DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA TECNOFACTORY S.A.S CON BASE EN LA NORMA ISO 27001:2013

ANA MARIA MARTINEZ JIMENEZ
MANUEL ALEJANDRO OVALLE HERNANDEZ

UNIVERSIDAD PILOTO DE COLOMBIA
DIRECCIÓN DE POSTGRADOS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2022

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA TECNOFACTORY S.A.S CON BASE EN LA NORMA ISO 27001:2013

ANA MARIA MARTINEZ JIMENEZ
MANUEL ALEJANDRO OVALLE HERNANDEZ

Proyecto de grado para optar por el título de Especialista en Seguridad Informática

Asesor:
Lorena Ocampo Correa
Ingeniera de Sistemas

UNIVERSIDAD PILOTO DE COLOMBIA
DIRECCIÓN DE POSTGRADOS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2022

Nota de aceptación:

Firma del presidente del jurado

Firma del Jurado

Firma del Jurado

Bogotá, D.C. octubre 2022

DEDICATORIA

Dedicamos este trabajo inicialmente a Dios que nos impulsó por este camino para lograr avanzar en la infinidad de escalas que tenemos que subir en nuestras vidas, al apoyo incondicional de nuestras familias.

Ana María Martínez Jiménez
Manuel Alejandro Ovalle Hernández

AGRADECIMIENTOS

Agradecemos a la universidad Piloto de Colombia y planta docente por los conocimientos impartidos especialmente a la ingeniera Lorena Ocampo por el apoyo brindado a lo lardo del desarrollo de proyecto y a la empresa Tecnofactory S.A.S por permitirnos desarrollar este proyecto en su organización.

CONTENIDO

LISTA DE CUADROS

pág

LISTA DE FIGURAS

pág.

GLOSARIO

ACTIVO DE INFORMACIÓN: cualquier elemento que tiene valor para la Organización. (Tecnología - Personas - Información)[1]

ACTIVOS DE SERVICIOS: servicios de computación y comunicaciones, servicios generales como por ejemplo iluminación, calefacción, energía y aire acondicionado.[2]

ACTIVOS DE SOFTWARE: software de aplicación, software del sistema, herramientas de desarrollo y utilidades.[3]

ACTIVOS FÍSICOS: equipos de computación, equipos de comunicaciones, medios removibles y otros equipos[4].

AMENAZA: causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.[5]

ANÁLISIS DE RIESGO: uso sistemático de la información para identificar las fuentes y estimar el riesgo para su correspondiente administración.[6]

ANTISPAM: son filtros automáticos para no recibir correo de remitente desconocido, no deseado o de tipo publicitario (correo basura)[7].

---

[1]ISO 27000.Es: Glosario [en línea]. Bogotá: ISO2700.Es, 2017 [fecha de consulta 28 de noviembre de 2021]. Disponible en: https://www.iso27000.es/glosario.html

[2] ISO 27000.Es: Gestión de activos [en línea]. Bogotá: ISO2700.Es, 2017 [fecha de consulta 28 de noviembre de 2021]. Disponible en: https://www.iso27000.es/iso27002_8.html

[3] Ibid.

[4] Ibid.

[5] [5]ISO 27000.Es: Glosario [en línea]. Bogotá: ISO2700.Es, 2017 [fecha de consulta 28 de noviembre de 2021]. Disponible en: https://www.iso27000.es/glosario.html

[6] (ISO GUÍA 73: 2009, IDT [en línea]. Bogotá: ISO 2009., 17 [fecha de consulta 28 de noviembre de 2021]. Disponible en: http://ftp.isdi.co.cu/Biblioteca/BIBLIOTECA%20UNIVERSITARIA%20DEL%20ISDI/COLECCION%20DIGITAL%20DE%20NORMAS%20CUBANAS/2015/nc%20iso%20guia%2073%20a2015%2017p%20iwk.pdf.

[7]Oficina de seguridad del internauta: Filtros de correo antispam: para que sirven y como configurarlos [en línea]. Bogotá: Oficina de seguridad del internauta [fecha de consulta 28 de noviembre de 2021]. Disponible en: https://www.osi.es/es/actualidad/blog/2018/09/26/filtros-de-correo-antispam-para-que-sirven-y-como-configurarlos

ANÁLISIS DE IMPACTO EMPRESARIAL (BIA - *BUSINESS IMPACT ASSESSMENT*): el propósito del BIA es crear un documento que ayude a entender el impacto que un desastre pueda tener sobre un negocio en particular.[8]

ATAQUE A *WEBSITE*: es una acción hostil efectuada contra el *Website*.[9]

ATAQUE DE DENEGACIÓN DEL SERVICIO: es la apropiación exclusiva de un recurso o servicio con la intención de evitar cualquier acceso de terceros. También es incluida en esta definición los ataques destinados a colapsar un recurso o sistema con la intención de destruir el servicio o recurso**.**[10]

BACK-UP: es una copia de los datos que se encuentran en un disco duro, y que se preservan en otro medio de almacenamiento (discos duros / *Datacenter*, etc.) con el fin de conservarlos y/o protegerlos en caso de posible daño y/o destrucción de la fuente original.[11]

BARRIDO DE PUERTOS: un barrido de puertos trata de identificar qué puertos TCP y UDP están abiertos en los equipos para aprovechar ciertos servicios que dependen de ellos para entrar en el sistema. Existen infinidad de herramientas de barrido de puertos accesibles en la red a cualquiera y ésta será una de las cosas que primero compruebe un atacante.[12]

CÓDIGO MALICIOSO: es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o Sistema de información sin el consentimiento de su propietario.[13]

COLABORADOR: persona que desempeña un cargo o trabajo y que a cambio de ello recibe un sueldo.[14]

COMITE: es un grupo de trabajo que, con arreglo a las leyes o reglas de una organización, institución o entidad, que tienen establecidas determinadas competencias.[15]

CONFIDENCIALIDAD: característica/propiedad en que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.[16]

---

[8] ISO 27000.Es: Glosario [en línea]. Bogotá: ISO2700.Es, 2017 [fecha de consulta 28 de noviembre de 2021]. Disponible en: https://www.iso27000.es/glosario.html
[9] Ibid.
[10] Ibid.
[11] Ibid.
[12] Ibid.
[13] Ibid.
[14] Ibid.
[15] Ibid.
[16] Ibid.

CONTROL: medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la Organización que pueden ser de naturaleza administrativa, técnica, y gestión o legal.[17]

CORRELACIONADOR DE EVENTOS: es la posibilidad de relacionar eventos entre sí, en pro de una finalidad específica. Muchas veces, sólo se menciona a la correlación como a una repetición de un mismo evento en el tiempo; o a la ejecución de una alerta, un aviso, o a una acción correctiva.[18]

CORTAFUEGOS (FIREWALL): es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.[19]

DENEGACIÓN DEL SERVICIO: es la imposibilidad de acceso a un recurso o servicio por parte de un usuario legítimo.[20]

EQUIPO DE EMERGENCIA (EDE): es un grupo de gestión flexible y móvil que puede ocuparse de cualquier plan de recuperación que sea necesario en cualquier sitio donde este la organización. Formado por miembros altamente cualificados del equipo directivo procedentes de áreas vitales dentro de la organización.[21]

PLAN DE CONTINUIDAD DEL NEGOCIO (BCP-BUSINESS CONTINUITY PLAN): es un plan documentado y probado con el fin de responder ante una emergencia de manera adecuada, logrando así el mínimo impacto a la operación del negocio de Tecnofactory S.A.S. El PCP es el encargado de continuar los procesos críticos indispensables para no detener el negocio a pesar de un desastre. Esto, para no desperdiciar recursos, tiempo y esfuerzos.[22]

PLAN DE CONTINGENCIA: es un subconjunto de un plan de continuidad de negocio (BCP), que contempla como reaccionar ante una contingencia que pueda afectar la disponibilidad o los servicios ofrecidos por los sistemas informáticos. Una contingencia puede ser un problema de corrupción de datos, suministro eléctrico, un problema de software o hardware, errores humanos, intrusión, etc.[23]

---

[17] ISO 27000.Es: Glosario [en línea]. Bogotá: ISO2700.Es, 2017 [fecha de consulta 28 de noviembre de 2021]. Disponible en: https://www.iso27000.es/glosario.html
[18] Ibid.
[19] Ibid.
[20] Ibid.
[21] Ibid.
[22] Ibid.
[23] Ibid.

INTRODUCCIÓN

Para las organizaciones la seguridad de la información está orientada a salvaguardar y proteger la información que es considerada como valiosa, crítica o sensible para el negocio; siendo uno de los activos más valiosos debe ser utilizado de forma adecuada, integra y oportuna e implica que sea administrado con una correcta gestión frente al control al debido acceso, tratamiento y uso.

Tecnofactory S.A.S es consciente de la gran pluralidad de amenazas existentes que día a día atentan contra la seguridad y la privacidad de la información, las cuales representan un riesgo altamente potencial que, al materializarse, puede ocasionar diversas afectaciones ya sea en pérdidas económicas, sanciones legales por acciones u omisiones, afectación de su reputación e imagen; que en estos momentos podría resultar catastrófico. Abonado a ello el cambiante entorno tecnológico en donde cada día se hace más compleja la administración y a su vez que todo esfuerzo para mitigar estas amenazas deben lograr alinearse de manera armónica a los objetivos y planes estratégicos de la organización.

Es por ello que este proyecto de grado tiene por objeto diseñar un sistema de gestión de seguridad de la información, teniendo en cuenta como marco de referencia la norma ISO 27001:2013 que proporciona un enfoque metodológico basado en buenas prácticas, para llevar a cabo la implementación en la empresa Tecnofactory S.A.S, con la que se logre mitigar, los riesgos frente a las amenazas a las que está expuesta y además le permitirá tener ventaja ante la competencia, mayor credibilidad y confianza ante los clientes, alianzas y futuros negocios.

1. JUSTIFICACIÓN

En Tecnofactory S.A.S una importante parte de la información se aloja de forma local en los equipos de los colaboradores, medios de almacenamiento y servidores de aplicación; recientemente se ha venido alojando gran parte de la información en servidores de Microsoft como repositorio de información en *SharePoint* e infraestructura en Azure DevOps. Si bien estos equipos solo son usados por personas internas de la compañía, están sujetos a múltiples factores de riesgo internos como externos, razón por la cual que se deben identificar las posibles amenazas o fraudes que puedan afectar la integridad, confidencialidad y disponibilidad de la información albergada en ellos.

Un sistema SGSI basado en la norma ISO 27001:2013 le permitirá a Tecnofactory S.A.S identificar los posibles riesgos de seguridad de la información a los que están expuestos actualmente, como virus, robos de información, de identidad y/o espionaje industrial, por nombrar algunos. Posteriormente establecer políticas, que conlleven a la esquematización de procesos, controles y una cultura al interior de la organización, lo que genera conciencia del impacto que esto puede desencadenar y con ello disminuir la probabilidad de que se materialicen los riesgos, adicionalmente se tendrá una base establecida para saber cómo gestionarlos.

El diseño del SGSI estará alineado a los objetivos estratégicos de la organización, su implementación logrará brindar confiabilidad y cultura del Sistema de Gestión de Seguridad de la Información a los colaboradores y terceros; brindando además confianza a sus clientes actuales, así como abrirá la puerta a nuevos mercados, al ser una empresa muy joven y con amplias ambiciones. El lograr articular la seguridad de la información en los procesos de la compañía de manera clara y concisa permitirá que pueda afrontar con más y mejores argumentos las brechas exigentes de los recientes desafíos de la ciberdelincuencia que enfrenta este país.

2. PLANTEAMIENTO DEL PROBLEMA

Tecnofactory S.A.S es una compañía dedicada a la transformación digital a través del desarrollo de software y soluciones tecnológicas aplicables a cualquier tipo de negocio; maneja proyectos de diseño personalizado de aplicaciones, actualización y modernización, desarrollo de aplicaciones web y móviles.

Tecnofactory S.A.S dentro de sus actividades ha estado expuesto a diversos riesgos como la recepción de correos maliciosos, que han servido como puente para la descarga de virus que en alguna oportunidad lograron cifrar la información de un servidor de aplicaciones importante; adicionalmente los colaboradores acostumbran a dejar sus sesiones abiertas de los computadores, dejan además información confidencial en la zona de impresión sin los cuidados respectivos, así como también borran información importante frecuentemente en los repositorios de *SharePoint*. Recientemente se han realizado desde diversos frentes, ataques de fuerza bruta al puerto RDP de los servidores de aplicaciones, de bases de datos; y sumado a ello gran parte de su plataforma tecnológica de su core de negocio se está migrando *Azure DevOps* y requiere de mayor gestión frente a la seguridad en estas plataformas.

Estas son algunas situaciones que dejan vislumbrar la enorme necesidad de diseñar un sistema de gestión de seguridad de la información (SGSI) con base en la norma ISO 27001:2013 y con ello poder evitar en su mayoría pérdidas importantes de información que podrían repercutir en el estado financiero del negocio.

2.1 FORMULACIÓN DEL PROBLEMA

¿De qué manera la empresa Tecnofactory S.A.S puede optimizar y mejorar los procesos, tomando como base un estándar de seguridad reconocido y aplicando los manuales de buenas prácticas?

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar un sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO/IEC 27001:2013 para Tecnofactory S.A.S.

3.2 OBJETIVOS ESPECIFICOS

- Valorar estado actual de la empresa Tecnofactory S.A.S en términos de seguridad de la información, de acuerdo con la norma ISO/IEC 27001:2013.
- Realizar del inventario de activos de información de la empresa Tecnofactory S.A.S
- Identificar y analizar los riesgos a los que están expuestos los activos de información de Tecnofactory S.A.S utilizando la metodología ISO 31000: 2018
- Plantear el tratamiento de los riesgos identificados con base en el anexo A de la norma ISO/IEC 27001:2013.
- Definir las políticas de seguridad de la información para Tecnofactory S.A.S
- Elaborar del plan de concientización dirigido a todos los colaboradores de Tecnofactory S.A.S.
- Elaboración de una propuesta de implementación de un SGSI para Tecnofactory S.A.S.

4. MARCO TEÓRICO

La continua modernización de la tecnología ha llevado de su mano nuevos desafíos, cada vez las empresas se vuelven más dependientes de sus sistemas informáticos, lo que lo hace un activo muy valioso.

La seguridad informática nació precisamente para proteger la información contra la perdida de integridad, confidencialidad, disponibilidad y otros factores que puedan ponerla en peligro.

4.1 NORMAS

Para el presente diseño se tomarán como base las siguientes normas:

4.1.1 Norma ISO/IEC 27001:2013. La norma ISO 27001:2013 es una norma internacional publicada por la ISO que en español significa Organización Internacional de Normalización y se dedican a la creación de normas y estándares como esta.

La norma permite a las organizaciones la evaluación de los riesgos y la aplicación de controles que permitan mitigarlos o eliminarlos.[24]

Su estructura es:

- **Delimitación del alcance:** En esta etapa se describe la limitación que tendrá la implementación del plan. En los capítulos del 4 al 10 se encuentran los requisitos obligatorios que se deben cumplir.

- **Referencias normativas:** La ISO 27002 sigue siendo necesaria para desarrollar la declaración de aplicabilidad a pesar de que ya no es una referencia normativa para la ISO 27001 2013.

- **Términos y definiciones:** Los podemos encontrar agrupados en la sección 3 con la finalidad de encontrar una sola guía consistente.

- **Contexto de la organización**: En esta etapa se debe realizar la valoración de los factores internos y externos que pueden afectar la organización.

[24] ISOTOOLS EXCELLENCE. ISO 27001: ¿Qué es la ISO 2701? [en línea]. Bogotá: ISO Tools, 2017 [fecha de consulta 30 de junio de 2020]. Disponible en: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

- **Liderazgo:** Es de vital importancia para el plan SGSI que la dirección asuma el compromiso de garantizar que se cumplan los objetivos, garantizar los recursos y velar que cada uno cumpla su rol y responsabilidad**.**

- **Planificación:** Se deben definir objetivos específicos y es de vital importancia que estén alineados con la estrategia de la organización, para lograrlos es fundamental estructurar de manera correcta los diferentes planes.

- **Soporte:** Compone los requisitos para poder implementar el sistema de gestión de seguridad de la información entre ellos la definición de los recursos, personal calificado e interés de todas las partes involucradas.

- Expone también de la importancia de documentar, controlar y mantener la documentación requerida para el SGSI.

- **Operación:** Se establecen todos los lineamientos necesarios para medir el correcto funcionamiento del SGSI, se toman en cuenta la realimentación de la alta dirección para cumplir las expectativas.

- **Evaluación del desempeño:** Se toman las métricas establecidas para evaluar el desempeño del SGSI, realizando auditorías internas para analizar los diferentes aspectos involucrados.

- **Mejora:** Se evalúan las no conformidades identificas y para cada una de ellas se debe aplicar una acción correctiva que permita solucionarlas de manera efectiva.[25]

4.1.2 Norma ISO/IEC 27002:2013. La NORMA ISO/IEC 27002:2013 es una norma internacional que establece el código de mejores prácticas para apoyar la implantación del Sistema de Gestión de Seguridad de la Información (SGSI) en las organizaciones.

El principal objetivo es establecer directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Esto también incluye la selección, implementación y administración de controles, teniendo en cuenta los entornos de riesgo encontrados en la empresa.

[25] **I**SOTOOLS EXCELLENCE. ISO 27001: ¿Cuál es la estructura de la nueva norma ISO 27001 2013? [en línea]. Bogotá: ISO Tools, 2017 [fecha de consulta 30 de junio de 2020]. Disponible en: https://www.isotools.com.mx/la-estructura-la-nueva-norma-iso-27001-2013/

Las ventajas proporcionadas por la certificación ISO 27002 son representativas para las empresas, sobre todo porque son reconocidas mundialmente. Conozca algunos beneficios asociados a la aplicación de la norma:

- Mejor concienciación sobre la seguridad de la información;
- Mayor control de activos e información sensible;
- Ofrece un enfoque para la implementación de políticas de control;
- Oportunidad de identificar y corregir puntos débiles;
- Reducción del riesgo de responsabilidad por la no implementación de un SGSI o determinación de políticas y procedimientos;
- Se convierte en un diferencial competitivo para la conquista de clientes que valoran la certificación;
- Mejor organización con procesos y mecanismos bien diseñados y gestionados;
- Promueve reducción de costos con la prevención de incidentes de seguridad de la información;
- Conformidad con la legislación y otras reglamentaciones.

Está organizada en base a: 14 Dominios, 35 Objetivos de control y 114 Controles.[26]

4.1.3 Norma ISO/IEC 31000:2018. La ISO 31000 señala una familia de normas sobre gestión del riesgo, normas codificadas por la International Organization for Standardization. El propósito de la norma ISO 31000:2009 es proporcionar principios y directrices para la gestión de riesgos y el proceso implementado en el nivel estratégico y operativo.

Su última versión de la norma ISO 31000 2018 “Gestión del riesgo. Principios y directrices”, sustituye a la versión de 2009 de dicha norma. Esta versión mantiene que una correcta gestión del riesgo en las empresas es lo que ayuda a establecer todos los objetivos alcanzables, tomando decisiones basadas en hechos objetivos.

La norma ISO 31000 se encuentra dirigida a personas que protegen el valor de la organización utilizando la gestión de riesgos, la toma de decisiones, el establecimiento y la consecución de objetivos, además de mejorar el rendimiento. Durante el proceso de revisión que se le ha realizado a la norma ISO 31000 se descubren las virtudes de mantener la gestión de riesgos simples.

La revisión se realiza para conseguir que las cosas se hagan de forma fácil y claras. Esto se consigue utilizando el lenguaje simple para expresar los fundamentos de la

[26] OSTEC: ISO 27002: Buenas prácticas para gestión de la seguridad de la información [en línea]. [fecha de consulta 5 de marzo de 2022]. Disponible en: https://ostec.blog/es/generico/iso-27002-buenas-practicas-gsi/

gestión de riesgos de una forma mucho más coherente y comprensible para los usuarios.[27]

4.1.4 Norma NIST 800-50. La Publicación especial 800-50 del NIST, es la creación de un programa de formación y concienciación sobre la seguridad de la tecnología de la información, proporciona orientación para crear un programa de seguridad de la tecnología de la información (TI) eficaz y respalda los requisitos especificados en la Ley federal de gestión de la seguridad de la información (FISMA) de 2002 y la Oficina de Circular de Gerencia y Presupuesto (OGP) A-130, Apéndice III. No se puede implementar un programa sólido de seguridad de TI sin prestar una atención significativa a los usuarios de TI de la agencia de capacitación sobre políticas, procedimientos y técnicas de seguridad, así como los diversos controles de gestión, operativos y técnicos necesarios y disponibles para proteger los recursos de TI. Además, aquellos en la agencia que administran la infraestructura de TI deben tener las habilidades necesarias para llevar a cabo sus funciones asignadas de manera efectiva. No prestar atención al área de capacitación en seguridad pone a la empresa en gran riesgo porque la seguridad de los recursos de la agencia es un problema tanto humano como tecnológico.[28]

La guía identifica cuatro pasos críticos en el ciclo de vida de un programa de concientización y entrenamiento:

- **Diseño del programa**: Se conduce un relevamiento dentro de la organización y, a partir de su resultado, se desarrolla y aprueba la estrategia a seguir durante el programa, alineada a la misión de la organización.

- **Desarrollo del material**: Se evalúa el alcance del entrenamiento deseado, el contenido necesario para cubrirlo y las posibles fuentes para desarrollarlo.
- **Implementación del programa**: Se comunica y lanza el programa de concientización y entrenamiento, a través de los medios definidos en la estrategia.
- **Post implementación**: Se busca mantener una ejecución continua del programa y monitorear su efectividad.[29]

[27] ISOTOOLS EXCELLENCE. ISO 31000: ISO 31000 [en línea]. Bogotá: ISO Tools, 2018 [fecha de consulta 10 de febrero de 2022]. Disponible en: https://www.isotools.org/2018/02/16/ya-se-ha-publicado-la-nueva-norma-iso-31000/

[29] SMARTFENSE**.** Casi 20 años del estándar para programas de concientización, NIST Special Publication 800-50 Nicolás Bruna / 10/05/2021 [en línea]. [fecha de consulta 5 de marzo de 2022]. Disponible en: https://blog.smartfense.com/2021/10/nist-special-publication-800-500.html

4.2 BENEFICIOS DE IMPLEMENTAR UN SGSI

Tecnofactory S.A.S, es una empresa que ofrece servicios a otras organizaciones, es de vital importancia cuidar su buena reputación en el mercado, por lo que implementar un sistema de gestión de la seguridad de la información basado en la norma ISO/IEC 27001:2013 beneficia la confianza de sus clientes actuales y potenciales nuevos clientes. La mala reputación que generaría un incidente de seguridad mal manejado podría llegar a ser catastrófico para la organización.

Se reducirá el porcentaje de probabilidad de impacto de los incidentes de los cuales se pueda ser objeto, ya que la organización no será tan vulnerable y esto reducirá la periodicidad con la que se presenten.

Se establece una metodología para el manejo de la seguridad informática estructurada, que cumple con la reglamentación actual y que permita disminuir el riesgo de pérdida, robo o integridad de la información.

Da una orientación de cómo actuar cuando se presenten incidentes de este tipo y la organización estará preparada para saber cómo afrontarlos. Con la implementación de controles se cierra considerablemente la brecha y se tiene un panorama más claro cuando se presenten.

Administrar de una manera adecuada y controlada los activos de información permite, realizar la mejora continua de los mismos sin necesidad de incurrir en gastos inesperados, esto permite que no se vean afectados los objetivos estratégicos de la organización al generar gastos innecesarios.

Con las métricas se puede evaluar diferentes aspectos como los gastos de seguridad, porcentaje de incidentes en un período de tiempo y con una base de conocimiento se conocerá como afrontarlos de manera más rápida y efectiva[30]

4.3 EVALUACIÓN DE RIESGOS

La parte principal de un sistema de gestión de la seguridad de la información comienza por la evaluación de los riesgos. A continuación, se explicará la metodología utilizada en la norma ISO/31000 de 2018 para realizar este proceso:

[30] PORTAL DE ISO 27001 EN ESPAÑOL. Beneficios [en línea]. Bogotá: ISO, 2016 [fecha de consulta 1 de julio de 2020]. Disponible en: http://www.iso27000.es/sgsi.html

Definición de contexto: Debe establecerse para definir los parámetros básicos dentro de los cuales se debe manejar el riesgo y para ofrecer orientación con relación a decisiones dentro del estudio de gestión de riesgos más detallados.

- **Contexto externo:** En esta primera etapa se determinan las características o aspectos esenciales del entorno en el cual opera la entidad, se consideran aspectos como: Políticos, sociales y culturales, legales y reglamentarios, tecnológicos, financieros y económicos.

- **Contexto interno:** Se determinan las características o aspectos esenciales del ambiente en el cual la organización busca alcanzar sus objetivos, se consideran factores como: estructura organizacional, funciones y responsabilidades, políticas, objetivos y estrategias implementadas, recursos y conocimientos con los que cuenta (personas, procesos, sistemas, tecnología), relación con las partes involucradas y cultura organizacional.

- **Contexto del proceso:** Se determinan las características o aspectos esenciales del proceso y sus interrelaciones. Se pueden considerar factores como: objeto del proceso, alcance del proceso, interrelación con otros procesos, procedimientos asociados y responsables del proceso.

- **Valoración del riesgo**: Determina el valor de los activos de información y está compuesta por el análisis de riesgos y evaluación de los riesgos. El análisis de riesgos está compuesto por las actividades de identificación de riesgos y la estimación de riesgos. La evaluación de riesgos comprende la comparación de los niveles de riesgo con los criterios de evaluación de riesgo.

- **Identificación de los riesgos**: el riesgo se mide como la posibilidad o probabilidad de que ocurra un evento y lo daremos después de la clasificación de los niveles de criticidad en el mapa de calor de los activos.

- **Identificación o inventario de activos de información:** En esta primera etapa se debe realizar un inventario de todos los activos de información que son importantes para la organización como lo puede ser archivos tanto digitales como físicos por ejemplo servidores de aplicación o base de datos y archivadores que custodian información importante.

- **Identificación de Amenazas:** seguido de que encontremos las vulnerabilidades debemos identificar las amenazas que pueden explotar dichas debilidades.

- **Identificación de controles existentes:** se identifican los controles existentes realizando inspecciones a sus áreas y comparando los controles detectados con la lista de controles recomendados por la norma ISO27001, este análisis se denomina análisis de brecha y permite en forma simultánea identificar el nivel de

madurez de la organización en cuanto a seguridad de la información y los controles existente.

- **Identificación de vulnerabilidades:** luego de realizar el inventario de activos de información a cada activo debemos encontrar las vulnerabilidades a las cuales está expuesto. Una vulnerabilidad se puede presentar por la ausencia de un control o por un control incorrectamente implementado.

- **Estimación del riesgo:** para el proceso de análisis de los riesgos se recomienda usar métricas cualitativas debido a que son más fáciles de entender y calcular. Se deben plantear unas escalas de calificación como lo son la Valoración de impactos, Valoración de probabilidad de ocurrencia de riesgo y Estimulación del nivel de riesgo.

- **Evaluación del riesgo:** luego de realizar las dos actividades de análisis de riesgos se procede con la evaluación de los riesgos. En esta etapa se comparan los niveles de riesgo contra los criterios de aceptación de los riesgos para determinar el orden de prioridades de los riesgos identificados.

- **Plan de tratamiento del riesgo:** después de identificar todo lo anterior, ya se puede definir la política de tratamiento del riesgo, se debe definir el manejo que se le dará a cada riesgo asumiéndolo o adoptando controles que permitan eliminarlo o por lo menos reducirlo.

  En el caso de contar con aliados terceros podríamos también hablar de transferirlos.[31]

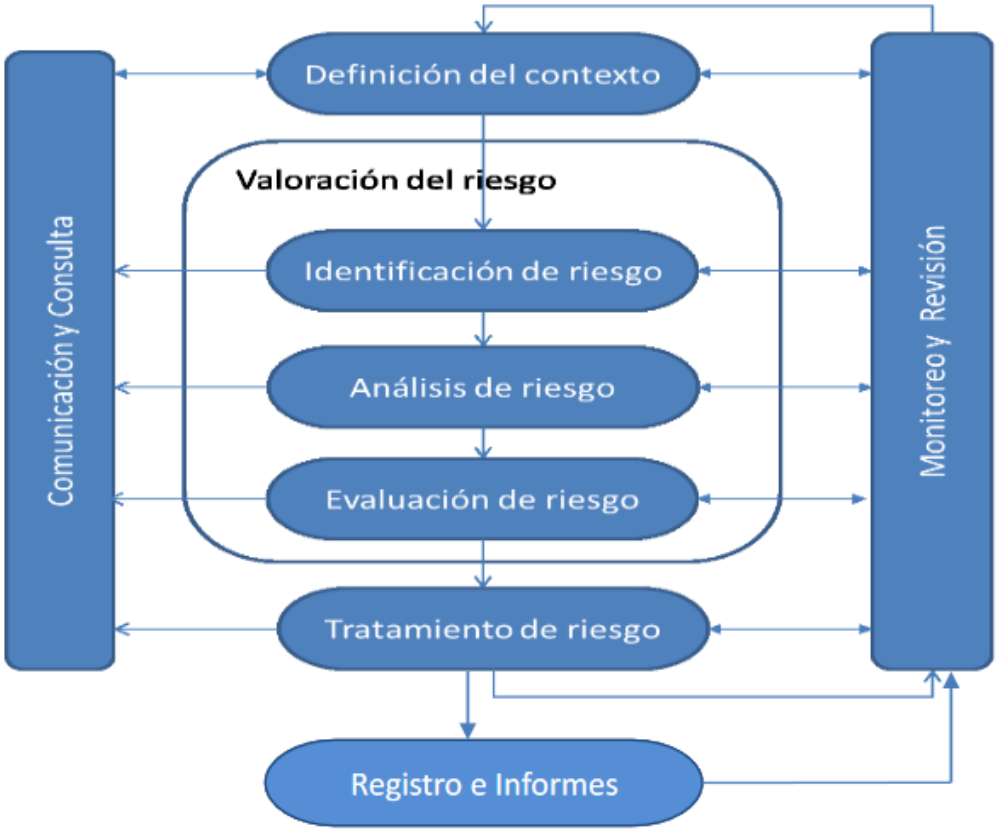
- **Evaluación del tratamiento de riesgos:** Después de identificar todo lo anterior; una vez que se determinan los controles que permiten el tratamiento del riesgo, se debe evaluar si el control reduce la probabilidad o impacto del riesgo, los nuevos valores de probabilidad o impacto permiten el cálculo del nuevo nivel de riesgo. Con el nuevo nivel de riesgo se realiza una comparación entre el riesgo antes de su tratamiento (Riesgo Inherente) y el riesgo con el control (riesgo residual).

