DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA SUPER SERVICIOS DEL VALLE S.A. BASADO EN LA NORMA ISO 27001:2013

CLAUDIA MARCELA NARVÁEZ VÉLEZ

UNIVERSIDAD NACIONAL ABIERTA A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

CARTAGO

2020

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA SUPER SERVICIOS DEL VALLE S.A. BASADO EN LA NORMA ISO 27001:2013

CLAUDIA MARCELA NARVÁEZ VÉLEZ

PROYECTO APLICADO

MARTIN CAMILO CANCELADO

DIRECTOR DE PROYECTO

UNIVERSIDAD NACIONAL ABIERTA A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

CARTAGO

2020

CONTENIDO

pág.

INDICE DE TABLAS

Pág.

INDICE DE FIGURAS

Pág.

INTRODUCCIÓN

Este proyecto plantea el diseño de un sistema de gestión de la seguridad de la información (SGSI) para la empresa Super Servicios del Valle S.A. Su desarrollo se basa en la norma ISO 27001:2013 la cual establece los requisitos para gestionar la seguridad de la información en una empresa.

Este SGSI se diseña con el propósito de garantizar la confidencialidad, integridad y disponibilidad de la información de la empresa y asimismo de los datos de carácter confidencial o personal de los usuarios y de los procesos.

Super Servicios del Valle S.A. consciente de los diversos riesgos, amenazas y vulnerabilidades existentes que atentan contra la seguridad y privacidad de la información, busca con el diseño de este sistema de gestión de seguridad de la información administrar y asegurar sus recursos mediante la implementación de políticas de seguridad, controles, asignación de responsables, auditorías y procesos de mejora que ayuden a garantizar la continuidad de las actividades de la empresa.

El diseño del SGSI para la empresa Super Servicios del Valle cuenta con el respaldo y compromiso de la dirección, parte fundamental dentro del proceso ya que se encarga de aprobar los controles planteados además de proveer los recursos necesarios para su desarrollo, mantenimiento y mejora continua.

1. TITULO

Diseño de un Sistema de Gestión de Seguridad de la Información para la empresa Super Servicios del Valle S.A. basado en la norma ISO 27001:2013.

Este proyecto se ubica en las siguientes áreas de conocimiento: tecnología de la información, seguridad de la Información, gestión de la seguridad, gestión de riesgos y sistema de gestión de seguridad de la información

2. DEFINICIÓN DEL PROBLEMA

2.1 ANTECEDENTES DEL PROBLEMA

Super Servicios del Valle, empresa operadora juegos de suerte y azar, además comercializa servicios como son recargas, SOAT y recaudos empresariales. En el desarrollo de sus actividades almacena información de carácter confidencial, lo cual genera un alto riesgo y la posibilidad de materialización de un ataque que pueda ocasionar la pérdida, alteración o divulgación de la información.

Actualmente, la empresa no cuenta con un SGSI que permita una adecuada gestión de riesgos, además entre los funcionarios no existe concientización y conocimiento referente a temas de seguridad, lo que genera poca efectividad de los mecanismos de control establecidos. Por nombrar algunos ejemplos de las fallas que se presentan están, el mal uso en las estaciones de trabajo de los dispositivos de almacenamiento portátil, uso de contraseñas débiles para los aplicativos, entre otros.

De aquí la importancia de diseñar un SGSI para la empresa que ayude, a partir de la evaluación de riesgos, la implementación de políticas y controles de seguridad, evitar que la información quede expuesta ante amenazas y vulnerabilidades; de igual forma se debe concientizar a los funcionarios el riesgo que representa para la empresa el no adoptar el uso de las buenas prácticas de seguridad en el desarrollo de sus funciones, más aún si se tiene acceso a procesos críticos que pueden generar una brecha de seguridad y una posible materialización de un riesgo.

2.2 FORMULACIÓN DEL PROBLEMA

¿Cómo proteger efectivamente la información de los sistemas de información usados en la empresa Super Servicios del Valle?

2.3 DESCRIPCIÓN

El desarrollo de un SGSI inicia por el inventario y categorización de los activos más críticos de la organización. Son a estos a los que se les realiza el análisis de riesgos, el cual permite identificar las vulnerabilidades y amenazas de seguridad que pueden afectar los activos de la empresa; el resultado de este análisis debe ser tanto cualitativo como cuantitativo por lo que se debe crear la matriz de riesgos que muestra gráficamente según una escala de valoración, cual es el impacto y la probabilidad de ocurrencia de una amenaza o vulnerabilidad identificada.

El SGSI permitirá valorar la efectividad de controles establecidos con anterioridad y a su vez, se deberán proponer otros controles que contrarresten los nuevos riesgos identificados durante el desarrollo del análisis de riesgos. Este proyecto incluye el establecimiento de políticas de seguridad de la información que respalden los controles asignados. Igualmente se deben proponer auditorías e indicadores de logro para visualizar los resultados obtenidos, garantizar la eficacia de los controles y generar opciones de mejora para el SGSI.

3. JUSTIFICACIÓN

El diseño de un Sistema de Gestión de Seguridad de la Información para la empresa Super Servicios del Valle, permitirá gestionar eficientemente los riesgos que se puedan presentar atentando contra la seguridad de la información. Para la empresa la preservación de la confidencialidad, integridad y disponibilidad de la información es indispensable dentro del diario desarrollo de sus actividades, ya que así se da cumplimiento a las normatividades vigentes y, se garantiza que, con la evaluación de las vulnerabilidades y los riegos, además de la implantación de políticas de seguridad y controles se protegerá la información, minimizando el impacto en Caso de que se materialice cualquier vulnerabilidad.

Este SGSI, asimismo permitirá a la empresa fortalecer sus procesos y procedimientos tecnológicos e igualmente mejorará la cultura de seguridad entre los funcionarios de todos los niveles de la organización, asumiendo un rol y adquiriendo responsabilidades en el uso de las buenas prácticas de seguridad facilitando la protección de los activos de información. Otro de los beneficios que se puede lograr a través del diseño de un SGSI es el poder optar por una certificación en ISO 27001 lo cual generaría una ventaja competitiva para la empresa.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Diseñar un Sistema de Gestión de la Seguridad de la Información para la empresa Super Servicios del Valle, que garantice la confidencialidad, integridad y disponibilidad de la información.

4.2 OBJETIVOS ESPECÍFICOS

- Clasificar los activos de información de la empresa Super Servicios del Valle.
- Analizar las vulnerabilidades, amenazas y riesgos presentes.
- Establecer políticas y controles de seguridad basados en la norma ISO 27001:2013 para mitigar y reducir los riesgos detectados.
- Definir la estructura organizacional, roles y responsabilidades de los funcionarios en cuanto a la Seguridad de la Información en la empresa Super Servicios del Valle.

5. MARCO REFERENCIAL

Proyectos sobre la creación de un sistema de gestión de seguridad de la información para desarrollarse en la empresa SSV S.A. no habían sido propuestos con anterioridad. Actualmente en la empresa, se están estableciendo procedimientos en cuanto a la protección de datos personales. Además, se están implementando políticas y controles de seguridad como, por ejemplo, para la creación de contraseñas seguras utilizadas en el ingreso a los aplicativos administrativos y a su vez la configuración de estos aplicativos para dar cumplimiento de las condiciones establecidas.

Al consultar sobre empresas del sector que cuenten con un SGSI y certificación ISO/IEC 27001 encontramos las siguientes:

Red de servicios del Quindío S.A. perteneciente al grupo de empresas de juegos suerte y azar, en la actualidad es la primera empresa quindiana en obtener la certificación ISO 27001 asegurando por medio de su SGSI y sus políticas de seguridad de la información que es una empresa con un nivel alto de confiabilidad en sus procesos transaccionales proporcionando así seguridad y confianza tanto a los usuarios de los servicios, como a sus aliados.

Codesa, empresa encargada de proveer tecnología y desarrollos informáticos para suplir necesidades de administración, consultoría, capacitación, desarrollo de software, del grupo de empresas asociadas y usuarias que la constituyen.

SuperGIROS, cuenta con SGI compuesto por las normas de Seguridad de la Información (ISO 27001:2013), Calidad (ISO 9001:2015) y SST (decreto 1072 de 2015). Articulando los requisitos transversales de los tres sistemas, contribuyendo así a la mejora continua en los procesos.

Es por esto la importancia que tiene para la empresa SSV S.A el desarrollo de este proyecto para así de la mano del proceso TIC realizar la adecuada implementación de controles necesarios para mitigar los riesgos de seguridad de la información.

5.1 MARCO TEÓRICO

Durante el desarrollo de este proyecto, se deberán tener en cuenta diferentes términos que permitirán comprender todo lo que reúne un SGSI y así poder realizar su diseño en una empresa, el cual será una herramienta que permitirá aumentar los niveles de seguridad y la protección de los activos de la empresa.

La seguridad de la información en una empresa, según ISO 27001:2013[1], consiste en:

• Preservar la confidencialidad, integridad y disponibilidad de la información. Asimismo, de los sistemas que estén implicados en su tratamiento.

• Confidencialidad: La información no se encuentra accesible para funcionarios, procesos o sistemas no autorizados para su tratamiento.

• Integridad: Se garantiza que la información no puede ser alterada, copiada o eliminada.

• Disponibilidad: El acceso y utilización de la información y los sistemas de tratamiento se encuentran disponibles en cualquier momento que sea requerido.

