 2016 {08 de septiembre de 2017} disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

DELOITTE, La Evolución de la Gestión de Ciber-Riesgos y Seguridad de la Información. Encuesta 2016 sobre Tendencias de Ciber-Riesgos y Seguridad de la Información en Latinoamérica. {En línea}. Julio 2016{08 de septiembre de 2017} disponible en: (https://www2.deloitte.com/content/dam/Deloitte/co/Documents/risk/Deloitte 2016 Cyber Risk Information Security Study - Latinoamérica - Resultados Generales vf.pdf)

DIGITAL OCEAN, How To Install and Use Logwatch Log Analyzer and Reporter on a VPS . {En línea}. {05 de noviembre de 2017} disponible en: (https://www.digitalocean.com/community/tutorials/how-to-install-and-use-logwatch-log-analyzer-and-reporter-on-a-vps)

DVWA, Damn Vulnerable Web Application . {En línea}. {28 de octubre de 2017} disponible en: (http://www.dvwa.co.uk/)

EL PORTAL DE ISO 27001 EN ESPAÑOL, ISO 27000 Sistemas de gestión de seguridad de la información. {En línea}. {08 de septiembre de 2017} disponible en: (http://www.iso27000.es/iso27000.html)

ESET, Eset security report Latinoamerica 2017 {En línea}. {consultado el 28 de octubre de 2017} disponible en: (https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf)

ESET, Eset Tendencias Latinoamérica 2017 {En línea}. {consultado el 28 de octubre de 2017} disponible en: (https://www.welivesecurity.com/wp-content/uploads/2016/12/Tendencias-2017-eset.pdf)

ICBF, Resolucion 10806: Políticas de Seguridad de la Información. {En línea}. {consultado el 28 de octubre de 2017} disponible en: (http://www.icbf.gov.co/portal/page/portal/Descargas1/Tratamiento%20de%20datos/10806%20-

%20Adopta%20Pol%C3%ADtica%20de%20Seguridad%20de%20la%20Informaci%C3%B3n.pdf)

KASPERSKY, Qué es unbotnet?. {En línea}. {08 de septiembre de 2017} disponible en:. https://www.kaspersky.es/blog/que-es-un-botnet/755/

M. AMUTIO, J. CANDAU AND J. MAÑAS, Eds., MAGERIT – Versión 3.0. Metodología de Análisis y Gestión de Riesgos de los SI. Libros I, II y III - Método. 2012.

MENDIOLA ZURIARRAIN,José, et al. Ataques Informáticos. En: El País. Bogotá D.C. 16, octubre, 2017. {En línea}. {08 de septiembre de 2017} disponible en: (https://elpais.com/tag/ataques_informaticos/a).

MICROSOFT, Herramienta de Evaluación de Seguridad de Microsoft (MSAT). 2014 {En línea}. {08 de octubre de 2017} disponible en: (https://technet.microsoft.com/es-es/library/cc185712.aspx)

MICROSOFT, Microsoft Baseline Security Analyzer 2.3 (for IT Professionals). {En línea}. {18 de octubre de 2017} disponible en: (https://www.microsoft.com/en-us/download/details.aspx?id=7558)

MOLINA MIRANDA, María Fernanda. Propuesta de un Plan de Gestión de Riesgos de Tecnología aplicado en la Escuela Superior Politécnica del Litoral. Trabajo de Grado Máster Universitario en Ingeniería de Redes y Servicios Telemáticos. Madrid - España. Universidad Politécnica de Madrid - Escuela Técnica Superior de Ingenieros de Telecomunicación, 2015, {En línea}. {consultado el 28 de octubre de 2017} disponible en: (http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Maria_Fernanda_Molina_Miranda_2015.pdf)

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS OEA, Impacto de los incidentes de seguridad digital en Colombia 2017. {En línea}. {consultado el 08 de octubre de 2017} disponible en: https://publications.iadb.org/bitstream/handle/11319/8552/Impacto_de_los_incidentes_de_seguridad_digital.pdf?sequence=1&isAllowed=y

OWASP, OWASP WebScarab Project. . {En línea}. {18 de noviembre de 2017} disponible en: (https://www.owasp.org/index.php/Category:OWASP_WebScarab_Project)

PERAFÁN RUIZ, John Jairo. CAICEDO CUCHIMBA, Mildred, Análisis de Riesgos de la Seguridad de la Información para la Institución Universitaria Colegio Mayor Del Cauca. Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas Tecnología e Ingeniería. Especialización en Seguridad Informática. Popayán. 2014

{En línea}. {consultado el 09 de octubre de 2017} disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/2655/3/76327474.pdf

PILAR TOOLS, EAR/Pilar, Entorno de análisis de riesgos. {En línea}. {08 de octubre de 2017} disponible en: (http://www.ar-tools.com/es/index.html)

PILAR TOOLS, Pilar, manual de usuario. {En línea}. {08 de octubre de 2017} disponible en: (http://www.pilar-tools.com/doc/v62/manual_std_risk_es_2016-08-21.pdf)

SQLMAP®, Automatic SQL injection and database takeover tool. {En línea}. {18 de noviembre de 2017} disponible en: (http://sqlmap.org//)

SYMANTEC CORPORATION, Internet Security Threat Report 2014: Volume 19. {En línea}. Abril de 2014 {08 de septiembre de 2017} disponible en: (http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf)

TARLOGIC, Nessus Vulnerability Scanner. {En línea}. {18 de noviembre de 2017} disponible en: (https://www.tarlogic.com/productos/nessus-vulnerability-scanner/)

TECNÓSFERA CON INFORMACIÓN DE AGENCIAS. Un nuevo ataque cibernético mundial afecta a varias multinacionales En: El Tiempo, Bogotá D.C. 27 de junio 2017. {En línea}. 27 de junio de 2017 {consultado el 08 de octubre de 2017} disponible en: (http://www.eltiempo.com/tecnosfera/novedades-tecnologia/nuevo-ataque-cibernetico-afecta-a-empresas-en-el-mundo-103092)

TOMSITPRO, Windows 10 Local Security Policy Editor). {En línea}. {18 de noviembre de 2017} disponible en: (http://www.tomsitpro.com/articles/windows-10-local-security-policy-editor,2-15.html)

UNAM, Reporte de incidente de seguridad informática. {En línea}. {consultado el 18 de octubre de 2017} disponible en: (http://redyseguridad.fi-p.unam.mx/proyectos/politicas/desc/formato_reporte.pdf)

VELÁSQUEZ DURÁN, Ana María. Colombia, entre los países con más ciberataques. En: El Tiempo. Bogotá D.C. 18, septiembre, 2017.. {En línea}. {consultado el 10 de noviembre de 2017} disponible en: (http://redyseguridad.fi-p.unam.mx/proyectos/politicas/desc/formato_reporte.pdf)

WELIVESECURITY, ¿Qué es una Declaración de Aplicabilidad (SoA) y para qué sirve? {En línea}. 01 de abril de 2015 {28 de septiembre de 2017} disponible en:

(https://www.welivesecurity.com/la-es/2015/04/01/que-es-declaracion-de-aplicabilidad-soa/)

WELIVESECURITY, Bondat, botnet fantasma en Latinoamérica {En línea}. 25 de abril de 2013 {08 de noviembre de 2017} disponible en: (https://www.welivesecurity.com/la-es/2016/06/03/bondat-botnet-fantasma-latinoamerica/)

ISO27001:2013 - ANEXO A		
OBJETIVOS DE CONTROL Y CONTROLES		
A.5. POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN.	A.5.1. Orientación de la Dirección para la Gestión de la Seguridad de la Información.	A.5.1.1. Políticas para la Seguridad de la Información. Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la Dirección, publicada y comunicada a los empleados y partes interesadas.
	Objetivo. Brindar orientación y soporte, por parte de la dirección, de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.	A.5.1.2. Revisión de las Políticas para seguridad de la información. Las Políticas para Seguridad de la Información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su idoneidad, adecuación y eficacia continúas.
A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.	A.6.1. Organización Interna.	A.6.1.1. Seguridad de la Información Roles y Responsabilidades. Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
	Objetivo. Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación del SGSI.	A.6.1.2. Separación de deberes. Las tareas y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos de la organización.
		A.6.1.3. Contacto con las autoridades. Se debe mantener contactos apropiados con las autoridades pertinentes.
		A.6.1.4. Contacto con grupos de interés especial. Se deben mantener controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
		A.6.1.5. Seguridad de la información en Gestión de Proyectos. La seguridad de la información se debe tratar en la gestión de proyectos, independiente del tipo de proyecto,
	A.6.2. Dispositivos Móviles y Teletrabajo.	A.6.2.1. Política para dispositivos móviles. Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
	Objetivo. Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.	A.6.2.2. Teletrabajo. Se deben implementar una política y medidas de seguridad de soporte para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
	A.7.1. Antes de asumir el empleo.	A.7.1.1. Selección. Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
	Objetivo. Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.	A.7.1.2. Términos y condiciones del empleo. Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información.

ISO27001:2013 - ANEXO A		
OBJETIVOS DE CONTROL Y CONTROLES		
A.7. SEGURIDAD DE LOS RECURSOS HUMANOS.	A.7.2. Durante la ejecución del empleo.	A.7.2.1. Responsabilidades de la Dirección. La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la organización.
	Objetivo. Asegurarse que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.	A.7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información. Todos los empleados de la organización y donde sea pertinente, los contratistas deben recibir educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
		A.7.2.3. Proceso disciplinario. Se debe contar con un proceso formal y comunicado para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
	A.7.3. Terminación y cambio de empleo.	A.7.3.1. Terminación o cambio de responsabilidades de empleo. Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.
	Objetivo. Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.	
A.8. GESTIÓN DE ACTIVOS.	A.8.1. Responsabilidad por los Activos.	A.8.1.1. Inventario de Activos. Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
	Objetivo. Identificar los activos organizacionales y definir las responsabilidades de protección apropiada.	A.8.1.2. Propiedad de los activos. Los activos mantenidos en el inventario deben ser propios.
		A.8.1.3. Uso Aceptable de los Activos. Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
		A.8.1.4. Devolución de Activos. Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
	A.8.2. Clasificación de la Información.	A.8.2.1. Clasificación de la Información. La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
	Objetivo. Asegurar que la organización recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.	A.8.2.2. Etiquetado de la Información. Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.

ISO27001:2013 - ANEXO A		
OBJETIVOS DE CONTROL Y CONTROLES		
		A.8.2.3. Manejo de Activos. Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
	A.8.3. Manejo de medios de soporte.	A.8.3.1. Gestión de medios de Soporte Removibles. Se deben implementar procedimientos para la gestión de medios de soporte removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
	Objetivo. Prevenir la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios de soporte.	A.8.3.2. Disposición de los medios de soporte. Se debe disponer en forma segura de los medios de soporte cuando ya no se requieran, utilizando procedimientos formales.
		A.8.3.3. Transferencia de medios de soporte físicos. Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
A.9. CONTROL DE ACCESO.	A.9.1. Requisitos del Negocio para Control de Acceso.	A.9.1.1. Política de Control de Acceso. Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
	Objetivo. Limitar el acceso a información y a instalaciones de procesamiento de información.	A.9.1.2. Acceso a redes y a servicios en red. Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
	A.9.2. Gestión de Acceso de Usuarios.	A.9.2.1. Registro y cancelación del registro de usuarios. Se debe implementar un proceso formal de registro y de cancelación del registro para posibilitar la asignación de los derechos de acceso.
	Objetivo. Asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios.	A.9.2.2. Suministro de acceso de usuarios. Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o cancelar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.
		A.9.2.3. Gestión de derechos de acceso privilegiado. Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
		A.9.2.4. Gestión de información de autenticación secreta de usuarios. La asignación de información de autenticación secreta se debe controlar por medio de un procedimiento de gestión formal.
		A.9.2.5. Revisión de los derechos de acceso de usuarios. Los dueños de los activos deben revisar los derechos de acceso de los usuarios a intervalos regulares.
		A.9.2.6. Cancelación o ajuste de los derechos de acceso. Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procedimiento de información se deben cancelar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
	A.9.3. Responsabilidades de los usuarios.	A.9.3.1.Uso de información secreta. Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.

ISO27001:2013 - ANEXO A		
OBJETIVOS DE CONTROL Y CONTROLES		
	Objetivo. Hacer que los usuarios rindan cuentas por la custodia de su información de autenticación.	
	A.9.4. Control de Acceso a Sistemas y Aplicaciones.	A.9.4.1. Restricción de acceso a información. El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
	Objetivo. Prevenir el uso no autorizado de sistemas y aplicaciones.	A.9.4.2. Procedimiento de Conexión Segura. Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de conexión segura.
		A.9.4.3. Sistema de Gestión de Contraseñas.los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.
		A.9.4.4. Uso de programas utilitarios privilegiados. Se debe restringir y controlar estrechamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.
		A.9.4.5. Control de Acceso a Códigos Fuente de Programas. Se debe restringir el acceso a códigos fuente de programas.
A.10. CRIPTOGRAFÍA	A.10.1. Controles Criptográficos.	A.10.1.1. Política sobre el uso de controles Criptográficos. Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para protección de información.
	Objetivo. Asegurar el uso apropiado y eficaz de la criptografía para proteger la confiabilidad, la autenticidad y/o la integridad de la información.	A.10.1.2. Gestión de Claves. Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de claves criptográficas, durante todo su ciclo de vida.
	A.11.1. Áreas Seguras.	A.11.1.1. Perímetro de Seguridad Física. Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.
	Objetivo. Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.	A.11.1.2. Controles Físicos de entrada. Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.

ISO27001:2013 - ANEXO A		
OBJETIVOS DE CONTROL Y CONTROLES		
A.11. SEGURIDAD FÍSICA Y AMBIENTAL.		A.11.1.3. Seguridad de oficinas, salones e instalaciones. Se debe diseñar y aplicar seguridad física a oficinas, salones e instalaciones.
		A.11.1.4. Protección contra amenazas externas y ambientales. Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
		A.11.1.5. Trabajo en áreas seguras. Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.
		A.11.1.6. Áreas de despacho y carga. Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
	A.11.2. Equipos.	A.11.2.1. Ubicación y protección de los equipos. Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales y las posibilidades de acceso no autorizado.
	Objetivo. Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	A.11.2.2. Servicios Públicos de soporte. Los equipos se deben proteger de fallas de potencia y otras interrupciones causadas por fallas en los servicios públicos de soporte.
		A.11.2.3. Seguridad del cableado. El cableado de potencia y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptaciones, interferencia o daño.
		A.11.2.4. Mantenimiento de equipos. Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
		A.11.2.5. Retiro de Activos. Los equipos, información o software no se deben retirar de su sitio sin autorización previa.
		A.11.2.6. Seguridad de equipos y activos fuera del predio. Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de los predios de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichos predios.

ISO27001:2013 - ANEXO A		
OBJETIVOS DE CONTROL Y CONTROLES		
		A.11.2.7. Disposición segura o reutilización de equipos. Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software con licencia haya sido retirado o sobre escrito en forma segura antes de su disposición o reuso.
		A.11.2.8. Equipos sin supervisión de los usuarios. Los usuarios deben asegurarse de que el equipo sin supervisión tenga la protección apropiada.
		A.11.2.9. Política de escritorio limpio y pantalla limpia. Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información.
A.12. SEGURIDAD DE LAS	A.12.1. Procedimientos operacionales y responsabilidades.	A.12.1.1. Procedimientos de operación documentadas. Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan.
	Objetivo. Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.	A.12.1.2. Gestión de Cambios. Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
		A.12.1.3. Gestión de Capacidad. Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.
		A.12.1.4. Separación de los ambientes de desarrollo, ensayo y operación. Se deben separar los ambientes de desarrollo, ensayo y operativos, para reducir los riesgos de acceso o cambios no autorizados al ambiente operacional.
	A.12.2. Protección contra códigos maliciosos.	A.12.2.1. Controles contra códigos maliciosos. Se deben implementar controles de detección, de prevención y de recuperación, combinarlos con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
	Objetivo. Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.	
	A.12.3. Copias de Respaldo.	A.12.3.1. Copias de respaldo de la información. Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.
	Objetivo. Proteger contra la pérdida de datos.	
	A.12.4. Registro y Seguimiento.	A.12.4.1. Registro de eventos. Se deben elaborar, conservar y revisar regularmente los registros de eventos acerca de actividades del usuario, excepcionales, fallas y eventos de seguridad de la información.

ISO27001:2013 - ANEXO A		
OBJETIVOS DE CONTROL Y CONTROLES		
OPERACIONES.	Objetivo. Registrar eventos y generar evidencia.	A.12.4.2. Protección de la información de registro. Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.
		A.12.4.3. Registros del administrador y del operador. Las actividades del administrador y del operador del sistema se deben registrar y los registros se deben proteger y revisar con regularidad.
		A.12.4.4. Sincronización de relojes. Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.
	A.12.5. Control de Software Operacional.	A.12.5.1. Instalación de software en sistemas operativos. Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
	Objetivo. Asegurarse de la integridad de los sistemas operacionales.	
	A.12.6. Gestión de vulnerabilidad técnica.	A.12.6.1. Gestión de las vulnerabilidades técnicas. Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
	Objetivo. Prevenir el aprovechamiento de las vulnerabilidades técnicas.	A.12.6.2. Restricciones sobre la instalación de Software. Se debe establecer e implementar el reglamento de instalación de software por parte de los usuarios.
	A.12.7. Consideraciones sobre auditorías de sistemas de información.	A.12.7.1. Controles sobre auditorías de Sistemas de Información. Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
	Objetivo. Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.	
A.13. SEGURIDAD DE LAS COMUNICACIONES.	A.13.1. Gestión de Seguridad de Redes.	A.13.1.1. Controles de redes. Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
	Objetivo. Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.	A.13.1.2. Seguridad de los servicios de red. Se deben identificar los mecanismos de seguridad y los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.
		A.13.1.3. Separación en las redes. Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.
	A.13.2. Transferencia de información.	A.13.2.1. Políticas y procedimientos de transferencia de información. Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información, mediante el uso de todo tipo de instalaciones de comunicaciones.

ISO27001:2013 - ANEXO A		
OBJETIVOS DE CONTROL Y CONTROLES		
	Objetivo. Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.	A.13.2.2. Acuerdos sobre transferencia de información. Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.
		A.13.2.3. Mensajes electrónicos. Se debe proteger apropiadamente la información incluida en los mensajes electrónicos.
		A.13.2.4. Acuerdos de confidencialidad o de no divulgación. Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.	A.14.1. Requisitos de seguridad de los sistemas de información.	A.14.1.1. Análisis y especificación de requisitos de seguridad de la información. Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
	Objetivo. Garantizar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye los requisitos para sistemas de información que prestan servicios sobre redes públicas.	A.14.1.2. Seguridad de servicios de las aplicaciones en redes públicas. La información involucrada en servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
		A.14.1.3. Protección de transacciones de servicios de aplicaciones. La información involucrada en las transacciones de servicios de aplicaciones se debe proteger para prevenir la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes. La divulgación no autorizada y la duplicación o reproducción de mensajes no autorizados.
	A.14.2. Seguridad en los procesos de desarrollo y de soporte.	A.14.2.1. Política de desarrollo seguro. Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas a los desarrollos dentro de la organización.
	Objetivo. Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.	A.14.2.2. Procedimiento de control de cambios en sistemas. Los cambios a los sistemas dentro del ciclo de vida de desarrollo de software y de sistemas a los desarrollos dentro de la organización.
		A.14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones. Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y poner a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad organizacionales.
		A.14.2.4. Restricciones sobre los cambios de paquetes de software. Se deben desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.

ISO27001:2013 - ANEXO A		
OBJETIVOS DE CONTROL Y CONTROLES		
		A.14.2.5. Principios de construcción de sistemas de seguros. Se deben establecer, documentar y mantener principios para la organización de sistemas seguros, y aplicarlos a cualquier trabajo de implementación de sistemas de información.
		A.14.2.6. Ambiente de desarrollo seguro. Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
		A.14.2.7. Desarrollo contratado externamente. La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas subcontratados.
		A.14.2.8. Pruebas de seguridad de sistemas. Durante el desarrollo se deben llevar a cabo ensayos de funcionalidad de la seguridad.
		A.14.2.9. Pruebas de aceptación de sistemas. Para los sistemas de información nuevos, actualizaciones y nuevas versiones se deben establecer programas de ensayo y criterios relacionados.
	A.14.3. Datos de ensayo.	A.14.3.1. Protección de datos de ensayo. Los datos de ensayo se deben seleccionar, proteger y controlar cuidadosamente.
	Objetivo. Asegurar la protección de los datos usados para ensayos.	
A.15. RELACIONES CON LOS PROVEEDORES.	A.15.1. Seguridad de la información en las relaciones con los proveedores.	A.15.1.1. Política de seguridad de la información para las relaciones con proveedores. Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.
	Objetivo. Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.	A.15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores. Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que puedan tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.
		A.15.1.3. Cadena de suministro de tecnología de información y comunicación. Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.
	A.15.2. Gestión de la prestación de servicios de proveedores.	A.15.2.1. Seguimiento y revisión de los servicios de los proveedores. Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
	Objetivo. Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.	A.15.2.2. Gestión de cambios a los servicios de los proveedores. Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados y la reevaluación de los riesgos.
	A.16.1. Gestión de incidentes y mejoras en la seguridad de la información.	A.16.1.1. Responsabilidades y procedimientos. Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

ISO27001:2013 - ANEXO A		
OBJETIVOS DE CONTROL Y CONTROLES		
A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.	Objetivo. Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidad.	A.16.1.2. Informe de eventos de seguridad de la información. Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible.
		A.16.1.3. Informe de debilidades de seguridad de la información. Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que se observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
		A.16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.
		A.16.1.5. Respuesta a incidentes de seguridad de la información. Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
		A.16.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información. El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.
		A.16.1.7. Recolección de evidencia. La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO.	A.17.1. Continuidad de seguridad de la información	A.17.1.1. Planificación de la continuidad de la seguridad de la información. La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastres.
	Objetivo. La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.	A.17.1.2. Implementación de la continuidad de la seguridad de la información. La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
		A.17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información. La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información implementados con el fin de asegurar que los válidos y eficaces durante situaciones adversas.
	A.17.2. Redundancia	A.17.2.1. Disponibilidad de instalaciones de procesamiento de información. Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
	Objetivo. Asegurarse de la disponibilidad de instalaciones de procesamiento de información.	

ISO27001:2013 - ANEXO A		
OBJETIVOS DE CONTROL Y CONTROLES		
A.18. CUMPLIMIENTO.	A.18.1. Cumplimiento de requisitos legales y contractuales.	A.18.1.1. Identificación de los requisitos de legislación y contractuales aplicables. Se deben identificar, documentar y mantener actualizados explícitamente todos los requisitos legislativos estatutarios, de reglamentación y contractuales pertinentes, y el enfoque de la organización para cada sistema de información y para la organización.
	Objetivo. Evitar violaciones de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.	A.18.1.2. Derechos de Propiedad Intelectual. Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software licenciados.
		A.18.1.3. Protección de registros. Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
		A.18.1.4. Privacidad y protección de la información identificable personalmente. Se deben asegurar la privacidad y la protección de la información identificable personalmente, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.
		A.18.1.5. Reglamentación de Controles Criptográficos. Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos
	A.18.2. Revisiones de seguridad de la información	A.18.2.1. Revisión independiente de la seguridad de la información. El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, la políticas, los procesos y los procedimientos para seguridad de la información se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
	Objetivo. Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimiento organizacionales.	A.18.2.2. Cumplimiento con las políticas y normas de seguridad. Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas y cualquier otro requisito de seguridad.
		A.18.2.3. Revisión del Cumplimiento Técnico. Los Sistemas de información se deben revisar con regularidad para determinar el cumplimiento con las políticas y normas de seguridad de la información.

Anexo B. Documentos Escaneados

CARTA RADICADA DE SOLICITUD A LA EMPRESA.

Fusagasugá, octubre 11 de 2017

Transportes Tierra Grata y Cía. Ltda.
FECHA 11/octubre/2017
HORA 10:19 am.
RECIBÍ

Señores

TRANSPORTES TIERRA GRATA Y CIA LTDA

La ciudad

Cordial saludo, deseándoles éxitos en sus actividades diarias.

La presente, va con el fin de solicitar se me permita realizar una actividad academica dentro de su empresa, la cual consiste en la elaboración del **Diseño de Controles de Seguridad para los Activos Informáticos en la empresa Transportes Tierra Grata y Compañía Ltda**, esto con el fin de cumplir con los requisitos del proyecto de grado de la **Especialización de Seguridad Informática** de la Universidad Nacional Abierta y a Distancia, que busca que se puedan realizar las diferentes fases dentro de los cursos Proyecto de Seguridad Informática I y II.

Los ítems a realizar son:

- Identificar los riesgos, las vulnerabilidades e impactos que puedan tener las pérdidas de confiabilidad, integridad y disponibilidad sobre los activos de la empresa Transportes Tierra Grata y Compañía Ltda
- Establecer índices de gestión para el control de seguridad de activos informáticos capaces de permitir una pronta detección y de respuesta a incidentes de seguridad
- Mediante una metodología de análisis de riesgos se identifican qué activos informáticos son los más críticos y de mayor impacto que requieren mayores controles de seguridad y así establecer un plan para la continuidad de los servicios.
- Definir controles de seguridad que posibiliten asegurar la disponibilidad, confiabilidad y continuidad de los activos, ofreciendo unos adecuados niveles de servicio

El compromiso con la empresa esta dado en que, si la investigación tiene viabilidad, la empresa tendrá derechos sobre el documento resultante y su respectiva copia para uso interno.

Agradezco la colaboración que pudieren prestarme en este aspecto.

Cordialmente,

Ing- YON IVAN MARQUEZ BUITRAGO

CC 82391374

CARTA DE APROBACION POR PARTE DE LA EMPRESA

Transportes Tierra Grata y Cia Ltda

NIT 800.041.255-9

Servicio de Calidad con Eficiencia y Responsabilidad

Fusagasugá, noviembre 21 de 2017

Señores

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

La ciudad

Cordial saludo, deseándoles éxitos en sus actividades diarias.

La presente, va con el fin de aprobar al Ingeniero de Sistemas **YON IVAN MARQUEZ BUITRAGO**, identificado con cedula de ciudadanía número de 82391374 de Fusagasugá, la realización del proyecto titulado **Diseño de Controles de Seguridad para los Activos Informáticos en la empresa Transportes Tierra Grata y Compañía Ltda. de** Fusagasugá, esto con el fin de cumplir con los requisitos del proyecto de grado de la **Especialización de Seguridad Informática** de la Universidad Nacional Abierta y a Distancia, que busca que se puedan realizar las diferentes fases dentro de los cursos Proyecto de Seguridad Informática I y II.

Objetivo General:

Diseñar los Controles de Seguridad para los Activos Informáticos en la empresa Transportes Tierra Grata y Compañía Ltda. de Fusagasugá haciendo uso de metodologías para análisis y control del riesgo, basados en la norma ISO 27001:2013.

Objetivos Específicos:

1. Identificar los riesgos, las vulnerabilidades e impactos que puedan tener los activos de información de la empresa Transportes Tierra Grata y Compañía Ltda.
2. Establecer índices de gestión para el control de seguridad de activos informáticos capaces de permitir una pronta detección y de respuesta a incidentes de seguridad
3. Definir controles de seguridad que posibiliten asegurar la disponibilidad, confiabilidad y continuidad de los activos, ofreciendo unos adecuados niveles de servicio
4. Realizar la Declaración de Aplicabilidad (SoA) que permite mantener el registro y control de las medidas de seguridad que se aplican socializándolos con la alta dirección de la empresa Transportes Tierra Grata y Compañía Ltda.

El compromiso con la empresa está dado en que, si el proyecto tiene viabilidad, la empresa tendrá derechos sobre los productos resultantes para uso interno.

Agradezco la colaboración que pudieren prestarme en este aspecto.

Cordialmente,

JORGE HUMBERTO PULIDO PARDO
GERENTE
TRANSPORTES TIERRA GRATA Y CIA LTDA

VIGILADO SUPERTRANSPORTE

FUSAGASUGÁ
Gerencia: calle 19 No. 10-12
Tel fijo 871 7185 Celular 320 3496886 E-Mail: transttgrata@hotmail.com
Terminal de Transportes: taquilla No. 07 Teléfono 867 1841
BOGOTÁ, D.C.
Terminal Salitre: modulo amarillo, taquilla No. 128A Teléfono 5708880
Terminal del sur: taquilla No. 42

APROBACION DE SOCIALIZACION Y ASISTENCIA

Transportes Tierra Grata y Cia Ltda

NIT 800.041.255-9

Servicio de Calidad con Eficiencia y Responsabilidad

Fusagasugá 21 de mayo de 2018.

Señor
YON IVAN MARQUEZ BUITRAGO
Ingeniero de Sistemas

REF: Aprobación socialización

Cordialmente le informamos que le fue aprobada la socialización de los objetivos de la elaboración del proyecto Diseño de Controles de Seguridad para los Activos Informáticos que se llevó acabo en la empresa Transportes Tierra Grata y Compañia Ltda.

Los ítems a socializar:

- Dar a conocer el resultado de la investigación realizada sobre los riesgos, las vulnerabilidades e impactos que puedan tener las pérdidas de confiabilidad, integridad y disponibilidad sobre los activos de la empresa Transportes Tierra Grata y Compañia Ltda.
- Informar sobre los índices de gestión para el control de seguridad de activos informáticos capaces de permitir una pronta detección y de respuesta a incidentes de seguridad
- Rendición de informe sobre los activos informáticos más críticos y de mayor impacto que requieren mayores controles de seguridad y estableciendo un plan para la continuidad de los servicios.
- Dar a conocer los controles de seguridad que posibiliten asegurar la disponibilidad, confiabilidad y continuidad de los activos, ofreciendo unos adecuados niveles de servicio.

El día autorizado para dicha socialización es el día 23 de mayo de 2018, a las 8:00 a.m. en las instalaciones ubicadas en la Calle 19 # 10-12 Barrio Balmoral.

Esperamos contar con su puntualidad.

Atentamente,

LINA MARIA ACOSTA MORENO
ASISTENTE DE GERENCIA
Transportes Tierra Grata y Cia Ltda.

VIGILADO SUPERTRANSPORTE

FUSAGASUGÁ
Gerencia: calle 19 No. 10-12
Tel fijo 871 7185 Celular 320 3496886 E-Mail: transttgrata@hotmail.com
Terminal de Transportes: taquilla No. 07 Teléfono 867 1841
BOGOTÁ, D.C.
Terminal Salitre: modulo amarillo, taquilla No. 128A Teléfono 5708880
Terminal del sur: taquilla No. 42

Transportes Tierra Grata y Cia Ltda

NIT 800.041.255-9

Servicio de Calidad con Eficiencia y Responsabilidad

PARTICIPACION EMPLEADOS ADMINISTRATIVOS DE LA EMPRESA TRANSPORTES TIERRA GRATA Y COMPAÑÍA LIMITADA EN LA SOCIALIZACION DEL PROYECTO DISEÑO DE CONTROLES DE SEGURIDAD PARA LOS ACTIVOS INFORMÁTICOS.

NOMBRE	CARGO	CEDULA
Ana Delia Galindo	Asistente Contable	52849518
KAREN LIZETH CONTRERAS	Auxiliar Contable	1067956901
Francisco Alberto Benitez M	Jefe Contable	82390296
Alexandra Benedetti M.	Practicante	53015861
CARLOS ARTURO FUYA	ASIST. CONTABILIDAD	1069.719.404
Monica V. Rodriguez	J. Talento Humano	1.012.3[illegible]
Lina Maria Acosta Moreno.	Asistente de Gerencia.	1069742643.

Se firma a los 23 dias del mes de mayo de 2018 en las instalaciones administrativas de la empresa TRANSPORTES TIERRA GRATA Y COMPAÑÍA LIMITADA.

YON IVAN MARQUEZ BUITRAGO
CAPACITADOR

VIGILADO SUPERTRANSPORTE

FUSAGASUGA
Gerencia: calle 19 No. 10-12
Tel fijo 871 7185 Celular 320 3496886 E-Mail: transttgrata@hotmail.com
Terminal de Transportes: taquilla No. 07 Teléfono 867 1841
BOGOTÁ, D.C.
Terminal Salitre: modulo amarillo, taquilla No. 128A Teléfono 5708880
Terminal del sur: taquilla No. 42

Anexo C. ENTREVISTA APLICADA

Nombre de la empresa: TRANSPORTES TIERRA GRATA Y COMPANIA LTDA
Nombre y Cargo de las personas entrevistadas: FRANCISCO ALBERTO BENITEZ MANJARRES (Contador) y YON IVAN MARQUEZ (Asesor TIC)

Fecha: 11/09/2017

En esta fase del trabajo que se está elaborando por parte de un profesional a la Empresa TRANSPORTES TIERRA GRATA Y COMPANIA LTDA, en la siguiente entrevista a cada uno de los funcionarios y usuario del sistema dentro de la Empresas, se hará una serie de consultas, para detectar las posibles fallas y requerimientos necesarios para el buen funcionamiento de la Empresa.

A. ¿Cómo se ve usted como Empresa?

R/ El Empleado de una Empresa, debe asumir el rol de la responsabilidad Técnica, Administrativa y Financiara, para que haya un buen desempeño y eficacia dentro de la misma.

B. ¿Con cuantas Sedes cuenta la empresa?

R/. Con una principal en la Ciudad de Fusagasugá donde se concentra la planta administrativa, una oficina y una taquilla en el Terminal de Transportes de Fusagasugá, Una taquilla en la Terminal de Transportes del Salitre en Bogotá y otra taquilla en el Terminal del Sur de Bogotá.

C. ¿Con que equipos sofisticados trabaja la Empresa en Tecnología?

R/. Realmente en la Empresa solo hay equipo de Tecnología en una fase media, le falta implementación de software de control administrativo.

D. ¿Cuál es la actividad critica que tenga que ver con procesos informáticos que se hace en la empresa?

R/. El proceso principal es la recolección, transporte y contabilización de la venta de tiquetes ya que es un proceso que se hace desde cada taquilla, allí se llenan los despachos tanto en la página de internet habilitada para tal objetivo, así mismo de forma manual para que los supervisores lleven las cuentas a la empresa. La plata se consigna al banco de acuerdo al lugar de ubicación del supervisor y luego envían o se acercan con las consignaciones y las planillas de control. Esto es desgastante ya que es un proceso que se debe hacer a diario.

E. ¿Con respecto a los aspectos generales de la Seguridad en Redes, cree usted que es suficiente la existente?

R/. En realidad, es muy baja por el firewall que se implementa en el sistema operativo, se debe aplicar una metodología basada en protocolos que permita salvaguardar los datos y la información que a diario se suministra.

F. . ¿Qué medidas internas concretas utilizan en la empresa u organización, con respecto a las medidas que se deben tener en cuenta en las organizaciones mediante el filtrado de diversos protocolos en los routers de acceso?

R/. En el router no sabemos qué medidas se tengan porque dependen directamente del proveedor, de igual manera no tenemos filtrado a nivel de servicios, puertos y protocolos ni tampoco se maneja en equipos UTM tanto de entrada como de salida, en si no hay políticas bien definidas de acuerdo al servicio prestado.

G. Con respecto a que gran parte de los ataques que se producen son debidos a la obtención de las claves empleando un programa de sniffing en una red Ethernet.

Pregunta 1:¿Está preparada la Empresa para contrarrestar un ataque a las Redes y equipamiento en general?

R/. Generalmente no existe una política de seguridad, ni un plan de contingencia que determine que reacciones y acciones tomar en el momento de presentarse un incidente informático.

Pregunta 2: Cual estrategia tienen planteada en su empresa para contrarrestar estos ataques a la seguridad?

R/. No existe estrategia como tal, ni tampoco se tienen políticas configuradas en algún firewall de acuerdo a servicios, protocolos y puertos desde internet, hacia internet y entre zonas, que permiten en cierto grado minimizar este tipo de amenaza, además por la funcionalidad de protección de servidores http o de correo mediante el IPS.

Pregunta 3: Que estrategias utilizan para descongestionar el tráfico y para permitir una mayor descongestión del tráfico interno.

R/. No se tiene segmentada la red, ni el diseño del direccionamiento y el subneting de acuerdo al número de equipos por segmento además de la creación de VLANs que son los que mejoran el rendimiento de la red y eliminan tráfico innecesario no están configurados, tampoco está configurado NAT para equipos de uso administrativo ni el servicio Proxy para todos los equipos; para agilizar las búsquedas de recursos compartidos y equipos en red debería tenerse configurado un servidor Wins.

Pregunta 4: En la empresa se han presentado ataques informáticos? ¿De qué clase? Por favor describirlos a detalle.

R/. Hubo un ataque hace 1 año aproximadamente donde se comprometió la seguridad, configuración e información del servidor web y de correo en ese entonces, al parecer se aprovechó un agujero de seguridad en un framework de programación utilizado y abrió un puerto ftp embebido con privilegios por consola, hicieron escalada de privilegios y afectaron la interfaz gráfica, algunos servicios y archivos y obtuvieron la clave de acceso al motor mysql, esto se dio por desconocimiento en aspectos de seguridad y la falta de un escenario de pruebas para no comprometer directamente el servidor de

producción y primero haber probado el aplicativo y funcionalidades del mismo.

Además de esto, se tuvo una pérdida de información por modificación de datos en algunos archivos de Excel que controlan el ingreso de datos económicos, frente a este ataque no se pudo definir si era una incursión externa o si hubo sabotaje interno.

Pregunta 4: Que mecanismos y que servicios de seguridad se usa en la empresa?

R/. Ninguno en realidad. Se considera que se debería tener UTM con los módulos de filtrado, protección y análisis de tráfico, Sistema de protección Antivirus, Firewall personal por equipo (Administrativos), segmentación de red y diseño del direccionamiento con subneting. En la parte física se tienen 6 cámaras IP, un sistemas de alarmas en la sede principal

Pregunta5: Describa con sus palabras que haría por la seguridad de la Empresa?

R/. Como usuario de la Empresa y conociendo los movimientos que hay dentro de la Organización, contrataría una Empresa y un grupo de profesionales para que hagan un análisis profundo de las redes que están en servicio y junto a este test, se determinar que tipo de controles se deben implementar a cada uno de los activos que pertenecen a la Empresa y, por consiguiente aportar los recursos informáticos para el buen funcionamiento de la Empresa.

H. Con respecto a la Ubicación Del IDS En Una Organización. Mecanismos de Seguridad

Pregunta: Existen principalmente tres zonas en las que podríamos poner un sensor – Si lo tienen en que zona está ubicado, si no donde lo ubicarían.

R. / No se tiene, se debe tener en cuenta que el UTM incorpora un sistema IPS y este debería encontrarse activo en dos zonas, la primera es a la

entrada del canal de Internet e Interconexión con las sede alternas y en la zona DMZ.

I. Con respecto a los tipos de amenazas humanas. Los actos humanos que pueden afectar la seguridad de un sistema son variados, entre los más comunes e importantes están: Curiosos, Intrusos remunerados, Personal enterado, Terroristas, Robo, Sabotaje, Fraude.

Pregunta: Cuál de estos tipos de amenaza se ha presentado en su empresa?

R./ Si hubiese un buen sistema de seguridad informático los IPS en sus logs de corta duración, generalmente informarían de intentos de ataque a los servidores, al parecer según los ataques que se previenen vienen de herramientas de scanning y sniffing, creemos que pueden ser personas Curiosas o Personas entrenadas. También se han tenido casos de robo, sabotaje y fraude debido a que el dinero se movía físicamente entre sedes.

J. Con respecto a la Implementación de plan de seguridad Para la implementación del Plan de Seguridad para cualquier organización, se debe tener en cuenta principalmente aquellas herramientas que nos permitirán tener una información confiable mediante archivos de trazas o logísticos de todos los intentos de conexión que se han producido sobre un sistema, así como intentos de ataque de forma sistemática a puertos tanto de TCP como de UDP.

Pregunta: Describa el Plan de Seguridad Implementado en la organización

R/. Actualmente la Empresa No tiene un plan de seguridad implementado. Dentro de las recomendaciones hechas, se sugiere comenzar con un estudio de análisis de riesgos para evaluar el nivel de seguridad actual en la Institución, según los resultados obtenidos generar un marco de trabajo que permita establecer la adopción de controles para los riesgos encontrados, diseñar políticas de seguridad y aprobar en un futuro la implantación de un Sistema de Gestión de Seguridad de la Información.

ANEXO D. Cuestionario: Estado de la seguridad de la información

Nombre Cargo Fecha

SECCIÓN I Información general

1. Seleccione por favor la cantidad de pesos colombinos que mejor representa los ingresos anuales brutos o el presupuesto operativo para su organización, incluya todas las plantas, divisiones, ramas, matrices y subsidiarias en todo el mundo

	No aplica (no lucrativo/gobierno/educación
	Menos de $25 millones
	De $25 a $99 millones
	De $100 a $ 499 millones
	De $500 a $ 999 millones
	De $1 a $4.9 miles de millones
	De $5 a $9.9 miles de millones
	De $10 a 14.9 miles de millones
	De $15 a 24.9 miles de millones
	Más de $ 25 mil de millones
	No sé

2. ¿Aproximadamente a cuántas personas emplea su organización o empresa entera? (Por favor incluya todas las plantas, divisiones, ramas, matrices y subsidiarias en todo el mundo

	De 1 a 10
	De 11 a 50
	De 51 a 100
	De 101 a 500
	De 501 a 1.000
	De 1.001 a 5.000
	De 5.001 a 10.000
	De 10.001 a 20.000
	De 20.001 a 50.000
	De 50.001 a 75.000
	De 75.001 a 100.000
	De 100.001 a 200.000
	Más de 200.000
	No se

3. ¿Algunos de los siguientes forman parte de la responsabilidad de su organización en cuanto a la información de seguridad?