  El riesgo residual, se vuelve a comparar con los criterios de aceptación de riesgo. Si el riesgo residual está dentro de los límites de riesgo aceptable, el análisis termina y se puede aprobar el análisis y tratamiento de riesgo. En caso de que el nuevo nivel de riesgo residual no esté dentro de los límites aceptables, se deben buscar nuevas opciones de tratamiento de riesgo, hasta lograr que el nivel de riesgo residual sea aceptable.

[31] Normas ISO. ¿En qué consiste la evaluación de riesgos? [en línea]. España: Normas ISO, 2020 [fecha de consulta 1 de julio de 2020]. Disponible en: https://www.normas-iso.com/ iso-27001/

En la figura 1. Se relaciona en orden los pasos a seguir según la norma ISO 31000:2008 para definir, identificar, analizar, evaluar, tratar y realizar seguimiento a la gestión del riesgo.

Figura 1. Modelo de gestión del riesgo



Fuente. Normas ISO. ¿En qué consiste la evaluación de riesgos? [en línea]. España: Normas ISO, 2020 [fecha de consulta 1 de julio de 2020]. Disponible en: https://www.normas-iso.com/iso-27001/

4.4 CONTROLES

La norma ISO 27001:2013 requiere la implementación obligatoria de controles que permitan controlar, medir y monitorear los riesgos de perdida de integridad, confidencialidad y disponibilidad de la información. En su anexo A encontraremos 114 controles propuestos y clasificados de la siguiente manera:

- **Políticas de seguridad de la información:** hablan sobre la implementación de las políticas de seguridad y su continúa revisión para verificar que estén actualizadas con los cambios importantes de la organización.

- **Organización de la seguridad de la información:** recalcan la importancia de la asignación de roles y responsabilidades dentro de la organización para el manejo de información.

- **Seguridad de los recursos humanos:** describen la importancia de verificar la idoneidad y responsabilidad de cada colaborador con el manejo de la información y procesos disciplinarios al incurrir en faltas.

- **Gestión de Activos:** se utilizan para la constante identificación de activos de información clasificándolos, dándoles correcto manejo y brindándoles soporte.

- **Controles de acceso:** sugiere los controles que se pueden implementar para el ingreso a redes, aplicaciones, bases de datos o centros de datos.

- **Criptografía – Cifrado y gestión de claves:** tratan sobre la implementación de criptografía para la protección de la información y el manejo de claves de autenticación.

- **Seguridad física y ambiental:** indican los controles adecuados para darle manejo a los factores físicos o ambientales que pueden afectar los activos.

- **Seguridad operacional:** instruyen sobre la correcta manera de manejar la gestión del cambio en procesos o infraestructura que puedan afectar, la integridad, confidencialidad o disponibilidad de la información.

- **Seguridad de las comunicaciones:** plantean los controles que se pueden implementar para asegurar las redes de comunicación, la transferencia de información y planes de mantenimiento que se le debe dar a la infraestructura.

- **Adquisición, desarrollo y mantenimiento del sistema:** identifica los controles que se pueden implementar para el desarrollo de software seguro y sus ambientes, indican también la manera adecuada de gestionar los cambios**.**

- **Gestión de incidentes de seguridad de la información:** plasman los controles que se pueden utilizar para darle manejo a los incidentes que se pueden presentar, acordando responsables para el tratamiento de cada incidente y generando informes de estos.

- **Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio**: hablan sobre la planificación de los planes de continuidad del

negocio garantizando la disponibilidad, confidencialidad e integridad de la información cuando se presenten incidentes graves.

- **Cumplimiento:** Propone los controles necesarios para garantizar que la organización está cumpliendo con todas las normativas legales e internamente.[32]

4.5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Para el cumplimiento del objetivo del presente proyecto, en cuanto a la documentación de políticas de seguridad, se establece tomar como referencia lo estipulado por el Ministerio de Tecnologías de la Información (MINTIC), para las entidades públicas y privadas que deseen tener una guía para la implementación de las políticas de seguridad dentro del desarrollo del sistema de gestión y seguridad, y a su vez en este documento todas las referencias a las políticas, definiciones o contenido relacionado, se encuentran publicadas en la norma técnica colombiana NTC ISO/IEC 27001:2013.[33]

En este documento del Ministerio de Tecnologías de la Información (MINTIC) ofrece un formato que puede ser utilizado como plantilla para la elaboración de la política general de seguridad y privacidad de información para las entidades públicas, como parte del Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea, según lo establecido en el Decreto 1078 de 2015.

4.5.1 Fases de implementación de políticas de seguridad de la información. Para realizar una correcta implementación de políticas de seguridad de la información, es necesario cumplir con una serie de fases que se sugieren en este documento, las cuales tienen como objetivo que la entidad desarrolle, apruebe, implemente y socialice e interiorice las políticas para un uso efectivo por parte de todos los funcionarios, contratistas y/o terceros de la entidad.

A continuación, se describen cada una de las diferentes fases:

---

[32] SGSI Blog especializado en sistemas de Gestión de Seguridad de la Información: Anexo A en ISO 27001, objetivos y controles de referencia [en línea]. Bogotá: SGSI, 2020 [fecha de consulta 30 de junio de 2020]. Disponible en: https://www.pmg-ssi.com/2020/03/anexo-a-en-iso-27001-objetivos-de-control-y-controles-de-referencia/

[33] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Guía 02 – Elaboración de la política general de seguridad y privacidad de la información. [en línea]. Colombia: La entidad. [consultado el 01 de febrero de 2022]. Disponible en internet: < https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf >

Desarrollo de las políticas: en esta fase se debe responsabilizar a los encargados de la creación de las políticas donde se deben escribir, estructurar, revisarlas y aprobarlas, dentro de este desarrollo se deben tener en cuenta aspectos como:

- Justificación de la creación de política: Debe identificarse el por qué la Entidad requiere la creación de la política de seguridad de información y determinar el control al cual hace referencia su implementación.

- Alcance: Debe determinarse el alcance, ¿A qué población, áreas, procesos o departamentos aplica la política?, ¿Quién debe cumplir la política?

- Roles y Responsabilidades: Se debe definir los responsables y los roles para la implementación, aplicación, seguimiento y autorizaciones de la política.

- Revisión de la política: Es la actividad mediante la cual la política una vez haya sido redactada pasa a un procedimiento de evaluación por parte de otros individuos o grupo de individuos que evalúen la aplicabilidad, la redacción y se realizan sugerencias sobre el desarrollo y creación de esta.

- Aprobación de la Política: Se debe determinar al interior de la entidad la persona o rol de la alta dirección que tiene la competencia de formalizar las políticas de seguridad de la información mediante la firma y publicación de estas. Es importante que la Alta Gerencia de la Entidad muestre interés y apoyo en la implementación de dichas políticas.

- Cumplimiento: fase mediante la cual todas aquellas políticas escritas deben estar implementadas y relacionadas a los controles de seguridad de la Información, esto con el fin de que exista consistencia entre lo escrito en las políticas versus los controles de seguridad implementados y documentados.

- Comunicación: fase en la cual se da a conocer las diferentes políticas a los empleados.

- Monitoreo: en esta fase es importante que las políticas sean supervisadas con el fin de determinar el cumplimiento.

- Mantenimiento: en esta fase de realiza la actualización de la política.

- Retiro: fase en la cual se realiza la eliminación de la política ya sea porque esta ha cumplido su objetivo o ya no es necesaria para la empresa.

4.6 LA EMPRESA

Tecnofactory S.A.S es una compañía que le apuesta a la transformación digital a través del desarrollo de software y soluciones tecnológicas aplicables a cualquier tipo de negocio. Ofrecen servicios de diseño personalizado de aplicaciones. Su experticia proviene de más de una década trabajando en la generación de soluciones de alto valor aplicables al sector de la consultoría en Colombia, experiencia que han venido capitalizando y extendiendo a todos los sectores de la economía nacional.

Su misión es ser una fábrica dedicada al desarrollo de sistemas y aplicaciones informáticas, ofreciendo soluciones innovadoras para automatizar.

La visión es ser una compañía competitiva referente en el mercado global de la transformación digital, orientada a crear diferencia corporativa como proveedor de servicios eficiente con enfoque hacia la mejora continua en la calidad.

4.6.1 Estructura organizacional. El organigrama de Tecnofactory S.A.S está conformado por un sistema uniforme de clasificación de cargos para los colaboradores de la compañía. La definición y las funciones de los cargos que conforman la planta de personal, así como las responsabilidades, requerimientos de conocimiento, experiencia y demás competencias exigidas para el desempeño de estos. En el cuadro 1 se describen los 5 niveles de clasificación.

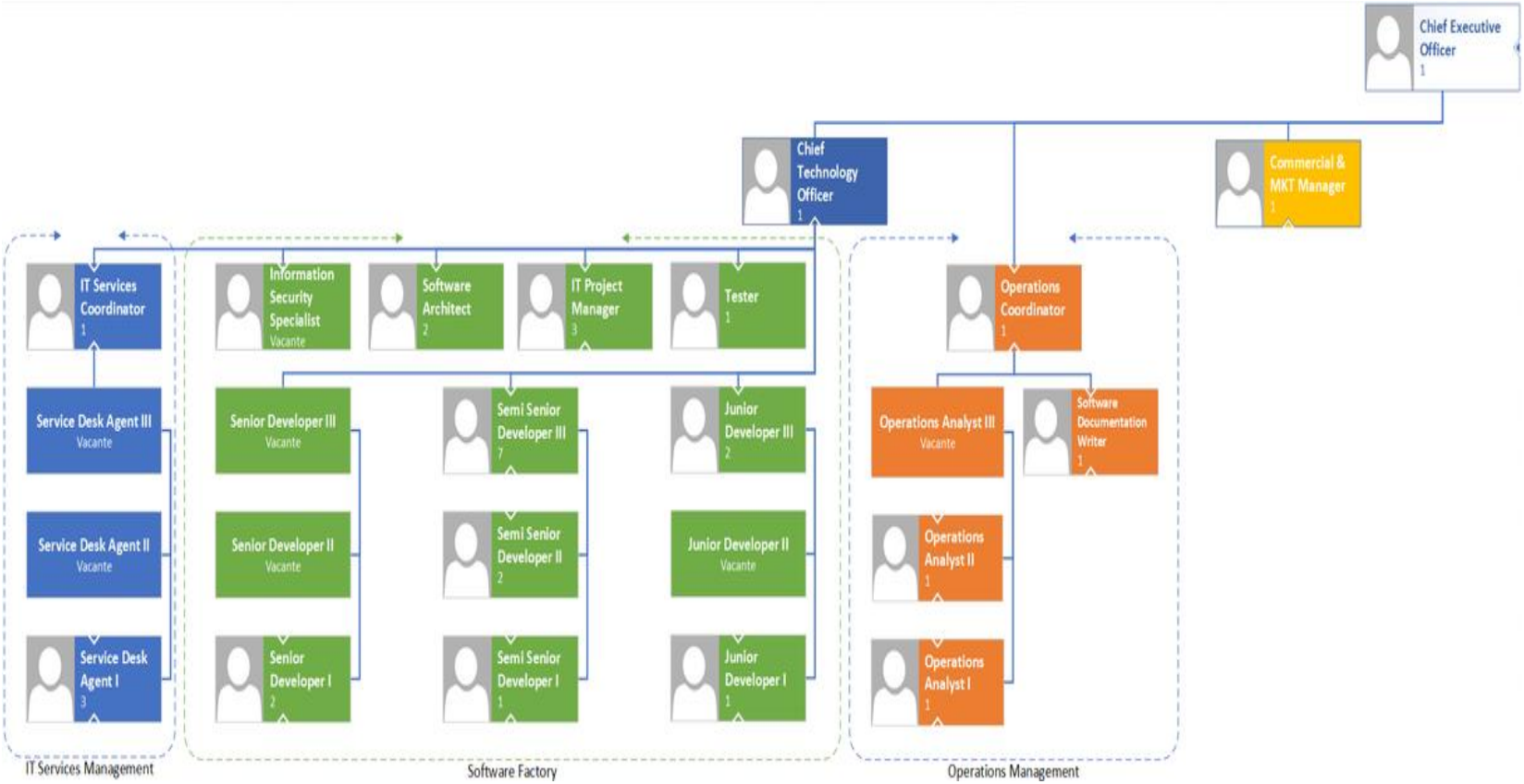
Cuadro 1. Lista de cargos

Clasificación de cargos		
Nivel Directivo:	Corresponde a los cargos de la Alta Dirección, quienes formulan y plantean el direccionamiento estratégico de la organización, planes, programas y proyectos.	Chief Executive Officer - CEO
Nivel Ejecutivo:	Comprende cargos de la dirección, jefatura, control de dependencias internas encargadas de ejecutar y desarrollar los planes, programas y proyectos.	Chief Technology Officer - CTO
Nivel Profesional:	Constituye el nivel más importante de la empresa. Agrupa los cargos cuya naturaleza demanda la ejecución y aplicación de los conocimientos propios de cualquier carrera profesional, técnica profesional y/o tecnológica para la ejecución de las tareas que se realizan en la organización.	Arquitecto de software Desarrollares Senior Desarrollares Semi Senior Desarrollares Junior IT Services Coordinator Operations Coordinator
Nivel Asistencial:	Comprende los cargos cuyas funciones implican el ejercicio de actividades de apoyo y complementarias de las tareas propias de los niveles superiores o de labores, que se caracterizan por el predominio de actividades manuales o tareas de dificultad media y/o baja en su ejecución.	Operations Analyst Software Documentation Writer
Nivel Asistencial:	Comprende los cargos cuyas funciones exigen el desarrollo de procesos y procedimientos en labores asistenciales misionales y de apoyo.	Service Desk Agent

Fuente. Los Autores

Después de conocer la descripción de los diferentes niveles de cargos, en la figura 2 se describe como está conformado el organigrama de Tecnofactory S.A.S

Figura 2. Organigrama



Fuente: Tecnofactory S.A.S

4.6.2 Procesos organizacionales. Teniendo como referencia que Tecnofactory S.A.S es una empresa conexa de la casa raíz C&M Consultores S.A.S, se ha establecido una alianza con el fin de coordinar los procesos y las operaciones de la empresa según lo estipulado en el Acuerdo Marco de Operación Conjunta suscrito con C&M Consultores S.A.S, propiciando, una adecuada sinergia con las diferentes áreas y garantizando la funcionabilidad transversal entre ellas, con el fin de asegurar que todos los sistemas están funcionando correctamente. En tanto las áreas que son soportadas por C&M Consultores S.A.S, son Gestión de Talento Humano, Gestión de Recursos, Gestión Jurídica, Gestión Financiera, Gestión de Comunicaciones, y Tecnofactory S.A.S contribuye por su aporte como proveedor de servicios tecnológicos.

En el mapa de procesos de Tecnofactory S.A.S se describen las interacciones de cada uno de los procesos estratégicos, misionales y de soporte determinados en la organización para cumplir con el principio de gestión por procesos. En dicha determinación se han tenido en cuenta las siguientes definiciones:

Procesos Estratégicos: definen y despliegan la política y la estrategia de la empresa, constituyen el marco de referencia para los demás procesos.

Procesos Misionales: constituyen la secuencia de valor agregado, desde la determinación de necesidades hasta la realización de los servicios ofrecidos por la empresa.

Procesos de Soporte: son aquellos que sirven de apoyo fundamentalmente a los procesos operativos de la organización

Actualmente Tecnofactory S.A.S cuenta con 8 procesos ya definidos, los cuales se describen a continuación en el cuadro 2:

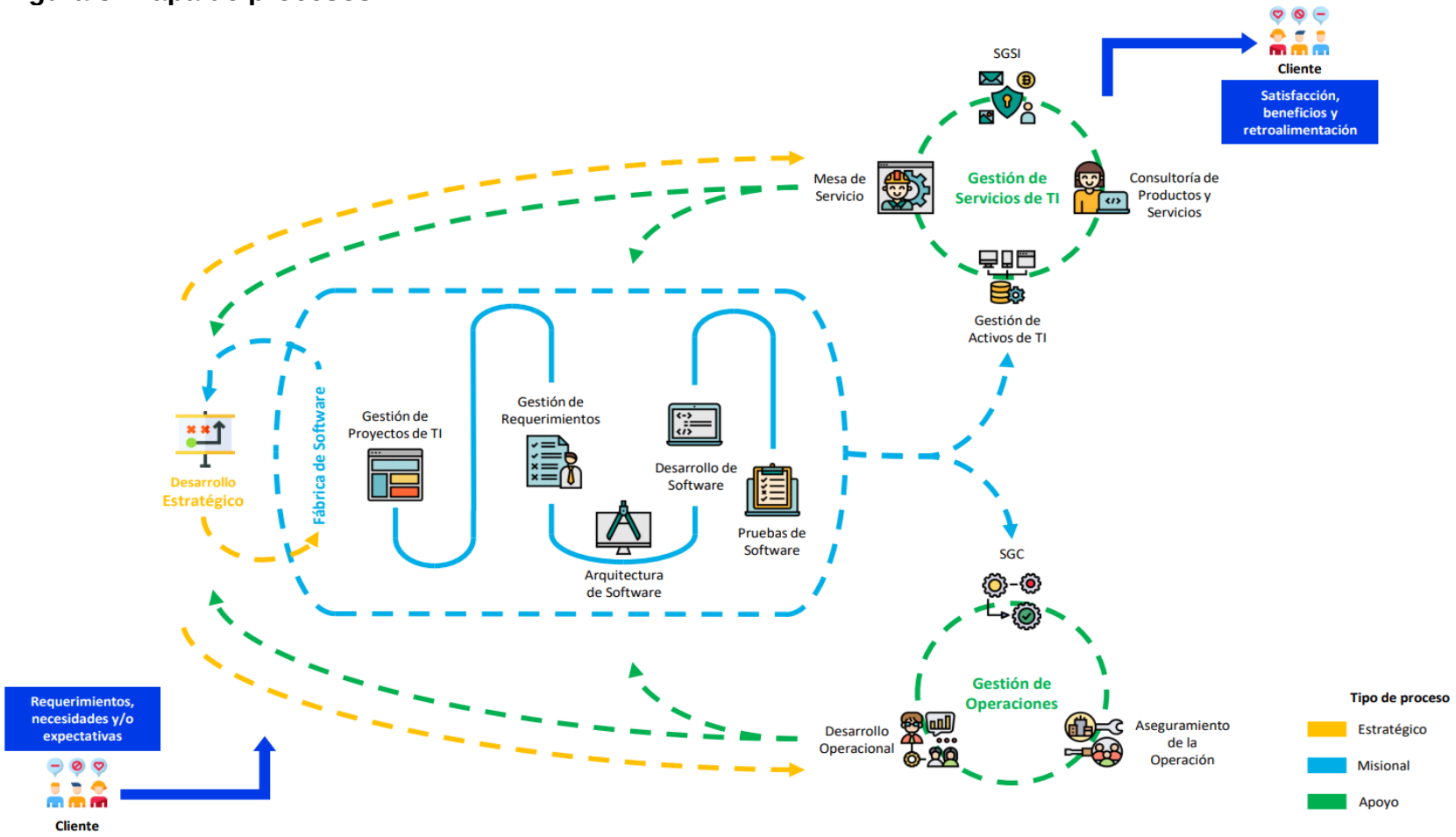
Cuadro 2. Lista de procesos

PROCESO	OBJETIVO GENERAL
DIRECCIONAMIENTO ESTRATÉGICO	Plan estratégico
FÁBRICA DE SOFTWARE	Cronograma del Proyecto
	Cambios en requerimientos
	Recursos propios de los proyectos
	Desviaciones frente al Cronograma del Proyecto
DESARROLLO OPERACIONAL	Identificación de requisitos reglamentarios y legales
	Propuestas Comerciales
	Dar a conocer los productos/servicios de la empresa
	Evaluación y seguimiento de la satisfacción del cliente
	Gestión de cobro
	Plan Operativo
	Seguimiento y control
	Cierre
ASEGURAMIENTO DE LA OPERACIÓN	Interlocución de las necesidades de la compañía a C&M Consultores.
SGC	Enfoque de procesos del Sistema de Gestión de Calidad
	Misión, Visión, Valores Corporativos y Objetivos de Corporativos y Objetivos de la Compañía
	Política de Calidad y Objetivos de Calidad
	Certificación y Renovación del Sistema de Gestión de Calidad
	Comunicación interna y externa en el SGC
MESA DE SERVICIO	Especificaciones de acuerdo de Nivel de Servicio.
GESTIÓN DE ACTIVOS	Requisitos de Compra
	Selección, Evaluación y reevaluación de Proveedores
CONSULTORIA DE PRODUCTOS Y SERVICIOS	Identificación de requisitos reglamentarios y legales
	Propuesta Comercial
	Dar a conocer los servicios ofertados de la empresa
	Evaluación y seguimiento de la satisfacción del cliente
	Gestión de cobro
SGSI	Por definir

Fuente: Tecnofactory S.A.S

En la figura 3. Representación gráficamente las interrelaciones que tienen los procesos de Tecnofactory S.A.S.

Figura 3. Mapa de procesos



Fuente: Tecnofactory S.A.S.

5. DISEÑO METODOLÓGICO

El diseño de un SGSI de la empresa Tecnofactory S.A.S requirió las siguientes actividades, con el fin de obtener conocimiento del manejo actual de la información:

- Reuniones con la Gerencia
- Entrevistas con el área de Tecnología
- Visitas de campo

Se hicieron visitas a la empresa Tecnofactory S.A.S. en la cual se hizo un recorrido por las instalaciones para conocer las diferentes áreas y tener un entendimiento más a fondo del manejo de la seguridad de la información. Así mismo, se hicieron reuniones con el IT Services Coordinator, CTO e ingenieros de desarrollo para identificar la necesidad en la protección de la información.

A continuación, se muestra un plan de desarrollo por etapas para el diseño del Sistema de Gestión de Seguridad:

- Identificar estado actual de la seguridad de la información.
- Identificación de activos.
- Identificación de amenazas.
- Identificación de vulnerabilidades.
- Identificación de controles existentes.
- Determinar impactos y consecuencias.
- Análisis de riesgos.
- Valoración probabilidades / impactos.
- Estimación de riesgo (probabilidades x impacto).
- Plan de tratamiento de los riesgos.
- Diseñar políticas de seguridad de acuerdo con la Norma ISO 27001:2013 las cuales deben estar como información documentada y estar disponibles para las partes interesadas.
- Diseñar plan de concientización del modelo de seguridad.

5.1. ESTADO ACTUAL DE LA SEGURIDAD

Actualmente Tecnofactory S.A.S no cuenta con un SGSI, es por ello que se debe iniciar realizando un diagnóstico sobre el estado actual de la organización en cuanto a seguridad informática se refiere y para esto se procede a realizar entrevistas con los lideres de proceso y a revisar la documentación relacionada con los controles que se tienen implementados hasta el momento.

5.1.1 Evaluación de los dominios de la norma ISO/IEC 27001:2013 a la empresa Tecnofactory S.A.S. Para conocer el diagnóstico se realiza un análisis GAP o también conocido como análisis de brecha, basado en el cumplimiento de los controles propuestos en el anexo A, de la norma ISO 27001:2013 y se establecen unos niveles definidos por unos porcentajes y argumentando la descripción correspondiente a cada uno como se puede ver en el cuadro 3.

Cuadro 3. Niveles de cumplimiento

Nivel	Porcentaje de cumplimiento	Descripción
Inexistente	0%	-La organización no cuenta con el control implementado. -Aún no han identificado una situación que deba ser tratada.
Inicial	1-20 %	-Se ha identificado una situación que requirió la implementación del control, pero no existe documentación alguna.
Repetible	21-50 %	-El control esta implementado pero la documentación no está completa a pesar de que lo han utilizado varias veces.
Definido	51-80 %	-El control está completamente documentado y publicado pero el cumplimiento depende de cada uno de los involucrados. No se realizan mediciones de la efectividad del control
Gestionado	81-100%	-Se encuentra en un proceso de mejora continua.

Fuente. Los Autores

Ya teniendo definidos los niveles se debe calcular el porcentaje de cumplimiento de cada control y el nivel en el que se encuentra, adicional se dejaran las observaciones correspondientes como se puede observar en el cuadro 4:

Cuadro 4. Análisis GAP

A.5 Políticas de la seguridad de la información				
5.1 Orientación de la dirección para la gestión de la seguridad de la información				
Numeral	**Control**	**%**	**Nivel**	**Observaciones**
5.1.1	Políticas para la seguridad de la información	**40**	Repetible	Aunque existe una Política de Seguridad no está completa, hay apartes que no son claros o carecen de soportes existentes.
5.1.2	Revisión de la política seguridad de la información	**40**	Repetible	Se debe terminar y publicar la política de seguridad, adicional proponer revisiones frecuentes o si ocurren cambios de gran impacto en la organización.
Cumplimiento de Subdominios: 40 %				
A 6. Organización de la seguridad de la información				
6.1 Organización interna				
6.1.1	Asignación de responsabilidades para la seguridad de la información	**40**	Repetible	Existe una definición de roles y responsabilidades, pero no se encuentran las actas de asignación de roles.
6.1.2	Distribución (segregación) de funciones	**40**	Repetible	Si bien las responsabilidades están asignadas, falta completar la documentación.
6.1.3	Contacto con las autoridades	**40**	Repetible	Se conocen los datos de la unidad de delitos informáticos de la policía, pero es necesario plasmarlo en un documento de fácil consulta.
6.1.4	Contacto con grupos de interés especial	**40**	Repetible	Se solicitan asesorías en temas de seguridad a los aliados, pero se aconseja inscribirse en boletines diarios para estar actualizados.
6.1.5	Seguridad de la información en gestión de proyectos	**40**	Repetible	Se cuenta con una matriz crud, pero no es fácil de interpretar así que se aconseja cambiarla.
Cumplimiento de Subdominios: 40 %				

Cuadro 4. (Continuación)

Numeral	Control	%	Nivel	Observaciones
6.2 Dispositivos móviles y teletrabajo				
6.2.1	Política para dispositivos móviles	**0**	Inexistente	No se cuenta con el control
6.2.2	Teletrabajo	**0**	Inexistente	No se cuenta con el control
Cumplimiento de Subdominios: 0 %				
Cumplimiento del Dominio: 28 %				
A.7 Seguridad de los Recursos humanos				
7.1 Antes de asumir el empleo				
7.1.1	Selección	**0**	Inexistente	No se cuenta con el control
7.1.2	Términos condiciones del empleo	**0**	Inexistente	No se cuenta con el control
Cumplimiento de Subdominios: 0 %				
7.2 Durante la ejecución del empleo				
7.2.1	Selección	**0**	Inexistente	No se cuenta con el control
7.2.2	Términos condiciones del empleo	**0**	Inexistente	No se cuenta con el control
Cumplimiento de Subdominios: 0 %				
7.3 Terminación y cambio de empleo				
7.3.1	Terminación o cambio de responsabilidades de empleo	**0**	Inexistente	No se cuenta con el control
Cumplimiento de Subdominios: 0 %				
Cumplimiento del Dominio: 0 %				
A.8 Gestión de activos				
8.1 Responsabilidad por los activos				
8.1.1	Inventario de activos	**40**	Repetible	Se cuenta con un inventario inicial. Pendiente aprobación.
8.1.2	Propiedad de los activos	**40**	Repetible	Falta identificar los propietarios de varios activos de información.
8.1.3	Uso aceptable de los activos	**40**	Repetible	Se debe generar una campaña y actualización del documento que habla del uso correcto de los activos de información.