Activo: Cualquier elemento o información, que represente o no valor contable para la organización.

Sistemas de control de acceso: Mecanismos que permiten acceder a información o recursos mediante una identificación previamente autenticada.

Pueden ser de tipo:

• Físico: Carné, Vigilantes, CCTV, controles biométricos.

• Administrativos: Procesos de selección, políticas de seguridad.

• Técnicos: Firewall, Usuario – Contraseña, privilegios de usuario, listas de control de acceso, detectores de intrusos, reglas y filtrado, segmentación de la red.

Se conoce que los controles de seguridad más implementados en Latinoamérica son el antivirus (83%), el firewall (75%) y el backup de la información (67%). [2]

---

[1] NTC-ISO-IEC 27001. {en línea}. {06 de noviembre de 2017}. Disponible en: (https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-ISO-IEC27001.pdf).

[2] ESET Security Report Latinoamérica 2017. {en línea}. {13 de noviembre de 2017}. Disponible en:

5.1.1. Riesgo informático: Es la probabilidad de que una amenaza se materialice generando pérdidas o daños en equipos, periféricos, instalaciones, aplicaciones y sistemas de información.

Se presentan en cualquiera de los elementos de un computador: hardware, S.O., o en el software. Cuando existe una vulnerabilidad en un equipo no significa que obligatoriamente va a fallar, pero sí es posible que alguien ataque el equipo aprovechando este punto débil.

5.1.2. Auditoría: Proceso sistemático, independiente y documentado que permite obtener evidencias de auditoria para determinar el grado de cumplimiento de acuerdo con los criterios de auditoria. (ISO/IEC 27000)

5.1.3. SGSI: Permite la gestión de la seguridad de la información mediante procesos sistemáticos, documentados y de conocimiento por parte de toda la organización. Su propósito principal es garantizar que los sistemas de información en las empresas estén protegidos por mecanismos de control físicos y lógicos que protejan estos activos frente a cualquier vulnerabilidad o amenaza. Entre los ejemplos más comunes están: modalidades de fraude, espionaje, sabotaje o vandalismo, virus informáticos, el "hacking" o ataques cibernéticos o incluso incidentes de seguridad causados voluntaria o involuntariamente en la empresa o aquellos que surgen accidentalmente por catástrofes naturales y fallas técnicos.

Las practicas más utilizadas para la gestión de la seguridad en Latinoamérica son:[3]

políticas de seguridad (74%).

Auditorías internas y/o externas (38%) y la clasificación de la información (31%).

5.1.4. ISO 27001
Busca minimizar el riesgo en los sistemas de información de las empresas mediante la especificación de requisitos para establecer, implementar, mantener y mejorar continuamente un SGSI. Permite que una empresa sea certificada confirmando el cumplimiento de esta norma en la organización.

5.1.5. ISO 27002
Proporciona directrices detalladas para la implantación de controles y el uso de buenas prácticas dentro de una organización.[4]

---

[3] ESET Security Report Latinoamérica 2017. {en línea}. {13 de noviembre de 2017}. Disponible en: (https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf).

[4] GTC–ISO/IEC 27002. {en línea}. {13 de Noviembre de 2017}. Disponible en: (https://tienda.icontec.org/wp-content/uploads/pdfs/GTC-ISO-IEC27002.pdf

Esta norma define 14 dominios, 35 objetivos y 114 controles, de acuerdo con cada grupo de activos que se pueden encontrar en una empresa, lo que facilita identificar las actividades necesarias para la implementación de la seguridad informática y así lograr la protección de los activos y la identificación de cada uno de los posibles riesgos que se pueden presentar en la empresa. Estos son:

5.1.5.1 Objetivos de control

- Política de seguridad

Teniendo en cuenta los objetivos establecidos en la empresa para garantizar soporte y gestión, se requiere implantar políticas de seguridad de la información acordes, que permitan ejercer control de forma general en cada uno de los procesos. En la tabla 1 se relacionan los controles de seguridad que se deben cumplir al plantear políticas de seguridad de la información.

Tabla 1. Política de seguridad

Objetivo de control	Control
Política de seguridad de la información.[5]	Documento de política de seguridad de la información. Revisión de la política de seguridad de la información.

Fuente: ISO27002. Controles de seguridad.

- Aspectos organizativos de la seguridad de la información

Tiene como finalidad instaurar un marco de referencia que permita definir el camino para la implantación y control de la seguridad de la información dentro de la empresa. En donde la alta gerencia tiene como responsabilidades establecer:

- Políticas de seguridad.
- Roles de los comités y encargados de coordinar y supervisar el proceso.

[5] Norma técnica colombiana ntc-iso/iec 27001. Anexo A (normativo) Objetivos De Control Y Controles {en línea}. {25 de febrero 2020}. Disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

En la tabla 2 se relacionan los controles de seguridad que se deben cumplir al plantear de acuerdo con los aspectos organizativos de la seguridad de la información.

Tabla 2. Aspectos organizativos de la seguridad de la información.

Objetivo de control	Control
Organización interna[6]	Compromiso de la gerencia con la seguridad de la información. Asignación de responsabilidades relativas a la S.I. Proceso de autorización de recursos para el tratamiento de la información. Acuerdos de confidencialidad. Contacto con las autoridades y grupos de especial interés. Revisión independiente de la seguridad de la información. Terceros. Identificación de los riesgos derivados del acceso de terceros y tratamiento de la seguridad en la relación con los clientes y terceros.

Fuente: ISO27002. Controles de seguridad.

- Seguridad ligada a los recursos humanos

Establece las medidas necesarias para controlar la seguridad de la información, que ha sido manejada por el proceso de recurso humano de la empresa durante el ciclo de vida de contratación de los empleados de la empresa (ingreso – traslado - retiro) y procesos de capacitación. En la tabla 3 se relacionan los controles de seguridad de la información, que se deben tener en cuenta en los procesos que se realizan por el proceso de gestión humana.

[6] Norma técnica colombiana ntc-iso/iec 27001. Anexo A (normativo) Objetivos De Control Y Controles {en línea}. {25 de febrero 2020}. Disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

Tabla 3. Seguridad ligada a los recursos humanos.[7]

Objetivo de control	Control
Antes de la contratación.	Funciones y responsabilidades. Investigación de antecedentes. Términos y condiciones de contratación.
Durante la contratación.	Responsabilidades de la Dirección. Concienciación, formación y capacitación en S.I Proceso disciplinario.
Cese del empleo o cambio de puesto de trabajo.	Responsabilidad del cese o cambio. Devolución de activos. Cancelación de los derechos de acceso.

Fuente: ISO27002. Controles de seguridad.

- Gestión de activos

Su enfoque principal es la protección de los activos de la empresa. Garantizando que se encuentren inventariados y asignados a un responsable quien a su vez debe garantizar hacer un buen uso y tener una correcta manipulación durante su manipulación en el desarrollo de sus funciones. La tabla 4 lista los controles de seguridad para realizar la gestión de activos en la empresa.

Tabla 4. Gestión de activos.

Objetivo de control	Control
Responsabilidad sobre los activos.[8]	Inventario y propiedad de los activos. Uso aceptable de los activos. Clasificación de la información. Directrices, etiquetado y manipulación de la información.

Fuente: ISO27002. Controles de seguridad.

[7] Norma técnica colombiana ntc-iso/iec 27001. Anexo A (normativo) Objetivos De Control Y Controles {en línea}. {25 de febrero 2020}. Disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

[8] Norma técnica colombiana ntc-iso/iec 27001. Anexo A (normativo) Objetivos De Control Y Controles {en línea}. {25 de febrero 2020}. Disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

- Control de acceso

Se garantiza que para cada usuario el acceso a los sistemas de información de la empresa se realizará de forma controlada, es decir incluyendo única y exclusivamente los permisos para manipular la información que requiera para el desempeño de sus labores dentro de la empresa. En la tabla 5 se relacionan los controles de seguridad que se deben aplicar para garantizar el control de acceso lógico y físico de la empresa.

Tabla 5. Control de acceso.[9]

Objetivo de control	Control
Requisitos de negocio para el control de acceso.	Política de control de acceso.
Gestión de usuarios.	Registro y gestión de privilegios de usuario. Revisión de los derechos de acceso de usuario.
Responsabilidades de usuarios.	Uso de contraseñas. Equipo desatendido. Política de puesto de trabajo despejado y pantalla limpia.
Control de acceso a la red.	Política de uso de los servicios en red. Autenticación e identificación de usuario y equipos en las redes. Protección de los puertos de diagnóstico y configuración remotos. Segregación de las redes. Control de la conexión a la red. Control de encaminamiento (routing) de red.
Control de acceso al sistema operativo.	Procedimientos seguros de inicio de sesión. Identificación y autenticación de usuario. Sistema de gestión de contraseñas. Uso de los recursos del sistema. Desconexión automática y limitación del tiempo de conexión.
Control de acceso a las aplicaciones y a la información.	Restricción del acceso a la información. Aislamiento de sistemas sensibles.
Ordenadores portátiles y teletrabajo.	Ordenadores portátiles móviles y teletrabajo.

Fuente: ISO27002. Controles de seguridad.

[9] Ibid.

- Cifrado

Uso de sistemas y técnicas criptográficas que permitan proteger y garantizar la confidencialidad e integridad de la información que es manejada por el personal de la empresa de acuerdo con el análisis de riesgo efectuado. En la tabla 6 se relacionan los controles de seguridad criptográficos.