	Privacidad
	Continuidad/ recuperación de desastres empresariales

Presupuesto para tecnología de la información, (2018) (Hardware/ Software/ Salarios/ Consultores/ Otro) (Por favor responda en pesos colombianos)

4. Proporcione su mejor estimación del dinero total invertido en tecnología de la información. Esto debe reflejar el presupuesto destinado a la tecnología de la información MÁS el dinero usado de cualquier otro presupuesto o departamento para tratar asuntos relacionados con la tecnología de la información.

	Menos de $500,000
	De $500,000 a $999,999
	De $1 a $4,9 millones
	De $5 a $9.9 millones
	De $10 a $49,9 millones
	De $50 a $99.9 millones
	De $100 a $499,9 millones
	De $500 a $999,9 millones
	Mil millones o más
	No sé

Presupuesto para tecnología de la Información para el 2018 incluyendo Hardware/ Software/ Salarios/ Consultores/ otro. (Por favor responda en pesos colombianos)

5. Proporcione por favor su mejor estimación del dinero total invertido en seguridad de la información. Esto debe reflejar el presupuesto para seguridad de la información MÁS el dinero usado de cualquier otro presupuesto o departamento para tratar asuntos relacionados con la seguridad de la información.

	Menos de $10,000
	De $10,000 a $49,999
	De $50,000 a $99,999
	De $100,000 a $499,999
	De $500,000 a $999,999
	De $1 a $1,9 millones
	De $2 a $4,9 millones
	De $5 a $9,9 millones
	De $10 a $19,9 millones
	De $20 a $29,9 millones
	$30 millones o más
	No sé

6. Comparado con el año pasado, el gasto en seguridad para los próximos 12 meses:

	Aumentará más de 30%
	Aumentará 11-30%
	Aumentará hasta un máximo de 10%
	Permanecerá igual
	Disminuirá hasta un mínimo de 10%
	Disminuirá 11-30%

	Disminuirá más de 30%
	No sé

SECCIÓN II Las implicaciones de la depresión del mercado actual en la función de seguridad

7. ¿qué efecto ha tenido la actual depresión económica en la función de seguridad de su compañía?

	En desacuerdo	Algo de acuerdo	De acuerdo	Totalmente de acuerdo	No sé
Las amenazas a la seguridad de nuestros recursos de información han aumentado.					
Los esfuerzos para reducir los costos hacen que sea más difícil lograr la seguridad adecuada.					
El ambiente normativo se ha hecho más complejo y gravoso.					
Puesto que nuestros socios comerciales se han debilitado con la depresión, nosotros enfrentamos riesgos de seguridad adicionales.					
Puesto que los proveedores se han debilitado con la depresión, nosotros enfrentamos riesgos de seguridad adicionales.					
Los riesgos de la información de la compañía han aumentado debido a los despidos temporales de empleados.					
La depresión no ha sido tan grave para nuestro negocio como ha sido para otros.					
La depresión no ha afectado nuestra función de seguridad					
El ambiente de riesgo aumentado a elevado el papel e importancia de la función de seguridad					

8. ¿Para continuar cumpliendo con sus objetivos de seguridad en el contexto de estas realidades económicas más difíciles? ¿qué tan importantes son las siguientes estrategias?

	No son importantes	Algo importantes	Importantes	Muy importantes	Son de suma prioridad en este momento	No sé
La cancelación, aplazamiento o reducción de las iniciativas						

relacionadas con la seguridad que requieren gastos de capital						
La cancelación, aplazamiento o reducción de las iniciativas relacionadas con la seguridad que requieren gastos operativos.						
Asignar prioridades a inversiones de seguridad con base en el riesgo.						
Incrementar el enfoque en la protección de la información. Buscar una configuración más completa de las herramientas DLP (Data Lost Prevention)						
Acelerar la adopción de tecnologías de automatización relacionadas con la seguridad para aumentar la eficiencia y reducir el costo.						
Aumentar la dependencia en servicios de seguridad administrados.						
Mejorar la administración de privilegios.						
Reducir el número de personal de seguridad de tiempo completo. Emplear más personal de seguridad temporal o de medio tiempo.						
Asignar tareas relacionadas con la seguridad a empleados de tecnología de la información que no son de seguridad.						
Preparar una nueva ola de requerimientos relacionados con la seguridad reglamentaria.						
Adoptar un marco de trabajo de seguridad reconocido como medio para preparar los requerimientos regulatorios futuros.						
Reforzar la autoridad, el riesgo y programa de conformidad de la compañía.						
Volverse a enfocar en el núcleo de la estrategia existente.						
Reducir, mitigar o transferir riesgos mayores						

Extraer beneficios de seguridad indirectos de los esfuerzos de reducción de costos.						

9. ¿Su compañía ha aplazado cualquier iniciativa relacionada con la seguridad que requiere gastos de CAPITAL en el 2017?

	No ha aplazado
	Ha aplazado por menos de 6 meses
	Ha aplazado de 6 a 12 meses
	Ha aplazado por 1 año o más

10. ¿Su compañía ha reducido presupuestos para cualquier iniciativa relacionada con la seguridad de requiera gastos de CAPITAL en el 2017?

	No ha reducido
	Ha reducido el costo de la iniciativa entre 1 y 9 %
	Ha reducido el costo de la iniciativa entre 10 y 19 %
	Ha reducido el costo de la iniciativa entre 20 y 39 %
	Ha reducido el costo de la iniciativa entre 40 y 49 %
	Ha reducido el costo de la iniciativa más de 50%

11. ¿Su compañía ha aplazado cualquier iniciativa relacionada con la seguridad que requiere gastos OPERATIVOS en el 2017?

	No ha aplazado
	Ha aplazado por menos de 6 meses
	Ha aplazado de 6 a 12 meses
	Ha aplazado por 1 año o más

12. ¿Su compañía ha reducido presupuestos para cualquier iniciativa relacionada con la seguridad de requiera gastos OPERATIVOS en el 2017?

	No ha reducido
	Ha reducido el costo de la iniciativa entre 1 y 9 %
	Ha reducido el costo de la iniciativa entre 10 y 19 %
	Ha reducido el costo de la iniciativa entre 20 y 39 %
	Ha reducido el costo de la iniciativa entre 40 y 49 %
	Ha reducido el costo de la iniciativa más de 50%

SECCIÓN III Arquitectura y tecnologías de seguridad

Esta sección identifica un número de elementos de seguridad que pueden tener un impacto en el perfil de seguridad de una organización.

13. ¿Con qué frecuencia realiza usted una evaluación de riesgos empresariales?

	Dos veces al año (o más)
	Una vez al año

	Menos de una vez al año
	No realizo una evaluación de riesgos empresariales

14. ¿Con qué salvaguardias para la privacidad de la información cuenta su organización? (Marque TODAS las opciones aplicables)

Personas	
	Empleamos a un Director de Privacidad
	Requerimos a nuestros empleados certificar por escrito que están cumpliendo con nuestras políticas de privacidad.
	Requerimos a nuestros empleados completar una capacitación en políticas y prácticas de privacidad.
	Proveemos a nuestros empleados una capacitación en políticas y prácticas de privacidad

Proceso	
	Política de privacidad publicada en nuestro sitio web interno
	Política de privacidad publicada en nuestro sitio web externo
	Política de privacidad revisada al menos una vez al año
	Realizamos pruebas de privacidad internas (por ejemplo, a través de auditorías internas)
	Auditamos las normas de privacidad a través de una evaluación de terceros. Inventario preciso de donde se recogen, trasmiten y almacenan los datos de los empleados y los clientes.
	Inventario preciso de las ubicaciones o jurisdicciones donde se almacenan los datos
	Debida gestión de terceros que manejan los datos personales de clientes y empleados.
	Proceso de respuesta de incidentes para informar incumplimientos o infracciones a terceros a cargo del manejo de los datos.
	Inventario de todos los terceros que manejan datos personales de los empleados y clientes.
	Requerimos a todos los terceros (incluyendo subcontratistas) cumplir con nuestras políticas de privacidad.

Tecnología	
	Cifrado del disco completo en computadoras portátiles.
	Copia masiva en dispositivos externos (por ejemplo, USB) bloqueados
	Trasmisión de datos cifrados
	Controles de acceso actualizados
	Transacciones web seguras

	No sé

	Otro (por favor especifique)

15. ¿Con qué salvaguardias de seguridad de la información relacionadas con PERSONAS cuenta con su organización? (Marque TODAS las opciones aplicables)

	Actualmente implementamos	No implementamos pero es una prioridad para los próximos 12 meses
Empleamos a un gerente de seguridad de la información		
Empleamos a un director de seguridad		
Empleamos guardias de seguridad u otras medidas de seguridad físicas para la infraestructura de información.		
Empleamos a consultores de seguridad de la información		
Tenemos gente dedicada a programas de concientización del empleado en las políticas, procedimientos y estándares técnicos internos.		
Realizamos verificaciones de antecedentes del personal		
Tenemos gente dedicada a supervisar el uso de los activos de Internet/ información por parte de los empleados		
Integramos el personal de seguridad físico con el de seguridad de la información		
Vinculamos la seguridad, ya sea a través de una estructura o política organizacional, con el cumplimiento de las normas.		
Asignar tareas y capacitar al personal de tecnología de información como “representantes de cuenta” que sirvan al negocio interno		

16. ¿Con qué salvaguardias de PROCESO de seguridad de la información cuenta su organización? (Marque TODAS las opciones aplicables)

Estrategia y estándares			
	Actualmente implementamos	Actualmente subcontratamos	No implementamos pero es una prioridad para los próximos 12 meses
Estrategia global de seguridad de la información			
Lineamientos básicos de seguridad establecidos para socios/ clientes/ proveedores/ vendedores externos			
Proceso centralizado de administración de la información de seguridad			
Estándares/ procedimientos establecidos para el despliegue de la infraestructura.			
Estrategia de gestión de identidades			
Planes de continuidad/ recuperación de desastres empresariales			
Procedimientos/ estándares de seguridad para dispositivos portátiles (por ejemplo memoria flash, unidad externa)			
Niveles de autenticación en capas basados en la clasificación del riesgo del usuario			
Estándares/procedimientos de seguridad para : celulares/ PCS/ inalámbricos			
Programa de capacitación para la concientización de los empleados acerca de la seguridad.			
Ninguna de las anteriores.			

Evaluación y conformidad			
	Actualmente implementamos	Actualmente subcontratamos	No implementamos pero es una prioridad para los próximos 12 meses
Monitoreo/ análisis activo de la inteligencia de la seguridad de la información (por ejemplo informes de vulnerabilidad, archivos de registros)			
Pruebas de conformidad			
Auditorías de seguridad			
Pruebas de penetración			
Evaluación de amenazas y vulnerabilidad			
Evaluaciones de riesgo (internas)			

Evaluaciones de riesgo (por terceros)			
Integración con planes de privacidad/conformidad			
Auditorías/ monitoreos de conformidad de usuarios con la política de seguridad			
Auditorías/ monitoreos de publicaciones de empleados en blogs externos o sitios de redes de socialización			
Ninguna de las anteriores			

Operaciones			
	Actualmente implementamos	Actualmente subcontratamos	No implementamos pero es una prioridad para los próximos 12 meses
Operaciones del centro de datos			
Eliminación segura del hardware tecnológico			
Administración delegada del restablecimiento de contraseñas.			
Seguridad subcontratada (parte o toda)			
Ninguna de las anteriores			

17. ¿Con qué salvaguardias de TECNOLOGÍA para la seguridad de la información cuenta su organización? (Marque TODAS las opciones aplicables)

Firewalls			
	Actualmente implementamos	Actualmente subcontratamos	No implementamos pero es una prioridad para los próximos 12 meses
Firewalls de aplicaciones			
Firewalls de redes			
Firewalls de usuario final/ personales			
Ninguna de las anteriores			

Usuario			
	Actualmente implementamos	Actualmente subcontratamos	No implementamos pero es una prioridad para los próximos 12 meses
Aprovisionamiento automatizado de cuentas			
Biometría			
Restablecimiento de contraseñas automatizado			
Soluciones de administración de identidades			
Almacén centralizado de datos de usuario			
Contraseñas desechables/ tarjetas inteligentes/ fichas para autenticación.			
Software de inicio de sesión reducido/único			
Herramientas de monitoreo de actividad de los usuarios			
Ninguna de las anteriores			

Cifrado			
	Actualmente implementamos	Actualmente subcontratamos	No implementamos pero es una prioridad para los próximos 12 meses
Bases de datos			
Recursos compartidos de archivos			
Computadoras portátiles			
Cintas de respaldo			
Medios extraíbles			
Ninguna de las anteriores			

18. ¿Con qué salvaguardias de TECNOLOGÍA para la seguridad de la información cuenta su organización? (Marque TODAS las opciones aplicables)

Detección			
	Actualmente implementamos	Actualmente subcontratamos	No implementamos pero es una prioridad para los próximos 12 meses
Herramientas de detección de código malicioso (spyware y adware)			
Herramientas para detectar dispositivos no autorizados			
Herramientas de detección de intrusiones			
Suscripción a servicios de alertas de vulnerabilidad			
Herramientas de escaneo de vulnerabilidad			
Herramientas de correlación de eventos de seguridad			
Herramientas de prevención de fuga de datos			
Ninguna de las anteriores			

Prevención			
	Actualmente implementamos	Actualmente subcontratamos	No implementamos pero es una prioridad para los próximos 12 meses
Herramientas de prevención de intrusiones			
Herramientas de administración de parches			
Candados/ llaves/ seguridad física para hardware computacional.			
Ninguna de las anteriores			

Web/ Internet			
	Actualmente implementamos	Actualmente subcontratamos	No implementamos pero es una prioridad para los próximos 12 meses
Filtros de contenidos web			
Certificación/ acreditación de sitios Web			
Servidores seguros			
Seguridad de servicios web			
Ninguna de las anteriores			

Otro			
	Actualmente implementamos	Actualmente subcontratamos	No implementamos pero es una prioridad para los próximos 12 meses
Tecnologías de seguridad compatibles con intercambios de web 2.0. tales como redes de socialización, blogs, wikis u otros colaboradores			
Seguridad de dispositivos inalámbricos de mano			
Herramientas de administración de activos			
Software de control de acceso a la PC			
Software de control de acceso para redes			
Acceso remoto seguro			
Seguridad de VoIP (voz sobre IP)			
Herramientas de análisis de códigos			
Aplicación de administración de seguridad empresarial.			

Ninguna de las anteriores			

SECCIÓN IV: Incidentes relacionados con la seguridad durante el año pasado

Esta sección se enfoca en qué tipos de incidentes relacionados con la seguridad afectaron su organización durante los últimos 12 meses, así como en la naturaleza del impacto y en cómo respondió la organización.

Un incidente de seguridad se define como cualquier situación negativa en la que (ya sea de manera maliciosa o accidental) los datos corporativos, sistemas o redes se vieron comprometidos provocando un daño que requirió una respuesta de su equipo de seguridad de la información.

Número de incidentes de seguridad en los últimos doce meses:		No sé	

19. Rango de incidentes de seguridad en los últimos doce meses:

	0 o ninguno
	1 – 2
	3 – 9
	10 – 49
	50 – 499
	500 – 4,999
	5000 – 99,999
	100,000 o más
	No sé

20. ¿Qué tipos de incidentes de seguridad ocurrieron? (Marque todas las opciones aplicables):

	Explotación de datos
	Explotación de dispositivos
	Explotación de aplicaciones
	Explotación de sistemas
	Explotación de redes
	Explotación humana (ingeniería social)
	Desconocido
	Otro (por favor especifique)

21. Fuente probable del incidente (marque todas las opciones aplicables):

	Empleado
	Ex empleado
	Cliente
	Socio/ Proveedor
	Pirata informático
	Terrorista
	Proveedor de servicios/ consultor / contratista
	Gobierno extranjero
	Desconocido
	Otro (por favor especifique)

22. ¿Cuál fue el impacto del incidente de seguridad en su organización?

Negocio	
	Pérdidas financieras
	Robo de propiedad intelectual
	Marca/ reputación comprometida
	Página web de la compañía alterada/ deformada
	Pérdida de valores para los accionistas
	Extorsión
	Fraude
	Responsabilidad legal/ demanda

Datos	
	Registros confidenciales comprometidos
	Registros de clientes comprometidos o no disponibles
	Registros de empleados comprometidos
	Robo de identidad (información de cliente o empleados robados)
	Registros internos perdidos o dañados

Sistema	
	Programas de sistemas operativos alterados/ archivos alterados
	Almacenados de sistemas usados/ archivos no autorizados depositados
	Sistemas destruidos / dejados inservibles

Red	
	Correo electrónico y aplicaciones no disponibles
	Red más lenta / no disponible (es decir, pérdida de productividad)
	Correo no deseado y no autorizado enviado desde los servidores de la compañía

Aplicación

	Aplicaciones de software alteradas

Otro	
	Otro (por favor especifique)

23. La manera en que la organización se enteró de los eventos de seguridad (Marque todas las opciones aplicables):

	Alertados por un colega
	Alertados por un cliente / proveedor
	Alertados por un oficial del gobierno
	Alertados por un proveedor de servicios administrados
	Alertados por los medios
	Alertados por el perpetrador
	Análisis del servidor o archivos y registros del firewall
	Alertados por sistemas de detección/ prevención de intrusiones
	Alertados por software de monitoreo de correlación de eventos de seguridad

24. Tiempo total fuera de servicio en los últimos 12 meses como consecuencia de eventos de seguridad (servicios/ aplicaciones/ redes no disponibles):

	Ninguno
	Menos de 1 hora
	De 1 a 2 horas
	De 3 a 8 horas
	De 9 a 24 horas
	De 1 a 2 días
	De 3 a 5 días
	Más de 5 días
	No se aplica

SECCIÓN V: Planeación, políticas y procedimientos de seguridad

Esta sección explora algunos de los parámetros básicos que ayudan a definir cómo las organizaciones se enfocan en la arquitectura organizativa de la seguridad de la información.

25. ¿Su organización contrata activamente a encargados de la toma de decisiones tanto en el área de negocios como en la de tecnología de la información al tratar asuntos de seguridad de la información?

	Sólo a encargados de toma de decisiones en el área de negocios

	Solo a encargados de toma de decisiones en el área de TI
	Ambos
	Ninguno

26. Durante el año pasado, ¿su compañía ha medido y revisado la eficacia de sus políticas y procedimientos de seguridad de la información?

	Sí
	No

27. ¿cuáles de los siguientes elementos, si los hay, están incluidos en la política de seguridad de su organización? (Marque TODAS las opciones aplicables):

	Respaldo y recuperación/ Continuidad del negocio		Evaluación de riesgos de seguridad
	Administración de usuarios		Mecanismo de cumplimiento de normas
	Control de accesos		Procedimientos con los que socios/ proveedores deben estar en conformidad
	Seguridad de aplicaciones –segregación de tareas		Uso apropiado de la tecnología (Internet, correo electrónico, etc.)
	Registro y monitoreo		Uso de tecnologías Web 2.0
	Seguridad física		Acceso y publicación en sitios de redes de socialización.
	Administración de cambios		Estándares técnicos de configuración de seguridad
	Seguridad en desarrollo de sistemas		Capacitación de concientización de seguridad y comunicaciones del usuario final
	Clasificación del valor comercial de los datos		Administración de parches
	Inventario de activos de información / administración de activos de información		Reportes de recolección y administración de criterios de seguridad
	Protección, divulgación y destrucción de datos		Conformidad con requerimientos legales/ regulatorios
	Administración de seguridad de sistemas		Procedimientos destinados a proteger la propiedad intelectual
	Respuesta a incidentes		Monitoreo de contenidos
	Administración de seguridad de redes		No aplicable/ no existe política escrita

28. En su opinión, ¿qué tan bien las POLÍTICAS de seguridad de su compañía están alineadas con los objetivos empresariales de la compañía?

	Completamente alineadas
	Algo alineadas
	Deficientemente alineadas
	No alineadas

29. En su opinión, ¿qué tan bien los GASTOS en seguridad de su compañía están alineados co los objetivos empresariales de la compañía?

	Completamente alineados
	Algo alineados
	Deficientemente alineados
	No alineados

30. ¿Con qué frecuencia su compañía da prioridad a los activos de datos y de información según su nivel de riesgo?

	Continuamente
	Periódicamente
	No clasificamos los activos de datos y de información
	Otro (por favor especifique)

31. ¿Qué asuntos o factores de negocios están impulsando su gasto en seguridad de la información? (Marque TODAS las opciones aplicables):

	Depresión económica
	Cambio
	Planes de continuidad/ recuperación de desastres empresariales
	Subcontratación
	Tendencias de convergencia digital (VoIP, etc.)
	Reputación de la compañía
	Terrorismo
	Actividad de fusión/ adquisición
	Cumplimiento regulatorio
	Política interna de cumplimiento
	Otro (por favor especifique)

32. ¿Cómo se justifica el gasto en seguridad de la información en su empresa? (marque TODAS las opciones aplicables):

	Requisito del cliente
	Práctica común en la industria
	Criterio profesional
	Rendimiento económico sobre inversión
	Requisito legal / regulatorio
	Requisito de socio / vendedor
	Responsabilidad/ exposición potencial
	Impacto potencial en ingresos
	Calificación de reducción de riesgos
	No lo justifica
	Otro (por favor especifique)

33. ¿Cómo mide su empresa la eficiencia del gasto en seguridad de la información? (Marque TODAS las opciones aplicables):

	Criterio profesional
	Rendimiento de las inversiones
	Período de amortización
	Valor actual neto
	Costo total de titularidad
	Tasa de rentabilidad neta
	No sé
	Otro (por favor especifique)

34. ¿Qué tan seguro está usted de que las actividades relacionadas con la seguridad de la información de su organización son eficaces?

	Nada seguro
	Poco seguro
	Muy seguro
	No sé

35. ¿Qué tan seguro está usted de que las actividades relacionadas con la seguridad de la información de sus socios/ proveedores?

	Nada seguro
	Poco seguro
	Muy seguro
	No sé

36. ¿Actualmente usa un servidor, almacenamiento u otro medio de virtualización de recursos de tecnología de información?

	Sí
	No

37. ¿Cuál es la fuente de vulnerabilidad potencial en su ambiente virtualizado? (Marque todas las opciones que correspondan):

	Configuración errónea o implementación deficiente
	Falta de salvaguardas adicionales
	Enfoque obsoleto a cortafuegos, al manejo de de la identidad o al control de acceso
	Aplicación de política no definida en un ambiente virtualizado
	Falta de personal de tecnología de información bien capacitado

38. ¿Actualmente usa servicios en nube tales como software como servicio, una plataforma como servicio o una infraestructura como servicio?

	Sí
	No

39. ¿Cuál es el mayor riesgo a la seguridad para su estrategia de informática en nube?

	Habilidad incierta para hacer cumplir las políticas de seguridad en un sitio de proveedor
	Capacitación y auditoría de tecnología de información inadecuada
	Control de acceso privilegiado cuestionable en un sitio de proveedor
	Proximidad de su información con los de alguien más
	Habilidad incierta para recuperar datos
	Existencia continua incierta de un proveedor
	Cumplimiento normativo incierto de un proveedor
	Habilidad incierta para auditar a un proveedor

40. ¿Cuál es la capacidad general más crítica que se tiene en un ambiente de datos distribuidos?

	Conocimiento y control del punto final

	Cooperación y apoyo de las unidades comerciales, socios y proveedores
	Consistencia de la seguridad a nivel de sistema
	Evaluación del riesgo
	Ubicación de los datos
	Guardianes de datos
	Inventario de datos
	Capacidad para predecir y mitigar nuevas fuentes de riesgo

41. ¿Cuál es la estrategia de administración de la seguridad más crítica para tener en un ambiente colaborativo con muchos usuarios?

	Especialistas que pueden predecir y combatir nuevos tipos de ataques
	Detección anómala extensa
	Perfiles de antecedentes de aquellos con formas de acceso privilegiado
	Estrategia y política consistente entre las organizaciones
	Administración de la identidad federado y sistemático
	Servidores de acceso privado y limitado

42. ¿Cuántas horas al año invierte personalmente con los auditores?

	4 – 50 horas	51 – 100 horas	101 a 200 horas	201 horas o más
Auditores externos (Auditores de estados financieros)				
Auditores internos				
Auditores regulatorios				
Auditores de clientes o proveedores				
Otra (especifique quien y cuanto tiempo se invierte en ellos):				

43. ¿Cuáles considera que son las métricas de seguridad más efectivas?:

LISTAS DE CHEQUEO

DISEÑO DE INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN (ENTREVISTAS, CUESTIONARIOS, LISTAS DE CHEQUEO) USADOS PARA OBTENER LA INFORMACIÓN ACERCA DE LA SEGURIDAD INFORMÁTICA EN LA EMPRESA.

LISTA DE CHEQUEO 1

Empresa TRANSPORTES TIERRA GRATA Y COMPAÑÍA LTDA			
Dominio	PSI		
Proceso	Orientación de la dirección para la seguridad de la información		
Objetivo de Control	Brindar Orientación y soporte, por parte d la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes		
Cuestionario			
Pregunta	SI	NO	N/A
¿Cuenta la empresa con política de seguridad de la información?		X	
¿Se da a conocer la política de seguridad de la Información a los empleados?		X	
¿Se revisa las políticas para la seguridad de la información?		X	

LISTA DE CHEQUEO 2

Empresa TRANSPORTES TIERRA GRATA Y COMPAÑÍA LTDA			
Dominio	ORGANIZACIÓN Y SEGURIDAD DE LA INFORMACIÓN		
Proceso	Organización Interna		
Objetivo de Control	Establecer el marco de referencia de gestión para iniciar y controlar con la implementación y la operación de la seguridad de la información dentro de la organización.		
Cuestionario			
Pregunta	SI	NO	N/A
¿Se definen las responsabilidades de la seguridad de información?		X	
¿Hay separación de deberes dentro de la empresa?	X		
¿Se mantiene contacto con las autoridades pertinentes?			X
¿Tiene contacto con grupos de interés especial?		X	
¿Realiza gestión de proyectos para tratar la seguridad de la información?		X	

LISTA DE CHEQUEO 3

Empresa TRANSPORTES TIERRA GRATA Y COMPAÑÍA LTDA			
Dominio	SEGURIDAD EN LOS RECURSOS HUMANOS		
Proceso	Durante la ejecución del empleo		
Objetivo de Control	Asegurarse que los empleados y contratistas tomen conciencia de sus responsabilidades en SI y las cumplan		
Cuestionario			
Pregunta	SI	NO	N/A
¿Existe responsabilidad de la dirección para exigir a los empleados a la aplicación de la SI?	X		

¿Se realizan capacitaciones en toma de conciencia a los empleados, contratistas y la dirección?		X	
¿Se realiza proceso disciplinario a los empleados que violen la Seguridad de la Información?		X	

LISTA DE CHEQUEO 4

Empresa TRANSPORTES TIERRA GRATA Y COMPAÑÍA LTDA				
Dominio	Gestión de activos			
Proceso	Responsabilidad por los activos Clasificación de la Información. Manejo de Medios			
Objetivos de Control	Establecer el marco de referencia de gestión para iniciar y controlar con la implementación y la operación de la seguridad de la información dentro de la organización. Asegurar que la información recibe un nivel apropiado de protección de acuerdo con su importancia para la organización. Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.			
Cuestionario				
Pregunta		SI	NO	N/A
¿Existe un inventario donde se identifique los activos de la empresa?		X		
¿Se tiene destinado a quien pertenece cada activo?		X		
¿Los empleados devuelven los activos una vez terminado el contrato con la empresa?		X		
¿Se clasifica la información teniendo en cuenta las responsabilidades?			X	
¿Se etiqueta la información de acuerdo al esquema de clasificación?			X	
¿Hay procedimientos para el manejo de activos?		X		
¿Existen procedimientos para la gestión de medios removibles?			X	
¿Hay procedimientos formales para disponer los medios cuando ya no se requieran?			X	
¿Se protegen los medios físicos que contiene información?		X		

LISTA DE CHEQUEO 5

Empresa TRANSPORTES TIERRA GRATA Y COMPAÑÍA LTDA				
Dominio	CONTROL DE ACCESO			
Proceso	Requisitos del Negocio para el control de acceso. Gestión de Acceso a Usuarios Responsabilidad de los usuarios Control de Acceso a Sistemas y Aplicaciones			
Objetivos de Control	Limitar el acceso a la información y a instalaciones de procesamiento de información. Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios. Hacer que los usuarios rindan cuentas por la salvaguarda de la información de autenticación. Evitar el acceso no autorizado a sistemas y aplicaciones.			
Cuestionario				
Pregunta		SI	NO	N/A
¿Existe una política de control de acceso con base en los requisitos del negocio y la seguridad de la información?			X	
¿La empresa ha establecido roles para el acceso a redes y a servicios de red?			X	

¿Tienen proceso de registro y cancelación de usuarios?	X		
¿Se tiene procesos de suministro de acceso a usuarios)?	X		
¿Hay restricción de acceso a información?		X	
¿Cumplen con el uso de información autenticada secreta?	X		
¿Existen controles para el acceso al código fuente de programas?		X	
¿Existe una política de control de accesos?		X	
¿Existe un procedimiento formal de registro y baja de accesos?		X	
¿Se controla y restringe la asignación y uso de privilegios?		X	
¿Existe una gestión de las contraseñas de usuarios?		X	
¿Existe una revisión de los derechos de acceso de los usuarios?		X	

LISTA DE CHEQUEO 6

Empresa TRANSPORTES TIERRA GRATA Y COMPAÑÍA LTDA			
Dominio	CRIPTOGRAFÍA		
Proceso	Controles Criptográficos		
Objetivos de Control	Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.		
Cuestionario			
Pregunta	SI	NO	N/A
¿Existe una política de uso de controles criptográficos?		X	
¿La empresa cuenta con política sobre uso de llaves criptográficas?		X	
¿Existe métodos para tratar la protección de claves criptográficas y la recuperación de información?		X	

LISTA DE CHEQUEO 8

Empresa TRANSPORTES TIERRA GRATA Y COMPAÑÍA LTDA			
Dominio	SEGURIDAD FÍSICA Y DEL ENTORNO		
Proceso	- Áreas Seguras. - Equipos.		
Objetivos de Control	Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización. Prevenir la perdida, daño, robo o compromiso de activos y la interrupción de las operaciones de la organización		
Cuestionario			
Pregunta	SI	NO	N/A
¿Cuenta la empresa con lugares de acceso restringido?	X		
¿Hay control de Seguridad de acceso a lugares restringidos?	X		
¿Se ha encontrado alguna falla en el control?		X	
¿Tiene plan ante la falla del sistema de seguridad?		X	
¿Se registran las personas que ingresan a las instalaciones de la empresa?		X	

¿Se encuentra definido el perímetro de Seguridad Física?		X	
¿Existe Política de control de Acceso a las Instalaciones?		X	
¿Hay mecanismos de protección frente a amenazas externas?		X	
¿Se trabaja en áreas seguras?	X		
¿Existen control para el acceso al área despacho y cargue?	X		
¿Existe protección del cableado de energía eléctrica y de telecomunicaciones?		X	
¿Hay política de equipos desatendidos?		X	
¿Cuentan con política de escritorio limpio?		X	
¿Se controla el retiro de activos en la empresa?	X		

LISTA DE CHEQUEO 9

Empresa TRANSPORTES TIERRA GRATA Y COMPAÑÍA LTDA				
Dominio	SEGURIDAD DE LAS OPERACIONES			
Proceso	Procedimientos Operacionales. Protección Contra Códigos maliciosos. Registro y Seguimiento. Control de Software Operacional. Gestión de la Vulnerabilidad Técnica			
Objetivos de Control	Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información. Asegurarse de que la información y las instalaciones de procesamiento de la información estén protegidas contra códigos maliciosos. Registrar eventos y generar evidencia. Asegurarse de la integridad de los sistemas operacionales. Prevenir el aprovechamiento de las vulnerabilidades técnicas.			
Cuestionario				
Pregunta		SI	NO	N/A
¿Tiene plan para protección de registros?			X	
¿Se establece condiciones y términos de servicios?		X		
¿Hace control para evitar la propagación de código Malicioso?		X		
¿Utiliza medida de protección de los registros?			X	
¿Existe Manual de procedimientos documental?			X	
¿Existe manual de políticas de respaldo de la información?			X	
¿Evalúa periódicamente los SI en busca de vulnerabilidades?			X	
¿Existe manual de procedimientos y restricción para controlar la instalación de software?			X	
¿Existen medidas de protección para contrarrestar las vulnerabilidades?			X	
¿Existe plan de auditoria donde se implementa control, establecimiento de requisitos y actividades de auditoria?			X	

LISTA DE CHEQUEO 10

Empresa TRANSPORTES TIERRA GRATA Y COMPAÑÍA LTDA	
Dominio	SEGURIDAD DE LAS COMUNICACIONES
Proceso	Gestión de la Seguridad de Redes Transferencia de Información.

Objetivos de Control	Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte. Mantener la Seguridad de la información Transferida dentro de una organización.		
Cuestionario			
Pregunta	SI	NO	N/A
¿Existen controles sobre las redes y en la seguridad de los servicios de red?	X		
¿Se establecen las responsabilidades y los procedimientos para la gestión de equipos remotos, incluyendo los equipos en áreas de usuarios?		X	
¿Establecer el registro y monitoreo adecuados para permitir el registro de acciones de seguridad pertinentes?		X	
¿Existen políticas, procedimientos y controles para la transferencia de la información?		X	
¿Existen acuerdos de confidencialidad o de no divulgación para la transferencia de la información?		X	
¿Existen controles que garanticen la seguridad incluida en la mensajería electrónica?	X		

LISTA DE CHEQUEO 11

Empresa TRANSPORTES TIERRA GRATA Y COMPAÑÍA LTDA			
Dominio	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SI		
Proceso	Requisitos de seguridad de los SI. Seguridad en los procesos de desarrollo y de soporte. Datos de Prueba		
Objetivos de Control	Asegurar que la seguridad de la información sea una parte integral de los SI durante todo el ciclo. Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los SI		
Cuestionario			
Pregunta	SI	NO	N/A
¿Existen controles de seguridad en las redes públicas?	X		
¿Existen políticas para realizar análisis y especificaciones de requisitos de seguridad de la información?		X	
¿Existe ambiente de desarrollo seguro?		X	
¿Existen controles de restricción sobre cambios a paquetes de software?		X	
¿Existe política para desarrollo de software seguro?		X	
¿Hay política para realización de pruebas que incluye aceptación y de seguridad de sistemas?		X	

LISTA DE CHEQUEO 12

Empresa TRANSPORTES TIERRA GRATA Y COMPAÑÍA LTDA.			
Dominio	RELACIÓN CON LOS PROVEEDORES		
Proceso	Seguridad de información en las relaciones con los proveedores. Gestión de la prestación de servicios de proveedores.		
Objetivos de Control	Asegurar la protección de los activos de la organización que sean accesibles a los proveedores. Mantener nivel acordado de seguridad de la información y de prestación de servicios en línea con los acuerdos con los proveedores.		
Cuestionario			
Pregunta	SI	NO	N/A
¿Existe una política de seguridad de la información para proveedores?		X	

¿Procedimientos para hacer seguimiento y revisión de los servicios de los proveedores?	X		
¿Están claramente definidos los requisitos legales y de reglamentación, incluida la protección de datos, los derechos de propiedad intelectual y derechos de autor, y una descripción de cómo se asegurará que se cumplan?		X	
¿Existen acuerdos con proveedores que incluyen requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación?		X	

LISTA DE CHEQUEO 12

Empresa TRANSPORTES TIERRA GRATA Y COMPAÑÍA LTDA			
Dominio	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN		
Proceso	Gestión de incidentes y mejoras en la seguridad de la información		
Objetivos de Control	Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información incluida la comunicación sobre eventos de seguridad y debilidades.		
Cuestionario			
Pregunta	SI	NO	N/A
¿Establecen responsabilidades y procedimientos de gestión para dar respuesta a los incidentes y debilidad de la seguridad de la información?		X	
¿Existen canales apropiados para dar reportes de eventos de seguridad de información?		X	
¿Realizan evaluación de eventos de seguridad de la información?		X	
¿Existen procedimientos para recolección, identificación que puedan servir como evidencia?		X	

LISTA DE CHEQUEO 13

Empresa TRANSPORTES TIERRA GRATA Y COMPAÑÍA LTDA			
Dominio	ASPECTO DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO		
Proceso	Continuidad de seguridad de la información. Redundancias.		
Objetivos de Control	La continuidad de la seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización. Asegurar la disponibilidad de instalaciones de procesamiento de información.		
Cuestionario			
Pregunta	SI	NO	N/A
¿Existe plan de continuidad del negocio en la empresa?		X	
¿Existen procedimientos para la implementación de la continuidad de la seguridad de la información?		X	
¿Verifica los controles de continuidad de seguridad de la información?		X	
¿Existe un mecanismo de planificación para la continuidad del negocio?		X	

LISTA DE CHEQUEO 14

Empresa TRANSPORTES TIERRA GRATA Y COMPAÑÍA LTDA			
Dominio	CUMPLIMIENTO		
Proceso	Cumplimiento de requisitos legales y contractuales. Revisiones de Seguridad de Información.		
Objetivos de Control	Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de información y de cualquier requisito de seguridad. Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales		
Cuestionario			
Pregunta	SI	NO	N/A
¿Se tiene identificada la legislación aplicable y de los requisitos contractuales?	X		
¿Están definidos los procedimientos para establecer requisitos legales y de reglamentación, incluida la protección de datos, los derechos de propiedad intelectual y derechos de autor?		X	
¿Existe política de seguridad para asegurar la privacidad y la protección de la información como lo exige la legislación?		X	
¿Se usan los controles criptográficos?		X	
¿Se revisa periódicamente la seguridad de la información?		X	
¿Cumple con las políticas y normas de seguridad?		X	
¿Se revisa periódicamente los SI para determinar el cumplimiento con las políticas y normas de seguridad de información?		X	

ANEXO E. EVALUACIÓN DE PROCESOS VITALES EN LA ENTIDAD QUE SE SOPORTAN EN SERVICIOS DE TI

Macroproceso: Colocación	
Proceso: Seguimiento y desembolso de contratos	
Cargo: Jefe de Sistemas	
CRITERIOS DE EVALUACIÓN	RESPUESTAS
1. La interrupción de los servicios de sistemas que soportan este proceso tiene el siguiente impacto para la empresa:	
a) Catastrófico para mas de tres dependencias o áreas de la entidad	
b) Catastrófico para tres o menos dependencias o áreas de la entidad	
c) Moderado para mas de tres dependencias o áreas de la entidad	
d) Moderado para tres o menos dependencias o áreas de la entidad	
e) Menor para la empresa en general	
2. Cuanto tiempo puede permanecer la entidad operando sin el soporte usual de los servicios de sistemas que soportan al proceso (asumiendo que la interrupción de estos servicios se da en el pico más alto de carga de trabajo).	
a) Únicamente 24 horas	
b) Hasta tres días	
c) Hasta una semana	
d) Hasta un mes	
e) Más de un mes	
3. En caso de la interrupción de los servicios de sistemas que soportan este proceso, que riesgos se podrían materializar en la entidad (puede marcar varias opciones):	
a) Daño o destrucción de activos	
b) Hurto o Fraude	
c) Desventaja Competitiva	
d) Sanciones legales	
e) Pérdida de credibilidad pública	
f) Costos excesivos	
g) Toma errada de decisiones	
h) Pérdida de ingresos o rentas	
4. Se tienen implementados procedimientos alternos manuales que puedan ser utilizados en caso de la interrupción de los servicios de sistemas que soportan el proceso:	
a) No	
b) Si, pero no han sido probados	
c) Si y fueron probados hace varios años	
d) Si y fueron probados hace menos de un año	
e) Si y fueron probados durante los últimos 6 meses	
5. La interrupción de los servicios de sistemas que soportan el proceso puede propiciar la aparición de multas, sanciones, recargos, etc. a partir:	
a) Del primer día	
b) Del tercer día	
c) De la primera semana	
d) De la tercer semana	
e) Del primer mes	
6. La interrupción de los servicios de sistemas que soportan el proceso puede propiciar una disminución en los ingresos normales de la entidad a partir:	
a) Del primer día	

b) Del tercer día	
c) De la primera semana	
d) De la tercer semana	
e) Del primer mes	
7. La interrupción de los servicios de sistemas que soportan el proceso afectaría de manera directa a (puede marcar varias opciones):	
a) Clientes internos	
b) Clientes externos	
c) Proveedores externos	
d) Altos directivos, socios, inversionistas, etc. de la entidad	
e) La comunidad en general	
f) Otras organizaciones	
8. Dependencias que se verían afectadas por la interrupción de los servicios de sistemas que soportan al proceso:	
a) Más del 80% de las dependencias de la entidad	
b) Entre el 80% y el 60% de las dependencias de la entidad	
c) Entre el 60% y el 40%de las dependencias de la entidad	
d) Entre el 40% y el 20% de las dependencias de la entidad	
e) Menos del 20% de las dependencias de la entidad	
9. Grado de dependencia que el proceso tiene con la tecnología:	
a) El proceso está automatizado y depende enormemente de la tecnología	
b) El proceso está automatizado y depende moderadamente de la tecnología	
c) El proceso está automatizado pero depende muy poco de la tecnología	
d) El proceso se realiza principalmente en forma manual	
10. Equipos, instrumentos y dispositivos especiales utilizados en el proceso:	
a) Se utiliza una gran cantidad de equipos y dispositivos especiales para realizar las actividades del proceso	
b) Se utilizan algunos equipos y dispositivos especiales para realizar las actividades del proceso	
c) Se utilizan pocos equipos y dispositivos especiales para realizar las actividades del proceso	

Tabla de puntajes

Pregunta	Respuesta dada	Valor
1	a	5
	b	4
	c	3
	d	2
	e	1
2	a	5
	b	4
	c	3
	d	2
	e	1
3	a	2
	b	2
	c	2
	d	2
	e	2

	f	2
	g	2
	h	2
4	a	5
	b	4
	c	3
	d	2
	e	1
5	a	5
	b	4
	c	3
	d	2
	e	1
6	a	5
	b	4
	c	3
	d	2
	e	1
7	a	2
	b	2
	c	2
	d	2
	e	2
	f	2
8	a	5
	b	4
	c	3
	d	2
	e	1
9	a	5
	b	4
	c	3
	d	2
10	a	5
	b	4
	c	3

Resultados por puntaje

Proceso Crítico	54 - 68
Proceso Importante	40 - 53
Proceso criticidad media	27 - 39
Proceso criticidad baja	14 - 26
Proceso criticidad muy baja	0 - 13

Anexo F. CAPTURA DE REQUISITOS

En la captura de requisitos se recoge la mayor cantidad de información posible sobre la empresa. Equipos hardware actualmente instalados, distribución física del empresa, instalación actual y configuración de los sistemas operativos y software en los distintos sistemas que componen la red. También es necesario capturar los roles de la empresa, grupos de trabajo y usuarios de estos sistemas.

