ANÁLISIS DE CAUSAS DE RIESGOS EN LA PROTECCION DE LA INFORMACIÓN DE LA EMPRESA SOLTEC-ING Y RECOMENDACIONES DE SEGURIDAD

EDWIN OMAR ORTIZ MANRIQUE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIAS E INGENIERIAS
ESPECIALIZACION EN SEGURIDAD INFORMATICA
MALAGA
2018

ANÁLISIS DE CAUSAS DE RIESGOS EN LA PROTECCION DE LA INFORMACION DE LA EMPRESA SOLTEC-ING Y RECOMENDACIONES DE SEGURIDAD

EDWIN OMAR ORTIZ MANRIQUE

Proyecto de Grado para optar al título de:
Especialista en Seguridad Informática

DIRECTOR:
LUIS FERNANDO ZAMBRANO HERNÁNDEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIAS E INGENIERIAS
ESPECIALIZACION EN SEGURIDAD INFORMATICA
MALAGA
2018

DEDICATORIA

A Dios, por haberme permitido realizar todas mis acciones para llevar a cabo la realización de mis objetivos.

A mi esposa Ligia Johana y mi hija Laura Camila, quienes han sido mi motivación y apoyo constante para alcanzar mis metas.

A mi familia en general, por brindarme el apoyo incondicional en los momentos que se hacen difíciles.

AGRADECIMIENTOS

En primer lugar, quiero agradecer a Dios, por todas las bendiciones recibidas, que por medio del espíritu Santo nos da la fortaleza e ilumina nuestras acciones y nos lleva por el buen camino.

A mi director de proyecto Ing. Fernando Zambrano por su orientación, esfuerzo y compromiso que ha logrado que esta meta llegue con éxito.

Son muchas las personas que han logrados ser parte importante durante mi proceso de vida profesional, por tal motivo las recuerdo con aprecio, sé que con sus buenas obras han logrado marcar huella en la vida de cada persona que han recibido su orientación. Mil bendiciones y gratitud.

Edwin Omar Ortiz Manrique

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE IMÁGENES

Pág.

LISTA DE TABLAS

Pág.

LISTA DE ANEXOS

Pág.

INTRODUCCION

Actualmente los sistemas de información se han convertido en parte fundamental para empresas u organizaciones, estableciendo importantes directrices en búsqueda de mantener los datos de forma confiable, la seguridad informática se enfoca en la protección, integridad y privacidad de la misma, mencionando que por más seguro que sea el sistema se corre riesgo.

La información encierra aspectos que van desde la clasificación física de los documentos, su almacenamiento, y procesos de gestión, hasta obtener una organización adecuada y que cumpla con los estándares exigidos, para dar cumplimiento al óptimo almacenamiento e integridad de los datos, donde la documentación y archivos de información se han convertido día a día en parte vital de las organizaciones, siendo los dispositivos informáticos herramientas prácticas para salvaguardar y compartir la información por medio de redes y canales de transmisión; el auge de la tecnología ha llevado a ofertar nuevas alternativas para el tratamiento y almacenamiento de datos con disponibilidad inmediata y segura.

Con lo anterior se busca un análisis de riesgo que permita realizar un completo diagnóstico para observar las debilidades y fortalezas en los procesos desarrollados para la seguridad informática, las cuales pertenecen a políticas diseñadas según el sistema de gestión de seguridad de información (SGSI), facilitando el monitoreo continuo a través de autoría y mejoras continuas para la empresa SOLTEC-ING. realizando la identificación de las vulnerabilidades o situaciones de riesgo a las cuales está expuesto el sistema; con el objetivo de proteger la integridad, disponibilidad y confiabilidad de la información.

1. PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

La empresa Suministros Eléctricos y soluciones Tecnológicas “SOLTEC-ING SAS” de Málaga Santander, en el manejo de su información no cuenta con un sistema de seguridad, por lo cual presenta riesgo en la administración de sus datos, ostentando un alto índice de inseguridad, lo cual hace necesario realizar un análisis diagnóstico actual de las causas de riesgo, con el fin mitigar los impactos que conlleva la falta de protección en el sistema, desarrollando una propuesta de acuerdo a los hallazgos identificados, que permitan estrategias de prevención y seguridad.

1.2 PREGUNTA DE INVESTIGACIÓN

¿En qué medida el análisis de causa de riesgos en la protección de la información de la empresa Suministros Eléctricos y soluciones Tecnológicas “SOLTEC-ING SAS”, permite conocer las vulnerabilidades en el manejo de los datos, de tal forma que facilite realizar las recomendaciones de seguridad respecto a los mecanismos de control de la información?

2. JUSTIFICACION

La seguridad informática según Aguilera (2010)[1] se ocupa del diseño, procedimientos, métodos y técnicas destinadas a conseguir un sistema de información seguro y confiable, partiendo de esta premisa la empresa “SOLTEC-ING SAS” actualmente no cuenta con una protección en el manejo de la información buscando que esta base de datos esté libre de riegos externos, siendo de difícil acceso para personas ajenas a la empresa, el presente trabajo busca identificar las fallas en el sistema que permiten la vulnerabilidad, y así implementar acciones correctivas en el manejo de la misma, reduciendo los puntos críticos que faciliten ataques a la información.

[1] AGUILERA LOPEZ, Purificación. Seguridad informática. Madrid: Editex, 2010. p.9. ISBN 8497717619

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Identificar los principales riegos en el sistema de información para generar controles que minimicen la ocurrencia de impactos asociados a las vulnerabilidades en el manejo de los datos en la empresa Suministros Eléctricos y Soluciones Tecnológicas “SOLTEC–ING S.A.S” en Málaga Santander.

3.2 OBJETIVOS ESPECÍFICOS

Determinar los riesgos que se presentan la empresa con la información, a través de un diagnóstico descriptivo y aplicado.

Clasificar y evaluar el nivel de impacto de los riesgos de acuerdo a la escala definida por la metodología Magerit.

Establecer mecanismos de control y gestión de acuerdo a la norma ISO 27001 que minimicen las vulnerabilidades encontradas en el estudio del análisis de riesgos realizado en la empresa “SOLTEC–ING S.A.S”

4. MARCO DE REFERENCIA

4.1 ANTECEDENTES

Aguirre y Aristizabal (2012)[2] sustentan que cada vez están más en auge las empresas que diseñan un sistema de gestión de seguridad de la información SGSI. Convirtiéndose actualmente en una técnica utilizada de acuerdo a las circunstancias cambiantes que han generado preocupación y prevención en cada una de las organizaciones. Lo anterior, hace que se establezca como prioridad un sistema de gestión de seguridad de la información como parte relevante de una Organización. En algunos grupos empresariales como ComBanc S.A, Etek International Holding Corp., Financial Systems Company Ltda., Ricoh Colombia, S.A. están presentes estos sistemas de gestión desde hace muchos años, y es la caja fuerte personal (a nivel web), en la que se puede guardar joyas, documentos críticos en papel, o cualquier elemento físico que no debe ser extraviado por el alto valor que tiene. Asumida en toda la sociedad la importancia de la información concentrada en vídeos, grabaciones de sonido, ficheros, documentos escaneados, fotografías, planos o todo lo que en si cada organización considere valioso, se necesita poder guardar cierta información en formato electrónico de modo completamente seguro a salvo de desastres; por tanto en el SGSI a diseñar, una de las medidas más importantes será el salvaguardar el activo más importante que es la información y establecer los controles necesarios para tal fin

Pulido y colaboradores (2011) [3] en su trabajo titulado: Diseño de políticas y controles para la seguridad de la información en pequeñas empresas con redes SOHO en el sector transporte de Bogotá., exponen que, a causa del creciente uso de Internet,

[2] AGUIRRE CARDONA, Juan David y ARISTIZABAL BETANCOURT, Catalina. Diseño del sistema de gestión de seguridad de la información para el grupo empresarial La Ofrenda. Tesis de Grado en Ingeniería de Sistemas: Universidad Tecnológica de Pereira. Facultad de Ingenierías, 2012, p.9.
[3] PULIDO, Andrea; RINCON, Paulo y VELASQUEZ, Oscar. Diseño de políticas y controles para la seguridad de la información en pequeñas empresas con redes SOHO en el sector transporte de Bogotá. Tesis de Grado en Ingeniería de Sistemas: Universidad de San Buenaventura. Facultad de Ingenierías, 2010, p.9.

más empresas aceptan que sus clientes, empleados, socios y proveedores ingresen a sus sistemas de información. Adicionalmente, por el estilo de vida migratorio que existe en la actualidad, donde los empleados acceden remotamente a los sistemas de información, se les pide a estos llevar consigo información fuera de la empresa. Por consiguiente, es de vital importancia conocer ¿qué recursos necesitan ser protegidos en las empresas? con el fin de tener control sobre la información, ¿qué personal ingresa al sistema? y ¿cuáles son sus permisos en éste? No solo deben emplearse soluciones técnicas, sino también, deben hacer énfasis en la capacitación y toma de conciencia por parte del usuario sobre la seguridad de la información, además de la aplicación de medidas claramente definidas. Las medidas que se adopten para la seguridad de la información pueden también producir molestias a los usuarios. A menudo, las reglas y los procedimientos se tornan cada vez más difíciles de cumplir e implementar cuando crece la red. Por tanto, la seguridad de la información debe garantizar que los usuarios hagan uso adecuado de ella. Además, deben identificarse las principales vulnerabilidades para conocer y deducir el camino del atacante. La intención de este proyecto es proponer políticas y controles de seguridad de la información, así como dar una visión general de los posibles atractivos de los atacantes, clasificarlos y dar una percepción de las vulnerabilidades de los sistemas de información para saber cuál es la forma más apropiada para reducir el riesgo de ataques e intrusiones.

4.2 MARCO TEÓRICO

4.2.1 Seguridad de la Información: hace referencia a la confidencialidad, integridad y disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan[4], en la seguridad

[4] BLOG ESPECIALIZADO EN SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. ISO 27001: ¿Qué significa la Seguridad de la Información? [En línea]. Bogotá D.C.: Blog especializado. 2015. (Recuperado en septiembre 2017.) Disponible en http://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

Informática[5], el objetivo de la protección son los datos mismos y trata de evitar su perdida y modificación no autorizado. La protección debe garantizar en primer lugar la confidencialidad, integridad y disponibilidad de los datos, sin embargo, existen más requisitos como por ejemplo la autenticidad entre otros. El motivo o el motor para implementar medidas de protección, que responden a la seguridad de la Información, es el propio interés de la institución o persona que maneja los datos, porque la pérdida o modificación, le puede causar un daño (material o inmaterial).

4.2.2 Análisis de riesgo[6]: como primera medida la gestión de riesgo es el análisis el cual tiene como propósito determinar los componentes de un sistema que requieren protección, sus vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo. Existen diversidad de métodos para valorar un riesgo y al final, todos tienen los mismos retos las variables son difíciles de precisar y en su mayoría son estimaciones y llegan casi a los mismos resultados y conclusiones.

4.2.3 Proceso del análisis del riesgo: para implementar una política de seguridad en un sistema de información es necesario seguir un esquema lógico[7].

- Hacer inventario y valoración de los activos.
- Identificar y valorar la amenaza que puedan afectar a la seguridad de los activos.
- Identificar las medidas de seguridad existentes.
- Identificar y evaluar las vulnerabilidades de los activos a las amenazas que les afectan.
- Identificar los objetivos de seguridad de la organización.

[5] ERB, Markus. Gestión de riesgo en la seguridad Informática facilitando el manejo seguro de la información en organizaciones sociales. [En línea]. España: Creative Commons Atribución. 2016. p.1 (Recuperado en septiembre 2017.) Disponible en https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion/
[6] Ibíd. p. 7.
[7] AGUILERA LOPEZ, Purificación. Óp. Cit.

- Determinar sistemas de medición de riesgo.
- Determinar el impacto que produciría un ataque.
- Identificar y seleccionar las medidas de protección

4.2.4 Política de seguridad: establece las directrices u objetivos de una empresa u organización con lo que respecta a la seguridad de la información, esta forma parte de la política general, lo cual debe de ser aprobada por la dirección general[8].

Su principal objetivo es concientizar a todo el personal de la organización o empresa, y en especial al directamente involucrado con el sistema de información, Dando a conocer lo principios y normas que rigen la seguridad de la entidad, para alcanzar los objetivos de la seguridad planificados.

Una política de seguridad contendrá los objetivos de la empresa en materia de seguridad del sistema de información, generalmente englobados en cuatro grupos:

- Identificar las necesidades de seguridad y los riesgos que amenazan al sistema de información, así evaluar los impactos ante un eventual ataque.

- Relacionar todas las medidas de seguridad que deben implementar para afrontar los riegos de cada activo o grupo de activos.

- Proporcionar una perspectiva general de las reglas y los procedimientos que deben aplicarse par a afrontar los riesgos identificados en los diferentes departamentos de la organización.

- Proporcionar una perspectiva general de las reglas y los procedimientos que deben aplicarse para afrontar los riesgos identificados en los diferentes departamentos de la organización.

[8] Ibíd. p.17

- Detectar todas las vulnerabilidades del sistema de información y controlar los fallos que se producen en los activos, incluidas las aplicaciones instaladas.

- Definir un plan de contingencia.

4.2.5 Auditoria: la auditoría es un análisis pormenorizado de un sistema de información que permite descubrir, identificar y corregir vulnerabilidades en los activos que lo componen y en los procesos que se realizan. Su finalidad es verificar que se cumplen los objetivos de la política de seguridad de la organización. Proporciona una imagen real y actual del estado de seguridad de un sistema de información[9].

Tras el análisis e identificación de vulnerabilidades, la perdona o equipo encargado de la auditoria emite un informe que contiene, como mínimo:

- Descripción de las características de los activos y procesos analizados.
- Análisis de las relaciones y dependencias entre activos o en el proceso de la información.
- Relación y evaluación de las vulnerabilidades detectadas en cada activo o subconjunto de activos y procesos.
- Verificación del cumplimiento de la normativa en el ámbito de la seguridad.
- Propuesta de medida preventiva y de corrección.

Para evaluar la seguridad de un sistema de información se necesita herramientas de análisis.

Manuales: observación de los activos, procesos y comportamientos, mediciones, entrevista, cuestionarios, cálculos, pruebas de funcionamiento.