Tabla 6. Cifrado.

Objetivo de control	Control
Controles Criptográficos.[10]	Política de uso de los controles criptográficos. Gestión de claves.

Fuente: ISO27002. Controles de seguridad.

- Seguridad física y del entorno

Busca la protección de las instalaciones de la empresa y a su vez de la información que se maneja durante el desarrollo de sus procesos, estableciendo barreras de seguridad lógicas y controles de acceso físico que impidan la filtración de información sensible por cualquier tipo de amenaza. En la tabla 7 se relacionan los controles de seguridad que se deben cumplir en la empresa para garantizar la seguridad física y del entorno.

Tabla 7. Seguridad física y del entorno.[11]

Objetivo de control	Control
Áreas seguras.	Controles físicos de entrada. Protección contra las amenazas externas y de origen ambiental.
Seguridad de los equipos.	Emplazamiento y protección de equipos. Seguridad del cableado.

[10] Norma técnica colombiana ntc-iso/iec 27001. Anexo A (normativo) Objetivos De Control Y Controles {en línea}. {25 de febrero 2020}. Disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

[11] Norma técnica colombiana ntc-iso/iec 27001. Anexo A (normativo) Objetivos De Control Y Controles {en línea}. {25 de febrero 2020}. Disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

	Mantenimiento de los equipos. Seguridad de los equipos fuera de las instalaciones. Reutilización o retirada segura de equipos. Disposición final de materiales propiedad de la empresa.

Fuente: ISO27002. Controles de seguridad.

- Seguridad de las operaciones

Se determinan los procesos y responsabilidades de las operaciones que lleva a cabo la organización, garantizando que cada proceso esté relacionado con la información ejecutada adecuadamente y cuente con la protección necesaria durante la gestión de cambios, la provisión de servicios por terceros, las copias de seguridad y el intercambio de la información.

En la tabla 8 se relacionan los controles de seguridad propios para que en la empresa se minimicen los riesgos en las relaciones con terceros, o los que son provocados por códigos maliciosos o fallos de red.

Tabla 8. Gestión de comunicaciones y operaciones.[12]

Objetivo de control	Control
Responsabilidades y procedimientos de operación.	Documentación de los procedimientos de operación. Gestión de cambios y segregación de tareas. Ambientes de desarrollo separados.
Gestión de la provisión de servicios por terceros.	Provisión de servicios. Supervisión de los servicios prestados por terceros. Gestión del cambio en los servicios prestados por terceros.
Planificación y aceptación del sistema.	Gestión de capacidades. Aceptación del sistema.
Protección contra el código malicioso y descargable.	Controles contra código malicioso.

[12] Norma técnica colombiana ntc-iso/iec 27001. Anexo A (normativo) Objetivos De Control Y Controles {en línea}. {25 de febrero 2020}. Disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

Copias de seguridad.	Copias de seguridad de la información.
Gestión de la seguridad de las redes.	Controles para los servicios de red.
Manipulación de los soportes.	Gestión de soportes extraíbles. Procedimientos de manipulación de la información. Seguridad de la documentación del sistema.
Intercambio de información.	Políticas y procedimientos de intercambio de información. Mensajería electrónica.
Servicios de comercio electrónico.	Comercio electrónico. Transacciones en línea. Información públicamente disponible.
Supervisión.	Registros de auditoría. Supervisión del uso del sistema. Protección de la información de los registros. Registros de administración y operación. Registro de fallos. Sincronización del reloj.

Fuente: ISO27002. Controles de seguridad.

- Seguridad de las comunicaciones

Busca el aseguramiento y protección de la información transmitida a través de las redes telemáticas, así como la protección de la infraestructura de las empresas. En algunos Casos se debe instaurar controles adicionales de protección para la información confidencial que pasa a través de redes públicas. En la tabla 9 se relacionan los controles de seguridad para tener una adecuada gestión de las redes de comunicaciones de la empresa.

Tabla 9. Gestión de comunicaciones y operaciones.[13]

Objetivo de control	Control
Gestión de la seguridad en las redes.	Controles de red.

[13] Norma técnica colombiana ntc-iso/iec 27001. Anexo A (normativo) Objetivos De Control Y Controles {en línea}. {25 de febrero 2020}. Disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

	Mecanismos de seguridad asociados a servicios de red. Segregación de redes.
Gestión de la seguridad en las redes.	Políticas y procedimientos de intercambio de información. Acuerdos de confidencialidad y secreto.

Fuente: ISO27002. Controles de seguridad.

- Adquisición, desarrollo y mantenimiento de sistemas de información

Dominio dirigido a las empresas que desarrollan software internamente o que tenga un contrato con otra empresa que se encarga de desarrollarlo. Establece los requisitos en la etapa de pruebas, implantación y desarrollo de software para que sea seguro. En la tabla 10 se muestran los controles de seguridad requeridos al momento de adquirir, desarrollar sistemas de información.

Tabla 10. Adquisición, desarrollo y mantenimiento de sistemas de información.[14]

Objetivo de control	Control
Requisitos de seguridad de los sistemas de información.	Análisis y especificación de los requisitos de seguridad.
Tratamiento correcto de las aplicaciones.	Validación de los datos de entrada y salida. Control del procesamiento interno. Integridad de los mensajes.
Controles criptográficos.	Política de uso de los controles criptográficos. Gestión de claves.
Seguridad de los archivos de sistema.	Control del software en explotación. Protección de los datos de prueba del sistema. Control de acceso al código fuente de los programas.
Seguridad en los procesos de desarrollo y soporte.	Procedimientos de control de cambios. Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. Restricciones a los cambios en los paquetes de software.

[14] Norma técnica colombiana ntc-iso/iec 27001. Anexo A (normativo) Objetivos De Control Y Controles {en línea}. {25 de febrero 2020}. Disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

	Fugas de información. Externalización del desarrollo de software.
Gestión de la vulnerabilidad técnica.	Control de las vulnerabilidades técnicas.

Fuente: ISO27002. Controles de seguridad.

- Relaciones con proveedores

Implementación de un nivel apropiado de seguridad de la información mediante acuerdos, monitorizar su cumplimiento y manejar los cambios para asegurar que los servicios sean entregados para satisfacer todos los requerimientos acordados con terceras personas. En la tabla 11 se muestran los controles de seguridad que se deben cumplir para evitar condiciones inseguras en las relaciones que se establezcan entre la empresa y los proveedores.

Tabla 11. Relaciones con proveedores.[15]

Objetivo de control	Control
Seguridad de la información en las relaciones con proveedores.	Política de seguridad de la información de proveedores. Tratamiento del riesgo dentro de acuerdos de proveedores.
Gestión de la prestación del servicio por proveedores.	Supervisión y revisión de los servicios prestados por terceros. Gestión de cambios en los servicios prestados por terceros.

Fuente: ISO27002. Controles de seguridad.

- Gestión de incidentes en la seguridad de la información

Dominio que aplica un proceso de mejora continua en la gestión de percances que se presenta en las empresas en el campo de seguridad de la información. En la

[15] Norma técnica colombiana ntc-iso/iec 27001. Anexo A (normativo) Objetivos De Control Y Controles {en línea}. {25 de febrero 2020}. Disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

tabla 12 se relacionan los controles de seguridad recomendados para realizar una correcta gestión de incidentes en la empresa.

Tabla 12. Gestión de incidentes en la seguridad de la información.[16]

Objetivo de control	Control
Notificación de eventos y puntos débiles de seguridad de la información.	Notificación de los eventos de seguridad de la información. Notificación de puntos débiles de seguridad.
Gestión de incidentes y mejoras de seguridad de la información.	Responsabilidades y procedimientos. Oportunidades de mejora a partir de incidentes de seguridad de la información. Recopilación de evidencias.

Fuente: ISO27002. Controles de seguridad.

- Gestión de la continuidad del negocio

Garantiza la continuidad operativa de la empresa, aplicando controles que eviten o minimicen todos los incidentes de las actividades desarrolladas por la empresa que puedan generar un impacto. En la tabla 13 se muestran que controles de seguridad se deben aplicar para crear en la empresa el modelo de continuidad del negocio.

Tabla 13. Gestión de la continuidad del negocio.[17]

Objetivo de control	Control
Aspectos de seguridad de la información en la gestión de la continuidad del negocio.	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio y evaluación de riesgos. Pruebas, mantenimiento y reevaluación de planes de continuidad.

Fuente: ISO27002. Controles de seguridad.

[16] Ibid.

[17] Norma técnica colombiana ntc-iso/iec 27001. Anexo A (normativo) Objetivos De Control Y Controles {en línea}. {25 de febrero 2020}. Disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/NTC-ISO-IEC%2027001.pdf

- Cumplimiento

Asegurar los requisitos legales aplicables en torno a la seguridad de la información que han sido referidos al diseño y gestión de los sistemas de informáticos. En la tabla 14 se muestran que controles de seguridad se deben aplicar en la empresa para dar cumplimiento a los requisitos legales.

Tabla 14. Cumplimiento.