Las vías de captura de requisitos del cliente son: formulario Web y entrevista presencial. Además, se detalla la información útil recogida para el desarrollo del proyecto.

Se indaga acerca de la disponibilidad, desempeño, confidencialidad, integridad y control de acceso físico y lógico, considerando componentes de la red como: Switches, Routers, Firewall, IPS/IDS, Gateway Antivirus de la empresa, desempeño de la Red, topología existente, con respecto a ello se pregunta acerca de conexiones, componentes software y hardware utilizados, planos existentes y diseño.

Nivel de usuario

- Número de usuarios de equipos TI (trabajadores): 14 usuarios de equipos informáticos actualmente.
- Roles en la empresa según necesidades TI (software y/o permisos específicos): Dirección, administración y trabajadores de la empresa.

Nivel de infraestructura

- Número de equipos de trabajo (máquinas cliente): Para personal de la empresa: 14.

En una entrevista realizada de forma personal, se completa la información necesaria hasta la fecha, que en principio será suficiente para terminar el proyecto. Al cliente se le informa de que es posible que se le hagan más consultas en otro momento. La información recogida en la entrevista es la siguiente:

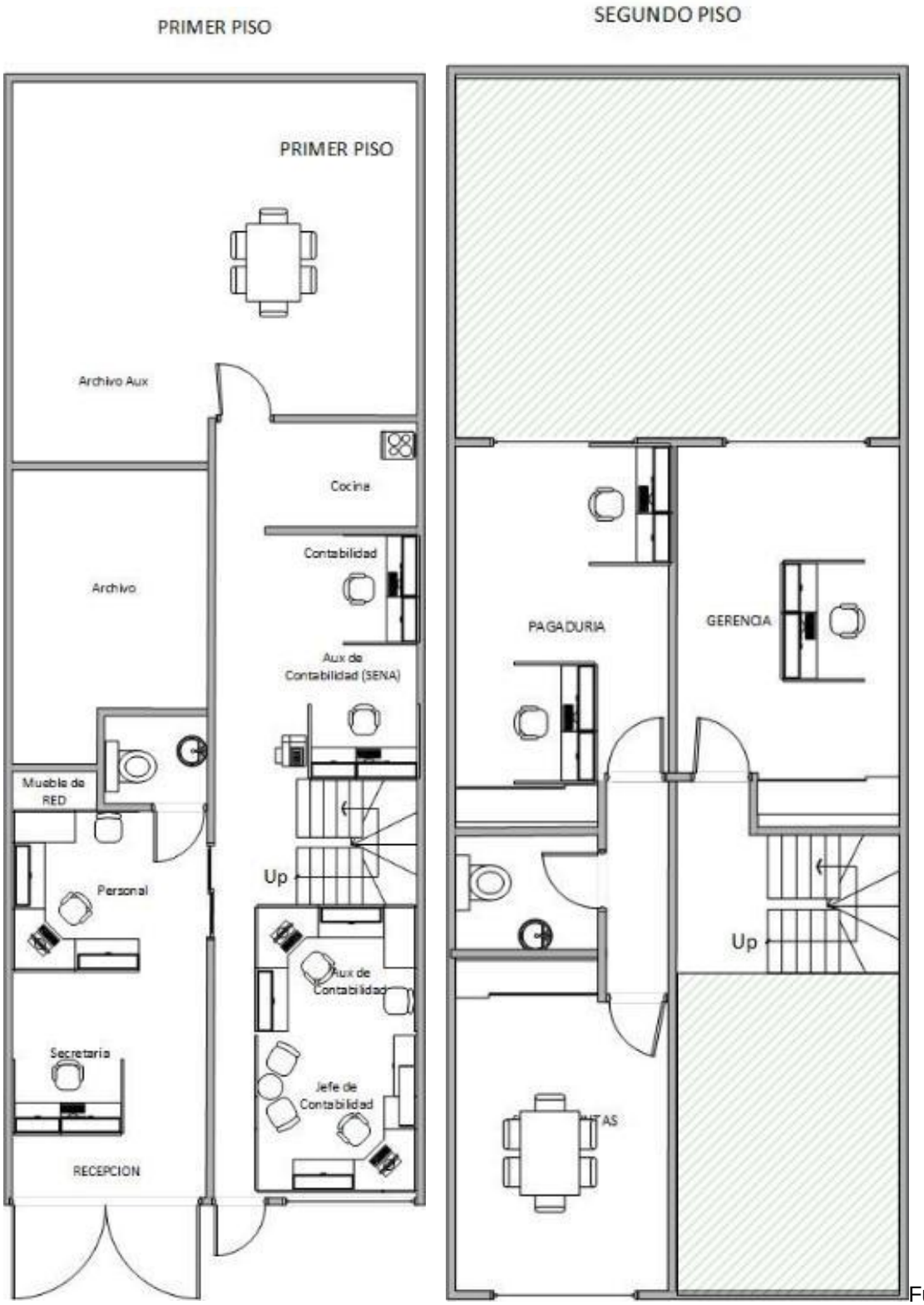
Nivel de servicios

- Copias de seguridad de datos: La información sensible se encuentra registrada y cumple con la Ley de Protección de Datos Personales [6] [7] (Ley Estatutaria de Protección de Datos (LEPD)). Es un fichero con información personal sobre los trabajadores que es consultado por todo el personal contratado.
- Conexión a la red sin cables (WiFi): Necesaria para conectividad de tabletas y teléfonos móviles corporativos.

Distribución física de la empresa:

- Número de equipos administrativos: 11, 10 en la sede principal y uno en el Terminal de Transportes de Fusagasugá
- Número de equipos operativos: 3, 1 en el Terminal de Transportes de Fusagasugá, 1 en la taquilla ubicada en el Terminal de Transportes de Bogotá y 1 en la taquilla ubicada en el Terminal satélite del Sur de Bogotá
- Número de plantas para empleados administrativos: 2. Se trata de una casa de dos plantas, con la siguiente distribución:

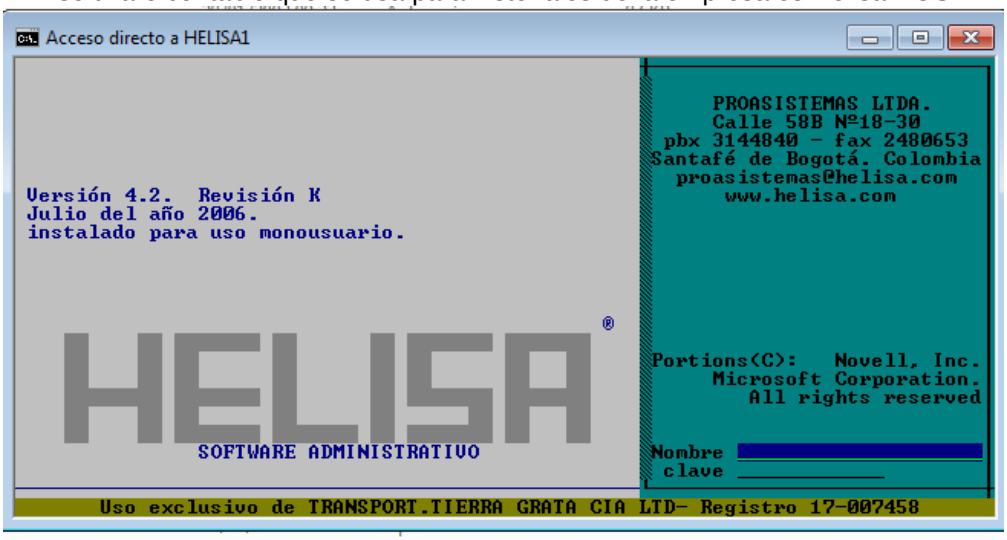
Figura 1: Planos Sede Principal.



Fuente. El Autor

Software: son dos los softwares que se usan al interior de la empresa: Helisa DOS y SIIGO, el primero que trae los historiales del 2016 hacia atrás y SIIGO que es el software contable que está en implementación.

Figura 2: El software contable que se usa para historiales de la empresa es Helisa DOS



Fuente. Empresa de Transportes Tierra Grata y Cia Ltda

Figura 3: Interfaz de SIIGO.

Fuente. Empresa de Transportes Tierra Grata y Cia Ltda

La seguridad en redes es muy baja por el firewall que se implementa en el sistema operativo, se debe aplicar una metodología basada en protocolos que permita salvaguardar los datos y la información que a diario se suministra.

Switch: Este equipo de comunicación de redes está ubicado en la oficina principal de Fusagasugá es un TP-LINK TL-SF1024D 24 Puertos 10/100 Mbps que es de baja velocidad, lo cual no garantiza en cierto grado la disponibilidad y el buen desempeño. El Switch no está configurado de acuerdo a la segmentación del diseño de red ni configurados en VLANs, lo cual maximiza los riesgos de acceso no autorizado entre subredes y no elimina tráfico innecesario. El control de acceso físico es deficiente, ya que el Switch aunque se encuentran en armario, la seguridad que brinda el armario de cableado no es la adecuada.

Figura 4: Fotografía de Switch y PatchPanel.

Fuente. El Autor

Router: La configuración, mantenimiento y disponibilidad del router ARRIS TG862 [8] depende del proveedor COMCEL, ya que se tiene en comodato de acuerdo al contrato adquirido actualmente por ellos.

Figura 5: Fotografía de Router.

Fuente. El Autor

Firewalls: No se tienen actualmente Firewalls o UTM (Equipos Unificados contra Amenazas).
Nota: Si se tuviesen estos equipos serían muy confiables por la seguridad parametrizable que tienen ya que son muy completos por la cantidad de módulos de seguridad que incorporan como antispam, Firewall con políticas fácilmente configurables, antivirus Web, Filtrado Web, monitor del estado de memoria y CPU del equipo, así como monitor de trafico In/Out por interfaz o zona y un Sistema IPS pre configurado bastante eficiente además de un administrador de ancho de banda por interfaz entre otras funcionalidades.

Antivirus: La institución actualmente no paga un licenciamiento anual por el sistema de protección antivirus, ni tampoco un servidor de políticas y de actualizaciones para clientes ni el derecho a usar la consola de administración de algún antivirus.

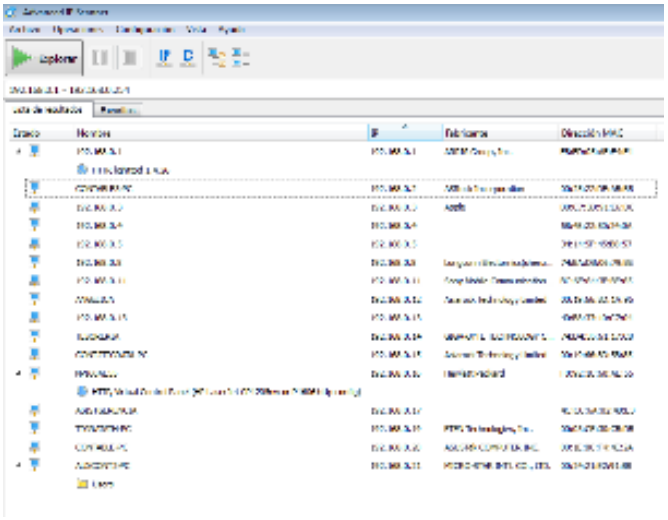
Desempeño de la Red: La disponibilidad y despeño de la red está sujeta a la misma confiabilidad de los equipos de red en sí. No se tiene como medida de prevención el stock de Switches. Como se observa se tiene instalado Switch 10/100 lo que no da un buen rendimiento en esos equipos. Se puede crear un cuello de botella en ocasiones en la sede principal en periodos de generación de nómina y pagos donde se accede al sistemas contable SIIGO y se realizan consultas y procesos con alto consumo de ancho de banda y las capacidades de la red no es la suficiente para atender estas solicitudes simultaneas además del tráfico normal existente (Internet, Servicios Internos de red, Video-Vigilancia IP, Telefonía IP entre otros).

Topología de Red: Nuestra topología de red se puede definir entre una mezcla de topología en árbol y topología en estrella. En árbol teniendo en cuenta que desde la sede principal se derivan todos los servicios y conexiones hacia las otras subsedes además de la conexión hacia las tres sedes alternas a través del canal de interconexión por fibra.

Planos, Conexiones y Diseño: La sede no tiene planos de red, no existen planos eléctricos ni de voz y datos. Estamos en proceso de actualización de la diagramación lógica y diseño de las redes. Se tiene la distribución lógica y diseño del direccionamiento de red en la LAN de la sede. En cuanto a conexiones y cableado se cuenta casi con el 90% de la red de datos con cable Cat 5 y la interconexión con las sedes alterna se hace por fibra óptica con velocidades de máximo 10Mbps.

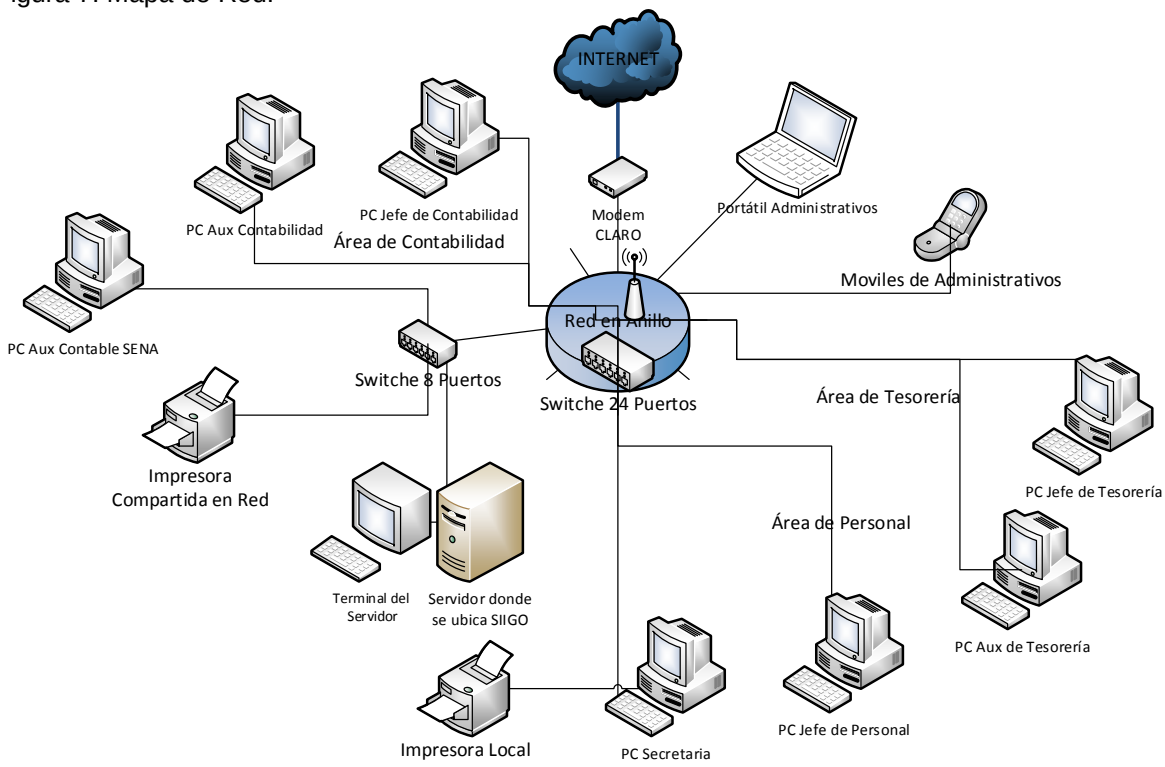
Este es el esquema de red de la sede principal tomado con el software Advance IP Scaner Version 24

Figura 6: esquema de red de la sede principal.



Fuente. El Autor

Figura 7: Mapa de Red.



Fuente. El Autor

Asignación de IP: La asignación de IP’s está definida de acuerdo a la siguiente tabla:

Tabla 1: Asignación de IP's. Informe generado en IPScan

Estado	Nombre	IP	Fabricante
Activado	192.168.0.1	192.168.0.1	ARRIS Group, Inc.
Activado	CONTABLE-PC	192.168.0.3	ASUSTek COMPUTER INC.
Activado	TTGRATATH-PC	192.168.0.4	ETEN Technologies, Inc.
Inactivo	192.168.0.5	192.168.0.5	Apple, Inc.
Inactivo	TESORERIA	192.168.0.6	GIGA-BYTE TECHNOLOGY CO.,LTD.
Activado	192.168.0.7	192.168.0.7	
Activado	192.168.0.8	192.168.0.8	Sony Mobile Communications AB
Activado	ANGELICA	192.168.0.9	Asiarock Technology Limited
Activado	192.168.0.10	192.168.0.10	BlackBerry RTS
Activado	DraMathaL	192.168.0.11	Asiarock Technology Limited
Activado	192.168.0.13	192.168.0.13	
Activado	ACTTGRATA-PC	192.168.0.15	Asiarock Technology Limited
Inactivo	192.168.0.16	192.168.0.16	
Activado	192.168.0.19	192.168.0.19	
Activado	NPI60AE55	192.168.0.20	Hewlett Packard
Inactivo	DESKTOP-T3FBQO5	192.168.0.21	Elitegroup Computer Systems Co.,Ltd.
Activado	192.168.0.100	192.168.0.100	

Fuente. El Autor

Servidor: No hay Servidor como tal, se usa un equipo normal donde se tiene instalado el sistema contable SIIGO y los demás se conectan por red, esto hace que el equipo se cuelgue y que haya constantes caídas que no permiten el trabajo normal desde las terminales clientes.

Tabla 2: Equipo

Tipo de equipo	Equipo basado en ACPI x86
Sistema operativo	Microsoft Windows 7 Professional
Service Pack del SO	-
Internet Explorer	8.0.7600.16385 (IE 8.0 - Windows 7)
DirectX	DirectX 11.0
Nombre del equipo	CONTABLE-PC
Nombre de usuario	CONTABLE

Dominio de inicio de sesión	CONTABLE -PC

Fuente: El Autor

Tabla 3: Placa base

Tipo de CPU	QuadCore Intel Core i5-4460, 3400 MHz (34 x 100)
Nombre de la placa base	MSI H81M-E33 (MS-7817) (1 PCI-E x1, 1 PCI-E x16, 2 DDR3 DIMM, Audio, Video, Gigabit LAN)
Chipset de la placa base	Intel Lynx Point H81, Intel Haswell
Memoria del sistema	3968 MB (DDR3-1600 DDR3 SDRAM)
DIMM3: SuperTalent SUPERTALENT02	4 GB DDR3-1600 DDR3 SDRAM (11-11-11-28 @ 800 MHz) (10-10-10-27 @ 761 MHz) (9-9-9-24 @ 685 MHz) (8-8-8-22 @ 609 MHz) (7-7-7-19 @ 533 MHz) (6-6-6-16 @ 457 MHz)
Tipo de BIOS	AMI (07/22/2014)
Puerto de comunicación	Puerto de comunicaciones (COM1)

Fuente: El Autor

Enumeración de requisitos

A partir de la información capturada de la empresa podemos definir los siguientes requisitos para la infraestructura.

Instalación y configuración de Windows Server 2012 R2: actualmente es una referencia en el mundo de los sistemas operativos de servidor. Instalando un servidor de este tipo se da la alternativa de Microsoft para servidores:

- Creación de dominio Windows.
- Repositorio y directorio activo: usuarios y grupos.

Instalación y configuración de cliente Windows 8/10 para personal de la empresa (14 equipos): el último sistema operativo de Microsoft para clientes, con entorno corporativo

- Inicio de sesión en el dominio.
- Copias de seguridad funcionales: la copia de respaldo se hace necesaria ya que entre los documentos que maneja la empresa hay ficheros en formato digital con datos de carácter personal. Es indispensable crear un contexto de copia donde el personal de la empresa pueda guardar ficheros teniendo garantías de respaldo de los mismos.

Presupuesto: sin un límite presupuestario, el objetivo es garantizar la funcionalidad y unos mínimos de escalabilidad para el futuro, ajustarlo a las necesidades del caso estudiado. Cada uno de los conceptos del presupuesto son argumentados individualmente y justificada la inversión que suponen.

Pruebas del sistema.

- Conectividad de la red local.
  a) Servidor Cliente.
  b) Cliente Servidor.
  c) Acceso remoto al servidor.
- Recursos compartidos (directorio centralizado)
- Restauración de datos.

Anexo G: Cargos y Funciones del Área Informática.

Área encargada de dotar a la Empresa de efectivos SI y comunicaciones, acordes con la tecnología de punta, que permitan simplificar los procesos administrativos, propendiendo al ahorro de tiempo, esfuerzos y reducción de costos; así como administrar las redes informáticas, telefónicas y otras.

Área de Proyectos y Desarrollo de Sistemas Informáticos

- Planificar, organizar, dirigir y controlar el desarrollo de los procesos de análisis y diseño de los SI de la empresa.
- Coordinar con las diversas áreas de la empresa las necesidades de formulación y/o modificación del software acorde con los cambios de procesos o tecnologías.
- Dirigir y supervisar la aplicación de los procesos de prueba e implementación de los SI, así como de la optimización de los mismos, aplicando metodologías y técnicas modernas.
- Determinar, previo estudio, las necesidades de software y hardware para los SI.
- Dirigir y evaluar la formulación de estudios de factibilidad para la implementación de nuevas técnicas de procesamiento de información y/o adquisición de equipos de cómputo.
- Desarrollar estrategias de seguridad e integridad de las bases de datos.
- Realizar el control de calidad de los programas aplicativos que se implementen y de las modificaciones que se realicen
- Coordinar con el Área de Organización y Métodos la formulación de procedimientos que optimicen las actividades que involucren a los SI.
- Diseñar, desarrollar e implementar las aplicaciones informáticas que permitan integrar y dinamizar la gestión de la empresa.
- Verificar el estado operativo de los SI, efectuando periódicamente las evaluaciones correspondientes y determinando los estándares de fallas.
- Administrar la base de datos de los sistemas.

Área de Infraestructura Técnica y Comunicaciones

- Programar, dirigir y evaluar el mantenimiento preventivo y correctivo de los equipos de cómputo.

- Supervisar la aplicación de medidas de seguridad de los sistemas, para garantizar la continuidad de las operaciones de procesamiento de datos.

- Formular, actualizar y comprobar, mediante técnicas de simulación, los planes de contingencia que garanticen la continuidad de las operaciones de procesamiento de datos, así como efectuar periódicamente los respaldos de la información en los servidores.

- Supervisar y evaluar la instalación oportuna del software, hardware y antivirus, verificando que cumplan con los estándares respectivos.

- Diseñar la red informática de la Empresa y proponer su aprobación e implementación

- Evaluar las características técnicas de los equipos de cómputo, redes de comunicación y otros.

- Supervisar y evaluar el mantenimiento preventivo, correctivo, cableado y repotenciación de equipos realizado por terceros.

- Proponer y evaluar la adquisición del software que requiere la Empresa y custodiar los programas originales.

- Supervisar que el software instalado en los diversos equipos de cómputo, cuenten con la debida licencia de autorización, así como mantener en custodia todas las licencias de uso originales de la Empresa.

- Llevar un registro actualizado del contenido, existencia y situación de los manuales y documentación de sistemas.

- Realizar estudios de factibilidad para la implementación de nuevas técnicas de procesamiento de información y/o adquisición de equipos de cómputo.

- Planificar y organizar la distribución física de los equipos informáticos, llevando un control de los mismos.

- Impartir instrucción para el manejo de los terminales del computador, así como de programas y redes propias del proceso automatizado de datos.

- Organizar, dirigir, supervisar y evaluar la instalación de equipos telefónicos (fijos y fax), así como la asignación de telefonía móvil (celulares), llevando un control y registro de los mismos.

Descripción de las Principales Funciones por Cargo

Se han considerado los cargos que son responsables de cada una de las áreas.

- Gerente De Departamento: Encargado de administrar y representar a DTSI, proponer proyectos y liderar los procesos de implementación y mejoramiento continuo.
- Sub Gerente De Servicios Informáticos: Responsable de todos los procesos del área de sistemas, desde la planificación hasta le entrega y puesta en marcha de los sistemas informáticos.
- Sub Gerente De Infraestructura Técnica Y Comunicaciones: Responsable de todos los procesos de las áreas técnicas, redes y seguridad de TI.
- Jefe De Infraestructura Y Redes: Responsable de la instalación y administración de los servidores físicos y virtuales y servicios de red, equipos de red como switches, routers, access points, puntos de acceso, cortafuegos, entre otros. Además, se responsabiliza de la conexión continua e ininterrumpible de la red interna y de internet; así como también de las redes virtuales que conectan a las subsedes.
- Jefe De Sistemas Administrativos Y Financieros (Contables): Responsable de la resolución de problemas, solicitud de acceso, solicitud de instalación o actualización, solicitud de capacitación, solicitud de cambios de los sistemas Administrativos y financieros.
- Responsable De Base De Datos: Responsable de conceder los permisos de acceso a los usuarios en las aplicaciones dependiendo de las solicitudes realizadas por los responsables de los procesos, y además del mantenimiento, configuración y soporte de las bases de datos.
- Jefe Técnico: Responsable del mantenimiento y configuración de los computadores de escritorio, portátiles y periféricos; instalación de los programas utilitarios. Además, es responsable de resolver problemas a la alimentación eléctrica del centro de datos y UPS.

Anexo H: AMENAZAS

Mapa de Riesgos

De la valoración de los activos realizada se han considerado las amenazas que producen más daños, para evaluar el nivel de degradación, frecuencia y el riesgo implicado.

Caracterización de las Amenazas

Las amenazas están clasificadas en cuatro grupos:

- [N] Desastres Naturales y de Entorno
- [I] De origen industrial
- [E] Errores y fallos no intencionados (Ataque no deliberado)
- [A] Ataque intencionados (Ataque deliberado)

Identificación de las Amenazas

El objetivo de esta tarea: Identificar las amenazas relevantes sobre cada activo.

Tabla 1. Identificación de las amenazas

TIPO ACTIVOS	ACTIVOS	AMENAZAS POR ACTIVOS
Equipamiento - Hardware	Computador de Personal	[A.6] Abuso de privilegios de acceso
		[A.7] Uso no previsto
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)
		[E.24] Caída del sistema por agotamiento de recursos
		[I.*] Desastres industriales
		[I.5] Avería de origen físico o lógico
		[I.7] Condiciones inadecuadas de temperatura o humedad
		[N.*] Desastres naturales
		[N.2] Daños por agua
	Equipos de Comunicaciones	[A.10] Alteración de secuencia
		[A.11] Acceso no autorizado
		[A.12] Análisis de tráfico

		[A.14] Interceptación de información (escucha)
		[A.5] Suplantación de la identidad del usuario
		[A.7] Uso no previsto
		[A.9] [Re-]encaminamiento de mensajes
		[E.1] Errores de los usuarios
		[E.10] Errores de secuencia
		[E.15] Alteración de la información
		[E.19] Fugas de información
		[E.9] Errores de [re-]encaminamiento
		[I.3] Contaminación medioambiental
		[I.5] Avería de origen físico o lógico
		[I.7] Condiciones inadecuadas de temperatura o humedad
		[I.8] Fallo de servicios de comunicaciones
		[N.*] Desastres naturales
		[N.1] Fuego
		[N.2] Daños por agua
	Respaldos	[A.11] Acceso no autorizado
		[A.15] Modificación de la información
		[A.19] Revelación de información
		[E.15] Alteración de la información
		[E.19] Fugas de información
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)
		[I.5] Avería de origen físico o lógico
		[I.7] Condiciones inadecuadas de temperatura o humedad
	Servidores	[A.11] Acceso no autorizado
		[A.23] Manipulación del hardware
		[E.2] Errores del administrador del sistema / de la seguridad
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)
		[I.3] Contaminación medioambiental
		[I.5] Avería de origen físico o lógico
		[I.7] Condiciones inadecuadas de temperatura o humedad
		[N.*] Desastres naturales
		[N.1] Fuego
		[N.2] Daños por agua
Equipamiento - Software	Almacenamiento - Bases de Datos	[A.10] Alteración de secuencia
		[A.11] Acceso no autorizado
		[A.5] Suplantación de la identidad del usuario
		[A.9] [Re-]encaminamiento de mensajes
		[E.10] Errores de secuencia
		[E.9] Errores de [re-]encaminamiento

		[I.8] Fallo de servicios de comunicaciones
	Correo Electrónico	[A.10] Alteración de secuencia
		[A.11] Acceso no autorizado
		[A.5] Suplantación de la identidad del usuario
		[A.9] [Re-]encaminamiento de mensajes
		[E.10] Errores de secuencia
		[E.9] Errores de [re-]encaminamiento
		[I.8] Fallo de servicios de comunicaciones
	Internet	[A.5] Suplantación de la identidad del usuario
		[A.7] Uso no previsto
		[E.20] Vulnerabilidades de los programas (software)
		[E.21] Errores de mantenimiento / actualización de
		I.5] Avería de origen físico o lógico
	Sistemas Financieros (contables) y Administrativos	[A.7] Uso no previsto
		[A.8] Difusión de software dañino
		[E.1] Errores de los usuarios
		[E.20] Vulnerabilidades de los programas (software)
		[E.21] Errores de mantenimiento / actualización de programas (software)
		[E.8] Difusión de software dañino
		[I.5] Avería de origen físico o lógico
	Virtualización	[A.10] Alteración de secuencia
		[A.11] Acceso no autorizado
		[A.5] Suplantación de la identidad del usuario
		[A.9] [Re-]encaminamiento de mensajes
		[E.10] Errores de secuencia
		[E.9] Errores de [re-]encaminamiento
		[I.8] Fallo de servicios de comunicaciones
Equipamiento Auxiliar	Cableado eléctrico	[A.6] Abuso de privilegios de acceso
		[A.7] Uso no previsto
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)
		[E.24] Caída del sistema por agotamiento de recursos
		[I.*] Desastres industriales
		[I.3] Contaminación medioambiental
		[I.5] Avería de origen físico o lógico
		[I.7] Condiciones inadecuadas de temperatura o humedad
		[N.*] Desastres naturales
		[N.2] Daños por agua
	Equipos de Climatización	[A.6] Abuso de privilegios de acceso
		[A.7] Uso no previsto
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)
		[E.24] Caída del sistema por agotamiento de recursos

		[I.*] Desastres industriales
		[I.3] Contaminación medioambiental
		[I.5] Avería de origen físico o lógico
		[I.7] Condiciones inadecuadas de temperatura o humedad
		[N.*] Desastres naturales
		[N.2] Daños por agua
	Generadores Eléctricos	[A.6] Abuso de privilegios de acceso
		[A.7] Uso no previsto
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)
		[E.24] Caída del sistema por agotamiento de recursos
		[I.*] Desastres industriales
		[I.3] Contaminación medioambiental
		[I.5] Avería de origen físico o lógico
		[I.7] Condiciones inadecuadas de temperatura o humedad
		[N.*] Desastres naturales
		[N.2] Daños por agua
	UPS	[A.11] Acceso no autorizado
		[A.23] Manipulación del hardware
		[E.2] Errores del administrador del sistema / de la seguridad
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)
		[I.3] Contaminación medioambiental
		[I.5] Avería de origen físico o lógico
		[I.7] Condiciones inadecuadas de temperatura o humedad
		[N.*] Desastres naturales
		[N.1] Fuego
		[N.2] Daños por agua
Instalaciones	Centro de Datos	[A.27] Ocupación enemiga
		[I.*] Desastres industriales
		[N.*.1] Tormentas
		[N.*.11] Calor extremo
		[N.*.4] Terremotos
		[N.*.9] Tsunamis
		[N.2] Daños por agua
		[N.1] Fuego
	Cuartos de Red	[A.27] Ocupación enemiga
		[I.*] Desastres industriales
		[N.*.1] Tormentas
		[N.*.11] Calor extremo
		[N.*.4] Terremotos
		[N.*.9] Tsunamis
		[N.2] Daños por agua
		[N.1] Fuego

Personal	Administradores	[A.29] Extorsión
		[A.30] Ingeniería social (picaresca)
		[E.28.1] Enfermedad
		[E.28.2] Huelga
	Equipo de Desarrollo	[A.29] Extorsión
		[A.30] Ingeniería social (picaresca)
		[E.28.1] Enfermedad
		[E.28.2] Huelga
	Equipos Técnico	[A.29] Extorsión
		[A.30] Ingeniería social (picaresca)
		[E.28.1] Enfermedad
		[E.28.2] Huelga

Fuente: El Autor

Valoración de Amenazas por Activos

Tabla 2. Valoración de amenazas por Activos

Tipos de Activos	Activos	Amenazas Relevantes	Degradación	Frecuencia	Riesgo
Equipamiento - Hardware	Servidores	Incendio	MA	MB	Medio
		Terremoto	MA	MB	Medio
		Robo	A	B	Medio
		Acceso no autorizado	A	M	Alto
		Falla de generador eléctrico	A	B	Medio
	Equipos de comunicaciones	Incendio	MA	MB	Medio
		Terremoto	MA	MB	Medio
		Robo	A	B	Medio
		Acceso no autorizado	M	B	Alto
		Desconexión física lógica	MA	A	Alto
		Falla de generador eléctrico	A	MB	Medio
	Respaldos	Incendio	MA	MB	Medio
		Terremoto	MA	MB	Medio
		Robo	A	B	Medio
	Computador de personal	Incendio	MA	MB	Medio
		Terremoto	MA	MB	Medio
		Robo	MA	B	Medio
		Malware	M	A	Alto
Equipamiento - Software	Sistemas financieros (contables) y administrativos	Incendio	MA	MB	Medio
		Terremoto	MA	MB	Medio
		Acceso no autorizado	M	A	Alto

	Almacenamiento – bases de datos	Acceso no autorizado	M	M	Medio
		Desconexión física lógica	MA	B	Medio
		Agotamiento de recurso	MA	M	Alto
	Correo electrónico	Incendio	MA	MB	Medio
		Terremoto	MA	MB	Medio
		Acceso no autorizado	A	A	Alto
		Desconexión física lógica	MA	M	Alto
	Virtualización	Incendio	MA	MB	Medio
		Terremoto	MA	MB	Medio
		Acceso no autorizado	MA	A	Alto
		Desconexión física lógica	MA	M	Alto
	Internet	Incendio	MA	MB	Medio
		Terremoto	MA	MB	Medio
		Desconexión física lógica	MA	MA	Alto
Comunicaciones	Red Alambrica	Incendio	MA	MB	Medio
		Terremoto	MA	MB	Medio
	Red Inalambrica	Incendio	MA	MB	Medio
		Terremoto	MA	MB	Medio
	Enlace con Proveedor	Incendio	MA	MB	Medio
		Terremoto	MA	MB	Medio
		Desconexión física lógica	MA	A	Alto
Equipamiento Auxiliar	UPS	Incendio	MA	MB	Medio
		Terremoto	MA	MB	Medio
		Falla de equipos de climatización	A	MA	Alto
	Generador Electrico	Incendio	MA	MB	Medio
		Terremoto	MA	MB	Medio
	Equipos de Climatización	Incendio	MA	MB	Medio
		Terremoto	MA	MB	Medio
		Falla de equipos de climatización	MA	MA	Alto
	Cableado eléctrico	Incendio	MA	MB	Medio
		Terremoto	MA	MB	Medio
		Desconexión física lógica	MA	B	Medio
Instalaciones	Centro de datos	Incendio	MA	MB	Medio
		Terremoto	MA	MB	Medio
		Acceso no autorizado	MA	B	Medio
	Cuarto de Rack	Incendio	MA	MB	Medio
		Terremoto	MA	MB	Medio

		Acceso no autorizado	MA	B	Medio
Personal	Equipo de desarrollo	Incendio	MA	MB	Medio
		Terremoto	MA	MB	Medio
		Fuga de informacion	A	M	Medio
	Equipo Tecnico	Incendio	MA	MB	Medio
		Terremoto	MA	MB	Medio
		Fuga de informacion	A	A	Alto
	Administradores	Incendio	MA	MB	Medio
		Terremoto	MA	MB	Medio
		Fuga de informacion	A	A	Alto

Fuente: El Autor

Valoración de las Amenazas

Los objetivos planteados en esta tarea son:

- Evaluar la probabilidad de ocurrencia de cada amenaza concerniente a cada activo
- Estimar la degradación que causaría la amenaza en cada dimensión del activo si llegara a materializarse.

Para valorar las amenazas de cada activo se han tomado en cuenta la degradación de valor y la probabilidad de ocurrencia.

Tabla 3. Degradación del Valor y Probabilidad de Ocurrencia.

MA	MUY ALTA
A	ALTA
M	MEDIA
B	BAJA
MB	MUY BAJA

Degradación del valor

CS	CASI SEGURO
MA	MUY ALTO
P	POSIBLE
PP	POCO PROBABLE
MB	SIGLOS
MR	MUY RARA

Probabilidad de ocurrencia

Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1793-magerit-libro-iii-tecnicas/file.html

VALORACIÓN DE LAS AMENAZAS.

Tabla 4. Valoración de las amenazas encontradas en la empresa

ACTIVOS	AMENAZAS	PROBABILIDAD	[D]	[I]	[C]	[A]	[T]
TELEFONÍA IP	[E.1] Errores de los usuarios	A - P	0				
INTERNET	[A.7] Uso no previsto	B -PP	6				1
	[I.5] Avería de origen físico o lógico	A - MA	1	6	8		
	[E.20] Vulnerabilidades de los programas (software)	A - MA	1			10	8
	[E.21] Errores de mantenimiento / actualización de programas (software)	A - MA	0	7			
	[A.5] Suplantación de la identidad del usuario	A - P	0	10	10	10	10
OFIMÁTICA	[E.1] Errores de los usuarios	M - P	1				
	[E.20] Vulnerabilidades de los programas (software)	A - MA		1			
	[E.21] Errores de mantenimiento / actualización de programas (software)	A - P	1				
	[A.8] Difusión de software dañino	A - MA	0				
ANTIVIRUS	[E.8] Difusión de software dañino	A - MA		7	7	8	
	[E.20] Vulnerabilidades de los programas (software)	A - P	1		6		
	[E.21] Errores de mantenimiento / actualización de programas (software)	A - MA	0				
SISTEMA OPERATIVO	[I.5] Avería de origen físico o lógico	MA - CS	2	5	6	6	
	[E.1] Errores de los usuarios	M - P	2				
	[E.8] Difusión de software dañino	A - MA		7		6	
	[E.20] Vulnerabilidades de los programas (software)	M - P	1				
	[E.21] Errores de mantenimiento / actualización de programas (software)	MA - CS	2		4		
	[A.7] Uso no previsto	B - PP	1		8		
OTROS SOFTWARE	[E.8] Difusión de software dañino	M - P					1
	[E.20] Vulnerabilidades de los programas (software)	M - P			3		1
	[E.21] Errores de mantenimiento / actualización de	A - MA	1				1
	programas (software)						1
SERVIDOR DE BASE DE DATOS	[N.1] Fuego	A - MA	2	10	10	6	6
	[N.2] Daños por agua	A - P	2	10	10	0	8
	[N.*] Desastres naturales	M - P	2	10	10	3	8
	[I.3] Contaminación medioambiental	A - MA	2	6	6	6	
	[I.5] Avería de origen físico o lógico	MA - CS	4	9	9	3	1

ACTIVOS	AMENAZAS	PROBABILIDAD	[D]	[I]	[C]	[A]	[T]
	[I.7] Condiciones inadecuadas de temperatura o humedad	A - MA	4	9	9		
	[E.2] Errores del administrador del sistema / de la seguridad	M - P	1	8	8		
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	MA – CS	1	6	6		
	[A.11] Acceso no autorizado	A - MA	2	8	8	8	
	[A.23] Manipulación del hardware	A - MA	1		6		
MEDIOS DE IMPRESIÓN	[I.5] Avería de origen físico o lógico	MA - MA	2				1
	[I.7] Condiciones inadecuadas de temperatura o humedad	M -P	0				
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	MA - CS	1				1
	[A.11] Acceso no autorizado	A - P	2				3
COMPUTADORAS DE ESCRITORIO	[N.2] Daños por agua	M - P	0	10	10		9
	[N.*] Desastres naturales	M - PP	1	8			
	[I.*] Desastres industriales	M - PP	1	8			
	[I.5] Avería de origen físico o lógico	A - P	4	8	8	8	7
	[I.7] Condiciones inadecuadas de temperatura o humedad	M -P	0	6			
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A - MA	3	8	8		2
	[E.24] Caída del sistema por agotamiento de recursos	A - MA	1	8	8		
	[A.6] Abuso de privilegios de acceso	A - P	1	8	7	7	4
	[A.7] Uso no previsto	A –P	1		3		1
ROUTER	[N.1] Fuego [N.2] Daños por agua	M -P	1	7	7	7	4
	[N.*] Desastres naturales	M - PP	1	7	7	7	5
	[I.3] Contaminación medioambiental	M -PP	1	7	7		
	[I.5] Avería de origen físico o lógico	M - MA	3	7	7	7	5
	[I.7] Condiciones inadecuadas de temperatura o humedad	M - P	1	4	4	4	2
	[A.11] Acceso no autorizado	A - P	0				
	[I.8] Fallo de servicios de comunicaciones	A - MA	3	7	7	7	2
	[E.9] Errores de [re-]encaminamiento	A -P	3	7	7	7	2
	[E.15] Alteración de la información	A - P	0	10	10	10	7
	[E.19] Fugas de información	A - MA	0	10	10	10	7
	[A.7] Uso no previsto	M -P	1	7	7		1

ACTIVOS	AMENAZAS	PROBABILIDAD	[D]	[I]	[C]	[A]	[T]
	[A.9] [Re-]encaminamiento de mensajes	A-P	1				
	[A.10] Alteración de secuencia	A - P	1				
	[A.12] Análisis de tráfico	M - P	1				
	[A.14] Interceptación de información (escucha)	A - MA	0	7	8		5
WIFI	[I.8] Fallo de servicios de comunicaciones	MA - CS	0				2
	[E.9] Errores de [re-]encaminamiento	A - MA	0				
LAN	[I.8] Fallo de servicios de comunicaciones	A - MA	1				5
	[E.9] Errores de [re-]encaminamiento	MB - MR	1				5
	[E.10] Errores de secuencia	MB - MB	0				
	[A.5] Suplantación de la identidad del usuario	B - PP	1	10	10	10	5
	[A.9] [Re-]encaminamiento de mensajes	MB - MB	0				
	[A.10] Alteración de secuencia	MB - MR	1				
	[A.11] Acceso no autorizado	M - P	0				
INTERNET	[I.8] Fallo de servicios de comunicaciones	M –P	10	2	2		
	[E.15] Alteración de la información	A - P		2	2		
CABLEADO	[I.3] Contaminación medioambiental	0 - MR					1
	[I.7] Condiciones inadecuadas de temperatura o humedad	MB - MR					2
MOBILIARIO	[I.3] Contaminación medioambiental	0-0	0				
SISTEMA DE VIGILANCIA	[I.3] Contaminación medioambiental [I.7] Condiciones inadecuadas de temperatura o humedad	MB – MR	0	5	8		
ANTENAS	[I.3] Contaminación medioambiental	0 - 0	0				
RADIOS	[I.3] Contaminación medioambiental	0 - 0	0				
SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA	[I.3] Contaminación medioambiental	0 – 0	0				
CD	[E.15] Alteración de la información	MB - PP	0	8	8	8	2
	[E.19] Fugas de información	A - MA	4	7	7	7	5
	[A.15] Modificación de la información	MB - PP	0				
	[A.19] Revelación de información	M - MA	0				
EDIFICIO	[N.1] Fuego	MB - PP	1	9	9	9	9
	[N.2] Daños por agua	MB - PP	1	9	9	9	9

ACTIVOS	AMENAZAS	PROBABILIDAD	[D]	[I]	[C]	[A]	[T]
	[N.*.1] Tormentas	B – MB	0	9	9		9
	[N.*.4] Terremotos	MB - MR	0	9	9		6
	[N.*.9] Tsunamis	0 - 0	0				
	[N.*.11] Calor extremo	0 - 0	0				
	[I.*] Desastres industriales	MB - MR	0				
	[A.27] Ocupación enemiga	MB - MR	0		10		
PERSONAL	[E.28.1] Enfermedad	M - P	1				2
	[E.28.2] Huelga	MB – MR	0		3		
	[A.29] Extorsión	MB - MR	0	7	7		
	[A.30] Ingeniería social (picaresca)	0 - 0	0				

Anexo I: CARACTERIZACIÓN DE LAS SALVAGUARDAS.