[9] Ibíd. p.18

Software específico para auditoria: se le reconoce por la sigla CAAT (Comuter Assisted Audit Techniques). Los CATT son herramientas de gran ayuda para mejorar la eficiencia de la auditoria, pudiendo aplicarse sobre la totalidad o sobre una parte del sistema de información. Realizan pruebas de control y emiten informes en los que señalizan las vulnerabilidades y puntos débiles del sistema, así como las normativas que podrían estar incumpliéndose. La auditoría puede ser total, sobre todo el sistema de información, o parcial, sobre determinados activos o procesos[10]:. Esta puede realizarse por:

- Personal capacitado perteneciente a la propia empresa.
- Por una empresa externa especializada.

4.2.6 Metodología Magerit: MAGERIT[11] es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España. Actualizada en 2012 en su versión 3. Esta metodología contempla diferentes actividades enmarcadas a los activos que una organización posee para el tratamiento de la información. A continuación, se relacionan cada uno de los pasos que se deben contemplan en un proceso de análisis de riesgos, teniendo en cuenta un orden sistémico que permita concluir el riesgo actual en que se encuentra la empresa, los activos son todos los elementos que una organización posee para el tratamiento de la información (hardware, software, recurso humano, etc.). Magerit diferencia los activos agrupándolos en varios tipos de acuerdo a la función que ejercen en el tratamiento de la información. A la hora de realizar el análisis de riesgo el primer paso es identificar los activos que existen en la organización y determinar el tipo. Como se muestra en la tabla 1, se relacionan cada tipo de activos de seguridad de la información.

[10] Ibíd. p.18

[11] CORDERO MORENO, José Leonardo y GARCIA REYES, Yadimir Oswaldo. Análisis de riesgo y recomendaciones de seguridad de información del hospital E.S.E San Bartolomé de Capitanejo, Santander. Tesis de Grado Especialización en Seguridad Informática: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnologías e Ingenierías, 2016, p.19

Tabla 1. Relación de Activos de Seguridad de la información en la empresa "SOLTEC–ING S.A.S", con base a la metodología Margerit.

ID	NOMBRE CORTO	TIPO ACTIVO	ACTIVO
ID_01	AP	[HW][wap] punto de acceso inalámbrico	Tp-Link TL-WR840N
ID_02	Switch Principal	[HW] [switch] conmutadores	Switch tl-sf1016D
ID_03	Pc Escritorio Ventas	[HW] [pc] informática personal	Computadores de escritorio Lenovo Procesador Intel core i5, 4430S 2.70 Ghz de memoria Ram 6Gb Disco duro 500 Gb
ID_04	Impresora admin	[HW] [print] medios de impresión	Impresoras EPSON L555
ID_05	Impresora Ventas	[HW] [print] medios de impresión	Impresoras TMU
ID_06	Scaner	[HW] [scan] escáneres	
ID_07	Servidor	[HW] [pc] informática personal	Servidor HP ProLiant ML310e Gen8 V2 procesador Intel® Xeon® E5-2600 v2; memoria Ram máxima de 768 Gb
ID_08	Pc Escritorio admin	[HW] [pc] informática personal	Portátiles Lenovo Procesador: Intel Core i5 2410M (2300 MHz - 2900 MHz), RAM: 4 GB DDR3 (1066 MHz), Pantalla: 14.0" (1366x768), Almacenamiento: HDD 500 GB (5400 rpm)
ID_09	Tablet	[HW] [pc] informática personal	Tablet
ID_10	CCTV	[AUX] [LAN] red local	Cámaras de vigilancia
ID_11	Red telefónica	[HW] [PSTN] red telefónica	Teléfonos
ID_12	Software Contabilidad	[SW] [dbms]	Software Contable
ID_13	Antivirus	[SW] [av] anti virus	Antivirus
ID_14	Office	[SW] [office] ofimática	Paquete de office
ID_15	Disco Externo	[Media][electronic][disk] discos	Discos de 2TB
ID_16	USB	[Media][electronic][usb] memorias USB	Pen drive Memoria: Flash
ID_17	Archivo	[Media][non_electronic][printed] material impreso	Carpetas con información
ID_18	Internet	[COM] [Internet] [wifi]	Servicio de internet
ID_19	Red	[COM] [wifi] red inalámbrica	Servicio de internet
ID_20	Red Telefónica	[COM] [ADSL] ADSL	Red telefónica ADSL
ID_21	Telefonía	[COM] [mobile] telefonía móvil	Telefonía móvil
ID_22	Red	[COM] [LAN] red local	Red de cableado estructurado
ID_23	Ups	[AUX][ups] sistemas de alimentación ininterrumpida	Ups de respaldo

Fuente: SOLTEC–ING S.A.S, 2017.

4.2.7 Valoración de los activos: cada activo de información tiene una valoración distinta en la empresa, puesto que cada uno cumple una función diferente en la generación, almacenamiento o procesamiento de la información. Pero a la hora de valorarlos no sólo debemos tener en cuenta cuanto el costó a la empresa, sino que además debemos contemplar el costo por la función que ella desempeña y el costo que genera ponerlo nuevamente en marcha en caso de que éste llegase a dañarse o deteriorarse.

4.2.8 Dimensiones de seguridad: es necesario definir unos criterios de valoración que permitan ubicar la posición en que se encuentra cada activo frente a cada dimensión. A continuación, se relacionan los criterios que se podrían tener en cuenta para valorar los activos con respecto a cada dimensión de seguridad, como se muestra en la siguiente tabla.

Tabla 2. Valoración del riesgo

VALORACIÓN DEL RIESGO			
	Nomenclatura	**Categoría**	**Valoración**
Valoración del riesgo	MA	**Critico**	21 a 25
	A	**Importante**	16 a 20
	M	**Apreciable**	10 a 15
	B	**Bajo**	5 a 9
	MB	**Despreciable**	1 a 4

Fuente: Magerit, versión 3.0 (2012)

Con base a los criterios anteriores, se puede hacer una valoración cualitativa de cada activo en relación a las dimensiones de seguridad contempladas en la metodología.

4.2.9 Amenazas (identificación y valoración): existen actualmente múltiples amenazas que pueden afectar los activos de una empresa, es importante identificarlas y determinar el nivel de exposición en la que se encuentra cada activo de información en la organización. Se considera una amenaza, a cualquier situación que pueda dañar o deteriorar un activo, impactando directamente cualquiera de las dimensiones de seguridad. La ISO/IEC 13335-1:2004 define que una "amenaza es la causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización" [12].

4.2.10 Etical Hacking: actualmente debemos tener en cuenta que las computadoras en todo el mundo son susceptibles de ser atacadas por crackers o hackers capaces de comprometer los sistemas informáticos y robar información valiosa, o bien borrar una gran parte de ella. Esta situación hace imprescindible conocer si estos sistemas y redes de datos están protegidos de cualquier tipo de intrusiones[13].

Por tanto, el objetivo fundamental del Ethical Hacking (hackeo ético) es explotar las vulnerabilidades existentes en el sistema de "interés" valiéndose de test de intrusión, que verifican y evalúan la seguridad física y lógica de los sistemas de información, redes de computadoras, aplicaciones web, bases de datos, servidores, entre otros.

Con la intención de ganar acceso y "demostrar" que un sistema es vulnerable, esta información es de gran ayuda a las organizaciones al momento de tomar las

[12] Ibíd. p. 21
[13] Ibíd. p. 22

medidas preventivas en contra de posibles ataques malintencionados. Dicho lo anterior, el servicio de Ethical Hacking consiste en la simulación de posibles escenarios donde se reproducen ataques de manera controlada, así como actividades propias de los delincuentes cibernéticos, esta forma de actuar tiene su justificación en la idea de que: "Para atrapar a un intruso, primero debes pensar como intruso"

4.2.11 Kali Linux: es una distribución de Linux basada en Ubuntu que incluye numerosas aplicaciones para realizar test de seguridad y análisis informático forense.

Las aplicaciones Kali linux se ha convertido en una distribución imprescindible para los administradores de sistemas y profesionales de la auditoria informática.

La distribución incluye utilidades para la auditoría de redes Wireless, scanners de puertos y vulnerabilidades, sniffers, archivos de exploits, entre otros. La mayoría de ellas actualizadas a sus últimas versiones, Algunas de esas herramientas son: dnsmap, Netmask, PsTools, TCtrace, Nmap, Protos, utilidades para la detección de vulnerabilidad en redes Cisco, SQL Inject, SMB-NAT, SNMP Scanner, Pirana, Dsniff, Hydra, Sing, WebCrack, Wireshark, NSCX, Airsnort, aircrack, BTcrack, SNORT, Hexedit, entre otros. Hasta completar más de 300.

4.2.12 NMAP: Nmap es un programa de código abierto utilizado para efectuar rastreo de puertos fue desarrollado inicialmente para Linux, aunque en la actualidad es multiplataforma. Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática, para ello Nmap envía unos paquetes definidos a otros equipos y analiza sus respuestas[14]:.

[14] Ibíd. p. 22

4.3 MARCO LEGAL

El desarrollo del proyecto está basado en el desarrollo y aplicación de estándares, metodologías y buenas prácticas para tener un uso eficaz y seguro del sistema de información de la empresa Suministros Eléctricos y soluciones Tecnológicas SOLTEC – ING SAS de Málaga Santander; logrando minimizar todos los riesgos y vulnerabilidades a los cuales está expuesto ese bien tan preciado e intangible; para ello la empresa me dio el aval para desarrollar este proyecto en sus instalaciones y sistemas informáticos**.** Adicionalmente a lo mencionado anteriormente existe en nuestro medio un fundamento jurídico que logra parametrizar la utilización de los sistemas de información, y toma medidas contra aquellas personas que intentan realizar ataques contra ellos[15].

Algunas de las leyes y normas de la legislación colombiana relacionada con seguridad de la información tomadas son:

Ley 1273 de 2009: por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley estatutaria 1266 de 2008: por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Decreto No. 2693 de 2012: por el cual se establecen los lineamientos generales de Gobierno en línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, Y se dictan otras disposiciones.

[15] Ibíd. p. 24

4.4 MARCO CONCEPTUAL

A continuación, se definen algunos términos que serán mencionados y utilizados en el desarrollo del proyecto de acuerdo con:

Activos: los activos a nivel tecnológico, son todos los relacionados con los sistemas de información, las redes y comunicaciones y la información en sí misma, Por ejemplo, los datos, el hardware, el software, los servicios que se presta, las instalaciones, entre otros.

Amenazas: las amenazas siempre existen y son aquellas acciones que pueden ocasionar consecuencias negativas en las operaciones de la organización, comúnmente se referencia como amenazas a las fallas, a los ingresos no autorizados, a los virus, a los desastres ocasionados por fenómenos físicos o ambientales, entre otros. Las amenazas pueden ser de carácter físico como una inundación, o lógico como un acceso no autorizado a la base de datos.

Análisis de riesgos: es una herramienta de diagnóstico que permite establecer la exposición real a los riesgos por parte de una organización. Este análisis tiene como objetivos la identificación de los riesgos (mediante la identificación de sus elementos), lograr establecer el riesgo total y posteriormente el riesgo residual luego de aplicadas las contramedidas en términos cuantitativos o cualitativos.

Impactos: son las consecuencias de la ocurrencia de las distintas amenazas y los daños por pérdidas que éstas puedan causar. Las pérdidas generadas pueden ser financiaras, económicas, tecnológicas, físicas, entre otras.

Infraestructura computacional: parte esencial para gestionar, administrar y almacenar la información indispensable dentro del normal funcionamiento de la Institución. 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 (Perafan y Caicedo, 2014)[16]

Magerit: es un tipo de metodología que es una guía de referencia para realizar procesos de análisis de riesgos al igual que provee lineamientos para la gestión de riesgos en sistemas informáticos y todos los aspectos que giran alrededor de ellos en las organizaciones para lograr muchas de las metas planteadas al interior de las mismas y buscando cumplir las políticas de buen gobierno. El proyecto en mención se basa en esta metodología para poder efectuar el proceso de análisis de riesgos logrando identificar los activos, las amenazas, determinar tanto los riesgos como los impactos potenciales y se recomiendan como proceder a elegir las salvaguardas o contra medidas para minimizar los riesgos (Perafan y Caicedo, 2014)[17]

Probabilidad: para establecer la probabilidad de ocurrencia se puede hacerlo cualitativa o cuantitativamente, considerando lógicamente, que la medida no debe contemplar la existencia de ninguna acción de control, o sea, que debe considerarse en cada caso que las posibilidades existen, que la amenaza se presenta independientemente del hecho que sea o no contrarrestada.

Riesgo: se puede definir como aquella eventualidad que imposibilita el cumplimiento de un objetivo, de manera cuantitativa e, riesgo es una medida de las posibilidades de incumplimiento o exceso del objetivo planteado. Así definido un riesgo conlleva a dos tipos de consecuencias: Ganancias o pérdidas.
En lo relacionado con tecnología, generalmente el riesgo se plantea solamente como amenaza, determinando el grado de exposición o el grado de una perdida (Por ejemplo, el riesgo de que se pierdan los datos por el daño del disco duro, virus informáticos entre otros).

[16] PERAFÁN RUIZ, John Jairo y CAICEDO CUCHIMBA Mildred. Análisis de riesgos de la seguridad de la información para la institución Universitaria Colegio Mayor del Cauca. Tesis de Grado Especialización en Seguridad Informática: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnologías e Ingenierías, 2014, p.28.
[17] Ibíd. p.26.

SGSI: un sistema de gestión de la seguridad de la información, es como su nombre lo expresa un sistema que se encarga de proveer una cantidad de mecanismos y herramientas basados en la norma ISO 27001 y tiene por objetivo conocer al interior de la institución a los que puede estar expuesta la información, define como se deben gestionar los riesgos y debe ser un marco de referencia para la institución el cual debe ser conocido por todo el personal y debe estar sometido a una revisión y a un proceso de mejora constante.(Norma Técnica Colombiana, 2009 Citado por Perafan y Caicedo 2014)[18]

Vulnerabilidades: son ciertas condiciones inherentes a los activos, o presentes en su entorno, que facilitan que las amenazas se materialicen y los llevan a la condición de vulnerabilidad. Las vulnerabilidades son de diversos tipos como, por ejemplo: la falta de conocimiento de un usuario, la transmisión a través de redes públicas, entre otros.

4.5 MARCO CONTEXTUAL

Nombre de la empresa: Suministros eléctricos y soluciones tecnológicas S.A.S. – (SOLTEC-ING S.A.S.)