Objetivo de control	Control
Cumplimiento de los requisitos legales.[18]	Identificación de la legislación aplicable. Protección de los documentos de la organización. Protección de datos y privacidad de la información de carácter personal. Prevención del uso indebido de recursos de tratamiento de la información. Regulación de los controles criptográficos.
Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.	Cumplimiento de las políticas y normas de seguridad.
Consideraciones sobre las auditorías de los Sistemas de Información.	Controles de auditoría de los sistemas de información. Protección de las herramientas de auditoría de los S.I.

Fuente: ISO27002. Controles de seguridad.

5.1.8. Ciclo Deming

El concepto del PHVA nació a finales de la década de 1970 y fue propuesta por Edwards Deming. Nació del método científico: las etapas de hipótesis, experimentación y evaluación del método científico se relacionan a Plan, Do, y Check del ciclo de Deming.

Esto ciclo es utilizado ya que facilita la forma en que debe ser gestionado el SGSI. Como se muestra en la figura 1, en cada una de sus fases permite identificar que actividades se deben llevar a cabo para ejecutar el SGSI, por ejemplo:

[18] Ibid.

Planear:

En esta etapa del ciclo PHVA se define el alcance del SGSI de acuerdo con el contexto de la empresa, sus activos y los sistemas de información que maneja. Se realiza la identificación, el análisis y la evaluación de los riesgos, además de identificar como debe ser su tratamiento determinando los objetivos de control. A su vez se realiza la planeación de las actividades.

Hacer:

Es en esta parte del ciclo es en donde las acciones, los recursos y los responsables son identificados para realizar un plan que permita hacer un correcto tratamiento de los riesgos ya identificados. Igualmente, se deben definir métricas que permitan comparar y medir la eficacia de cada uno de los controles implementados permitiendo evaluar los resultados generados.

Finalmente, se debe crear el espacio para capacitar los funcionarios de la organización, gestionar el mantenimiento del SGSI y verificar que los controles que han sido propuestos brindad una rápida detección de las vulnerabilidades y la detención de la materialización de las amenazas.

Verificar:

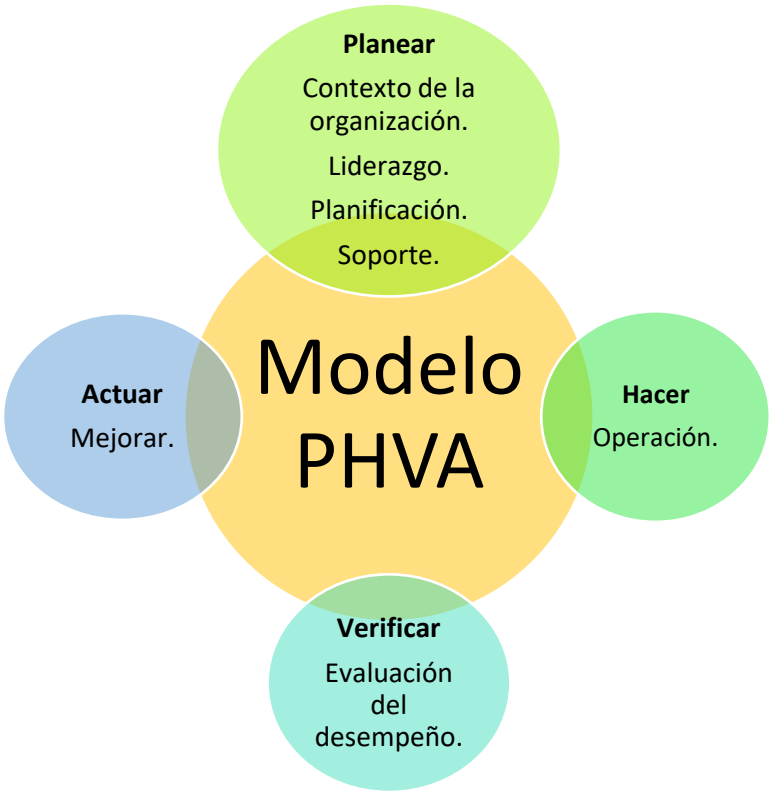
La empresa debe ejecutar procedimientos que permitan detectar posibles errores que se puedan presentar ya sean ocasionados por los funcionarios de la empresa o los sistemas o dispositivos tecnológicos. Del mismo modo, las auditorías internas deben ser periódicas, así como la revisión de cambios que se pueden producir en la empresa a nivel tecnológico, organizacional o procedimental para garantizar que el alcance definido inicialmente en el SGSI aún continúe siendo el preciso para el manejo de los riesgos de la empresa o en Caso tal realizar las mejoras necesarias.

Actuar:

La empresa debe regularmente verificar el cumplimiento de los objetivos propuestos, introducir mejoras y asegurarse de que estas sean pertinentes. En este punto del ciclo, al ser este de vida continua, puede llevar nuevamente a la fase de Planear iniciando así cada una de las fases, aunque no se debe tener una secuencia estricta.

Esta metodología PHVA permite el desarrollo de los objetivos específicos y, el alcance de los resultados esperados dentro de un SGSI además de su mejora continua. Es recomendada por la ISO como la metodología más usada para este tipo de proyectos.

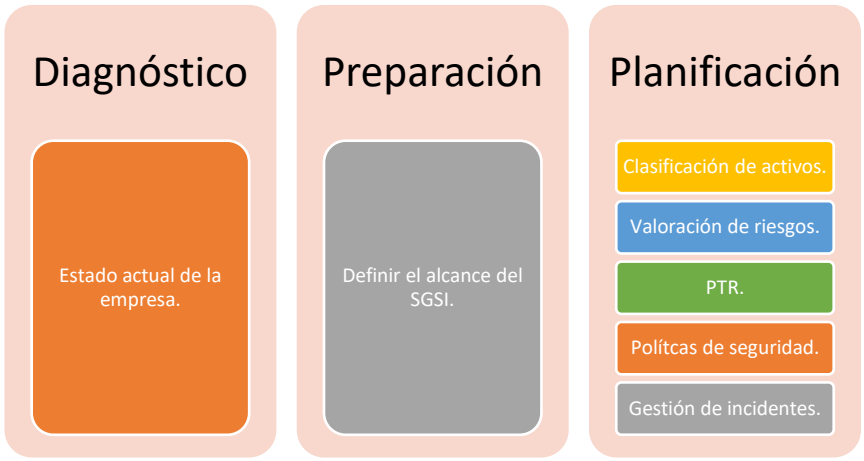
Figura 1. Modelo PHVA aplicado a procesos de SGSI.



Fuente: el autor.

En la figura 2 se muestra el proceso de diseño que se propone para el diagnóstico, preparación y planificación para llevar a cabo el desarrollo del Sistema de Gestión de Seguridad de la empresa Super Servicios del Valle S.A.:

Figura 2. Fases SGSI.



Fuente: El autor.

5.1.9. MAGERIT

Permite establecer controles preventivos y correctivos que contrarresten los efectos que se pueden presentar en el Caso de que las amenazas y las vulnerabilidades identificadas se materialicen y puedan desencadenar violaciones en la seguridad de la información de la empresa. Esta metodología actualmente se encuentra en la versión 3 y presenta una guía dividida en 3 libros para desarrollar paso a paso el análisis de riesgos de la empresa:

5.1.9.1. Libro I: El método

Describe la estructura que debe tener el modelo de gestión de riesgos, iniciando desde la conceptualización, la formalización de las actividades para realizar el tratamiento de los riesgos y su análisis, para finalmente lograr la gestión y la protección de los sistemas de información. Este libro está de acuerdo con lo que propone ISO para la gestión de riesgos.

5.1.9.2. Libro II: Catálogo de Elementos

Se utiliza para dar el enfoque al análisis del riesgo. Contiene como se deben categorizar los activos de información que deben considerarse en el SGSI, como valorar los activos inventariados de acuerdo con sus características y además un listado que incluye amenazas y controles para tener en cuenta.

5.1.9.3. Libro III: Guía de Técnicas

Describe técnicas utilizadas en el análisis y gestión de riesgos. Explicando los objetivos de su uso, elementos básicos asociados, principios fundamentales de elaboración, y se citan las fuentes bibliográficas para que se pueda profundizar acerca de cómo realizar un análisis de los riesgos.

5.2 MARCO CONCEPTUAL

5.2.1 Amenaza: Causa potencial de un incidente no deseado, que podría dañar uno o más activos de un sistema u organización.[19]

5.2.2 Vulnerabilidad: Es una debilidad del sistema informático que puede ser utilizada para causar daño.

5.2.3. Incidente de seguridad de la información: Evento o serie de eventos inesperados que tienden a comprometer o amenazar la seguridad de la información afectando su operación comercial. Estos pueden ser: fraude, espionaje, sabotaje, ataques de denegación del servicio, malware, son ejemplos comunes de las vulnerabilidades a las que se encuentran expuestos las empresas.

5.2.4. Riesgo: Grado de exposición de un activo que permite la materialización de una amenaza.

5.2.5. Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

5.2.6. Riesgo Residual: Nivel de riesgo remanente como resultado de la aplicación de medidas de seguridad sobre el activo

[19] NTC-ISO-IEC 27001. {en línea}. {06 de noviembre de 2017}. Disponible en: (https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-ISO-IEC27001.pdf).

5.3 MARCO LEGAL

El desarrollo del Sistema de Gestión de la Información en busca de la protección de los activos, los sistemas de información, los funcionarios, sus proveedores y comunidad en general debe considerar las siguientes leyes que buscan la regulación y penalización de los procedimientos que ponen en riesgo la confidencialidad, integridad y disponibilidad de la información o los servicios.