Cuadro 4. (Continuación)

Numeral	Control	%	Nivel	Observaciones
8.1.4	Devolución de activos	**0**	Inexistente	No se cuenta con el control
Cumplimiento de Subdominios: 30 %				
8.2 Clasificación de la información				
8.2.1	Clasificación de la información	**40**	Repetible	Se encuentra vinculación en el Sistema Integrado de Gestión HSEQ, pero no es define claramente para el SGSI.
8.2.2	Etiquetado de la información	**0**	Inexistente	No se cuenta con el control
8.2.3	Manejo de activos	**0**	Inexistente	No se cuenta con el control
Cumplimiento de Subdominios: 13 %				
8.3 Manejo de medios de soporte				
8.3.1	Gestión de medios de soporte removibles.	**40**	Repetible	Existe una guía de solicitudes para eliminación de medios, muy somera.
8.3.2	Disposición de los medios de soporte.	**40**	Repetible	Existe una guía de solicitudes para eliminación de medios, falta especificar más detalladamente.
8.3.3	Transferencia de medios de soporte físicos.	**40**	Repetible	Existe el procedimiento de seguridad de los equipos fuera de las instalaciones, documentación incompleta.
Cumplimiento de Subdominios: 40 %				
Cumplimiento del Dominio: 28 %				
A.9 Control de acceso				
9.1 Requisitos del negocio para control de acceso				
9.1.1	Política de control de acceso	**40**	Repetible	Si bien existe la política es muy general y falta detallar más de tal forma cumpla su deber ser.
9.1.2	Acceso a redes y a servicios en red	**40**	Repetible	El Procedimiento de control de acceso lógico, está incompleto.
Cumplimiento de Subdominios: 40 %				

Cuadro 4. (Continuación)

Numeral	Control	%	Nivel	Observaciones
9.2 Gestión de acceso de usuarios				
9.2.1	Registro y cancelación del registro de usuarios.	**40**	Repetible	Si bien el Procedimiento de control de acceso lógico tiene esta aparte falta definición.
9.2.2	Suministro de acceso de usuarios.	**40**	Repetible	El Procedimiento de control de acceso lógico está incompleto en este aparte.
9.2.3	Gestión de derechos de acceso privilegiado.	**40**	Repetible	Si bien existe una Matriz Crud, no se encuentra actualizada, y no es de conocimiento de todos los interesados en asignación de privilegios.
9.2.4	Gestión de información de autenticación secreta de usuarios.	**40**	Repetible	Se encuentra este aparte en el Procedimiento de control de acceso lógico, pero falta ampliarlo.
9.2.5	Revisión de los derechos de acceso de usuarios.	**40**	Repetible	Se tienen definidos los permisos de acceso, pero no se están haciendo revisiones periódicas de los privilegios otorgados.
9.2.6	Cancelación o ajuste de los derechos de acceso.	**40**	Repetible	Se debe mejorar el proceso de retiro de privilegios ya que no está automatizado y pueden quedar privilegios aplicados.
Cumplimiento de Subdominios: 40 %				
9.3 Responsabilidades de los usuarios				
9.3.1	Uso de la información de autenticación secreta.	**40**	Repetible	Se debe ajustar la cláusula de confidencialidad en el contrato de cada colaborador.
Cumplimiento de Subdominios: 40 %				
9.4 Control de acceso a sistemas y aplicaciones				
9.4.1	Restricción de acceso a información	**40**	Repetible	En la Política de control de acceso, falta precisión en este control y los demás que se siguen ausentes de definición.

Cuadro 4. (Continuación)

Numeral	Control	%	Nivel	Observaciones
9.4.2	Procedimiento de ingreso seguro.	**0**	Inexistente	No se cuenta con el control.
9.4.3	Sistema de gestión de contraseñas.	**0**	Inexistente	No se cuenta con el control.
9.4.4	Uso de programas utilitarios privilegiados.	**0**	Inexistente	No se cuenta con el control.
9.4.5	Control de acceso a códigos fuente de programas.	**0**	Inexistente	No se cuenta con el control.
Cumplimiento de Subdominios: 8 %				
Cumplimiento del Dominio: 32 %				
A.10 Criptografía				
10.1 Controles criptográficos				
10.1.1	Política sobre el uso de controles criptográficos.	**0**	Inexistente	No se cuenta con el control.
10.1.2	Gestión de claves.	**0**	Inexistente	No se cuenta con el control.
Cumplimiento del Subdominios: 0 %				
Cumplimiento del Dominio: 0 %				
A.11 Seguridad física y ambiental				
11.1 Áreas Seguras				
11.1.1	Perímetro de seguridad física.	**0**	Inexistente	No se cuenta con el control.
11.1.2	Controles de acceso físico,	**0**	Inexistente	No se cuenta con el control.
11.1.3	Seguridad de oficinas, recintos e instalaciones.	**0**	Inexistente	No se cuenta con el control.
11.1.4	Protección contra amenazas externas y ambientales	**0**	Inexistente	No se cuenta con el control.

Cuadro 4. (Continuación)

Numeral	Control	%	Nivel	Observaciones
11.1.5	Trabajo en áreas seguras.	**0**	Inexistente	No se cuenta con el control.
11.1.6	Áreas de despacho y carga.	**0**	Inexistente	No se cuenta con el control.
Cumplimiento de Subdominios: 0 %				
11.2 Equipos				
11.2.1	Ubicación y protección de los equipos.	**50**	Definido	Se tiene el control habilitado para el ingreso y seguridad de las áreas físicas de la compañía cumpliendo con los lineamientos del control, pero se ha evidenciado falencia en el cumplimiento del control en los roles operativos.
11.2.2	Servicios públicos de soporte.	**50**	Definido	El Procedimiento de Control físico de entrada, se identifica que se cumple esporádicamente.
11.2.3	Seguridad del cableado.	**50**	Definido	No se evidencia la realización del monitoreo periódico mensual sobre las redes de cableado para detectar, eliminar o prevenir el uso de dispositivos no autorizados conectados a los cables.
11.2.4	Mantenimiento de equipos.	**50**	Definido	El control en el Pro. Mantenimiento de equipos se encuentra definido, pero no se ha cumplido el plan de mantenimientos establecido.
11.2.5	Retiro de activos.	**50**	Definido	La política de seguridad física contiene la implementación del control, pero se identifica que se cumple esporádicamente.

Cuadro 4. (Continuación)

Numeral	Control	%	Nivel	Observaciones
11.2.6	Seguridad de equipos y activos fuera del predio.	**50**	Definido	Política Seguridad Física Numeral 5.2.5 Pro. Seguridad de los equipos fuera de las instalaciones, se debe reajustar teniendo en cuenta las nuevas implicaciones de teletrabajo obligatorio debido a las medidas de aislamiento consecuencia de la pandemia.
11.2.7	Disposición segura o reutilización de equipos.	**50**	Definido	La política de seguridad física contiene la implementación del control, pero se identifica que se incumple constantemente.
11.2.8	Equipos de usuario desatendido.	**50**	Definido	La política de seguridad física contiene la implementación del control, pero se identifica que se cumple esporádicamente.
11.2.9	Política de escritorio y pantalla limpios.	**50**	Definido	La política de seguridad física contiene la implementación del control, pero se identifica que se cumple esporádicamente.
Cumplimiento de Subdominios: 50 %				
Cumplimiento del Dominio: 25 %				
A.12 Seguridad de las aplicaciones				
12.1 Procedimientos Operacionales y Responsabilidades				
12.1.1	Documentación de los procedimientos de operación.	**0**	Inexistente	No se cuenta con el control.
12.1.2	Gestión de cambios.	**0**	Inexistente	No se cuenta con el control.
12.1.3	Gestión de la capacidad.	**0**	Inexistente	No se cuenta con el control.
12.1.4	Separación de las instalaciones de desarrollo, pruebas y operación.	**0**	Inexistente	No se cuenta con el control.

Cuadro 4. (Continuación)

Numeral	Control	%	Nivel	Observaciones
12.2 Protección contra códigos maliciosos				
12.2.1	Controles contra códigos maliciosos.	**0**	Inexistente	No se cuenta con el control.
Cumplimiento del Subdominios: 0 %				
12.3 Copias de respaldo				
12.3.1	Copias de respaldo de la información.	**50**	Definido	Se cuenta con office 365 lo cual garantiza el respaldo en la nube y se tiene otra *backup* en cloud para servidores locales. Se identifican algunos servidores nuevos MV sin incluir.
Cumplimiento del Subdominios: 50 %				
12.4 Registro y seguimiento				
12.4.1	Registro de eventos.	**50**	Definido	En la Política de Seguridad Operativa Numeral 5.4.1, Estipula el control y en él la revisión del registro de eventos, pero no se cumple cada que se presenta un incidente.
12.4.2	Protección de la información de registro.	**50**	Definido	Se implementa para garantizar que todos los procedimientos que impliquen la modificación o manipulación de un activo de información queden registrados tanto del lado cliente, como del lado administrador, pero los *logs* no cuentan con la revisión regular como lo establece el control.
12.4.3	Registros del administrador y del operador	**50**	Definido	Se implementa el control, pero el documento Procedimiento Registro de fallas del sistema no está contemplado en la Política se seguridad operativa.

Cuadro 4. (Continuación)

Numeral	Control	%	Nivel	Observaciones
12.4.4	Sincronización de relojes.	**50**	Definido	Sin bien el control se implementa la política no indica de qué forma lograría sincronizar con una única fuente de referencia de tiempo.
Cumplimiento de Subdominios: 50 %				
12.5 Control de software operacional				
12.5.1	Instalación de software en sistemas operacionales.	**50**	Definido	Toda instalación de software tendrá previa autorización de la Gerencia de Tecnología, con su respectiva evaluación de riesgos, y pruebas realizadas antes de su instalación, aunque teniendo en cuenta los PC dispuestos para desarrollo este control no se cumple debidamente.
Cumplimiento de Subdominios: 50 %				
12.6 Gestión de la vulnerabilidad técnica				
12.6.1	Gestión de las vulnerabilidades técnicas.	**50**	Definido	Si bien la política está enfocada en los permisos a los usuarios autorizados, el control indica es la realización del análisis de vulnerabilidades técnicas de los sistemas de información que se usen; para así evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
12.6.2	Restricciones sobre la instalación de software.	**50**	Definido	Cuenta con un documento de referencia (Guía *Check list* para entrega de Pc) el cual no está siendo periódicamente actualizado ya que por la dinámica de la empresa es muy cambiante las herramientas que se instalan en la máquina de los desarrolladores.
Cumplimiento de Subdominios: 50 %				

Cuadro 4. (Continuación)

Numeral	Control	%	Nivel	Observaciones
12.7 Consideraciones sobre auditorías de sistemas de información				
12.7.1	Controles de auditorías de sistemas de información.	**50**	Definido	No se están evidenciando las actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y tal planificación no se evidencia.
Cumplimiento de Subdominios: 50 %				
Cumplimiento del Dominio: 35 %				
A.13 Seguridad de las comunicaciones				
13.1 Gestión de la seguridad de las redes				
13.1.1	Controles de redes.	**20**	Inicial	En la política de seguridad en las telecomunicaciones, se ha establecido el control ya que han ocurrido incidentes de seguridad, pero falta por definir y afinar la política.
13.1.2	Seguridad de los servicios de red.	**20**	Inicial	Falta por detallar este control dentro de la política de seguridad en las telecomunicaciones.
13.1.3	Separación en las redes.	**20**	Inicial	Falta por especificar este control dentro de la política de seguridad en las telecomunicaciones, aunque si se ha implementado.
Cumplimiento de Subdominios: 20 %				
13.2 Transferencia de información				
13.2.1	Políticas y procedimientos de transferencia de información.	**20**	Inicial	Hace falta documentar la política para transferencia de información.

Cuadro 4. (Continuación)

Numeral	Control	%	Nivel	Observaciones
13.2.2	Acuerdos sobre transferencia de información.	**20**	Inicial	En los contratos se están implementando acuerdos sobre la transferencia de información**.**
13.2.3	Mensajes electrónicos.	**20**	Inicial	Se debe documentar una política sobre el uso correcto y seguro del correo electrónico
13.2.4	Acuerdos de confidencialidad o de no divulgación.	**20**	Inicial	Falta actualizar los acuerdos de confidencialidad sobre la información que conocen los colaboradores.
Cumplimiento de Subdominios: 20 %				
Cumplimiento del Dominio: 20 %				
A 14 Adquisición, desarrollo y mantenimiento de sistemas				
14.1 Requisitos de seguridad de los sistemas de información				
14.1.1	Análisis y especificación de requisitos de seguridad de la información.	**20**	Inicial	En los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes no se plantea este análisis; siendo una fábrica de software debe definirse esta política.
14.1.2	Seguridad de servicios de las aplicaciones en redes públicas.	**20**	Inicial	Se incorporan mecanismos de protección de la seguridad de la información en las transacciones sobre redes públicas, pero no se respaldan con una política que ponga en claro las acciones realizadas.

Cuadro 4. (Continuación)

Numeral	Control	%	Nivel	Observaciones
14.1.3	Protección de transacciones de servicios de aplicaciones.	**20**	Inicial	Se incorporan mecanismos de protección de la seguridad de la información en las transacciones entre las aplicaciones, pero no se respaldan con una política que ponga en claro las acciones realizadas.
Cumplimiento de Subdominios: 20 %				
14.2 Seguridad en los procesos de desarrollo y de soporte				
14.2.1	Política de desarrollo seguro.	**20**	Inicial	No cuenta con una política que sirva de guía y control a los desarrollos nuevos y existentes, a pesar de implementarse mecanismos que protegen la información; no se encuentra documentación alguna, si se encuentra la empresa en un proceso de mejora en cuánto a la implementación de estándares de calidad en el desarrollo, pero de este tema de seguridad no se ha abordado.
14.2.2	Procedimientos de control de cambios en sistemas.	**20**	Inicial	Si bien se nombra en la documentación el procedimiento de desarrollo de software, no se encuentra definido un paso a paso para los cambios en los sistemas nuevos o existentes.

Cuadro 4. (Continuación)

Numeral	Control	%	Nivel	Observaciones
14.2.3	Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones.	**20**	Inicial	En los cambios a las plataformas de operación, se revisan las aplicaciones críticas del negocio, y se prueba para asegurar que no haya impacto adverso en las operaciones y de la seguridad de la organización. No se encuentra documentada esta revisión.
14.2.4	Restricciones en los cambios a los paquetes de software.	**20**	Inicial	Si existe un paso a paso frente a los cambios del software mediante la utilización de repositorios de datos en la nube, y bajo ciertos privilegios el rol específico realiza la modificación de los paquetes, pero esto no se encuentra definido en un documento.
14.2.5	Principios de construcción de los sistemas seguros.	**20**	Inicial	Se está definiendo procedimientos en el establecimiento de buenas prácticas en el desarrollo de software y esto debe contemplar la parte de aseguramiento de la información en la construcción de los sistemas de información y la implementación de estos estándares en las ya existentes.

Cuadro 4. (Continuación)

Numeral	Control	%	Nivel	Observaciones
14.2.6	Ambiente de desarrollo seguro.	**20**	Inicial	El área de desarrollo se encuentra configurando y estableciendo los distintos ambientes que deben tener los despliegues de los desarrollos; estas definiciones deben ser documentados para poder establecerlos de manera segura.
14.2.7	Desarrollo contratado externamente	**20**	Inicial	Este control no se encuentra documentado.
14.2.8	Pruebas de seguridad de sistemas	**20**	Inicial	Durante el desarrollo se llevan a cabo pruebas de funcionalidad de la seguridad bastante básicas, requiere incorporar mecanismos que prueben verdaderamente este aspecto y documentarlo.
14.2.9	Prueba de aceptación de sistemas	**20**	Inicial	Se encuentra en el proceso de análisis para el establecimiento de metodologías que permitan asegurar que se pueda dar implementación a este control, pero en tanto no se ha definido la documentación pertinente.
Cumplimiento de Subdominios: 20 %				

Cuadro 4. (Continuación)

14.3 Datos de Prueba				
Numeral	**Control**	**%**	**Nivel**	**Observaciones**
14.3.1	Protección de datos de prueba.	**20**	Inicial	A través del rol de Senior Developer se protege, controla, autoriza, selecciona y registra cuidadosamente los datos de prueba, a través de enmascaramiento. Pero dicho proceso no es explicado en la documentación.
Cumplimiento de Subdominios: 20 %				
Cumplimiento del Dominio: 20 %				
A.15 Relaciones con los proveedores				
15.1 Seguridad de la información en las relaciones con los proveedores				
15.1.1	Política de seguridad de la información para las relaciones con proveedores.	**20**	Inicial	Se tienen acuerdos de confidencialidad con los proveedores, pero falta una política clara que los defina.
15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores.	**20**	Inicial	Se deben definir acuerdos para el manejo de la información, a la cual tienen acceso los proveedores sobre la organización.
15.1.3	Cadena de suministro de tecnología de información y comunicación.	**20**	Inicial	Se debe documentar un proceso para llevar a cabo una cadena de suministro segura, para los productos y servicios de información recibidos.
Cumplimiento de Subdominios: 20 %				

Cuadro 4. (Continuación)

15.2 Gestión de la prestación de servicios				
Numeral	**Control**	**%**	**Nivel**	**Observaciones**
15.2.1	Seguimiento y revisión de los servicios de los proveedores.	**20**	Inicial	Se han realizado revisiones a los servicios prestados por los proveedores, pero no existe una documentación definida.
15.2.2	Gestión de cambios a los servicios de los proveedores.	**20**	Inicial	Se debe documentar una política de control de cambios para el manejo de información con los proveedores.
Cumplimiento de Subdominios: 20 %				
Cumplimiento del Dominio: 20 %				
A.16 Gestión de incidentes de seguridad de la información.				
16.1 Gestión de incidentes y mejoras en la seguridad de la información				
16.1.1	Responsabilidades y procedimientos.	**20**	Inicial	Falta establecer un proceso que indique los responsables de atender los incidentes según su clasificación.
16.1.2	Reporte de eventos de seguridad de la información.	**20**	Inicial	Falta un mecanismo definido para el reporte de los eventos.
16.1.3	Reporte de debilidades de seguridad de la información.	**20**	Inicial	Falta un mecanismo definido para el informar las debilidades encontradas.
16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.	**20**	Inicial	Falta una política que establezca el manejo de eventos.
16.1.5	Respuesta a incidentes de seguridad de la información.	**20**	Inicial	Falta generar la documentación necesaria para establecer procesos de respuesta a incidentes.

Cuadro 4. (Continuación)

Numeral	Control	%	Nivel	Observaciones
16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información.	**20**	Inicial	Se debe generar un portal de conocimiento de las lecciones aprendidas.
16.1.7	Recolección de evidencia.	**20**	Inicial	Falta una política de buenas prácticas de manejo de evidencia electrónica, tomando como referente la norma ISO 27037-2013.
Cumplimiento de Subdominios: 20 %				
Cumplimiento del Dominio: 20 %				
A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio.				
17.1 Continuidad de seguridad de la información				
17.1.1	Planificación de la continuidad de la seguridad de la información.	**20**	Inicial	Se debe definir un (BCI) plan de continuidad de negocio y un DRP (Plan de continuidad de negocio).
17.1.2	Implementación de la continuidad de la seguridad de la información.	**20**	Inicial	Se aconseja implementar Procesos de *Backup* y redundancia para dar continuidad a la organización.
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	**20**	Inicial	Se realizan pruebas parciales, más sin embargo no se tiene definido un proceso de simulacros.
Cumplimiento de Subdominios: 20 %				

Cuadro 4. (Continuación)

Numeral	Control	%	Nivel	Observaciones
17.2 Redundancias				
17.2.1	Disponibilidad de instalaciones de procesamiento de información.	**20**	Inicial	Se debe avanzar en la implementación de redundancia en servidores y canales para evitar la indisponibilidad de la información.
Cumplimiento de Subdominios: 20 %				
Cumplimiento del Dominio: 20 %				
A.18 Cumplimiento				
18.1 Cumplimiento de requisitos legales y contractuales				
18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales.	**50**	Definido	La gerencia jurídica realizó un análisis de la legislación aplicable en cuanto a seguridad de la información y se incluyeron como clausulas en los contratos y otros, si de los colaboradores de la compañía para garantizar el cumplimiento de estas.
18.1.2	Derechos de propiedad Intelectual.	**50**	Definido	La gerencia jurídica se realizó un análisis de la legislación aplicable en cuanto a seguridad de la información y referente a la propiedad intelectual de estricto cumplimiento aún se cuenta con aplicaciones que no han sido patentadas o registradas.

Cuadro 4. (Continuación)

Numeral	Control	%	Nivel	Observaciones
18.1.3	Protección de registros.	**50**	Definido	En los contratos de los funcionarios se encuentran clausuladas la normas que enmarcan este control y de estricto cumplimiento, pero hay contratos que requieren de otro si frente a las nuevas disposiciones legales que establece la empresa.
18.1.4	Privacidad y protección de información de datos personales.	**50**	Definido	La gerencia jurídica realizó un análisis de la legislación aplicable en cuanto a seguridad de la información y frente a la normatividad de protección de datos personales, pero se cuenta con algunos SI en donde se maneja información de los usuarios y no cuentan con la notificación para aceptación o negación, para el manejo de sus datos personales y debe ser implementado en todo sistema que cumpla lo reglamentado.
18.1.5	Reglamentación de controles criptográficos	**50**	Definido	Existe una política, pero no es implementada como se debiera y además existe un desconocimiento de estas.
Cumplimiento de Subdominios: 50 %				

Cuadro 4. (Continuación)

Numeral	Control	%	Nivel	Observaciones
18.2 Revisiones de seguridad de la información				
18.2.1	Revisión independiente de la seguridad de la información.	**0**	Inexistente	No se cuenta con el control, a falta de la completa gestión de la seguridad de la información no se ha establecido esta revisión.
18.2.2	Cumplimiento con las políticas y normas de seguridad.	**0**	Inexistente	No se cuenta con el control y debe hacer parte de las responsabilidades de los roles directivos de la compañía.
18.2.3	Revisión del cumplimiento técnico.	**0**	Inexistente	No se cuenta con el control y de debe incluir en el cronograma anual de auditorías de la compañía.
Cumplimiento de Subdominios: 0 %				
Cumplimiento del Dominio: 25 %				

Fuente: Los Autores

5.1.2 Resumen del cumplimiento de los controles de la norma ISO/IEC 27001:2013. En el cuadro 5 se puede evidenciar que el resultado del presente análisis arroja que Tecnofactory S.A.S, actualmente cumple con solo el 22 por ciento de los controles propuestos por el anexo A de la norma ISO 27001:2013 en sus diferentes dominios. Dicho lo anterior se hace evidente la necesidad de diseñar los controles faltantes para que posteriormente sean implementados y mejorar los que están parcialmente implementados.

Cuadro 5. Consolidado de cumplimiento de dominios

Numeral	Dominio	Porcentaje de cumplimiento
A.5	Políticas de Seguridad.	40%
A.6	Organización de la Seguridad de la Información.	28%
A.7	Seguridad en los Recursos Humanos.	0%
A.8	Gestión de Activos.	28%
A.9	Control de Acceso.	32%
A.10	Criptografía.	0%
A.11	Seguridad física y ambiental.	25%
A.12	Seguridad de las aplicaciones.	35%
A.13	Seguridad de las comunicaciones.	20%
A.14	Adquisición, desarrollo y mantenimiento de sistemas.	20%
A.15	Relaciones con los proveedores.	20%
A.16	Gestión de incidentes de seguridad de la información.	20%
A.17	Aspectos de seguridad de la información de la gestión de continuidad de negocio.	20%
A.18	Cumplimiento	25%
Estado de seguridad de los activos de información:		**22 %**

Fuente: Los Autores

5.2 IDENTIFICACIÓN, CLASIFICACIÓN Y VALORACIÓN DE ACTIVOS

5.2.1 Identificación de activos de información. Como parte de los requisitos mencionados en la norma ISO 27001:2013, es de vital importancia realizar y mantener actualizado el inventario de los activos de información y adicional debe clasificarse.

Atendiendo los anteriores criterios, se realizó el inventario de Activos de Tecnofactory S.A.S a través de diferentes reuniones con los lideres de cada proceso, para lograr establecer el listado y definir la codificación de cada categoría como se evidencia en el cuadro 6.

Cuadro 6. Categoría de activos

Categorías de activos	Identificador
Software	TSW
Información	TINF
Hardware	THW
Red	TRD
Persona	TPR

Fuente: Los Autores

En el cuadro 7 se observa el listado de activos de información de Tecnofactory SAS con su respectiva clasificación, identificador y descripción como se observa a continuación:

Cuadro 7. Lista de activos

Categoría de Activo	Id	Activo de Información	Descripción	Cantidad
Software	TSW1	Página Web	Página de la organización desarrollada en PHP. Incorpora despliegue de información vinculada a los clientes y proyectos desarrollados, lista de servicios que ofrece, descargas de APP, y la funcionalidad de convocatorias. Adicionalmente ofrece la posibilidad de consultar políticas de tratamiento de datos como de privacidad.	1
Software	TSW2	Backups	Alojados en máquinas virtuales en la nube de Microsoft Azure con el servicio Azure Backup. Debido a los costos generados por los b*ackup* generados, solo se conservan las copias de seguridad durante una semana.	1
Software	TSW3	Correo electrónico	Servidor de Microsoft Exchange online, con office 365, licenciamiento Bussines Standart, bussines Essentials, E3, E1.	1
Software	TSW4	Azure DevOps	Plataforma de servicios en la nube para repositorio, desarrollo, calidad y gestión de los proyectos de desarrollo de la compañía. Se posee una licencia bajo la cuenta corporativa de C&M Consultores tecnologiacm@outlook.com, se han implementado las siguientes herramientas dentro de la suite que cuenta: Azure Boards (etapa implementada) Azure Pipelines (etapa implementada) Azure Repos (etapa implementada) Azure Test Plans (etapa inicial)	1
Software	TSW5	Project	Herramienta Microsoft, que emplea la compañía para plasmar la administración de proyectos y programas de desarrollo. Versión cubierta por la adquirida de Office 365 que tiene la compañía.	1

Cuadro 7. (Continuación)

Categoría de Activo	Id	Activo de Información	Descripción	Cantidad
Software	TSW6	Power BI	Herramienta Microsoft para gestión de reportes gerenciales, se cuenta con licencias *BI Premium*.	15
Software	TSW7	SharePoint	Herramienta Microsoft empleada como repositorio de información de los proyectos de la compañía. Versión que se instala en las máquinas Office Pro-Plus con Office 365(última versión) a 64 bits o 32.	1
Software	TSW8	Antivirus	Herramienta para detección y eliminación de virus en los equipos de la compañía. Sophos ENDPOINT Security.	35
Software	TSW9	Licencias Visual Studio	Licencias de software para desarrollo	25
Software	TSW10	Licencias de Sistemas Operativos	Licenciamiento Windows 10 para los pc y portátiles	40
Software	TSW11	Licencias Office 365	Licenciamiento Office Pro-Plus con Office 365 (última versión) a 64 bits	25
Información	TINF1	Procedimientos del área	Documentación generada a partir del proceso de implementación del sistema de gestión de calidad, conteniendo variedad de formatos, guías que respaldan la organización corporativa de la empresa y apoyan las políticas establecidas. Dicho repositorio de información reposa en *SharePoint*.	1
Información	TINF2	Plan operativo	Documentación que se emplea como herramienta de gestión, que implementa la compañía para planificar las acciones que la empresa debe realizar para alcanzar los objetivos propuestos anualmente. Incluye procedimiento, tablero de control, gestión de indicadores, cronogramas e informes. Dicho repositorio de información reposa en *SharePoint*.	1

Cuadro 7. (Continuación)

Categoría de Activo	Id	Activo de Información	Descripción	Cantidad
Hardware	THW1	Servidor de Bases de datos Pruebas	Servidor alojado en máquina virtual en la nube Azure: Versión: MicrosoftSQL Server 2014 12.0.4 S.O: Windows (Windows Server 2012 R2 Datacenter) Tamaño: B2ms estándar (2 VCPU, 8 GiB de memoria) Azure Disk Encryption: No habilitado Disco de SO efímero: N/D Discos de datos:2	1
Hardware	THW2	Servidor de Bases de datos Producción	Servidor alojado en máquina virtual en la nube Azure: Versión: MicrosoftSQL Server 2014 12.0.4 S.O: Windows (Windows Server 2012 R2 Datacenter) Tamaño: B2ms estándar (4 VCPU, 14 GiB de memoria) Azure Disk Encryption: No habilitado Disco de SO efímero: N/D Discos de datos:8	1
Hardware	THW3	Servidor de Aplicaciones	Servidor Front End CMFE01 , alojado en máquina virtual en la nube Azure: S.O: (Windows Server 2012 R2 Datacenter) Tamaño: Estándar DS2, VCPU: 2, RAM: 7 GiB Azure Disk Encryption: No habilitado Disco de SO efímero: N/D Discos de datos:2	1
Hardware	THW4	Servidor de Aplicaciones	Servidor Front End TFFE03, alojado en máquina virtual en la nube Azure:S.O: (Windows Server 2016 Datacenter) Tamaño: Estándar DS1 v2 VCPU: 1 RAM: 3.5 GiB Azure Disk Encryption: No habilitado Disco de SO efímero: N/D Discos de datos:0	1

Cuadro 7. (Continuación)

Categoría de Activo	Id	Activo de Información	Descripción	Cantidad
Hardware	THW5	Servidor de Aplicaciones	Servidor Front End de pruebas, alojado en máquina virtual en la nube Azure: S.O: (Windows Server 2016 Datacenter) Tamaño: Estándar DS1 v2 VCPU: 1 RAM: 3.5 GiB Azure Disk Encryption: No habilitado Disco de SO efímero: N/D Discos de datos:0	1
Hardware	THW6	Computador AIO	Lenovo v530 Características: Procesador: i78700T. RAM:16 Gigabytes Monitor: Incorporado	9
Hardware	THW7	Computador AIO	Lenovo v530 Características: Procesador: i78700T. RAM:8 Gigabytes Monitor: Incorporado	1
Hardware	THW8	Computador AIO	Lenovo v530 Serie: MP1FK4BV Características: Procesador: I5 8400T. RAM:16 Gigabytes Monitor: Incorporado	4
Hardware	THW9	Computador AIO	Lenovo v530 Serie: SMP1FY40V Características: Procesador: I5 8400T. RAM:8 Gigabytes Monitor: Incorporado	1
Hardware	THW10	Computador Portátil	Lenovo E490 Procesador: i7 8550U RAM: 8 Gigabytes	1