Reseña histórica: SOLTEC-ING S.A.S., es una empresa privada, creada bajo representación legal mediante acta de creación y registrada en la Cámara de Comercio de Bucaramanga, el principal objetivo es mejorar la productividad de los clientes suministrando un completo portafolio de productos eléctricos acompañado de un servicio excepcional e innovador, la empresa trabaja con un equipo idóneo y capacitado en instalaciones de baja, media y alta tensión, así como todo lo relacionado con el ramo eléctrico.

Misión: SOLTEC-ING S.A.S es una empresa comprometida con nuestros clientes para entregarles soluciones innovadoras e integrales en materiales eléctricos,

[18] Ibíd. p. 27

Ofreciendo la más alta calidad y respaldo en cada uno de, los productos que comercializamos para satisfacer las necesidades y expectativas de nuestros clientes. Nuestro valor agregado es la atención y servicio personalizado cumpliendo con todas las normas técnicas de seguridad y protección ambiental requeridas.

Visión: en el 2018 se pretende posicionarse como una de las empresas líderes en la distribución eléctrica y afines asumiendo con entereza los retos tecnológicos de nuevos productos para así posicionarnos en el mercado como una empresa solida al servicio de nuestros clientes. La cual permitirá iniciar la certificación de procesos de calidad para mantener nuestra competitividad.

Política de Calidad: la empresa suministros eléctricos y soluciones tecnológicas (SOLTEC-ING S.A.S.) asume un compromiso social en la distribución de productos de alta calidad que cumplan con los estándares exigidos, buscando entregar lo mejor a nuestros clientes para cumplir con la misión y la visión.

Naturaleza Jurídica: la empresa SOLTEC-ING S.A.S. pertenece al sector privado, con existencia y representación legal mediante acta inscrita en la cámara de Comercio el día 30 de agosto de 2011, patrimonio independiente con domicilio en la ciudad de Málaga Santander.

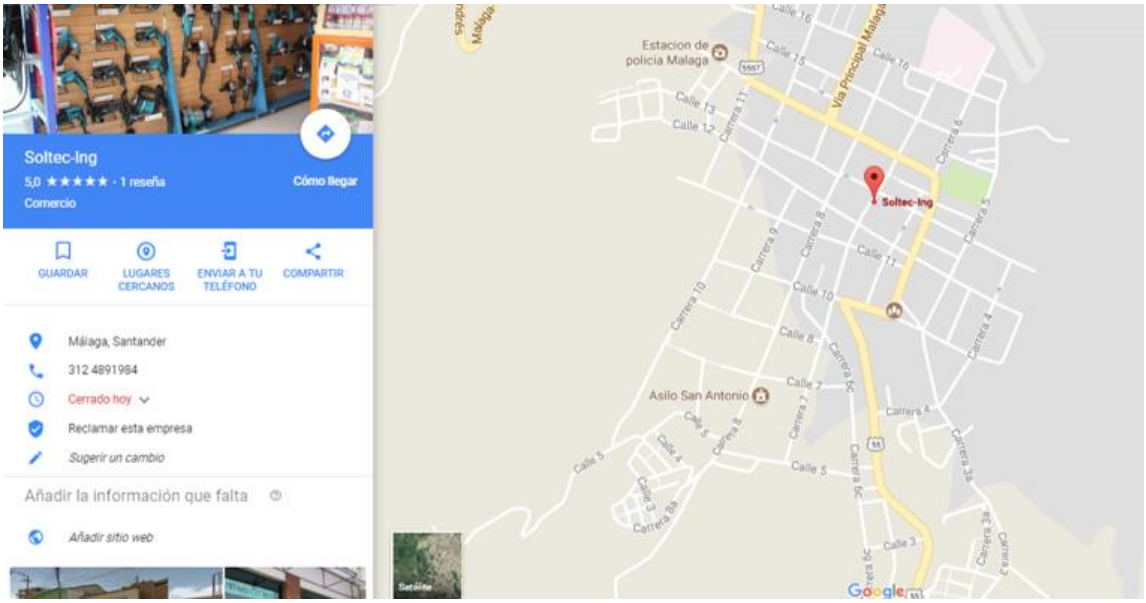
5. DISEÑO METODOLOGICO

Partiendo de la necesidad de determinar el estado de seguridad de la información mediante un diagnóstico en la empresa Suministros Eléctricos y Soluciones Tecnológicas “SOLTEC-ING S.A.S”, se desarrolló un estudio de tipo descriptivo aplicado, este tipo de investigación permite la búsqueda de una posible solución a las complicaciones generadas por causa de riesgos informáticos, tratando de dar una solución práctica a una problemática definida a través de respuestas a las necesidades que la investigación sugiere y que puede valerse de algún proceso sistemático para el desarrollo como tal del proyecto.

5.1 LOCALIZACION

El desarrollo de la investigación se llevó acabo en la empresa Suministros Eléctricos y Soluciones Tecnológicas “SOLTEC-ING S.A.S, la cual se encuentra ubicada en el Municipio de Málaga, Santander en el área urbana (Imagen 1)

Imagen 1. Localización de la empresa SOLTEC-ING S.A.S



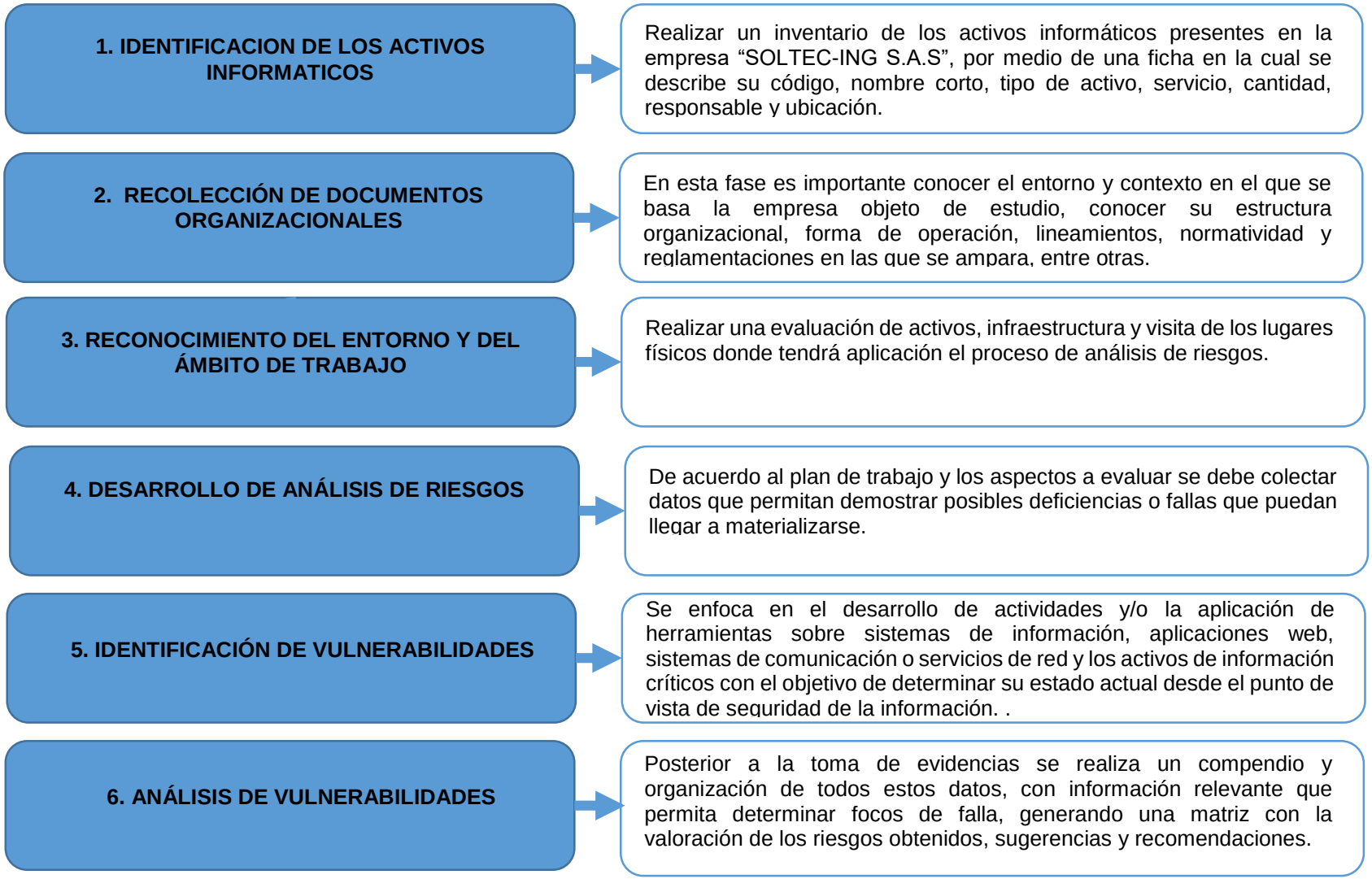
Fuente: Google maps, 2017.

5.2 METODOLOGIA

La metodología planteada pretende dar cumplimiento a los objetivos trazados en el estudio, para lo cual, se tuvo en cuenta el marco de referencia de la norma ISO 27001 que especifica, entre otros aspectos, los requerimientos y actividades que se deben desarrollar para el manejo de un Sistema de Gestión de Seguridad de la Información; adicional, durante el desarrollo del proyecto se utilizó el método de investigación de campo, permitiendo el análisis sistemático del problema en la realidad, con el fin de describirlo e interpretarlo logrando explicar sus causas y efectos. En este tipo de investigación, la información de interés fue recogida de forma directa de la fuente, mediante entrevistas directas.

Como se mencionó anteriormente, Teniendo en cuenta los requerimientos establecidos en la norma ISO 27001 para la ejecución del proyecto se establecieron las siguientes fases (Figura 1)

Figura 1. Fases del diseño metodológico para la empresa "SOLTEC-ING S.A.S".



Fuente: El autor

6. ANALISIS DE RESULTADOS

6.1 IDENTIFICACION DE LOS ACTIVOS INFORMATICOS

Los activos requieren de una identificación de amenazas permisibles y salvaguardas propias del activo, la tabla 3 muestra la relación que clasifica a los activos dentro de una jerarquía, determinando para cada uno un código que refleja su posición de orden, un nombre y una breve descripción de las características que recoge el epígrafe. Nótese que la pertenencia de un activo a un tipo no es excluyente de su pertenencia a otro tipo; es decir, un activo puede ser simultáneamente de varios tipos.

Tabla 3. Inventario de los activos informáticos

ID	NOMBRE CORTO	TIPO ACTIVO	ACTIVO	SERVICIO	CANT	RESPONSABLE	UBICACIÓN
ID_01	AP	[HW][wap] punto de acceso inalámbrico	Tp-Link TL-WR840N	Trafico de internet y mensajería	**1**	[P][adm]	[building] edificio
ID_02	Switch Principal	[HW] [switch] conmutadores	Switch tl-sf1016D	Intercomunicación de la red LAN	1	[P][adm]	[AUX] [furniture] mobiliario: armarios,
ID_03	Pc Escritorio Ventas	[HW] [pc] informática personal	Computadores de escritorio LenovoProcesador Intel core i5, 4430S 2.70 Ghz de memoria Ram 6Gb Disco duro 500 Gb	Equipos de facturación	4	[P][adm]	[building] edificio
ID_04	Impresora admin	[HW] [print] medios de impresión	Impresoras EPSON L555	Impresora del area contable	2	[P][adm]	[building] edificio
ID_05	Impresora Ventas	[HW] [print] medios de impresión	Impresoras TMU	Impresora post de ventas	3	[P][adm]	[building] edificio
ID_06	Scaner	[HW] [scan] escáneres		Digitalización de información			[building] edificio

Tabla 3. (Continuación)

ID_07	Servidor	[HW] [pc] informática personal	Servidor HP ProLiant ML310e Gen8 V2 procesador Intel® Xeon® E5-2600 v2; memoria Ram máxima de 768 Gb	Almacenamiento de información contable	1	[P][adm]	[building] edificio
ID_08	Pc Escritorio admin	[HW] [pc] informática personal	Portátiles Lenovo Procesador: Intel Core i5 2410M (2300 MHz - 2900 MHz), RAM: 4 GB DDR3 (1066 MHz), Pantalla: 14.0" (1366x768), Almacenamiento: HDD 500 GB (5400 rpm)	Equipo de apoyo administrativo	2	[P][adm]	[building] edificio
ID_09	Tablet	[HW] [pc] informática personal	Tablet	Equipo de mensajería, marketing, ventas	2	[P][adm]	[building] edificio
ID_10	CCTV	[AUX] [LAN] red local	Cámaras de vigilancia	Vigilancia	32	[P][com]	[building] edificio
ID_11	Red Telefonica	[HW] [PSTN] red telefónica	Teléfonos	mensajería	3	[P][ue]	[building] edificio
ID_12	Software Contabilidad	[SW] [dbms]	Software Contable	Software Contable Word Office empresarial	3	[P][ue]	[site] recinto
ID_13	Antivirus	[SW] [av] anti virus	Antivirus	Server small	1	[P][adm]	[mobile] plataformas móviles
ID_14	Office	[SW] [office] ofimática	Paquete de office	Office 2016 Profesional	1	[P][adm]	[mobile] plataformas móviles
ID_15	Disco Externo	[Media][electronic][disk] discos	Discos de 2TB	Repaldo información electrónica	2	[P][adm]	[backup] instalaciones de respaldo
ID_16	USB	[Media][electronic][usb] memorias USB	Pen drive Memoria: Flash	Respaldo información electrónica	5	[P][adm]	[backup] instalaciones de respaldo
ID_17	Archivo	[Media][non_electronic][printed] material impreso	Carpetas con información	Respaldo físico de Información	1	[P][adm]	[furniture] mobiliario: armarios
ID_18	Internet	[COM] [Internet] [wifi]	Servicio de internet	Proveedor de internet	1	[P][ue]	[mobile] plataformas móviles

Tabla 3. (Continuación)

ID_19	Red	[COM] [wifi] red inalámbrica	Servicio de internet	Servicio de internet y Mensajería	1	[P][adm]	[building] edificio
ID_20	Red Telefónica	[COM] [ADSL] ADSL	Red telefónica ADSL	Intercomunicación	1	[P][com]	[L][channel] canalización
ID_21	Telefonía	[COM] [mobile] telefonía móvil	Telefonía móvil	telefonía y mensajería	6	[P][com]	[building] edificio
ID_22	Red	[COM] [LAN] red local	Red de cableado estructurado	Transporte de datos	1	[P][com]	[channel] canalización
ID_23	Ups	[AUX][ups] sistemas de alimentación ininterrumpida	Ups de respaldo	Regulación de energía del Servidor	5	[P][sec]	[site] recinto

Fuente: El autor

6.1.2 Caracterización y valoración de los activos: este aspecto involucra la evaluación general de los procesos de la empresa, así no sean los directamente implicados en realizar el análisis del riesgo. Lo primero que se hace es identificar los activos de la empresa para su posterior valoración, asignado un grado de importancia de seguridad: disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad. La metodología Magerit contempla dos tipos de valoraciones, cualitativa y cuantitativa. Las cuales hacen referencia al cálculo de un valor a través de una escala cualitativa donde se valora el activo de acuerdo al impacto que puede causar en la empresa su daño o perdida, en consecuencia, la escala se refleja en la tabla 4 (Garavito, 2015)[19]:

[19] GARAVITO ROBLES, Hina Luz. Análisis y gestión del riesgo de la información en los sistemas de información misionales de una entidad del estado, enfocado en un sistema de seguridad de la información. Tesis de Grado Especialización en Seguridad Informática: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnologías e Ingenierías, 2015, p.24.