- Decreto 103 de 2015

Reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones. Regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información, y constituye el marco general de la protección del ejercicio del derecho de acceso a la información pública en Colombia[20].

- Decreto 886 de 2014

Tiene por objeto "desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma"[21].

- Ley estatutaria 1581 de 2012

"Tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma".[22]

- Ley 1273 de 2009

Esta ley está compuesta por 2 capítulos que buscan regular los delitos informáticos en Colombia velando por la protección de la información, impidiendo que se atente contra su integridad, disponibilidad y confidencialidad; imponiendo las sanciones

---

[20] Suin.gov.co. *Decreto 103 de 2015.* (2015). [En línea]. Disponible en: http://suin.gov.co/viewDocument.asp?ruta=Decretos/30019726. [Consultada el 13 de mayo de 2019]

[21] Suin-juriscol.gov.co. *Decreto 886 de 2014.* (2014). [En línea]. Disponible en: http://www.suin-juriscol.gov.co/viewDocument.asp?id=1184150

[22] Alcaldiabogota.gov.co. *Consulta de la Norma: Ley 1581 de 2012.* (2018). [En línea]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981. [Consultado el 13 Feb. 2018].

pertinentes a las personas que practiquen estos hechos.[23] En la tabla 15 se presentan los artículos de esta ley.

Tabla 15. Artículos Ley 1273 de 2009. Delitos informáticos en Colombia.[24]

Capítulo	Artículo	Descripción	Sanción
CAPÍTULO I: "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos"	Artículo 269A: Acceso abusivo a un sistema informático.[25]	Se explota alguna vulnerabilidad en el acceso a los sistemas de información o debilidades en los procedimientos de seguridad.	Incurrirá en pena de prisión de 48 a 96 meses y multa de 100 a 1000 SMLMV.
	Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.[26]	Se bloquea de forma ilegal un sistema o se impide su ingreso o acceso a cuentas de correo electrónico de otras personas, sin el debido consentimiento.	Incurrirá en pena de prisión de 48 a 96 meses y multa de 100 a 1000 SMLMV. Siempre que la conducta no se constituya como un delito de pena mayor.
	Artículo 269C: Interceptación de datos informáticos.[27]	Se interceptan o captan datos transmitidos de forma ilegal o sin la debida autorización.	Incurrirá en pena de prisión de 36 a 72 meses.
	Artículo 269D: Daño Informático.[28]	Se destruye, borra o altera los datos o un activo	Incurrirá en pena de prisión de 48 a 96

[23] Mintic.gov.co. Ley 1273 de 2009 - Ministerio de Tecnologías de la Información y las Comunicaciones. (2018). [En línea] Disponible en: http://www.mintic.gov.co/portal/604/w3-article-3705.html [Consultada el 12 febrero 2018].
[24] COLOMBIA. Congreso de Colombia. Ley 1273 (5, enero, 2009). Bogotá, [En línea] 2009. {Consultada el febrero 2020}. Disponible en: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf
[25] Ibid.., Art:269A.
[26] Ibid.., Art:269B.
[27] Ibid.., Art:269C.
[28] Ibid.., Art:269D.

		tangible sin estar facultado para ello.	meses y multa de 100 a 1000 SMLMV.
	Artículo 269E: Uso de software malicioso.[29]	Se vende, instala o distribuye software malicioso o programas dañinos para los activos informáticos.	Incurrirá en pena de prisión de 48 a 96 meses y multa de 100 a 1000 SMLMV.
	Artículo 269F: Violación de datos personales.[30]	Se intercepte, venda, cambie, trafique o sustraiga información personal de los archivos o bases de datos sin la debida autorización.	Incurrirá en pena de prisión de 48 a 96 meses y multa de 100 a 1000 SMLMV.
	Artículo 269G: Suplantación de sitios web para capturar datos personales.[31]	Se diseñen, implementen o redireccionen sitios web fraudulentos con el objetivo de capturar datos sensitivos de las personas.	Incurrirá en pena de prisión de 48 a 96 meses. Multa de 100 a 1000 SMLMV. Siempre que la conducta no se constituya como un delito de pena mayor.
CAPÍTULO II: " De los atentados informáticos y otras infracciones"	Artículo 269H: Circunstancias de agravación punitiva.[32]	Se revele información confidencial de las empresas o pongan en riesgo la seguridad nacional.	Las penas de acuerdo con los artículos descritos en este título se aumentarán de la mitad a las tres cuartas partes si la

[29] COLOMBIA. Congreso de Colombia. Ley 1273 (5, enero, 2009). Bogotá, [En línea] 2009. {Consultada el febrero 2020}. Disponible en: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf
[30] Ibid., Art:269E.
[31] Ibid., Art:269F.
[32] Ibid., Art:269G.

			conducta se cometiere sobre: Redes o sistemas Informáticos o de comunicaciones estatales, oficiales o del sector financiero, nacionales o extranjeros. Por servidor público en ejercicio de sus funciones. Abuso de confianza. Revelando el contenido de la información en perjuicio de otro. Obteniendo provecho para sí o para un tercero. Con fines terroristas o generando riesgo para la seguridad o defensa nacional. Utilizando como instrumento a un tercero de buena fe.
	Artículo 269I: Hurto por medios informáticos y semejantes.[33]	Se superen las barreras de seguridad informáticas y se extraigan de manera ilegal los activos, así como suplantar las	Incurrirá en las penas señaladas en el artículo 240 de este código.

[33] COLOMBIA. Congreso de Colombia. Ley 1273 (5, enero, 2009). Bogotá, [En línea] 2009. {Consultada el febrero 2020}. Disponible en: https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

		identidades de las personas.	
	Artículo 269J: Transferencia no consentida de activos.[34]	Se extraiga y transmita información con ánimo de lucro en perjuicio de un tercero.	Incurrirá en pena de prisión de 48 a 120 meses. Multa de 200 a 1500 SMLMV. Siempre que la conducta no se constituya como un delito de pena mayor.

Fuente: Mintic.[35]

- Ley 1032 de 2006

De la prestación, acceso o uso ilegales de los servicios de telecomunicaciones. Por la cual se modifican los artículos 257, 271, 272 y 306 del Código Penal.

- Constitución Política de Colombia de 1991 (artículos 61 y 74)

Hace referencia en sus artículos 61 y 74 a la protección de la propiedad intelectual y al derecho que les asiste a todas las personas a acceder a los documentos públicos.

[34]Mintic.gov.co. Ley 1273 de 2009 - Ministerio de Tecnologías de la Información y las Comunicaciones. (2018). [En línea] Disponible en: http://www.mintic.gov.co/portal/604/w3-article-3705.html [Consultada el 12 marzo 2018].
[35] Ibid.

6. DISEÑO METODOLÓGICO

Para el diseño del SGSI para la empresa Super Servicios del Valle se usará como guía la norma ISO 27001:2013 que a su vez se basa en el ciclo PHVA, el cual según la norma ISO9001 “puede aplicarse a todos los procesos”.

6.1. FASES DE DESARROLLO DEL PROYECTO

- Análisis:

En esta fase se debe determinar inicialmente el alcance del SGSI que se desea implementar para la empresa SSV S.A. Durante este proceso se realiza el inventario y la valoración de los activos con el fin de identificar los recursos de la organización y posteriormente determinar que amenazas y riesgos se pueden presentar.

Para el análisis y gestión de los riesgos se elige la metodología Magerit, la cual fue desarrollada por el Consejo Superior de Administración Electrónica y publicada por el Ministerio de Administraciones Públicas español. Es apropiada ya que estudia los riesgos que pueden afectar los sistemas de información y el entorno asociado, además recomienda medidas para adoptarse con el propósito de conocer, prevenir impedir, reducir o controlar los riesgos investigados.

Tiene como ventajas:

- Prepara la organización para procesos de evaluación, auditoría, certificación o acreditación.
- Busca concientizar a los responsables de los sistemas de información de la existencia de riesgos y la necesidad de contenerlos a tiempo.
- Permite definir y planificar las medidas oportunas para mantener los riesgos bajo control.
- Permite expresar los resultados en valores cualitativos y cuantitativos para la empresa, lo que permite a los directivos tomar decisiones.

MAGERIT, plantea los siguientes pasos para realizar el análisis de riesgos:

- Inventario de Activos
- Valoración de los activos

- Amenazas (identificación y valoración)
- Salvaguardias
- Impacto y riesgo residuales.
- Resultados del análisis de riesgos.

De acuerdo con la documentación y conociendo los objetivos de control y que planes son necesarios para lograrlos, se deben establecer acciones que permitan realizar el tratamiento de los riesgos encontrados y los tipos de salvaguardas a utilizar.

- Ejecución y seguimiento

Durante esta etapa se diseñan para la empresa políticas de seguridad las cuales deben ser divulgadas por medio del SIG a los empleados y mediante formatos a los terceros ya que incluyen los compromisos que deben adquirir durante su vinculación con la empresa y así mismo proponer controles físicos y lógicos que permitan mitigar y gestionar los riesgos que se puedan presentar para los procesos.

También se realiza el análisis de vulnerabilidades, que permite identificar falencias que se presenten durante la ejecución de los procesos.

- Mantenimiento y mejora

Finalmente se realiza la presentación general del SGSI de la empresa, y se propone la implementación de procesos de auditoria que permitan evaluar y medir el desempeño de las políticas y los objetivos de seguridad. Estos resultados deberán ser reportados a la gerencia para su revisión tanto para dar seguimiento y evaluación, como para realizar ajustes que sean requeridos en los procesos.