Cuadro 7. (Continuación)

Categoría de Activo	Id	Activo de Información	Descripción	Cantidad
Hardware	THW11	Computador Portátil	Hewlett-Packard Modelo: 8265NGW Serial: 8CG9129YMM Características: Procesador: i7 7700HQ RAM: 12 Gigabytes	1
Hardware	THW12	Computador Portátil	Hewlett-Packard Modelo: omen 17 Serial: 5CD70370HV Características: Procesador: i7 7700HQ RAM: 12 Gigabytes	1
Hardware	THW13	Mac	Hewlett-Packard Modelo: Pro (retina 15-inch) Características: Procesador: i7 4 núcleos RAM: 16 Gigabytes	1
Hardware	THW14	Computador *Desktop*	Hewlett-Packard Modelo: JSD2 Procesador: i7 8700 RAM: 32 Gigabytes	1
Hardware	THW15	Dispositivos Biométricos	Las áreas de Tecnofactory S.A.S., se encuentran provistas con sistema de control de acceso a través de biométrico, lector de huellas dactilares conectado a la puerta de acceso de la oficina.	4

Cuadro 7. (Continuación)

Categoría de Activo	Id	Activo de Información	Descripción	Cantidad
Hardware	THW16	Impresora	La sede cuenta con un área de impresión con opción de impresión, escaneo y fotocopias. Impresora multifuncional HP 550 color laser jet	2
Red	TRD1	Switch	Herramienta para gestión de las comunicaciones de red de la compañía dispositivo Aruba de 24 puertos	1
Red	TRD2	Firewall	Herramienta para gestión de accesos de los computadores a la red de la compañía. *Firewall* en Nube BDOM Fortinet.	1
Red	TRD3	Telefonía	Servicio de telefonía fija planta y PBX administrables con 24 extensiones.	1
Red	TRD4	Red	Servicio de conectividad, con proveedor de servicios Claro.	1
Persona	TPR1	Arquitecto de software	Su objetivo es definir la arquitectura de los sistemas tomando las decisiones de diseño de alto nivel y estableciendo los estándares técnicos, incluyendo plataformas, herramientas y estándares de programación, teniendo en cuenta los requisitos funcionales, no funcionales y las necesidades del negocio. **Nivel educativo**: Profesional **Titulo obtenido**: Pregrado en Ingeniería de Sistemas, Ingeniería Electrónica, Ingeniería Telemática o afines. Posgrado en Gerencia de Tecnología, Arquitectura Empresarial de Software. **Experiencia**: +2 años de experiencia como Desarrollador Senior o equivalentes. +5 años de experiencia como coordinador o profesional en el área de desarrollo de sistemas de información. +6 años de experiencia en diseño y desarrollo de Software.	2

Cuadro 7. (Continuación)

Categoría de Activo	Id	Activo de Información	Descripción	Cantidad
			Complementaria: Herramientas ofimáticas; Office 365; desarrollo de Software bajo plataformas Android; patrones de diseño de interfaz; desarrollo en lenguaje .Net, bases de datos SQL; conocimiento en metodología ágil SCRUM.	
Persona	TPR2	Ingenieros Senior	Su objetivo es el generar un desarrollo de software centrado en el diseño, la codificación, las pruebas y la garantía de calidad de funciones complejas del producto. **Nivel educativo**: Profesional **Titulo obtenido**: Pregrado en Ingeniería de Sistemas, Ingeniería Electrónica, Ingeniería Telemática o afines. Posgrado en Gerencia Tecnología, Proyectos Informáticos o áreas relacionadas. **Experiencia**: +2 años de experiencia como Desarrollador Semi Senior o equivalentes. +2 años de experiencia como profesional en el área de desarrollo de sistemas de información. +3 años de experiencia en diseño y desarrollo de software. **Complementaria:** Herramientas ofimáticas; Office 365; desarrollo de Software bajo plataformas Android; patrones de diseño de interfaz; desarrollo en .Net, Golang, Angular, Vue y React; bases de datos SQL; conocimiento en metodología ágil SCRUM; integración de arquitecturas; integración de componentes tecnológicos de distintos fabricantes; repositorios de código fuente; parámetros de seguridad implícita en el código fuente.	2

Cuadro 7. (Continuación)

Categoría de Activo	Id	Activo de Información	Descripción	Cantidad
Persona	TPR3	Ingenieros Semi Senior	Su objetivo es coadyuvar en la planificación, diseño y desarrollo de sistemas de información para alcanzar el logro de los objetivos empresariales y la satisfacción de los clientes. **Nivel educativo**: Profesional **Titulo obtenido**: Pregrado en Ingeniería de Sistemas, Ingeniería Telemática, Ingeniería Electrónica o afines. **Experiencia:** +2 años de experiencia como Desarrollador Junior o equivalentes. +2 años de experiencia en diseño y desarrollo de software	2
Persona	TPR4	Ingenieros Junior	Su objetivo es coadyuvar en la planificación, diseño y desarrollo de sistemas de información para alcanzar el logro de los objetivos empresariales y la satisfacción de los clientes. **Nivel educativo**: Técnico, tecnólogo o profesional **Titulo obtenido**: Técnico o tecnólogo en sistemas o afines o recién graduados de Pregrado en Ingeniería de Sistemas, Ingeniería Telemática, Ingeniería Electrónica o afines o certificaciones de cursos de programación en plataformas reconocidas. **Experiencia:** Primer empleo o experiencia máxima de 6 meses en desarrollo de Sistemas de Información. **Complementaria:** Herramientas ofimáticas; Office 365; patrones de diseño de interfaz; desarrollo en lenguajes de nivel básico.	6

Cuadro 7. (Continuación)

Categoría de Activo	Id	Activo de Información	Descripción	Cantidad
Persona	TPR5	It Services Coordinator	Administrar la plataforma de Office 365, garantizar el correcto funcionamiento de equipos, red de internet, fibra óptica, WIFI, LAN y WAN. **Nivel educativo**: Técnico, tecnólogo o profesional **Titulo obtenido**: Técnico o Tecnólogo Sistemas, estudiante de últimos semestres o profesional en Ingeniería de Sistemas, Ingeniería Electrónica o afines **Experiencia:** +3 años de experiencia en actividades como administrador de plataformas, coordinador de soporte, mesa de ayuda y/o soporte técnico. **Complementaria:** Herramientas ofimáticas; Office 365; ISO 27001:13; conocimiento específico en plataformas tecnológicas (SharePoint, Orfeo)	1
Persona	TPR6	Service desk Analist	Su objetivo es analizar, revisar y documentar los requisitos de un plan de proyecto durante su ciclo de vida, hacer seguimiento y control con el fin de completar la ejecución dentro de su alcance planificado. **Nivel educativo**: Profesional **Titulo obtenido**: Profesional o estudiante últimos semestres de Ingeniería Industrial, Administración de Empresas o carreras administrativas. **Experiencia:** +6 meses y hasta 1 año de experiencia en actividades de soporte en gestión y operación de proyectos.	1

Cuadro 7. (Continuación)

Categoría de Activo	Id	Activo de Información	Descripción	Cantidad
Persona	TPR7	Service desk Agent	Su objetivo es realizar la instalación, configuración y puesta en marcha de equipos nuevos. **Nivel educativo**: Técnico, tecnólogo o profesional **Titulo obtenido**: Técnico o tecnólogo en Sistemas o afines o recién graduados de Pregrado en Ingeniería de Sistemas, Ingeniería Telemática, Ingeniería Electrónica o afines. **Experiencia:** Primer empleo o experiencia máxima de 6 meses de experiencia en atención a usuario final presencial y remoto. **Complementaria:** Herramientas ofimáticas; Office 365; ISO 27001; servicio al cliente; administración e instalación de equipos periféricos y prestación de servicios de tecnologías de la información bajo el marco de referencia ITIL.	1
Persona	TPR8	Software Documentation Writer	Su objetivo es investigar y producir las guías de instrucción, guías de ayuda en línea y de escritorio, interfaces de usuario, manuales de referencia y ayudas de trabajo para software informático y revisar la correcta utilización idiomática en estas. **Nivel educativo:** Técnico, tecnólogo o profesional **Titulo obtenido**: Tecnología en Gestión Documental o Pregrado en Ciencias de la Información y Bibliotecología o afines. **Experiencia:** +2 años como Analista o Personal de apoyo en Gestión Documental.	1

Fuente: Los Autores

5.2.2 Valoración y clasificación de activos de información. Posterior a la identificación y categorización de los activos de información se realiza una valoración de todos los activos identificados anteriormente y clasificados como en cada uno de los pilares de la información en una escala de 1 a 5 dependiendo de su importancia. En el cuadro 8. se define cada uno de estos criterios.

Cuadro 8. Criterios para la valoración de activos

Valor	Escala	Confidencialidad	Integridad	Disponibilidad
5	Muy Alto	La información del activo es catalogada como restringida y divulgación puede acarrear consecuencias casi irreparables.	La modificación de la información del activo afecta críticamente a la organización con daños casi irreparables.	El activo de información no está disponible por más de un día.
4	Alto	La información contenida por el activo requiere de una autorización para su divulgación.	La modificación de la información detiene todos los procesos hasta que se recupere su integridad.	El activo de información no está disponible en un rango de 8 a 24 horas.
3	Medio	La información contenida en el activo solo puede ser consultada por los procesos que les compete en la organización, o por requerimientos legales.	La modificación de la información del activo afecta determinados procesos hasta que se recupere la integridad de esta.	El activo de información no está disponible en un rango de 1 a 8 horas.

Cuadro 8. (Continuación)

Valor	Escala	Confidencialidad	Integridad	Disponibilidad
2	Bajo	La información contenida en el activo puede ser consultada por cualquiera en la organización.	Si se modifica la información del activo se puede recuperar su integridad con facilidad.	El activo de información no está disponible en un rango de 15 minutos a 1 hora.
1	Muy bajo	La información del activo puede ser publica y no afecta en a la organización.	La modificación de la información no genera daños significativos y se puede restablecer con facilidad.	El activo de información no está disponible por 15 minutos o menos.

Fuente: Los Autores

5.2.3 Criticidad de los activos de información. Para poder establecer la valoración del activo, se calcula con la sumatoria de la calificación otorgada en cada uno de los diferentes criterios (Confidencialidad, Integridad y Disponibilidad) teniendo como valor máximo el número 15 y como mínimo 3, con dichos valores se logra establecer la escala de criticidad como se muestra en el cuadro 9.

Cuadro 9. Escala de criticidad

Criticidad	Valoración
Muy Alto	**15**
	14
	13
Alto	**12**
	11
	10
Medio	**9**
	8
	7
Bajo	**6**
	5
	4
Muy bajo	**3**

Fuente: Los Autores

Teniendo en cuenta los criterios definidos previamente, en el cuadro 10 se realiza la valoración de criticidad correspondiente a cada uno de los activos de información, deteniendo en cuenta el identificador, nombre del activo, valoración y escala de criticidad.

Cuadro 10. Valoración de criticidad de activos de información

Id	Activo	Confidencialidad	Integridad	Disponibilidad	Valor	Criticidad
TSW1	Página Web	1	2	2	5	Bajo
TSW2	Backups	5	5	5	15	Muy Alto
TSW3	Correo electrónico	5	5	5	15	Muy Alto
TSW4	Azure DevOps	5	5	5	15	Muy Alto
TSW5	Project	5	5	2	12	Alto
TSW6	Power BI	4	5	3	12	Alto
TSW7	SharePoint	3	5	4	12	Alto
TSW8	Antivirus	5	5	5	15	Muy Alto
TSW9	Licencias Visual Studio	3	5	5	13	Muy Alto
TSW10	Licencias de Sistemas Operativos	3	5	5	13	Muy Alto
TSW11	Licencias Office 365	4	5	3	12	Alto
TINF1	Procedimientos del área	3	5	1	9	Medio
TINF2	Plan operativo	3	5	1	9	Medio
THW1	Servidor de Bases de datos Pruebas	2	4	3	9	Medio
THW2	Servidor de Bases de datos Producción	3	5	5	13	Muy Alto

Cuadro 10. (Continuación)

Id	Activo	Confidencialidad	Integridad	Disponibilidad	Valor	Criticidad
THW3	Servidor de Aplicaciones	**3**	**3**	**2**	**8**	Medio
THW4	Servidor de Aplicaciones	**3**	**3**	**2**	**8**	Medio
THW5	Servidor de Aplicaciones	**2**	**2**	**2**	**6**	Bajo
THW6	Computador AIO	**3**	**3**	**2**	**8**	Medio
THW7	Computador AIO	**2**	**3**	**2**	**7**	Medio
THW8	Computador AIO	**2**	**3**	**2**	**7**	Medio
THW9	Computador AIO	**3**	**3**	**2**	**8**	Medio
THW10	Computador Portátil	**3**	**3**	**2**	**8**	Medio
THW11	Computador Portátil	**3**	**3**	**2**	**8**	Medio
THW12	Computador Portátil	**2**	**3**	**2**	**7**	Medio
THW13	Mac	**3**	**3**	**2**	**8**	Medio
THW14	Computador Desktop	**3**	**3**	**2**	**7**	Medio
THW15	Dispositivos Biométricos	**3**	**2**	**2**	**7**	Medio
THW16	Impresora	**3**	**2**	**2**	**7**	Medio
TRD1	Switch	**2**	**4**	**3**	**9**	Medio
TRD2	Firewall	**5**	**5**	**5**	**15**	Muy Alto

Cuadro 10. (Continuación)

Id	Activo	Confidencialidad	Integridad	Disponibilidad	Valor	Criticidad
TRD3	Telefonía	**2**	**2**	**2**	**6**	Bajo
TRD4	Internet	**5**	**5**	**5**	**15**	Muy Alto
TPR1	Arquitecto de software	**2**	**1**	**1**	**4**	Bajo
TPR2	Ingenieros Senior	**2**	**1**	**1**	**4**	Bajo
TPR3	Ingenieros Semi Senior	**2**	**1**	**1**	**4**	Bajo
TPR4	Ingenieros Junior	**2**	**1**	**1**	**4**	Bajo
TPR5	It Services Coordinator	**2**	**1**	**1**	**4**	Bajo
TPR6	Service desk Analist	**2**	**1**	**1**	**4**	Bajo
TPR7	Service desk Agent	**2**	**1**	**1**	**4**	Bajo
TPR8	Software Documentation Writer	**2**	**1**	**1**	**4**	Bajo

Fuente: Los Autores

5.3 IDENTIFICACIÓN DEL RIESGO

5.3.1 Identificación de amenazas. Es de vital importancia identificar aquellos elementos que pueden afectar de manera negativa a los activos de información de Tecnofactory S.A.S, por ello se identifican las amenazas a las que puede estar más expuesta la organización y se categorizan estos elementos en el cuadro 11:

Cuadro 11. Amenazas

Categoría	Código	Descripción de Amenazas
Acciones no autorizadas	AMZ 1	Documentos corruptos o defectuosos
	AMZ 2	Suplantación de la cuenta
	AMZ 3	Uso no autorizado de equipo
	AMZ 4	Procesamiento ilegal de datos
	AMZ 5	Copia fraudulenta de software
Amenaza informática humana	AMZ 6	*Hacker, Cracker*
	AMZ 7	Ciber crimen
	AMZ 8	Terrorismo
	AMZ 9	Espionaje industrial
	AMZ 10	Infiltrados
Compromiso de funciones	AMZ 11	Generación corrupta o defectuosa de *backups*
	AMZ 12	Abuso de privilegios
	AMZ 13	Olvido de privilegios
	AMZ 14	Error en uso
	AMZ 15	Denegación de acciones
	AMZ 16	Brecha en disponibilidad de personal
Daños físicos	AMZ 17	Daño del servidor/dispositivo
Fallas técnicas	AMZ 18	Falla en el mantenimiento de sistema
	AMZ 19	Saturación del sistema
	AMZ 20	Funcionamiento deficiente de software
	AMZ 21	Funcionamiento deficiente de equipo
	AMZ 22	Falla de equipo
Información comprometida	AMZ 23	Revelación de información
	AMZ 24	Modificación de software con fines criminales
	AMZ 25	Modificación de hardware con fines criminales
	AMZ 26	Datos de fuentes no confiables
	AMZ 27	Robo de equipos
	AMZ 28	Robo de medios y/o documentos

Cuadro 11. (Continuación)

Categoría	Código	Descripción de Amenazas
Perdida de servicios esenciales	AMZ 29	Falla del servicio
	AMZ 30	Falla de energía eléctrica
	AMZ 31	Falla de equipo de comunicaciones

Fuente: Los Autores

5.3.2 Identificación de vulnerabilidades. Las vulnerabilidades son condiciones que pueden hacer que una amenaza afecte a un activo. Por sí solas no causan daños a los activos de información, a continuación, se categorizan y describen las vulnerabilidades a las que está expuesta Tecnofactory S.A.S en el cuadro 12.

Cuadro 12. Vulnerabilidades

Categoría	ID	Descripción de la Vulnerabilidad
Hardware	V 1	Falta o ausencia de mantenimiento
	V 2	Ausencia de sistema eficiente de control de cambios
	V 3	Ausencia de procedimiento de destrucción de medios
	V 4	Copias no controladas
Software	V 5	Fallas conocidas en el software
	V 6	Sesiones abiertas sin usuario presente
	V 7	Reusó de medios sin procedimiento de borrado seguro
	V 8	Incorrecta asignación de privilegios
	V 9	Parámetros incorrectos de configuración
	V 10	Ausencia de mecanismos para identificación y autenticación de usuarios
	V 11	Servicios innecesarios habilitados
	V 12	Ausencia de proceso efectivo de control de cambios
	V 13	Uso no controlado de software descargado
	V 14	Ausencia de protecciones físicas en puertas y ventanas
	V 15	Líneas de comunicación desprotegidas
Redes	V 16	Tráfico de datos sensibles no protegido
	V 17	Puntos únicos de falla
	V 18	Conexiones a redes públicas desprotegidas
	V 19	Ausencia de personal
	V 20	Procedimientos de selección de personal deficientes

Cuadro 12. (Continuación)

Categoría	ID	Descripción de la Vulnerabilidad
Personal	V 21	Entrenamiento en seguridad de la información deficiente o insuficiente
	V 22	Ausencia de mecanismos de monitoreo de personal
	V 23	Ausencia de políticas de uso correcto de activos de información
	V 24	Ausencia de conciencia en seguridad de la información
	V 25	Ausencia de procedimientos formales para registro y eliminación de usuarios
	V 26	Ausencia de procedimientos formales para revisión de privilegios
Organización	V 27	Ausencia de auditorías regulares de seguridad de la información
	V 28	Ausencia de procedimientos efectivos para gestión de riesgos
	V 29	Inadecuados tiempos de respuesta para servicios de mantenimiento
	V 30	Acuerdo de niveles de servicio desactualizados
	V 31	Ausencia de procedimientos para control de documentación
	V 32	Ausencia de procedimientos para la revisión de la seguridad
	V 33	Planes de continuidad desactualizados
	V 34	Ausencia de procedimientos para el control de paso a producción de software
	V 35	Ausencia de cláusulas sobre la seguridad de la información en los contratos de funcionarios
	V 36	Políticas de seguridad de la información desactualizadas

Fuente: Los Autores

5.4 ANALISIS DE RIESGO

Se realiza el análisis del riesgo utilizando la metodología cuantitativa para calcular su estimación, para ello se establecerán unos niveles de criticidad entre 1 y 5 tanto para la probabilidad como en el impacto y con ello se podrá realizar la multiplicación entre probabilidad e impacto para conocer el valor del riesgo.

5.4.1 Valoración de probabilidad. El cuadro 13 de valoración de la probabilidad fue establecido de acuerdo con los datos históricos de frecuencia de ocurrencia y a la experiencia brindada por los funcionarios responsables de los activos de información y se establecieron 5 niveles, un id, escala y descripción como se observa a continuación:

Cuadro 13. Valoración de probabilidad

Nivel	Id	Escala	Descripción
5	M+	Muy Alto	El evento ocurre con regularidad, una o varias veces al mes
4	A	Alto	El historial indica que tiene una alta probabilidad de ocurrir cada 3 meses
3	M	Medio	El evento puede ocurrir cada 6 meses
2	B	Bajo	El evento nunca ha ocurrido, pero puede que alguna vez suceda.
1	M-	Muy bajo	Es muy improbable que ocurra el evento, pero se puede generar en alguna circunstancia excepcional.

Fuente: Los Autores

5.4.2 Valoración del impacto. Se tendrá presente el aspecto financiero, ya que representa para Tecnofactory S.A.S pérdidas de dinero de manera directa o indirecta que impacta respectivamente según la escala estimada en violaciones a la confidencialidad, integridad y disponibilidad de la información.

En el aspecto legal representa para Tecnofactory S.A.S, posibles participaciones en acciones que incluyan responsabilidad penal o civil, e incluso puede llegar a incurrirse en violaciones a la legislación que resulten en la imposición de sanciones legales.

El otro aspecto que se contemplará en la escala de impactos es el aspecto de la imagen que puede comprometer a la empresa Tecnofactory S.A.S, en pérdida de

oportunidades de negocio/competencia, como también de pérdida de participación en el mercado.

Para la valoración del impacto se definen 5 niveles de criticidad con su respectivo id y tomando como referencia el impacto que tendría a nivel de confidencialidad, integridad y disponibilidad de la información, con respecto a los criterios definidos con anterioridad como se puede observar en el cuadro 14.

Cuadro 14. Valoración de impacto

Impacto					
Nivel	**ID**	**Escala**	**Confidencialidad**	**Integridad**	**Disponibilidad**
5	M+	Muy Alto	Si se pierde la confidencialidad del activo acarrea: Pérdida económica superior a 100 millones de pesos. Inicio de un proceso Penal. Afectación publica de la reputación de la organización.	Si se pierde la Integridad del activo acarrea: Pérdida económica superior a 100 millones de pesos. Inicio de un proceso Penal. Afectación publica de la reputación de la organización.	Si se pierde la Disponibilidad del activo acarrea: Pérdida económica superior a 100 millones de pesos. Inicio de un proceso Penal. Afectación publica de la reputación de la organización.
4	A	Alto	Si se pierde la confidencialidad del activo acarrea: Pérdida económica en un rango de 20 a 100 millones de pesos. Inicio de procesos jurídicos por parte de los clientes alegando daños y perjuicios.	Si se pierde la integridad del activo eso acarrea: Pérdida económica en un rango de 20 a 100 millones de pesos. Inicio de procesos jurídicos por parte de los clientes alegando daños y perjuicios.	Si se pierde la integridad del activo eso acarrea: Pérdida económica en un rango de 20 a 100 millones de pesos. Inicio de procesos jurídicos por parte de los clientes alegando daños y perjuicios.

Cuadro 14. (Continuación)

Nivel	ID	Escala	Confidencialidad	Integridad	Disponibilidad
			Es conocido por los clientes de la organización.	Es conocido por los clientes de la organización.	Es conocido por los clientes de la organización.
3	M	Medio	Si se pierde la confidencialidad del activo acarrea: Pérdida económica entre 5 a 20 millones de pesos. Inicio de auditorías externas donde se identifican los incumplimientos para sancionar a la organización. Es conocido por todos los miembros de la organización.	Si se pierde la integridad del activo acarrea: Pérdida económica entre 5 a 20 millones de pesos. Inicio de auditorías externas donde se identifican los incumplimientos para sancionar a la organización. Es conocido por todos los miembros de la organización.	Si se pierde la disponibilidad del activo acarrea: Pérdida económica entre 5 a 20 millones de pesos. Inicio de auditorías externas donde se identifican los incumplimientos para sancionar a la organización. Es conocido por todos los miembros de la organización.
2	B	Bajo	Si se pierde la confidencialidad del activo acarrea: Pérdida económica entre 500.000 pesos a 5 millones de pesos. Inicio de auditorías internas donde se establecen cambios correctivos. Es conocido solamente por el proceso responsable del activo.	Si se pierde la integridad del activo acarrea: Pérdida económica entre 500.000 pesos a 5 millones de pesos. Inicio de auditorías internas donde se establecen cambios correctivos. Es conocido solamente por el proceso responsable del activo.	Si se pierde la disponibilidad del activo acarrea: Pérdida económica entre 500.000 pesos a 5 millones de pesos. Inicio de auditorías internas donde se establecen cambios correctivos. Es conocido solamente por el proceso responsable del activo.

Cuadro 14. (Continuación)

Nivel	ID	Escala	Confidencialidad	Integridad	Disponibilidad
1	M-	Muy Bajo	Si se pierde la confidencialidad del activo: No tiene costo o es menor a 500.000 pesos. No se presenta ningún inconveniente jurídico. No se genera afectación a la imagen de la organización.	Si se pierde la confidencialidad del activo: No tiene costo o es menor a 500.000 pesos. No se presenta ningún inconveniente jurídico. No se genera afectación a la imagen de la organización.	Si se pierde la confidencialidad del activo: No tiene costo o es menor a 500.000 pesos. No se presenta ningún inconveniente jurídico. No se genera afectación a la imagen de la organización.

Fuente: Los Autores

5.4.3 Valoración del riesgo. Para la valoración del riesgo en el cuadro 15. se realiza la clasificación de las zonas de riesgo y los rangos de valoración para cada uno, este valor se obtiene de la multiplicación entre el valor asignado a la probabilidad de ocurrencia por el valor asignado al impacto que esto genera.

Cuadro 15. Valoración zona de riesgo

Zona de Riesgo	Valoración
Muy Alto	**15-25**
Alto	**10-14**
Medio	**5-9**
Bajo	**3-4**
Muy bajo	**2**

Fuente: Los Autores

5.4.4 Aceptación del riesgo. Según la valoración del riesgo obtenida se clasifican los riesgos aceptables e inaceptables para la organización, como se puede observar en el cuadro 16, los riesgos aceptables serán los valorados como medio, bajo o muy bajo los cuales no serán tratados y los asumirá Tecnofactory S.A.S, en el caso de los riesgos inaceptables serán aquellos valorados como muy alto y alto para los cuales se propone establecer un tratamiento que permita mitigarlos.

Cuadro 16. Aceptación del riesgo

Aceptables	Inaceptables
Medio	Muy Alto
Bajo	Alto
Muy bajo	

Fuente: Los Autores

5.4.5 Evaluación del riesgo Inherente. De acuerdo con la norma ISO 31000: 2018 de debe realizar primero el análisis del riesgo y posteriormente evaluar si el riesgo es aceptable o no según los criterios definidos con anterioridad, para cumplir con este requisito se diseñó el cuadro 17 en el cual encontramos el análisis de riesgo y la evaluación de cada uno según los parámetros que se definieron previamente.