Tabla 4. Valoración del riesgo para la empresa SOLTEC-ING S.A.S

VALORACIÓN DEL RIESGO	
IMPACTO	**VALORACIÓN**
Muy alto (MA)	21 a 25
Alto (A)	16 a 20
Medio (M)	10 a 15
Bajo (B)	5 a 9
Muy Bajo (MB)	1 a 4

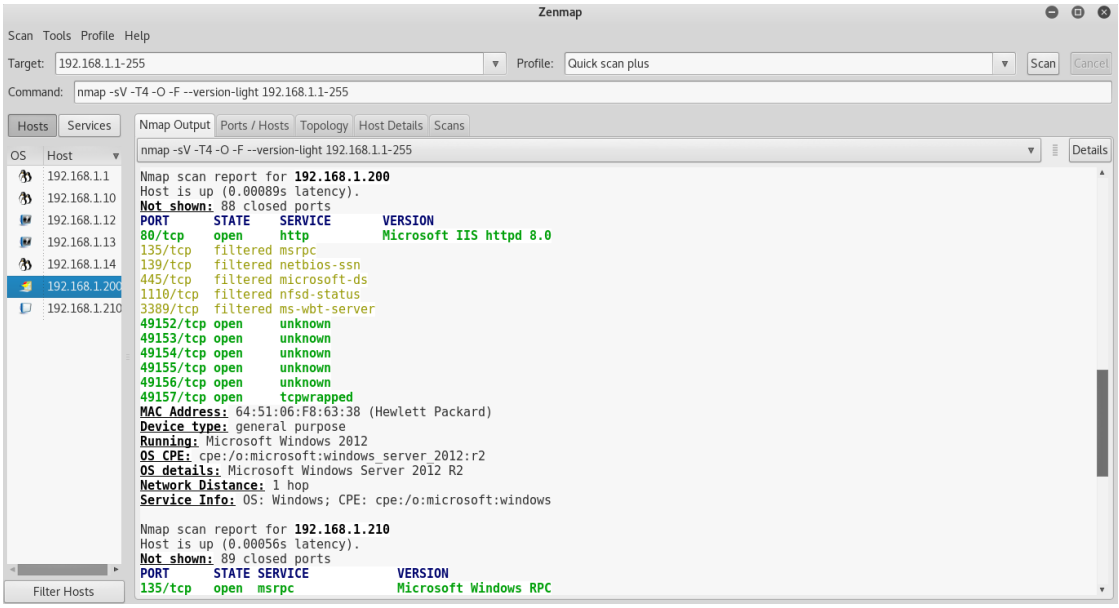
Fuente: Curso Sistema de Gestión de la Seguridad de Información SGSI, UNAD, citado por Garavito (2015).

6.2 ANALISIS DE VULNERABILIDADES

El estudio pretende dar a conocer algunas de las pruebas, análisis y resultados obtenidos con base a herramientas utilizadas tomando como guía la metodología Magerit v.3 para el análisis y gestión de los riesgos hallados, así como los posibles puntos críticos (fallas, amenazas o vulnerabilidades) que se pueden existir en la empresa SOLTEC-ING S.A.S, afectando la seguridad de la información, donde estos datos son el resultado de los movimientos internos y comerciales de la empresa los cuales pueden ser hackeados y sufrir modificaciones por la ausencia de protocolos, políticas, planes y mecanismos que garanticen la confiabilidad, confidencialidad y protección de la información e infraestructura tecnológica presente y futura de la empresa, teniendo en cuenta lo anterior se realizó una búsqueda de los focos vulnerables por medio de pruebas que utilizan herramientas tecnológicas como es el software de Zenmap y Kali- Linux, como observa en la

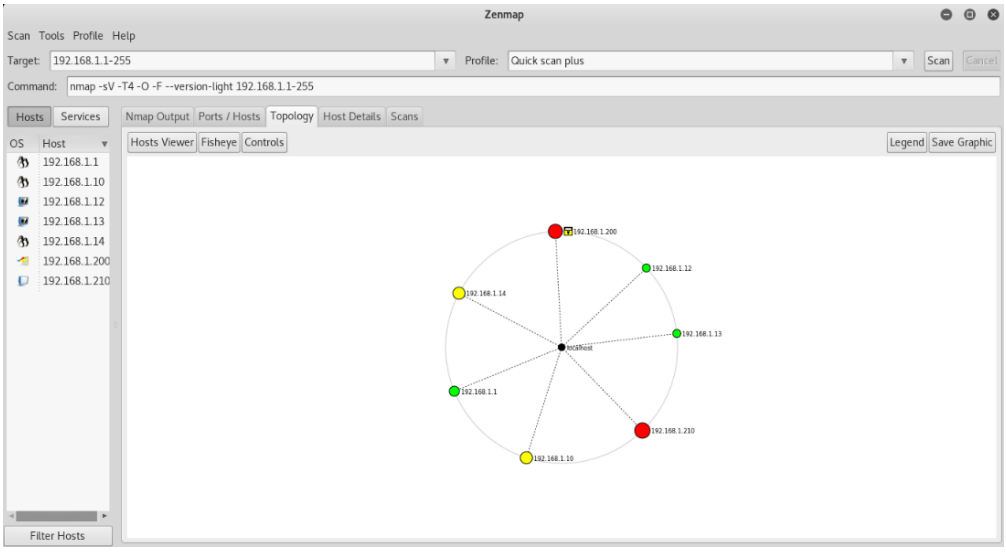
imagen 2, 3 y 4, pruebas que se ejecutaron al servidor principal para identificar los diferentes puertos susceptibles.

Imagen 2. Análisis de puertos a través del software Zenmap



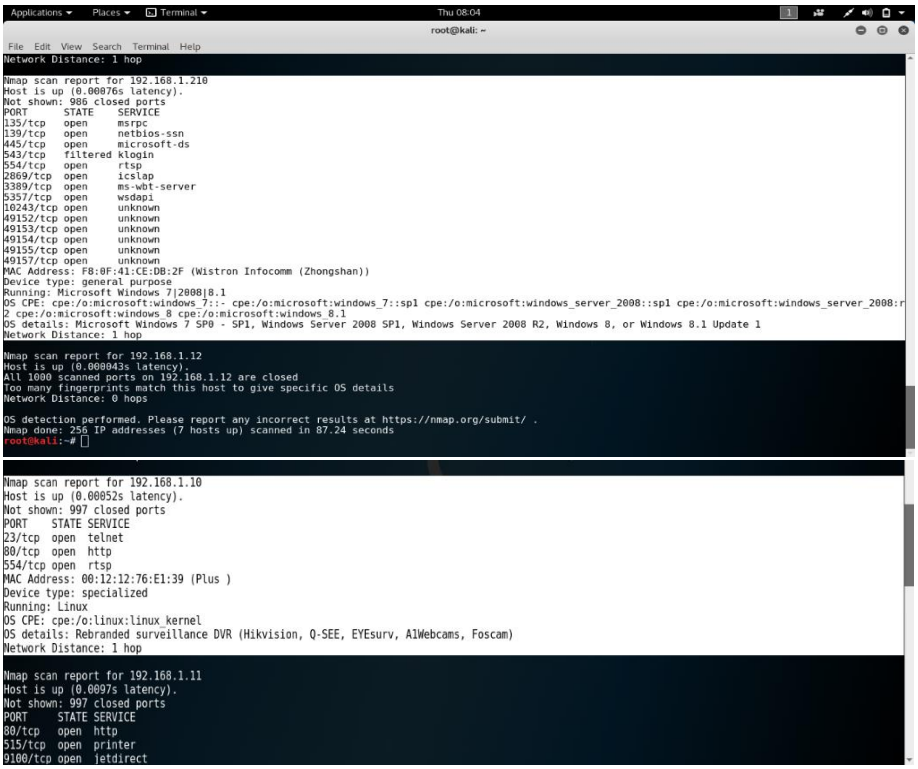
Fuente: Software Zenmap

Imagen 3. Análisis de Host a través del software Zenmap



Fuente: Software Zenmap

Imagen 4. Análisis de puestos a través del software Kali- Linux

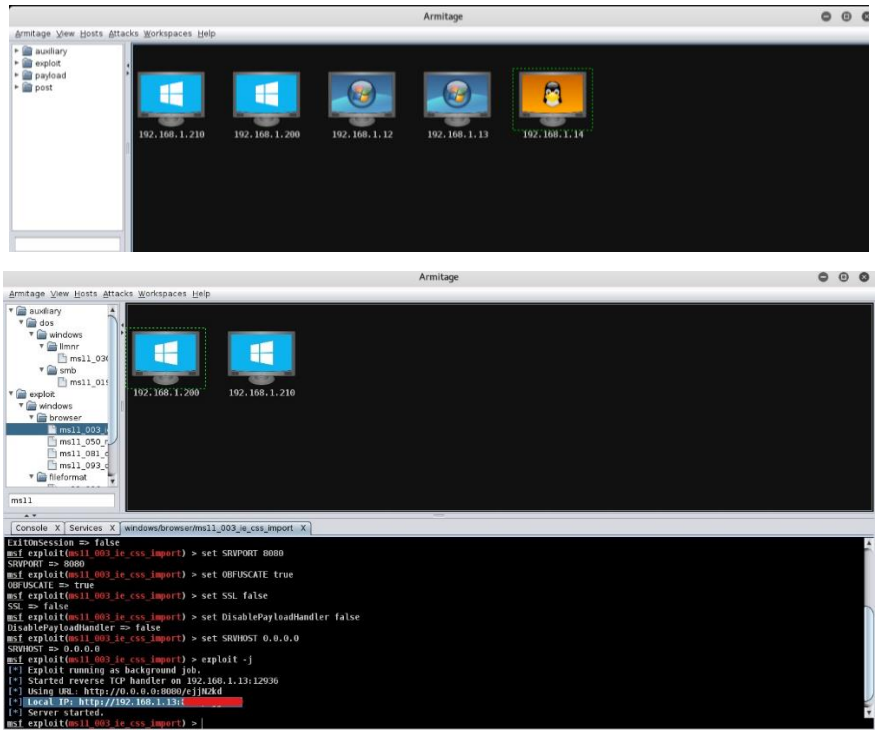


Fuente: Software Kali- Linux

6.2.1 Prueba afectada: una vez escaneados los equipos por medio de los programas Zenmap y Kali- Linux, se identificaban los puertos susceptibles y servicios activos más relevantes, los cuales pasaban por una segunda prueba para determinar la vulnerabilidad de los mismos, detallando los servidores de web, encontrando diferentes aspectos como malas configuraciones, vulnerabilidades entre otras.

Adicional se aplicó el software armitage, que es una herramienta de programa Kali-Linux para complementar en detalle las vulnerabilidades del sistema, el cual realiza un escaneo a los hosts de la empresa, identificando las características de cada uno de ellos, alterno se ejecutó la herramienta nmap, la cual realiza una revisión de estado de puertos para corroborar los resultados de dichos programas y su correlación con los diagnósticos.

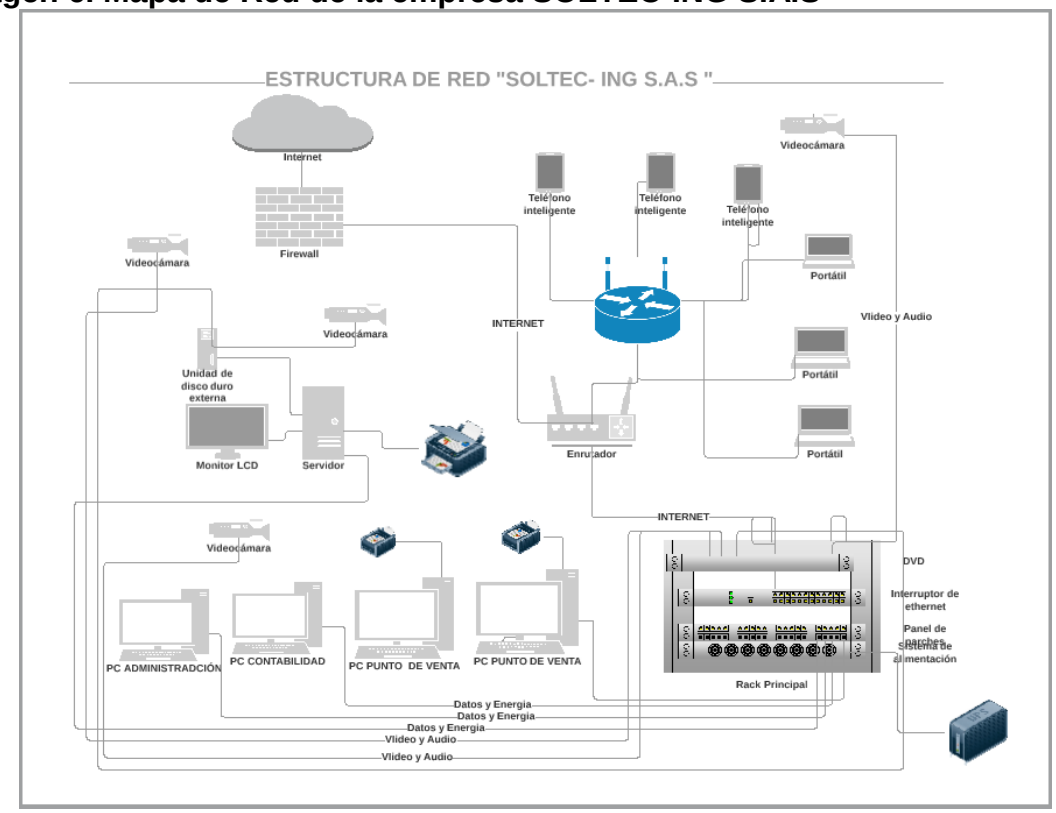
Imagen 5. Equipos activos en la red



Fuente: Software Armitage

6.2.2 Mapa de red

Imagen 6. Mapa de Red de la empresa SOLTEC-ING S.A.S



Fuente: Software Lucidchart, 2017.