6.2. LÍNEA Y TIPO DE INVESTIGACIÓN

Este proyecto es de carácter descriptivo y analítico, dado que se realiza la observación de las características, los factores y procedimientos para así realizar el análisis e interpretación de la información sin manipular las variables estudiadas facilitando su comprensión.

6.3. INSTRUMENTOS DE RECOLECCION DE INFORMACIÓN

Para el desarrollo del presente trabajo de grado, se utilizarán los siguientes mecanismos e instrumentos para realizar la recolección de información:

- Cuestionario.
- Observación.
- Entrevistas con funcionarios especialmente el personal del proceso de T.I. de la empresa.
- Sistema de gestión calidad.
- Fuentes de información disponible física y digital como, tesis, libros, textos, revistas, normas, entre otros.

7. DESARROLLO DEL PROYECTO

7.1 ESTRUCTURA ORGANIZACIONAL

Super Servicios del Valle S.A. Nit. 900026727-3

Carrera 5 # 10-93, Cartago, Valle del Cauca. Colombia.

PBX: +57 (2) 210 7171

Correo: info@ganesuperservicios.co

Código de la actividad económica No. 9242 (Según Decreto 1607 del 31 de Julio de 2002 del Ministerio de Protección Social – Tabla de clasificación de actividades económicas)

Sector económico: Privado

SUPER SERVICIOS DEL VALLE S.A. es una empresa Norte Vallecaucana con más de 20 años de experiencia en el sector de juegos de suerte y azar. Cuenta con una amplia infraestructura, en la cual se tienen más de 400 puntos de venta fijos y móviles para brindar un servicio constante y confiable que permite satisfacer las necesidades y expectativas del cliente a través de un amplio portafolio de productos y servicios, estos son:

- Recargas móviles y de televisión.
- Venta de SOAT.
- Envío y pago de Giros nacionales.
- Recaudos empresariales.
- Chance tradicional, lotería virtual y física.

La excelente proyección comercial y crecimiento empresarial de Super Servicios del Valle S.A. ha permitido que tenga presencia en los municipios de Alcalá, Ansermanuevo, El Águila, Argelia, Bolívar, Caicedonia, Cartago, El Cairo, El Dovio, Obando, La Paila, Roldanillo, Sevilla, Toro, Ulloa, La Unión, Versalles, La Victoria, Zarzal, donde además de ofrecer productos y servicios, aporta al crecimiento de la sociedad y genera empleo a la comunidad.

7.2 MISIÓN

Super Servicios del Valle S.A, es una empresa operadora de juegos de suerte y azar, comercializadora de una amplia gama de servicios (recargas móviles y de televisión, SOAT, giros y recaudos empresariales), estamos comprometidos en satisfacer las necesidades de nuestros clientes, colaboradores y accionistas, contribuyendo con responsabilidad social al desarrollo de la comunidad.[36]

7.3 VISIÓN

Ser en el 2020 una organización empresarial líder a nivel regional en la comercialización de juegos de suerte y azar y servicios de valor agregado, por medio de una sólida plataforma tecnológica y un grupo humano orientado al servicio bajo principios éticos y morales, que genere confianza a sus clientes, rentabilidad a sus accionistas y aportes a la sociedad y al estado.

[36] Gane Super Servicios. (2018). Nosotros | Gane Super Servicios. [en línea] Disponible en: https://ganesuperservicios.co/nosotros/ [Consultado el 4 mayo 2018].

8. ALCANCE

8.1 ENTREGABLES

- Inventario de activos.
- Análisis de vulnerabilidades.
- Metodología de análisis y gestión de riesgos.
- Declaración de aplicabilidad.
- Política del Sistema de Gestión de Seguridad de la Información.
- Manual de seguridad de la información.

9. PLANIFICACIÓN DEL SGSI

9.1 METODOLOGÍA DE EVALUACIÓN DE RIESGOS

La metodología MAGERIT será utilizada para el análisis de riesgos de la empresa Super Servicios del Valle, para determinar qué medidas de control se deben establecer para dar tratamiento a las amenazas y vulnerabilidades identificadas para los activos inventariados de la empresa.

9.2 DESARROLLO DE LA METODOLOGÍA

Se desarrollará el siguiente paso a paso para establecer el SGSI de la empresa:

- Identificación y valoración de los activos
- Identificación y valoración de amenazas.
- Salvaguardas.
- Impacto y riesgo residuales.
- Capacitación y presentación de resultados.

9.3 IDENTIFICACIÓN Y VALORACIÓN DE ACTIVOS

En la tabla 16 se muestra el inventario de activos de la empresa Super Servicios del Valle S.A. el cual se realizó con la colaboración del personal de TI – Comunicaciones – Logística de quienes se recolectó la información necesaria.

Tabla 16. Identificación de activos

Tipo	Id	Cod	Nombre	Descripción
[D] Datos / Información	D01	[int]	Formato	Actualización de DB. Mantenimiento a DB.
	D02	[source]	Hera	Gestión Centralizada de Información
	D03	[source]	Inventory	Inventario.
	D04	[source]	Sitio WEB	Sitio web empresa. ganesuperservicios.co
	D05	[source]	Intranet	Portal Corporativo SSVSA.
	D06	[log]	Logs venta	Registro automático de actividades desarrollados por un usuario o aplicativo. Eventos de hardware, software operativo, software aplicativo y archivos respaldados.
	D07	[test]	Ambiente de desarrollo	Pruebas de software - parametrización de productos
[K] Claves Criptográficas	K01	[x509]	Certificado autofirmado Servidor intranet	Certificado de seguridad servidor intranet.
	K02	[info]-[encrypt]-[shared_secret]	Certificado SSL Sitio WEB	Certificado SSL sitio web empresa.
	K03	[com]-[authentication]	Claves de autenticación aplicativos administrativos	Credenciales de acceso para los aplicativos administrativos.
	K04	[disk]	Cifrado de soportes de información	Cifrado de discos duros externos, memorias usb.
	K05	[encrypt]	Claves de cifrado	Contraseñas de seguridad (keepass)

[S] Servicios	S01	[int]	Soporte Técnico	Asistencia técnica para personal administrativo de le empresa.
	S02	[www]	Sitio WEB	Administración de contenido del sitio web.
	S03	[email]	Creación - eliminación de cuentas de correo corporativas	Creación - eliminación y configuración de cuentas de correo electrónico para personal administrativo.
	S04	[ftp]	Transferencia de ficheros	Copia de respaldo de información de las estaciones de trabajo administrativas de tipo incremental subidas automáticamente al servidor NAS.
	S05	[idm]	gestión de identidades	Asignación de credenciales de acceso a los aplicativos administrativos.
	S06	[pki]	Infraestructura de clave pública	Certificado autofirmado servidor intranet
	S07	[ipm]	gestión de privilegios	Asignación de roles de usuario dependiendo de las funciones a cumplir dentro de la empresa.
[SW] Software	SW01	[prp]	Hera	Gestión Centralizada de Información
	SW04	[prp]	Inventory	Inventario de activos.
	SW13	[browser]	Mozilla Firefox 52.9.0ESR	Navegador predeterminado para el uso de aplicativos webs.
	SW16	[email_server]	Zimbra	Servidor de correo electrónico.
	SW17	[office]	2007-2010-2013-365	Sistema operativo licenciado para equipos administrativos.
	SW18	[office]	OFFICE para MAC 2011	Sistema operativo licenciado para equipos administrativos.

	SW19	[os]	S.O Windows	Sistema operativo licenciado para equipos administrativos.
	SW20	[os]	MAC OS X	Sistema operativo licenciado para equipos administrativos.
	SW21	[os]	Windows Server 2016	Controlador de dominio
	SW22	[av]	Forticlient 6.0.8.0261	Controles de seguridad, administración de aplicaciones, dispositivos y acceso a internet.
	SW23	[hypervisor]	VMWARE VSPHERE	Centralización y virtualización de servidores.
	SW24	[backup]	Cobian Backup 11	Automatización de backups de información de estaciones de trabajo de tipo incremental
[HW] Equipamiento Informático	HW01	[host]	Grandes equipos	Servidor de producción
	HW02	[mid]	equipos medios	Servidor de aplicaciones.
	HW03	[data]	informática personal	Servidor de intranet
	HW04	[pc]	informática personal	Equipo personal de T.I / Comunicaciones
	HW08	[vhost]	equipo virtual	máquinas virtualizadas
	HW09	[network] - [switch]	Switch	Switch
	HW10	[network] - [router]	Router	Router
	HW11	[network] - [firewall]	Cortafuegos	Fortinet
[COM] Redes de Comunicaciones	COM01	[radio]	Conectividad	Conectividad de los puntos de venta
	COM02	[wifi]		Red inalámbrica para visitantes
	COM03	[LAN]	Red LAN	Red LAN sede principal
	COM04	[Internet]	Conexión a internet	Conexión a internet para administrativos y puntos de venta
	MEDIA01	[electronic] -[disk]	Discos externos -	Información respaldada por cada líder de proceso