Se pueden definir varias etapas de estudio que pueden abarcar lapsos de tiempo corto o largos incluso de un año, pero nuestro caso de estudio tomaremos tres fases:

- Primera etapa llamada POTENCIAL (Potential)
- Segunda etapa llamada SITUACIÓN ACTUAL (Current)
- Tercera etapa llamada OBJETIVO (Target)

Identificación de las Salvaguardas.

Protecciones generales u horizontales

H Protecciones Generales - H.IA Identificación y autenticación - H.AC Control de acceso lógico

Se escogió esta salvaguarda ya que cualquier persona puede acceder a los activos inclusive los más importantes. La misma por que hace frente a las amenazas a las que están expuestos los activos. Y esta pueda ser aplicada a estas clases de activos: Datos/ Información, Servicios, Aplicaciones (software), Equipamiento informático (hardware), Redes de comunicaciones y Soportes de información Protege a las siguientes dimensiones de seguridad: Integridad, Confidencialidad y Autenticidad.

Hace frente a las siguientes amenazas:

- Errores de los usuarios
- Errores del administrador del sistema/ de la seguridad
- Difusión de software dañino
- Errores de [re]-encaminamiento
- Errores de secuencia
- Alteración de la información
- Fugas de información
- Vulnerabilidad de los programas (software)
- Errores de mantenimiento /actualización de programas (software)
- Suplantación de la identidad del usuario
- Abuso de privilegios de acceso

- Uso no previsto
- [Re-]encaminamiento de mensajes
- Alteración de secuencia
- Acceso no autorizado
- Modificación de la información
- Revelación de información y Manipulación de hardware

H.tools.AV Herramienta contra código dañino

La empresa posee herramientas contra código dañino, pero no siempre esta actualizado, o se encuentran caducados lo que hace fácil la propagación de virus, troyanos, etc. Por eso se escogió las siguientes salvaguardas:

- El programa se actualiza regularmente
- La base de datos de virus se actualiza regularmente
- Se revisan los programas y servicios de arranque del sistema
- Centralización de administración de permisos y roles de antivirus.

Estas salvaguardas solo pueden ser aplicado a la capa de: Aplicaciones (software), y hacen frente al siguiente amenaza: Difusión de software dañino y Aseguramiento de la disponibilidad. Dentro de este grupo de salvaguardas están:

- Se han previsto protecciones frente ataques de denegación de servicio (DoS)
- Procedimientos Operativos
- Se toman medidas frente a ataques originados en las propias instalaciones.

Se escogió estas salvaguardas por que la empresa no posee ningún de estas medidas de seguridad, las mismas que son pueden ser aplicadas en la capa: Servicios Internos y asegura la dimensión de la Disponibilidad.

Protección de las aplicaciones (software).

SW Protecciones de las Aplicaciones Informáticas

Se seleccionó las siguientes salvaguardas ya que la empresa no posee estas normas de seguridad como son:

- Se dispone de normativa sobre el uso autorizado de las aplicaciones

- Se dispone de normativa relativa al cumplimiento de los derechos
- Se controla la instalación de software autorizado y productos con licencia
- Se dispone de procedimientos para realizar copias de seguridad

SW.SC Se aplican perfiles de seguridad

Esta salvaguarda se encuentra muy básica, porque solo existe cuentas de usuario lo que es suficiente para acceder a cualquier parte del sistema, pero mediante el uso de esta salvaguarda podemos hacer frente a estas amenazas: Errores de los usuarios, Difusión de software dañino, Vulnerabilidad de los programas (software), Errores de mantenimiento/actualización de programas (software) y Uso no previsto.

Se debería tratar de cumplir con lo siguiente:

- Seguridad de los ficheros de datos de la aplicación
- Se protegen los ficheros de configuración
- Seguridad de los mecanismos de comunicación entre procesos
- Además de que se debe de llevar un Control de versión de toda actualización de software, ayuda a saber que cualquier software que posea la empresa esté libre de errores y hacer frente amenazas como son: Vulnerabilidades de los programas (software) y Errores de mantenimiento/actualización de programas (software).

Protección de los equipos (hardware).

HW Protección de los Equipos Informáticos

- Salvaguardas adecuadas para la protección de los equipos:
- Se dispone de normativa sobre el uso correcto del equipo.
- Se dispone de procedimientos de uso de equipamiento.

HW.SC Se aplican perfiles de seguridad

Esta salvaguarda en la empresa minimiza amenazas como son: Errores del administrados del sistema / de la seguridad, Uso no previsto y Acceso no autorizado, además de asegurar las dimensiones: integridad y confidencialidad.

Protección de las comunicaciones.

COM Protección de las Comunicaciones - COM.SC Se aplican perfiles de seguridad

Se han seleccionado las siguientes salvaguardas para minimizar riesgos:

- Se deben de aplicar perfiles de seguridad para garantizar la comunicación en la empresa y para hacer frente amenazas como: Errores de [re] – encaminamiento, Errores de secuencia, Alteración de la información, Uso no previsto, [Re-]encaminamiento de mensajes, Alteración de secuencia y Acceso no autorizado.
- La empresa no posee dispone de normativa de uso de los servicios de red.
- Así mismo no dispone de un Control de filtrado.
- Ni siquiera de mecanismos como son: Comprobación de origen y destino, Mecanismos de control, No tiene ninguna: Seguridad de los servicios de red.

COM internet Internet: uso de acceso a

Para garantizar las comunicaciones cuando están utilizando el internet es necesario emplear siguientes salvaguardas:

- Herramienta de control de contenidos con filtros actualizados
- Se controla la configuración de los navegadores
- Se registra la descarga
- Se han instalado herramientas anti spyware
- Se deshabilitan las “cookies” en los navegadores
- Se registra la navegación web
- Se dispone de normativa sobre el uso de los servicios Internet
- Herramienta de monitorización del tráfico
- Se toman medidas frente a la inyección de información espuria
- Se aplica la regla de “seguridad por defecto”
- Se requiere autorización para que medios y dispositivos que tengan acceso a redes y servicios

Protección de los soportes de información.

MP Protección de los Soportes de Información.

Para proteger el único activo se han escogido las salvaguardas más apropiadas:

- Proteger en uso de contenedores cerrados
- Disponer de normativa de relativa a la protección criptográfica de los contenidos

Protección de los elementos auxiliares.

AUX Elementos Auxiliares.

Se asegura la disponibilidad como:

- Siguiendo las recomendaciones del fabricante o proveedor
- Continuidad de operaciones: para asegurar la disponibilidad de los equipos auxiliares además para contrarrestar la amenaza de contaminación medioambiental.
- Climatización: La adecuada climatización de cada equipo ayuda a enfrentar la amenaza que tiene la mayoría de estos componentes que es: Condiciones inadecuadas de temperatura o humedad.

Seguridad física – Protección de las instalaciones.

L Protección de las Instalaciones.

- Se dispone de normativa de seguridad para la seguridad de las instalaciones.
- Se dispone de áreas específicas para equipos informáticos, para protegerlos de la Ocupación enemiga.
- Además de la Protección del perímetro y reforzar la Vigilancia en las instalaciones de la empresa.
- Protección frente a explosivos.

Salvaguardas relativas al personal.

PS Gestión del Personal

Se deben de crear las siguientes normas de seguridad.

- Se dispone de normativa relativa a la gestión de personal (materia de seguridad).
- Se dispone de procedimientos para la gestión de personal (materia de seguridad).
- Creación de normas del personal: Propio y Subcontratado.
- Se dispone de normativa de obligado cumplimiento en el desempeño del puesto de trabajo.
- Se establecen normas para la contratación de personal, para garantizar la confidencialidad de los datos, frente ataques de cómo Extorsión y Ataque desde el interior.
- Procedimientos relevantes de seguridad: Emergencias, incidencias.

Valoración de las Salvaguardas.

Tabla 1. Niveles de Madurez

Eficacia	*Nivel*	*Madurez*	*Estado*
0%	L0	inexistente	inexistente
10%	L1	inicial/ad hoc	iniciado
50%	L2	reproducible, pero intuitivo	parcialmente realizado
90%	L3	proceso definido	en funcionamiento
95%	L4	gestionado y medible	monitorizado
100%	L5	optimizado	mejora continua

Fuente: https://www.ccn-cert.cni.es/documentos-publicos/1793-magerit-libro-iii-tecnicas/file.html

Tabla 2. Evaluación de Salvaguardas

Riesgos	Salvaguardas	Actual	Objetivo
Incendio y Terremoto	Instalación de sistemas contra incendio	L3	L4
	Instalación de alarmas contra incendio	L3	L4
	Uso y mantenimiento de extintores	L4	L5
	Desarrollo de plan de emergencia ante incendios	L2	L3
	Desarrollo de plan de contingencia ante desastres	L0	L3
	Realizar simulacros de forma periódica	L0	L3
	Almacenar las cintas de respaldo en otra oficina	L3	L3
Falla de generador eléctrico	Mantenimiento semanal de generador eléctrico	L4	L5
	Mantenimiento de equipos de climatización	L4	L5

Riesgos	Salvaguardas	Actual	Objetivo
Falla de equipos de climatización	Adquirir nuevos equipos de climatización	L1	L3
Agotamiento de recursos	Mantenimiento preventivo de servidores y robot de cinta	L3	L4
	Revisión de directiva de copias de seguridad de forma regular	L0	L3
	Monitoreo de recursos de los equipos críticos	L3	L4
Desconexión Física o lógica	Asegurar los equipos de comunicaciones y servidores en armarios cerrados	L1	L3
Robo	Uso de cables de seguridad para computadores de personal y portátiles	L0	L3
Virus	Instalación de antivirus en servidores	L3	L4
	Instalación de antivirus en equipos de personal	L4	L4
	Actualizar periódicamente las firmas del antivirus	L4	L4
Malware	Instalación de antimalware en servidores	L0	L3
	Instalación de antimalware en equipos de personal	L0	L3
Errores de configuración	Realizar pruebas de actualizaciones previo a la instalación	L1	L3
	Pruebas periódicas del cortafuegos	L0	L3
Acceso no autorizado	Establecer controles de acceso físico	L3	L4
	Analizar directivas de cortafuegos con regularidad	L1	L3
	Implementación de sistema de detección de intrusos	L0	L3
	Asignar cuentas para la administración de sistemas	L1	L3
	Utilizar autenticación multifactor para conexión remota	L0	L3
	Implementar control de cuarentena en VPN	L0	L3
	Implementar directivas de contraseñas complejas	L2	L4
	Implementar controles avanzados de gestión de cuentas	L2	L4
Fuga de información	Implementar cifrado de datos	L2	L3
	Contratar personal responsable de la seguridad	L0	L4
	Solicitar historial de personal antes de ser contratado	L2	L3
	Dar charlas al personal referente a la seguridad	L1	L3

Fuente: El Autor

Anexo J. IMPACTO

Impacto Potencial.

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo el impacto que estas tendrían sobre el sistema.

Los impactos que se muestran con la siguiente escala según su valor:

[10]: Crítico
[9]: Muy alto
[8]: Muy Alto
[7]: Alto
[6]: Alto
[5]: Medio
[4]: Medio
[3]: Bajo
[2]: Bajo
[1]: Despreciable
[0]: Despreciable

Impacto Residual Acumulado.

El impacto acumulado se calcula con los datos de impacto acumulado sobre un activo y salvaguardas apropiadas para las amenazas sobre dicho activo.

Estimación del Riesgo

Riesgo Potencial. Es al que está sometido el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas; pero no las salvaguardas actualmente desplegadas. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener la probabilidad de ocurrencia. Los riesgos se muestran con la siguiente escala según su valor:

{9} NIVEL 9
{8} NIVEL 8
{7} Extremadamente crítico
{6} muy crítico
{5} Crítico
{4} Muy alto
{3} Alto
{2} Medio
{1} Bajo
{0} Despreciable

Riesgo Residual.

Riesgo Residual. Es al que está sometido el sistema teniendo en cuenta el valor de los activos y la valoración de las amenazas, así como eficacia de las salvaguardas actualmente desplegadas.

Riesgo Residual Acumulado. La estimación de riesgo residual acumulado nos indica la medida que las amenazas que afectan a los activos de orden superior que dependen de dicho activo.

Posteriormente se debe hacer una descripción del área informática o departamento de sistemas identificando los activos informáticos, los procesos que se realiza dentro del área y los servicios que presta a las demás áreas de la organización.

Finalmente se debe determinar las vulnerabilidades, amenazas y riesgos de seguridad del área informática o departamento de sistemas en cada uno de los activos informáticos categorizados de acuerdo al activo donde se presentan (talento humano, hardware, seguridad física, redes de datos, sistemas operativos, bases de datos, seguridad lógica, entre otros) y se debe entregar un cuadro con las categorías de los activos, las vulnerabilidades, amenazas de seguridad encontrados en dicha organización.

Tabla 1. Evaluación de impacto y riesgo

Activos	Amenaza	Impacto Potencial	Impacto Actual	Impacto Objetivo	Riesgo Potencial	Riesgo Actual	Riesgo Objetivo
Servidores	Incendio	10	7	5	4	4	2
	Terremoto	10	7	5	4	4	2
	Robo	9	6	3	4	4	2
	Acceso no autorizado	9	6	3	6	5	4
	Falla de generador eléctrico	9	5	3	6	5	4
Equipos de comunicaciones	Incendio	10	7	5	4	4	2
	Terremoto	10	7	5	4	4	2
	Robo	9	6	3	4	4	2

	Acceso no autorizado	9	6	3	6	5	2
	Desconexión Física o lógica	9	6	3	6	4	2
	Falla de generador eléctrico	9	5	3	6	4	2
Robot de cintas	Incendio	10	7	5	4	4	2
	Terremoto	10	7	5	4	4	2
	Robo	9	6	3	6	4	2
Computador de personal	Incendio	10	7	5	4	4	2
	Terremoto	10	7	5	4	4	2
	Robo	9	6	3	6	4	2
	Malware	9	8	3	7	6	4
Sistemas financieros y administrativos	Incendio	10	7	5	4	4	2
	Terremoto	10	7	5	4	4	2
	Acceso no autorizado	9	6	3	6	6	2
Almacenamiento – bases de datos	Acceso no autorizado	9	6	3	6	6	2
	Desconexión física o lógica	9	6	3	6	4	2
	Agotamiento de recursos	9	6	3	7	5	2
Correo electrónico	Incendio	10	7	5	4	4	2
	Terremoto	10	7	5	4	4	2
	Acceso no autorizado	9	6	3	6	6	2
	Desconexión física o lógica	9	6	3	6	6	2
Virtualización	Incendio	10	7	5	4	4	2
	Terremoto	10	7	5	4	4	2
	Acceso no autorizado	9	6	3	6	6	2
	Desconexión física o lógica	9	6	3	6	6	2
Internet	Incendio	10	7	5	4	4	2
	Terremoto	10	7	5	4	4	2
	Desconexión física o lógica	9	6	3	6	6	2
Red alámbrica	Incendio	10	7	5	4	4	2
	Terremoto	10	7	5	4	4	2
Red alámbrica	Incendio	10	7	5	4	4	2
	Terremoto	10	7	5	4	4	2
Enlace con proveedor	Incendio	10	7	5	4	4	2
	Terremoto	10	7	5	4	4	2
	Desconexión física o lógica	9	6	3	6	4	2
UPS	Incendio	10	7	5	4	4	2

	Terremoto	10	7	5	4	4	2
	Falla de equipos de climatización	9	7	3	8	8	4
Generador eléctrico	Incendio	10	7	5	4	4	2
	Terremoto	10	7	5	4	4	2
Equipos de climatización	Incendio	10	7	5	4	4	2
	Terremoto	10	7	5	4	4	2
	Falla de equipos de climatización	9	7	3	8	8	4
Cableado eléctrico	Incendio	10	7	5	4	4	2
	Terremoto	10	7	5	4	4	2
	Desconexión física o lógica	9	6	3	6	6	2
Centro de datos	Incendio	10	7	5	4	4	2
	Terremoto	10	7	5	4	4	2
	Acceso no autorizado	9	6	3	6	4	2
Cuarto de rack	Incendio	10	7	5	4	4	2
	Terremoto	10	7	5	4	4	2
	Acceso no autorizado	9	6	3	6	4	2
Equipo de desarrollo	Incendio	10	7	5	4	4	2
	Terremoto	10	7	5	4	4	2
	Fuga de información	9	6	3	7	5	3
Equipo técnico	Incendio	10	7	5	4	4	2
	Terremoto	10	7	5	4	4	2
	Fuga de información	9	6	3	7	5	3
Administradores	Incendio	10	7	5	4	4	2
	Terremoto	10	7	5	4	4	2
	Fuga de información	9	6	3	7	5	3

Fuente: El Autor

En la tabla anterior se han evaluado el impacto y riesgo de cada amenaza que afecta a los activos. En la evaluación del impacto potencial, actual y el objetivo se han valorado las salvaguardas actuales antes de ser implementadas, el estado actual y el nivel que se lograría al implementar las nuevas salvaguardas; obteniéndose bajos niveles de impacto considerado como residual, el cual debería ser parte de un nuevo análisis de riesgo.

Mientras la evaluación del riesgo potencial, actual y objetivo se ha considerado el impacto y la probabilidad de que pueda materializarse; también obteniéndose un riesgo residual que debería ser analizado para un nuevo estudio.

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN (PSI)

EMPRESA DE TRANSPORTES TIERRA GRATA COMPAÑÍA LTDA

MAYO 2018

CONTENIDO

1. INTRODUCCION

La Empresa de Transportes Tierra Grata Compañía Ltda., Identifica la información como un componente indispensable en la conducción y consecución de los objetivos definidos por la estrategia de la entidad, razón por la cual es necesario que la empresa establezca un marco de actuación y gobierno en el cual se asegure que la información es protegida de una manera adecuada independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada. La seguridad de la información es una prioridad para la Empresa de Transportes Tierra Grata Compañía Ltda., y por tanto es responsabilidad de todos velar por que no se realicen actividades que contradigan la esencia y el espíritu de cada una de estas políticas. Este documento describe las Políticas y Procedimientos de Seguridad de la Información definidas por la Empresa de Transportes Tierra Grata Compañía Ltda., Para la elaboración del mismo, se toman como base las leyes y demás regulaciones aplicables, el capítulo décimo segundo del título primero de la Circular Básica Jurídica de la Superintendencia Financiera de Colombia, la norma ISO 27001:2013 y las recomendaciones del estándar ISO 27002:2013. Las políticas incluidas en este manual se constituyen como parte fundamental del sistema de gestión de seguridad de la información de la Empresa de Transportes Tierra Grata Compañía Ltda., y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos.

2. OBJETIVO

El objetivo de este documento es establecer las políticas en seguridad de la información de la Empresa de Transportes Tierra Grata Compañía Ltda.,, con el fin de regular la gestión de la seguridad de la información al interior de la entidad.

3. ALCANCE

Las PSI cubren todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios y terceros que laboren o tengan relación con la Empresa de Transportes Tierra Grata Compañía Ltda.,, para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada.

4. POLÍTICA GLOBAL DE SEGURIDAD DE LA INFORMACIÓN

En la Empresa de Transportes Tierra Grata Compañía Ltda., la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

Consciente de las necesidades actuales, la Empresa de Transportes Tierra Grata Compañía Ltda., implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.

Los funcionarios, personal externo, proveedores y todos aquellos que tengan responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información de la Empresa de Transportes Tierra Grata Compañía Ltda., deben adoptar los lineamientos contenidos en el presente documento y en los documentos relacionados con él, con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información.

La Política Global de Seguridad de la Información de la Empresa de Transportes Tierra Grata Compañía Ltda., se encuentra soportada por políticas y procedimientos específicos los cuales guiarán el manejo adecuado de la información de la empresa. Adicionalmente, se establecerán políticas específicas de seguridad de la información las cuales se fundamentan en los dominios y objetivos de control del Anexo A de la norma internacional ISO 27001:2013.

El Comité de Seguridad tendrá la potestad de modificar la Política Global o las Políticas Específicas de Seguridad de la Información de acuerdo con las necesidades de revisión establecidas periódicamente o a la aplicabilidad de las mismas.

5. COMPROMISO DE LA DIRECCION

La Junta Directiva de la Empresa de Transportes Tierra Grata Compañía Ltda., Aprueba esta Política de Seguridad de la Información como muestra de su compromiso y apoyo

en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la entidad.

La Junta Directiva y la Alta Dirección de la entidad demuestran su compromiso a través de:

- La revisión y aprobación de las PSI contenidas en este documento.
- La promoción activa de una cultura de seguridad.
- Facilitar la divulgación de este manual a todos los funcionarios de la entidad.
- El aseguramiento de los recursos adecuados para implementar y mantener las PSI.
- La verificación del cumplimiento de las políticas aquí mencionadas.

6. SANCIONES PARA LAS VIOLACIONES A LAS PSI

Las PSI pretenden instituir y afianzar la cultura de seguridad de la información entre los funcionarios, personal externo y proveedores de la Empresa de Transportes Tierra Grata Compañía Ltda., Por tal razón, es necesario que las violaciones a las Políticas Seguridad de la Información sean clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información. Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan.

7. POLÍTICAS DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

7.1. POLÍTICA DE ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACION

La Empresa de Transportes Tierra Grata Compañía Ltda.,, establecerá un esquema de seguridad de la información en donde existan roles y responsabilidades definidos que consideren actividades de administración, operación y gestión de la seguridad de la información.

Procedimientos que rigen para la estructura organizacional de seguridad de la información

Procedimientos dirigidos a: ALTA DIRECCION

- La Alta Dirección de la Empresa de Transportes Tierra Grata Compañía Ltda.,, debe definir y establecer los roles y responsabilidades relacionados con la seguridad de la información en niveles directivo y operativo.
- La Alta Dirección debe definir y establecer el procedimiento de contacto con las autoridades en caso de ser requerido, así como los responsables para establecer dicho contacto.
- La Alta Dirección debe revisar y aprobar las PSI contenidas en este documento.
- La Alta Dirección debe promover activamente una cultura de seguridad de la información en la empresa.
- La Alta Dirección debe facilitar la divulgación de las PSI a todos los funcionarios de la entidad y al personal provisto por terceras partes.

Procedimientos dirigidos a: ALTA DIRECCION Y SECRETARIA GENERAL

- La Alta Dirección y la Secretaria General de la Empresa de Transportes Tierra Grata Compañía Ltda.,, deben asignar los recursos, la infraestructura física y el personal necesario para la gestión de la seguridad de la información de la empresa.

Procedimientos dirigidos a: COMITÉ DE SEGURIDAD DE LA INFORMACION

- El Comité de Seguridad de la Información debe actualizar y presentar ante la Junta Directiva las PSI, la metodología para el análisis de riesgos de seguridad y la metodología para la clasificación de la información, según lo considere pertinente.
- El Comité de Seguridad de la Información debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.

- El Comité de Seguridad de la Información debe verificar el cumplimiento de las PSI aquí mencionadas.

Procedimientos dirigidos a: OFICINA DE RIESGOS

- La Oficina de Riesgos debe liderar la generación de lineamientos para gestionar la seguridad de la información de la Empresa de Transportes Tierra Grata Compañía Ltda., y el establecimiento de controles técnicos, físicos y administrativos derivados de análisis de riesgos de seguridad.
- La Oficina de Riesgos debe validar y monitorear de manera periódica la implantación de los controles de seguridad establecidos.

Procedimientos dirigidos a: OFICINA DE CONTROL INTERNO

- La Oficina de Control Interno debe planear y ejecutar las auditorías internas al Sistema de Gestión de Seguridad de la Información de la Empresa de Transportes Tierra Grata Compañía Ltda., a fin de determinar si las políticas, procesos, procedimientos y controles establecidos están conformes con los requerimientos institucionales, requerimientos de seguridad y regulaciones aplicables.
- La Oficina de Control Interno debe ejecutar revisiones totales o parciales de los procesos o áreas que hacen parte del alcance del Sistema de Gestión de Seguridad de la Información, con el fin de verificar la eficacia de las acciones correctivas cuando sean identificadas no conformidades.
- La Oficina de Control Interno debe informar a las áreas responsables los hallazgos de las auditorías.

Procedimientos dirigidos a: DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología debe asignar las funciones, roles y responsabilidades, a sus funcionarios para la operación y administración de la plataforma tecnológica de la empresa. Dichas funciones, roles y responsabilidades deben encontrarse documentadas y apropiadamente segregadas.

Procedimientos dirigidos a: TODOS LOS USUARIOS

- Los funcionarios y personal provisto por terceras partes que realicen labores en o para la Empresa de Transportes Tierra Grata Compañía Ltda.,, tienen la responsabilidad de cumplir con las políticas, Procedimientos, procedimientos y estándares referentes a la seguridad de la información.

7.2. POLÍTICAS DE SEGURIDAD DEL PERSONAL

7.2.1. Política relacionada con la vinculación de funcionarios

La Empresa de Transportes Tierra Grata Compañía Ltda., reconoce la importancia que tiene el factor humano para el cumplimiento de sus objetivos misionales y, con el interés de contar con el personal mejor calificado, garantizará que la vinculación de nuevos funcionarios se realizará siguiendo un proceso formal de selección, acorde con la legislación vigente, el cual estará orientado a las funciones y roles que deben desempeñar los funcionarios en sus cargos.

7.2.2. Procedimientos relacionados con la vinculación de funcionarios

Procedimientos dirigidos a: SECRETARIA GENERAL - GRUPO DE TALENTO HUMANO

- El Grupo de Talento Humano debe realizar las verificaciones necesarias para confirmar la veracidad de la información suministrada por el personal candidato a ocupar un cargo en la Empresa de Transportes Tierra Grata Compañía Ltda., antes de su vinculación definitiva.
- El Grupo de Talento Humano debe certificar que los funcionarios de la empresa firmen un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de PSI; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo.

Procedimientos dirigidos a: SUPERVISORES DE CONTRATO, VICEPRESIDENTES, DIRECTORES Y JEFES DE OFICINA

- Cada Supervisor de Contrato, Vicepresidente, Director y Jefe de Oficina debe verificar la existencia de Acuerdos y/o Cláusulas de Confidencialidad y de la documentación de Aceptación de Políticas para el personal provisto por terceras

partes, antes de otorgar acceso a la información de la Empresa de Transportes Tierra Grata Compañía Ltda.,

Procedimientos dirigidos a: PERSONAL PROVISTOS POR TERCERAS PARTES

- El personal provisto por terceras partes que realicen labores en o para la Empresa de Transportes Tierra Grata Compañía Ltda.,, deben firmar un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de PSI, antes de que se les otorgue acceso a las instalaciones y a la plataforma tecnológica.
- El personal provisto por terceras partes, deben garantizar el cumplimiento de los Acuerdos y/o Cláusulas de Confidencialidad y aceptación de las PSI de la empresa.

7.2.3. Política aplicable durante la vinculación de funcionarios y personal provisto por terceros

La Empresa de Transportes Tierra Grata Compañía Ltda., en su interés por proteger su información y los recursos de procesamiento de la misma demostrará el compromiso de la Alta Dirección en este esfuerzo, promoviendo que el personal cuente con el nivel deseado de conciencia en seguridad de la información para la correcta gestión de los activos de información y ejecutando el proceso disciplinario necesario cuando se incumplan las PSI de la empresa.

Todos los funcionarios de la Empresa de Transportes Tierra Grata Compañía Ltda., deben ser cuidadosos de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgos la seguridad y el buen nombre de la entidad.

Procedimientos aplicables durante la vinculación de funcionarios y personal provisto por terceros

Procedimientos dirigidos a: ALTA DIRECCION

La Alta Dirección debe demostrar su compromiso con la seguridad de la información por medio de su aprobación de las políticas, Procedimientos y demás lineamientos que desee establecer la Empresa.

La Alta Dirección debe promover la importancia de la seguridad de la información entre los funcionarios la Empresa de Transportes Tierra Grata Compañía Ltda., y el personal provisto por terceras partes, así como motivar el entendimiento, la toma de conciencia y el cumplimiento de las políticas, Procedimientos, procedimientos y estándares para la seguridad de la información establecidos.

La Alta Dirección debe definir y establecer el proceso disciplinario o incluir en el proceso disciplinario existente la empresa, el tratamiento de las faltas de cumplimiento a las políticas de seguridad o los incidentes de seguridad que lo ameriten.

Procedimientos dirigidos a: OFICINA DE RIESGOS

La Oficina de Riesgos debe diseñar y ejecutar de manera permanente un programa de concienciación en seguridad de la información, con el objetivo de apoyar la protección adecuada de la información y de los recursos de procesamiento la misma.

La Oficina de Riesgos debe capacitar y entrenar a los funcionarios la Empresa de Transportes Tierra Grata Compañía Ltda., en el programa de concienciación en seguridad de la información para evitar posibles riesgos de seguridad.

Procedimientos dirigidos a: SECRETARIA GENERAL

La Secretaria General debe aplicar el proceso disciplinario de la empresa cuando se identifiquen violaciones o incumplimientos a las PSI.

Procedimientos dirigidos a: SECRETARIA GENERAL - GRUPO DE TALENTO HUMANO

El Grupo de Talento Humano debe convocar a los funcionarios a las charlas y eventos programados como parte del programa de concienciación en seguridad de la información, proveer los recursos para la ejecución de las capacitaciones y controlar la asistencia a dichas charlas y eventos, aplicando las sanciones pertinentes por la falta de asistencia no justificada.

Procedimientos dirigidos a: TODOS LOS USUARIOS

Los funcionarios y personal provisto por terceras partes que por sus funciones hagan uso de la información de la Empresa de Transportes Tierra Grata Compañía Ltda.,, deben dar cumplimiento a las políticas, Procedimientos y procedimientos de seguridad de la información, así como asistir a las capacitaciones que sean referentes a la seguridad de la información.

7.2.4. Política de desvinculación, licencias, vacaciones o cambio de labores de los funcionarios y personal provisto por terceros

La Empresa de Transportes Tierra Grata Compañía Ltda., asegurará que sus funcionarios y el personal provisto por terceros serán desvinculados o reasignados para la ejecución de nuevas labores de una forma ordenada, controlada y segura.
Procedimientos para la desvinculación, licencias, vacaciones o cambios de labores de los funcionarios y personal provisto por terceros

Procedimientos dirigidos a: SECRETARIA GENERAL - GRUPO DE TALENTO HUMANO

- El Grupo de Talento Humano debe realizar el proceso de desvinculación, licencias, vacaciones o cambio de labores de los funcionarios de la empresa llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin.

Procedimientos dirigidos a: SUPERVISORES DE CONTRATO, VICEPRESIDENTES, DIRECTORES Y JEFES DE OFICINA

- Cada Supervisor de Contrato, Vicepresidente, Director y Jefe de Oficina debe monitorear y reportar de manera inmediata la desvinculación o cambio de labores de los funcionarios o personal provistos por terceras partes a la Oficina de Riesgos.

Procedimientos dirigidos a: OFICINA DE RIESGOS

- La Oficina de Riesgos debe verificar los reportes de desvinculación o cambio de labores y posteriormente debe solicitar la modificación o inhabilitación de usuarios a la Dirección de Tecnología.

7.3. POLÍTICAS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

7.3.1. Política de responsabilidad por los activos

La Empresa de Transportes Tierra Grata Compañía Ltda., como propietario de la información física, así como de la información generada, procesada, almacenada y transmitida con su plataforma tecnológica, otorgará responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.

La información, archivos físicos, los sistemas, los servicios y los equipos (ej. estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y fases, entre otros) propiedad de la Empresa de Transportes Tierra Grata Compañía Ltda.,, son activos de la institución y se proporcionan a los funcionarios y terceros autorizados, para cumplir con los propósitos del negocio.

Toda la información sensible de la Empresa de Transportes Tierra Grata Compañía Ltda.,, así como los activos donde ésta se almacena y se procesa debe ser asignada a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y los criterios que dicte la Oficina de Riesgos. Los propietarios de los activos de información deben llevar a cabo el levantamiento y la actualización permanente del inventario de activos de información al interior de sus procesos o áreas.

Procedimientos de responsabilidad por los activos

Procedimientos dirigidos a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

- Las Vicepresidencias, Direcciones y Oficinas Asesoras de la Empresa de Transportes Tierra Grata Compañía Ltda., deben actuar como propietarias de la información física y electrónica de la entidad, ejerciendo así la facultad de aprobar o revocar el acceso a su información con los perfiles adecuados para tal fin.

- Los propietarios de los activos de información deben generar un inventario de dichos activos para las áreas o procesos que lideran, acogiendo las indicaciones de las guías de clasificación de la información; así mismo, deben mantener actualizado el inventario de sus activos de información.
- Los propietarios de los activos de información deben monitorear periódicamente la validez de los usuarios y sus perfiles de acceso a la información.
- Los propietarios de los activos de información deben ser conscientes que los recursos de procesamiento de información de la empresa, se encuentran sujetos a auditorías por parte de la Oficina de Control Interno y a revisiones de cumplimiento por parte de la Oficina de Riesgos.

Procedimientos dirigidos a: DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología es la propietaria de los activos de información correspondientes a la plataforma tecnológica de la Empresa de Transportes Tierra Grata Compañía Ltda., y, en consecuencia, debe asegurar su apropiada operación y administración.
- La Dirección de Tecnología en conjunto con el Comité de Control de Cambios, son quienes deben autorizar la instalación, cambio o eliminación de componentes de la plataforma tecnológica de la Empresa de Transportes Tierra Grata Compañía Ltda.,
- La Dirección de Tecnología debe establecer una configuración adecuada para los recursos tecnológicos, con el fin de preservar la seguridad de la información y hacer un uso adecuado de ellos.
- La Dirección de Tecnología es responsable de preparar las estaciones de trabajo fijas y/o portátiles de los funcionarios y de hacer entrega de las mismas.
- La Dirección de Tecnología es responsable de recibir los equipos de trabajo fijo y/o portátil para su reasignación o disposición final, y generar copias de seguridad de la información de los funcionarios que se retiran o cambian de labores, cuando les es formalmente solicitado.

Procedimientos dirigidos a: OFICINA DE RIESGOS

- La Oficina de Riesgos debe realizar un análisis de riesgos de seguridad de manera periódica, sobre los procesos de la Empresa de Transportes Tierra Grata Compañía Ltda.,
- La Oficina de Riesgos debe definir las condiciones de uso y protección de los activos de información, tanto los tecnológicos como aquellos que no lo son.
- La Oficina de Riesgos debe realizar revisiones periódicas de los recursos de la plataforma tecnológica y los SI de la empresa.

Procedimientos dirigidos a: VICEPRESIDENTES, DIRECTORES Y JEFES DE OFICINA

- Los Vicepresidentes, Directores y Jefes de Oficina, o quien ellos designen, deben autorizar a sus funcionarios el uso de los recursos tecnológicos, previamente preparados por la Dirección de Tecnología.
- Los Vicepresidentes, Directores y Jefes de Oficina, o quien ellos designen, deben recibir los recursos tecnológicos asignados a sus colaboradores cuando estos se retiran de la empresa o son trasladados de área.

Procedimientos dirigidos a: TODOS LOS USUARIOS

- Los recursos tecnológicos de la Empresa de Transportes Tierra Grata Compañía Ltda., deben ser utilizados de forma ética y en cumplimiento de las leyes y reglamentos vigentes, con el fin de evitar daños o pérdidas sobre la operación o la imagen de la empresa.
- Los recursos tecnológicos de la Empresa de Transportes Tierra Grata Compañía Ltda., provistos a funcionarios y personal suministrado por terceras partes, son proporcionados con el único fin de llevar a cabo las labores de la empresa; por consiguiente, no deben ser utilizados para fines personales o ajenos a este.
- Los funcionarios no deben utilizar sus equipos de cómputo y dispositivos móviles personales para desempeñar las actividades laborales.
- Los funcionarios no deben utilizar software no autorizado o de su propiedad en la plataforma tecnológica de la Empresa de Transportes Tierra Grata Compañía Ltda.,
- Todas las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos son asignados a un responsable, por lo cual es su compromiso hacer uso adecuado y eficiente de dichos recursos.
- En el momento de desvinculación o cambio de labores, los funcionarios deben realizar la entrega de su puesto de trabajo al Vicepresidente, Director o Jefe de Oficina o quien este delegue; así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.

7.3.2. Política de clasificación y manejo de la información

La Empresa de Transportes Tierra Grata Compañía Ltda., definirá los niveles más adecuados para clasificar su información de acuerdo con su sensibilidad, y generará una

guía de Clasificación de la Información para que los propietarios de la misma la cataloguen y determinen los controles requeridos para su protección.

Toda la información de la Empresa de Transportes Tierra Grata Compañía Ltda., debe ser identificada, clasificada y documentada de acuerdo con las guías de Clasificación de la Información establecidas por el Comité de Seguridad de la Información.

Una vez clasificada la información, La Empresa de Transportes Tierra Grata Compañía Ltda., proporcionará los recursos necesarios para la aplicación de controles en busca de preservar la confidencialidad, integridad y disponibilidad de la misma, con el fin de promover el uso adecuado por parte de los funcionarios de la empresa y personal provisto por terceras partes que se encuentre autorizado y requiera de ella para la ejecución de sus actividades.

Procedimientos para la clasificación y manejo de la información

Procedimientos dirigidos a: COMITÉ DE SEGURIDAD DE LA INFORMACION

- El Comité de Seguridad de la Información debe recomendar los niveles de clasificación de la información propuestos por la Oficina de Riesgos y la guía de clasificación de la Información de la Empresa de Transportes Tierra Grata Compañía Ltda., para que sean aprobados por la Junta Directiva.

Procedimientos dirigidos a: OFICINA DE RIESGOS

- La Oficina de Riesgos debe definir los niveles de clasificación de la información para la Empresa de Transportes Tierra Grata Compañía Ltda., y, posteriormente generar la guía de clasificación de la Información.
- La Oficina de Riesgos debe socializar y divulgar la guía de clasificación de la Información a los funcionarios de la empresa.
- La Oficina de Riesgos debe monitorear con una periodicidad establecida la aplicación de la guía de clasificación de la Información.

Procedimientos dirigidos a: DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología debe proveer los métodos de cifrado de la información, así como debe administrar el software o herramienta utilizado para tal fin.
- La Dirección de Tecnología debe efectuar la eliminación segura de la información, a través de los mecanismos necesarios en la plataforma tecnológica, ya sea cuando son dados de baja o cambian de usuario.

Procedimientos dirigidos a: DIRECCION DE TECNOLOGIA Y OFICINA DE RIESGOS

- La Dirección de Tecnología junto con la Oficina de Riesgo deben definir los métodos de cifrado de la información de la Entidad de acuerdo al nivel de clasificación de los activos.