6.3 IDENTIFICACION Y CARACTERIZACION DEL RIESGO

Apoyados en la metodología Magerit se realizó una matriz de análisis para los activos informáticos presentes en la empresa, evaluando los siguientes aspectos:

- Probabilidad de riesgo
- Impacto de riesgo
- Valoración del riesgo

El objetivo de esta actividad es determinar el alcance del daño producido sobre los activos de información en caso de ocurrir una amenaza, se procede a evaluar el grado de impacto que pueda mostrar los activos, dentro de las dimensiones de

valoración analizadas: Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad, haciendo uso de la siguiente tabla de doble entrada (ver tabla 5 y 6) propuestas por Magerit v.3. Los activos con calificación Media deberán ser re-evaluados para mejorar, cambiar o adaptar nuevos controles, los de calificación Alta y muy alta deberán ser objeto atención Urgente.

Tabla 5 Matriz de la valoración del riesgo en los activos de información (Magerit)

PROBABILIDAD DEL RIESGO

	Nomenclatura	Categoría	Valoración
Probabilidad	MA	Prácticamente seguro	5
	A	Probable	4
	M	Posible	3
	B	Poco probable	2
	MB	muy raro	1

IMPACTO DEL RIESGO

	Nomenclatura	Categoría	Valoración
Impacto	MA	Muy Alto	5
	A	Alto	4
	M	Medio	3
	B	Bajo	2
	MB	Muy Bajo	1

VALORACIÓN DEL RIESGO

IMPACTO						
	MA	5	10	15	20	25
	A	4	8	12	16	20
	M	3	6	9	12	15
	B	2	4	6	8	10
	MB	1	2	3	4	5
RIESGO		MB	B	M	A	MA

VALORACIÓN DEL RIESGO

	Nomenclatura	Categoría	Valoración
Valoracion del riesgo	MA	Critico	21 a 25
	A	Importante	16 a 20
	M	Apreciable	10 a 15
	B	Bajo	5 a 9
	MB	Despreciable	1 a 4

Fuente: Magerit versión 3.0 (2012)

Tabla 6. Valoración Cualitativa de la empresa "SOLTEC–ING S.A.S", con base a la metodología Margerit.

DATOS DEL ACTIVO DE INFORMACION	DIMENSION				
Nombre del activo de información	Dimensión Autenticidad(B / M /A / MA/ MB)	Dimensión Trazabilidad (B / M /A / MA/ MB)	Dimensión Confidencialidad (B / M /A / MA/ MB)	Dimensión Integridad (B / M /A / MA/ MB)	Dimensión Disponibilidad (B / M /A / MA/ MB)
[AP][wap] punto de acceso inalámbrico	M	M	B	M	M
[Switch Principal]	B	M	M	M	A
[Pc Escritorio Ventas]	A	M	A	B	M
[Impresora admin]	B	B	B	B	B
[Impresora Ventas]	M	M	B	M	A
[Scaner_ Principal]	B	B	B	B	B
[Servidor _Contable]	MA	MA	MA	MA	MA
[Pc Escritorio admin]	A	M	A	M	M
[Tablet_ Ventas]	B	B	B	B	B
[CCTV_seguridad]	B	B	B	B	B
[Red _telefónica]	B	B	B	B	B
[SW_Paquete_Contable]	MA	MA	MA	MA	MA
[SW_Antivirus]	MA	MA	MA	MA	MA
[Office]	M	M	M	M	M
[Aux_Disco Externo]	M	M	A	A	M
[Aux_memorias USB]	M	M	A	A	M
[Archivo_Fisico]	M	M	M	M	M
[Internet]	A	M	A	M	M
[Red] [wifi] red inalámbrica	A	M	A	M	M
[Red Telefonica]	B	B	B	B	B
[Telefonia] [mobile] telefonía móvil	B	B	B	B	B
[Red][LAN] red local	A	M	A	A	A
[Ups] sistemas de alimentación ininterrumpida	A	M	A	A	M

La valoración cualitativa muestra el estado actual de los activos, facilitando identificar el riesgo en el cual se encuentra cada uno de ellos, donde aquellos que presentan la letra MA son los más vulnerables.

Tabla 7. Valoración cuantitativa e la empresa "SOLTEC–ING S.A.S", con base a la metodología Margerit.

NOMBRE	RIESGO	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR
[AP][wap] punto de acceso inalámbrico	MEDIO	15	15	9	15	15	14
[Switch Principal]	MEDIO	9	15	15	15	20	15
[Pc Escritorio Ventas]	ALTO	20	15	20	9	15	16
[Impresora admin]	BAJO	9	9	9	9	9	9
[Impresora Ventas]	MEDIO	15	15	9	15	20	15
[Scaner_ Principal]	BAJO	9	9	9	9	9	9
[Servidor_Contable]	MUY ALTO	25	25	25	25	25	25
[Pc Escritorio admin]	ALTO	20	15	20	15	15	17
[Tablet_ Ventas]	BAJO	9	9	9	9	9	9
[CCTV_seguridad]	BAJO	9	9	9	9	9	9
[Red Telefonica]	BAJO	9	9	9	9	9	9
[SW_Paquete_Contable]	MUY ALTO	25	25	25	25	25	25
[SW_Antivirus]	MUY ALTO	25	25	25	25	25	25
[Office]	MEDIO	15	15	15	15	15	15
[Aux_Disco Externo]	ALTO	15	15	20	20	15	17
[Aux_memorias USB]	ALTO	15	15	20	20	15	17
[Archivo_Fisico]	MEDIO	15	15	15	15	15	15
[Internet]	ALTO	20	15	20	15	15	17
[Red] [wifi] red inalámbrica	ALTO	20	15	20	15	15	17
[Red Telefonica]	BAJO	9	9	9	9	9	9
[Telefonia] [mobile] telefonía móvil	BAJO	9	9	9	9	9	9
[Red][LAN] red local	ALTO	20	15	20	20	20	19
[Ups] sistemas de alimentación ininterrumpida	ALTO	20	15	20	20	15	18

En el análisis de riesgo cuantitativo se busca saber qué y cuanto hay, cuantificando en su mayoría los posibles aspectos, no trabaja sobre una escala discreta de valores, sino con números reales como se muestra en la tabla anterior.

Tabla 8. Mapa de calor

		IMPACTO				
		Insignificante	Menor	Moderado	Mayor	Catastrófico
IMPACTO	MUY ALTA		R2	R19, R16, R15, R13, R10, R3, R1	R23, R18, R12, R8, R7, R6, R5, R4	
	ALTA		R11			
	MEDIA					
	BAJA					
	MUY BAJA					
RIESGO		MUY BAJA	BAJA	MEDIA	ALTA	MUY ALTA
		PROBABILIDAD				

Teniendo en cuenta el mapa de calor, los riesgos de mayo amenaza se encuentran ubicados en los activos de informáticos denominados: R4: impresoras administrador, R5:impresora de ventas, R6:scanner principal, R7 servidor contable, R8: pc escritorio de administración , R12 paquete contable, R18: red de comunicación (internet) y R23: sistemas de equipamiento auxiliar (sistemas de alimentación ininterrumpidas), los cuales requieren de mayor control en la seguridad, adicional se puede observar que no se encuentran riesgos catastróficos, siendo un aspecto positivo para la empresa, como se muestra en el anexo b de amenaza-plan de tratamiento.

6.4 DECLARACIÓN DE APLICABILIDAD

Posterior al tratamiento de los riesgos se construyó la declaración de aplicabilidad, el cual es un elemento para la implementación de modelos de seguridad y privacidad de la información, indicando si los objetivos de control se encuentran implementados y activos como se muestra en el anexo C.

6.5 POLITICAS DE SEGURIDAD INFORMATICA

Antes de presentar la política de seguridad informática para la empresa SOLTEC-ING S.A.S, es importante mencionar que su diseño está basado bajo la guía que propone el Ministerio de Tecnologías de la Información y Comunicaciones (MINTIC)[20], ya que contempla los principios básicos a tener en cuenta en su elaboración dentro de la planeación del sistema de gestión de seguridad de la información en una entidad.

La empresa de Suministros eléctricos y soluciones tecnológicas “SOLTEC-ING S.A.S”, en el interés de mantener protegida la información que allí se genera, busca mantener un equilibrio en el ejercicio de sus deberes en los aspectos referentes en el marco legal, de la mano con la misión y visión de la empresa. Para “SOLTEC-ING S.A.S”, la seguridad de la información busca reducir al máximo las vulnerabilidades sobre sus activos, iniciando con la identificación de puntos críticos, de forma sistematizada de tal forma que logre mantener un nivel confianza y seguridad que responda a la integridad y privacidad, conforme a las necesidades identificadas.

6.5.1 Finalidad de la política: con la creación de la política de seguridad informática, se genera control de los documentos y la información, es por ello que la política aplica a la empresa según como se precise el alcance, donde sus empleados, distribuidores y demás personal vinculado aprueben e implementen los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI, las cuales estarán determinadas por las siguientes premisas:

- Reducir el riesgo en las funciones más importantes de la empresa.

[20] MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES. Guía 2. Elaboración de la política general de seguridad y privacidad de la información. [En línea]. Bogotá D.C.: MINTIC. 2016. (Recuperado en noviembre 2017.) Disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

- Llevar a cabo los principios establecidos para el manejo de la seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener y fortalecer la confianza del personal relacionado con la empresa (clientes, socios y empleados).
- Aplicar y apoyar las alternativas de innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer e implementar las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fomentar la cultura de seguridad de la información en el personal de SOLTEC-ING S.A.S
- Garantizar la continuidad del negocio frente a incidentes.
- La empresa de Suministros eléctricos y soluciones tecnológicas ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

6.5.2 Alcance/Aplicabilidad: la política de seguridad para la empresa “SOLTEC-ING S.A.S”, acopla en forma conjunta a sus funcionarios, distribuidores y demás personal vinculado, infundiendo la importancia del manejo de la información y documentos a fines como un activo estratégico, de tal forma que requiere de control para lograr los objetivos de la empresa.

6.5.3 Nivel de cumplimiento: el personal relacionado con la empresa según su alcance y aplicabilidad tienen el compromiso de aplicar la política. A continuación, se implantan las 12 políticas de seguridad que soportan el SGSI de la empresa “SOLTEC-ING S.A.S”:

1. SOLTEC-ING S.A.S en búsqueda de controlar la seguridad de la empresa ha identificado e implementado un Sistema de Gestión de Seguridad de la Información, basado en criterios que apuntan a las necesidades de la empresa y sus exigencias.

2. La responsabilidad y compromiso de los funcionarios de la empresa frente a la seguridad de la información será definidos, compartidos, divulgados y aceptados.

3. La empresa de Suministros eléctricos y soluciones tecnológicas debe asegurar la información de tal forma que minimice riegos en los procesos de negocio y activos de información que hacen parte de los mismos.

4. La empresa protegerá la información que se genere en cada proceso, mitigando las vulnerabilidades de acuerdo a los aspectos: financieros, técnicos o legales por causa errores en el proceso, requiriendo de controles de seguridad oportunos.

5. . SOLTEC-ING S.A.S resguardará su información de las amenazas originadas por parte del personal.

6. Amparar las estructuras de procesamiento tecnológico que toleran los procesos críticos.

7. La empresa SOLTEC-ING S.A.S explorará la operación de sus procesos de negocio respondiendo por la seguridad de los recursos y las redes que generen información

8. La empresa efectuará control de acceso de los datos, técnicas y recursos de red.

9. SOLTEC-ING S.A.S buscará la integridad en los procesos de acuerdo al ciclo de vida de los sistemas de información.

10. La empresa por medio de una adecuada gestión en los procesos de seguridad y control en las debilidades asociadas con el sistema de datos busca mejorar la eficiencia y sus riesgos.

11. La empresa de Suministros eléctricos y soluciones tecnológicas asegura el manejo y los procesos, con base en el impacto que lleguen a generar los eventos.

12. Y finalmente la empresa garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

Partiendo de lo anterior, el incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la empresa, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

6.5.4 Seguridad Relacionada Al Personal

6.5.4.1 Funcionarios

- El personal de SOLTEC-ING S.A.S, deben salvaguardar y proteger los registros e información manejada en la estructura tecnológica, preservando la seguridad de la red a nivel interno como externo.
- La información producida y/o maniobrada por los funcionarios es propiedad del SOLTEC-ING S.A.S.
- Todos los archivos que maneje el personal (programas, software, bases de datos, documentos y hojas de cálculo) se deben confirmar y escanear de tal forma que estén libres de virus, utilizando el software antivirus autorizado en la empresa SOLTEC-ING S.A.S. antes de ejecutarse.
- El personal deberá solo tener manejo de la información necesaria para el desarrollo de las actividades establecidas según su función.

- La información manipulada por el empleado debe ser reserva de la empresa.
- El usuario de la red SOLTEC-ING S.A.S debe aplicar las normas y disposiciones de seguridad informática que establece la empresa.
- El funcionario es el único responsable de la información y operaciones causadas al momento de manipulación de equipos de cómputo y de la red.

6.5.4.2 Capacitación

- El personal que use la red de datos de la empresa está en la obligación de recibir capacitación en temas básicos de seguridad de la información evitando la creación de focos de vulnerabilidad por desconocimiento de los funcionarios.
- Las medidas de seguridad que se apliquen a la empresa no deben comprometer los activos de información y se deben desarrollar en zonas de prueba y/o simuladores.
- Las capacitaciones de seguridad informática se manejarán muy acordes con la función del personal, usando los materiales idóneos para la misma.
- Las capacitaciones se realizarán en ambientes de prueba acordes con la realidad de la empresa.
- Es deber del personal asistir a las capacitaciones y obedecer a sus funciones.