Cuadro 17. Análisis y evaluación de riesgos

Id Riesgo	Id Activo	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Riesgo I	Valoración	Aceptable Si/No
TRI1	TSW1	AMZ 6	V5	3	5	15	Muy Alto	No
TRI2		AMZ 18	V29	3	5	15	Muy Alto	No
TRI3	TSW2	AMZ 22	V4	3	5	15	Muy Alto	No
TRI4		AMZ 6	V9	3	5	9	Muy Alto	No
TRI5	TSW3	AMZ 3	V8	2	4	8	Medio	Si
TRI6		AMZ 6	V9	3	4	12	Alto	No
TRI7	TSW4	AMZ 29	V2	3	4	12	Alto	No
TRI8		AMZ 2	V5	3	4	12	Alto	No
TRI9	TSW5	AMZ 9	V26	3	3	9	Medio	Si
TRI10		AMZ 13	V8	3	3	12	Alto	No
TRI11	TSW6	AMZ 22	V1	4	3	12	Alto	No
TRI12		AMZ 6	V9	3	3	9	Medio	Si
TRI13	TSW7	AMZ 22	V1	4	3	12	Alto	No
TRI14		AMZ 6	V9	3	3	9	Medio	Si
TRI15	TSW8	AMZ 29	V1	4	3	12	Alto	No
TRI16		AMZ 6	V9	3	3	9	Medio	Si
TRI17	TSW9	AMZ 22	V1	4	3	12	Alto	No
TRI18		AMZ 6	V9	3	3	9	Medio	Si
TRI19	TSW10	AMZ 22	V1	4	3	12	Alto	No
TRI20		AMZ 6	V9	3	3	9	Medio	Si
TRI21	TSW11	AMZ 22	V1	3	3	9	Medio	Si
TRI22		AMZ 6	V9	2	3	6	Medio	Si
TRI23	TINF1	AMZ 23	V4	4	3	12	Alto	No

Cuadro 17. (Continuación)

Id Riesgo	Id Activo	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Riesgo I	Criticidad	Aceptable Si/No
TRI24		AMZ 6	V9	3	3	9	Medio	Si
TRI25	TINF2	AMZ 23	V4	4	3	12	Alto	No
TRI26		AMZ 6	V9	3	3	9	Medio	Si
TRI27	THW1	AMZ 17	V11	3	4	12	Alto	No
TRI28		AMZ 18	V29	3	4	12	Alto	No
TRI29	THW2	AMZ 22	V4	3	5	15	Muy Alto	No
TRI30		AMZ 6	V9	3	5	9	Muy Alto	No
TRI31	THW3	AMZ 3	V8	3	5	15	Muy Alto	No
TRI32		AMZ 6	V9	3	5	15	Muy Alto	No
TRI33	THW4	AMZ 3	V11	3	5	15	Muy Alto	No
TRI34		AMZ 2	V5	3	5	15	Muy Alto	No
TRI35	THW5	AMZ 9	V26	3	3	9	Medio	Si
TRI36		AMZ 13	V8	3	4	12	Alto	No
TRI37	THW6	AMZ 22	V1	4	3	12	Alto	No
TRI38		AMZ 6	V9	3	3	9	Medio	Si
TRI39	THW7	AMZ 22	V1	4	3	12	Alto	No
TRI40		AMZ 6	V9	3	3	9	Medio	Si
TRI41	THW8	AMZ 22	V1	4	3	12	Alto	No
TRI42		AMZ 6	V9	3	3	9	Medio	Si
TRI43	THW9	AMZ 22	V1	4	3	12	Alto	No
TRI44		AMZ 6	V9	3	3	9	Medio	Si
TRI45	THW10	AMZ 22	V1	4	3	12	Alto	No
TRI46		AMZ 6	V9	3	3	9	Medio	Si
TRI47	THW11	AMZ 22	V1	3	3	9	Medio	Si

Cuadro 17. (Continuación)

Id Riesgo	Id Activo	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Riesgo I	Criticidad	Aceptable Si/No
TRI48		AMZ 6	V9	3	3	9	Medio	Si
TRI49	THW12	AMZ 22	V1	4	3	12	Alto	No
TRI50		AMZ 6	V9	3	3	9	Medio	Si
TRI51	THW13	AMZ 22	V1	4	3	12	Alto	No
TRI52		AMZ 6	V9	3	3	9	Medio	Si
TRI53	THW14	AMZ 22	V1	4	3	12	Alto	No
TRI54		AMZ 6	V9	3	3	9	Medio	Si
TRI55	THW15	AMZ 11	V4	3	4	12	Alto	No
TRI56		AMZ 6	V9	3	3	9	Medio	Si
TRI57	THW16	AMZ 22	V1	4	3	12	Alto	No
TRI58		AMZ 6	V9	3	3	9	Medio	Si
TRI59	TRD1	AMZ 5	V13	3	4	12	Alto	No
TRI60		AMZ 6	V9	3	3	9	Medio	Si
TRI61	TRD2	AMZ 23	V9	3	5	15	Muy Alto	No
TRI62		AMZ 6	V9	3	2	6	Medio	Si
TRI63	TRD3	AMZ 22	V1	4	3	12	Alto	No
TRI64		AMZ 6	V9	3	3	9	Medio	Si
TRI65	TRD4	AMZ 22	V1	4	3	12	Alto	No
TRI66		AMZ 6	V9	3	3	9	Medio	Si
TRI67	TPR1	AMZ 12	V26	3	3	9	Medio	Si
TRI68		AMZ 23	V21	3	3	9	Medio	Si
TRI69	TPR2	AMZ 13	V27	3	2	6	Medio	Si
TRI70		AMZ 24	V22	3	2	6	Medio	Si
TRI71	TPR3	AMZ 12	V24	3	2	6	Medio	Si

Cuadro 17. (Continuación)

Id Riesgo	Id Activo	Amenaza	Vulnerabilidad	Probabilidad	Impacto	Riesgo	Criticidad	Aceptable Si/No
TRI72		AMZ 14	V8	3	2	6	Medio	Si
TRI73	TPR4	AMZ 14	V23	3	2	6	Medio	Si
TRI74		AMZ 15	V26	3	2	6	Medio	Si
TRI75	TPR5	AMZ 12	V26	3	3	9	Medio	Si
TRI76		AMZ 23	V24	3	3	9	Medio	Si
TRI77	TPR6	AMZ 15	V27	3	1	6	Medio	Si
TRI78		AMZ 23	V24	3	1	3	Bajo	Si
TRI79	TPR7	AMZ 14	V22	3	1	3	Bajo	Si
TRI80		AMZ 28	V26	3	1	3	Bajo	Si
TRI81	TPR8	AMZ 15	V31	3	1	3	Bajo	Si
TRI82		AMZ 23	V24	2	2	4	Bajo	Si

Fuente. Los Autores

5.4.6 Mapa de calor del riesgo. De acuerdo con el análisis del riesgo anterior, se diseña un mapa de calor que permita identificar los riesgos en cada una de las zonas definidas de acuerdo con las valoraciones establecidas como se puede observar en el cuadro 18, con ello se identificará la zona de riesgo a la cual pertenece cada uno y esto facilitará la toma de decisiones para los criterios de aceptación y tratamiento.

Cuadro 18. Clasificación del mapa de calor

Tipo	**Categoría**	**Cantidad de riesgos por categoría**				
Impacto	Muy Alto	5	10	15	20	25
	Alto	4	8	12	16	20
	Medio	3	6	9	12	15
	Bajo	2	4	6	8	10
	Muy Bajo	1	2	3	4	5
		Muy Bajo	Bajo	Media	Alto	Muy Alto
		Probabilidad				

Fuente: Los Autores

Posterior a ello se clasifica cada uno de los riesgos en el mapa de calor, dependiendo de la valoración obtenida por cada uno como se puede observar en el cuadro 19.

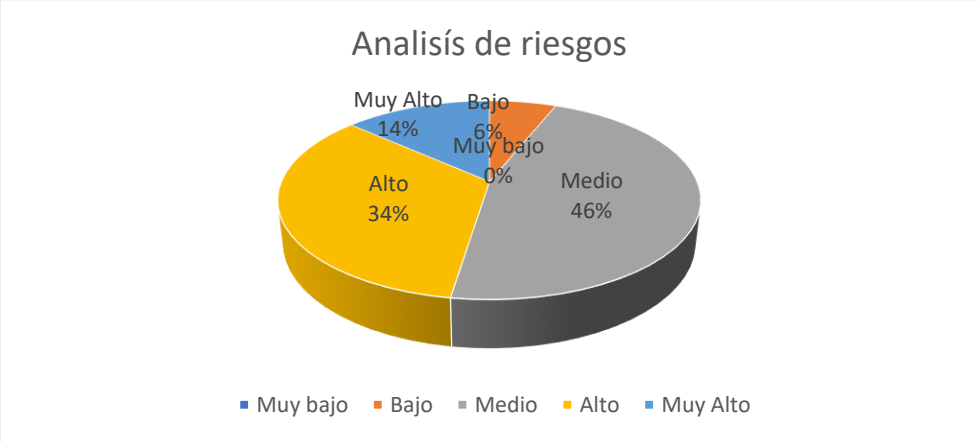
Cuadro 19. Mapa de calor

Tipo	Categoría	Tratamiento de riesgos por categoría				
Impacto	Muy Alto (5)			TRI1, TRI2, TRI3, TRI4, TRI29, TRI30, TRI31, TRI32, TRI33, TRI34, TRI61,		
	Alto (4)		TRI5	TRI6, TRI7, TRI8, TRI10, TRI27, TRI28, TRI36, TRI55, TRI59,		
	Medio (3)		TRI21,	TRI9, TRI12, TRI14, TRI16, TRI18, TRI20, TRI22, TRI24, TRI26, TRI35, TRI38, TRI40, TRI42, TRI44, TRI46, TRI47, TRI48, TRI50, TRI52, TRI54, TRI56, TRI58, TRI60, TRI64, TRI66, TRI67, TRI68, TRI75, TRI76,	TRI11, TRI13, TRI15, TRI17, TRI19, TRI23, TRI25, TRI37, TRI39, TRI41, TRI43, TRI45, TRI49, TRI51, TRI53, TRI57, TRI62, TRI63, TRI65,	
	Bajo (2)		TRI82	TRI62, TRI69, TRI70, TRI71, TRI72, TRI73, TRI74, TRI77,		
	Muy Bajo (1)			TRI78, TRI79, TRI80, TRI81,		
		Muy Bajo	Bajo	Media	Alto	Muy Alto
		Probabilidad				

Fuente: Los Autores

Como resultado del análisis se puede observar en la figura 4 los porcentajes correspondientes al resultado de la cantidad de riesgos clasificados en cada una de las escalas definidas.

Figura 4. Análisis de riesgos



Fuente: Los autores

Posterior al Análisis en la figura 5. Se puede observar los porcentajes de la evaluación realizada dando como resultado que el 52 % de los riesgos son aceptables, debido a que se encuentran en los rangos bajo y medio y el 48% de los riesgos no son aceptables ya que están categorizados en los rangos alto y muy alto, por lo cual se procederá a proponer un debido tratamiento para ellos.

Figura 5. Evaluación del riesgo

Fuente: Los autores

5.5 TRATAMIENTO DEL RIESGO

Después de clasificar cada uno de los riesgos y plasmarlos en el mapa de calor anterior, se tratarán aquellos catalogados como no aceptables según los criterios establecidos previamente con la finalidad de disminuir el impacto que puedan tener en caso de que se lleguen a materializar.

En el tratamiento descrito en el cuadro 20. se plantearon los controles propuestos en el anexo A de la norma ISO 27001:2013 para tratar los riegos no aceptables. Su posterior implementación permitirá conocer el riesgo residual realizando una nueva evaluación de la eficacia de cada control implementado.

Cuadro 20. Tratamiento del Riesgo

Id Riesgo	Control	Tratamiento
TRI1	A.14.1.1	Se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
	A.14.1.2	La información involucrada en servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
	A.14.2.2	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.
TRI2	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
	A.14.2.8	Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad
	A.14.2.9	Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba y criterios relacionados.
TRI3	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.

Cuadrado 20. Continuación

Id Riesgo	Control	Tratamiento
	A.12.6.1	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado
	A.12.3.1	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.
TRI4	A.12.6.1	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
	A.12.6.2	Se debe establecer e implementar el reglamento de instalación de software por parte de los usuarios.
	A.13.2.1	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
TRI6	A.12.3.1	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.
	A.9.4.1	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
	A.9.4.2	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de conexión segura.
TRI7	A.11.2.1	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, y las posibilidades de acceso no autorizado.
	A.11.2.2	Los equipos se deben proteger de fallas de potencia y otras interrupciones causadas por fallas en los servicios públicos de soporte.

Cuadrado 20. Continuación

Id Riesgo	Control	Tratamiento
	A.12.1.2	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
TRI8	A.11.2.8	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.
	A.12.4.1	Se deben elaborar, conservar y revisar regularmente los registros de eventos acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
	A.12.4.2	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.
TRI10	A.9.2.5	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben cancelar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
	A.9.2.6	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben cancelar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
	A.7.1.1	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
TRI11	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.

Cuadrado 20. Continuación

Id Riesgo	Control	Tratamiento
	A.12.6.1	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado
	A.12.3.1	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.
TRI13	A.9.4.4	Se debe restringir y controlar estrechamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.
	A.12.6.1	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado
	A.12.3.1	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.
TRI15	A.12.2.1	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.
	A.12.4.1	Se deben elaborar, conservar y revisar regularmente los registros de eventos acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
	A.12.4.4	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.

Cuadrado 20. Continuación

Id Riesgo	Control	Tratamiento
TRI17	A.11.2.7	Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reusó.
	A.11.2.6	Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de los predios de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichos predios.
	A.11.2.5	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.
TRI19	A.11.2.7	Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reusó.
	A.11.2.6	Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de los predios de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichos predios.
	A.11.2.5	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.
TRI23	A.9.1.2	Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
	A.7.1.2	Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información
	A.7.2.3	Se debe contar con un proceso formal y comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.

Cuadrado 20. Continuación

Id Riesgo	Control	Tratamiento
TRI25	A.9.2.6	Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben cancelar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.
	A.7.1.2	Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información
	A.7.2.3	Se debe contar con un proceso formal y comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
TRI27	A.12.3.1	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.
	A.9.4.1	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
	A.11.1.1	Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.
TRI28	A.9.2.2	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o cancelar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.
	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
	A.12.4.4	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.

Cuadrado 20. Continuación

Id Riesgo	Control	Tratamiento
TRI29	A.9.2.3	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
	A.13.1.1	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
	A.12.4.3	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad
TRI30	A.11.1.4	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
	A.12.2.1	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.
	A.12.6.1	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
TRI31	A.9.1.1	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.
	A.9.2.1	Se debe implementar un proceso formal de registro y de cancelación del registro, para posibilitar la asignación de los derechos de acceso.
	A.9.2.3	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.
TRI32	A.12.1.2	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
	A.11.1.4	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.

Cuadrado 20. Continuación

Id Riesgo	Control	Tratamiento
	A.12.2.1	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.
TRI33	A.9.4.1	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
	A.9.4.5	Se debe restringir el acceso a códigos fuente de programas.
	A.9.4.5	Se debe restringir y controlar estrechamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.
TRI34	A.12.2.1	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.
	A.10.1.2	Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de claves criptográficas, durante todo su ciclo de vida.
	A.11.2.8	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.
TRI36	A.9.4.3	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.
	A.9.4.4	Se debe restringir y controlar estrechamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.
	A.9.4.2	Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de conexión segura.

Cuadrado 20. Continuación

Id Riesgo	Control	Tratamiento
TRI37	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
	A.12.5.1	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
	A.12.1.4	Se deben separar los ambientes de desarrollo, prueba y operativos, para reducir los riesgos de acceso o cambios no autorizados al ambiente operacional.
TRI39	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
	A.12.5.1	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
	A.12.1.4	Se deben separar los ambientes de desarrollo, prueba y operativos, para reducir los riesgos de acceso o cambios no autorizados al ambiente operacional.
TRI41	A.12.6.2	Se debe establecer e implementar el reglamento de instalación de software por parte de los usuarios.
	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
	A.12.5.1	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
TRI43	A.12.6.2	Se debe establecer e implementar el reglamento de instalación de software por parte de los usuarios.
	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
	A.12.5.1	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.

Cuadrado 20. Continuación

Id Riesgo	Control	Tratamiento
TRI45	A.12.6.2	Se debe establecer e implementar el reglamento de instalación de software por parte de los usuarios.
	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
	A.12.5.1	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
TRI49	A.12.6.2	Se debe establecer e implementar el reglamento de instalación de software por parte de los usuarios.
	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
	A.12.5.1	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
TRI51	A.12.6.2	Se debe establecer e implementar el reglamento de instalación de software por parte de los usuarios.
	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
	A.12.5.1	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
TRI53	A.12.6.2	Se debe establecer e implementar el reglamento de instalación de software por parte de los usuarios.
	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
	A.12.5.1	Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.
TRI55	A.12.3.1	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.

Cuadrado 20. Continuación

Id Riesgo	Control	Tratamiento
	A.12.4.2	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado
	A.12.4.4	Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo
TRI57	A.13.2.4	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
	A.17.2.1	Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
TRI59	A.12.6.1	Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
	A.13.1.3	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes
	A.13.1.1	Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.
TRI61	A.13.1.2	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.
	A.12.4.1	Se deben elaborar, conservar y revisar regularmente los registros de eventos acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

Cuadrado 20. Continuación

Id Riesgo	Control	Tratamiento
	A.12.4.2	Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.
TRI63	A.12.6.1	Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
	A.11.2.4	Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.
	A.15.1.3	Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.
TRI65	A.15.2.2	Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos.
	A.16.1.3	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
	A.17.1.2	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.

Fuente: Los Autores

5.6 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

La política general rige el sistema de gestión de seguridad de la Información (SGSI), con el cual se establece el diseño, implantación, mantenimiento de procesos, donde se busca asegurar los principios de seguridad que comprenden la confidencialidad, integridad y disponibilidad de los activos de información que se alinean con la razón de ser de Tecnofactory S.A.S., empleándose como marco de referencia la norma ISO/IEC 27001:2013, se permite proteger y garantizar la seguridad de las personas, información y tecnología,

En virtud del Acuerdo de Operación conjunto suscrito por la compañía, todas las acciones de apoyo y documentación de estas en materia comercial (sector público), de gestión administrativa de talento humano, jurídica, gestión documental, mensajería, compras, financiera, tributaria, contable y de comunicaciones serán asumidas por las áreas o dependencias competentes de C & M Consultores S.A.S. bajo los procedimientos, guías y registros de sus Sistemas de Gestión de Calidad.

Objetivo. La presente Política de Seguridad de la Información tiene los siguientes objetivos:

- Garantizar la gestión y el funcionamiento de la seguridad de la información al interior de Tecnofactory S.A.S.

- Divulgar el Sistema de Seguridad de la Información dentro y fuera de Tecnofactory S.A.S.

- Proteger la información (medios de almacenamiento magnéticos, procesos y personas) de posibles fraudes, sabotajes, y riesgos que puedan poner en peligro los principios de la seguridad de la información confidencialidad, integridad y disponibilidad) lo cual es uno de los principales activos de Tecnofactory S.A.S.

- Definir los roles y responsabilidades de los propietarios de la información para garantizar el cumplimiento del SGSI.

Alcance**.** La organización ha definido el presente alcance del Sistema de Gestión de Seguridad de la información para sus operaciones a nivel nacional con única sede en Bogotá, ubicada en la Carrera 13 No. 97-76 oficina 502. Involucra todos los procesos establecidos en el Mapa de Procesos, para prestar servicios de fábrica de software, consultoría informática, administración de instalaciones informáticas, desarrollo de productos y soluciones de software y de sistemas informáticos (planificación, análisis, diseño, programación, pruebas), dando cumplimiento a las normas.

Tecnofactory S.A.S. ejerce control sobre las actividades contratadas para los procesos misionales y ejerce influencia decisoria sobre los productos y servicios contratados para los procesos de apoyo. En conclusión, el alcance para el Sistema de Gestión de Seguridad de la información y de acuerdo con los servicios que presta la organización es: “Servicios de fábrica de software, desarrollo de productos y soluciones tecnológicas y de sistemas informáticos que respondan a las necesidades y expectativas de los clientes”.

Declaración de la política de seguridad de la información: La presente política implanta las normas a seguir por los colaboradores de Tecnofactory S.A.S., donde se debe cumplir con los principios de seguridad (confidencialidad, integridad y disponibilidad) y calidad de la información (eficiencia, efectividad y confiabilidad) para configurar el Sistema de Gestión de Seguridad de la Información con el objetivo de:

- Proteger los activos de la información de posibles fraudes o amenazas que puedan materializarse e impactar.
- Definir e implementar las Políticas de Seguridad de la Información.
- Mantener la confiabilidad y la cultura del Sistema de Gestión de Seguridad de la Información, de los colaboradores y terceros.
- Estar a la vanguardia de la innovación tecnológica, al alcance de los recursos económicos para el mantenimiento del sistema de seguridad de la Información.

5.7 POLÍTICA TALENTO HUMANO

Objetivo: Hay que asegurar que todo el personal que mantiene algún tipo de relación contractual o comercial con Tecnofactory S.A.S. comprenda, aplique y controle sus actividades bajo los lineamientos de seguridad de la información, con el fin de mitigar los niveles de riesgo a los que pueden estar sometidos los activos de información (Personas - Procesos -Tecnología).

Alcance: La presente política aplica desde el proceso de reclutamiento, selección, durante la relación contractual y hasta la desvinculación parcial o total del personal de Tecnofactory S.A.S.

Declaración de la política: Se debe establecer procesos estrictos para el reclutamiento, la selección, vinculación y desvinculación de los colaboradores que tengan interacción con los activos de la información de la organización, con el fin de velar por la seguridad de la información y evitar pérdida de esta.

Lineamientos propuestos:

- Antes de la relación contractual**.** El área Administrativa de Talento Humano ha definido mediante el Manual de Descripción de Cargos los requisitos que debe cumplir el personal que ingresa a la compañía de acuerdo con las funciones y actividades que va a ejercer.

  Tecnofactory S.A.S. debe realizar el proceso de selección según las necesidades requeridas para la ejecución de sus actividades o la de sus proyectos, cumpliendo con lo determinado en la guía de reclutamiento, selección y vinculación de personal.

  Investigación de Antecedentes**.** El área de Talento Humano de Tecnofactory S.A.S. debe verificar los antecedentes laborales y judiciales de los candidatos, bajo lo establecido en la guía de reclutamiento, selección y vinculación de personal. Adicionalmente, Tecnofactory S.A.S. garantiza la protección de los datos recolectados.

- Los candidatos que cumplan con el perfil y sean seleccionados, deben firmar el acuerdo de aceptación y cumplimiento de la política de seguridad de la información (cláusula de confidencialidad) a través de la suscripción de su contrato.

- Términos y Condiciones del Empleo**.** Los candidatos que cumplan con el perfil y sean seleccionados, deben firmar el acuerdo de aceptación y cumplimiento de la política de seguridad de la información (cláusula de confidencialidad) a través de la suscripción de su contrato.

- Durante la relación contractual. En Tecnofactory S.A.S. se debe garantiza a través de la suscripción del contrato y la inducción de ingreso, que todos los colaboradores conozcan la política de seguridad de la información, las responsabilidades y los deberes que tienen con los activos de información asignados.

- Responsabilidades de la Gestión. En cumplimiento con la presente política los colaboradores de Tecnofactory S.A.S. deben aplicar sus responsabilidades en cuanto al manejo de los activos de información que tengan bajo su custodia o aquellos que por sus operaciones tengan acceso a los mismos. Al iniciar el vínculo contractual con la compañía serán conocedores de sus obligaciones, compromisos y normas que acatan el cumplimiento de la presente política. Los colaboradores de Tecnofactory S.A.S. deben contemplar las siguientes responsabilidades en cuanto al manejo de los activos de información:

- Evitar la destrucción, pérdida, modificación o fraude de los activos de información de acuerdo con las normas establecidas por la empresa en la Política de Gestión de Incidentes.

- Proceder acorde con la política general establecida para la seguridad de la información.

- En caso de ocurrir un incidente de seguridad de la información que comprometa los activos de información reportar el mismo de manera oportuna, de acuerdo con lo estipulado en la Política de Gestión de Incidentes.

- Concientización, educación y capacitación en seguridad de la información. El área de Talento Humano, según lo establecido en el procedimiento de gestión de recursos, debe realizar periódicamente capacitaciones en diversas temáticas, incluyendo, la seguridad de la información. Adicionalmente se lleva a cabo socialización de cambios o modificaciones de la política de seguridad de la información a través del área de comunicaciones.

  La inducción a la compañía incluirá aspectos como introducción a la política de seguridad de la información, responsabilidades y deberes del personal frente al sistema de gestión en seguridad de la información.

- Proceso Disciplinario. Cuando el personal de Tecnofactory S.A.S. incumple los parámetros establecidos en la Política de Seguridad de la Información se aplicará el procedimiento disciplinario del SGSI con el fin de investigar y sancionar dicha actuación.

  La Gerencia administrativa de Talento Humano de Tecnofactory S.A.S. verifica previamente si el personal vinculado ha incurrido en un incidente que ha puesto en riesgo la integridad, confidencialidad y disponibilidad de la información, El proceso se realiza de acuerdo con el impacto que haya tenido el incidente en la organización.

  Si se trata de una conducta inadecuada, de acuerdo con la Política de Gestión de Incidentes, se procederá a retirar inmediatamente los derechos de acceso a la plataforma tecnológica, contraseñas y privilegios y dependiendo de la gravedad se procederá de inmediato con la desvinculación contractual según el Procedimiento de Proceso Disciplinario. Se debe contar con la Política de Gestión de Incidentes.

  Desvinculación. El área Administrativa de Talento Humano ha establecido un proceso para la desvinculación del personal.

  Cese o Cambios de Puesto de Trabajo**.** El área Administrativa de Talento Humano con el apoyo del comité de seguridad de Tecnofactory S.A.S. es responsable del proceso de terminación contractual. En cumplimiento con la presente política los colaboradores que sean desvinculados deben completar el formato de paz y salvo, el cual, entre otros, deberá indicar que:

- Se ha hecho entrega de la información que tenían bajo su custodia.

- Se han entregado los activos de información a su cargo al jefe inmediato.

Dando cumplimiento a lo estipulado en la guía de contratación de personal, todos los trabajadores y contratistas de Tecnofactory S.A.S., una vez finalizada la relación contractual, tendrán la responsabilidad de hacer devolución de los activos de información, físicos y lógicos que le fueron entregados bajo su custodia.

Asimismo, procederá el bloqueo de todos los accesos lógicos a los sistemas de información y sistemas biométricos, evitando así los ingresos no autorizados.

5.8 POLÍTICA GESTIÓN DE ACTIVOS

Objetivo. Garantizar que todo el personal (colaboradores y terceros) comprenda las responsabilidades y el uso adecuado de los activos de información (Personas - Información -Tecnología), asignados por Tecnofactory S.A.S., que tiene bajo su custodia, con el fin de minimizar riesgos en los activos de información que puedan comprometer la continuidad del negocio.

Alcance. La presente política aplica desde la clasificación de la información, uso adecuado de todos los activos (Personas, Información, Tecnología), y los sistemas de información que hacen parte de Tecnofactory S.A.S. y está dirigida a todos los colaboradores y terceros, que sean propietarios de los activos de información o tengan acceso a ellos.

Declaración de la política. La Dirección General de Tecnofactory S.A.S. debe establecer procesos estrictos para las responsabilidades sobre los activos, clasificación de la información y administración de los activos de información, y de considerar que son de uso exclusivo de la organización y serán utilizados para la actividad comercial. Tecnofactory S.A.S. debe mantener actualizado el registro de sus activos y de los propietarios de la información encargados de su clasificación.

Lineamientos propuestos:

Responsabilidad por los activos. Tecnofactory S.A.S. debe proteger adecuadamente los activos de la organización asignándoles un propietario que se responsabiliza e identifica los controles apropiados para conservar la información de estos.

Inventario de activos. Todo activo tecnológico propio o en categoría de préstamo donde se guarde información de los procesos de Tecnofactory S.A.S. se debe encontrar en el inventario de activos de la organización, el cual debe actualizarse cada vez que se adquiera un activo nuevo, en calidad de préstamo o haya finalizado

su vida útil, con el fin de proteger la información contenida en ellos. Ver Procedimiento Gestión de Activos. El área Administrativa de Talento Humano maneja un listado de los colaboradores que se encuentran vinculados a la organización. La Dirección general maneja un listado maestro de registros y documentos importantes para la organización, con el fin de conocer el manejo y custodia de la información.

Propiedad de los Activos de Información. A través del inventario de activos de la organización se identifica el responsable y propietario de los activos de información, su manejo y uso adecuado. Se debe contar con (Procedimiento Gestión de Activos). Tecnofactory S.A.S. debe establecer que el propietario de los activos de información es responsable de:

- Garantizar y velar por la protección de la información de los activos de información que tiene bajo su custodia.

- Establecer parámetros de acceso a los activos de información de acuerdo con lo contemplado en la Política de Seguridad Física y Política de Control de Acceso.

- Uso Aceptable de los Activos**.** La presente política define las reglas de uso de los activos de información de Tecnofactory S.A.S. Es de cumplimiento obligatorio para colaboradores y terceros de Tecnofactory S.A.S.

- El correo electrónico corporativo y el manejo de internet son de uso exclusivo para la actividad comercial y administrativa de la organización.

- El uso de portátiles manejados dentro y fuera de la organización es permitido para la operación de sus funciones alineadas con la actividad comercial y operativa de la organización.

- Los activos de información solo serán utilizados para la operación de sus funciones y alineados con la actividad comercial de la organización y cualquier recurso o activo de información que se encuentre bajo su responsabilidad.

- Devolución de activos. Cuando se finaliza cualquier relación contractual con un colaborador o tercero y que maneje los activos de Tecnofactory S.A.S., el colaborador debe hacer entrega oficial de los activos que se encuentran definidos en el inventario de la organización, como se encuentra establecido en la Política de Talento Humano.

- Clasificación de la información. Tecnofactory S.A.S. define que el activo más significativo es la información por lo tanto debe ser protegida y administrada de manera adecuada, con el fin de garantizar la integridad, confidencialidad y disponibilidad de esta. La clasificación de la información evita el acceso no

autorizado, modificación o eliminación de la información garantizando la calidad del Sistema de Gestión de Seguridad de la Información.

- El CEO a través de los directores y líderes de área de Tecnofactory S.A.S. para afirmar la seguridad y protección de los activos de información, define e implementa una serie de controles de acuerdo con su necesidad comercial, considerando los siguientes aspectos para su correcta clasificación:

- Toda la información física o lógica de la organización es clasificada en los siguientes niveles de acuerdo con su grado de sensibilidad: Confidencial, Privada y Pública.

- La información clasificada puede ser reclasificada según el criterio de su propietario o por requerimientos legales.

- La información se debe clasificar de acuerdo con los niveles de protección establecidos en la Políticas de Control de Acceso Lógico y la Políticas de Seguridad Física por lo tanto se definió el Procedimiento Administración de Documentos y Registros de acuerdo con el riesgo, prioridad y grado de protección del activo.

Niveles de clasificación: Para garantizar los principios básicos de la seguridad de la información (confidencialidad, integridad y disponibilidad), Tecnofactory S.A.S. define los siguientes criterios de clasificación:

- Información Confidencial: Se considera confidencial, aquella información cuyo acceso no autorizado o acceso exclusivo a nivel de área, su divulgación representa algún riesgo económico, comercial o legal para Tecnofactory S.A.S.

- Información Privada: Se considera privada, aquella información que su acceso es compartido por su propietario para los colaboradores de la organización, donde no se ve comprometida la integridad y disponibilidad de procesos internos de Tecnofactory S.A.S.

- Información Pública: Se considera pública toda información que ha sido declarada de conocimiento público por su propietario. Su acceso, uso, disponibilidad, no representa algún riesgo para Tecnofactory S.A.S.

Responsables de la clasificación de la información**:** El colaborador propietario de la información es responsable de brindarle la protección de acuerdo con los niveles (Confidencial, Privada y Pública). El colaborador propietario tiene la responsabilidad de actualizar su criterio de clasificación periódicamente y reafirmar la asignación para verificar su aplicabilidad.