			líderes de proceso	
[Media] Soportes de Información	MEDIA02	[electronic]-[vdisk]	Máquinas virtualizadas	Virtualización de máquinas
	MEDIA03	[electronic]-[san]	Servidor NAS	Servidor de almacenamiento de ejecutables de aplicativos administrativos. Almacenamiento de carpetas por procesos compartidas en la red. Backup de respaldo de información de las estaciones de trabajo administrativas.
	MEDIA04	[non_electronic]-[printed]	Información impresa - archivo	Información impresa ingresos - traslado - retiro de colocadores. Evaluación de proveedores. Caracterización del proceso, protocolos y procedimientos.
[AUX] Equipamiento Auxiliar	AUX01	[power]	Energía eléctrica	Fuente de alimentación primaria para la conexión de equipos administrativos.
	AUX02	[gen]	Generador eléctrico sede principal	Planta eléctrica de respaldo.
	AUX03	[ac]	Ventilación cuarto inteligente	Aire acondicionado graduable para el cuarto inteligente.
	AUX04	[ups]	UPS de respaldo puntos de venta - oficinas principales de municipios - cuarto inteligente.	Sistema de alimentación eléctrica ininterrumpida de respaldo.
	AUX05	[destroy]	Cortadora de papel.	Cortadora de papel para la eliminación de documentos que pierden valor para la empresa pero que por su

				contenido deben ser destruidos.
[L] Instalaciones	L02	[local]	Cuarto inteligente	Cuarto de servidores, central telefónica.
	L03	[building]	Sede administrativa principal	Sede principal de la empresa.
	L04	[backup]	Sede contingencia	Sede de contingencia para proporcionar continuidad al negocio en Caso de algún evento catastrófico que impida la operabilidad de la sede principal
[P] Personal	P01	[adm]	Administradores de sistemas	Administración de aplicativos administrativos.
	P02	[dba]	Administradores de bases de datos	Administración y gestión de la base de datos
	P03	[des]	desarrolladores / programadores	Desarrolladores de sistemas de información a la medida
	P04	[com]	administradores de comunicaciones	Administrador de la red
	P05	[sec]	administradores de seguridad	Control de seguridad
	P06	[prov]	Proveedores.	Suministros de hardware y software para la empresa.

Fuente: el autor.

9.4 IDENTIFICACIÓN Y VALORACIÓN DE AMENAZAS

En el Anexo A, se encuentra la tabla 35 en la cual se relacionan las amenazas identificadas que pueden afectar los activos de información de la empresa Super Servicios del Valle S.A. el nivel de riesgo que presentan, su opción de tratamiento y su objetivo de control.

9.5 ANALISIS DE VULNERABILIDADES Y AMENAZAS PRESENTES

En la empresa Super Servicios del Valle S.A. se realizan pruebas básicas y diferentes validaciones

para identificar vulnerabilidades que se puedan presentar durante el desarrollo de las actividades de los funcionarios.

Se realizan verificaciones sobre el acceso físico:

- Visitas de terceros: Todo el personal externo es registrado al ingresar además se le entrega un carné de visitantes, el cual debe portar durante su estadía en la empresa en un lugar visible.
- Cuando el personal externo requiere ingresar equipo de cómputo a la empresa éste debe ser registrado en la recepción en la bitácora asignada a tal fin en la cual se indican datos generales como marca, serial, responsable y fecha de ingreso y egreso.
- La empresa cuenta con el servicio de CCTV continuo las 24 horas del día, los registros de grabación son verificados por muestreo diariamente.
- Para controlar y direccionar todo el personal que ingresa a la empresa, en la puerta principal siempre permanece un guarda de seguridad privada el cual verifica que los funcionarios ingresen portando su carné de identificación o si es personal externo lo dirige a las cajas o a la recepción.
- En la empresa se tiene el control de acceso controlado por biométrico a zonas restringidas como el área de tesorería, logística, cuarto inteligente y entrada principal.
- Todo el personal vinculado a la empresa cuenta con identificación basado en el uso del carné obligatorio y el acceso controlado por lector biométrico en la entrada principal para además gestionar su hora de ingreso y salida de la empresa.

Vinculaciones y tratamiento de información personal:

- El proceso de gestión humana realiza la contratación del personal administrativo, bajo un rigoroso proceso que incluye: entrevista, prueba de polígrafo, verificación de antecedentes y vinculación en listas de riesgos.
- La empresa cuenta con una política de protección de datos personales el responsable del tratamiento de la información y cada una de las finalidades con las que son recolectadas la información.
- La contratación de servicios con terceros es auditada por el proceso de gestión de riesgos, el cual verifica que en las carpetas de los proveedores con los que se tienen vínculos laborales reposa la información completa sobre el representante legal, la vinculación accionaria, reportes de listas de riesgos entre otros.

Acceso lógico:

La empresa cuenta con los siguientes mecanismos de control:

- Política de contraseña segura en la cual se establecen las condiciones que se debe cumplir al asignar una contraseña por los usuarios para el ingreso a los aplicativos corporativos además del tiempo de caducidad de cada una de ellas.
- El proceso TIC utiliza la gestión de usuarios y la asignación de privilegios a cada usuario según su rol en la empresa, para que tenga un acceso controlado a cada una de las aplicaciones corporativas asignadas.
- El proceso de comunicaciones realiza la asignación de ip a cada equipo de las estaciones de trabajo, únicamente con privilegios de acceso según la autorización de navegación de cada perfil.
- Todos los aplicativos corporativos cuentan con validación de datos requeridos para diligenciar registros de información.
- Se revisan los usuarios con privilegios de administrador en el directorio activo, los cuales solo corresponden al proceso de T.I

Pruebas en servidores:

- Despliegue de actualizaciones en ambientes demo.
- Verificación de periodos de caducidad de contraseñas de acceso.
- Uso de KeePass como administrador de contraseñas para usuarios de procesos críticos como contabilidad y T.I.

Para realizar el análisis de vulnerabilidades se realizaron las siguientes revisiones:

En la consola de administración del WSUS se realizó la revisión del estado de aprobación y de instalación de las actualizaciones del S.O para los equipos de la empresa, como se encontraron equipos con estado sin conexión se realiza la verificación en las estaciones de trabajo con este inconveniente y se encuentra que el firewall de Windows se encontraba activo; por lo que se realiza la desactivación y se verifica nuevamente la conexión en el WSUS.

Se implemento un control manual mensual para revisar que las copias de respaldo de las estaciones de trabajo y bases de datos se estén ejecutando y almacenando, por esto fue posible identificar que en algunas estaciones no se encontraron archivos de respaldo. Para mitigar este caso, se verificó en las estaciones de trabajo la configuración de la herramienta Cobian y si presentaba errores se reconfiguró. Además, en algunos casos se presentó que el usuario no estaba almacenando la información en la ruta predeterminada, por esto se le informó las consecuencias y el debido proceso que debería continuar realizando.

Se realizó la actualización del socket de venta en producción, el cual fallo en el momento de conexión de los usuarios de forma masiva presentando inconvenientes para la reconexión de los dispositivos. Esta vulnerabilidad no se presento en las pruebas demo que se realizan por lo que al momento de identificar la causa se devuelve la actualización y se escala al proveedor tecnológico CODESA.

Como requisito de la gerencia se configura el tiempo de protector de pantalla automático para que se dispare a los 5 minutos de encontrarse el equipo sin usar. Esta medida se toma porque es frecuente que los usuarios no bloquean la sesión al abandonar su sitio de trabajo.

Se presentó falla en el fluido eléctrico dejando en evidencia problemas en la planta de respaldo principal del edificio, la cual después de 40 minutos no realizó la conmutación por lo que se estuvo sin iluminación en las oficinas y se requirió dejar habilitados únicamente los equipos requeridos con prioridad.

En la tabla 17 se presentan las vulnerabilidades identificadas, las cuales son reportadas y corregidas para evitar posibles fallos de seguridad de la información.

Tabla 17. Reporte de vulnerabilidades y amenazas encontradas.

Activo	Vulnerabilidades	Amenazas
Estaciones de trabajo	Sistema operativo o software desactualizado.	Error en configuraciones básicas de los equipos.
	Interceptación de datos.	Phishing
	Desincronización de copias de seguridad respaldadas en el NAS.	Uso de dispositivos de almacenamiento externo.
	Hardware y software obsoleto.	
Gestión de la seguridad de la información en la empresa	Los funcionarios de la empresa tienen poco conocimiento y concienciación sobre temas de seguridad informática.	
	No existe participación activa para la definición e identificación de procedimientos de control. El	

	proceso no es manejado como una prioridad en la empresa.	
Directorio activo	Descarga de actualizaciones pendientes.	
	Tiempos de bloqueo de pantalla extensos.	
	Contingencia	
Operativa	Falla en la actualización del socket de venta que solo se pudo evidenciar durante la operación de venta de la empresa.	
Técnica	Falla en la plata eléctrica de respaldo del edificio.	

Fuente: el autor.

La empresa Super Servicios del Valle S.A. ha realizado la implementación de controles en pro de garantizar la seguridad de la información a través de mecanismos de control como:

- Buenas prácticas para el desarrollo seguro de aplicaciones, como ambientes de desarrollo y producción separados. Así mismo despliegue de actualizaciones en demo y verificación por lista de chequeo antes de lanzar la actualización en producción.
- Existen planes de contingencia para respaldar la operación en caso de fallas eléctricas e interrupciones del servicio de comunicaciones, estas últimas se realizan con acompañamiento del proveedor tecnológico Codesa ya que requiere el cambio de los puertos destino y origen además de la lógica de operación.
- En el SIG se publican las políticas creadas de control de acceso físico y lógico para que cada usuario las revise y así capacitar e informar al personal administrativo sobre sus responsabilidades y deberes para garantizar un entorno seguro para la información.
- El coordinador de comunicaciones como administrador del firewall es el responsable de garantizar que los puertos no requeridos para la operación estén deshabilitados.