6.5.4.3 Incidentes del personal

- Generar back-ups periódicamente para salvaguardar la información crítica de los datos significativos. Las copias de seguridad deben rotularse para ser almacenados, las cuales contengan su descripción general.
- Todo incidente de accidente de seguridad informática debe ser reportado, dando respuesta rápidamente al problema.
- Se documentará la novedad que ocurra en los formatos generados para el riesgo de la seguridad de la información, de tal forma que se realice el respectivo cambio en el control de la seguridad.

- El personal encargado directamente del sistema de incidencias (atención a usuarios) deberá priorizar las solicitudes y asignar los funcionarios adecuados para dar solución a los problemas.

Seguridad lógica

6.5.4.4 Control de acceso

- El funcionario encargado del manejo de la información proporcionará los documentos necesarios (formatos, guías, entre otros.) para el uso de los sistemas.
- De acuerdo a la norma ISO 27001. Los funcionarios de SOLTEC-ING S.A.S deben tener definidas sus actividades dentro de la empresa Por lo anterior, no es permito que de un trabajador a otro se intercambien roles y/o cuentas para accesos al sistema.

6.5.4.5 Administración de acceso de usuarios

- Los usuarios en su totalidad deben contar con un identificador único (ID de usuario) para su uso personal exclusivo.
- Si los funcionarios no han cumplido con los requerimientos no pueden tener acceso como usuario
- Es de vital importancia que la empresa implemente un sistema de administración de contraseñas, donde se contemple los siguientes parámetros:

✓ Establecer contraseñas individuales
✓ Estar actualizando las contraseñas de calidad para evitar vulnerabilidades.
✓ Mantener un registro de las últimas contraseñas utilizadas por el usuario, y evitar la reutilización de las mismas.
✓ Almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación.

✓ Avalar la técnica para acceder en el sistema de contraseñas, evitando el acceso a información temporal o en tránsito de forma no protegida.

6.5.4.6 Uso de contraseñas

Las contraseñas establecidas por los funcionarios deben cumplir con los siguientes requisitos:

- Usar una combinación alfanumérica
- la contraseña debe tener una longitud mínima de 10 caracteres.
- La contraseña debe tener un periodo de vigencia, luego deberá ser cambiada por una nueva y diferente a la anterior.
- No deberá usarse datos personales, acrónimos ni datos directamente relacionado con el usuario.

6.5.4.7 Uso del correo electrónico

- Los usuarios informáticos de empresa SOLTEC-ING S.A.S, deben manejar la información de los correos como información de propiedad de la empresa.
- Prohibido usar cuentas de correo electrónico asignadas a otros usuarios.
- El correo electrónico de la empresa es un servicio gratuito y la empresa no se responsabiliza por el mal uso que se dé.

6.5.4.8 Acceso a la red

- Cualquier funcionario que indague los recursos informáticos de la empresa SOLTEC-ING S.A.S. sin haber generado la orden se considerará como un ataque a la información y por tanto una falta grave la cual será reportada.
- El personal autorizado debe tener una cuenta de acceso a la red proporcionada por la administración y dependencia encargada del manejo de información.

- La empresa está en la terea de proporcionar los mecanismos de seguridad necesarios para realizar bloqueos, enrutamiento y filtrado de red, manteniendo el acceso controlado desde la red pública a la red interna y viceversa.

6.5.4.9 Backups

- La copia de seguridad se debe almacenar en un lugar exclusivo designado para este fin, garantizando su protección, evitando posibles daños o hurto de personal interno y/o externo.
- El personal a cargo de la seguridad informática está en la obligación de realizar procedimientos que generen o restauren los backups de información.
- Los backups son de obligatoriedad evitando cualquier tipo de incidente, este procedimiento debe ser documentado e informado.

6.5.4.10 Servidores

- El manejo y configuración de sistemas operativos de servidores es labor exclusiva del personal autorizado y de su administrador.
- Establecer perfiles de usuario y asignar exclusivamente el permiso en el acceso a los módulos que este debe manipular.
- El administrador tiene la responsabilidad de velar por la seguridad cada uno de los servicios que reposan en el servidor y eliminar los que por defecto se crean.

6.5.4.11 Equipos de cómputo

- Los equipos que se requieran para el manejo de información en la empresa deben estar configurados y hacer uso de cuentas de usuario y contraseña.
- Los usuarios de SOLTEC-ING S.A.S., no deben cambiar o reinstalar sin autorización los programas que están en los equipos.
- Es responsabilidad de los usuarios almacenar su información únicamente en la

partición del disco duro diferente, destinada para archivos de programas y sistemas operativos generalmente /c:/

6.5.4.12 Responsabilidades y procedimientos operativos

Al terminar la jornada laboral los usuarios deberán dejar apagados los equipos de cómputo evitando el acceso no autorizado a terceros

6.5.4.13 Protección contra software malicioso

- Para evitar la presencia de virus extraños y perjudiciales en el manejo de la información el personal debe utilizar los programas que solo han sido proporcionados en la empresa. En el caso de sospecha de infección de virus, debe dejar de usar inmediatamente el equipo y notificar la sospecha a la oficina.

- El usuario encargado del manejo de la información debe proporcionar software de protección como antivirus, antimalware y/o seguridad perimetral (firewall) para protección de la información manipulada y almacenada en los equipos de cómputo y servidores.

6.5.4.14 Mantenimiento

- Este aspecto es exclusivo del departamento de soporte técnico.
- Antes de realizar algún tipo de mantenimiento este debe ser reportado con anterioridad.
- El personal encargado del mantenimiento de equipos debe llevar el registro de los mantenimientos y cambios realizados a los equipos de cómputo y de red.

7. DIVULGACION

con el fin de dar a conocer el trabajo de investigación realizado en la empresa Suministros Eléctricos y soluciones Tecnológicas “SOLTEC-ING SAS” de Málaga Santander, se realizaron las siguientes actividades:

- Campaña informativa mediante afiches y carteles dirigidas a la comunidad estudiantil de la UNAD y demás personas interesadas en conocer dicho trabajo.
- Extensión del trabajo al personal de la empresa Suministros Eléctricos y soluciones Tecnológicas “SOLTEC-ING SAS”, con las medidas de seguridad procedentes de este proyecto, siendo aprobada por el gerente de la empresa en cuanto haya sido aprobado.
- Posterior a su socialización en la empresa, se considera oportuno reuniones de capacitación al personal vinculado con el fin de mitigar las vulnerabilidades encontradas en el estudio.

8. CONCLUSIONES

Se identificó los activos presentes en la empresa con la finalidad de conocer y evaluar los riegos en el sistema de información, para lo cual se implementó los controles de acuerdo a la norma ISO 27001, encargados de minimizar las ocurrencias de impactos asociados a las vulnerabilidades en el manejo de los datos en la empresa Suministros Eléctricos y Soluciones Tecnológicas “SOLTEC–ING S.A.S” en Málaga Santander.

El uso de herramientas tecnológicas facilita la toma de decisiones dentro de la empresa, para lo cual el estudio implemento la metodología Magerit para el análisis de riesgo, garantizando la seguridad de los activos de información y el normal funcionamiento interno de la empresa, donde los puntos críticos al ser identificados facilitan la proposición de controles de seguridad, facilitando el manejo de la información y brindando soporte para el diseño del SGSI; encaminado a incrementar la confiabilidad, integridad y disponibilidad de la información

Mediante el análisis de riesgo de orden cualitativo, facilito conocer el grado de seguridad aplicada en la empresa SOLTEC-ING S.A.S, sugiriendo las salvaguardas necesarias con la finalidad de reducir los niveles de riesgo e impacto.

Finalmente, con el diseño de la política de seguridad se busca mejorar en los procesos, aplicando medidas correctivas y preventivas para reducir los niveles de riesgos existentes, facilitando el reconocimiento de riesgos residuales a los cuales aún se encuentra expuesto la empresa.

9. RECOMENDACIONES

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.

Con los resultados obtenidos en el presente trabajo se realizará la 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 scanner e identificación para generar correctivos.

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

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.

BIBLIOGRAFIA

AGUILERA LOPEZ, Purificación. Seguridad informática. Madrid: Editex, 2010. 240p. ISBN 8497717619

AGUIRRE CARDONA, Juan David y ARISTIZABAL BETANCOURT, Catalina. Diseño del sistema de gestión de seguridad de la información para el grupo empresarial La Ofrenda. Tesis de Grado: Universidad Tecnológica de Pereira. Facultad de Ingenierías, 2012, 84p.

BLOG ESPECIALIZADO EN SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. ISO 27001: ¿Qué significa la Seguridad de la Información? [En línea]. Bogotá D.C.: Blog especializado. 2015. (Recuperado en septiembre 2017.) Disponible en http://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

CORDERO MORENO, José Leonardo y GARCIA REYES, Yadimir Oswaldo. Análisis de riesgo y recomendaciones de seguridad de información del hospital E.S.E San Bartolomé de Capitanejo, Santander. Tesis de Grado Especialización en Seguridad Informática: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnologías e Ingenierías, 2016, 84p.

ERB, Markus. Gestión de riesgo en la seguridad Informática facilitando el manejo seguro de la información en organizaciones sociales. [En línea]. España: Creative Commons Atribución. 2016. (Recuperado en septiembre 2017.) Disponible en https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion/

GARAVITO ROBLES, Hina Luz. Análisis y gestión del riesgo de la información en los sistemas de información misionales de una entidad del estado, enfocado en un sistema de seguridad de la información. Tesis de Grado Especialización en Seguridad Informática: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnologías e Ingenierías, 2015, p.24.

MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES. Guía 2. Elaboración de la política general de seguridad y privacidad de la información. [En línea]. Bogotá D.C.: MINTIC. 2016. 25p. (Recuperado en noviembre 2017.) Disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. MAGERIT-versión 3.0 metodología de análisis y gestión de riesgos de los sistemas de información. [En línea]. Madrid (España).: Ministerio de Hacienda y Administraciones Públicas. 2012. 42p. (Recuperado en noviembre 2017.) Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1793-magerit-libro-iii.../file.html

PERAFÁN RUIZ, John Jairo y CAICEDO CUCHIMBA Mildred. Análisis de riesgos de la seguridad de la información para la institución Universitaria Colegio Mayor del Cauca. Tesis de Grado Especialización en Seguridad Informática: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnologías e Ingenierías, 2014, 132p.

PULIDO, Andrea; RINCON, Paulo y VELASQUEZ, Oscar. Diseño de políticas y controles para la seguridad de la información en pequeñas empresas con redes SOHO en el sector transporte de Bogotá. Tesis de Grado en Ingeniería de Sistemas: Universidad de San Buenaventura. Facultad de Ingenierías, 2010, 120p.

ANEXOS

Anexo A. Resumen RAE

1. Información General	
Título del documento	ANÁLISIS DE CAUSAS DE RIESGOS EN LA PROTECCION DE LA INFORMACIÓN DE LA EMPRESA SOLTEC-ING Y RECOMENDACIONES DE SEGURIDAD
Autor	ORTIZ MANRIQUE EDWIN OMAR
Director	ZAMBRANO HERNÁNDEZ LUIS FERNANDO
Palabras Claves	Seguridad Informática, Vulnerabilidad, Riesgo, Análisis, Empresa, Datos, Hackeo, hackers.

2. Descripción
Trabajo de grado para optar al título de: Especialista en Seguridad Informática. Universidad Nacional Abierta y a Distancia UNAD.

3. Fuentes
AGUILERA LOPEZ, Purificación. Seguridad informática. Madrid: Editex, 2010. 240p. ISBN 8497717619 AGUIRRE CARDONA, Juan David y ARISTIZABAL BETANCOURT, Catalina. Diseño del sistema de gestión de seguridad de la información para el grupo empresarial La Ofrenda. Tesis de Grado: Universidad Tecnológica de Pereira. Facultad de Ingenierías, 2012, 84p. BLOG ESPECIALIZADO EN SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. ISO 27001: ¿Qué significa la Seguridad de la Información? [En línea]. Bogotá D.C.: Blog especializado. 2015. (Recuperado en septiembre 2017.) Disponible en http://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

CORDERO MORENO, José Leonardo y GARCIA REYES, Yadimir Oswaldo. Análisis de riesgo y recomendaciones de seguridad de información del hospital E.S.E San Bartolomé de Capitanejo, Santander. Tesis de Grado Especialización en Seguridad Informática: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnologías e Ingenierías, 2016, 84p.

ERB, Markus. Gestión de riesgo en la seguridad Informática facilitando el manejo seguro de la información en organizaciones sociales. [En línea]. España: Creative Commons Atribución. 2016. (Recuperado en septiembre 2017.) Disponible en https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion/

GARAVITO ROBLES, Hina Luz. Análisis y gestión del riesgo de la información en los sistemas de información misionales de una entidad del estado, enfocado en un sistema de seguridad de la información. Tesis de Grado Especialización en Seguridad Informática: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnologías e Ingenierías, 2015, p.24.

MINISTERIO DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIONES. Guía 2. Elaboración de la política general de seguridad y privacidad de la información. [En línea]. Bogotá D.C.: MINTIC. 2016. 25p. (Recuperado en noviembre 2017.) Disponible en https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PUBLICAS. MAGERIT-versión 3.0 metodología de análisis y gestión de riesgos de los sistemas de información. [En línea]. Madrid (España).: Ministerio de Hacienda y Administraciones Públicas. 2012. 42p. (Recuperado en noviembre 2017.) Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1793-magerit-libro-iii.../file.html

PERAFÁN RUIZ, John Jairo y CAICEDO CUCHIMBA Mildred. Análisis de riesgos de la seguridad de la información para la institución Universitaria Colegio Mayor del Cauca. Tesis de Grado Especialización en Seguridad Informática: Universidad

Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnologías e Ingenierías, 2014, 132p.

PULIDO, Andrea; RINCON, Paulo y VELASQUEZ, Oscar. Diseño de políticas y controles para la seguridad de la información en pequeñas empresas con redes SOHO en el sector transporte de Bogotá. Tesis de Grado en Ingeniería de Sistemas: Universidad de San Buenaventura. Facultad de Ingenierías, 2010, 120p.