Directrices de clasificación: Se consideran los siguientes aspectos generales para la clasificación:

- Cada área debe definir la clasificación de los activos de información que tengan a su custodia.

- Todos los archivos, e-mail, registros sensibles de la operación, cualquier obtención física o lógica almacenadas o en tránsito que contengan diferentes niveles de clasificación se protegen según el nivel.

- Los colaboradores no deben tener información confidencial de la organización almacenada en sus dispositivos o equipos de escritorio a menos que sea solo una copia del original.

- La información digital de Tecnofactory S.A.S. que se encuentra almacenada en dispositivos de propiedad tercerizada (arriendo) debe ser eliminada antes de la devolución.

Etiquetado y manejo de la información: La Dirección General de Tecnofactory S.A.S. estableció el método de clasificación de la información que adoptó la organización, donde se incluyen los activos de información en formato físico o electrónico. El procedimiento utilizado cubre los siguientes tipos de recursos de información:

- Copia.
- Almacenamiento.
- Transmisión por correo personalizado y correo electrónico.
- Transmisión verbal, a través de telefonía móvil, reuniones y máquinas de respuesta automática.
- Destrucción de información.
- Impresión.

Manipulación de activos: Para determinar el criterio de clasificación de la información, el propietario debe tener en cuenta el impacto que puede generar a la organización, en caso de ser divulgada, alterada o destruida sin previa autorización. El propietario debe tener en cuenta los siguientes aspectos:

- Costos para la organización para reemplazarla o reconstruirla.
- Interrupción en las actividades comerciales y operativas de la organización.
- Pérdida de confianza por parte de los clientes, proveedores o colaboradores hacia la organización.
- Incumplimiento en las normas regulatorias y legales en las que está expuesta la organización.
- Perdida de integridad y disponibilidad de los datos críticos de la organización.

Gestión de soportes extraíbles: La Gerencia de Tecnología a través del *IT Support Coordinator* establece la forma para el adecuado uso y administración de todo dispositivo u objeto que contiene información de Tecnofactory S.A.S. Es indispensable contar con los siguientes aspectos:

- El contenido de todo medio reutilizable debe ser irrecuperable, si ya no son necesarios realizando un formateo a bajo nivel por parte del Analista de soporte.
- Mantener el almacenaje de la información de usuarios retirados a través del Analista de soporte.

- Eliminación de medios. La Gerencia de Tecnología a través del *IT Support Coordinator* establece que los Analistas de soporte son el personal autorizado para la adecuada eliminación de medios de información perteneciente a Tecnofactory S.A.S. para llevar a cabo esta actividad de forma controlada. Cada proceso de eliminación deberá ser analizado, autorizado, documentado y ejecutado por personal autorizado.

- Medios físicos en tránsito: La información es protegida en el momento de ser transportada al interior o exterior de las instalaciones de Tecnofactory S.A.S, asignando externamente responsables en el momento de su transporte, mediante los servicios de mensajería propios, servicios de mensajería tercerizada y embalaje dependiendo el tipo de información a manejar.

5.9 POLÍTICA CONTROL DE ACCESOS

Objetivo: Definir todas las pautas para reglamentar el acceso de los usuarios a los recursos tecnológicos de Tecnofactory S.A.S, con el fin de preservar la integridad, confidencialidad y disponibilidad de la información y de los mismos recursos.

Alcance: Esta política aplicará a todo el personal vinculado laboralmente con Tecnofactory S.A.S, contratistas y terceros que tengan acceso a los recursos físicos y de información de la organización.

Declaración de la política: Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado; esto es, de su identificador de usuario (*userID*) y contraseña (*password*) necesarios para acceder a la información y a la infraestructura tecnológica de Tecnofactory S.A.S, por lo cual deberá mantenerlo de forma confidencial. Tecnofactory, otorga la autorización para que se tenga acceso a la información que se encuentra en la infraestructura tecnológica, concediendo los permisos mínimos necesarios para el desempeño de sus actividades.

Controles de acceso lógico:

- El acceso a la infraestructura tecnológica de Tecnofactory S.A.S, para personal externo debe ser autorizado por funcionario competente, quien deberá notificar por el medio establecido (correo electrónico) al área de operaciones o soporte que este asignado para habilitar el respectivo acceso.

- Se prohíbe que los usuarios utilicen la infraestructura tecnológica de Tecnofactory S.A.S, para obtener acceso no autorizado a la información u otros sistemas de información.

- Todos los usuarios de los servicios de información son responsables por su identificador de usuario y contraseña que recibe para el uso y acceso adecuado.

- Todos los usuarios deberán autenticarse por los mecanismos de control de acceso establecidos por la Gerencia de Tecnología, dar su aceptación de uso razonable y firmar la aceptación de políticas del SGSI antes de poder utilizar la infraestructura tecnológica.

- Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica Tecnofactory S.A.S, a menos que se tenga autorización por parte de la Dirección General de la compañía.

- Cada usuario que accede a la infraestructura tecnológica de Tecnofactory S.A.S, debe contar con un identificador de usuario único y personalizado, por lo cual no está permitido el uso de un mismo identificador de usuario por varios usuarios.

- Los usuarios tienen prohibido compartir su identificador de usuario y contraseña, ya que todo lo que ocurra con ese identificador y contraseña será responsabilidad exclusiva del usuario al que pertenezcan, salvo prueba de que le fueron usurpados esos controles.

Administración de privilegios:

- Cualquier cambio en los roles y responsabilidades de los usuarios, que modifique sus privilegios de acceso a la infraestructura tecnológica de Tecnofactory S.A.S., deberán ser notificados por escrito o vía correo electrónico, con el visto bueno del líder del área solicitante, para realizar el ajuste.

Equipo desatendido:

Los usuarios de Tecnofactory S.A.S., deberán mantener sus equipos de cómputo con controles de acceso como contraseñas y protectores de pantalla previamente

configurados y autorizados, como una medida de seguridad cuando el usuario necesita ausentarse de su escritorio por un tiempo prolongado.

Administración y uso de contraseñas:

La asignación de la contraseña para acceso a la red y la contraseña para acceso a los sistemas de información debe ser realizada de forma individual, por lo que queda prohibido el uso de contraseñas compartidas.
Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá reportarlo por escrito mediante los canales de comunicación establecidos, indicando si es de acceso a la red o a otros sistemas, para que se le proporcione una nueva contraseña.

La obtención o cambio de una contraseña debe hacerse de forma segura; el usuario deberá acreditarse ante los sistemas de información, como usuario autorizado.

Está prohibido que los identificadores de usuarios y contraseñas se encuentren de forma visible en cualquier medio impreso o escrito en el área de trabajo del usuario, de manera de que se permita a personas no autorizadas su conocimiento.

Todos los usuarios deberán observar los siguientes lineamientos para la construcción y manejo de sus contraseñas:

- No deben contener números consecutivos.

- Deben estar compuestos de al menos ocho (8) caracteres, estos caracteres deben ser alfanuméricos, o sea, números y letras.

- Todo usuario que tenga la sospecha de que su contraseña es conocido por otra persona, tendrá la obligación de cambiarlo inmediatamente.

- Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione facilidad de acceso.

- Los cambios o desbloqueo de contraseñas solicitados por el usuario serán solicitados por correo electrónico por el jefe inmediato del usuario que lo requiere.

5.10 POLÍTICA CIFRADO

Objetivo: El objetivo del presente documento es definir reglas para el uso de los controles y claves criptográficas para proteger la confidencialidad, integridad, autenticidad e inviolabilidad de la información.

Alcance: Esta política aplica a todo tipo de información que sea gestionada, almacenada, trasmitida o transportada usando la infraestructura de tecnología de información y comunicaciones, o medios de almacenamiento de Tecnofactory S.A.S. y que de acuerdo con su nivel de clasificación o riesgos puede estar expuesta y debe ser cifrada para evitar su acceso a personas o sistemas de información no autorizados.

Declaración de la política: La Política de Cifrado de Información hace referencia a la declaración de los lineamientos definidos por la Dirección General de Tecnofactory S.A.S., para comprender y aplicar el manejo de cifrado de datos relacionada con la seguridad de la información y que proporciona los criterios necesarios para definir y delimitar las responsabilidades que intervienen en las diversas actuaciones técnicas, operacionales y administrativas.

Frente a los controles criptográficos:

- La información con carácter reservado o que por los procesos en que se utilice esté expuesta a riesgos de pérdida de confidencialidad se debe cifrar.

- El comité de Seguridad de la Información de Tecnofactory S.A.S. determinará los mecanismos de cifrado de datos que mejor se ajusten a las necesidades específicas de cada tipo de información.

- Las contraseñas para cifrado de información se deben proteger y gestionar siguiendo los controles de seguridad definidos para la protección de contraseñas de Tecnofactory S.A.S.

- Cuando se utilicen sistemas de intercambio de información como correos electrónicos, sistemas de transferencias de datos o sistemas de información para intercambio de datos con otras entidades u organizaciones en los que viaje información con carácter reservado deben emplear mecanismos de cifrados autorizados por los responsables de áreas y procesos.

- Al realizar el cifrado de información, se debe mantener copia de las llaves de cifrado en lugar seguro de forma que la recuperación de la información cifrada sea factible en caso de ausencia temporal o permanente del custodio de la información cifrada.

5.11 POLÍTICA SEGURIDAD FÍSICA

Objetivo: Prevenir e imposibilitar el acceso físico no autorizado a los activos críticos de Tecnofactory S.A.S., preservando las áreas seguras, acceso público, protección de los equipos, ante daños o perdidas de los activos de la organización e interrupciones a las actividades del negocio.

Alcance: La presente política compromete a todo el personal interno y externo que tiene relación contractual con Tecnofactory S.A.S. y aplica a todo tipo de acceso físico a los activos de información que integran los sistemas de la organización.

Declaración de la política: El acceso a las instalaciones de Tecnofactory S.A.S. debe cumplir con las políticas funcionales y procedimientos de seguridad física, con el fin de evitar el acceso no autorizado, que puedan ocasionar daño perdida o interferencia a los recursos e infraestructura de la organización.

Lineamientos propuestos:

- Áreas seguras: Tecnofactory S.A.S. protege los activos de información de acceso físicos no autorizados y a todas las áreas en las que se manejen información sensible o crítica, entre las cuales se consideran: Oficina Principal Carrera 13 No 97 - 76 Of. 502 - Centro de datos - Discos duros con *Backups* históricos - Servidores externos de servicio web y correo electrónico.

Perímetro de Seguridad Física:

- La Dirección estableció el uso de barreras como puertas de acceso Puerta principal Of.502, control de acceso biométrico, muros y paredes, puesto de recepción atendido por el personal del edificio Astaf.
- El área de instalaciones de procesamiento o información sensible cuenta con solidez física (puertas para racks, puertas para servidores).
- El área que contiene equipos o dispositivos que suministren y soporten las funciones críticas del negocio se encuentran completamente restringidos del acceso a personal no autorizado y separadas del ambiente de las oficinas. Toda persona que ingrese o acceda a las áreas seguras debe registrarse en la recepción de Tecnofactory S.A.S. y deberá portar visiblemente un *sticker* que lo identificará como visitante.
- El acceso principal de atención al público de Tecnofactory S.A.S. se encuentra monitoreado con cámaras de seguridad para la vigilancia del acceso a las áreas seguras.
- Las áreas o puertas que indican acceso restringido permanecen cerradas, con acceso autorizado y controlado por el registro de visitantes en la recepción de Tecnofactory S.A.S.

Controles de Acceso Físico:

- Tecnofactory S.A.S. establece el registro de entrada y salida ubicado en la recepción para visitantes, el cual será monitoreado de manera periódica y aleatoria.
- En caso de terminación, transferencia o cambio de las funciones del personal, los privilegios de acceso físico deben ser bloqueados o modificados por la mesa de servicios, una vez sea reportada la novedad por el área Administrativa de Talento Humano. En caso de terceros que se encuentren laborando dentro de las instalaciones deben ser identificados como visitantes y cumplir con los controles y lineamientos de seguridad establecidos por Tecnofactory S.A.S.
- El personal que este prestando un servicio temporal a la compañía (Consultorías, Mantenimientos, asesorías entre otros) contará con autorización previa de acceso e identificación clara de la empresa a la cual está vinculado que deberá portar de forma visible.
- Se realiza entrega de documentos y archivos transportados hacia las instalaciones de Tecnofactory S.A.S. en la recepción a través del analista Administrativo.

Seguridad en Oficinas Recintos e Instalaciones:

- Las áreas de Tecnofactory S.A.S. se encuentran provistas con sistema de control de acceso a través de biométrico, CCTV, control de incendios y todos aquellos sistemas que garanticen la continuidad del servicio y seguridad de la información.
- La gestión de TI realizará la programación de visitas de proveedores para realizar revisión del funcionamiento de manera periódica a todos los sistemas de control de acceso de la organización. (cuenta con Procedimiento de mantenimiento de los equipos). • Sistema biométrico • Cámaras de • Detectores de humo
- Los recursos tecnológicos críticos de Tecnofactory S.A.S. que procesan, almacenan o transmiten información no deben tener acceso al público.

Ubicación de Impresora, Copiadoras y Maquinas de Fax:

- Las impresoras se encuentran en áreas seguras para prevenir el acceso, transmisión no autorizada o duplicación de documentos.

- La información sensible proveniente de medios de impresión, copiadoras, y máquinas de fax debe ser retirada de forma inmediata y no se debe dejar por tiempo prolongado.

Protección Contra Amenazas Externas y Ambientales:

- Todos los sistemas de controles ambientales, tales como: sistemas contra fuego, sistemas de refrigeración, ventilación y sistemas eléctricos de la organización deben estar en permanente funcionamiento y estar localizados adecuadamente. Ver Procedimiento de Mantenimiento de Equipos

- Los procedimientos de emergencia fueron definidos por la organización, documentados y aprobados mediante la implementación del Plan de Emergencia aplicable en la sede de Tecnofactory S.A.S.

- Está prohibido el consumo de cigarrillo, bebidas alcohólicas y comidas en las áreas de Tecnofactory S.A.S. que procesan, almacenan o transmiten información.

- En caso de contratos con proveedores que tengan acceso a la información de Tecnofactory S.A.S., se debe contemplar acuerdos de confidencialidad.

Trabajo en Áreas Seguras:

Las áreas de procesamiento, almacenamiento y transmisión de información serán conocidas por los colaboradores y terceros de Tecnofactory S.A.S. solo cuando sea necesario o sus funciones lo requieran.

Todas las labores que sean de procesamiento y manejo de información confidencial corporativa serán monitoreadas y supervisadas por La gestión de TI cuando se requiera, con:

- CCTV
- *Firewall*
- Sistema Biométrico
- Registro de *logs* de los sistemas

Los colaboradores, y terceros que mantienen una relación contractual con Tecnofactory S.A.S., sólo podrán acceder a las áreas seguras de la organización que procesan, almacenan o transmiten información cuando sea requerido. Este acceso será planeado, autorizado y supervisado. (ver Procedimiento control físico de entrada)

Áreas de Carga, Despacho y Acceso Público. Tecnofactory S.A.S. en las áreas de carga y despacho definió controles para restringir acceso al personal no autorizado:

- No se cuenta con área de carga y despacho, por tal motivo el horario definido para el ingreso de suministros o correspondencia estará coordinado con la administración del edificio.

- El personal autorizado tiene la responsabilidad de la custodia de los activos de información que se encuentren en el área. c. Se realizará monitoreo y supervisión periódica de las entradas y salidas de las mercancías con su respectivo inventario.

- En caso de que un colaborador requiera ingresar a las instalaciones de Tecnofactory S.A.S. los sábados, domingos o festivos deberá enviar un correo el día hábil anterior en horario laboral al jefe inmediato, posteriormente se informará a la administración del edificio, informando los días y horarios en los cuales se encontrará dentro de las instalaciones.

- Todos los colaboradores de Tecnofactory S.A.S. tendrán acceso a registro biométrico en la recepción del edificio para facilitar el respectivo ingreso al edificio.

Ubicación y Protección de los Equipos:

- Se analizará y establecerá la ubicación de los equipos de Tecnofactory S.A.S. teniendo en cuenta el peligro ambiental, acceso no autorizado, retiro de activos sin autorización y otras amenazas a los que puedan estar sometidos.

- Los equipos de la organización se encuentran ubicados en áreas de trabajo donde haya poco tráfico de personal.

- Los sistemas de información implementados en la organización y los equipos de comunicaciones que requieren protección especial se encontrarán aislados.

- Se realizará supervisión a las instalaciones de procesamiento y almacenamiento de información de la organización, que manejan información sensible o crítica, para evitar acceso ilegal a los equipos.

- Los puestos de trabajo deben permanecer en orden y libres de documentos que contengan información de la organización que pueda comprometer la continuidad del negocio.

Servicios de Suministro:

- Los servicios de suministro como, electricidad, agua, alcantarillado, aire acondicionado, ventilación tendrán inspección regular y se someterán por parte del operador o administrados a pruebas para garantizar su buen funcionamiento en el soporte de las operaciones, (Procedimiento de Mantenimiento de los Equipos)

- Frente a posibles fallas en el suministro de energía y agua para los equipos de Tecnofactory S.A.S., especialmente todos aquellos que sustenten las operaciones críticas para la continuidad de las actividades, se cuenta con la provisión de suministro de energía (planta electica), dispone de fuentes de energía in interrumpible (UPS) y suministro de agua (Tanques de agua).

- Se realizará monitoreo y pruebas periódicas del funcionamiento de los equipos de soporte de energía (UPS, Planta eléctrica), verificando que cumplan con requisitos de configuración y capacidad requeridos para dar un adecuado apoyo ante eventuales anomalías de energía.

- Se cuenta con señalización de emergencia en caso de producirse una falla en el suministro principal de energía. Ver Señalización y Demarcación

- La administración del edificio en donde se encuentran las instalaciones de Tecnofactory S.A.S. realiza el control y verificación del suministro de agua que alimenta el aire acondicionado, sistemas de extinción de incendios y humidificación, ya que podrían causar fallas a los equipos o evitar la acción ineficaz de la extinción de incendios.

Seguridad del Cableado:

- El cableado de energía eléctrica y comunicaciones que transporta datos o brinda apoyo a los servicios de información se encuentra protegido contra interceptación o daño. Los cables de energía eléctrica están separados de los cables de comunicaciones para evitar interferencias. se incluye en el cronograma de mantenimientos la revisión física cada 3 años.

- El cableado de red se encuentra peinado, protegido y organizado, evitando la interceptación no autorizada o daño.

- Tecnofactory realiza monitoreo periódico mensual sobre las redes de cableado para detectar, eliminar o prevenir el uso de dispositivos no autorizados conectados a los cables.

Mantenimiento de los Equipos:

- Tecnofactory S.A.S. define que el personal de la mesa de servicios es especializado para realizar el mantenimiento de los equipos de cómputo, el cual se llevará a cabo a través del Procedimiento Mantenimiento de los Equipos.

- Ningún colaborador interno o externo podrá destapar, mover, configurar, instalar o cambiar los elementos de trabajo, direcciones IP o identificadores de las máquinas, manipular tomas, cables y conectores. En caso de presentarse un daño sobre algún elemento de trabajo por causas como: golpes, derrame de

bebidas, elementos extraños, etc., la reparación o reposición debe estar a cargo del responsable del elemento.

- Los equipos y dispositivos críticos que pertenezcan a la organización deben revisarse con mayor regularidad, y su mantenimiento debe realizarse acorde con las instrucciones del fabricante.

- Tecnofactory define el cronograma de los mantenimientos preventivos a los equipos. (Ver Procedimiento Mantenimiento de los Equipos).

Seguridad de los Equipos Fuera de las Instalaciones:

- Los activos de infraestructura (portátiles, dispositivos móviles, documentación, entre otros) de Tecnofactory S.A.S., destinados al procesamiento de información y que se encuentren fuera de la organización, serán protegidos con un nivel de seguridad equivalente a los equipos que se encuentran dentro de la organización, teniendo en cuenta el control de acceso lógico para acceder a la información. (se cuenta con el Procedimiento Seguridad de los equipos fuera de las instalaciones)

- Todo equipo propio de Tecnofactory S.A.S., que esté fuera de las instalaciones, no debe ser desatendido por su responsable en lugares públicos.

- Todo equipo de procesamiento de información que deba ser utilizado por fuera de las instalaciones, debe ser solicitado por el líder de área a Tecnofactory para ser autorizado por correo electrónico, con orden de salida en documento físico a la administración del edificio.

Seguridad en la Reutilización o Eliminación de los Equipos:

- La información sensible y el software licenciado de la organización que se encuentre en los medios de almacenamiento y equipos con dispositivos de almacenamiento no removibles que van a ser reutilizados, debe ser físicamente destruidos o sobrescritos en forma segura antes de darles un nuevo uso, de manera que no haya ninguna forma de recuperar la información eliminada. (se cuenta con el Procedimiento Disposición de los Medios de Soporte)

- En el caso de los medios de almacenamiento dañados, que contienen información confidencial, será Tecnofactory quien a partir de los diagnósticos determinará si los medios deben ser destruidos, reparados o desechados. (se cuenta con el Procedimiento Disposición de los Medios de Soporte)

Retiro de Activos:

- Los activos de información y tecnológicos no serán retirados de las instalaciones de Tecnofactory S.A.S. sin previa autorización.

- El equipo auditor realizará auditorías de inventarios cada seis meses para detectar el retiro no autorizado de activos de la organización. (se cuenta con Procedimiento de auditoría Interna)

Políticas de escritorio y pantallas despejadas:

- La gestión de TI (Tecnofactory) asegura las estaciones de trabajo contra el uso no autorizado, a través del bloqueo automático de la sesión.
- No se encuentra permitido la exposición de información confidencial en los puestos de trabajo y los accesos directos en los escritorios de las estaciones de trabajo.

5.12 POLÍTICA SEGURIDAD OPERACIONAL

Objetivo: Establecer los procedimientos junto a sus responsables para la implantación adecuada de los controles que garanticen el apropiado desarrollo de todas las operaciones y servicios de procesamiento de la información en Tecnofactory S.A.S.

Alcance: Esta política aplica para todas las operaciones, procesos y procedimientos que se generen y desarrollen en Tecnofactory S.A.S. los cuales utilicen o tengan acceso a los sistemas de información de la organización.

Declaración de la política: Esta política declara las responsabilidades y procedimientos que deberían tener la gestión y operación de todos los servicios de procesamiento de información apropiados en Tecnofactory S.A.S. Toda operación y procedimiento con los activos de información (Personas – Información - Tecnología) de Tecnofactory S.A.S. deberá ser documentada, definida y delimitada especificando las responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran al respecto.

Lineamientos propuestos:

- Es de obligatorio cumplimiento por parte de todos los colaboradores documentar, mantener y tener disponible la descripción de los procedimientos de los procesos que estén bajo su responsabilidad, donde se logre la ejecución efectiva, eficiente, segura y precisa de los procesos de la organización.

- La Dirección de Tecnofactory S.A.S. es responsable de infundir y presentar a todos los colaboradores y responsables de la información de los procedimientos operativos documentados, para las actividades del sistema y su respectivo cumplimiento.

- Cualquier modificación a dichos documentos será revisada y aprobada exclusivamente por el dueño de proceso.

Gestión de cambios:

- La Gerencia de Tecnología controla y gestiona los cambios en los servicios y los sistemas de procesamiento de información de Tecnofactory S.A.S. que se requieran garantizando siempre que la seguridad y la continuidad de la operación no se vea afectada de ninguna forma.

  Todo cambio significativo en el sistema de información deberá pasar el filtro de calidad de implementación (planificación, evaluación de riesgos, aprobación, registro y documentación) antes de ponerse en operación junto a la comprobación funcional en un ambiente de pruebas. (Ver Pro. Control de Cambios).

Gestión de capacidades:

- Para asegurar el funcionamiento actual y futuro en el aspecto de almacenamiento de los sistemas de información de Tecnofactory S.A.S. la Gerencia de Tecnología a través del *IT Services Coordinator* monitorea, proyecta y planea la gestión para evitar desbordamientos de información o negación de servicios, asimismo los responsables de la información deberán informar problemas que afecten la operación. (Ver Procedimiento Gestión de las Capacidades).

Separación de entornos de desarrollo, prueba y producción:

- Para fortalecer el control de acceso a los activos de información (Personas – Información -Tecnología) y proteger la confidencialidad de cada área funcional de Tecnofactory S.A.S., la Gerencia de Tecnología deberá definir los requerimientos adecuados que garanticen la seguridad de la información, la Coordinación de Compras y Adquisiciones será el responsable de asignar dicha área física (desarrollo, prueba y producción). Los ambientes lógicos de desarrollo, prueba y producción se encuentran debidamente separados, para reducir el riesgo de los cambios involuntarios según la metodología aplicada CMMI. El proceso de Fábrica de Software de Tecnofactory S.A.S. es responsable de la creación de perfiles de usuario diferentes para los sistemas de prueba, como también el software de desarrollo y el de producción se

ejecutan en diferentes sistemas o procesadores de computación y en los diferentes ambientes.

Protección contra código malicioso:

- La Gerencia de Tecnología de Tecnofactory S.A.S. protege la información contra virus, por medio de herramientas que permiten proteger, detectar e identificar la presencia de códigos maliciosos, no autorizados que pongan en riesgo la integridad del software y de la información. La Gerencia de Tecnología de Tecnofactory S.A.S. realiza control de virus mediante el (Procedimiento Protección contra software malicioso) el cual permite actualizar, verificar y monitorear el software de detección y reparación de códigos maliciosos.

- La Gerencia de Tecnología de Tecnofactory S.A.S. establece los lineamientos de rutina que definen la gestión de copias de respaldo de la información; desde la creación, comprobación, clasificación (etiquetas) y almacenamiento de *backup* de Tecnofactory S.A.S. Para el buen estado y funcionamiento de los *backups* o respaldos se estableció el (Procedimiento *BackUp* o Respaldo de Información) que avala la continuidad del negocio si se llegara a presentar algún incidente que obligara a la organización a restaurar parcial o totalmente un sistema de información. Toda falla, error o desastre que se presente y afecte un sistema de información se deberá registrar, documentar y almacenar adecuadamente como base de conocimiento (experiencia).

- La Gerencia de Tecnología de Tecnofactory S.A.S. a través del *IT Services Coordinator* verifica los registros y eventos generados por el acceso a *SharePoint* de los diferentes usuarios de la organización, donde se garantiza que los colaboradores únicamente acceden a la información autorizada a su cargo. Se revisarán con regularidad los resultados de las actividades de monitoreo. La Gerencia de Tecnología es responsable de verificar la gestión en los momentos de fallas del sistema de información, análisis y toma de decisiones para acciones preventivas adecuadas a aquellas que no se han materializado y correctivas para las que ya fueron materializadas. (Ver Procedimiento Registro de fallas del sistema)

- La Gerencia de Tecnología de Tecnofactory S.A.S. a través del *IT Services Coordinator* define que provee, protege, garantiza y controla los registros de monitoreo, por medio de la Matriz Crud. La Gerencia de Tecnología a través del *IT Services Coordinator* verifica que los incidentes de los sistemas de información sean claros, que identifique adecuada y detalladamente el evento de seguridad y que estén evidenciados de actividades de manipulación, modificación y/o eliminación.

- La Gerencia de Tecnología de Tecnofactory S.A.S. a través del *IT Services Coordinator* determina realizar monitoreo de las actividades de los sistemas y de la administración de la red a través del registro (log) de actividades del administrador y del operador cuando sea necesario, permitiendo identificar o detectar el uso y/o acceso no autorizado. (Ver Procedimiento Registro de fallas del sistema)

- La Gerencia de Tecnología de Tecnofactory S.A.S. a través del *IT Services Coordinator* asegura que la hora de todos los sistemas de procesamiento de información estén sincronizados, por esto los *logs* serán la evidencia de uso (formal y legal) de los diferentes recursos informáticos por parte de los colaboradores.

Control de software en explotación:

- La Gerencia de Tecnología de Tecnofactory S.A.S. establece la restricción para el uso de software no autorizado en los equipos de propiedad y uso exclusivo de Tecnofactory S.A.S.) Toda instalación de software tendrá previa autorización de la Gerencia de Tecnología, con su respectiva evaluación de riesgos, y pruebas realizadas antes de su instalación.

- La Gerencia de Tecnología de Tecnofactory S.A.S. restringe la instalación de aplicaciones, para garantizar la integridad en el procesamiento de información en las aplicaciones que se utilizan en la organización. La Gerencia de Tecnología define los pasos para la gestión de las actualizaciones del software (aprobación, verificación, validación y documentación) para asegurar que las estaciones de trabajo tienen debidamente todos los parches de seguridad otorgados por parte del proveedor ya sea del sistema operativo o de la aplicación. Si los cambios son necesarios el software original se deberá conservar y los cambios se realizarían a una copia claramente identificada. Se cuenta con una herramienta (Guía *Check list* para entrega de Pc)

- La Coordinación de Soporte de Tecnología debe elaborar, definir y mantener durante un periodo acordado las grabaciones de los registros (*logs*) para auditoria de las actividades de los usuarios, las excepciones y los eventos de seguridad de la información con el fin de facilitar las investigaciones futuras y el monitoreo del control de acceso, asegurando los datos y privacidad de la información de carácter personal o corporativo de Tecnofactory S.A.S. que se registren, sin excepción. Se cuenta con el Procedimiento Auditoría Interna.