Procedimientos dirigidos a: SECRETARIA GENERAL – COORDINACION DE ARCHIVO

- La Coordinación de Archivo debe utilizar los medios de los cuales está dotada para destruir o desechar correctamente la documentación física, con el fin de evitar la reconstrucción de la misma, acogiéndose a procedimiento establecido para tal fin.
- La Coordinación de Archivo debe realizar la destrucción de información cuando se ha cumplido su ciclo de almacenamiento.
- La Coordinación de Archivo debe administrar el contrato de almacenamiento y resguardo de las cintas de backup, otros medios de almacenamiento y documentos físicos de la Empresa de Transportes Tierra Grata Compañía Ltda., con el proveedor del servicio.
- La Coordinación de Archivo debe verificar el cumplimiento de los Acuerdos de Niveles de Servicio y Acuerdos de intercambio con el proveedor de custodia externo de los medios de almacenamiento y documentos de la empresa.

Procedimientos dirigidos a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

- Los propietarios de los activos de información deben clasificar su información de acuerdo con las guías de clasificación de la Información establecida.
- Los propietarios de los activos de información son responsables de monitorear periódicamente la clasificación de sus activos de información y de ser necesario realizar su re-clasificación.

Procedimientos dirigidos a: TODOS LOS USUARIOS

- Los usuarios deben acatar los lineamientos guía de clasificación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la empresa.
- La información física y digital de la Empresa de Transportes Tierra Grata Compañía Ltda., debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado en las tablas de retención documental y cuando se cumpla el periodo de expiración, toda la información debe ser eliminada adecuadamente.
- Los usuarios deben tener en cuenta estas consideraciones cuando impriman, escaneen, saquen copias y envíes faxes: verificar las áreas adyacentes a impresoras, escáneres, fotocopiadoras y máquinas de fax para asegurarse que no quedaron documentos relacionados o adicionales; asimismo, recoger de las impresoras, escáneres, fotocopiadoras y máquinas de fax, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada.
- Tanto los funcionarios como el personal provisto por terceras partes deben asegurarse que en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.
- La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.

7.4. POLÍTICA DE USO DE PERIFERICOS Y MEDIOS DE ALMACENAMIENTO

El uso de periféricos y medios de almacenamiento en los recursos de la plataforma tecnológica de la Empresa de Transportes Tierra Grata Compañía Ltda., será reglamentado por la Dirección de Tecnología, junto con la Oficina de Riesgos, considerando las labores realizadas por los funcionarios y su necesidad de uso.

Procedimientos uso de periféricos y medios de almacenamiento

Procedimientos dirigidos a: DIRECCION DE TECNOLOGIA Y OFICINA DE RIESGOS

- La Dirección de Tecnología y la Oficina de Riesgos deben establecer las condiciones de uso de periféricos y medios de almacenamiento en la plataforma tecnológica de la Empresa de Transportes Tierra Grata Compañía Ltda.,

Procedimientos dirigidos a: DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología debe implantar los controles que regulen el uso de periféricos y medios de almacenamiento en la plataforma tecnológica de la empresa, de acuerdo con los lineamientos y condiciones establecidas.
- La Dirección de Tecnología debe generar y aplicar lineamientos para la disposición segura de los medios de almacenamiento de la empresa, ya sea cuando son dados de baja o re-asignados a un nuevo usuario.

Procedimientos dirigidos a: OFICINA DE RIESGOS

- La Oficina de Riesgos debe autorizar el uso de periféricos o medios de almacenamiento en la plataforma tecnológica de la empresa de acuerdo con el perfil del cargo del funcionario solicitante.
- Los funcionarios y el personal provisto por terceras partes deben acoger las condiciones de uso de los periféricos y medios de almacenamiento establecidos por la Dirección de Tecnología.
- Los funcionarios de la Empresa de Transportes Tierra Grata Compañía Ltda., y el personal provisto por terceras partes no deben modificar la configuración de periféricos y medios de almacenamiento establecidos por la Dirección de Tecnología.
- Los funcionarios y personal provisto por terceras partes son responsables por el custodio de los medios de almacenamiento institucionales asignados.
- Los funcionarios y personal provisto por terceras partes no deben utilizar medios de almacenamiento personales en la plataforma tecnológica de la Empresa de Transportes Tierra Grata Compañía Ltda.,

7.5. POLÍTICAS DE CONTROL DE ACCESO

7.5.1. Política de acceso a redes y recursos de red

La Dirección de Tecnología de la Empresa de Transportes Tierra Grata Compañía Ltda., como responsables de las redes de datos y los recursos de red de la empresa, debe

propender porque dichas redes sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico.

Procedimientos de acceso a redes y recursos de red

Procedimientos dirigidos a: DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología debe establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red de la Empresa de Transportes Tierra Grata Compañía Ltda.,
- La Dirección de Tecnología debe asegurar que las redes inalámbricas de la empresa cuenten con métodos de autenticación que evite accesos no autorizados.
- La Dirección de Tecnología, en conjunto con la Oficina de Riesgos, debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de red de la Empresa de Transportes Tierra Grata Compañía Ltda.,, así como velar por la aceptación de las responsabilidades de dichos terceros. Además, se debe formalizar la aceptación de las PSI por parte de estos.

Procedimientos dirigidos a: OFICINA DE RIESGOS

- La Oficina de Riesgos debe autorizar la creación o modificación de las cuentas de acceso a las redes o recursos de red de la Empresa de Transportes Tierra Grata Compañía Ltda.,
- La Oficina de Riesgos debe verificar periódicamente los controles de acceso para los usuarios provistos por terceras partes, con el fin de revisar que dichos usuarios tengan acceso permitido únicamente a aquellos recursos de red y servicios de la plataforma tecnológica para los que fueron autorizados.

Procedimientos dirigidos a: TODOS LOS USUARIOS

- Los funcionarios y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos de la Empresa de Transportes Tierra Grata Compañía Ltda., deben contar con el formato de creación de cuentas de usuario debidamente autorizado y el Acuerdo de Confidencialidad firmado previamente.

- Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos de la empresa deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

7.5.2. Política de administración de acceso de usuarios

La Empresa de Transportes Tierra Grata Compañía Ltda, establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los SI de la empresa. Así mismo, velará porque los funcionarios y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulada por Procedimientos y procedimientos establecidos para tal fin.

Procedimientos de administración de acceso de usuarios

Procedimientos dirigidos a: DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología debe establecer un procedimiento formal para la administración de los usuarios en las redes de datos, los recursos tecnológicos y SI de la empresa, que contemple la creación, modificación, bloqueo o eliminación de las cuentas de usuario.
- La Dirección de Tecnología, previa solicitud de los Jefes inmediatos de los solicitantes de las cuentas de usuario y aprobación tanto de los propietarios de los SI como de la Oficina de Riesgos, debe crear, modificar, bloquear o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los SI administrados, acorde con el procedimiento establecido.
- La Dirección de Tecnología, en conjunto con la Oficina de Riesgos, debe definir lineamientos para la configuración de contraseñas que aplicaran sobre la plataforma tecnológica, los servicios de red y los SI de la Empresa de Transportes Tierra Grata Compañía Ltda., dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros.
- La Dirección de Tecnología debe establecer un procedimiento que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los SI de manera oportuna, cuando los funcionarios se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo.

- La Dirección de Tecnología debe asegurarse que los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica sean inhabilitados o eliminados.

Procedimientos dirigidos a: OFICINA DE RIESGOS

- La Oficina de Riesgos debe autorizar la creación o modificación de las cuentas de acceso de los recursos tecnológicos y SI de la empresa.

Procedimientos dirigidos a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACION

- Es responsabilidad de los Propietarios de los activos de información, definir los perfiles de usuario y autorizar, conjuntamente con la Oficina de Riesgos, las solicitudes de acceso a dichos recursos de acuerdo con los perfiles establecidos.
- Los propietarios de los activos de información deben verificar y ratificar periódicamente todas las autorizaciones sobre sus recursos tecnológicos y SI.

Procedimientos dirigidos a: VICEPRESIDENTES, DIRECTORES Y JEFES DE OFICINA

- Los Vicepresidentes, Directores y Jefes de Oficina deben solicitar la creación, modificación, bloqueo y eliminación de cuentas de usuario, para los funcionarios que laboran en sus áreas, acogiéndose al procedimiento establecidos para tal fin.

7.5.3. Política de responsabilidades de acceso de los usuarios

Los usuarios de los recursos tecnológicos y los SI de la Empresa de Transportes Tierra Grata Compañía Ltda., realizarán un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual les es permitido el acceso.

Procedimientos de responsabilidades de acceso de los usuarios

Procedimientos dirigidos a: TODOS LOS USUARIOS

- Los usuarios de la plataforma tecnológica, los servicios de red y los SI de la Empresa de Transportes Tierra Grata Compañía Ltda., deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.
- Los funcionarios no deben compartir sus cuentas de usuario y contraseñas con otros funcionarios o con personal provisto por terceras partes.
- Los funcionarios y personal provisto por terceras partes que posean acceso a la plataforma tecnológica, los servicios de red y los SI de la empresa deben acogerse a lineamientos para la configuración de contraseñas implantados por la empresa.

7.5.4. Política de uso de altos privilegios y utilitarios de administración

La Dirección de Tecnología de la Empresa de Transportes Tierra Grata Compañía Ltda., velará porque los recursos de la plataforma tecnológica y los servicios de red de la empresa sean operados y administrados en condiciones controladas y de seguridad, que permitan un monitoreo posterior de la actividad de los usuarios administradores, poseedores de los más altos privilegios sobre dichos plataforma y servicios.

Procedimientos de uso de altos privilegios y utilitarios de administración

Procedimientos dirigidos a: DIRECCION DE TECNOLOGIA, ADMINISTRADORES DE LOS RECURSOS TECNOLOGICOS Y SERVICIOS DE RED

- La Dirección de Tecnología debe otorgar los privilegios para administración de recursos tecnológicos, servicios de red y SI sólo a aquellos funcionarios designados para dichas funciones.
- La Dirección de Tecnología debe establecer cuentas personalizadas con altos privilegios para cada uno de los administradores de los recursos tecnológicos, servicios de red y SI.
- La Dirección de Tecnología debe verificar que los administradores de los recursos tecnológicos y servicios de red no tengan acceso a SI en producción.
- La Dirección de Tecnología debe restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado, de acuerdo con las labores desempeñadas.
- La Dirección de Tecnología debe asegurarse que los usuarios o perfiles de usuario que traen por defecto los sistemas operativos, el firmware y las bases de datos sean suspendidos o renombrados en sus autorizaciones y que las contraseñas que traen por defecto dichos usuarios o perfiles sean modificadas.

- La Dirección de Tecnología debe establecer los controles para que los usuarios finales de los recursos tecnológicos, los servicios de red y los SI no tengan instalados en sus equipos de cómputo utilitarios que permitan accesos privilegiados a dichos recursos, servicios o sistemas.
- Los administradores de los recursos tecnológicos y servicios de red, funcionarios de la Dirección de Tecnología, no deben hacer uso de los utilitarios que permiten acceso a los sistemas operativos, firmware o conexión a las bases de datos para pasar por alto la seguridad de los SI alojados sobre la plataforma tecnológica de la Empresa de Transportes Tierra Grata Compañía Ltda.,
- Los administradores de los recursos tecnológicos deben deshabilitar las funcionalidades o servicios no utilizados de los sistemas operativos, el firmware y las bases de datos. Se debe configurar el conjunto mínimo requerido de funcionalidades, servicios y utilitarios.
- La Dirección de Tecnología debe generar y mantener actualizado un listado de las cuentas administrativas de los recursos de la plataforma tecnológica.

Procedimientos dirigidos a: OFICINA DE RIESGOS

- La Oficina de Riesgos debe validar que las políticas de contraseñas establecidas sobre la plataforma tecnológica, los servicios de red y los SI son aplicables a los usuarios administradores; así mismo, debe verificar que el cambio de contraseña de los usuarios administradores acoja el procedimiento definido para tal fin.
- La Oficina de Riesgos debe revisar periódicamente la actividad de los usuarios con altos privilegios en los registros de auditoria de la plataforma tecnológica y los SI.

7.5.5. Política de control de acceso a sistemas y aplicativos

Las Vicepresidencias, Direcciones o Jefaturas de Oficina como propietarias de los SI y aplicativos que apoyan los procesos y áreas que lideran, velarán por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada.

La Dirección de Tecnología, como responsable de la administración de dichos SI y aplicativos, propenderá para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Así mismo, velará porque los desarrolladores, tanto internos como externos, acojan buenas prácticas de desarrollo en los productos generados para controlar el acceso lógico y evitar accesos no autorizados a los sistemas administrados.

Procedimientos de control de acceso a sistemas y aplicativos

Procedimientos dirigidos a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACION

- Los propietarios de los activos de información deben autorizar los accesos a sus SI o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos.
- Los propietarios de los activos de información deben monitorear periódicamente los perfiles definidos en los SI y los privilegios asignados a los usuarios que acceden a ellos.

Procedimientos dirigidos a: DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología debe establecer un procedimiento para la asignación de accesos a los sistemas y aplicativos de la Empresa de Transportes Tierra Grata Compañía Ltda.,
- La Dirección de Tecnología debe establecer ambientes separados a nivel físico y lógico para desarrollo, pruebas y producción, contando cada uno con su plataforma, servidores, aplicaciones, dispositivos y versiones independientes de los otros ambientes, evitando que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad de la información de producción.
- La Dirección de Tecnología debe asegurar, mediante los controles necesarios, que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción, y así mismo que los menús muestren los mensajes de identificación apropiados para reducir los riesgos de error.
- La Dirección de Tecnología debe establecer el procedimiento y los controles de acceso a los ambientes de producción de los SI; así mismo, debe asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.
- La Dirección de Tecnología debe proporcionar repositorios de archivos fuente de los SI; estos deben contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.

Procedimientos dirigidos a: DESARROLLADORES (INTERNOS Y EXTERNOS)

- Los desarrolladores deben asegurar que los SI construidos requieran autenticación para todos los recursos y páginas, excepto aquellas específicamente clasificadas como públicas.
- Los desarrolladores deben certificar la confiabilidad de los controles de autenticación, utilizando implementaciones centralizadas para dichos controles.
- Los desarrolladores deben certificar que no se almacenen contraseñas, cadenas de conexión u otra información sensible en texto claro y que se implementen controles de integridad de dichas contraseñas.
- Los desarrolladores deben establecer los controles de autenticación de tal manera que cuando fallen, lo hagan de una forma segura, evitando indicar específicamente cual fue la falla durante el proceso de autenticación y, en su lugar, generando mensajes generales de falla.
- Los desarrolladores deben asegurar que no se despliegan en la pantalla las contraseñas ingresadas, así como deben deshabilitar la funcionalidad de recordar campos de contraseñas.
- Los desarrolladores deben certificar que se inhabilitan las cuentas luego de un número establecido de intentos fallidos de ingreso a los sistemas desarrollados.
- Los desarrolladores deben asegurar que, si se utiliza la reasignación de contraseñas, únicamente se envíe un enlace o contraseñas temporales a cuentas de correo electrónico previamente registradas en los aplicativos, los cuales deben tener un periodo de validez establecido; se deben forzar el cambio de las contraseñas temporales después de su utilización.
- Los desarrolladores deben certificar que el último acceso (fallido o exitoso) sea reportado al usuario en su siguiente acceso exitoso a los SI.
- Los desarrolladores deben asegurar la re-autenticación de los usuarios antes de la realización de operaciones críticas en los aplicativos.
- Los desarrolladores deben, a nivel de los aplicativos, restringir acceso a archivos u otros recursos, a direcciones URL protegidas, a funciones protegidas, a servicios, a información de las aplicaciones, a atributos y políticas utilizadas por los controles de acceso y a la información relevante de la configuración, solamente a usuarios autorizados.
- Los desarrolladores deben establecer que periódicamente se re-valide la autorización de los usuarios en los aplicativos y se asegure que sus privilegios no han sido modificados.

7.6. POLÍTICAS DE CRIPTOGRAFIA

7.6.1. Política de controles criptográficos

La Empresa de Transportes Tierra Grata Compañía Ltda., velará porque la información de la empresa, clasificada como reservada o restringida, será cifrada al momento de almacenarse y/o transmitirse por cualquier medio.

Procedimientos de controles criptográficos

Procedimientos dirigidos a: DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología debe almacenar y/o transmitir la información digital clasificada como reservada o restringida bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad
- La Dirección de Tecnología debe verificar que todo sistema de información o aplicativo que requiera realizar transmisión de información reservada o restringida, cuente con mecanismos de cifrado de datos.
- La Dirección de Tecnología debe desarrollar y establecer un procedimiento para el manejo y la administración de llaves de cifrado.
- La Dirección de Tecnología, debe desarrollar y establecer estándares para la aplicación de controles criptográficos.

Procedimientos dirigidos a: DESARROLLADORES (INTERNOS O EXTERNOS)

- Los desarrolladores deben cifrar la información reservada o restringida y certificar la confiabilidad de los sistemas de almacenamiento de dicha información.
- Los desarrolladores deben asegurarse que los controles criptográficos de los sistemas construidos cumplen con los estándares establecidos por la Dirección de Tecnología.

7.7. POLÍTICAS DE SEGURIDAD FISICA Y MEDIOAMBIENTAL

7.7.1. Política de áreas seguras

La Empresa de Transportes Tierra Grata Compañía Ltda., proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus sedes. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los SI y comunicaciones, se consideras áreas de acceso restringido.

Procedimientos de áreas seguras

Procedimientos dirigidos a: DIRECCION DE TECNOLOGIA

- Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas por funcionarios de la Dirección de Tecnología autorizados; no obstante, los visitantes siempre deberán estar acompañados de un funcionario de dicha dirección durante su visita al centro de cómputo o los centros de cableado.
- La Dirección de Tecnología debe registrar el ingreso de los visitantes al centro de cómputo y a los centros de cableado que están bajo su custodia, en una bitácora ubicada en la entrada de estos lugares de forma visible.
- La Dirección de Tecnología debe descontinuar o modificar de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de un funcionario autorizado.
- La Dirección de Tecnología debe proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.
- La Dirección de Tecnología debe velar porque los recursos de la plataforma tecnológica de la Empresa de Transportes Tierra Grata Compañía Ltda., ubicados en el centro de cómputo se encuentran protegidos contra fallas o interrupciones eléctricas.
- La Dirección de Tecnología debe certificar que el centro de cómputo y los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.
- La Dirección de Tecnología debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.

Procedimientos dirigidos a: VICEPRESIDENTES, DIRECTORES Y JEFES DE OFICINA

- Los Vicepresidentes, Directores y Jefes de Oficina que se encuentren en áreas restringidas deben velar mediante monitoreo por la efectividad de los controles de acceso físico y equipos de vigilancia implantados en su áreas.
- Los Vicepresidentes, Directores y Jefes de Oficina que se encuentren en áreas restringidas deben autorizar cualquier ingreso temporal a sus áreas, evaluando la pertinencia del ingreso; así mismo, deben delegar en personal del área el registro y supervisión de cada ingreso a sus áreas.
- Los Vicepresidentes, Directores y Jefes de Oficina deben velar porque las contraseñas de sistemas de alarma, cajas fuertes, llaves y otros mecanismos de seguridad de acceso a sus áreas solo sean utilizados por los funcionarios autorizados y, salvo situaciones de emergencia u otro tipo de eventos que por su naturaleza lo requieran, estos no sean transferidos a otros funcionarios de la empresa.

Procedimientos dirigidos a: SECRETARIA GENERAL – GRUPO DE RECURSOS FISICOS

- El Grupo de Recursos Físicos debe proporcionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implantados en las instalaciones de la Empresa de Transportes Tierra Grata Compañía Ltda.,
- El Grupo de Recursos Físicos debe identificar mejoras a los mecanismos implantados y, de ser necesario, la implementación de nuevos mecanismos, con el fin de proveer la seguridad física de las instalaciones de la empresa.
- El Grupo de Recursos Físicos debe almacenar y custodiar los registros del sistema de control de acceso a las instalaciones de la Empresa de Transportes Tierra Grata Compañía Ltda.,
- El Grupo de Recursos Físicos debe certificar la efectividad de los mecanismos de seguridad física y control de acceso al centro de cómputo, centros de cableado y demás áreas de procesamiento de información.
- El Grupo de Recursos Físicos debe controlar el ingreso de los visitantes a los centros de cableado que están bajo su custodia.
- El Grupo de Recursos Físicos debe cerciorarse de que los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.
- El Grupo de Recursos Físicos, con el acompañamiento de la Dirección de Tecnología, debe verificar que el cableado se encuentra protegido con el fin de disminuir las intercepciones o daños.

Procedimientos dirigidos a: TODOS LOS USUARIOS

- Los ingresos y egresos de personal a las instalaciones de la Empresa de Transportes Tierra Grata Compañía Ltda., deben ser registrados; por consiguiente, los funcionarios y personal provisto por terceras partes deben cumplir completamente con los controles físicos implantados.
- os funcionarios deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de la empresa; en caso de pérdida del carné o tarjeta de acceso a las instalaciones, deben reportarlo a la mayor brevedad posible.
- Aquellos funcionarios o personal provisto por terceras partes para los que aplique, en razón del servicio prestado, deben utilizar prendas distintivas que faciliten su identificación.
- Los funcionarios de la Empresa de Transportes Tierra Grata Compañía Ltda., y el personal provisto por terceras partes no deben intentar ingresar a áreas a las cuales no tengan autorización.

7.7.2. Política de seguridad para los equipos institucionales

La Empresa de Transportes Tierra Grata Compañía Ltda., para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica de la empresa que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

Procedimientos de seguridad para los equipos institucionales

Procedimientos dirigidos a: DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de la Empresa de Transportes Tierra Grata Compañía Ltda.,
- La Dirección de Tecnología debe realizar mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica de la empresa.
- La Dirección de Tecnología, en conjunto con la Coordinación de Recursos Físicos debe propender porque las áreas de carga y descarga de equipos de cómputo se encuentren aisladas del centro de cómputo y otras áreas de procesamiento de información.

- La Dirección de Tecnología debe generar estándares de configuración segura para los equipos de cómputo de los funcionarios de la empresa y configurar dichos equipos acogiendo los estándares generados.
- La Dirección de Tecnología debe establecer las condiciones que deben cumplir los equipos de cómputo de personal provisto por terceros, que requieran conectarse a la red de datos de la empresa y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.
- La Dirección de Tecnología debe aislar los equipos de áreas sensibles, como la Dirección de Tesorería para proteger su acceso de los demás funcionarios de la red de la empresa.
- La Dirección de Tecnología debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los funcionarios de la empresa, ya sea cuando son dados de baja o cambian de usuario.

Procedimientos dirigidos a: OFICINA DE CONTROL INTERNO

- La Oficina de Control Interno tiene la responsabilidad de incluir dentro del plan anual de auditorías la verificación aleatoria a los equipos de cómputo de todas las dependencias y puntos de atención de la entidad.

Procedimientos dirigidos a: OFICINA DE RIESGOS

- La Oficina de Riesgos debe evaluar y analizar los informes de verificación de equipos de cómputo de las diferentes áreas de la empresa, en particular de las áreas sensibles.

Procedimientos dirigidos a: SECRETARIA GENERAL – GRUPO DE RECURSOS FISICOS

- El Grupo de Recursos Físicos debe revisar los accesos físicos en horas no hábiles a las áreas donde se procesa información.
- El Grupo de Recursos Físicos debe restringir el acceso físico a los equipos de cómputo de áreas donde se procesa información sensible.
- El Grupo de Recursos Físicos debe velar porque la entrada y salida de estaciones de trabajo, servidores, equipos portátiles y demás recursos tecnológicos institucionales de las instalaciones de la Empresa de Transportes Tierra Grata Compañía Ltda., cuente con la autorización documentada y aprobada previamente por el Coordinador de Recursos Físicos.

- El Grupo de Recursos Físicos debe velar porque los equipos que se encuentran sujetos a traslados físicos fuera de la empresa, posean pólizas de seguro.

Procedimientos dirigidos a: TODOS LOS USUARIOS

- La Dirección de Tecnología es la única área autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos de la empresa.
- Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a los funcionarios y personal provisto por terceras partes deben acoger las instrucciones técnicas de proporcione la Dirección de Tecnología.
- Cuando se presente una falla o problema de hardware o software en una estación de trabajo u otro recurso tecnológico propiedad de la Empresa de Transportes Tierra Grata Compañía Ltda., el usuario responsable debe informar a la Mesa de Ayuda en donde se atenderá o escalará al interior de la Dirección de Tecnología, con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.
- La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la empresa, solo puede ser realizado por los funcionarios de la Dirección de Tecnología, o personal de terceras partes autorizado por dicha dirección.
- Los funcionarios de la empresa y el personal provisto por terceras partes deben bloquear sus estaciones de trabajo en el momento de abandonar su puesto de trabajo.
- Los funcionarios de la Empresa de Transportes Tierra Grata Compañía Ltda., y el personal provisto por terceras partes no deben dejar encendidas las estaciones de trabajo u otros recursos tecnológicos en horas no laborables.
- Los equipos de cómputo, bajo ninguna circunstancia, deben ser dejados desatendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados.
- Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física.
- Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.
- En caso de pérdida o robo de un equipo de cómputo de la Empresa de Transportes Tierra Grata Compañía Ltda.,, se debe informar de forma inmediata al líder del proceso para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.

- Los funcionarios de la empresa y el personal provisto por terceras partes deben asegurar que sus escritorios se encuentran libres de los documentos que son utilizados durante el desarrollo de sus funciones al terminar la jornada laboral y, que estos sean almacenados bajo las protecciones de seguridad necesarias.

7.8. PSI EN LAS OPERACIONES

7.8.1. Política de asignación de responsabilidades operativas

La Dirección de Tecnología, encargada de la operación y administración de los recursos tecnológicos que apoyan los procesos de la Empresa de Transportes Tierra Grata Compañía Ltda.,, asignará funciones específicas a sus funcionarios, quienes deben efectuar la operación y administración de dichos recursos tecnológicos, manteniendo y actualizando la documentación de los procesos operativos para la ejecución de las actividades. Así mismo, velará por la eficiencia de los controles implantados en los procesos operativos asociados a los recursos tecnológicos con el objeto de proteger la confidencialidad, la integridad y la disponibilidad de la información manejada y asegurará que los cambios efectuados sobre los recursos tecnológicos, serán adecuadamente controlados y debidamente autorizados.

La Dirección de Tecnología proveerá la capacidad de procesamiento requerida en los recursos tecnológicos y SI de la empresa, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica con una periodicidad definida.

Procedimientos de asignación de responsabilidades operativas

Procedimientos dirigidos a: DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología debe efectuar, a través de sus funcionarios, la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica de la empresa.
- La Dirección de Tecnología debe proporcionar a sus funcionarios manuales de configuración y operación de los sistemas operativos, firmware, servicios de red, bases de datos y SI que conforman la plataforma tecnológica de la Empresa de Transportes Tierra Grata Compañía Ltda.,
- La Dirección de Tecnología debe proveer los recursos necesarios para la implantación de controles que permitan la separación de ambientes de desarrollo, pruebas y producción, teniendo en cuenta consideraciones como: controles para

el intercambio de información entre los ambientes de desarrollo y producción, la inexistencia de compiladores, editores o fuentes en los ambientes de producción y un acceso diferente para cada uno de los ambientes.

- La Dirección de Tecnología, a través de sus funcionarios, debe realizar estudios sobre la demanda y proyecciones de crecimiento de los recursos administrados (capacity planning) de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica. Estos estudios y proyecciones deben considerar aspectos de consumo de recursos de procesadores, memorias, discos, servicios de impresión, anchos de banda, internet y tráfico de las redes de datos, entre otros.

Procedimientos dirigidos a: OFICINA DE RIESGOS

- La Oficina de Riesgos debe emitir concepto y generar recomendaciones acerca de las soluciones de seguridad seleccionadas para la plataforma tecnológica de la empresa.

7.8.2. Política de protección frente a software malicioso

La Empresa de Transportes Tierra Grata Compañía Ltda., proporcionará los mecanismos necesarios que garanticen la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso. Además, proporcionará los mecanismos para generar cultura de seguridad entre sus funcionarios y personal provisto por terceras partes frente a los ataques de software malicioso.

Procedimientos de protección frente a software malicioso

Procedimientos dirigidos a: DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología debe proveer herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica de la Empresa de Transportes Tierra Grata Compañía Ltda., y los servicios que se ejecutan en la misma.

- La Dirección de Tecnología debe asegurar que el software de antivirus, antimalware, antispam y antispyware cuente con las licencias de uso requeridas, certificando así su autenticidad y la posibilidad de actualización periódica de las últimas bases de datos de firmas del proveedor del servicio.
- La Dirección de Tecnología debe certificar que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.
- La Dirección de Tecnología, a través de sus funcionarios, debe asegurarse que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware.
- La Dirección de Tecnología, a través de sus funcionarios, debe certificar que el software de antivirus, antispyware, antispam, antimalware, posea las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.

Procedimientos dirigidos a: TODOS LOS USUARIOS

- Los usuarios de recursos tecnológicos no deben cambiar o eliminar la configuración del software de antivirus, antispyware, antimalware, antispam definida por la Dirección de Tecnología; por consiguiente, únicamente podrán realizar tareas de escaneo de virus en diferentes medios.
- Los usuarios de recursos tecnológicos deben ejecutar el software de antivirus, antispyware, antispam, antimalware sobre los archivos y/o documentos que son abiertos o ejecutados por primera vez, especialmente los que se encuentran en medios de almacenamiento externos o que provienen del correo electrónico.
- Los usuarios deben asegurarse que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.
- Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar a la Mesa de Ayuda, para que, a través de ella, la Dirección de Tecnología tome las medidas de control correspondientes.

7.8.3. Política de copias de respaldo de la información

La Empresa de Transportes Tierra Grata Compañía Ltda., certificará la generación de copias de respaldo y almacenamiento de su información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la

realización de estas actividades. Las áreas propietarias de la información, con el apoyo de la Dirección de Tecnología, encargada de la generación de copias de respaldo, definirán la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información.

Así mismo, la empresa velará porque los medios magnéticos que contienen la información crítica sean almacenados en una ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados.

Procedimientos de copias de respaldo de la información

Procedimientos dirigidos a: DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología, a través de sus funcionarios, debe generar y adoptar los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad.
- La Dirección de Tecnología debe disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.
- La Dirección de Tecnología, a través de sus funcionarios, debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.
- La Dirección de Tecnología debe definir las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información que son almacenadas externamente.
- La Dirección de Tecnología debe proporcionar apoyo para la definición de las estrategias de generación, retención y rotación de las copias de respaldo de la los activos información de la empresa.

Procedimientos dirigidos a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

- Los propietarios de los recursos tecnológicos y SI deben definir, en conjunto con la Dirección de Tecnología, las estrategias para la generación, retención y rotación de las copias de respaldo de los activos de información.

Procedimientos dirigidos a: TODOS LOS USUARIOS

- Es responsabilidad de los usuarios de la plataforma tecnológica de la Empresa de Transportes Tierra Grata Compañía Ltda., identificar la información crítica que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.

7.8.4. Política de registro de eventos y monitoreo de los recursos tecnológicos y los SI

La Empresa de Transportes Tierra Grata Compañía Ltda., realizará monitoreo permanente del uso que dan los funcionarios y el personal provisto por terceras partes a los recursos de la plataforma tecnológica y los SI de la empresa. Además, velará por la custodia de los registros de auditoria cumpliendo con los periodos de retención establecidos para dichos registros.

La Dirección de Tecnología y la Oficina de Riesgos definirán la realización de monitoreo de los registros de auditoria sobre los aplicativos donde se opera los procesos misionales de la empresa. El Comité de revisión de logs mensualmente se reunirá a analizar los resultados del monitoreo efectuado.

Procedimientos de registro de eventos y monitoreo de los recursos tecnológicos y los SI

Procedimientos dirigidos a: DIRECCION DE TECNOLOGIA Y OFICINA DE RIESGOS

- La Dirección de Tecnología, en conjunto con la Oficina de Riesgos, debe determinar los eventos que generarán registros de auditoría en los recursos tecnológicos y los SI de la Empresa de Transportes Tierra Grata Compañía Ltda.,
- La Dirección de Tecnología y la Oficina de Riesgos, a través del Comité de revisión de logs, deben definir de manera mensual cuáles monitoreos se realizarán de los registros de auditoria sobre los aplicativos donde se opera los procesos misionales de la empresa. Así mismo, se deben reunir para analizar los resultados de cada monitoreo efectuado.
- La Dirección de Tecnología, a través de sus funcionarios, debe habilitar los registros de auditoría y sistemas de monitoreo de la plataforma tecnológica administrada, acorde con los eventos a auditar establecidos.

- La Dirección de Tecnología debe certificar la integridad y disponibilidad de los registros de auditoria generados en la plataforma tecnológica y los SI de la Empresa de Transportes Tierra Grata Compañía Ltda., Estos registros deben ser almacenados y solo deben ser accedidos por personal autorizado.

Procedimientos dirigidos a: OFICINA DE CONTROL INTERNO

- La Oficina de Control Interno debe determinar los periodos de retención de los registros (logs) de auditoria de los recursos tecnológicos y los SI de la empresa.
- La Oficina de Control Interno debe revisar periódicamente los registros de auditoria de la plataforma tecnológica y los SI con el fin de identificar brechas de seguridad y otras actividades propias del monitoreo.

Procedimientos dirigidos a: DESARROLLADORES (INTERNOS Y EXTERNOS)

- Los desarrolladores deben generar registros (logs) de auditoría de las actividades realizadas por los usuarios finales y administradores en los SI desarrollados. Se deben utilizar controles de integridad sobre dichos registros.
- Los desarrolladores deben registrar en los logs de auditoría eventos como: fallas de validación, intentos de autenticación fallidos y exitosos, fallas en los controles de acceso, intento de evasión de controles, excepciones de los sistemas, funciones administrativas y cambios de configuración de seguridad, entre otros, de acuerdo con las directrices establecidas por la Dirección de Tecnología y la Oficina de Riesgos.
- Los desarrolladores deben evitar almacenar datos innecesarios de los sistemas construidos en los logs de auditoria que brinden información adicional a la estrictamente requerida.

7.8.5. Política de control al software operativo

La Empresa de Transportes Tierra Grata Compañía Ltda.,, a través de la Dirección de Tecnología, designará responsables y establecerá procedimientos para controlar la instalación de software operativo, se cerciorará de contar con el soporte de los proveedores de dicho software y asegurará la funcionalidad de los SI que operan sobre la plataforma tecnológica cuando el software operativo es actualizado.

Procedimientos de control al software operativo

Procedimientos dirigidos a: DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología debe establecer responsabilidades y procedimientos para controlar la instalación del software operativo, que interactúen con el procedimiento de control de cambios existente en la empresa.
- La Dirección de Tecnología debe asegurarse que el software operativo instalado en la plataforma tecnológica de la Empresa de Transportes Tierra Grata Compañía Ltda., cuenta con soporte de los proveedores.
- La Dirección de Tecnología debe conceder accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones.
- La Dirección de Tecnología debe validar los riesgos que genera la migración hacia nuevas versiones del software operativo. Se debe asegurar el correcto funcionamiento de SI y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software operativo es actualizado.
- La Dirección de Tecnología debe establecer las restricciones y limitaciones para la instalación de software operativo en los equipos de cómputo de la empresa.

7.8.6. Política de gestión de vulnerabilidades

La Empresa de Transportes Tierra Grata Compañía Ltda.,, a través de la Dirección de Tecnología y la Oficina de Riesgos, revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de la realización periódica de pruebas de vulnerabilidades, con el objetivo de realizar la corrección sobre los hallazgos arrojados por dichas pruebas. Estas dos áreas conforman en Comité de vulnerabilidades encargado de revisar, valorar y gestionar las vulnerabilidades técnicas encontradas.

Procedimientos para la gestión de vulnerabilidades

Procedimientos dirigidos a: OFICINA DE RIESGOS

- La Oficina de Riesgos debe adelantar los trámites correspondientes para la realización de pruebas de vulnerabilidades y hacking ético con una periodicidad establecida, por un ente independiente al área objeto de las pruebas, con el fin de garantizar la objetividad del desarrollo de las mismas.

- La Oficina de Riesgos debe generar los lineamientos y recomendaciones para la mitigación de vulnerabilidades, resultado de las pruebas de vulnerabilidades y hacking ético.

Procedimientos dirigidos a: DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología debe revisar periódicamente la aparición de nuevas vulnerabilidades técnicas y reportarlas a los administradores de la plataforma tecnológica y los desarrolladores de los SI, con el fin de prevenir la exposición al riesgo de estos.
- La Dirección de Tecnología, a través de sus funcionarios, debe generar y ejecutar o monitorear planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica.

Procedimientos dirigidos a: DIRECCION DE TECNOLOGIA Y OFICINA DE RIESGOS

- La Dirección de Tecnología y la Oficina de Riesgos, a través del Comité de vulnerabilidades, deben revisar, valorar y gestionar las vulnerabilidades técnicas encontradas, apoyándose en herramientas tecnológicas para su identificación.

7.9. POLÍTICAS DE SEGURIDAD EN LAS COMUNICACIONES

7.9.1. Política de gestión y aseguramiento de las redes de datos

La Empresa de Transportes Tierra Grata Compañía Ltda., establecerá, a través de la Dirección de Tecnología, los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas; así mismo, velará por que se cuente con los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos.

De igual manera, propenderá por el aseguramiento de las redes de datos, el control del tráfico en dichas redes y la protección de la información reservada y restringida de la empresa.

Procedimientos de gestión y aseguramiento de las redes de datos

Procedimientos dirigidos a: DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología debe adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red de la Empresa de Transportes Tierra Grata Compañía Ltda.,
- La Dirección de Tecnología debe implantar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.
- La Dirección de Tecnología debe mantener las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier otra tipificación que se considere conveniente para la empresa.
- La Dirección de Tecnología debe identificar los mecanismos de seguridad y los niveles de servicio de red requeridos e incluirlos en los acuerdos de servicios de red, cuando estos se contraten externamente.
- La Dirección de Tecnología debe establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red de la plataforma tecnológica de la empresa, acogiendo buenas prácticas de configuración segura.
- La Dirección de Tecnología, a través de sus funcionarios, debe identificar, justificar y documentar los servicios, protocolos y puertos permitidos por la empresa en sus redes de datos e inhabilitar o eliminar el resto de los servicios, protocolos y puertos.
- La Dirección de Tecnología debe instalar protección entre las redes internas de la Empresa de Transportes Tierra Grata Compañía Ltda., y cualquier red externa, que este fuera de la capacidad de control y administración de la empresa.
- La Dirección de Tecnología debe velar por la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos de la Empresa de Transportes Tierra Grata Compañía Ltda.,

7.9.2. Política de uso del correo electrónico

La Empresa de Transportes Tierra Grata Compañía Ltda.,, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre funcionarios y terceras partes, proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

Procedimientos de uso del correo electrónico

Procedimientos dirigidos a: DIRECCION DE TECNOLOGIA Y OFICINA DE RIESGOS

- La Dirección de Tecnología debe generar y divulgar un procedimiento para la administración de cuentas de correo electrónico.
- La Dirección de Tecnología debe diseñar y divulgar las directrices técnicas para el uso de los servicios de correo electrónico.
- La Dirección de Tecnología debe proveer un ambiente seguro y controlado para el funcionamiento de la plataforma de correo electrónico.
- La Dirección de Tecnología debe establecer procedimientos e implantar controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes.
- La Dirección de Tecnología, con el apoyo de la Oficina de Riesgos, debe generar campañas para concientizar tanto a los funcionarios internos, como al personal provisto por terceras partes, respecto a las precauciones que deben adoptar en el intercambio de información sensible por medio del correo electrónico.

Procedimientos dirigidos a: TODOS LOS USUARIOS

- La cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún funcionario de la empresa o provisto por un tercero, bajo ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya.
- Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada usuario en apoyo al objetivo misional de la Empresa de Transportes Tierra Grata Compañía Ltda., El correo institucional no debe ser utilizado para actividades personales.
- Los mensajes y la información contenida en los buzones de correo son propiedad de la Empresa de Transportes Tierra Grata Compañía Ltda., y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.
- Los usuarios de correo electrónico institucional tienen prohibido el envió de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los funcionarios de la empresa y el personal provisto por terceras partes.
- No es permitido el envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.
- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por la Empresa de Transportes Tierra Grata Compañía Ltda., y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

7.9.3. Política de uso adecuado de internet

La Empresa de Transportes Tierra Grata Compañía Ltda., consciente de la importancia de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la empresa.

Procedimientos de uso adecuado de internet

Procedimientos dirigidos a: DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.
- La Dirección de Tecnología debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.
- La Dirección de Tecnología debe monitorear continuamente el canal o canales del servicio de Internet.
- La Dirección de Tecnología debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.
- La Dirección de Tecnología debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de Internet.

Procedimientos dirigidos a: OFICINA DE RIESGOS

- La Oficina de Riesgos debe generar campañas para concientizar tanto a los funcionarios internos, como al personal provisto por terceras partes, respecto a las precauciones que deben tener en cuenta cuando utilicen el servicio de Internet.

Procedimientos dirigidos a: TODOS LOS USUARIOS

- Los usuarios del servicio de Internet de la Empresa de Transportes Tierra Grata Compañía Ltda., Deben hacer uso del mismo en relación con las actividades laborales que así lo requieran.
- Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.
- No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.
- Los usuarios del servicio de internet tienen prohibido el acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Kazaa, MSN, Yahoo, Sype, Net2phome y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del negocio de la Empresa de Transportes Tierra Grata Compañía Ltda.
- No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el jefe respectivo y la Dirección de Tecnología, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.
- No está permitido el intercambio no autorizado de información de propiedad de la Empresa de Transportes Tierra Grata Compañía Ltda., de sus clientes y/o de sus funcionarios, con terceros.