4. Contenidos

La empresa Suministros Eléctricos y soluciones Tecnológicas “SOLTEC-ING SAS” de Málaga Santander, en el manejo de su información no cuenta con un sistema de seguridad, por lo cual presenta riesgo en la administración de sus datos, ostentando un alto índice de inseguridad, lo cual hace necesario realizar un análisis diagnóstico actual de las causas de riesgo, con el fin mitigar los impactos que conlleva la falta de protección en el sistema, desarrollando una propuesta de acuerdo a los hallazgos identificados, que permitan estrategias de prevención y seguridad.

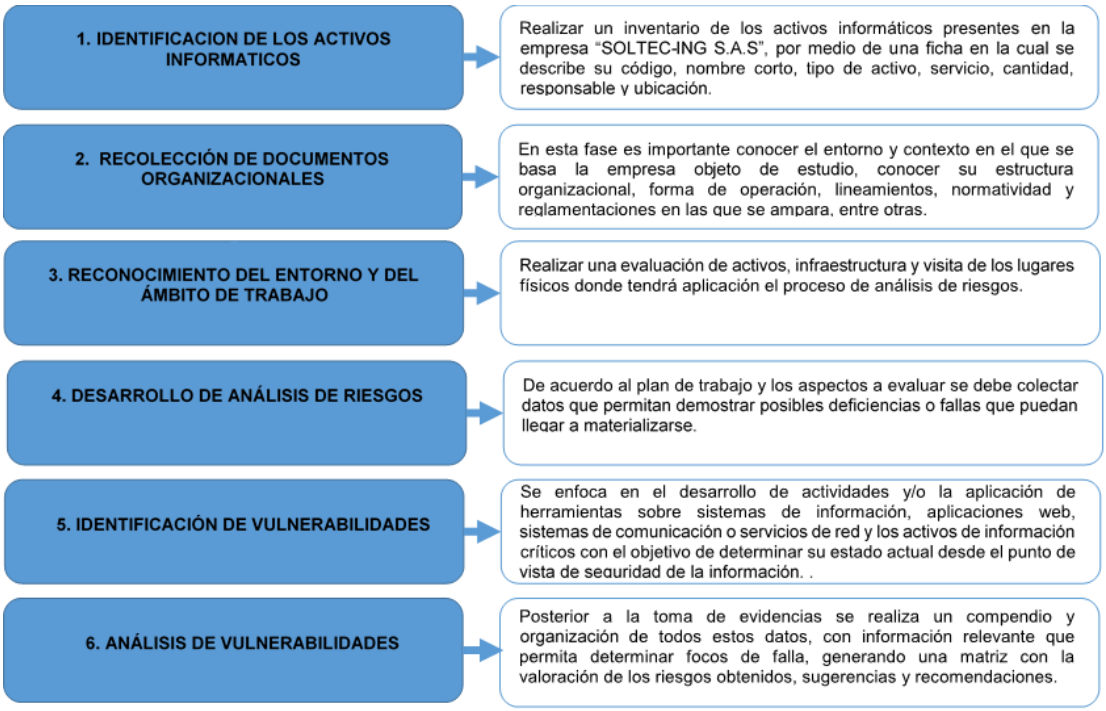
5. Metodología

Partiendo de la necesidad de determinar el estado de seguridad de la información mediante un diagnóstico en la empresa Suministros Eléctricos y Soluciones Tecnológicas “SOLTEC-ING S.A.S”, se desarrolló un estudio de tipo descriptivo aplicado, este tipo de investigación permite la búsqueda de una posible solución a las complicaciones generadas por causa de riesgos informáticos, tratando de dar una solución práctica a una problemática definida a través de respuestas a las necesidades que la investigación sugiere y que puede valerse de algún proceso sistemático para el desarrollo como tal del proyecto.

La metodología planteada pretende dar cumplimiento a los objetivos trazados en el estudio, para lo cual, se tuvo en cuenta el marco de referencia de la norma ISO 27001 que especifica, entre otros aspectos, los requerimientos y actividades que

se deben desarrollar para el manejo de un Sistema de Gestión de Seguridad de la Información; adicional, durante el desarrollo del proyecto se utilizó el método de investigación de campo, permitiendo el análisis sistemático del problema en la realidad, con el fin de describirlo e interpretarlo logrando explicar sus causas y efectos. En este tipo de investigación, la información de interés fue recogida de forma directa de la fuente, mediante entrevistas directas.

Fases del diseño metodológico para la empresa "SOLTEC-ING S.A.S".



6. Conclusiones

Se identificó los activos presentes en la empresa con la finalidad de conocer y evaluar los riegos en el sistema de información, para lo cual se implementó los controles de acuerdo a la norma ISO 27001, encargados de minimizar las ocurrencias de impactos asociados a las vulnerabilidades en el manejo de los

datos en la empresa Suministros Eléctricos y Soluciones Tecnológicas “SOLTEC–ING S.A.S” en Málaga Santander.

El uso de herramientas tecnológicas facilita la toma de decisiones dentro de la empresa, para lo cual el estudio implemento la metodología Magerit para el análisis de riesgo, garantizando la seguridad de los activos de información y el normal funcionamiento interno de la empresa, donde los puntos críticos al ser identificados facilitan la proposición de controles de seguridad, facilitando el manejo de la información y brindando soporte para el diseño del SGSI; encaminado a incrementar la confiabilidad, integridad y disponibilidad de la información

Mediante el análisis de riesgo de orden cualitativo, facilito conocer el grado de seguridad aplicada en la empresa SOLTEC-ING S.A.S, sugiriendo las salvaguardas necesarias con la finalidad de reducir los niveles de riesgo e impacto.

Finalmente, con el diseño de la política de seguridad se busca mejorar en los procesos, aplicando medidas correctivas y preventivas para reducir los niveles de riesgos existentes, facilitando el reconocimiento de riesgos residuales a los cuales aún se encuentra expuesto la empresa.

7. Recomendaciones

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.

Con los resultados obtenidos en el presente trabajo se realizará la 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 scanner e identificación para generar correctivos.

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

Elaborado por:	Ortiz Manrique Edwin Omar
Revisado por:	González García Salomón

Fecha de elaboración del Resumen:	17	Febrero	2018

Anexo B Análisis y gestión del riesgo de los sistemas de información de la empresa SOLTEC – ING.S.A.S

OBJETIVO	Determinar el estado actual de la seguridad informática de la empresa Suministros Eléctricos y Soluciones tecnológicas SOLTEC – ING. Mediante el análisis de riesgos y propuesta de solución.
ALCANCE	El SGSI, específicamente se aplicará al Área metropolitana de Málaga Santander. Este proyecto se basa en el diseño y la implementación de un análisis de riesgos dentro de la empresa, la documentación y diseño de las recomendaciones necesarias a través de políticas, procedimientos y controles de seguridad dentro del contexto de acceso y administración de la red, tanto interna como pública, abarcando dentro de esta solución el diseño de las herramientas de hardware y software, aplicando métodos y técnicas a utilizar para proteger la información, definición del marco teórico de la metodología, caracterización y evaluación de activos, identificación de vulnerabilidades, análisis y evaluación de Riesgos para finalmente realizar una propuesta aplicando un plan de acción y recomendaciones para controlar los riesgos hallados al aplicar el modelo seleccionado en la implementación de las políticas de Seguridad de la Información a la empresa Suministros Eléctricos y soluciones tecnológicas S.A.S. " SOLETC-ING S.A.S" en la vigencia del año 2017.
NOMBRE DE LA EMPRESA:	Suministros Eléctricos y Soluciones tecnológicas SOLTEC – ING.
CONTEXTO LEGAL	NTC ISO/IEC 27001 - NTC ISO/IEC 27005 - NTC ISO/IEC 31000
ENFOQUE METODOLOGICO	El enfoque de gestión de riesgos a aplicar está basado en la metodología **MAGERIT**
TRATAMIENTO	Se tratarán los riesgos cuyos niveles sean:
	• INACEPTABLE
	Se aceptarán los riesgos cuyo resultado después de la valoración de riesgos sean:
	• ADMISIBLE (3 – 43) • MODERADO (44 – 104)
	Niveles de aceptación del riesgo (1 a 5 aceptable (A), 6 a 15 moderado (M), 16 a 26 inaceptable(I))
	Una vez aplicados los controles se acepta un riesgo de residual en niveles APRECIABLE o IMPORTANTE
	Criticidad residual (1 a 4 despreciable (d), 5 a 9 baja (B), 10 a 15 apreciable (a), 16 a 20 importante (i), 21 a 25 crítico(C))

Activos y Valoración Cualitativa

MATRIZ DE LEVANTAMIENTO DE INFORMACION DE ACTIVOS
SEGÚN METODOLOGIA MAGERIT Y NORMA ISO 27001:2013

LEVANTAMIENTO DE INFORMACIÓN, INVENTARIO Y CLASIFICACiÓN DE ACTIVOS - SEGURIDAD DE LA INFORMACIÓN							
1	Nombre Entrevistado 1:	David Leonardo Parra		Cargo	[adm] administradores de sistemas	Proceso	Sistemas
2	Nombre Entrevistado 2:	Victor Hugo Ortiz		Cargo	[com] administradores de comunicaciones	Proceso	Seguridad y comunicaciones
3	Nombre Entrevistado 3:	Olga Yaneth Ortiz		Cargo	[dba] administradores de BBDD - Contabilidad	Proceso	Conatabilidad
4	Nombre Entrevistado 4:	Yefry Yorland Mayo		Cargo	[ui] usuarios internos	Proceso	Ventas
5	Nombre Entrevistado 5:	Jovino Oviedo Manrique		Cargo	[des] desarrolladores / programadores	Proceso	Desarrollo y software

INFORMACIÓN DE LOS ACTIVOS

No.	DATOS DEL ACTIVO DE INFORMACION			TIPO									DIMENSION					ATRIBUTOS									UBICACIÓN	
	Nombre del activo de información	Proceso propietario del activo	Responsable	[D] DATOS	[K] CLAVES CRIPTOGRAFICAS	[S] SERVICIOS	[SW] SOFTWARE	[HW] EQUIPAMIENTO	[COM] REDES DE	[Media] SOPORTE DE	[AUX] EQUIPAMIENTO AUXILIA	[L] INSTALACIONES	[P] PERSONAL	Dimensión Autenticidad(B / M /A / MA/ MB)	Dimensión Trazabilidad (B / M /A / MA/ MB)	Dimensión Confidencialidad (B / M /A / MA/ MB)	Dimensión Integridad (B / M /A / MA/ MB)	Dimensión Disponibilidad (B / M /A / MA/ MB)	¿Es activo de información de terceros o de clientes que debe protegerse?	¿Activo de información que debe ser restringido a un número limitado de empleados?	Activo de información que debe ser restringido a personas externas	Activo de información que puede ser alterado o comprometido para fraudes ó corrupción	Activo de información que es muy crítico para las operaciones internas	Activo de información que es muy crítico para el servicio hacia terceros	Activo de información que en caso de ser conocido, utilizado o modificado por alguna persona o sistema sin la debida autorización, impactaría negativamente a los sistemas y/o procesos de la empresa, de manera: Leve	Importante	Grave	Físico	Electrónico
1	[AP][wap] punto de acceso inalámbrico	Sistemas	David Parra					X					M	M	B	M	M	X	X	X	X	X	X			X	Administración	
2	[Switch Principal]	Sistemas	David Parra					X					B	M	M	M	A	X	X	X	X	X	X		X		Rack Principal	
3	[Pc Escritorio Ventas]	Sistemas	David Parra					X					A	M	A	B	M	X		X	X	X	X		X		Área de Ventas	
4	[Impresora admin]	Sistemas	David Parra					X					B	B	B	B	B			X				X			Área administrativa	
5	[Impresora Ventas]	Sistemas	David Parra					X					M	M	B	M	A	X	X	X	X			X			Área de Ventas	
6	[Scaner_ Principal]	Sistemas	David Parra					X					B	B	B	B	B							X			Área administrativa	
7	[Servidor_Contable]	Sistemas	David Parra			X							MA	MA	MA	MA	MA	X	X	X	X	X	X			X	Área administrativa	
8	[Pc Escritorio admin]	Sistemas	David Parra					X					A	M	A	M	M	X	X	X	X	X	X		X		Área administrativa	
9	[Tablet_ Ventas]	Sistemas	David Parra					X					B	B	B	B	B			X				X			Área de Ventas	
10	[CCTV_seguridad]	Seguridad	David Parra								X		B	B	B	B	B							X			Área Interna y externa	
11	[Red Telefonica]	Comunicaciónes	Victor Ortiz						X				B	B	B	B	B							X			Área Interna	
12	[SW_Paquete_Contable]	Sistemas	David Parra				X						MA	MA	MA	MA	MA	X	X	X	X	X	X			X		Instalado en el Servidor.
13	[SW_Antivirus]	Sistemas	David Parra				X						MA	MA	MA	MA	MA	X							X			Instalado en el Servidor y pc de la impresa.
14	[Office]	Sistemas	David Parra				X						M	M	M	M	M							X				Instalado en el Servidor y pc de la impresa.
15	[Aux_Disco Externo]	Sistemas	David Parra						X				M	M	A	A	M	X	X	X	X	X	X		X		Área administrativa	
16	[Aux_memorias USB]	Sistemas	David Parra						X				M	M	A	A	M	X	X	X	X	X	X		X		Área administrativa	
17	[Archivo_Fisico]	Contabilidad	Olga Ortiz								X		M	M	M	M	M	X	X	X	X	X	X			X	Área administrativa	
18	[Internet]	Sistemas	David Parra			X							A	M	A	M	M		X	X			X		X			Rack Principal
19	[Red] [wifi] red inalámbrica	Sistemas	David Parra			X							A	M	A	M	M	X	X	X	X	X	X		X			Área administrativa
20	[Red Telefonica]	Comunicaciónes	Victor Ortiz			X							B	B	B	B	B							X			Rack Principal	
21	[Telefonia] [mobile] telefonía móvil	Comunicaciónes	Victor Ortiz						X				B	B	B	B	B							X			Área Interna y externa	
22	[Red][LAN] red local	Sistemas	David Parra						X				A	M	A	A	A	X	X	X	X	X			X		Área Interna	
23	[Ups] sistemas de alimentación ininterrumpida	Seguridad	David Parra								X		A	M	A	A	M							X			Rack Principal	