5.13 POLÍTICA SEGURIDAD EN LAS TELECOMUNICACIONES

Objetivo: Establecer los lineamientos y sus responsables para la implantación adecuada de los controles que garanticen el apropiado desarrollo de todas las operaciones y servicios de procesamiento y sopor de la información en Tecnofactory S.A.S

Alcance: Esta política aplica para todas las actividades que se lleven a cabo en la administración, control de las redes y sistemas de telecomunicaciones de Tecnofactory S.A.S.

Declaración de la política: Esta política declara las responsabilidades y procedimientos que deben tener la gestión y operación de todos los servicios de procesamiento de información incluyendo el desarrollo de procedimientos operativos apropiados en Tecnofactory S.A.S. Toda operación y procedimiento con los activos de información (Personas - Información -Tecnología) de Tecnofactory S.A.S. deberá ser documentada, definida y delimitada especificando las responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran al respecto.

Lineamientos propuestos:

Controles de red:

- El *Chief Technology Officer* a través del *IT Services Coordinator establece* controles contra el acceso no autorizado que proteger todos los activos de información, asegurar permanente y adecuadamente las redes de información junto a las aplicaciones que se usan en Tecnofactory S.A.S., de los diferentes riesgos a los que se exponen.

Las siguientes son las operaciones que ejecuta el *IT Services Coordinator* para una correcta administración de las redes:

- Realiza identificación de la red por puestos de trabajo.

- Define responsables y procedimientos para la gestión de equipos remotos, incluyendo la información en tránsito. (Ver Procedimiento de Intercambio de información).

- Protege la confidencialidad, integridad y disponibilidad de la información en tránsito (redes públicas e inalámbricas) con control de acceso (ver Procedimiento de control de acceso lógico) y de estructura cifrada. (ver Gestión de Claves Criptográficas)

- Lleva registro (*logs*) y monitoreo adecuado para acciones de seguridad pertinentes (ver Uso de servicios de Red y Aplicaciones).

- Toda implementación de un nuevo punto de red es aprobada por la Gerencia de Tecnología.

- Cualquier equipo que presente un riesgo para la red de comunicaciones de Tecnofactory S.A.S., podrá ser desconectado de la red y la persona que tiene asignado el equipo será notificado.

- Se realizará certificación a los puntos de red de forma periódica (cada 3 años). (Ver Política de Seguridad Física)

Mecanismos de seguridad asociados a servicios en red:

- Se acuerda con los niveles de servicio (SLA - ANS) con los terceros que suministran el servicio de red de Internet. (Claro 99.6% próximamente IFX 99.7%). Para asegurar la correcta y continua prestación de servicios por parte de los terceros, se realiza una planeación y monitorización regulada a la gestión del servicio por medio del firewall, respecto a las características de seguridad y niveles de servicio acordados.

Segregación de redes:

- El *IT Services Coordinator* controla el acceso a la información, identificando lógicamente los grupos de servicios de información, usuarios y sistemas de información de acuerdo con el tipo, clase, sensibilidad y confidencialidad de la información que manejan, para minimizar el riesgo de acceso no autorizado a los sistemas de información entre redes, sin tener en cuenta si el uso de la información sea interna o externa.

Intercambio de información con partes externas:

- Para garantizar la protección y el cumplimiento del intercambio de información interna o externa, la Gerencia de Tecnología, ha establecido procedimientos y controles formales de intercambio físico o lógico para proteger la información mediante el uso de todo tipo de servicios de comunicación. (Existencia del Procedimiento de Intercambio de Información). La Gerencia de Tecnología de Tecnofactory S.A.S., establece el cifrado en el envío de información interna y externa a la organización, a través de correo electrónico y chat corporativo como mecanismo de protección de la información confidencial.

Acuerdos de intercambio: Tecnofactory S.A.S. establece esta política por medio del Procedimiento Intercambio de Información, para proteger la información y los

medios físicos en tránsito, incluyendo el software que se utilice con terceros, considerando las siguientes condiciones de seguridad:

- Trazabilidad y no- repudio
- Transmisión
- Informar incidentes; como perdida de datos
- Cifrado de información

La Gerencia de Tecnología garantiza la confidencialidad de la información, sin importar el tipo de intercambio (físico o lógico) o medio en tránsito que se utilice. La Gerencia de Tecnología implanta las políticas, procedimientos y normas consistentes de conformidad al aseguramiento de la seguridad de la información. El área Jurídica establece los acuerdos o contratos de confidencialidad, tanto para colaboradores de la organización, como para terceros.

Mensajería electrónica:

Todo intercambio de información por medio electrónico se encuentra protegido contra software malicioso, de igual forma usando las herramientas corporativas para enviar información que contenga datos considerados como importantes o confidenciales viajaran de manera cifrada.

- No debe existir suplantación de ninguna índole en las firmas electrónicas usadas por el área Financiera, y respuestas de correos electrónicos, así la persona se encuentre en ausencia de sus funciones. La Gerencia de Tecnología de Tecnofactory S.A.S. a través del área financiera son los responsables de gestionar adecuadamente el Procedimiento Gestión de Claves Criptográficas.

- La Gerencia de Tecnología implanta el Procedimiento Gestión de Claves Criptográficas que permite verificar la identidad del dueño, reduciendo la posibilidad de suplantación y asegurando la confidencialidad e integridad de la información a la cual tiene acceso.

- La Gerencia de Tecnología implanta el Procedimiento Intercambio de Información para evitar el no repudio de una determinada información electrónica por parte del receptor.

- La Gerencia de Tecnología a través del *IT Services Coordinator* controla y administra el uso de las redes inalámbricas (Ver Procedimiento Uso de servicios de Red y Aplicaciones).

- La Gerencia de Tecnología a través del *IT Services Coordinator* controla y administra los aplicativos necesarios para la detección y protección de virus en la información que se recibe o envía electrónicamente. (Ver Política de Seguridad en la Operativa).

Acuerdos de confidencialidad y secreto:

- La Gerencia Jurídica de Tecnofactory S.A.S., establece por medio del contrato (colaboradores y terceros), la protección de la información sensible y crítica de la organización a través de acuerdos de no divulgación. Todas las personas que laboren para Tecnofactory S.A.S. deben firmar la cláusula de confidencialidad definida por la organización, el cual hará parte integral de los contratos.

  La cláusula debe ser firmada también por personal temporal, o cualquier tercero que tenga acceso a los activos de información de la organización o a su infraestructura.

5.14 POLÍTICA RELACIONES CON PROVEEDORES

Objetivo: Identificar, definir y documentar los requisitos de seguridad ante la prestación de servicios de entes externos, y la necesidad de implementar acuerdos de nivel de servicio y acuerdos de confidencialidad para el manejo de la información que hace parte entre los procesos de Tecnofactory S.A.S. y los proveedores o terceros, en cumplimiento con el Sistema de Gestión de Seguridad de la Información.

Alcance: La presente política compromete toda relación contractual entre proveedores o terceros y Tecnofactory S.A.S.

Declaración de la política: La política de relaciones con suministradores es la declaración de principios de la Dirección de Tecnofactory S.A.S., que comprende la identificación y definición de los requisitos de seguridad ante proveedores y/o terceros que tengan relación contractual con la organización. Esta política concreta en una serie de normas, reglamentos y protocolos a seguir, donde se definen las distintas medidas a tomar para justificar, acordar y documentar todos los requisitos de seguridad para el sistema de gestión de seguridad de la información.

Lineamientos propuestos:

- La Dirección General de Tecnofactory S.A.S. define los lineamientos para el cumplimiento de todo personal que sea contratado como tercero, donde se encuentra en la obligación de ejecutar las actividades de acuerdo con las normas establecidas por la organización.

- La Dirección General de Tecnofactory S.A.S., define los accesos lógicos donde se encuentra permitido para todo tercero que tenga relación contractual con la organización, procesar, almacenar, comunicar o suministrar información de los procesos de Tecnofactory S.A.S., hasta un nivel definido por la organización y

los contratos establecidos entre las partes interesadas. Ver Cláusula de confidencialidad terceros.

- Los activos de información (Personas - Información -Tecnología) de Tecnofactory S.A.S., cumplen con los requisitos de seguridad exigiendo a todos los terceros la utilización de alguna forma de identificación visible y se notificará inmediatamente al personal de seguridad si se encuentran visitantes o acompañantes y cualquiera que no use identificación visible.

- La Dirección General de Tecnofactory S.A.S., implanta controles y define un convenio con los terceros por medio del contrato en las cláusulas que definen el acuerdo de confidencialidad que deben cumplir con la organización.

- Está política garantiza el cumplimiento del Sistema de Gestión de Seguridad de la Información por Tecnofactory S.A.S., la responsabilidad y las obligaciones legales que interponen dentro de un contrato con terceros.

Cadena de suministro en tecnologías de la información y comunicaciones:

- La Dirección General de Tecnofactory S.A.S. a través del área de Compras hace la evaluación de proveedores, de esta manera realiza una gestión para tratar el riesgo, minimizarlo y establecer un responsable por los terceros.

Gestión de la prestación del servicio por proveedores:

- El Comité de Seguridad de la Información planificará auditorías a los servicios de terceros críticos para la revisión y monitoreo periódico de los contratados externamente constatando que se están cumpliendo los acuerdos de nivel de servicio, evaluación de proveedores, y de haber incidentes, verificar que se estén gestionando correctamente, procurando así la seguridad de la información de Tecnofactory S.A.S.

Gestión de cambios en los servicios prestados por terceros:

- Todo cambio en un servicio (software o hardware) o en su prestación, incluyendo mantenimiento y mejora, adquirido a un tercero, deberá cumplir con los controles definidos y aplicados desde su aprobación hasta la correcta gestión teniendo en cuenta la importancia de los sistemas y procesos del negocio involucrados en Tecnofactory S.A.S.

Acuerdos de nivel de servicios: Se contará con acuerdos de nivel de servicio para los servicios contratados:

- Azure: https://azure.microsoft.com/es-es/support/legal/sla/
- Office 365: https://www.21vbluecloud.com/office365/O365-SLA/

- Servicios de internet: Ifx networks Contratos de Servicios de internet.
- Servicios de telefonía: claro Contratos de servicios.

5.15 POLÍTICA GESTIÓN DE INCIDENTES

Objetivo**:** Establecer los lineamientos generales para la gestión de incidentes de seguridad de la información, con el fin de prevenir y limitar el impacto de estos.

Alcance: Aplica para todo el personal interno y externo de Tecnofactory S.A.S. que interactúe y tenga acceso a los sistemas de información de la organización y a los activos de información (Personas – Información - Tecnología), donde se presenten incidentes que puedan afectar la seguridad de la información.

Declaración de la política: La política de Gestión de Incidentes de Seguridad de la Información es la declaración de principios de la Dirección General de Tecnofactory S.A.S., que comprende el manejo de los incidentes relacionados con la seguridad de la información y que proporciona los criterios básicos para definir y delimitar las responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran al respecto. Esta política se concreta en una serie de normas, reglamentos y protocolos a seguir, los cuales definen las distintas medidas a tomar para identificar, prevenir, priorizar, atender los incidentes relacionados con los sistemas de información, las funciones y responsabilidades de los elementos de la organización.

Lineamientos propuestos:

Responsabilidades y procedimientos:

Dirección: Aprobar y garantizar el cumplimiento de la política, garantizar los recursos económicos necesarios para que se cumpla con la política.

Colaboradores y terceros: Conocer y cumplir la política, las normas y los procesos de la Gestión de Incidentes de Seguridad de la Información y reportar los incidentes

Área de Talento Humano: Garantizar el entrenamiento y programas de inducción relacionados con la gestión de incidentes de Seguridad de la Información.

Comité de Seguridad de la Información: Liderado por la dirección con el apoyo de colaboradores de la compañía. Las principales funciones son:

- Evidenciar correlación de eventos.
- Evidenciar la gestión de las alertas enviadas por terceros y mesa de servicio.

- Evidenciar las debilidades obtenidas en los activos (personas, tecnología, información) y servicios de procesamiento de información de Tecnofactory S.A.S.
- Atender los incidentes críticos reportados por la mesa de servicio y proveer los métodos, técnicas y recursos aplicados en la atención del incidente.
- Coordinar actividades de respuesta apoyándose en las áreas necesarias o grupos interdisciplinarios necesarios.

IT Services Coordinator: Auditar, medir y vigilar que se cumpla con la política y las normas asociadas. Ejecutar la política y velar por su cumplimiento, además:

- Gestionar la actualización del proceso de atención de incidentes.
- Recibir los reportes de eventos o debilidades detectadas por los colaboradores o terceros, documentando el evento con la información del incidente. (Ver Procedimiento gestión de incidentes)
- Categorizar, de acuerdo con la severidad, el evento o debilidad reportada.
- Solicitar o adjuntar a la documentación las pantallas de error, log´s, entre otros, facilitados por los colaboradores, terceros, clientes o usuarios.

Procedimientos:

El procedimiento de atención de Incidentes de Tecnofactory S.A.S. debe como mínimo contar con los siguientes aspectos (Ver Procedimiento Gestión de Incidentes):

- Un análisis de riesgo, a fin de encontrar las causas probables de su origen e identificar los controles que mitigarán los riesgos asociados.

- Registro de incidentes a fin de anotar en un sistema de información, los síntomas, las pruebas o evidencias del origen del incidente, su trazabilidad, la solución, la clasificación, la codificación y todos los datos que servirán para análisis de riesgo, su mitigación y datos que conformarán las estadísticas de gestión sobre incidentes.

- El seguimiento que permita las anotaciones, producto de las investigaciones o acciones que se generen en su solución, así como, la trazabilidad a través de las áreas involucradas en la solución del incidente.

- Contemplar las diferentes opciones de escalabilidad a fin de que el análisis y solución sean generados por la mesa de servicio correspondiente que deba resolver el incidente de forma rápida y oportuna. La escalabilidad debe incluir puntos múltiples, dependiendo de la severidad del incidente con miras a recoger evidencia y que el daño o la restauración se pueda terminar en el menor tiempo posible.

- Control de los incidentes reportados, con el fin de asegurar el cierre definitivo de un reporte y que se hayan establecido las causas y medidas de solución a fin de mitigar el riesgo que pueda producir un incidente.

- Un código o *ticket* para cada incidente que lo identifique de forma única desde el momento de su radicación hasta su cierre.

- Establecer las funciones y responsabilidades para la administración de los incidentes que se presenten y se reporten.

Notificación de los eventos de seguridad de la información:

- Es obligación de cada colaborador reportar a la mesa de servicio que se determine dentro de Tecnofactory S.A.S. las violaciones a las políticas de seguridad de la información y a la Gestión de Incidentes de Seguridad de la Información que sean detectadas o cualquier incidente que se produzca sobre cualquier recurso informático que pueda parecer sospechoso.

Notificación de los puntos débiles de la seguridad:

- Para garantizar la utilización de los procesos definidos y en cumplimiento de la política establecida, todos los colaboradores de Tecnofactory S.A.S., contratistas y terceros tienen la obligación de conocer, capacitarse y apoyar la implementación de la gestión de incidentes y en consecuencia, informar sobre los incidentes que afecten la seguridad de la información, los procesos del negocio, los sistemas de información y los recursos tecnológicos afectados utilizando los canales de comunicación que la organización destinó para estos propósitos. (Ver Procedimiento de Gestión de Incidentes)

  Así mismo, se deben realizar los procesos de retroalimentación posteriores a la ocurrencia y atención de incidente, con el fin de dar a conocer las lecciones aprendidas y en consecuencia mejorar la prevención de estos eventos y los tiempos de atención y retorno a la normalidad.

Valoración de eventos de seguridad de la información y toma de decisiones:

- El *IT Services Coordinator* será la persona encargada de evaluar la serie de eventos inesperados, que pueden comprometer los activos de seguridad de la información y el nivel de los incidentes. Es responsabilidad de la Gerencia de Tecnología evaluar si el nivel del incidente puede llegar a disparar el plan de continuidad (Ver procedimiento de Gestión de Incidentes).

Respuesta a los incidentes de seguridad:

- La Gerencia de Tecnología a través del *IT Services Coordinator* cuenta con una mesa de servicio con los mecanismos suficientes para detectar los incidentes de manera inmediata como se indica en el procedimiento de Gestión de Incidentes.

Aprendizaje de los incidentes de seguridad de la información:

- Como parte de esta política Tecnofactory S.A.S., asegura que los colaboradores reciben capacitación continua para desarrollar y mantener sus conocimientos, competencia, habilidades y conciencia en materia de seguridad informática y de la Gestión de Incidentes, dentro del nivel requerido a fin de lograr un desempeño oportuno y eficaz. (Ver Política de Talento Humano).

Recopilación de evidencias:

- Para Tecnofactory S.A.S. cuando un incidente implica acciones legales (civiles o penales) el *IT Services Coordinator* debe recolectar la evidencia, transportarla y protegerla realizando el buen manejo de evidencia digital o física y garantizando la cadena de custodia. (Ver Procedimiento Gestión de Incidentes) y (Ver Política de Cumplimiento).

5.16 POLÍTICA DE CONTINUIDAD DEL NEGOCIO

Objetivo: Evitar interrupciones a los procesos críticos del negocio como consecuencia de fallas o desastres.

Alcance: Esta política aplicará para todo el personal que labore Tecnofactory S.A.S., con el fin de poder garantizar la continuidad del negocio (BCP/DRP), en caso de un evento que afecte la operación normal.

Declaración de la política: Debido a que cualquier interrupción en los procesos de negocio afecta la operación, es responsabilidad de las directivas de la organización aprobar un plan de continuidad de negocio (BCP, DRP), que cubra las actividades esenciales y críticas de Tecnofactory S.A.S.

Lineamientos propuestos:

Inicio del plan de continuidad del negocio (BCP):

- El comité de seguridad de la Información de Tecnofactory S.A.S, es responsable de dar inicio al Plan de Continuidad del Negocio (BCP)., el cual es esencial para poder continuar las actividades críticas del negocio de Tecnofactory S.A.S, en el

evento de una falla inesperada, que pudiera seriamente interrumpir los procesos y actividades importantes de su operación.

El proyecto del Plan de Continuidad del negocio (BCP) necesita ser iniciado y formalmente aprobado, por las directivas de Tecnofactory S.A.S. Es importante considerar lo siguiente:

- Se establece la necesidad del Plan de continuidad del negocio (BCP)

- Se obtiene el compromiso de las directivas de Tecnofactory S.A.S y se les presenta un reporte inicial que informe como el BCP cumplirá sus objetivos.

- Para que el plan de continuidad del negocio (BCP) sea eficaz, se requiere la conformación de un Equipo de Emergencia (EDE), que está compuesto por miembros altamente cualificados del equipo directivo procedentes de áreas vitales dentro de la organización. Los miembros del equipo tienen cometidos y responsabilidades concretas cuando se produce un desastre en cualquier instalación de Tecnofactory S.A.S y se pone en práctica el Plan de Recuperación de Desastres - DRP. El Equipo de Emergencia (EDE) está formado por personas procedentes de las áreas siguientes: Talento Humano, Administración, Financiera y Tecnología. Los integrantes de la Gestión del Proyecto y de la Gestión del Nivel Directivo coordinan los esfuerzos del Equipo de Emergencia (EDE).

El Equipo de Emergencia (EDE) es un grupo de gestión flexible y móvil que puede ocuparse de cualquier plan de recuperación que sea necesario en cualquier sitio donde este Tecnofactory S.A.S.

Desarrollo y administración del plan de continuidad del negocio:

- Las directivas de Tecnofactory S.A.S. deben desarrollar un Plan de Continuidad del Negocio (BCP,) que cubra los aspectos críticos y esenciales de la actividad social. El Plan de Continuidad del Negocio (BCP), es esencial para poder continuar con las actividades críticas del negocio, en el evento de una falla inesperada.

  El Plan de Continuidad del negocio es un proyecto con características de detalle y complejidad, independiente del entorno tecnológico y probablemente contendrá una serie de acciones críticas enfocadas a lograr el retorno a la operación normal.

Recomendaciones adicionales al desarrollo y administración del plan de continuidad del negocio:

- Entender plenamente los riesgos a que está enfrentado Tecnofactory S.A.S, incluyendo e identificando los procesos críticos del negocio.

- Entender el posible impacto que una interrupción a la operación normal pueda tener.

Considerar la adquisición y renovación de una póliza de seguros de protección de activos como parte del plan de continuidad de negocio (BCP).

- Formular y documentar una estrategia de continuidad del negocio de acuerdo con los objetivos y prioridades. Formular y documentar una estrategia consistente con los objetivos y prioridades acordadas, y a su vez, se debe documentar el plan de continuidad del negocio de acuerdo con la estrategia anteriormente definida.

Evaluación de riesgo del plan de continuidad del negocio BCP:

- Dentro del plan de continuidad de negocio (BCP) se debe realizar una evaluación formal de riesgo, o análisis de impacto sobre el negocio (BIA-*Business Impact Assessment*), con el fin de determinar los requerimientos del Plan de Continuidad del Negocio e identificar eventos que puedan causar interrupciones a los procesos de negocio. Es importante considerar que se deben evaluar y analizar todos los procesos de negocio y no limitarse exclusivamente a los recursos e infraestructura asociados a los productos, soluciones o. Sistemas de información.

Recomendaciones adicionales:

- El Plan de Continuidad del Negocio (BCP,), es esencial para poder continuar con las actividades críticas del negocio de Tecnofactory S.A.S, en el evento de una falla inesperada, que pudiera seriamente interrumpir los procesos y actividades importantes de la operación de la compañía. La evaluación de riesgo en el BCP analiza la naturaleza de la ocurrencia de eventos inesperados, su impacto potencial y la probabilidad de que estos eventos lleguen a ser incidentes críticos para el negocio.

Aspectos de la seguridad de la información a ser considerados cuando se implementan estas políticas son:

- Comprender que así el proyecto formal del Plan de continuidad del Negocio se haya iniciado, si los recursos humanos o financieros son insuficientes, es muy probable que el plan no tenga éxito.

- Si se subestima el impacto a corto y mediano plazo de un incidente de seguridad se puede tener un nivel no adecuado de respuesta que afecte la elaboración de un Plan de Continuidad de Negocio.

Los pasos involucrados en el análisis de impacto hacia el negocio (BIA) comprenden:

- Análisis de la información.
- Determinar los tiempos críticos de las diferentes funciones del negocio,
- Determinar los tiempos máximos tolerables de caída por proceso (MTD-*Maximum Tolerable Downtime*)
- Priorizar la recuperación de las funciones críticas del negocio
- Documentar y preparar reportes de recomendaciones.

Características del plan de continuidad de negocio (BCP)**: c**on el fin de garantizar su consistencia a lo largo de las diferentes unidades de negocio, el plan de continuidad de negocio debe considerar:

- para la activación del plan de continuidad (BCP) Una estrategia de recuperación de desastres teniendo en cuenta aspectos como: Costos de las diferentes alternativas, Costos de servicios alternos, Prioridades y tiempos de recuperación, Negocios, usuarios, servicios, aspectos técnicos e información.

- Identificación de las responsabilidades y procedimientos de emergencia.
- Implementación de procedimientos de emergencia para permitir la recuperación en un tiempo limitado.
- Procedimientos de contingencia y procedimientos de regreso a la operación normal
- Documentación de procedimientos y procesos acordados.
- Educación apropiada sobre manejo de emergencias.
- Cronograma de pruebas del plan de continuidad del negocio (BCP)
- Responsabilidades individuales de ejecución y propietarios de cada plan de continuidad (BCP).

Entrenamiento y concientización del plan de continuidad del negocio (BCP):

- Todo el personal de Tecnofactory S.A.S, debe conocer el Plan de Continuidad del Negocio (BCP) y su respectiva función dentro de él, una vez se haya realizado su aprobación.

Recomendaciones Adicionales:

- El Plan de Continuidad del Negocio (BCP), es esencial para poder continuar con las actividades críticas del negocio de Tecnofactory S.A.S, en el evento de una falla inesperada, que pudiera seriamente interrumpir los procesos y actividades importantes de la operación de la compañía. Para que el Plan de Continuidad del Negocio (BCP) pueda ser ejecutado exitosamente, todo el personal no sólo

debe estar consciente de su existencia, sino conocer su contenido, junto con las actividades y responsabilidades de cada parte.

Aspectos de la seguridad de la información a ser considerados cuando se implementan estas políticas:

- Aun cuando el Plan de Continuidad de Negocio (BCP) haya sido probado, aun puede fallar, si el personal no está lo suficientemente familiarizado con sus contenidos.

- Cuando en el Plan de Continuidad del negocio (BCP), las personas involucradas olvidan su percepción de la cercanía del riesgo, se puede presentar cierta apatía, la cual disminuye su importancia, y la necesidad de una participación en él.

- Se deberá crear un plan de concientización sobre la importancia del BCP y los DRP para Tecnofactory S.A.S, y el compromiso de todos los empleados para garantizar su éxito.

Prueba del plan de continuidad del negocio:

- El Plan de Continuidad del Negocio (BCP) necesita ser probado periódicamente, con el fin de garantizar que la compañía entienda claramente como debe ser ejecutado.

- El hecho de probar el Plan de Continuidad del negocio (BCP) en la organización, evalúa su viabilidad, y garantiza que los empleados estén familiarizados; Si la prueba del Plan de Continuidad del Negocio (BCP) no reproduce las condiciones reales, el valor de tales pruebas es limitado y deficiente.

Las fallas en el análisis del plan de pruebas del BCP, ocasionarán una disminución de la validez de la prueba. Los diferentes tipos de prueba incluyen:

- Pruebas sobre la mesa de los diferentes escenarios (Por medio del uso de listas de verificación y análisis paso a paso) del BCP.
- Simulaciones del Plan de Continuidad.
- Pruebas de recuperación técnicas del BCP.
- Pruebas de recuperación en sitio alterno del BCP.
- Prueba de servicios externos (Energía, comunicaciones etc.) del BCP.
- Prueba completa, con el fin de evaluar personal, equipos, recursos físicos, para entender su capacidad de soportar interrupciones. Esta prueba implica detener las operaciones de Tecnofactory S.A.S, y no es recomendable ya que puede originar un desastre real.

Una vez aprobado y desarrollado, el plan de continuidad de negocio (BCP) debe ser probado con el fin de mostrar su eficacia, y nivel de actualidad. El periodo de pruebas sobre la mesa de los diferentes escenarios no debe ser mayor a 6 meses.

Mantenimiento y actualización del plan de continuidad de negocio (BCP):

- El Plan de Continuidad del Negocio (BCP) debe estar actualizado y revisado periódicamente.

- El mantenimiento y actualización del Plan de Continuidad del Negocio (BCP) es muy importante si se requiere una operación exitosa en un momento dado. Se requiere probar las implicaciones por cambios en el BCP, de lo contrario su ejecución puede resultar en una serie de fallas y debilidades.

Si el Plan de Continuidad del Negocio no es actualizado periódicamente, su éxito puede ser cuestionable. Estos cambios deben incluir:

- Adquisiciones de nuevos equipos
- Actualizaciones en los sistemas operacionales
- Personal
- Direcciones o números telefónicos
- Estrategias de negocio
- Ubicaciones físicas
- Leyes
- Contratistas, proveedores de servicio y clientes muy importantes
- Procesos nuevos o eliminados
- Riesgo (Operacional y financiero)

5.17 POLÍTICA DE ESCRITORIOS LIMPIOS

Objetivo: Reducir los riesgos de pérdida o daño de la información en el ambiente cotidiano de trabajo: escritorios y monitores, garantizando los principios de confidencialidad integridad y disponibilidad de esta evitando el acceso no autorizado.

Alcance: Aplica para todos los colaboradores de Tecnofactory S.A.S.

Declaración de la política: Debido a que cualquier interrupción en los procesos de negocio afecta la operación, es responsabilidad de las directivas de la organización aprobar un plan de continuidad de negocio (BCP, DRP), que cubra las actividades esenciales y críticas de Tecnofactory S.A.S.

Lineamientos propuestos:

- Se prohíbe tener información en el escritorio virtual de los equipos, toda la información debe reposar en la nube o en casos especiales en la carpeta documentos.
- Toda información confidencial física que se maneje en los puestos de trabajo deberá ser guardada bajo llave, cuando el personal no se encuentre en su puesto de trabajo o termine la jornada laboral.
- En los archiveros ubicados en cada puesto de trabajo solo debe reposar información de carácter público, la información confidencial o privada se debe guardar bajo llave cuando el colaborador se ausente de su puesto de trabajo o termine la jornada laboral.
- Se prohíbe que los libros de archivado (A-Z) se guarden en el puesto de trabajo del colaborador, estos deben ubicarse en el espacio asignado al archivo.
- La información que se imprima y tenga carácter privada o confidencial debe ser retirada de forma inmediata de las impresoras.

Registros:

- Revisiones Mensuales al cumplimiento de las políticas.

6. PLAN DE CONCIENTIZACIÓN

6.1 INTRODUCCIÓN

Para lograr que Tecnofactory S.A.S, obtenga resultados positivos en términos de seguridad de la información, no solo es necesario que se cuente con políticas, procedimientos y controles definidos, sino que también se cuente con un recurso humano con una cultura de seguridad clara y defensiva.

Empleando como referencia la normal NIST 800-50 “Creación de un programa de capacitación y concientización sobre la seguridad de la tecnología de la información” que tiene como propósito dar a conocer las estrategias que se llevarán a cabo para lograr que el recurso humano de la compañía Tecnofactory S.A.S sea consciente de los riesgos a los que se encuentra expuesto.

6.2 OBJETIVOS

- Diseñar el plan con base en la identificación de las actividades a ser realizadas para cumplir con las metas de toma de conciencia de los colaboradores de Tecnofactory S.A.S.
- Desarrollo del plan enfocado en las fuentes de información disponible, alcance y contenidos del material de toma de conciencia.
- Implementación de las actividades diseñadas.
- Mejoramiento para mantener el plan actualizado, monitorizando su efectividad.