7.9.4. Política de intercambio de información

La Empresa de Transportes Tierra Grata Compañía Ltda.,, asegurará la protección de la información en el momento de ser transferida o intercambiada con otras entidades y establecerá los procedimientos y controles necesarios para el intercambio de información; así mismo, se establecerán Acuerdos de Confidencialidad y/o de Intercambio de Información con las terceras partes con quienes se realice dicho intercambio. La empresa propenderá por el uso de tecnologías informáticas y de telecomunicaciones para llevar a cabo el intercambio de información; sin embargo, establecerá directrices para el intercambio de información en medio físico.

Procedimientos de intercambio de información

Procedimientos dirigidos a: SECRETARIA GENERAL – GRUPO DE CONTRATACION

- El Grupo de Contratación, en acompañamiento con la Oficina de Riesgos, debe definir los modelos de Acuerdos de Confidencialidad y/o de Intercambio de Información entre la empresa y terceras partes incluyendo los compromisos adquiridos y las penalidades civiles o penales por el incumplimiento de dichos acuerdos. Entre los aspectos a considerar se debe incluir la prohibición de divulgar la información entregada por La Empresa de Transportes Tierra Grata Compañía Ltda., a los terceros con quienes se establecen estos acuerdos y la destrucción de dicha información una vez cumpla su cometido.
- El Grupo de Contratación debe establecer en los contratos que se establezcan con terceras partes, los Acuerdos de Confidencialidad o Acuerdos de intercambio dejando explícitas las responsabilidades y obligaciones legales asignadas a dichos terceros por la divulgación no autorizada de información de beneficiarios de la empresa que les ha sido entregada en razón del cumplimiento de los objetivos misionales de la Empresa de Transportes Tierra Grata Compañía Ltda.

Procedimientos dirigidos a: OFICINA DE RIESGOS

- La Oficina de Riesgos debe definir y establecer el procedimiento de intercambio de información con los diferentes terceros que, hacen parte de la operación de la Empresa de Transportes Tierra Grata Compañía Ltda., reciben o envían información de los beneficiarios de la empresa, que contemple la utilización de medios de transmisión confiables y la adopción de controles, con el fin de proteger la confidencialidad e integridad de la misma.
- La Oficina de Riesgos debe velar porque el intercambio de información de la Empresa de Transportes Tierra Grata Compañía Ltda., con entidades externas se realice en cumplimiento de las Políticas de seguridad para el intercambio de información aquí descritas, los Acuerdos de Intercambio de Información y el procedimiento definido para dicho intercambio de información.
- La Oficina de Riesgos debe autorizar el establecimiento del vínculo de transmisión de información con terceras partes, para que posteriormente las áreas funcionales realicen las actividades de transmisión requeridas en cada caso.

Procedimientos dirigidos a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACION

- Los propietarios de los activos de información deben velar porque la información de la Empresa de Transportes Tierra Grata Compañía Ltda., o de sus beneficiarios sea protegida de divulgación no autorizada por parte de los terceros a quienes se entrega esta información, verificando el cumplimiento de las cláusulas relacionadas en los contratos, Acuerdos de confidencialidad o Acuerdos de intercambio establecidos.
- Los propietarios de los activos de información deben asegurar que los datos requeridos de los beneficiarios sólo puedan ser entregada a terceros, previo consentimiento de los titulares de los mismos, salvo en los casos que lo disponga una ley o sea una solicitud de los entes de control.
- Los propietarios de los activos de información, o a quien ellos deleguen, deben verificar que el intercambio de información con terceros deje registro del tipo de información intercambiada, el emisor y receptor de la misma y la fecha de entrega/recepción.
- Los propietarios de los activos de información deben autorizar los requerimientos de solicitud/envío de información de la Empresa de Transportes Tierra Grata Compañía Ltda., por/a terceras partes, salvo que se trate de solicitudes de entes de control o de cumplimiento de la legislación vigente.
- Los propietarios de los activos de información deben asegurarse que el Intercambio de información (digital) solamente se realice si se encuentra autorizada y dando cumplimiento a las Políticas de administración de redes, de acceso lógico y de protección de datos personales de la Empresa de Transportes Tierra Grata Compañía Ltda., así como del procedimiento de intercambio de información.
- Los propietarios de los activos de información deben verificar la destrucción de la información suministrada a los terceros, realizada por ellos una vez esta ha cumplido el cometido por el cual fue enviada.

Procedimientos dirigidos a: SECRETARIA GENERAL – COORDINACION DE CORRESPONDENCIA

- La Coordinación de Correspondencia debe acoger el procedimiento para el intercambio, de información (medios de almacenamiento y documentos) con terceras partes y la adopción de controles a fin de proteger la información sensible contra divulgación, pérdida o modificaciones.
- La Coordinación de Correspondencia debe certificar que todo envió de información física a terceros (documento o medio magnético) utilice únicamente los servicios de transporte o servicios de mensajería autorizados por La Empresa de Transportes Tierra Grata Compañía Ltda., y que estos permitan ejecutar rastreo de las entregas.

Procedimientos dirigidos a: DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología debe ofrecer servicios o herramientas de intercambio de información seguros, así como adoptar controles como el cifrado de información, que permitan el cumplimiento del procedimiento para el intercambio de información (digital o medio magnético), con el fin de proteger dicha información contra divulgación o modificaciones no autorizadas.

Procedimientos dirigidos a: TERCEROS CON QUIENES SE INTERCAMBIA INFORMACION de la Empresa de Transportes Tierra Grata Compañía Ltda.,

- Los terceros con quienes se intercambia información de la Empresa de Transportes Tierra Grata Compañía Ltda., deben darle manejo adecuado a la información recibida, en cumplimiento de las Políticas de seguridad de la empresa, de las condiciones contractuales establecidas y del Procedimiento de intercambio de información.
- Los terceros con quienes se intercambia información de la empresa deben destruir de manera segura la información suministrada, una vez esta cumpla con la función para la cual fue enviada y demostrar la realización de las actividades de destrucción.

Procedimientos dirigidos a: TODOS LOS USUARIOS:

- Los usuarios no deben utilizar el correo electrónico como medio para enviar o recibir información sensible de la EMPRESA o de sus beneficiarios.
- No está permitido el intercambio de información sensible de la empresa por vía telefónica.

7.10. POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SI

7.10.1. Política para el establecimiento de requisitos de seguridad

La Empresa de Transportes Tierra Grata Compañía Ltda., asegurará que el software adquirido y desarrollado tanto al interior de la empresa, como por terceras partes, cumplirá con los requisitos de seguridad y calidad establecidos por él. Las áreas propietarias de SI, la Dirección de Tecnología y la Oficina de Riesgos incluirán requisitos de seguridad en la definición de requerimientos y, posteriormente se asegurarán que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido.

Procedimientos para el establecimiento de requisitos de seguridad

Procedimientos dirigidos a: PROPIETARIOS DE LOS SI, DIRECCION DE TECNOLOGIA Y OFICINA DE RIESGOS

- Todos los SI o desarrollos de software deben tener un área propietaria dentro de la EMPRESA formalmente asignada.
- La Dirección de Tecnología debe establecer metodologías para el desarrollo de software, que incluyan la definición de requerimientos de seguridad y las buenas prácticas de desarrollo seguro, con el fin de proporcionar a los desarrolladores una visión clara de lo que se espera.
- Las áreas propietarias de los SI, en acompañamiento con la Dirección de Tecnología y la Oficina de Riesgos deben establecer las especificaciones de adquisición o desarrollo de SI, considerando requerimientos de seguridad de la información.
- Las áreas propietarias de los SI deben definir qué información sensible puede ser eliminada de sus sistemas y solicitar que estos soporten la eliminación de dicha información, como es el caso de los datos personales o financieros, cuando estos ya no son requeridos.
- La Oficina de Riesgos debe liderar la definición de requerimientos de seguridad de los SI, teniendo en cuenta aspectos como la estandarización de herramientas de desarrollo, controles de autenticación, controles de acceso y arquitectura de aplicaciones, entre otros.

Procedimientos dirigidos a: DESARROLLADORES (INTERNOS O EXTERNOS)

- Los desarrolladores deben documentar los requerimientos establecidos y definir la arquitectura de software más conveniente para cada sistema de información que se quiera desarrollar, de acuerdo con los requerimientos de seguridad y los controles deseados.

- Los desarrolladores deben certificar que todo sistema de información adquirido o desarrollado utilice herramientas de desarrollo licenciadas y reconocidas en el mercado.
- Los desarrolladores deben deshabilitar las funcionalidades de completar automáticamente en formularios de solicitud de datos que requieran información sensible.
- Los desarrolladores deben establecer el tiempo de duración de las sesiones activas de las aplicaciones, terminándolas una vez se cumpla este tiempo.
- Los desarrolladores deben asegurar que no se permitan conexiones recurrentes a los SI construidos con el mismo usuario.
- Los desarrolladores deben utilizar usar los protocolos sugeridos por la Dirección de Tecnología y la Oficina de Riesgos en los aplicativos desarrollados.
- Los desarrolladores deben certificar la transmisión de información relacionada con pagos o transacciones en línea a los operadores encargados, por medio de canales seguros.

7.10.2. Política de desarrollo seguro, realización de pruebas y soporte de los sistemas

La Empresa de Transportes Tierra Grata Compañía Ltda., velará porque el desarrollo interno o externo de los SI cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, se asegurará que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido por la empresa.

Procedimientos de desarrollo seguro, realización de pruebas y soporte de los sistemas

Procedimientos dirigidos a: PROPIETARIOS DE LOS SI

- Los propietarios de los SI son responsables de realizar las pruebas para asegurar que cumplen con los requerimientos de seguridad establecidos antes del paso a producción de los sistemas, utilizando metodologías establecidas para este fin, documentado las pruebas realizadas y aprobando los pasos a producción. Estas pruebas deben realizarse por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica en la cual funcionan los aplicativos.

- Los propietarios de los SI deben aprobar las migraciones entre los ambientes de desarrollo, pruebas y producción de SI nuevos y/o de cambios o nuevas funcionalidades.

Procedimientos dirigidos a: DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología debe implantar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.
- La Dirección de Tecnología debe contar con sistemas de control de versiones para administrar los cambios de los SI de la Empresa de Transportes Tierra Grata Compañía Ltda.,
- La Dirección de Tecnología debe asegurase que los SI adquiridos o desarrollados por terceros, cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.
- La Dirección de Tecnología debe generar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.
- La Dirección de Tecnología, a través de sus funcionarios, se debe asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.
- La Dirección de Tecnología debe incluir dentro del procedimiento y los controles de gestión de cambios el manejo de los cambios en el software aplicativo y los SI de la empresa.

Procedimientos dirigidos a: DESARROLLADORES (INTERNOS O EXTERNOS)

- Deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el diseño hasta la puesta en marcha.
- Deben proporcionar un nivel adecuado de soporte para solucionar los problemas que se presenten en el software aplicativo de la Empresa de Transportes Tierra Grata Compañía Ltda., este soporte se debe cumplir en tiempos de respuesta aceptables.
- Deben construir los aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.

- Los desarrolladores deben asegurar que los SI construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.
- Los desarrolladores deben suministrar opciones de desconexión o cierre de sesión de los aplicativos (logout) que permitan terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.
- Los desarrolladores deben asegurar el manejo de operaciones sensibles o críticas en los aplicativos desarrollados permitiendo el uso de dispositivos adicionales como tokens o el ingreso de parámetros adicionales de verificación.
- Los desarrolladores deben asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.
- Los desarrolladores deben garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.
- Los desarrolladores deben remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.
- Los desarrolladores deben prevenir la revelación de la estructura de directorios de los SI construidos.
- Los desarrolladores deben remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.
- Los desarrolladores deben evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales se recomienda que estén cifrados.
- Los desarrolladores deben certificar el cierre de la conexión a las bases de datos desde los aplicativos tan pronto como estas no sean requeridas.
- Los desarrolladores deben desarrollar los controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos solo tengan privilegios de lectura.
- Los desarrolladores deben proteger el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.
- Los desarrolladores deben asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

Procedimientos dirigidos a: OFICINA DE RIESGOS

- La Oficina de Riesgos debe verificar que las pruebas de seguridad sobre los SI se realicen de acuerdo con las metodologías definidas, contando con pruebas debidamente documentadas.

7.10.3. Política para la protección de los datos de prueba

La Dirección de Tecnología de la Empresa de Transportes Tierra Grata Compañía Ltda., Protegerá los datos de prueba que se entregarán a los desarrolladores, asegurando que no revelan información confidencial de los ambientes de producción.

Procedimientos para la protección de los datos de prueba

Procedimientos dirigidos a: DIRECCION DE TECNOLOGIA

- La Dirección de Tecnología debe certificar que la información a ser entregada a los desarrolladores para sus pruebas será enmascarada y no revelará información confidencial de los ambientes de producción.
- La Dirección de Tecnología debe eliminar la información de los ambientes de pruebas, una vez estas han concluido.

7.11. POLÍTICAS QUE RIGEN DE LA RELACION CON TERCERAS PARTES

7.11.1. Política de inclusión de condiciones de seguridad en la relación con terceras partes

La Empresa de Transportes Tierra Grata Compañía Ltda., establecerá mecanismos de control en sus relaciones con terceras partes, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por las mismas, cumplan con las políticas, Procedimientos y procedimientos de seguridad de la información.

Los funcionarios responsables de la realización y/o firma de contratos o convenios con terceras partes se asegurarán de la divulgación de las políticas, Procedimientos y procedimientos de seguridad de la información a dichas partes.

Procedimientos de inclusión de condiciones de seguridad en la relación con terceras partes

Procedimientos dirigidos a: DIRECCION DE TECNOLOGIA, OFICINA ASESORA JURIDICA Y OFICINA DE RIESGOS

- La Dirección de Tecnología, la Oficina Asesora Jurídica y la Oficina de Riesgos deben generar un modelo base para los Acuerdos de Niveles de Servicio y requisitos de Seguridad de la Información, con los que deben cumplir terceras partes o proveedores de servicios; dicho modelo, debe ser divulgado a todas las áreas que adquieran o supervisen recursos y/o servicios tecnológicos.
- La Dirección de Tecnología, la Oficina Asesora Jurídica y la Oficina de Riesgos deben elaborar modelos de Acuerdos de Confidencialidad y Acuerdos de Intercambio de Información con terceras partes. De dichos acuerdos deberá derivarse una responsabilidad tanto civil como penal para la tercera parte contratada.

Procedimientos dirigidos a: DIRECCIÓN DE TECNOLOGIA

- La Dirección de Tecnología debe establecer las condiciones de conexión adecuada para los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la empresa.
- La Dirección de Tecnología debe establecer las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.
- La Dirección de Tecnología debe mitigar los riesgos relacionados con terceras partes que tengan acceso a los SI y la plataforma tecnológica de la Empresa de Transportes Tierra Grata Compañía Ltda.,

Procedimientos dirigidos a: OFICINA DE RIESGOS

- La Oficina de Riesgos debe evaluar y aprobar los accesos a la información de la EMPRESA requeridos por terceras partes.

- La Oficina de Riesgos debe identificar y monitorear los riesgos relacionados con terceras partes o los servicios provistos por ellas, haciendo extensiva esta actividad a la cadena de suministro de los servicios de tecnología o comunicaciones provistos.

Procedimientos dirigidos a: SUPERVISORES DE CONTRATOS CON TERCEROS

- Los Supervisores de contratos con terceros deben divulgar las políticas, Procedimientos y procedimientos de seguridad de la información de la Empresa de Transportes Tierra Grata Compañía Ltda., a dichos terceros, así como velar porque el acceso a la información y a los recursos de almacenamiento o procesamiento de la misma, por parte de los terceros se realice de manera segura, de acuerdo con las políticas, Procedimientos y procedimientos de seguridad de la información.

7.11.2. Política de gestión de la prestación de servicios de terceras partes

La Empresa de Transportes Tierra Grata Compañía Ltda., propenderá por mantener los niveles acordados de seguridad de la información y de prestación de los servicios de los proveedores, en concordancia con los acuerdos establecidos con estos. Así mismo, velará por la adecuada gestión de cambios en la prestación de servicios de dichos proveedores.

Procedimientos de gestión de la prestación de servicios de terceras partes

Procedimientos dirigidos a: DIRECCION DE TECNOLOGIA Y OFICINA DE RIESGOS

- La Dirección de Tecnología debe verificar en el momento de la conexión y, cuando se considere pertinente, el cumplimiento de las condiciones de conexión de los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la empresa.
- La Gerencia de Tecnologías de la Información y la Oficina de Riesgos deben verificar las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.

Procedimientos dirigidos a: OFICINA DE RIESGOS Y SUPERVISORES DE CONTRATOS CON TERCEROS

- La Oficina de Riesgos y los Supervisores de contratos con terceros deben monitorear periódicamente, el cumplimiento de los Acuerdos de Niveles de Servicio, Acuerdos de Confidencialidad, Acuerdos de Intercambio de información y los requisitos de Seguridad de la Información de parte de los terceros proveedores de servicios.
- Los Supervisores de contratos con terceros, con el apoyo de la Oficina de Riesgos, deben administrar los cambios en el suministro de servicios por parte de los proveedores, manteniendo los niveles de cumplimiento de servicio y seguridad establecidos con ellos y monitoreando la aparición de nuevos riesgos.

7.12. POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD

7.12.1. Política para el reporte y tratamiento de incidentes de seguridad

La Empresa de Transportes Tierra Grata Compañía Ltda., promoverá entre los funcionarios y personal provisto por terceras partes el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como la plataforma tecnológica, los SI, los medios físicos de almacenamiento y las personas.

De igual manera, asignará responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad.

La Alta Dirección o a quien delegue, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas.

Procedimientos para el reporte y tratamiento de incidentes de seguridad

Procedimientos dirigidos a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

- Los propietarios de los activos de información deben informar a la Oficina de Riesgos, los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización.

Procedimientos dirigidos a: OFICINA DE RIESGOS

- La Oficina de Riesgos debe establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.
- La Oficina de Riesgos debe evaluar todos los incidentes de seguridad de acuerdo a sus circunstancias particulares y escalar al Comité de Seguridad de la Información aquellos en los que se considere pertinente.
- La Oficina de Riesgos debe designar personal calificado, para investigar adecuadamente los incidentes de seguridad reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo su re- ocurrencia.
- La Oficina de Riesgos debe, con el apoyo con la Dirección de Tecnología y la Secretaría General, crear bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento.

Procedimientos dirigidos a: COMITÉ DE SEGURIDAD DE LA INFORMACION

- El Comité de Seguridad de la Información debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.

Procedimientos dirigidos a: TODOS LOS USUARIOS

- Es responsabilidad de los funcionarios de la Empresa de Transportes Tierra Grata Compañía Ltda., y del personal provisto por terceras partes reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos con la mayor prontitud posible.
- En caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno, reservada o restringida, los funcionarios deben notificarlo a la Oficina de Riesgo para que se registre y se le dé el trámite necesario.

7.13. POLÍTICAS DE INCLUSION DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

7.13.1. Política de continuidad, contingencia, recuperación y retorno a la normalidad con consideraciones de seguridad de la información

La Empresa de Transportes Tierra Grata Compañía Ltda., proporcionará los recursos suficientes para proporcionar una respuesta efectiva de funcionarios y procesos en caso de contingencia o eventos catastróficos que se presenten en la empresa y que afecten la continuidad de su operación.

Además, responderá de manera efectiva ante eventos catastróficos según la magnitud y el grado de afectación de los mismos; se restablecerán las operaciones con el menor costo y pérdidas posibles, manteniendo la seguridad de la información durante dichos eventos. La Empresa de Transportes Tierra Grata Compañía Ltda., mantendrá canales de comunicación adecuados hacia funcionarios, proveedores y terceras partes interesadas.

Procedimientos de continuidad, contingencia, recuperación y retorno a la normalidad con consideraciones de seguridad de la información

Procedimientos dirigidos a: OFICINA DE RIESGOS

- La Oficina de Riesgos, debe reconocer las situaciones que serán identificadas como emergencia o desastre para la empresa, los procesos o las áreas y determinar cómo se debe actuar sobre las mismas.
- La Oficina de Riesgos, debe liderar los temas relacionados con la continuidad del negocio y la recuperación ante desastres
- La Oficina de Riesgos debe realizar los análisis de impacto al negocio y los análisis de riesgos de continuidad para, posteriormente proponer posibles estrategias de recuperación en caso de activarse el plan de contingencia o continuidad, con las consideraciones de seguridad de la información a que haya lugar.
- La Oficina de Riesgos debe seleccionar las estrategias de recuperación más convenientes para la empresa.
- La Oficina de Riesgos debe validar que los procedimientos de contingencia, recuperación y retorno a la normalidad incluyan consideraciones de seguridad de la información.

- La Oficina de Riesgos, deben asegurar la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de negocio, verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.

Procedimientos dirigidos a: DIRECCION DE TECNOLOGIA Y OFICINA DE RIESGOS

- La Oficina de Riesgos, en conjunto con la Dirección de Tecnología, deben elaborar un plan de recuperación ante desastres para el centro de cómputo y un conjunto de procedimientos de contingencia, recuperación y retorno a la normalidad para cada uno de los servicios y sistemas prestados.
- La Dirección de Tecnología y la Oficina de Riesgos deben participar activamente en las pruebas de recuperación ante desastres.

Procedimientos dirigidos a: VICEPRESIDENTES, DIRECTORES Y JEFES DE OFICINA

- Los Vicepresidentes, Directores y Jefes de Oficina deben identificar y, al interior de sus áreas, generar la documentación de los procedimientos de continuidad que podrían ser utilizados en caso de un evento adverso, teniendo en cuenta la seguridad de la información. Estos documentos deben ser probados para certificar su efectividad.

7.13.2. Política de redundancia

La Empresa de Transportes Tierra Grata Compañía Ltda., propenderá por la existencia de una plataforma tecnológica redundante que satisfaga los requerimientos de disponibilidad aceptables para la empresa.

Procedimientos de redundancia

Procedimientos dirigidos a: DIRECCION DE TECNOLOGIA Y OFICINA DE RIESGOS

- La Dirección de Tecnología y la Oficina de Riesgos deben analizar y establecer los requerimientos de redundancia para los SI críticos para la empresa y la plataforma tecnológica que los apoya.

- La Dirección de Tecnología y debe evaluar y probar soluciones de redundancia tecnológica y seleccionar la solución que mejor cumple los requerimientos de la Empresa de Transportes Tierra Grata Compañía Ltda.,
- La Dirección de Tecnología, a través de sus funcionarios, debe administrar las soluciones de redundancia tecnológica y realizar pruebas periódicas sobre dichas soluciones, para asegurar el cumplimiento de los requerimientos de disponibilidad de la empresa.

7.14. POLÍTICAS DE CUMPLIMIENTO

7.14.1. Política de cumplimiento con requisitos legales y contractuales

La Empresa de Transportes Tierra Grata Compañía Ltda., velará por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información, entre ella la referente a derechos de autor y propiedad intelectual, razón por la cual propenderá porque el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.

Procedimientos de cumplimiento con requisitos legales y contractuales

Procedimientos dirigidos a: OFICINA ASESORA JURIDICA Y OFICINA DE RIESGOS

- La Oficina Asesora Jurídica y la Oficina de Riesgos deben identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a la empresa y relacionados con seguridad de la información.

Procedimientos dirigidos a: DIRECCIÓN DE TECNOLOGIA

- La Dirección de Tecnología debe certificar que todo el software que se ejecuta en la EMPRESA esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso.
- La Dirección de Tecnología debe establecer un inventario con el software y SI que se encuentran permitidos en las estaciones de trabajo o equipos móviles de la EMPRESA para el desarrollo de las actividades laborales, así como verificar periódicamente que el software instalado en dichas estaciones de trabajo o equipos móviles corresponda únicamente al permitido.

Procedimientos dirigidos a: TODOS LOS USUARIOS

- Los usuarios no deben instalar software o SI en sus estaciones de trabajo o equipos móviles suministrados para el desarrollo de sus actividades.
- Los usuarios deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software. Es ilegal duplicar software o su documentación sin la autorización del propietario de los derechos de autor y, su reproducción no autorizada es una violación de ley; no obstante, puede distribuirse un número de copias bajo una licencia otorgada.

7.14.2. Política de privacidad y protección de datos personales

En cumplimiento de la de Ley 1581 de 2012, por la cual se dictan disposiciones para la protección de datos personales, La Empresa de Transportes Tierra Grata Compañía Ltda., a través de la Oficina de Riesgos, propenderá por la protección de los datos personales de sus beneficiarios, proveedores y demás terceros de los cuales reciba y administre información.

Se establecerán los términos, condiciones y finalidades para las cuales La Empresa de Transportes Tierra Grata Compañía Ltda.,, como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratará la información de todas las personas que en algún momento, por razones de la actividad que desarrolla la empresa, hayan suministrado datos personales. En caso de delegar a un tercero el tratamiento de datos personales, la Empresa de Transportes Tierra Grata Compañía Ltda., exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos personales.

Así mismo, buscará proteger la privacidad de la información personal de sus funcionarios, estableciendo los controles necesarios para preservar aquella información que la empresa conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de la empresa y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización.

Procedimientos de privacidad y protección de datos personales

Procedimientos dirigidos a: AREAS QUE PROCESAN DATOS PERSONALES

- Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la empresa.
- Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben asegurar que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos.
- Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben establecer condiciones contractuales y de seguridad a las entidades vinculadas o aliadas delegadas para el tratamiento de dichos datos personales.
- Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para el intercambio de estos datos con los terceros delegados para el tratamiento de dichos datos personales.
- Las áreas que procesan datos personales de beneficiarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para enviar a los beneficiarios, proveedores u otros terceros mensajes, a través de correo electrónico y/o mensajes de texto.

Procedimientos dirigidos a: OFICINA DE RIESGOS

- La Oficina de Riesgos debe establecer los controles para el tratamiento y protección de los datos personales de los beneficiarios, funcionarios, proveedores y demás terceros de la Empresa de Transportes Tierra Grata Compañía Ltda., de los cuales reciba y administre información.

Procedimientos dirigidos a: DIRECCIÓN DE TECNOLOGIA

- La Dirección de Tecnología debe implantar los controles necesarios para proteger la información personal de los beneficiarios, funcionarios, proveedores u otras terceras partes almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida.

Procedimientos dirigidos a: TODOS LOS USUARIOS

- Los usuarios deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la empresa o de sus funcionarios de cual tengan conocimiento en el ejercicio de sus funciones.
- Es deber de los usuarios, verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por fax, por correo electrónico o por correo certificado, entre otros.

Procedimientos dirigidos a: USUARIOS DE LOS PORTALES de la Empresa de Transportes Tierra Grata Compañía Ltda.,

- Los usuarios de los portales de la Empresa de Transportes Tierra Grata Compañía Ltda., deben asumir la responsabilidad individual sobre la clave de acceso a dichos portales que les es suministrada; así mismo, deben cambiar de manera periódica esta clave de acceso.
- Los usuarios de los portales de la Empresa de Transportes Tierra Grata Compañía Ltda., deben contar con controles de seguridad en sus equipos de cómputo o redes privadas para acceder a los portales de la Empresa de Transportes Tierra Grata Compañía Ltda.,
- Los usuarios de los portales de la Empresa de Transportes Tierra Grata Compañía Ltda., deben aceptar el suministro de datos personales que pueda hacer la empresa a los terceros delegados para el tratamiento de datos personales, a entidades judiciales y demás entes del Estado que, en ejercicio de sus funciones, solicitan esta información; de igual manera, deben aceptar que pueden ser objeto de procesos de auditoria interna o externa.

Anexo L. POLÍTICAS DE SEGURIDAD DE LOS ACTIVOS DE LA INFORMACIÓN Y ALCANCES DEL SGSI PARA LA EMPRESA

POLÍTICA DE SEGURIDAD GENERAL

Todos los directivos y funcionarios se obligarán a conservar la información lo más segura posible. Se prohíbe la reproducción total o parcial de los documentos clasificados como confidenciales, sin la correspondida autorización o aprobación del ente competente, así como el deterioro adrede de los mecanismos informáticos, software, cableado de datos, suministro eléctrico, o cualquier activo de la empresa.

POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN EN GENERAL

Se utilizarán políticas y lineamientos de seguridad que obliguen a mantener la información de en un entorno seguro. Estas políticas estarán enviadas a conservar los principios de la Seguridad Informática como lo son la Confidencialidad, Integridad y Disponibilidad, así como los Planes de Continuidad del Negocio y Recuperación de Desastres.

POLÍTICA DE SEGURIDAD A LOS SERVICIOS DE LA EMPRESA

Para el acceso a los servicios de los SI de la empresa, se pedirán siempre los permisos de acceso conseguidas por la oficina de Sistemas y Telecomunicaciones, este será una única cuenta personal e intransferible. Si los datos de ingresos son perdidos, se lograrán recuperar a través del usuario del correo de la empresa.

POLÍTICA DEL DESARROLLO DE APLICACIONES

Para la contratación de software de aplicación de terceros, éste será valorado por el personal de sistemas capacitado de la empresa, para comprobar si cumple con las exigencias de la empresa y de seguridad, y de acuerdo a su valoración, se utilizará un período de pruebas no menor a 3 meses y no mayor a 6 meses.

Para el desarrollo de software de aplicación por grupos o proyectos de investigación, se comprobarán que sean bajo las herramientas de desarrollo de software, multimedia con los cuales la empresa conserva contratos de licencia. El período de evaluación y prueba efectúa con las iguales situaciones del software desarrollado por terceros.

Para el software de aplicación se necesitan las credenciales de acceso, éste realizará o implementaran para los usuarios, conexiones seguras.

POLÍTICA DE LA GESTIÓN DE RIESGO

Se utilizarán los mecanismos de gestión de riesgos y controles que se requieran para conservar el normal funcionamiento de los procesos.

POLÍTICA DE LA PROTECCIÓN DE DATOS

Se implementará un sistema de protección varios niveles para los datos e información que se recogen en las bases de datos de la empresa. Se usarán prohibiciones a nivel de usuario en base al rol y perfil.

POLÍTICA DE AUDITORÍA

Para conservar la calidad de los procesos organizativos, se crearán auditorías programadas en cada una de las dependencias y procesos críticos de la empresa.

POLÍTICA DE CALIDAD

Se comprometerá a la oficina de Sistemas y Telecomunicaciones de la empresa a realizar controles y cambios con el objetivo de mejorar continuamente sus procesos. Se ejecutarán evaluaciones periódicas para evaluar el nivel de calidad en los lugares críticos y en otras donde sea necesario.

La calidad será una situación fundamental. Se debe de cumplir con los requerimientos de gestión para poder conseguir las certificaciones de estándares internacionales, así como la formación con los sistemas de calidad históricos de la empresa.

POLÍTICA DE LOS DISPOSITIVOS TRAÍDOS POR EL USUARIO

Los funcionarios que elijan trabajar con sus equipos de uso personal, deben estar anteriormente autorizados para hacerlo, el equipo se configurará de acuerdo a las políticas de la empresa y bajo iguales condiciones que los equipos de la entidad, ya que no se aceptarán riesgos inaceptables como la difusión de software de códigos maliciosos por una falla de seguridad en el equipo. Los computadores de uso personal deben suministrar mecanismos de autenticación aprobados por la oficina de Sistemas y Telecomunicaciones.

POLÍTICA DE DISPOSITIVOS PORTABLES

En las instalaciones de la empresa los dispositivos portables en los equipos, estos estarán escaneados automáticamente por la medio de antivirus contratado. No se admitirá su ejecución si se descubre el código malicioso y no es removido de la unidad. Si no puede ser removido, se expresará una alerta para su respectivo análisis.

POLÍTICA DE LA CREACIÓN DE USUARIOS

Los usuarios de la empresa podrán ingresar a los diferentes servicios manejando un esquema de identificación personal, único e intransferible. Y este será entregado de forma automática y online en un período no máximo a las 48 horas.

POLÍTICA DE LA INSTALACIÓN DE SOFTWARE Y HARDWARE

Para la instalación del software y hardware, estos mecanismos serán exclusivamente instalados por el personal técnico capacitado. A cada equipo se le efectuará un inventario de hardware y la información será conservada en una base de datos. Se hará un chequeo de estos dispositivos cada vez que se inicie el equipo y se conecte a la red; si se descubren cambios no autorizados, quedará deshabilitado automáticamente.

POLÍTICA DE LA COMUNICACIÓN

La comunicación y la información de la empresa serán utilizando los correos electrónicos de la empresa y no de los sitios web comerciales. Se harán escaneo con software antivirus a los documentos adjuntos tanto subidos como recibidos.

RESPONSABILIDAD

Cada persona administrativa de la oficina de Sistemas y Telecomunicaciones cuidará por la seguridad de los activos informáticos que están a su cargo, así como se obligará a seguir los lineamientos pactados en este documento de una forma satisfactoria y de acuerdo al régimen contractuales.

El no proceder con responsabilidad frente a la Política de la Seguridad de la Información, será sancionado de acuerdo al código ético de la empresa.

PROCEDIMIENTOS EN INCIDENTES DE SEGURIDAD

Si la persona administrativa descubre que ha sido quebrantado un procedimiento concerniente a las Políticas de Seguridad fundadas en este documento, le corresponderá informarlo inmediatamente al líder de la oficina de Sistemas y Telecomunicaciones mediante un documento formal informando el incidente, posibles causas y fallas que podrían haberlas causado, así como las recomendaciones y/o controles para mitigarlo.

ALCANCES DEL SGSI PARA LA EMPRESA

La Empresa de Transportes Tierra Grata Compañía Ltda, necesita crear los términos de la planeación del SGSI con el fin de salvaguardar sus activos informáticos de los servicios que prestan. Por ello es importante la fase de planeación de un SGSI mediante el estándar ISO/IEC 27001:2013, teniendo en cuenta las leyes y medidas que resguardan la información

Tabla 1. Resumen De Controles de la Empresa de Transportes Tierra Grata Compañía Ltda

OBJETIVO DEL CONTROL	CONTENIDO DEL CONTROL
Política de seguridad de información	
Documentar política de seguridad de información	La gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes.
Revisión de la política de seguridad de la información	La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad.
Organización de la seguridad de la información	
Compromiso de la gerencia con la seguridad de la información	La gerencia debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconocimiento de las responsabilidades de la seguridad de la información.
Coordinación de la seguridad de Información	Las actividades de seguridad de la información deben ser coordinadas por representantes de las diferentes partes de la organización con las funciones y roles laborales relevantes.
Asignación de responsabilidades de la seguridad de la información	Se deben definir claramente las responsabilidades de la seguridad de la información.
Acuerdos de confidencialidad	Se deben identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no-divulgación reflejando las necesidades de la organización para la protección de la información.
Gestión de activos	
Inventarios de activos	Todos los activos deben estar claramente identificados; y se debe elaborar y mantener un inventario de todos los activos
Uso aceptable de los activos	Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información.
Seguridad de los recursos humanos	
Roles y responsabilidades	Se deben definir y documentar los roles y responsabilidades de seguridad de los empleados, contratistas y terceros en concordancia con la política de la seguridad de información de la organización.
Seguridad física y ambiental	

OBJETIVO DEL CONTROL	CONTENIDO DEL CONTROL
Perímetro de seguridad física	Se debe utilizar perímetros de seguridad (barreras tales como paredes y puertas de ingreso controlado o recepcionistas) para proteger áreas que contienen información y medios de procesamiento de información.
Seguridad oficinas	Se debe diseñar y aplicar seguridad física en las oficinas, habitaciones y medios.
Seguridad de computadores	
Ubicación protección equipo	El equipo debe estar ubicado o protegido para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.
Seguridad en el cableado	El cableado de la energía y las telecomunicaciones que llevan data o sostienen los servicios de información deben ser protegidos de la intercepción o daño.
Mantenimiento de equipo	El equipo debe ser mantenido correctamente para permitir su continua disponibilidad e integridad.
Protección contra software malicioso	
Controles contra software malicioso	Se deben implementar controles de detección, prevención y recuperación para protegerse de códigos malicioso y se deben implementar procedimientos de conciencia apropiados.
Copias de seguridad o backup (respaldo de información)	Se deben realizar copias de back-up o respaldo de la información comercial y software esencial y se deben probar regularmente de acuerdo a la política.
Gestión de seguridad de redes	
Controles de red	Las redes deben ser adecuadamente manejadas y controladas para poderlas proteger de amenazas, y para mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito.
Seguridad de los servicios de red	Se deben identificar los dispositivos de seguridad, niveles de servicio y los requerimientos e incluirlos en cualquier contrato de servicio de red, ya sea que estos servicios sean provistos en-casa o sean abastecidos externamente.
Protección contra software malicioso	
Política de control de acceso	Se debe establecer, documentar y revisar la política de control de acceso.
Gestión de privilegios	Se debe restringir y controlar la asignación y uso de los privilegios.
Gestión de la clave del usuario	La asignación de claves se debe controlar a través de un proceso de gestión formal.
Control de acceso a redes	Los usuarios sólo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.