Amenaza plan de tratamiento

MATRIZ DE ANALISIS Y TRATAMIENTO DE RIESGOS																													
IDENTIFICACIÓN DE AMENAZAS, VULNERABILIDADES, ANALISIS DE RIESGOS, ESTRATEGIA DE CONTROLES Y PLAN DE TRATAMIENTO A APLICAR																													
INFORMACIÓN DE LOS ACTIVOS DE INFORMACION																													
GESTION DE RIESGOS: ANALISIS DE RIESGOS Y TRATAMIENTO DE LOS RIESGOS																													
Activos de Informacion	No. De Amenazas y Vulnerabilidades	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodologia Magerit	Vulnerabilidades	Probabilidad de vulneracion (1 Muy raro, 2 poco probable, 3 posible, 4 probable, 5 practicamente seguro)	Calculo del riesgo neto (Valoracion del riesgo * probabilidad de vulneración)	Criticidad neta (1 a 4 despreciable (d) 5 a 9 baja (B), 10 a 15 apreciable (a) 16 a 20 importante (i), 21 a 25 critico(C))	Calificacion de Gestion (1 control no existe, 2 existe pero no efectivo, 3 efectivo pero no documentado, 4 efectivo y documentado)	Si la opción es 2 - 3 o 4 indique el Control aplicado actual	Riesgo residual (riesgo neto dividido entre la calificación de gestión)	Criticidad residual (1 a 4 despreciable (d), 5 a 9 baja (B), 10 a 15 apreciable (a), 16 a 20 importante (i), 21 a 25 critico(C))	Niveles de aceptación del riesgo (1 a 5 aceptable (A), 6 a 15 moderado (M), 16 a 25 inaceptable(I))	Requerimiento Legal	Obligación Contractual	Requerimiento de Negocio	Analisis de Riesgo	Exclusión	Plan de Tratamiento									
																				Transferir	Aceptar	Mitigar	Si el plan de tratamiento es MITIGAR, indique el control aplicado a partir de la norma ISO 27001			Descripción de la aplicación del control	Eliminar
[HW] EQUIPAMENTO INFORMÁTICO	1	[AP][wap] punto de acceso inalámbrico	14	[A6] Abuso de privilegios de acceso	Posible perdida de informacion	3	42	C	3	Acceso autorizado por Dirección MAC	14	A	M																
[HW] EQUIPAMENTO INFORMÁTICO	2	[Switch Principal]	15	[I6] Corte del suministro eléctrico	Abuso de privilegios de acceso	2	30	C	2	Monitoreo continua por CCTV	15	A	I			X						A9.1.2	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.		
[HW] EQUIPAMENTO INFORMÁTICO	3	[Pc Escritorio Ventas]	16	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Posible perdida de informacion /Falla en el funcionamiento.	3	48	C	1		48	C	I			X						A9.2.2	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.		
[HW] EQUIPAMENTO INFORMÁTICO	4	[Impresora admin]	9	[I5] Avería de origen físico o lógico	Falla en el funcionamiento	4	36	C	1		36	C	I			X						A11.2.4	Mantenimiento de los equipos.	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.		
[HW] EQUIPAMENTO INFORMÁTICO	5	[Impresora Ventas]	15	[I5] Avería de origen físico o lógico	Falla en el funcionamiento	4	60	C	1		60	C	I			X						A11.2.4	Mantenimiento de los equipos.	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.		
[HW] EQUIPAMENTO INFORMÁTICO	6	[Scaner_ Principal]	9	[I5] Avería de origen físico o lógico	Falla en el funcionamiento	4	36	C	1		36	C	I			X						A11.2.4	Mantenimiento de los equipos.	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.		
[HW] EQUIPAMENTO INFORMÁTICO	7	[Servidor_Contable]	25	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Posible perdida de informacion /Falla en el funcionamiento.	4	100	C	2	Suministro de energía continuo y estabilizado	50	C	I			X						A9.1.1	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 la seguridad de la información.		
[HW] EQUIPAMENTO INFORMÁTICO	8	[Pc Escritorio admin]	17	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Posible perdida de informacion /Falla en el funcionamiento.	4	68	C	2	Mantener actualizado el software y hardware mediante actualizaciones automáticas.	34	C	I			X						A9.1.1	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 la seguridad de la información.		
[HW] EQUIPAMENTO INFORMÁTICO	9	[Tablet_ Ventas]	9	[E25] Pérdida de equipos	Posible perdida de informacion /Falla en el funcionamiento.	1	9	B	1		9	B	M															
[AUX] EQUIPAMENTO AUXILIAR	10	[CCTV_seguridad]	9	[I5] Avería de origen físico o lógico	Falla en el funcionamiento.	3	27	C	2	Realizar back up periódicamente (8) y verificar su funcionamiento.	14	A	M															
[COM] REDES DE COMUNICACIONES	11	[Red Telefonica]	9	[I8] Fallo de servicios de comunicaciones	Suspensión del servicio	2	18	I	1		18	I	I			X						A9.1.2	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.		

[COM] REDES DE COMUNICACIONES	11	[Red Telefonica]	9	[I8] Fallo de servicios de comunicaciones	Suspensión del servicio	2	18	I	1		18	I	I			X						A9.1.2	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.		
[SW] SOFTWARE	12	[sw_Paquete_Contable]	25	[E2] Errores del administrador	Posible perdida de informacion	4	100	C	2	Generación de Backup General y Automático	50	C	I	X								A9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.		
[SW] SOFTWARE	13	[SW_Antivirus]	25	[A15] Modificación deliberada de la información	alteración intencional de la información	3	75	C	2	Actializacón permante y configuaracion de firewall	38	C	I				X					A9.4.4	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el usos de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.		
[SW] SOFTWARE	14	[Office]	15	[E20] Vulnerabilidades de los programas (software)	alteración intencionada del funcionamiento	1	15	A	3	Ejecutar actualizaciones automática disponibles	5	B	M													
[Media] SOPORTE DE INFORMACIÓN	15	[Aux_Disco Externo]	17	[E19] Fugas de información	Posible perdida de informacion	3	51	C	2	Uso exclusivo para almacenamiento de Backus y mantener su integridad fisica.	26	C	I				X					A12.3.1	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.		
[Media] SOPORTE DE INFORMACIÓN	16	[Aux_memorias USB]	17	[E19] Fugas de información	Posible perdida de informacion	3	51	C	2	Uso exclusivo del área de sistemas y revisión periódica con antivirus.	26	C	I				X					A12.3.1	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.		
[Media] SOPORTE DE INFORMACIÓN	17	[Archivo_Fisico]	15	[E19] Fugas de información	Posible perdida de informacion	1	15	A	4	Mantener organizado siguiendo estándares.	4	D	A													
[COM] REDES DE COMUNICACIONES	18	[Internet]	17	[I8] Fallo de servicios de comunicaciones	Suspensión del servicio	4	68	C	3	Mantener la restricción a usuarios.	23	C	I			X						A13.1.2	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 contraten externamente.		
[COM] REDES DE COMUNICACIONES	19	[Red] [wifi] red inalámbrica	17	[A5] Suplantación de la identidad del usuario	Abuso De Derecho	3	51	C	3	Cambio de contraseñas de acceso con frecuencia.	17	I	I			X						A9.1.2	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.		
[COM] REDES DE COMUNICACIONES	20	[Red Telefonica]	9	[I9] Interrupción de otros servicios y suministros esenciales	Suspensión del servicio	1	9	B	1		9	B	M													
[COM] REDES DE COMUNICACIONES	21	[Telefonia] [mobile] telefonía móvil	9	[I9] Interrupción de otros servicios y suministros esenciales	Suspensión del servicio	1	9	B	1		9	B	M													
[COM] REDES DE COMUNICACIONES	22	[Red][LAN] red local	19	[I8] Fallo de servicios de comunicaciones	Suspensión del servicio	1	19	I	3	Analizar el tráfico de paquetes comprobando su integridad.	6	B	M													
[AUX] EQUIPAMENTO AUXILIAR	23	[Ups] sistemas de alimentación ininterrumpida	18	[I5] Avería de origen físico o lógico	Suspensión del servicio	4	72	C	2	Monitoreo del estado de la disponibilidad.	36	C	I				X					A11.2.4	Mantenimiento de los equipos.	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.		

Anexo C. Política de aplicabilidad

		DECLARACIÓN DE APLICACBILIDAD.						
			Objeto de control o control selecionado Si/No	Razón de la Selección	Objetivo de control o control Implementado Si/No	Justificación de exclusión	Referencia	Aprobado por la alta deirección Firma director de la entidad
Dominio	A5	POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION						
	A5.1	Orientación de la dirección para la gestión de la seguridad de la información						
Control	A5.1.1	Políticas para la seguridad de la información	Si	Se adopta este control, puesto que 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.	No	N /A	Protocolopara las politicas de control de acceso	Si
Control	A5.1.2	Revisión de las políticas para la seguridad de la información.	Si	Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.	No	N /A	Protocolopara las politicas de control de acceso	Si
Dominio	A6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION						
	A6.1	Organización interna						
Control	A6.1.1	Roles y responsabilidades para la seguridad de la información	Si	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	No	N /A	Protocolos para las politicas de control de acceso	Si
	A6.2	Dispositivos móviles y teletrabajo						
Control	A6.2.1	Política para dispositivos móviles	Si	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	No	N /A	Guias para las politicas de control de acceso	Si
Control	A6.2.2	Teletrabajo	Si	Control: Se deben 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	N /A	protocolo para las politicas de control de acceso	Si

Dominio	A9	CONTROL DE ACCESO						
	A9.1	Requisitos del negocio para el control de acceso						
Control	A9.1.1	Política de control de acceso	Si	Se adopta este control, puesto que 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	N /A	Instructivo para las politicas de control de acceso	Si
	A9.2	Gestión de acceso de usuarios						
Control	A9.2.2	Suministro de acceso de usuarios	Si	Se adopta este control, puesto que se debe implementar un proceso de suministro de acceso formal de usuario para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	Si	N /A	Formato de solicitud de creacion de usuario	Si
	A9.4	Control de acceso a sistemas y aplicaciones						
Control	A9.4.2	Procedimiento de ingreso seguro	Si	Se adopta este control, puesto que cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro	Si	N /A	Intructivo para administracion de usuarios	Si
Control	A9.4.4	Uso de programas utilitarios privilegiados	Si	Se adopta este control, puesto que se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	Si	N /A	Instructivo de control estricto del uso de programas utilitarios	Si
Dominio	A10	CRIPTOGRAFIA						
	A10.1	Controles criptográficos						
Control	A10.1.1	Política sobre el uso de controles criptográficos	Si	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	No	N /A	Protocolos para las politicas sobre uso de contro criptografico	Si
Control	A10.1.2	Gestión de llaves	Si	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	N /A	Guia para las politicas sobre creación de llaves criptograficas	Si
Dominio	A11	SEGURIDAD FISICA Y DEL ENTORNO						
	A11.2	Equipos						
Control	A11.2.4	Mantenimiento de los equipos.	Si	Se adopta este control, puesto que los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Si	N /A	Mantenimiento preventivo y correctivo	Si
Control	A11.2.4	Mantenimiento de los equipos.	Si	Se adopta este control, puesto que los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Si	N /A	Mantenimiento preventivo y correctivo	Si

Dominio	A12	SEGURIDAD DE LAS OPERACIONES						
	A12.2	Protección contra códigos maliciosos						
Control	A12.2.1	Controles contra códigos maliciosos	Si	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	No	N /A	Guia de control de protección para prevenir codigos maliciosos.	Si
	A12.3	Copias de respaldo						
Control	A12.3.1	Respaldo de la información	Si	Se adopta este control, puesto que 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	N /A	Guia de proceso para salvagurdar información	Si
	A12.5	Control de software operacional						
Control	A12.5.1	Instalación de software en sistemas operativos	Si	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	Si	N /A	Circular interna reglamentando la restricción de software en lso sistemas operativos de la empresa.	Si
Dominio	A13	SEGURIDAD DE LAS COMUNICACIONES						
	A13.1	Gestión de la seguridad de las redes						
Control	A13.1.2	Seguridad de los servicios de red	Si	Se adopta este control, puesto que 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.	No	N /A	Procedimiento de Gestión de telecomunicaciones	Si
Control	A13.1.3	Separación en las redes	Si	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	No	N /A	Procedimiento de Gestión de telecomunicaciones	Si
Dominio	A14	Adquisición, desarrollo y mantenimiento de sistemas						
	A14.1	Requisitos de seguridad de los sistemas de información						
Control	A.14.2.4	Restricciones en los cambios a los paquetes de software	Si	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	N /A	Protocolopara las politicas de control de acceso	Si
Dominio	A16	GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION						
	A16.1	Gestión de incidentes y mejoras en la seguridad de la información						
Control	A16.1.1	Responsabilidades y procedimientos	Si	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	N /A	Formato de registro y seguimeinto	Si
Control	A16.1.5	Respuesta a incidentes de seguridad de la información	Si	Control: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	No	N /A	Formato de respuesta a incidentes de seguridad informatica.	Si
Control	A16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Si	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o impacto de incidentes futuros.	No	N /A	Circular interna informativas del evento.	Si

Control	A16.1.7	Recolección de evidencia	Si	Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	No	N /A	Formato de registro y seguimeinto	Si
Dominio	A18	CUMPLIMIENTO						
	A18.1	Cumplimiento de requisitos legales y contractuales						
Control	A18.1.1	Identificación de la legislación aplicable.	Si	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.	Si	N /A	Reglamento interno de la empresa	Si
Control	A18.1.2	Derechos propiedad intelectual (DPI)	Si	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.	Si	N /A	Reglamento interno de la empresa	Si
Control	A18.1.3	Protección de registros	Si	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	No	N /A	Reglamento interno de la empresa	Si
Control	A18.1.4	Privacidad y protección de información de datos personales	Si	Control: Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige e la legislación y la reglamentación pertinentes, cuando sea aplicable.	No	N /A	Reglamento interno de la empresa	Si
Control	A18.1.5	Reglamentación de controles criptográficos.	Si	Control: Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	No	N /A	Reglamento interno de la empresa	Si
	A18.2	Revisiones de seguridad de la información						
Control	A18.2.1	Revisión independiente de la seguridad de la información	Si	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 independientemente a intervalos planificados o cuando ocurran cambios significativos.	No	N /A	Reglamento interno de la empresa	Si
Control	A18.2.2	Cumplimiento con las políticas y normas de seguridad	Si	Control: 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.	No	N /A	Reglamento interno de la empresa	Si
Control	A18.2.3	Revisión del cumplimiento técnico	Si	Control: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.	No	N /A	Reglamento interno de la empresa	Si