6.3 ALCANCE

El plan de toma de concientización va dirigido a todos los colaboradores y aliados de Tecnofactory S.A.S.

6.4 DISEÑO DEL PLAN DE TOMA DE CONCIENCIA EN EL SGSI.

En esta fase se identifican las necesidades y las prioridades que tiene Tecnofactory S.A.S respecto al tema de sensibilización y capacitación de los colaboradores, para establecer los niveles de complejidad, evaluar la estrategia de capacitación que será desarrollada y aprobada, es importante que el plan, apoye las necesidades de la empresa y sea relevante a la cultura organizacional.

Algunos de los métodos que se utilizaron para la evaluación de necesidades de sensibilización y capacitación dentro de Tecnofactory S.A.S fueron:

- Verificación de comportamientos generales de los colaboradores (sesiones abiertas, escritorios limpios, entre otros)
- Verificación de los incidentes de seguridad de la información.

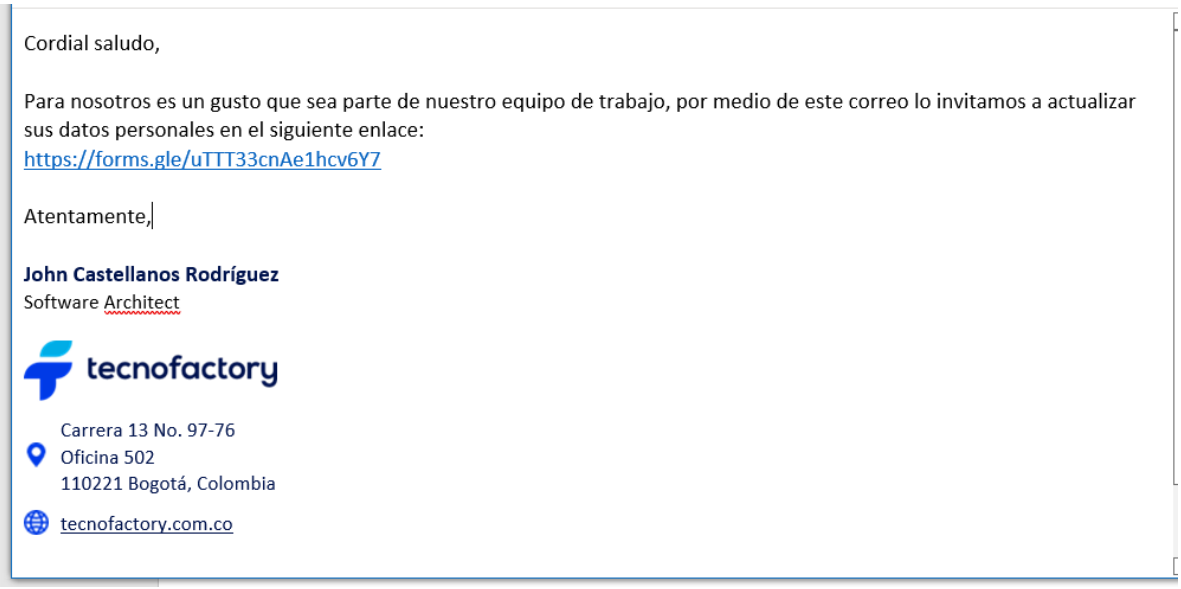
- Auditorías internas.
- Actividades de ingeniería social en diferentes niveles.

Actividad de Ingeniería Social para plantear:

Prueba de phishing: El *phishing* es un método que los ciberdelincuentes utilizan para engañarle y conseguir que revele información personal, como contraseñas o datos de tarjetas de crédito y de la seguridad social y números de cuentas bancarias. Lo hacen mediante el envío de correos electrónicos fraudulentos o dirigiéndole a un sitio web falso o suplantando destinatarios seguros.

Se lanzará una prueba en donde se enviará un correo suplantando un correo electrónico propio de empresa como se ve en la figura 6, dentro de este correo se solicitará información personal en un formulario creado en formularios de Google, esta información se anonimizara y se presentara como un estado inicial de concientización de los empleados, el cuerpo del correo es el siguiente:

Figura 6. Correo de phishing

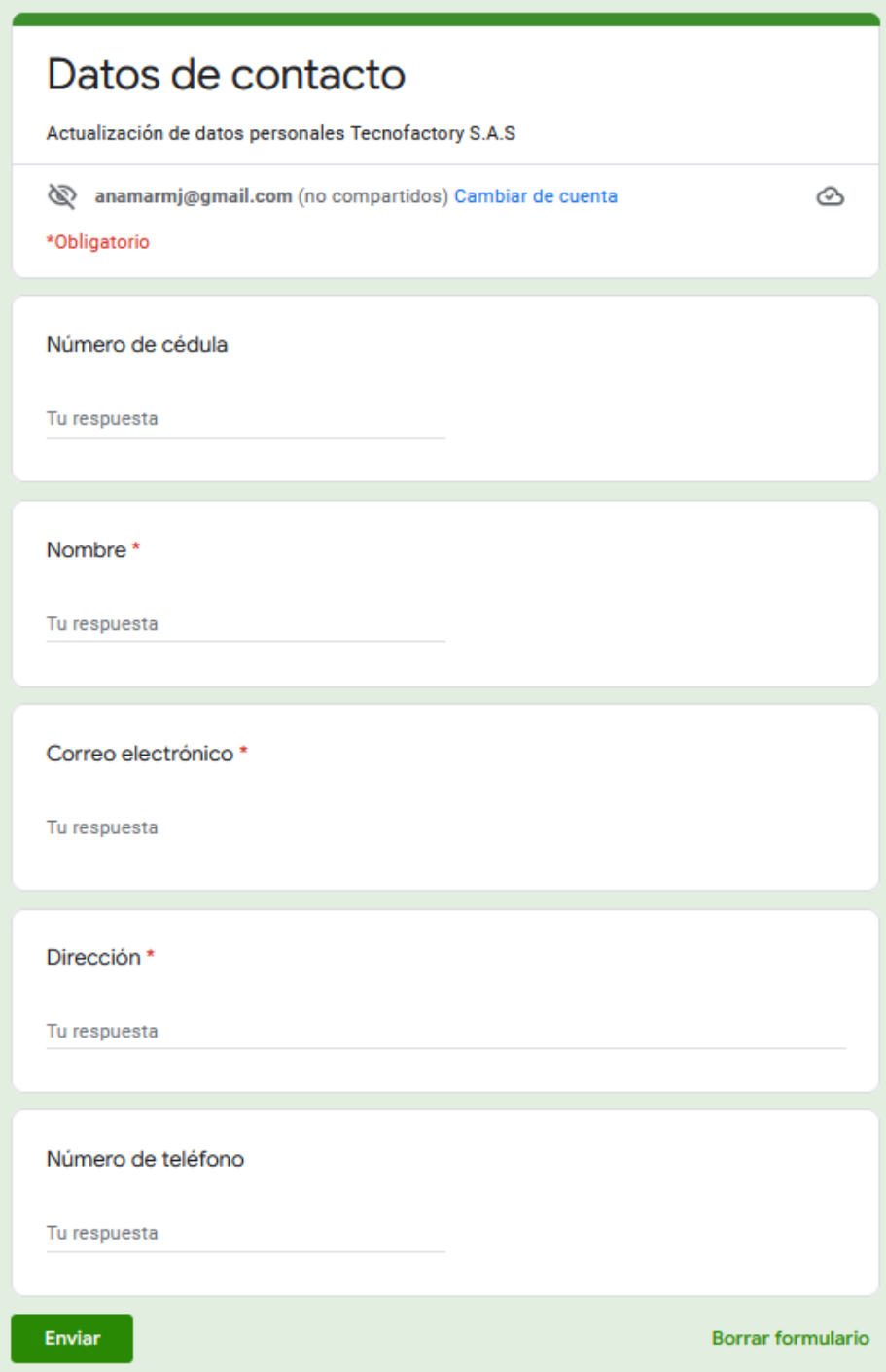


Fuente: Los autores

Teniendo en cuenta que la idea es realizar lo más creíble el correo se enviara desde la dirección “john.castellanos@tecnofactory.com.co” demostrando que este tipo de ataques son difíciles de detectar por el personal que no tenga los conocimientos básicos.

En la figura 7 se muestra el formulario al cual se direcciona el correo electrónico:

Figura 7. Formulario ficticio



Fuente: Los autores

Se realiza el ejercicio en una muestra de colaboradores y conociendo el porcentaje de personas que ingresaron información personal se podrá identificar la necesidad de sensibilizar a los colaboradores respecto a este tipo de ataque que son víctimas. Se realizan recolección de información teniendo en cuenta los métodos previamente señalados incluyendo los de Ingeniería Social, se lograr la evaluación de necesidades de sensibilización y capacitación.

Temas identificados que se deben sensibilizar y capacitar:

- Phishing
- Correos desconocidos
- Bloqueo de ordenador
- Roles y permisos
- Uso de memorias USB
- Herramientas de seguridad
- Ataques de ingeniería Social
- Destrucción de papeles/documentos
- Ley 1581: 2012 y ley 527 de 1999

6.5 DESARROLLO DEL PLAN DE TOMA DE CONCIENTIZACION EN SGSI.

Después de terminar con la evaluación de las necesidades, obtendremos la información necesaria para iniciar con la estrategia de desarrollo, implementación y mantenimiento del plan de toma de conciencia. Una vez se hayan identificado todas las oportunidades de mejora dentro de Tecnofactory S.A.S, se debe proceder con la elaboración del plan, el cual deberá contar con la viabilidad presupuestal que se requiere y debe contener entre otros los siguientes elementos, de acuerdo con un formato llamado *Formato de identificación de necesidades de toma de conciencia* de los colaboradores de Tecnofactory S.A.S.

Se inicia el plan poniendo en marcha una campaña de expectativa que permitirá enfocar a los colaboradores en la temática se seguridad en la información.

6.5.1 Campaña de expectativa. Para llamar la atención de todos los involucrados se propone iniciar una campaña de expectativa con consejos de seguridad que pueden ser difundidos utilizando herramientas y material como:

- Afiches
- Fondos de pantalla
- Posters
- Comunicados vía correo
- Mensajes en la intranet
- Material audiovisual

Se plantean algunos ejemplos de consejos de seguridad que pueden ser divulgados utilizando las herramientas antes mencionadas como se ve a continuación:

Uno de los temas a difundir para evitar ataques de *ransomware* es la importancia de no abrir correos de remitentes desconocidos por ello se hace el diseño de la figura 8.

Figura 8. Consejo de uso correcto del correo electrónico

Fuente: Los Autores

Para la protección de las contraseñas se diseña un fondo para impulsar el bloqueo de equipo y contraseñas visibles como se puede observar en la figura 9.

Figura 9. Consejo de resguardo de contraseña y bloqueo de equipo

Fuente: Los Autores

Para la parte de seguridad web se realiza un diseño sobre la importancia de verificar que las páginas cuenten con certificado SSL al momento de acceder a ellas como se evidencia en la figura 10.

Figura 10. Consejo de certificados de seguridad.

Fuente: Los Autores

6.6. IMPLEMENTACIÓN DEL PLAN DE TOMA DE CONCIENTIZACIÓN

En este paso consiste en implementar lo consignado en el diseño donde se identificó las necesidades de toma de conciencia. Empleando técnicas que permiten difundir o comunicar la información como lo son las sensibilizaciones o capacitaciones.

6.6.1 Capacitaciones o sensibilizaciones. En las capacitaciones o sensibilizaciones se abordarán los siguientes conceptos:

- Sistema de gestión de la seguridad de la información adoptado por Tecnofactory S.A.S.
- Socialización de la política de seguridad de la información.
- Riesgos de los activos de información
- Manejo de incidentes de seguridad.
- Regulaciones legales aplicables.

En estos espacios es importante cautivar a los colaboradores por ello se utilizarán diferentes estrategias como:

- Conferencias / Capacitaciones (según el rol en la compañía)
- Videos
- Juegos
- Simulacros
- Recordatorios

Se plantea un cronograma que incluye charlas y capacitaciones sobre los principales temas que se identificaron como prioritarios a tratar para generar conciencia en la seguridad de la información, en el cuadro 21 se describen los temas a tratar, población dirigida, tipo de actividad, encargado de realizar la actividad y propuesta de fechas.

Cuadro 21. Formato de identificación de necesidades de toma de conciencia

Tema	A quien va dirigido	Tipo de Actividad	Quién la realiza	Mes 1				Mes 2			
				Sem 1	Sem 2	Sem 3	Sem 4	Sem 1	Sem 2	Sem 3	Sem 4
Sensibilización de seguridad de la información.	Toda la compañía	Conferencia	Ing. Manuel Ovalle								
Socialización de la política de seguridad de la información	Toda la compañía	Conferencia y entrega de recordatorio	Ing. Ana Martinez								
Riesgos de los activos de información y Gestión de amenazas y vulnerabilidades	Personal de TI	Capacitación	Experto externo								
Riesgos de los activos de información	Personal de TI	Capacitación	Ing. Manuel Ovalle								
Manejo de incidentes de seguridad.	Personal de TI	Capacitación	Experto externo								
Regulaciones legales aplicables	Personal de TI / Directivos	Capacitación	Ing. Ana Martinez								

Fuente: Los Autores

6.6.2 Recursos necesarios. Para el desarrollo el plan de concientización planteado es importante calcular el gasto financiero para que la gerencia destine en el presupuesto los recursos para que se lleve a cabo.

Las capacitaciones serán impartidas por personal interno y se desarrollaran directamente en las instalaciones y de Tecnofactory SAS por lo tanto no se incurrirá en gastos adicionales de salas de capacitación, pero si es necesario contar con los recursos para la compra de los elementos descritos en el cuadro 22 como se puede observar a continuación:

Cuadro 22. Recursos Necesarios

Recurso	Costo
Papelería en general	$10.000
Afiches	$200.000
Conferencistas	$3’000.000
Posters	$120.000
Recordatorios	$500.000
Total	$3.830.000

Fuente: Los Autores

6.7 MEJORAMIENTO

Se debe tener un punto de medición es necesario realizar encuestas y evaluaciones sobre las actividades realizadas y con ello conocer el impacto positivo y deficiencias a mejorar.

Por ello que, en la última fase, después de implementar el plan de toma de concientización es necesario repetir la actividad de Ataques de ingeniería Social, lo cual deberá experimentar una disminución esperada de dicho porcentaje. Así se podría medir la efectividad del plan. También otro método es mediante evaluaciones o cuestionarios. Y el diligenciamiento de Actas de asistencia.

7. PROPUESTA DE IMPLEMENTACIÓN

Uno de los objetivos del presente proyecto aparte de diseñar un SGSI a partir de los objetivos y necesidades de la empresa Tecnofactory S.A.S, es el de realizar una propuesta de implementación con base en el estándar ISO 27001 y de algunos apartes del estándar de buenas prácticas ISO 27002 que definen un sistema de gestión de seguridad de la información (SGSI).

Es por ello por lo que Tecnofactory S.A.S debe contemplar también la seguridad de la información en el ciclo de vida de los activos y la naturaleza cambiante de los riesgos sobre ellos, propendiendo la mejora continua del SGSI.

Es así como el Sistema de Gestión de Seguridad de la Información (SGSI) debe tener un enfoque particular basado en “Planear - Hacer - Verificar- Actuar” PHVA, este permite establecer una mejora continua en la organización.

- **Planear**: Es una fase de diseño del SGSI, consistente en evaluar los riesgos de seguridad de la información y la selección de controles adecuados.

- **Hacer**: Es una fase que envuelve la implantación y operación de los controles.

- **Verificar**: Es una fase que tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del SGSI.

- **Actuar**: En esta fase se realizan cambios cuando sea necesario para llevar de vuelta el SGSI a máximo rendimiento.

Se presenta está teniendo como referencia todo lo expuesto en el diseño, desde la identificación de activos de información, la valoración del estado actual, el tratamiento de los riesgos y la presentación de políticas de seguridad.

En ese orden de ideas esta propuesta de implementación contempla las siguientes fases según el diseño planteado en este documento:

Fase 1: Identificación del inventario de los activos de información

De acuerdo con la política de Gestión todo activo tecnológico propio o en categoría de préstamo donde se guarde información de los procesos de Tecnofactory S.A.S. se debe encontrar en el inventario de activos de la organización, el cual debe actualizarse cada vez que se adquiera un activo nuevo, en calidad de préstamo o haya finalizado su vida útil, con el fin de proteger la información contenida en ellos.

Fase 2: Análisis de riesgos con su plan de tratamiento de riesgos

Se establecerá según su origen y contexto los diferentes riesgos que los activos de información se encuentren expuestos, efectuar una valoración y después de identificar todo lo anterior, ya se puede definir la política de tratamiento del riesgo, que defina el manejo que se le dará a cada riesgo asumiéndolo o adoptando controles que permitan eliminarlo o por lo menos reducirlo.

Fase 3: Gestión documental de las políticas de seguridad de la información

Siendo el Sistema de Gestión de Seguridad de la Información una decisión estratégica que debe involucrar a toda la organización y que debe ser apoyada y dirigida desde la Dirección General, y mediante el consenso del Comité de Seguridad de la Información, este último designado como responsable de la revisión y valoración de la Política General de Seguridad de la Información y las políticas que den como resultado del análisis del estándar de implementación (ISO 27002).

Dichas políticas se enumeran a continuación:

- Política Talento Humano
- Política Gestión de Activos
- Política Control de Accesos
- Política Cifrado
- Política Seguridad Física
- Política Seguridad Operacional
- Política Seguridad en las Telecomunicaciones
- Política Relaciones con Proveedores
- Política Gestión de Incidentes
- Política de Continuidad del Negocio
- Política de Escritorios Limpios

Fase 4: Implementación de controles

Teniendo en cuenta que un control es una medida u opción de contención aplicada para la modificación del riesgo, y se define de acuerdo con el nivel estimado para el riesgo, y los recursos de la organización. En el caso de la empresa Tecnofactory S.A.S. se identificaron un total de 82 riesgos, para los cuales se propone un plan de tratamiento de estos. Dados los hallazgos encontrados se recomienda iniciar con la aplicación de controles para los riesgos clasificados con niveles alto, o crítico, ya que, según el análisis de riesgos realizado en el presente documento, son los que mayor impacto ocasionarían sobre la empresa Tecnofactory S.A.S.

Fase 5: Ejecución del plan de concientización y capacitación

Esta fase requiere un tiempo de concienciación y formación para dar a conocer qué se está haciendo y qué fin persigue, a todo el personal de la empresa. Es una labor que contempla la capacitación a los colaboradores, posteriormente la planeación para la campaña de expectativa, la ejecución de esta y la evaluación de los conocimientos adquiridos, aspectos a mejorar y en general la adopción de un cambio de postura en la cultura organizacional frente a la seguridad de la información por parte de toda la compañía.

Fase 6: Evaluación del cumplimiento de la norma ISO 27001:2013

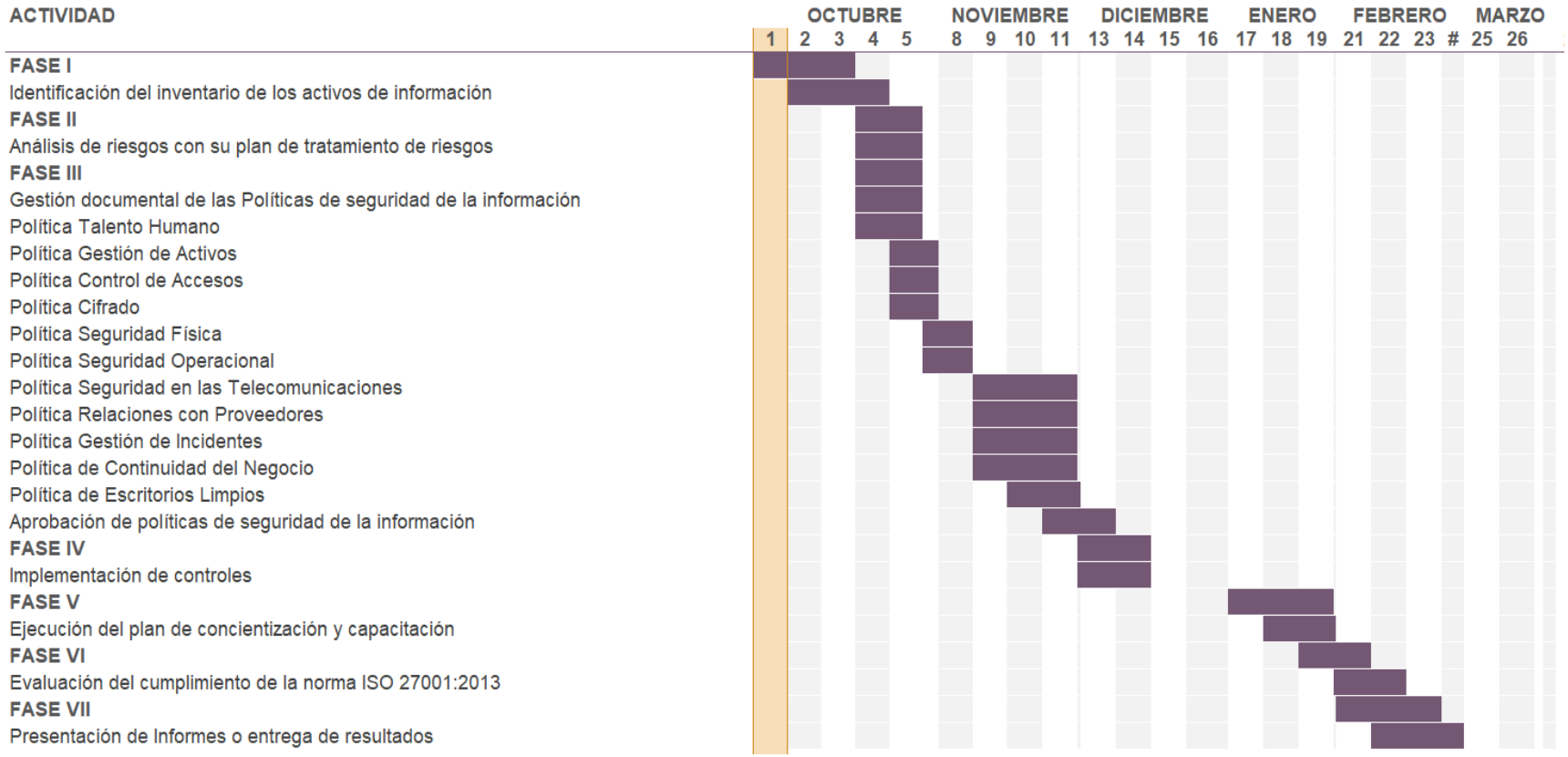
En esta fase se entra a realizarse auditorias que permitan evaluar el cumplimiento de la norma, se sugiere ya que la empresa cuenta con personal idóneo para realizar auditorías internas previo a solicitar a un ente externo la revisión del SGSI, estás decisiones se deben tomar en la medida que se tengan los registros que evidencian la efectiva implantación del sistema y el cumplimiento de los requisitos. Entre estos registros se incluyen indicadores y métricas de seguridad que permitan evaluar la consecuencia de los objetivos de seguridad establecidos.

Fase 7: Presentación de Informes o entrega de resultados

En esta última etapa tiene como finalidad la entrega de los resultados a los a Dirección General de Tecnofactory S.A.S., así como al Comité de Seguridad de la Información luego de la evaluación del cumplimiento de la norma. El tiempo estimado para la implementación contemplado es de alrededor de 5 a 6 meses.

Se propone un cronograma para determinar las actividades y tiempos requeridos en cada una de las faces descritas con anterioridad y plasmadas en el cuadro 23.

Cuadro 23. Cronograma del plan de implementación



Fuente: Los Autores

Costo de implementación: Uno de los factores más importantes para que Tecnofactory SAS tome la decisión de implementar el presente diseño es conocer los costos que deberían designar para ello.

En el cuadro 24 se realiza una descripción de las actividades y herramientas necesarias para ello, el costo que esto tendría y la recurrencia de los pagos que deben asumirse si deciden realizar la implementación.

Cuadro 24. Costo de la implementación de las herramientas propuestas

Descripción	Costo	Recurrencia	Total
Profesional o proveedor de servicios para la Creación y/o modificación de políticas, procedimientos, guías y formatos del SGSI.	$ 5.000.000	6 meses	$30.000.000
Se contempla un canal de respaldo aparte del proveedor de servicio de conectividad Claro y se encuentra el proveedor IFX con el servicio de INTERNET Premium y gestión del servicio por medio de Firewall online.	$ 5.498.250	Mensual	$5.498.250
Capacitación e implementación de Microsoft Secure Score.	$ 3.800.000	Único pago	$ 3.800.000
SonarQube. Permite el análisis de los códigos fuente en búsqueda de errores, malas prácticas o códigos excesivamente complejos que dificulten su legibilidad y mantenimiento. DB *Storage* temporal.	$ 297.008	Mensual	$297.008
Acunetix. Análisis de vulnerabilidades y recomendaciones para los sitios web que construye en fábrica. La versión Online Premium es 12 meses, para 10 licencias.	$ 2.056.750	Único pago	$24.681.000
Conferencista, material de apoyo e incentivos.	$ 8.000.000	Único pago	$8.000.000
Criptografía, implementación de herramienta para el cifrado de información, se encuentran varias de forma gratuita.	0	0	0

Cuadrado 24. Continuación

Monitoreo SGSI, se requiere un profesional que realice el análisis de los procesos actuales que se realizan en el SGSI, identificando las falencias, sugiriendo nuevos controles y procesos enfocados al cumplimiento de la norma ISO 27001:2013	$ 5.000.000	Mensual	$ 5.000.000
Total			**$ 77.276.258**

Fuente: Los Autores

8. CONCLUSIONES

En la realización del diseño del sistema de gestión de seguridad de la información bajo la norma ISO 27001:2013 para la empresa Tecnofactory S.A.S, se logró establecer una serie de controles, políticas de seguridad de la información y un plan de concientización, los cuales se aconseja implementar lo antes posible debido al bajo nivel de seguridad evidenciado.

Se logró identificar estado actual de la seguridad de la información en Tecnofactory S.A.S mediante un análisis GAP, basado en el cumplimiento de los controles propuestos en el anexo A de la norma ISO 27001:2013, en donde se concluyó que la empresa está en un estado crítico ya que actualmente cuenta con tan solo el 22% de cumplimiento del 100% esperado; debido a la falta de definición o inclusión parcial de la seguridad de la información en los procesos de la compañía y una precaria metodología para la gestión de riesgos, esto muestra la necesidad urgente de la implementación del diseño lo antes posible.

En el proceso de identificación, clasificación y valoración los activos de información de Tecnofactory S.A.S., se estableció una escala de mayor a menor criticidad, lo cual le permite a la organización centralizar sus esfuerzos en los más críticos, pero sin descuidar el resto de sus activos.

Mediante el análisis de riesgos basado en la norma ISO/31000:2018, se pudo establecer cuáles son los riesgos a los que está expuesta la organización, y así definir de acuerdo con los parámetros de medición establecidos dentro del análisis, cuáles son los riesgos más críticos y de mayor probabilidad e impacto para la organización y que en consecuencia se aconseja sean tratados cuanto antes.

Del resultado obtenido en el análisis y la gestión de riesgos se establecen los controles del anexo A de la norma ISO/IEC 27001:2013, en un plan de tratamiento adecuado que permita con su posterior implementación minimizar los riesgos inherentes aproximadamente en un 80 %, dejando probablemente tan solo un 20 % de riesgos residuales, lo que demuestra la importancia de una urgente implementación del diseño realizado en el presente proyecto.

La norma ISO/IEC 27001:2013 tiene definida una serie de controles y contramedidas adecuados para preservar la confidencialidad, integridad y disponibilidad de los activos de información. Su implementación no tendría un alto costo y si permitirá mitigar riesgos que de llegar a materializarse pueden causar graves pérdidas económicas a la organización.

BIBLIOGRAFÍA

Iso2007.Es. Iso2007.Es. [En línea] Disponible: https://www.iso27000.es/glosario.html. [Citado el: 8 de 11 de 2021.]

Iso27000.Es. 2021. Iso27000.Es. [En línea] Disponible https://www.iso27000.es/glosario.html. [Citado el: 28 de 11 de 2021.]

ISOTOOLS EXCELLENCE. ISO 27001: ¿Cuál es la estructura de la nueva norma ISO 27001 2013? [en línea]. Bogotá: ISO Tools, 2017 Disponible: https://www.isotools.com.mx/la-estructura-la-nueva-norma-iso-27001-2013/. [Citado el 30 de junio de 2020].

ISOTOOLS EXCELLENCE. ISO 27001: ¿Qué es la ISO 27001? [en línea]. Bogotá: ISO Tools, 2017. Disponible: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/. [Citado el 30 de junio de 2020]

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Guía 02 – Elaboración de la política general de seguridad y privacidad de la información. [en línea]. Colombia: La entidad. [consultado el 01 de febrero de 2022]. Disponible en internet: < https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf >

PORTAL DE ISO 27001 EN ESPAÑOL. Beneficios [en línea]. Bogotá: ISO, 2016. Disponible: http://www.iso27000.es/sgsi.html. [Citado el 1 de julio de 2020]

SGSI Blog especializado en sistemas de Gestión de Seguridad de la Información: Anexo A en ISO 27001, objetivos y controles de referencia [en línea]. Bogotá: SGSI, 2020. Disponible: https://www.pmg-ssi.com/2020/0. [Citado el 30 de junio de 2020]