Fuente: Autor

Tabla 2. Sistema de Control

Tipo de activo	Riesgos	Sistema de control
Hardware	R1. Robo de equipos de cómputo	• Restringir el acceso al personal fuera de la dependencia. • Instalar cámaras de seguridad, para identificar y disminuir los robos. • Contratar vigilancia a la organizacion. • Establecer política de seguridad, al ingreso de la oficina. • Implementar o redefinir la matriz de control de acceso.
	R2. Mal funcionamiento de los equipos y servicios.	• Definir un plan semestral de mantenimiento preventivo
	R3. Interface e Información	• Procedimiento formal de alta y baja de usuarios con objeto de garantizar y cancelar los accesos a todos los sistemas y servicios de información. • restringir y controlar la asignación y uso de los privilegios. • controlar la asignación de contraseñas mediante un proceso de gestión • revisar con regularidad los derechos de acceso de los usuarios, siguiendo un procedimiento formal.
Software	R4. Intrusión no autorizada en los equipos.	• Cifrar la base de datos y la información transferida. • Realizar una buena configuración del servidor web. • Realizar copias de seguridad de la base de datos. • Validar la asignación de claves robustas. • Capacitación del usuario al responder un correo no deseado. • Requerir SSL para todas las páginas sensibles • Crear atributo (secure) en todas las cookies sensibles. • Configuración en forma adecuada los Routers y el Firewalls • Realizar filtros de IP a paquetes procedentes de IP's autorizadas. • Configuración adecuada de puertos y deshabilitar los que no se utilicen. • Realizar la securización de la red de datos Configurar el servidor SSL para que acepte únicamente algoritmos considerados fuertes. • Implementar o redefinir la matriz de control de acceso. • Control permanente y verificación a las actualizaciones y parches de seguridad. • Configurar archivos logs de transacciones para las diferentes aplicaciones
	R5. Modificación, borrado o robo de información privilegiada	
	R6. Ataques de DoS, Malware y procesamiento	
	R7. Modificación y robo de identidades.	
	R8. Suplantación de Ip, dominio, páginas web.	
	R.9. Adecuacion y mantenimiento	

Tipo de activo	Riesgos	Sistema de control
		• Solicitar periódicamente auditoria a las diferentes áreas (Bases de Datos, Comunicaciones, Seguridad, etc.) • Restringir el acceso con rango de IP
Redes	R10. Disponibilidad de los servicios.	• Monitoreo continuo a las actividades propias de la red. • Configuraciones seguras para dispositivos de red. • Establecer mecanismos de defensa perimetral como Proxy, redes DMZ, sistemas de prevención de intrusos (IPS), firewalls. • Monitorización y análisis de registros de auditoría. • Acceso controlado a los recursos de red.
Seguridad Fisica	R11. Perdida de información, equipos o partes asociadas a su gestión.	• Realizar copia de seguridad de los datos guardados en el PC, en un lugar diferente a este. • Establecer políticas para la copia de seguridad. • Prohibir el acceso de personal ajeno a la oficina. • Definir el personal encargado de las copias de seguridad
	R12. Fallo eléctrico - corto circuito	
	R13. Incursión a instalaciones	
Seguridad Lógica	R14. Borrado, o eliminación de archivos, destrucción del S.O, robo de información personal.	• Encriptar la base de datos y la información contenida en ella. • Cifrar los datos transmitidos. • Generar claves robustas para el proceso de encriptado. • Instalación de antivirus y actualización permanente
	R15. Virus	
Personal Del Área	R16. Errores de Usuarios	• Capacitar a los funcionarios sobre la seguridad e inseguridad informática. • Dar a conocer los últimos tipos de ataque realizados a empresas. • Eliminar y/o deshabilitar las claves asignadas a los funcionario que ya no están vinculados con la empresa. • Establecer y dar a conocer un conjunto de buenas prácticas sobre el uso de las tics. • Hacer que los funcionarios firmen un documento de confidencialidad. • Evaluar las condiciones laborales de los trabajadores para identificar el inconformismo. • Dar a conocer las técnicas utilizadas por personas mal intencionadas para obtener información privada de la organización.
	R17. Sustracción, divulgación, venta o modificación de la información propia de la compañía.	
	R18. Alteración de archivos y registros.	
	R19. Robo o destrucción de información.	
	R20. Robo o destrucción de equipos de cómputo.	
	R21. Fuga de información.	
	R22. Ataque con ingeniería social	
	R23. Desconocimiento de las políticas de Seguridad	

Tipo de activo	Riesgos	Sistema de control
	R24. Relación e Integridad	
	R25. Ingeniería social	
Desastre natural - calamidad	R26. Terremoto, inundación, tormenta, etc	• Instalar UPS con buena capacidad • Instalar polos a tierra o para rayos

Fuente: El Autor

Anexo M. Dominios y controles de acuerdo a los activos informáticos existentes en la empresa

Núm.	Nombre	Descripción / Justificación	Pregunta existencia control	Si/No	Aplica?
A.5	Dominio: PSI				
A.5.1	*Directrices establecidas por la dirección para la seguridad de la*	*Objetivo: Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.*			
A.5.1.1	Políticas para la seguridad de la información	Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes	¿La empresa posee un conjunto de políticas para la seguridad de la información?	NO	SI
A.5.1.2	Revisión de las políticas para seguridad de la información	Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia	¿Se cuenta con un plan de revisión y cumplimiento de las políticas de la seguridad de la información?	NO	SI
A.6	Dominio: Organización de la seguridad de la información				
A.6.1	*Organización interna*	*Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.*			
A.6.1.1	Roles y responsabilidades para la seguridad de	Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.	¿Se cuenta con un equipo líder del proceso de seguridad informática?	NO	SI
A.6.1.2	Separación de deberes	Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	¿Se realizan verificaciones a las tareas asignadas al equipo encargado?	NO	SI
A.6.1.3	Contacto con las autoridades	Se deberían mantener los contactos apropiados con las autoridades pertinentes.	¿Existe contacto con las autoridades?	SI	SI
A.6.1.4	Contacto con grupos de interés especial	Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	¿Se realizar asignación de responsabilidades para la seguridad de la información?	NO	SI
A.6.1.5	Seguridad de la información en la gestión de proyectos	La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto.	¿Se cuenta con un protocolo de alerta en caso de la presentación de emergencias (robos, pérdidas, personas a las cuales	NO	SI

Núm.	Nombre	Descripción / Justificación	Pregunta existencia control	Si/No	Aplica?
A.6.2	*Dispositivos móviles y teletrabajo*	*Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.*			
A.6.2.1	Política para dispositivos móviles	Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el	¿La empresa tiene una política de uso de dispositivos para movilidad?	NO	NO
A.6.2.2	Teletrabajo	Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo	¿La empresa implementa el teletrabajo?	NO	NO
A.7	Dominio: Seguridad de los recursos humanos				
A.7.1	*Antes de asumir el empleo*	*Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.*			
A.7.1.1	Selección	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y	¿Se realiza Investigación de antecedentes?	SI	SI
A.7.1.2	Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	¿En los acuerdos contractuales en donde se especifiquen las responsabilidades y las de la organización en cuanto a la seguridad la información?	SI	SI
A.7.2	*Durante la ejecución del empleo*	*Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.*			
A.7.2.1	Responsabilidades de la dirección	La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	¿Se encuentra contratado un profesional específicamente para la realización del tema?	SI	SI
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y	¿la empresa capacita a sus funcionarios en cuanto a la seguridad de la información?	NO	SI
A.7.2.3	Proceso disciplinario	Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	¿Se realizan socializaciones para actualizar a los empleados en los diferentes cambios generados?	SI	SI

Núm.	Nombre	Descripción / Justificación	Pregunta existencia control	Si/No	Aplica?
A.7.3	*Terminación o cambio de empleo*	*Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.*			
A.7.3.1	Terminación o cambio de responsabilidades de empleo	Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.	¿Se tienen definidos las responsabilidades y deberes de seguridad de la información una vez el empleado termine su contratación o se le realice un cambio de puesto?	NO	SI
A.8	Dominio: Gestión de activos				
A.8.1	*Responsabilidad por los activos*	*Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.*			
A.8.1.1	Inventario de activos	Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.	¿Se cuenta con un inventario de activos actualizado?	SI	SI
A.8.1.2	Propiedad de los activos	Los activos mantenidos en el inventario deberían tener un propietario.	¿Se cuenta con un procedimiento para la solicitud de algún equipo faltante y necesario para el desempeño?	SI	SI
A.8.1.3	Uso aceptable de los activos	Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	¿Los funcionarios de la empresa hacen buen uso de los activos informáticos?	NO	SI
A.8.1.4	Devolución de activos	Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	¿Los empleados de la entidad al terminar su contrato hacen devolución de los activos?	SI	SI
A.8.2	*Clasificación de la información*	*Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.*			
A.8.2.1	Clasificación de la información	La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	¿Se cuenta con un sistema de etiquetado de los equipos para verificar su propiedad?	SI	SI

Núm.	Nombre	Descripción / Justificación	Pregunta existencia control	Si/No	Aplica?
A.8.2.2	Etiquetado de la información	Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	¿Se tienen implementado un procedimiento para el etiquetado de la información?	NO	SI
A.8.2.3	Manejo de activos	Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	¿Se manejan los activos de acuerdo al procedimiento implementado?	NO	SI
A.8.3	*Manejo de los soportes de almacenamiento*	*Objetivo:*			
A.8.3.1	Gestión de medios removibles	Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificaciónadoptado por la organización.	¿Se hace gestión de medios removibles de acuerdo al procedimiento implementado?	NO	SI
A.8.3.2	Disposición de los medios	Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	¿Se hace la disposición de medios de acuerdo al procedimiento implementado?	SI	SI
A.8.3.3	Transferencia de medios físicos	Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte	¿Se hace transferencia de medios fisicos de acuerdo al procedimiento implementado?	SI	SI
A.9	Dominio: Control de acceso				
A.9.1	*Requisitos del negocio para control de acceso*	*Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.*			
A.9.1.1	Política de control de acceso	Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	¿Se tiene control sobre los accesos a las redes por parte personas internas a la empresa?	SI	SI
A.9.1.2	Política sobre el uso de los servicios de red	Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	¿La empresa posee una política de control de accesos?	NO	SI
			¿Se tiene control sobre los accesos a las redes por parte personas externas a la empresa?	NO	SI
A.9.2	*Gestión de acceso de usuarios*	*Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.*			

Núm.	Nombre	Descripción / Justificación	Pregunta existencia control	Si/No	Aplica?
A.9.2.1	Registro y cancelación del registro de usuarios	Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	¿Se lleva un control sobre los usuarios de los SI?	NO	SI
A.9.2.2	Suministro de acceso de usuarios	Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	¿Se tiene un reporte de los procesos realizados por cada usuario en los SI?	NO	SI
A.9.2.3	Gestión de derechos de acceso privilegiado	Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado	¿La empresa realiza gestión de altas/bajas en el registro de usuarios?	NO	SI
A.9.2.4	Gestión de información de autenticación secreta de usuarios	La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.	¿Cuenta la empresa con un procedimiento que identifique los diferentes niveles de seguridad de acceso a las herramientas o SI?	NO	SI
A.9.2.5	Revisión de los derechos de acceso de usuarios	Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.	¿Se realiza una revisión periódica de los logs de acceso a las diferentes herramientas o SI?	NO	SI
A.9.2.6	Retiro o ajuste de los derechos de acceso	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o	¿Se realiza una revisión periódica de los derechos de acceso, realizando de esta manera la eliminación de los usuarios que ya no trabajan en la empresa?	NO	SI
A.9.3	*Responsabilidades de los usuarios*	*Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.*			
A.9.3.1	Uso de la información de autenticación secreta	Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	¿Los usuarios cumplen a cabalidad con el buen uso de la información secreta (No divulgación)?	SI	SI
A.9.4	*Control de acceso a sistemas y aplicaciones*	*Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.*			
A.9.4.1	Restricción de acceso Información	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de	¿Se cuenta con la decisión de niveles de acceso con relación a cada usuario?	NO	SI
A.9.4.2	Procedimiento de ingreso seguro	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.	¿Se cuenta con la asignación de contraseñas para el acceso a la información?	SI	SI

Núm.	Nombre	Descripción / Justificación	Pregunta existencia control	Si/No	Aplica?
A.9.4.3	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.	¿Se cuenta con un administrador de la base de datos y el código de aplicaciones?	SI	SI
A.9.4.4	Uso de programas utilitarios privilegiados	Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones	¿La empresa hace uso de herramientas de administración de sistemas?	NO	SI
A.9.4.5	Control de acceso a códigos fuente de programas	Se debería restringir el acceso a los códigos fuente de los programas.	¿Se tiene definido los roles de las personas que tienen acceso al código fuente y se encuentra esta información en lugares seguros?	SI	SI
A.10	Dominio: Criptografía				
A.10.1	*Controles criptográficos*	*Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.*			
A.10.1.1	Política sobre el uso de controles criptográficos	Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	¿Se tiene una política sobre el uso de controles criptográficos para la protección de la información?	NO	SI
A.10.1.2	Gestión de llaves	Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.	¿Se tiene una política con la cual se conoce el uso, protección y tiempo de vida de las llaves criptográficas?	NO	SI
A.11	Dominio: Seguridad física y del entorno				
A.11.1	*Áreas seguras*	*Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.*			
A.11.1.1	Perímetro de seguridad física	Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de	¿Los servidores y puntos de conexión se encuentran ubicados en un lugar seguro?	NO	SI
A.11.1.2	Controles físicos de entrada	Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	¿Las entradas a los lugares prohibidos se encuentran con algún mecanismo de seguridad, por ejemplo biométricos?	NO	SI

Núm.	Nombre	Descripción / Justificación	Pregunta existencia control	Si/No	Aplica?
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	¿Las oficinas, recintos e instalaciones cuentan con algún tipo de seguridad? Por ejemplo Vigilantes, cámaras.	NO	SI
A.11.1.4	Protección contra amenazas externas y ambientales	Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	¿El lugar donde se encuentran los servidores cuenta con las medidas de seguridad apropiadas (Extintores, aire acondicionado, entre otros)?	NO	SI
A.11.1.5	Trabajo en áreas seguras	Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.	¿Se tiene establecido un procedimiento que indique como se debe realizar el trabajo en las áreas seguras?	NO	SI
A.11.1.6	Áreas de despacho y carga	Se deberían controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es	¿El lugar donde se realiza el despacho y carga de herramientas (computadores, teclados, entre otros), cuenta con medidas de seguridad?	NO	NO
A.11.2	*Equipos*	*Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.*			
A.11.2.1	Ubicación y protección de los equipos	Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.	¿La infraestructura eléctrica se encuentra bien instalada y sin riesgos?	NO	SI
A.11.2.2	Servicios de suministro	Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	¿Los equipos informáticos y accesos de red, están seguros?	NO	SI
A.11.2.3	Seguridad del cableado	El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño	¿Se realiza mantenimiento a los equipos periódicamente?	NO	SI
A.11.2.4	Mantenimiento de equipos	Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.	¿Se cuenta con puestos de trabajos agradables y seguros?	SI	SI
A.11.2.5	Retiro de activos	Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.	¿Cuándo se va a realizar un cambio de algún computador a otro puesto de trabajo, se tiene un conducto regular para realizar dicho proceso?	NO	SI

Núm.	Nombre	Descripción / Justificación	Pregunta existencia control	Si/No	Aplica?
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	¿Cuándo un activo es sacado de la empresa, este cuenta con las medidas de seguridad en caso de tener pérdida?	NO	SI
A.11.2.7	Disposición segura o reutilización de equipos	Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con	¿Se realiza un backup y limpieza de los equipos de cómputo antes de entregarlo a otra persona?	SI	SI
A.11.2.8	Equipos de usuarion desatendidos	Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.	¿Los equipos que no tienen personal asignado se les dá una protección adecuada?	NO	SI
A.11.2.9	Política de escritorio limpio y pantalla limpia	Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en los	¿Se tiene una política de escritorio limpio para los papeles y medios de almacenamiento removibles?	NO	SI
A.12	Dominio: Seguridad de las operaciones				
A.12.1	*Procedimientos operacionales y responsabilidades*	*Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.*			
A.12.1.1	Procedimientos de operación documentados	Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.	¿Se documentan los procedimientos de operación y se ponen a disposición de los usuarios?	NO	SI
A.12.1.2	Gestión de cambios	Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	¿Se tiene un procedimiento de gestión de cambios en el área de desarrollo de los aplicativos?	SI	SI
A.12.1.3	Gestión de capacidad	Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.	¿Se realiza periódicamente revisión de los recursos, espacio de los diferentes servidores de la empresa?	NO	SI
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	¿Se cuenta con ambientes de desarrollo, pruebas y producción separados?	NO	NO
A.12.2	*Protección contra códigos maliciosos*	*Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.*			

Núm.	Nombre	Descripción / Justificación	Pregunta existencia control	Si/No	Aplica?
A.12.2.1	Controles contra códigos maliciosos	Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	¿Se cuenta con antivirus activo en todos los equipos de la empresa?	SI	SI
			¿Se realizan monitoreo en prevención a ataques que se generan al sistema?	SI	SI
A.12.3	*Copias de respaldo*	*Objetivo: Proteger contra la perdida de datos.*			
A.12.3.1	Respaldo de información	Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.	¿Se realizan periódicamente copias de seguridad de la información?	NO	SI
A.12.4	*Registro y seguimiento*	*Objetivo: Registrar eventos y generar evidencia.*			
A.12.4.1	Registro de eventos	Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	¿Se realiza revisión periódica de los logs de las diferentes herramientas con el fin de verificar las fallas y eventos de seguridad de la información?	NO	SI
A.12.4.2	Protección de la información de registro	Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.	¿Se tiene un control de acceso no autorizado, con el fin de proteger la información de algún tipo de modificación?	NO	SI
A.12.4.3	Registros del administrador y del operador	Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.	¿Las actividades realizadas por los administradores de las diferentes herramientas son monitoreadas?	NO	SI
A.12.4.4	sincronización de relojes	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de	¿Los relojes de los equipos de cómputo, servidores y demás sistemas, se encuentran sincronizados?	NO	SI
A.12.5	*Control de software operacional*	*Objetivo: Asegurar la integridad de los sistemas operacionales.*			
A.12.5.1	Instalación de software en sistemas operativos	Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.	¿Se tiene alguna regla que impida a los usuarios finales realizar la instalación de software?	NO	SI
A.12.6	*Gestión de la vulnerabilidad técnica*	*Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.*			
A.12.6.1	Gestión de las vulnerabilidades técnicas	Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los SI que se usen; evaluar la exposición de la organización a estas	¿Se realizan pruebas de penetración para encontrar vulnerabilidades en los sistemas y así prevenirlas?	NO	SI

Núm.	Nombre	Descripción / Justificación	Pregunta existencia control	Si/No	Aplica?
A.12.6.2	Restricciones sobre la instalación de software	Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.	¿Se tiene un procedimiento definido para las personas de soporte sobre la instalación del software que se puede realizar en los equipos?	NO	SI
A.12.7	Consideraciones sobre auditorias de SI	Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.			
A.12.7.1	Información controles de auditoría de sistemas	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	¿Los SI de la entidad, como las Bases de Datos cuentan con un sistema de auditoria activo?	NO	SI
A.13	Dominio: Seguridad de las comunicaciones				
A.13.1	*Gestión de la seguridad de las redes*	*Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.*			
A.13.1.1	Controles de redes	Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones	¿Se tiene un reporte de las transacciones realizadas en las redes de la empresa?	NO	SI
A.13.1.2	Seguridad de los servicios de red	Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten	¿En la empresa existen mecanismos de seguridad asociados a servicios de red?	NO	SI
A.13.1.3	Separación en las redes	Los grupos de servicios de información, usuarios y SI se deberían separar en las redes	¿Se tiene algún procedimiento sobre el acceso a las redes?	NO	SI
A.13.2	*Transferencia de información*	*Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.*			
A.13.2.1	Políticas y procedimientos de transferencia de	Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de	¿Se cuenta con protocolos de intercambio de información con externos?	NO	SI

Núm.	Nombre	Descripción / Justificación	Pregunta existencia control	Si/No	Aplica?
A.13.2.2	Acuerdos sobre transferencia de información	Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.	¿Se cuenta con servicio de email dentro del dominio de la empresa?	NO	SI
A.13.2.3	Mensajería electrónica	Se debería proteger adecuadamente la información incluida en la mensajería electrónica.	¿La información contenida en los correos cuenta con mecanismos de seguridad, como por ejemplo antivirus, protección por contraseña?	NO	SI
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	Se deberían identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	¿Se realiza revisión y actualización de los acuerdos de confidencialidad?	NO	SI
A.14	Dominio: Adquisición, desarrollo y mantenimientos de sistemas				
A.14.1.1	*Requisitos de seguridad de los SI*	*Objetivo: Asegurar que la seguridad de la información sea una parte integral de los SI durante todo el ciclo de vida. Esto incluye también los requisitos para SI que prestan servicios en redes públicas.*			
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos SI o para mejoras a los SI existentes.	Se han implementado protocolos de seguridad en los SI	NO	SI
A.14.1.2	Seguridad de servicios de las aplicaciones en redes publicas	La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	Se cuenta con control de las transacciones realizadas a nivel externo por medio del SI	NO	NO
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada	¿Se realiza la protección de la información involucrada en las transacciones de los servicios de las aplicaciones, por ejemplo certificados digitales?	NO	SI

Núm.	Nombre	Descripción / Justificación	Pregunta existencia control	Si/No	Aplica?
A.14.2	*Seguridad en los procesos de desarrollo y soporte*	*Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los SI.*			
A.14.2.1	Política de desarrollo seguro	Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización	Se cuenta con un procedimiento para la solicitud de desarrollo de software	NO	NO
A.14.2.2	Procedimientos de control de cambios en sistemas	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios	Se lleva un control de las versiones de las aplicaciones desarrolladas	NO	NO
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	Se cuenta con un protocolo para la aplicación de pruebas a los SI desarrollados	NO	NO
A.14.2.4	Restricciones en los cambios a los paquetes de software	Se deberían desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente	Se cuenta con un procedimiento para la puesta en producción de un desarrollo en SI	NO	NO
A.14.2.5	Principios de construcción de sistemas seguros	Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de SI.	Se tienen en cuenta principios de seguridad en un entorno de desarrollo	NO	NO
A.14.2.6	Ambiente de desarrollo seguro	Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	¿El lugar en donde se encuentra el código y las aplicaciones desarrolladas es seguro?	NO	NO
A.14.2.7	Desarrollo contratado externamente	La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	¿Cuenta la empresa con un hosting tercerizado?	NO	SI
A.14.2.8	Pruebas de seguridad de sistemas	Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad	¿Se realizan pruebas de funcionalidad a las aplicaciones desarrolladas?	NO	SI

Núm.	Nombre	Descripción / Justificación	Pregunta existencia control	Si/No	Aplica?
A.14.2.9	Prueba de aceptación de sistemas	Para los SI nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.	¿Cuándo se realizan actualizaciones a los desarrollos de aplicaciones, se hacen pruebas de aceptación?	NO	SI
A.14.3	*Datos de prueba*	*Objetivo: Asegurar la protección de los datos usados para pruebas.*			
A.14.3.1	Protección de datos de prueba	Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente.	¿Cuándo se realizan las pruebas se trabajan con datos falsos?	NO	SI
A.15	Dominio: Relación con los proveedores				
A.15.1	*Seguridad de la información en las relaciones con los proveedores*	*Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.*			
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberían acordar con estos y se deberían documentar.	¿Se cuenta con una política de seguridad de la información asociada a terceros?	NO	NO
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	¿Se tienen establecidos los requisitos y procedimientos de acceso a las instalaciones por parte de terceros?	NO	NO
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	¿Se tiene acuerdos con terceros que incluyan los requisitos para tratar los riesgos de seguridad de la información asociados a la cadena de suministro?	NO	NO
A.15.2	*Gestión de la prestación de servicios con los*	*Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.*			
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	¿Se hace un seguimiento de la prestación del servicio de terceros?	NO	NO

Núm.	Nombre	Descripción / Justificación	Pregunta existencia control	Si/No	Aplica?
A.15.2.2	Gestión de cambios en los servicios de proveedores	Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.	¿Se tiene una gestión de cambios en el suministro de servicios por parte de terceros?	NO	NO
A.16	Dominio: Gestión de incidentes de seguridad de la información				
A.16.1	*Gestión de incidentes y mejoras en la seguridad de la*	*Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.*			
A.16.1.1	Responsabilidad y procedimientos	Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	¿Se cuenta con un procedimiento para la identificación de un incidente de seguridad de la información?	NO	SI
A.16.1.2	Reporte de eventos de seguridad de la información	Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.	¿Se cuenta con un procedimiento para el reporte de un incidente de seguridad de la información?	NO	SI
A.16.1.3	Reporte de debilidades de seguridad de la información	Se debería exigir a todos los empleados y contratistas que usan los servicios y SI de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	¿Se cuenta con un procedimiento para el trámite de un incidente de seguridad de la información?	NO	SI
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.	¿Se tiene identificado un responsable para la gestión de los incidentes de seguridad de la información?	NO	SI
A.16.1.5	Respuesta a incidentes de seguridad de la	Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	¿Los incidentes informáticos son tratados y solucionados a tiempo?	NO	SI

Núm.	Nombre	Descripción / Justificación	Pregunta existencia control	Si/No	Aplica?
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros	¿Se solicitan evidencias de los incidentes de seguridad de información identificados?	NO	SI
A.16.1.7	Recolección de evidencia	La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	¿Se tiene definido un procedimiento en donde se especifique como debe realizarse la identificación, recolección, adquisición y preservación de información que es tomada como	NO	SI
A.17	Dominio: Aspectos de seguridad de la información de la gestión de continuidad de negocio				
A.17.1	*Continuidad de seguridad de la información*	*Objetivo: La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización.*			
A.17.1.1	Planificación de la continuidad de la seguridad de la información	La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	¿Se hace seguimiento a la seguridad de la información?	NO	SI
A.17.1.2	Implementación de la continuidad de la seguridad de la información	La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	¿Se tiene un plan de continuidad?	NO	SI
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son validos y eficaces durante situaciones adversas.	¿Se realiza regularmente la verificación del plan de continuidad?	NO	SI
A.17.2	*Redundancias*	*Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.*			
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	¿Las instalaciones de procesamiento de información se implementan con redundancia suficiente para cumplir los requisitos de disponibilidad?	NO	SI
A.18	Dominio: Cumplimiento				

Núm.	Nombre	Descripción / Justificación	Pregunta existencia control	Si/No	Aplica?
A.18.1	*Cumplimiento de requisitos legales y contractuales*	*Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.*			
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	¿Se realizan auditorías internas para verificar el cumplimiento de la norma?	NO	SI
A.18.1.2	Derechos de propiedad intelectual	Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	¿Se cuenta con mecanismos de protección de la información?	NO	SI
A.18.1.3	Protección de registros	Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	¿Se tiene documentado todo el proceso de seguridad y protección de la información?	NO	SI
A.18.1.4	Privacidad y protección de datos personales	Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.	¿Se asegura la privacidad y la protección de la información de datos personales?	NO	SI
A.18.1.5	Reglamentación de controles criptográficos	Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	¿Se controles criptográficos para la protección de la información de datos personales?	NO	SI
A.18.2	*Revisiones de seguridad de la información*	*Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.*			

Núm.	Nombre	Descripción / Justificación	Pregunta existencia control	Si/No	Aplica?
A.18.2.1	Revisión independiente de la seguridad de la información	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	¿Se cumple con las políticas y normas de seguridad?	SI	SI
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	¿Se realizan comités de seguridad con los altos directivos en donde se revisen con regularidad el cumplimiento de las políticas de seguridad en todas las áreas?	NO	SI
A.18.2.3	Revisión del cumplimiento técnico	Los SI se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	¿Se realiza revisión periódica de los sistemas con el fin de verificar el cumplimiento de las PSI?	NO	SI

Anexo N. Requisitos de la Norma ISO/IEC 27001:2013.

Tabla 1. Requisito de la Norma ISO/IEC 27001:2013. Contexto de la Empresa

REQUISITO	CONTEXTO DE LA EMPRESA	CUMPLE	¿QUÉ SE TIENE?	RECOMENDACIONES A IMPLEMENTAR
4.1	CONOCIMIENTO DE LA EMPRESA Y DE SU CONTEXTO	SI	Se tiene el conocimiento de la organización, su contexto, así como la comprensión de su misión, visión y objetivos estratégicos.	Implementar un Gobierno de Tecnología Informática que se ajuste a las necesidades de la organización y que esté acorde a los objetivos estratégicos, capacidades, recursos, SI y estructura organizacional.
4.2	COMPRENSIÓN DE LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS	SI	La oficina de Sistemas y Telecomunicaciones y todas las unidades administrativas que dependen de su correcto funcionamiento para ejercer el desarrollo normal de sus procesos, así como los empleados para realizar sus labores administrativas.	Relacionar a las unidades administrativas de más alto nivel y los beneficios que genera para la empresa en general.
4.3	DETERMINACIÓN DEL ALCANCE DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	SI	Hay que diseñar un SGSI para toda la empresa en general	Comunicarse a los empleados con el objetivo de establecer un nivel de compromiso, liderazgo y concientización con las PSI que allí sean contenidas.
4.4	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	NO	Actualmente no se tiene implementado un SGSI.	Diseñar y/o planear un SGSI que mediante un proceso sistemático y mejoramiento continuo ayude a establecer los niveles de riesgos aceptables para la empresa. La recomendación es el estándar internacional ISO 27001:2013 aplicable a las organizaciones de cualquier tamaño y actividad.

Tabla 2. Requisito de la Norma ISO/IEC 27001:2013. Liderazgo.

REQUISITO	LIDERAZGO	CUMPLE	¿QUÉ SE TIENE?	RECOMENDACIONES A IMPLEMENTAR
5.1	LIDERAZGO Y COMPROMISO	SI	La empresa tiene conocimiento de la importancia del SGSI, y beneficios que genera para la empresa.	Establecer una comunicación y liderazgo efectivo a los funcionarios que hagan parte del Proceso de Gestión del Desarrollo Tecnológico (de acuerdo al alcance) sobre la importancia del SGSI.
5.2	POLÍTICA	NO	No se tiene una política de seguridad de la información documentada.	Ajustar las políticas generales y detalladas del SGSI que sean de alcance para la empresa y que sean públicamente accesibles a todos los funcionarios para su conocimiento y aplicación.
5.3	ROLES, RESPONSABILIDADES. Y AUTORIDADES EN LA ORGANIZACIÓN	SI	Los roles y responsabilidades están asignadas.	Documentar los roles y responsabilidades en base a la seguridad de la información.

Tabla 3. Requisito de la Norma ISO/IEC 27001:2013. Planificación.

REQUISITO	PLANIFICACIÓN	CUMPLE	¿QUÉ SE TIENE?	RECOMENDACIONES A IMPLEMENTAR
6.1	ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES	-		-
6.1.1	GENERALIDADES	SI	Existen todas las condiciones para aplicar el SGSI.	No Aplica
6.1.2	VALORACIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN	NO	No existe una metodología claramente definida que clasifique, analice, evalúe y gestione los riesgos de la seguridad de la información. Se tienen clasificado pero los riesgos del Proceso de Gestión del Desarrollo Tecnológico.	Analizar las distintas metodologías de evaluación de riesgos, escoger la que mejor se adapte a las necesidades de la empresa y documentarla. Revisar los riesgos del Proceso de Gestión del Desarrollo Tecnológico e incluir los riesgos que apliquen al SGSI.

6.1.3	TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	NO	Se tiene la matriz de riesgos del Proceso de Gestión del Desarrollo Tecnológico, debe complementarse con los riesgos de seguridad de La Información.	Determinar los controles necesarios para mitigar los riesgos encontrados en el análisis y documentar el plan de tratamiento para cada uno de ellos justificando su elección.
6.2	OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN Y PLANES PARA LOGRARLO	NO	No están documentados los objetivos de la seguridad de la información.	Definir los objetivos de la seguridad de la información y establecer la forma de alcanzarlos comprometiendo a los empleados en su alcance y logro.

Tabla 4. Requisito de la Norma ISO/IEC 27001:2013. Soporte.

REQUISITO	SOPORTE	CUMPLE	¿QUÉ SE TIENE?	RECOMENDACIONES A IMPLEMENTAR
7.1	RECURSOS	NO	Proponer los recursos necesarios que requiera la empresa.	La empresa debe garantizar los recursos para Para un SGSI total.
7.2	COMPETENCIA	SI	Se tiene la persona con el conocimiento necesario para el diseño y planeación del SGSI.	Contratar a personas certificadas en implementar un SGSI con la norma ISO 27001:2013.
7.3	TOMA DE CONCIENCIA	NO	Aunque existen acuerdos de confidencialidad y los empleados emplean algunas técnicas de seguridad informática, no existen las PSI a cumplir así como los objetivos.	Informar a los empleados de las diferentes unidades administrativas la importancia de la seguridad de la información y los beneficios que genera para la empresa e incluso de forma personal.
7.4	COMUNICACIÓN	NO	Aunque existen los medios para la comunicación organizacional efectiva, aún no se realiza para efectos de la seguridad de la información.	Aprovechar los medios de comunicación organizacional para distribuir información relevante a la seguridad.
7.5	INFORMACIÓN DOCUMENTADA	-	-	-
7.5.1	GENERALIDADES	NO	No se tiene la información documentada relevante a un SGSI y al estándar ISO 27001:2013.	Redactar y documentar toda la información requerida por el estándar ISO 27001:2013.

7.5.2	CREACIÓN Y ACTUALIZACIÓN	NO	No se actualizan los documentos del SGSI ya que no hay uno implementado.	Actualizar los documentos del SGSI y del estándar ISO 27001:2013 cuando sea necesario incluyendo razones y autores.
7.5.3	CONTROL DE LA INFORMACIÓN DOCUMENTADA	NO	No existe un control de los documentos del SGSI ya que no hay uno implementado.	Mantener un control de los documentos del SGSI preservando su confidencialidad, integridad, disponibilidad y autenticidad, así como mantener el control de cambios en las actualizaciones.

Tabla 5. Requisito de la Norma ISO/IEC 27001:2013. Operación.

REQUISITO	OPERACIÓN	CUMPLE	¿QUÉ SE TIENE?	RECOMENDACIONES A IMPLEMENTAR
8.1	PLANIFICACIÓN Y CONTROL OPERACIONAL	NO	No se tiene implementado un control de los procesos necesarios para alcanzar los objetivos de la seguridad de la información.	Establecer los procesos necesarios para planear, implementar, mantener y mejorar el SGSI.
8.2	VALORACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	NO	No existe una valoración de riesgos informáticos que permita determinar la criticidad o el nivel de riesgo aceptable.	Establecer un esquema de clasificación de riesgos informáticos que permita analizarlos y valorarlos para determinar los controles a implementar con el fin de mitigarlos.
8.3	TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN	NO	No existe un plan para el tratamiento de riesgos.	Documentar el plan de tratamiento de riesgos informáticos.

Tabla 6. Requisito de la Norma ISO/IEC 27001:2013. Evaluación del Desempeño.

REQUISITO	EVALUACIÓN DEL DESEMPEÑO	CUMPLE	¿QUÉ SE TIENE?	RECOMENDACIONES A IMPLEMENTAR

9.1	SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN	NO	No se tienen los métodos definidos así como tampoco los procesos y controles de seguridad que deben ser medidos, analizados y evaluados.	Establecer los métodos para realizar el seguimiento, medición, análisis y evaluación de los procesos y controles de seguridad del SGSI.
9.2	AUDITORIA INTERNA	NO	No está definido un plan de auditorías internas, así como tampoco los formatos para llevarla a cabo en relación a la seguridad de la información.	Planear, implementar y mantener un plan de auditoría interna que permita medir el estado de la seguridad de la información en base al estándar ISO 27001:2013.
9.3	REVISIÓN POR LA DIRECCIÓN	NO	No está documentado un plan de la revisión del SGSI por parte de la dirección.	Documentar y planear a intervalos regulares una revisión al SGSI de forma general y a las PSI con el fin de implementar las acciones correctivas pertinentes.

Tabla 7. Requisito de la Norma ISO/IEC 27001:2013. Mejora.

REQUISITO	10 MEJORA	CUMPLE	¿QUÉ SE TIENE?	RECOMENDACIONES A IMPLEMENTAR
10.1	NO CONFORMIDADES Y ACCIONES CORRECTIVAS	NO	No está documentada la forma de cómo tratar a las no conformidades con el SGSI.	Determinar y documentar las causas de las no conformidades con el SGSI e implementar acciones correctivas identificando la vulnerabilidad.
10.2	MEJORA CONTINUA	NO	No se tiene el SGSI implementado.	Proponer un sistema que permita mejorar continuamente el SGSI mediante un proceso sistemático.

Anexo O: FORMATOS DE CHEQUEO PROPUESTO

CONTROL	NOMBRE DEL CONTROL	DESCRIPCION DEL CONTROL	APLICA SI/NO	JUSTIFICACIÓN	CUMPLIMIENTO (%)	OBSERVACIONES
PSI.						
A.5.1.1	Políticas para la seguridad de la información	*Control*: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	NO		2	La Empresa debe definir un tipo de política y la característica específica a aplicar
A.5.1.2	Revisión de las políticas para la seguridad de la información	*Control*: Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúa.	NO		2	Se debe implementar una política de seguridad que permita la revisión continua.
A.6.1.1	Roles y responsabilidades para la seguridad de la información	*Control*: Se debe definir y asignar todas las responsabilidades de la seguridad de la información	SI	A cada funcionario y responsable de las actividades asignadas, se les induce un protocolo de cumplimiento.	35	
Organización de la Seguridad de la Información						
A.6.1.2	Separación de deberes	*Control*: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	NO		14	
A.6.1.3	Contacto con las autoridades	*Control*: Se debe mantener contacto apropiados con las autoridades pertinentes	SI	La empresa Informa todo tipo de anomalía que se presente	35	
A.6.1.4	Contacto con grupos de interés especial	*Control*: Se debe mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones	NO			

CONTROL	NOMBRE DEL CONTROL	DESCRIPCION DEL CONTROL	APLICA SI/NO	JUSTIFICACIÓN	CUMPLIMIENTO (%)	OBSERVACIONES
		profesionales especializadas en seguridad				
A.6.1.5	Seguridad de la Información en la gestión de proyectos	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	SI	La entidad cuenta con los reglamentos técnicos para la gestión de los mismos.		
A.6.2.1	Políticas para dispositivos moviles	Control: Se debe adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	NO			Se debe implementar un software que controle los accesos de los dispositivos móviles, evitando la compatibilidad entre el dispositivo y la maquina física de la Entidad.
A.6.2.2	Teletrabajo	Control: Se debe implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	NO			
Seguridad de los recursos humanos.						
A.7.1.1	Selección.	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	SI	La empresa hace un análisis técnico y administrativo para el ingreso de cada uno de los funcionarios de la Entidad.	55	Este tipo de seguridad se debe implementar en cada una de las oficinas y dependencias donde se maneje recursos humanos y técnicos.
A.7.1.2	Técnicas y condiciones de empleo.	Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.	SI	A cada contratista se le asigna un manual de funciones que debe cumplir con los reglamentos de Contro Interno.	65	

CONTROL	NOMBRE DEL CONTROL	DESCRIPCION DEL CONTROL	APLICA SI/NO	JUSTIFICACIÓN	CUMPLIMIENTO (%)	OBSERVACIONES
A.7.2.1	Responsabilidades de la dirección	*Control*: La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.	NO			El personal que Labora en la entidad esta en un porcentaje bajo de conocimientos de Tecnologias de InformaciónInformación
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y donde sea pertinente, los contratistas, deben recibir la educación y formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.	NO			La entidad no cuenta con los recursos para las acapacitaciones del personal adscrito a la Entidad.
A.7.2.3	Proceso disciplinario	Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	SI	El departamento jurídico es el encargado de aunar esfuerzos para cumplir con este requisito en la Entidad	70	
A.7.3.1	Terminación o cambio de responsabilidades de empleo.	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	SI	La Entidad informa con anticiopación los posibles sucesos y cambios que se presenten en cada una de las áreas.	50	
Gestión de activos						
A.8.1.1	Inventario de activos	*Control*: Se deben identificar los activos asociados con la información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	SI	En la Empresa se lleva un inventario de Activos, para que permita realizar los cambios pertinenentes cuando sea necesario.	60	
A.8.1.2	propiedad de los activos	*Control*: Los activos mantenidos en el inventario deben tener un propietario.	SI	Todo activo posee su factura y registro original.	60	

CONTROL	NOMBRE DEL CONTROL	DESCRIPCION DEL CONTROL	APLICA SI/NO	JUSTIFICACIÓN	CUMPLIMIENTO (%)	OBSERVACIONES
A.8.1.4	Devolución de activos	*Control*: Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	SI	Los activos asignados a cada funcionario se lleva un inventario.	80	
A.8.2.1	Clasificación de la Información	*Control*: La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	NO			
A.8.2.2	Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	SI	Los Activos de la Información están etiquetados con un número y una serie.		
A.8.2.3	Manejo de activos	Control: Se debe desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	NO			
A.8.3.1	Gestión de medios removibles	Control: Se debe implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	NO			
A.8.3.2	Disposición de los medios	Control: Se debe disponer de forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	NO			
A.8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	NO			
Control de acceso						

CONTROL	NOMBRE DEL CONTROL	DESCRIPCION DEL CONTROL	APLICA SI/NO	JUSTIFICACIÓN	CUMPLIMIENTO (%)	OBSERVACIONES
A.9.1.1	Política de control de acceso	*Control*: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	SI	El Administrador del sistema organiza el acceso a las bases de datos	52	
A.9.1.2	Acceso a redes y a servicios en red	*Control*: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	NO			Se debe implementar un sistema de control que permita el acceso restringido a las redes.
A.9.2.1	Registro y cancelación del registro de usuarios.	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	NO			Se debe implementar un software que habilite y desabilite los usuarios de las bases de datos para msntener la integridad de los datos.
A.9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para *todos los sistemas y servicios.*	NO			
A.9.2.3	Gestión de derecho de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	NO			
A.9.2.4	Gestión de información de autenticación secreta de usuarios	Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	NO			
A.9.2.5	Revisión de los derechos de acceso de usuarios.	Control: Los propietarios de los activos deben revisar los derechos de acceso de usuarios, a intervalos regulares.	NO			
A.9.2.6	Retiro o ajuste de los derecho de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se				

CONTROL	NOMBRE DEL CONTROL	DESCRIPCION DEL CONTROL	APLICA SI/NO	JUSTIFICACIÓN	CUMPLIMIENTO (%)	OBSERVACIONES
		deben ajustar cuando se hagan cambios.				
A.9.3.1	Uso de información de autenticación secreta	Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticidad secreta.	NO			La Empresa debe asignar un protocolo de seguridad respecto a la responsabilidad y confiabilidad de los datos que maneja el usuario interno.
A.9.4.1	Restricción de acceso a la información.	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con las políticas de control de acceso.	NO			Los accesos de la Información debe manejarse con confiabilidad del administrador del sistema.
A.9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiera la política de control de acceso, el acceso al sistema y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	NO			
A.9.4.3	Sistema de gestión de contraseñas	*Control*: Los sistemas de gestión de contraseña deben ser interactivos y deben asegurar la calidad de las contraseñas.	NO			
A.9.4.4	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente l uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	NO			
A.9.4.5	Control de acceso a códigos fuente de programas	Control: Se debe restringir el acceso a los códigos fuente de los programas.	NO			
Criptografía						
A.10.1.1	Política sobre el uso de controles criptográficos.	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	NO			

CONTROL	NOMBRE DEL CONTROL	DESCRIPCION DEL CONTROL	APLICA SI/NO	JUSTIFICACIÓN	CUMPLIMIENTO (%)	OBSERVACIONES
A.10.1.2	Gestión de llaves.	Control: Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	NO			
Seguridad física y del entorno						
A.11.1.1	Perímetro de seguridad física	*Control*: Se debe definir y usar perímetro de seguridad, y usarlo para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	SI	El área donde se encuentra el sistema informático es amplia y con buenos accesos	70	
A.11.1.2	Controles de acceso físicos	*Control*: Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado.	SI	El área se encuentra protegida	70	Se debe mejorar los accesos para evitar que usuarios externos ingresen directamente al área de informática
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	*Control*: Se debe diseñar y ampliar seguridad física a oficinas, recintos e instalaciones.	NO		26	S e debe aplicar un sistema que permita garantizar la seguridad física de los equipos de cómputo.
A.11.1.4	Protección contra amenazas externas y ambientales	*Control*: Se debe diseñar y ampliar protección física contra desastres naturales, ataques maliciosos o accidentes.	SI	El edificio donde funciona la Empresa cuenta con un buen aislamiento por lo tanto evita el riesgo de inundación	80	
A.11.1.5	Trabajo en áreas seguras	*Control*: Se deben diseñar y ampliar procedimientos para trabajo en áreas seguras.	NO			
A.11.1.6	Áreas de despacho y carga	*Control*: Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlo de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	NO			N o es la actividad que compete a la administración

CONTROL	NOMBRE DEL CONTROL	DESCRIPCION DEL CONTROL	APLICA SI/NO	JUSTIFICACIÓN	CUMPLIMIENTO (%)	OBSERVACIONES
A.11.2.1	Ubicación y protección de los equipos	*Control*: Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	NO		12	Se debe implementar un sistema de protección y aislamiento en los equipos de informática y servidores
A.11.2.3	Seguridad del cableado	*Control*: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra intercepciones, interferencia o daño.	SI	El sistema de cableado es mínimo se maneja por sistema wifi	60	
A.11.2.4	Mantenimiento de equipos	*Control*: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	SI	Se hace mantenimiento periódico de los equipos	55	
A.11.2.5	Retiro de activos	*Control*: Los equipos, información o software no se deben retirar de un sitio sin autorización previa.	SI	Solo se hace con autorización del jefe se sistemas		
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	SI	Los Equipos se encuentran en el área de informática.	80	
A.11.2.7	Disposición segura o reutilización de equipos.	Control: Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reuso.	NO			
A.11.2.8	Equipos de usuario desatendido	Control: Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.	NO			
A.11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	SI	Generalmente los equipos se mantienen en un buen aspecto de limpieza y orden interno.	80	

CONTROL	NOMBRE DEL CONTROL	DESCRIPCION DEL CONTROL	APLICA SI/NO	JUSTIFICACIÓN	CUMPLIMIENTO (%)	OBSERVACIONES
Seguridad de las Operaciones						
A.12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	NO			
A.12.1.2	Gestión de cambios	Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	NO			
A.12.1.3	Gestión de capacidad	*Control*: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	NO			
A.12.1.4	Separación de los ambientes de desarrollo, pruebas, y operaciones	Control: Se deben separar los ambientes de desarrollo, prueba y operaciones, para reducirlos riesgos de acceso o cambios no autorizados al ambiente de operación.	NO			
A.12.2.1	Controles contra códigos maliciosos	*Control*: Se deben implementar controles de detención, de prevención y recuperación, combinado con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	NO			
A.12.3.1	Respaldo de la información	*Control*: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	SI	Se hace copia de seguridad a los sistema de información		

CONTROL	NOMBRE DEL CONTROL	DESCRIPCION DEL CONTROL	APLICA SI/NO	JUSTIFICACIÓN	CUMPLIMIENTO (%)	OBSERVACIONES
A.12.4.1	Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	NO			
A.12.4.2	Protección de la información de registro	Control: La instalaciones y la información de registro se deben proteger contra alteraciones y acceso no autorizado.	NO			
A.12.4.3	Registro del administrador y del operador.	Control: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	NO			
12.4.4	Sincronización de relojes.	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	NO			
A.12.5.1	Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	NO			
A.12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los SI que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	NO			

CONTROL	NOMBRE DEL CONTROL	DESCRIPCION DEL CONTROL	APLICA SI/NO	JUSTIFICACIÓN	CUMPLIMIENTO (%)	OBSERVACIONES
A.12.6.2	Restricciones sobre la instalación de software.	Control: Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.	NO			
A.12.7.1	Controles de auditorías de SI.	Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	NO			
Seguridad de las comunicaciones						
A.13.1.1	Controles de redes.	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	NO			
A.13.1.2	Seguridad de los servicios de red.	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contrate externamente.	NO			
A.13.1.3	Separación en las redes.	Control: Los grupos de servicios de información, usuarios y SI se deben separar en las redes.	NO			
A.13.2.1	Políticas y procedimientos de transferencia de información.	Control: Se debe contar con políticas, procedimiento y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	NO			

CONTROL	NOMBRE DEL CONTROL	DESCRIPCION DEL CONTROL	APLICA SI/NO	JUSTIFICACIÓN	CUMPLIMIENTO (%)	OBSERVACIONES
A.13.2.2	Acuerdos sobre transferencia de información.	Control: Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	NO			
A.13.2.3	Mensajería electrónica.	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	NO			
A.13.2.4	Acuerdos de confidencialidad o de no divulgación.	Control: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	NO			
Adquisición, desarrollo y mantenimiento de Sistemas						
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información.	Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos SI o para mejoras a los SI existentes.	NO			
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas.	Control: La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	NO			

CONTROL	NOMBRE DEL CONTROL	DESCRIPCION DEL CONTROL	APLICA SI/NO	JUSTIFICACIÓN	CUMPLIMIENTO (%)	OBSERVACIONES
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones.	Control: La información involucrada de las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	NO			
A.14.2.1	Política de desarrollo seguro.	Control: Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	NO			
A.14.2.2	Procedimientos de control de cambios en sistemas.	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante uso de procedimientos formales de control de cambio.				
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación.	Control: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	NO			
A.14.2.4	Restricciones en los cambios a los paquetes de software.	Control: Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	NO			
A.14.2.5	Principios de construcción de los sistemas seguro.	Control: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguro, y aplicarlos a cualquier actividad de implementación de SI.	NO			

CONTROL	NOMBRE DEL CONTROL	DESCRIPCION DEL CONTROL	APLICA SI/NO	JUSTIFICACIÓN	CUMPLIMIENTO (%)	OBSERVACIONES
A.14.2.6	Ambiente de desarrollo seguro.	Control: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguro para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	NO			
A.14.2.7	Desarrollo contratado externamente.	Control: La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	NO			
A.14.2.8	Pruebas de seguridad de sistemas.	Control: Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.	NO			
A.14.2.9	Prueba de aceptación de sistemas.	Control: Para los SI nuevos, actualizaciones y nuevas versiones, se deben establecer programa de prueba para aceptación y criterios de aceptación relacionados.	NO			
A.14.3.1	Protección de datos de prueba.	Control: Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.				
Relación con los proveedores						
A.15.1.1	Política de seguridad de la información para las relaciones	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con éstos y se deben documentar.	NO			Se debe implementar un plan que permita mejorar los requisitos para mejorar los riesgos en la información

CONTROL	NOMBRE DEL CONTROL	DESCRIPCION DEL CONTROL	APLICA SI/NO	JUSTIFICACIÓN	CUMPLIMIENTO (%)	OBSERVACIONES
	con proveedores.					
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores.	Control: Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	NO			
A.15.1.3	Cadena de suministro de tecnología de información y comunicación.	Control: Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	NO			
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores.	Control: Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	NO			Se debe realizar una auditoria en la administración para verificar el alcance del mismo
A.15.2.2	Gestión de cambios en los servicios de los proveedores.	Control: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existente, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos.	NO			
Gestión de incidentes de seguridad de la información						

CONTROL	NOMBRE DEL CONTROL	DESCRIPCION DEL CONTROL	APLICA SI/NO	JUSTIFICACIÓN	CUMPLIMIENTO (%)	OBSERVACIONES
A.16.1.1	Responsabilidades y procedimiento	Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	NO			
A.16.1.2	Reporte de eventos de seguridad de la información.	Control: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	NO			
A.16.1.3	Reporte de debilidades de seguridad de la información.	Control: Se debe exigir a todos los empleados y contratistas que usan los servicios y SI de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	NO			
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	Control: Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información	NO			
A.16.1.5	Respuesta a incidentes de seguridad de la información.	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo procedimientos documentados.	NO		32	SE DEBE TENER UN PLAN DE RESPUESTA INMEDIATA A LOS INCIDENTES SUCEDIDOS EN LOS PROCESOS.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información.	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.	NO			Se debe implementar un sistema que permita de forma inmediata solucionar incidentes en los SI dentro de la Empresa.

CONTROL	NOMBRE DEL CONTROL	DESCRIPCION DEL CONTROL	APLICA SI/NO	JUSTIFICACIÓN	CUMPLIMIENTO (%)	OBSERVACIONES
A.16.1.7	Recolección de evidencia.	Control: La organización definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	NO			
A.17.1.1	Planificación de la continuidad de la seguridad de la información.	Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	NO			
A.17.1.2	Implementación de la continuidad de la seguridad de la información.	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	NO			La Empresa debe tener una visión de implementación, de mejora continua de los procesos que se ejecutan dentro de la Organización.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	NO			
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Control: Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	NO			
Cumplimiento						

CONTROL	NOMBRE DEL CONTROL	DESCRIPCION DEL CONTROL	APLICA SI/NO	JUSTIFICACIÓN	CUMPLIMIENTO (%)	OBSERVACIONES
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales.	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la organización.	NO			
A.18.1.2	Derechos de propiedad intelectual.	Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	NO			
A.18.1.3	Protección de registros.	Control: Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	NO			S e debe implementar un plan de acción que permita salvaguardar los registros que a diario se registran en la Empresa, ubicando en un lugar seguro y confiable.
A.18.1.4	Privacidad y protección de información de datos personales.	Control: Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.	NO			Los datos deben tener un sistema de seguridad que evite la vulnerabilidad y sabotaje de los mismos.
A.18.1.5	Reglamentación de controles criptográficos.	Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	NO			Debe Existir una política de seguridad, que permita asegurar los accesos a los SI.
A.18.2.1	Revisión independiente de la seguridad de la información.	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deben revisar	NO			

CONTROL	NOMBRE DEL CONTROL	DESCRIPCION DEL CONTROL	APLICA SI/NO	JUSTIFICACIÓN	CUMPLIMIENTO (%)	OBSERVACIONES
		independientemente a intervalos planificados o cuando ocurran Cambios significativos.				
A.18.2.2	Cumplimiento con las políticas y normas de seguridad.	Control: Los directores deben revisar con regularidad el cumplimiento de procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	NO			
A.18.2.3	Revisión del cumplimiento técnico.	Control: Los SI se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	NO			Se debe implementar un cronograma de actividades que permita hacer revisión periódica y rutinaria a los Equipos y SI

Anexo P. Declaración De Aplicabilidad SOA

La presente declaración los controles que son relevantes para el SGSI de la Empresa de Transportes Tierra Grata Compañía Ltda. y aplicables a la misma. Adicionalmente en ella se encuentran justificada la exclusión de algunos de los controles y se muestra el motivo de selección de los controles aplicables, entre los motivos de selección se pueden encontrar: resultados y conclusiones de la evaluación de riesgos y en los procesos de tratamiento del riesgo, requisitos legales o reglamentos, obligaciones contractuales y necesidades empresariales de la empresa en materia de seguridad de la información:

L: Requerimiento Regulatorio C: Obligación contractual N: Requerimiento del negocio R: Análisis de riesgos

Tabla 1. Diseño del cuadro de Declaración de aplicabilidad SOA teniendo en cuenta los resultados de las listas de chequeo y los activos informáticos existentes en la empresa

Sección	Controles ISO 27001:2013	Justificación para exclusión	Salvaguardas Seleccionadas		Razones para la selección de los controles[1]			
			Salvaguardas existentes	Salvaguardas planeadas	L	C	N	R
A.5	Dominio: PSI							
A.5.1	*Directrices establecidas por la dirección para la seguridad de la información*	*Objetivo: Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.*						
A.5.1.1	Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.			Redacción del documento: "Política de Seguridad de la Información" (PSI)	X		X	
A.5.1.2	Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.			En el documento: "Política de Seguridad de la Información" se establece un procedimiento de revisión de la política de seguridad	X		X	
A.6	Dominio: Organización de la seguridad de la información							

[1] **L**: Requerimiento Regulatorio **C**: Obligación contractual **N**: Requerimiento del negocio **R**: Análisis de riesgos

Sección	Controles ISO 27001:2013	Justificación para exclusión	Salvaguardas Seleccionadas		Razones para la selección de los controles[1]			
			Salvaguardas existentes	Salvaguardas planeadas	L	C	N	R
A.6.1	*Organización interna*	*Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.*						
A.6.1.1	Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.			Las responsabilidades deben ser conocidas a nivel informal en la organización			X	
A.6.1.2	Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.			Los roles serán segregados informalmente, las funciones de los cargos del área de sistemas se encuentran documentados en el manual de funciones.			X	
A.6.1.3	Se deberían mantener los contactos apropiados con las autoridades pertinentes.			Gestionar un proceso de gestión legal y cumplimiento normativo en donde se establecen los procedimientos para gestionar las relaciones con las autoridades reguladoras		X		
A.6.1.4	Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.			Mantener contactos informales con proveedores de servicios de información	X		X	
A.6.1.5	La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto.			Establecer un protocolo de alerta en caso de la presentación de emergencias (robos, pérdidas, personas a las cuales se debe acudir)	X		X	
A.6.2	*Dispositivos móviles y teletrabajo*	*Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.*						
A.6.2.1	Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	La empresa no autoriza la transferencia de información por medio de dispositivos móviles bajo ningún concepto						

Sección	Controles ISO 27001:2013	Justificación para exclusión	Salvaguardas Seleccionadas		Razones para la selección de los controles[1]			
			Salvaguardas existentes	Salvaguardas planeadas	L	C	N	R
A.6.2.2	Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	La empresa no autoriza la implementación del teletrabajo bajo ningún concepto						
A.7	Dominio: Seguridad de los recursos humanos							
A.7.1	*Antes de asumir el empleo*	*Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.*						
A.7.1.1	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.		Se investigan los antecedentes para los candidatos a cargos en la empresa	En los procedimientos de Contratación y Selección de personal se establece el procedimiento de verificación de antecedentes para los candidatos. En el procedimiento de Selección de proveedores" se establece el procedimiento de verificación de antecedentes a terceros		X	X	
A.7.1.2	Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.		La dirección reconoce a la seguridad con un factor decisivo en el negocio	Al inicio del contrato laboral, de debe dar a conocer el código de Seguridad de la Información de la empresa, el empleado, este se debe comprometer a cumplirlo junto con las políticas de seguridad de la empresa.			X	
A.7.2	*Durante la ejecución del empleo*	*Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.*						
A.7.2.1	La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.		La dirección reconoce a la seguridad con un factor decisivo en el negocio	Al inicio del contrato laboral, de debe dar a conocer el código de Seguridad de la Información de la empresa, el empleado, este se debe comprometer a cumplirlo junto con las políticas			X	

Sección	Controles ISO 27001:2013	Justificación para exclusión	Salvaguardas Seleccionadas		Razones para la selección de los controles[1]			
			Salvaguardas existentes	Salvaguardas planeadas	L	C	N	R
A.7.2.2	Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.			Asignación de las responsabilidades de Capacitación. Adicionalmente los procedimientos e instructivos de usuario se constituyen en una herramienta adicional de capacitación.			X	
A.7.2.3	Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.			Especificar las sanciones previstas por incumplimiento de la Política de Seguridad de la Información			X	
A.7.3	*Terminación o cambio de empleo*	*Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.*						
A.7.3.1	Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.			El departamento de sistemas actualiza los permisos de acceso cuando se entera del retiro de un funcionario. En el procedimiento Deshabilitación de usuarios" se establecen los procedimientos de retiro de permisos para los usuarios en los SI. Cuando se presenta un cambio o retiro del cargo se debe diligenciar el formato: Acta de Entrega de Cargo"			X	X
A.8	Dominio: Gestión de activos							
A.8.1	*Responsabilidad por los activos*	*Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.*						
A.8.1.1	Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.		Se cuenta con un inventario de equipos y aplicaciones	Existe un inventario actualizado con los activos de información de la empresa y su respectivo responsable.				

Sección	Controles ISO 27001:2013	Justificación para exclusión	Salvaguardas Seleccionadas		Razones para la selección de los controles[1]			
			Salvaguardas existentes	Salvaguardas planeadas	L	C	N	R
A.8.1.2	Los activos mantenidos en el inventario deberían tener un propietario.		Se tiene identificado informalmente al responsable de los activos	En el Inventario de Activos de Información se encuentran documentados los responsables de dichos activos de información.			X	
A.8.1.3	Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.			Las regulaciones para el uso adecuado de la información y los activos para su administración, se encuentran documentadas en el manual de políticas de sistemas			X	
A.8.1.4	Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.		Se solicita la devolución de tarjetas de acceso al finalizar el contrato	Al finalizar un contrato con la empresa, el área de recursos humanos y administrativos es responsable de verificar que todos los activos de la organización que estén en posesión empleados, contratistas y terceros sean devueltos.		X	X	
A.8.2	*Clasificación de la información*	*Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.*						
A.8.2.1	La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.		Los roles están segregados informalmente	Las funciones de los cargos del área de sistemas se encuentran documentados en el manual de funciones	X		X	
A.8.2.2	Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.			El procedimiento de etiquetado se encuentra documentado la Política de Seguridad de la Información			X	
A.8.2.3	Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.			Se estableció un sistema de manejo de activos en la Política de Seguridad de la información	X		X	

Sección	Controles ISO 27001:2013	Justificación para exclusión	Salvaguardas Seleccionadas		Razones para la selección de los controles[1]			
			Salvaguardas existentes	Salvaguardas planeadas	L	C	N	R
A.8.3	*Manejo de los soportes de almacenamiento.*	*Objetivo:*						
A.8.3.1	Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.			La empresa cuenta un software que permite bloquear el uso de los puertos en las estaciones de trabajo. Lo que permite administrar las políticas. Las políticas de gestión de medios extraíbles están estipuladas en la Política de Seguridad de la Información. Cuando por motivos de trabajo los empleados requieran retirar información de la compañía se debe cumplir con lo estipulado en el procedimiento de autorización de retiro de información de la compañía.			X	X
A.8.3.2	Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.		Existe un procedimiento informal de retirada de soportes	En LA Política de Seguridad de la Información, En Eliminación de Medios de Información se establece el procedimiento de eliminación de medios de información.			X	X
A.8.3.3	Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.		Se tiene identificadas las personas autorizadas a retirar medios de información de la empresa	En el procedimiento de autorización de retiro de información de la empresa se especifica la autorización de retiro de medios de información de la empresa.	X	X	X	X
A.9	Dominio: Control de acceso							
A.9.1	*Requisitos del negocio para control de acceso*	*Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.*						
A.9.1.1	Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.		Las tareas de la empresa se encuentran segregadas en roles	En la Política de Seguridad de la Información se encuentran establecidas las políticas de control de acceso de la	X		X	

Sección	Controles ISO 27001:2013	Justificación para exclusión	Salvaguardas Seleccionadas		Razones para la selección de los controles[1]			
			Salvaguardas existentes	Salvaguardas planeadas	L	C	N	R
A.9.1.2	Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.			En la Política de Seguridad de la Información, en la Administración de Privilegios, se establece el control de la asignación de privilegios			X	X
				Según lo establecido en la Política de Seguridad de la Información, en la Revisión de Derechos de Acceso de Usuarios: Los derechos de acceso son revisados por el área de Control Interno de la empresa			X	X
A.9.2	*Gestión de acceso de usuarios*	*Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.*						
A.9.2.1	Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.			En la Política de Seguridad de la Información, en la Revisión de Derechos de Acceso de Usuarios: Los derechos de acceso son revisados por el área de Control Interno de la compañía	X			
A.9.2.2	Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.			Se realiza una identificación individualizada de todos los usuarios Existen procedimientos de alta y baja de usuarios: Habilitación de usuarios en los SI Deshabilitación de usuarios	X		X	X
A.9.2.3	Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.			Se realiza una identificación individualizada de todos los usuarios Existen procedimientos de alta y baja de usuarios: Habilitación de usuarios en los SI Deshabilitación de usuarios	X		X	X

Sección	Controles ISO 27001:2013	Justificación para exclusión	Salvaguardas Seleccionadas		Razones para la selección de los controles[1]			
			Salvaguardas existentes	Salvaguardas planeadas	L	C	N	R
A.9.2.4	La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.			Las tareas de la compañía se encuentran segregadas en roles En la Política de Seguridad de la Información se encuentran establecidas las políticas de control de acceso de la compañía.				
A.9.2.5	Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.			Se llevan estadísticas del uso de la plataforma de información "Monitoreo del Acceso y Uso de los Sistemas" se establecen los parámetros de monitoreo de los sistemas de la compañía.	X			X
A.9.2.6	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.			El departamento de sistemas actualiza los permisos de acceso cuando se entera del retiro de un funcionario. En el procedimiento Deshabilitación de usuarios" se establecen los procedimientos de retiro de permisos para los usuarios en los SI. Cuando se presenta un cambio o retiro del cargo se debe diligenciar el formato: Acta de Entrega de Cargo"			X	X
A.9.3	*Responsabilidades de los usuarios*	*Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.*						
A.9.3.1	Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.			Cuando se entregan las contraseñas se da la información sobre el manejo de estas, en la Política de Seguridad de la Información, Uso de Contraseñas, se establecen las buenas prácticas que los usuarios de la empresa deben tener con sus contraseñas.	X		X X	

Sección	Controles ISO 27001:2013	Justificación para exclusión	Salvaguardas Seleccionadas		Razones para la selección de los controles[1]			
			Salvaguardas existentes	Salvaguardas planeadas	L	C	N	R
A.9.4	*Control de acceso a sistemas y aplicaciones*	*Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.*						
A.9.4.1	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.			Las contraseñas iniciales son únicas. En el documento Política de Seguridad de la Información, Administración de Contraseñas de Usuario y Administración de Contraseñas Críticas, se establece el proceso formal de gestión de contraseñas. Así mismo en el documento Administración de contraseñas de la plataforma de información, están registrados los procedimientos de gestión de contraseñas de la compañía.				
A.9.4.2	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.			Se aplican las mismas consideraciones del numeral anterior				
A.9.4.3	Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.			Se aplican las mismas consideraciones del numeral anterior			X	X
A.9.4.4	Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.			La empresa cuenta con software de gestión de seguridad que bloquea el acceso a programas utilitarios a usuarios no autorizados En PSI se establece que: Los usuarios finales y los operadores por ningún motivo tendrán acceso a programas fuente, ni a utilitarios de uso de desarrollo, ni a líneas de comando.			X	X

Sección	Controles ISO 27001:2013	Justificación para exclusión	Salvaguardas Seleccionadas		Razones para la selección de los controles[1]			
			Salvaguardas existentes	Salvaguardas planeadas	L	C	N	R
A.9.4.5	Se debería restringir el acceso a los códigos fuente de los programas.		El acceso al código fuente de los programas está restringido	PSI Control de Acceso a las Bibliotecas de Programas Fuentes	X		X	
A.10	Dominio: Criptografía							
A.10.1	*Controles criptográficos*	*Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.*						
A.10.1.1	Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.			Se conoce la norma de uso de controles criptográficos. Política de Utilización de Controles Criptográficos.	X		X	
A.10.1.2	Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.			La generación de claves se hace a través de un dispositivo informático. Política de Administración de claves criptográficas	X		X	
A.11	Dominio: Seguridad física y del entorno							
A.11.1	*Áreas seguras*	*Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.*						
A.11.1.1	Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.			Las instalaciones de la empresa con los siguientes controles de acceso físico: tarjetas de acceso, paredes sólidas y un puesto de recepción			X	
A.11.1.2	Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.			Los controles de las áreas de seguridad se detallan en el documento de Política de Seguridad de la Información			X	
A.11.1.3	Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.			Existe una empresa de seguridad encargada de la protección de las instalaciones			X	

Sección	Controles ISO 27001:2013	Justificación para exclusión	Salvaguardas Seleccionadas		Razones para la selección de los controles[1]			
			Salvaguardas existentes	Salvaguardas planeadas	L	C	N	R
A.11.1.4	Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.			La empresa cuenta con un programa de brigadas de acción en caso de emergencia. Implementos de seguridad ambiental y física a. Extintor de Solkaflam b. Sistema de aire acondicionado c. Red regulada de voltaje d. Detector de humo y/o incendio			X	
A.11.1.5	Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.			La empresa cuenta con un programa de aplicar procedimientos para trabajo en áreas seguras.			X	
A.11.1.6	Se deberían controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible,		Las áreas de carga y descarga se encuentran fuera de las instalaciones de la empresa.	En el documento Política de Seguridad de la Información se dictan las normas para recepción y distribución.			X	
A.11.2	*Equipos*	*Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización*						
A.11.2.1	Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.			En el procedimiento de Instalación de equipos de cómputo se define el procedimiento seguro para			X	X
A.11.2.2	Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.			La empresa cuenta con una UPS que funciona en caso de presentarse una falta de energía.			X	
A.11.2.3	El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.			El cableado de las instalaciones de la empresa se encuentra protegido con pisoducto metálico según el Código eléctrico colombiano – NTC			X	X

Sección	Controles ISO 27001:2013	Justificación para exclusión	Salvaguardas Seleccionadas		Razones para la selección de los controles[1]			
			Salvaguardas existentes	Salvaguardas planeadas	L	C	N	R
A.11.2.4	Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.		El mantenimiento a los equipos se hace de acuerdo a la garantía por personal debidamente autorizado	El mantenimiento de la plataforma tecnológica se encuentra documentado en los procesos de Solicitud de Soporte Técnico y de Mantenimiento de los equipos de cómputo. En la Política de Seguridad de la Información se establece la normatividad de mantenimiento de equipos de la empresa			X	X
A.11.2.5	Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.		Se tiene identificadas las personas autorizadas a retirar equipos de la empresa	En el procedimiento deTrasporte de equipos se establece el sistema de autorización de retiro de equipos de la empresa.En el procedimiento de autorización de retiro de información de la empresa se especifica la autorización de retiro de información de la empresa.	X	X	X	X
A.11.2.6	Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	No aplica debido a que la empresa no cuenta con equipos fuera de sus instalaciones	No aplica debido a que la empresa no cuenta con equipos fuera de sus instalaciones	Las medidas a seguir para equipamiento fuera de la instalaciones de la empresa se encuentran descritas en el documento Política de Seguridad de la Información, en el procedimiento de Transporte equipos de cómputo, se establece el correcto envío y entrega de equipos de cómputo a las sucursales de la empresa				

Sección	Controles ISO 27001:2013	Justificación para exclusión	Salvaguardas Seleccionadas		Razones para la selección de los controles[1]			
			Salvaguardas existentes	Salvaguardas planeadas	L	C	N	R
A.11.2.7	Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.		Se retiran los archivos cuando el computador cambia de usuario	En la Política de Seguridad de la Información se establece que: Los medios de almacenamiento conteniendo material sensible, por ejemplo, discos rígidos no removibles, serán físicamente destruidos o sobrescritos en forma segura en lugar de utilizar las funciones de borrado estándar.			X	X
A.11.2.8	Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.			Los de la empresa están programados para que su acceso sea bloqueado después de un periodo de inactividad determinado			X	
A.11.2.9	Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.		Se cuenta con bloqueo de pantalla	Registro de políticas en el documento Política de Seguridad de la información			X	
A.12	Dominio: Seguridad de las operaciones							
A.12.1	*Procedimientos operacionales y responsabilidades*	*Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.*						
A.12.1.1	Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.			En la intranet de la compañía se encuentran publicados los procedimientos de la compañía, así como instructivos de usuario para operaciones específicas. La metodología de documentación de procesos se encuentra registrada la Documentación de procedimientos y en la Guía			X	X

Sección	Controles ISO 27001:2013	Justificación para exclusión	Salvaguardas Seleccionadas		Razones para la selección de los controles[1]			
			Salvaguardas existentes	Salvaguardas planeadas	L	C	N	R
A.12.1.2	Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.		Los cambios son realizados por el personal debidamente autorizado	El control de cambios de los SI se estipula en la Elaboración del requerimiento y en el Desarrollo del requerimiento de la Política de Seguridad de la Información	X		X	X
A.12.1.3	Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.		Los recursos de información se monitorean informalmente	En las PSI esta la Planificación y Aprobación de Sistemas, donde se establecen las responsabilidades en la monitorización del uso de los recursos.	X			
A.12.1.4	Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	No se cuenta con ambientes de desarrollo, pruebas y producción separados						
A.12.2	*Protección contra códigos maliciosos*	*Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.*						
A.12.2.1	Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.		Los equipos de la compañía se encuentran protegidos por software de detección y reparación de virus y mensualmente se publican las estadísticas de virus como forma de concienciación.	Políticas establecidas en la Política de Seguridad de la Información se establecen las medidas de protección frente a código malicioso			X	
A.12.3	*Copias de respaldo*	*Objetivo: Proteger contra la perdida de datos.*						
A.12.3.1	Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.		Se realizan copias de seguridad en soportes	En la Política de Seguridad de la Información, en Resguardo de la Información se establecen las políticas de backup de la compañía. En el instructivo de Backup de servidores, se establecen los procedimientos para el backup diario de servidores	X	X	X	X

Sección	Controles ISO 27001:2013	Justificación para exclusión	Salvaguardas Seleccionadas		Razones para la selección de los controles[1]			
			Salvaguardas existentes	Salvaguardas planeadas	L	C	N	R
A.12.4	*Registro y seguimiento*	*Objetivo: Registrar eventos y generar evidencia.*						
A.12.4.1	Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.			Monitoreo del Acceso y Uso de los Sistemas se establecen los parámetros de monitoreo de los sistemas de la compañía.	X		X	
A.12.4.2	Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.			La empresa cuenta con un detector de vulnerabilidades (p.ej.Netclarity) que previene frente acciones forzosas o no autorizadas. Anualmente se realiza una prueba de penetración sobre los sistemas de la empresa	X			X
A.12.4.3	Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.			Diariamente se registran logs de las acciones sobre el sistema, servidores Windows y Linux que quedan almacenados en un disco duro Monitoreo del Acceso y Uso de los Sistemas se establecen los parámetros de monitoreo de los sistemas de la compañía.	X		X	
A.12.4.4	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.			En la empresa se sincronizarán los relojes con el reloj de industria y comercio.	X		X	
A.12.5	*Control de software operacional*	*Objetivo: Asegurar la integridad de los sistemas operacionales.*						
A.12.5.1	Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.			Se implementa software que controla la instalación de software en las estaciones de trabajo. En el PSI, Procedimiento de Control de Cambios, se definen los controles a realizar durante la implementación del software en producción	X		X	

Sección	Controles ISO 27001:2013	Justificación para exclusión	Salvaguardas Seleccionadas		Razones para la selección de los controles[1]			
			Salvaguardas existentes	Salvaguardas planeadas	L	C	N	R
A.12.6	*Gestión de la vulnerabilidad técnica*	*Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.*						
A.12.6.1	Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los SI que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.			La compañía cuenta con hardware de propósito específico para la detección y remediación de vulnerabilidades. El diagnostico de vulnerabilidades se realiza de acuerdo a lo especificado en Detección y remediación de vulnerabilidades	X		X	X
A.12.6.2	Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.			Se implementa software que controla la instalación de software en las estaciones de trabajo. En el PSI, Procedimiento de Control de Cambios, se definen los controles a realizar durante la implementación del software en operación	X		X	
A.12.7	Consideraciones sobre auditorias de SI	Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.						
A.12.7.1	Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.			Los procedimientos de la auditoría de sistemas llevados a cabo en la empresa son previamente definidos y comunicados. PSI Consideraciones de Auditorías de Sistemas, se establece adicionalmente el		X		
A.13	Dominio: Seguridad de las comunicaciones							
A.13.1	*Gestión de la seguridad de las redes*	*Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.*						

Sección	Controles ISO 27001:2013	Justificación para exclusión	Salvaguardas Seleccionadas		Razones para la selección de los controles[1]			
			Salvaguardas existentes	Salvaguardas planeadas	L	C	N	R
A.13.1.1	Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.			La red de la compañía se encuentra protegida por los siguientes componentes: Firewall (prevención frente a intrusos) p.ej. Netclarity (Detección y prevención de vulnerabilidades) En el procedimiento Detección y remediación de vulnerabilidades, se documentan los pasos de diagnostico de la red con el sistema Netclarity	X		X	X
A.13.1.2	Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.			Los nodos de acceso a la red se autentican. Se define una norma de acceso a la red, y se incluye en los acuerdos de servicio lo enumerado en el Documento de Política de Seguridad de la Información, Seguridad Frente al Acceso por Parte de			X	
A.13.1.3	Los grupos de servicios de información, usuarios y SI se deberían separar en las redes.			Se segregan los grupos de usuarios en la red La segregación de usuarios en las redes se encuentra en la PSI:Control de Conexión a la Red				X
A.13.2	*Transferencia de información*	*Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.*						
A.13.2.1	Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.			Las políticas de protección de información asociada con la interconexión, se encuentran publicadas en el documento Política de Seguridad de la Información				X
A.13.2.2	Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes			La organización incluye clausulas de confidencialidad en sus contratos con terceros		X	X	

Sección	Controles ISO 27001:2013	Justificación para exclusión	Salvaguardas Seleccionadas		Razones para la selección de los controles[1]			
			Salvaguardas existentes	Salvaguardas planeadas	L	C	N	R
A.13.2.3	Se debería proteger adecuadamente la información incluida en la mensajería electrónica.			Las políticas de uso del correo electrónico, se encuentran publicadas en el documento Política de Seguridad de la Información			X	X
A.13.2.4	Se deberían identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.			Existe un acuerdo de confidencialidad en los contratos laborales En el procedimiento Selección de proveedores" y el procedimiento Compras, se establece la firma por parte del proveedor de un acuerdo de confidencialidad diseñado y aprobado por el departamento jurídico de la compañía. Los acuerdos de confidencialidad son revisados periódicamente por el departamento jurídico	X	X	X	
A.14	Dominio: Adquisición, desarrollo y mantenimientos de sistemas							
A.14.1.1	*Requisitos de seguridad de los SI*	*Objetivo: Asegurar que la seguridad de la información sea una parte integral de los SI durante todo el ciclo de vida. Esto incluye también los requisitos para SI que prestan servicios en redes públicas.*						
A.14.1.1	Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos SI o para mejoras a los SI existentes.			Se conocen las leyes y contratos de seguridad de la información aplicables En PSI: Seguridad en los Sistemas de Aplicación, se especifican los requisitos de seguridad para los sistemas de seguridad. En el procedimiento Elaboración del requerimiento se encuentran contemplados los aspectos de seguridad como parte del proceso de desarrollo			X	X

Sección	Controles ISO 27001:2013	Justificación para exclusión	Salvaguardas Seleccionadas		Razones para la selección de los controles[1]			
			Salvaguardas existentes	Salvaguardas planeadas	L	C	N	R
A.14.1.2	La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	La empresa no cuenta con aplicaciones de comercio electrónico	NO APLICA	La empresa no cuenta con aplicaciones de comercio electrónico				
A.14.1.3	La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	La empresa no cuenta con aplicaciones de comercio electrónico	NO APLICA	La empresa no cuenta con aplicaciones de comercio electrónico				
A.14.2	*Seguridad en los procesos de desarrollo y soporte*	*Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los SI.*						
A.14.2.1	Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.	La empresa no hace desarrollo de software y de	NO APLICA	La empresa no hace desarrollo de software y de sistemas				
A.14.2.2	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios.	La empresa no hace desarrollo de software y de sistemas	NO APLICA	La empresa no hace desarrollo de software y de sistemas				
A.14.2.3	Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.	La empresa no hace desarrollo de software y de sistemas	NO APLICA	La empresa no hace desarrollo de software y de sistemas				
A.14.2.4	Se deberían desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.	La empresa no hace desarrollo de software y de sistemas	NO APLICA	La empresa no hace desarrollo de software y de sistemas				

Sección	Controles ISO 27001:2013	Justificación para exclusión	Salvaguardas Seleccionadas		Razones para la selección de los controles[1]			
			Salvaguardas existentes	Salvaguardas planeadas	L	C	N	R
A.14.2.5	Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de SI.	La empresa no hace desarrollo de software y de sistemas	NO APLICA	La empresa no hace desarrollo de software y de sistemas				
A.14.2.6	Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	La empresa no hace desarrollo de software y de sistemas	NO APLICA	La empresa no hace desarrollo de software y de sistemas				
A.14.2.7	La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.			Existen procedimientos informales de monitorización del software PSI: Requerimientos de Seguridad en Contratos de Tercerización	X			
A.14.2.8	Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.			Existe un proceso informal de aceptación de cambios en el departamento de sistemas En el PSI: Planificación y Aprobación de Sistemas se establecen los criterios de aprobación de nuevos SI.	X		X	
A.14.2.9	Para los SI nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.			Existe un proceso informal de aceptación de cambios en el departamento de sistemas En el PSI: Planificación y Aprobación de Sistemas se establecen los criterios de aprobación de nuevos SI.	X		X	
A.14.3	*Datos de prueba*	*Objetivo: Asegurar la protección de los datos usados para pruebas.*						
A.14.3.1	Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente.			Las pruebas se realizan en un habiente de pruebas separado PSI, Protección de los Datos de Prueba del Sistema	X		X	
A.15	Dominio: Relación con los proveedores							

Sección	Controles ISO 27001:2013	Justificación para exclusión	Salvaguardas Seleccionadas		Razones para la selección de los controles[1]			
			Salvaguardas existentes	Salvaguardas planeadas	L	C	N	R
A.15.1	*Seguridad de la información en las relaciones con los proveedores*	*Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.*						
A.15.1.1	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberían acordar con estos y se deberían documentar.	La empresa no autoriza una política asociada a terceros	NO APLICA	La empresa no autoriza una política asociada a terceros				
A.15.1.2	Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	La empresa no autoriza una política asociada a terceros	NO APLICA	La empresa no autoriza una política asociada a terceros				
A.15.1.3	Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	La empresa no autoriza una política asociada a terceros	NO APLICA	La empresa no autoriza una política asociada a terceros				
A.15.2	*Gestión de la prestación de servicios con los proveedores*	*Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.*						
A.15.2.1	Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	La empresa no autoriza una política asociada a	NO APLICA	La empresa no autoriza una política asociada a terceros				
A.15.2.2	Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes , teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.	La empresa no autoriza una política asociada a terceros	NO APLICA	La empresa no autoriza una política asociada a terceros				
A.16	Dominio: Gestión de incidentes de seguridad de la información							

Sección	Controles ISO 27001:2013	Justificación para exclusión	Salvaguardas Seleccionadas		Razones para la selección de los controles[1]			
			Salvaguardas existentes	Salvaguardas planeadas	L	C	N	R
A.16.1	*Gestión de incidentes y mejoras en la seguridad de la información*	*Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.*						
A.16.1.1	Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.			Existe un procedimiento informal de registro de fallos En el documento PSI Procedimientos de Manejo de Incidentes se estipula que se establecerán funciones y procedimientos de manejo de incidentes, estos se encuentran Gestión de incidentes de seguridad de la información	X		X	
A.16.1.2	Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.			Las comunicaciones de eventos de riesgo operativo se comunican en el contexto establecido por el sistema de administración del riesgo operativo. PSI Comunicación de Incidentes Relativos a la Seguridad	X		X	
A.16.1.3	Se debería exigir a todos los empleados y contratistas que usan los servicios y SI de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.			PSI: Comunicación de Debilidades en Materia de Seguridad	X		X	

Sección	Controles ISO 27001:2013	Justificación para exclusión	Salvaguardas Seleccionadas		Razones para la selección de los controles[1]			
			Salvaguardas existentes	Salvaguardas planeadas	L	C	N	R
A.16.1.4	Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.			En el sistema de administración del riesgo operativo se encuentran identificados una serie de riesgos que pueden interrumpir las operaciones del negocio, estos están valorados frente a su impacto y probabilidad de ocurrencia En el análisis de riesgos de seguridad de la información se identificaron específicamente las amenazas sobre los activos de información y el impacto de dichas amenazas para la seguridad de la información. PSI: Continuidad de las Actividades y Análisis de los Impactos	X		X	
A.16.1.5	Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.			Existe un procedimiento informal de registro de fallos En el documento PSI Procedimientos de Manejo de Incidentes se estipula que se establecerán funciones y procedimientos de manejo de incidentes, estos se encuentran Gestión de incidentes de seguridad de la información	X		X	
A.16.1.6	El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.			El área de control interno es la encargada de efectuar las gestiones al interior de la organización para el tratamiento de evidencia frente a incidentes de seguridad de la información.	X		X	

Sección	Controles ISO 27001:2013	Justificación para exclusión	Salvaguardas Seleccionadas		Razones para la selección de los controles[1]			
			Salvaguardas existentes	Salvaguardas planeadas	L	C	N	R
A.16.1.7	La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.			En el contexto del sistema de administración del riesgo operativo se cuantifican y categorizan los riesgos presentados en la organización En el documento de PSI: Aprendiendo de los Incidentes, se estipula el establecimiento de proceso que permita documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías, esta documentación de incidentes se realizará a través de lo estipulado en Gestión de incidentes de seguridad de la información			X	X
A.17	Dominio: Aspectos de seguridad de la información de la gestión de continuidad de negocio							
A.17.1	*Continuidad de seguridad de la información*	*Objetivo: La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización.*						
A.17.1.1	La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.			Existe un plan de continuidad del negocio debidamente documentado PSI: Proceso de la Administración de la Continuidad de la Organización				
A.17.1.2	La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante			Existe un plan de recuperación de la base de datos PSI: Elaboración e Implementación de los Planes de Continuidad de las				

Sección	Controles ISO 27001:2013	Justificación para exclusión	Salvaguardas Seleccionadas		Razones para la selección de los controles[1]			
			Salvaguardas existentes	Salvaguardas planeadas	L	C	N	R
A.17.1.3	La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.			En el manual de continuidad del negocio se encuentra establecido que las pruebas al plan de continuidad del negocio se realizaran anualmente de acuerdo al procedimiento establecido en este. PSI: Ensayo, Mantenimiento y Reevaluación de los Planes de Continuidad de la organización				
A.17.2	*Redundancias*	*Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.*						
A.17.2.1	Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.			Controles de Procesamiento Interno				
A.18	Dominio: Cumplimiento							
A.18.1	*Cumplimiento de requisitos legales y contractuales*	*Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.*						
A.18.1.1	Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.			Las leyes y normatividad aplicables a la seguridad de la información que rigen sobre la empresa se encuentran documentadas en PSI Identificación de la Legislación Aplicable	X		X	
A.18.1.2	Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.			Los derechos de propiedad intelectual son contemplados en los acuerdos de servicios PSI: Derechos de Propiedad Intelectual, la empresa cuenta con un software que permite detectar el uso de software no autorizado en la empresa	X	X	X	

Sección	Controles ISO 27001:2013	Justificación para exclusión	Salvaguardas Seleccionadas		Razones para la selección de los controles[1]			
			Salvaguardas existentes	Salvaguardas planeadas	L	C	N	R
A.18.1.3	Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.			Existe un área de archivo en donde se custodian los registros importantes de la compañía, por otra parte, las garantías de contratos se encuentran debidamente custodiadas en caja fuerte. PSI: Protección de los Registros de la organización En el proceso "Creación e ingreso de garantías al sistema" se estipula del proceso para el correcto archivo de garantías y en el Préstamo de garantía se establece el procedimiento de préstamo. El único departamento autorizado para solicitar garantías es el departamento jurídico. -El encargado del área de archivo cuenta con una lista de personas autorizadas para el préstamo de carpetas. El uso de esta lista se encuentra registrado en los procesos de Solicitud	X	X	X	
A.18.1.4	Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.			Existe una definición de la responsabilidad del manejo de los datos de carácter personal PSI: Protección de Datos y Privacidad de la Información Personal	X		X	
A.18.1.5	Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.			Se conocen y cumplen los requisitos emitidos por la Superintendencia Financiera sobre los controles cifrados PSI: Regulación de Controles para el Uso de Criptografia.	X		X	
A.18.2	*Revisiones de seguridad de la información*	*Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.*						

Sección	Controles ISO 27001:2013	Justificación para exclusión	Salvaguardas Seleccionadas		Razones para la selección de los controles[1]			
			Salvaguardas existentes	Salvaguardas planeadas	L	C	N	R
A.18.2.1	El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.		Las políticas de sistemas son revisadas anualmente por el comité de tecnología	Se establece el procedimiento Documentación de procedimientos en donde se establece la metodología de actualización y creación de nuevos procedimientos. Así mismo se establece el instructivo Guía para la elaboración, manejo y control de documentos	X		X	
A.18.2.2	Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.		Las políticas de sistemas son revisadas anualmente por el comité directivo.	En laPolítica de Seguridad de la Información se establece un procedimiento de revisión de la política de seguridad	X		X	
A.18.2.3	Los SI se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.		Las políticas de sistemas son revisadas anualmente por el comité de tecnología	En laPolítica de Seguridad de la Información se establece un procedimiento de revisión de la política de seguridad	X		X	