En la tabla 18 se listan los cambios sugeridos para contrarrestar las vulnerabilidades encontradas. Las cuales son aplicadas de forma inmediata por el proceso de T.I.

Tabla 18. Recomendaciones para contener vulnerabilidades y o amenazas encontradas.

Equipo	Actividad sugerida
Estaciones de trabajo	Desactivación de firewall de Windows, para que los equipos se puedan conectar al directorio activo y puedan realizar la descarga de las actualizaciones del S.O.
	Se implementa un nuevo servidor NAS con la tecnología de alta disponibilidad activo-pasivo.
	Se solicita la compra de software actualizado para las estaciones de trabajo: Renovación de equipos, licencias de Microsoft Office. Está pendiente la actualización del aplicativo de venta ya que es la limitante para actualizar el navegador Mozilla a su última versión pues se requiere utilizar los plugins de JAVA.
	Se establecen cronogramas de capacitación del personal administrativo en temas de seguridad informática. Además, se implementan campañas informativas en la intranet y por correo electrónico para fomentar el buenos uso de las herramientas tecnológicas durante el desarrollo de las funciones del personal y se publican las políticas de seguridad establecidas en el sistema integrado de calidad.
Directorio Activo	Se revisan y actualizan las políticas de usuario para configurar el tiempo de bloqueo de pantallas para que se realice cada 5 minutos.
	Se incrementan los requisitos de complejidad de las contraseñas de inicio de sesión para las estaciones de trabajo y por ende de los aplicativos corporativos vinculados.
	Se asigna responsable para verificar la aprobación de las descargas de actualizaciones del WSUS.
Operativa	El proceso de gestión de riesgos indica que se debe realizar una evaluación de medidas alternativas para respaldar el fluido eléctrico en caso de que falle la planta del edificio. Además, el proceso de SST propone la instalación de luces de emergencia en sitios claves para evitar la oscuridad total en zonas de alto riesgo.

Fuente: el autor.

9.6 ELECCIÓN DE SALVAGUARDAS

Se plantean las salvaguardas de acuerdo con los diferentes niveles de defensa. Se debe tener en cuenta que toda acción de protección tiene un costo, por lo que debe ser evaluado el valor de la información que se desea proteger vs el costo que se generaría por la pérdida o ataque, para así planificar las acciones de control para información.

En la tabla 19 se pueden observar los mecanismos para salvaguardar los activos y el nivel de defensa actual y el deseado. En el nivel L0 se incluyen los procedimientos inexistentes hasta la fecha en la empresa. En los niveles L1 y L2 se incluyen aquellos procedimientos implementados pero que pueden ser mejorados. Para el Caso de las salvaguardas con nivel L3 y L4 representan aquellas que se

han implementado de forma correcta y que se pueden optimizar, mejorando la seguridad física y lógica de los activos de la empresa. El nivel objetivo es el L5 dependiendo del Caso, siempre con la mira de que los procedimientos de seguridad de la información sean los óptimos.

Tabla 19. Evaluación de salvaguardas.

Riesgo	Salvaguarda	Estado	
		Actual	Objetivo
Fuego, daño por agua, desastre natural.	Detectores de humo.	L1	L3
	Alarmas contra incendio	L4	L5
	Uso y mantenimiento de extintores.	L3	L4
	Plan de emergencia ante incendios.	L3	L4
	Brigada de emergencias.	L3	L4
	Simulacros periódicos.	L4	L5
	Información de respaldo en CLOUD.	L3	L4
Falla de generador eléctrico alterno	Mantenimiento quincenal de generador eléctrico alterno.	L2	L3
Falla en los equipos de climatización	Mantenimiento	L3	L4
	Adquisición de nuevos equipos	L2	L3
Avería de origen físico o lógico	Mantenimiento preventivo de servidores	L3	L4
	Revisión de política de generación y restauración de copias de seguridad.	L2	L3
	Monitoreo de recursos de los equipos.	L3	L4
Difusión de software dañino.	Instalación de antivirus	L4	L5
	Actualización de base de datos	L3	L4
	Programación de tareas	L3	L4
Acceso no autorizado	Controles de acceso físico.	L4	L5
	Firewall	L3	L4
	IDS	L0	L3
	Identificador único por usuario para acceder a las aplicaciones.	L4	L5
	Gestión de cuentas de usuario.	L4	L5

	Asignación y uso de privilegios de usuario.	L4	L5
Fuga de información	Acuerdo de confidencialidad y no divulgación de información, entre funcionarios, contratistas y usuarios.	L3	L4
Robo	Equipos ubicados o protegidos reduciendo el riesgo frente a amenazas o peligros del entorno, y las oportunidades de acceso no autorizado.	L3	L4
	Empresa de seguridad privada.	L3	L4
	Alarma.	L3	L4
	CCTV.	L3	L4
	Cable de seguridad para computadores y portátiles.	L0	L3
Errores de mantenimiento / actualización de programas (software)	Criterios de aceptación para: Sistemas de información nuevos. Actualizaciones y nuevas versiones.	L3	L4
	Ambiente de prueba para desarrollos y nuevas versiones	L3	L4
Errores de configuración	Pruebas periódicas del firewall	L0	L3
	Verificación periódica de los sistemas de información.	L2	L4

Fuente el autor.

9.7 POLÍTICAS DE SEGURIDAD

Las políticas de seguridad diseñadas para la empresa Super Servicios del Valle, detallan mecanismos de control y procedimientos internos que tienen como propósito evitar incidentes de seguridad generados tanto por aspectos técnicos como por errores o descuidos de los funcionarios de la empresa.

Las políticas de seguridad se han socializado a todo el personal de la empresa a través de diferentes medios como son, el sistema de gestión de calidad, intranet, correo corporativo y capacitaciones.

A continuación, se relaciona el contenido de las políticas de seguridad de la entidad:

9.7.1 POLITICA DE CONTROL DE ACCESO A LA INFORMACIÓN

El presente documento plantea la política y normas para garantizar un adecuado control, en el acceso a la información del personal administrativos y terceros tanto en las instalaciones físicas como a nivel lógico de la empresa Súper Servicios del Valle.

- Objetivo

Establecer medidas de control para proteger el acceso a la información de la empresa Súper Servicios del Valle, en lo relacionado a datos personales e información general, con el fin de evitar su divulgación, modificación, destrucción, pérdida o mal uso.

- Alcance

La política y normas definidas en este documento buscan establecer controles para restringir el acceso no autorizado a la información. Aplican para todos los funcionarios que durante el desarrollo de sus funciones en la empresa hacen uso y manipulan la información.

- Responsabilidades

Proceso Gestión humana:

Controlar el acceso a archivadores donde son almacenadas las bases de datos físicas con la información de hojas de vida de administrativos, aspirantes y colocadores independientes, y la base de datos digital con información biométrica del personal administrativo de la empresa.

Manejan la información personal en el Caso de los empleados de la empresa para el pago de aportes de EPS, ARL, fondos de pensiones y cesantías, cajas de compensación familiar, revisión y pago de nómina. Son los encargados de que cada

empleado reciba por correo corporativo su comprobante de pago de nómina minimizando el riesgo de que sus datos estén accesibles o se puedan visualizar por personas distintas a él.

Notificar a los diferentes procesos de la empresa el ingreso, traslado, retiro y novedades del personal administrativo para la asignación, modificación, bloqueo y eliminación de usuarios y roles en los diferentes sistemas y/o aplicativos autorizados.

Proceso Logística.

Debe evitar el acceso no autorizado a las bases de datos físicas y digitales con la información de proveedores y arrendadores, garantizando así la protección de la información de los titulares. Así mismo debe dar un buen uso a la información recolectada.

Proceso de T.I.

Evaluar los riesgos a los cuales se expone la información digital en la empresa con el objeto de determinar controles de acceso y mecanismos de autenticación para ser implementados en cada Caso. Realizar capacitaciones al personal que permitan fomentar una cultura de seguridad tanto en la organización como en sus procesos.

Verificar el cumplimiento de las políticas establecidas relacionadas con la creación de usuarios, administración de privilegios para el uso de aplicativos de acuerdo con el perfil de cada funcionario, administración de contraseñas, control y autenticación de usuarios.

El coordinador de TIC es la única persona autorizada para realizar la gestión y administración de la base de dato del aplicativo de ventas, cualquier cambio o anomalía detectada debe ser notificada a la gerencia para dar trámite o recibir autorización.

Proceso Comunicaciones:

Realizar el filtrado agregando la dirección MAC de cada equipo, garantizando así el acceso a los servicios corporativos única y exclusivamente a los dispositivos añadidos a la lista de direcciones

Segmentar las redes de datos y controlar los puertos de conexión a la red, habilitar los puertos de red seguros y deshabilitando puertos no requeridos. Configurar e instalar el software necesario de red que permita el control y monitoreo del tráfico diario de información.

Gestión Comercial:

El Asistente Comercial es la persona autorizada para acceder y controlar el uso de la base de datos con información de ganadores de promocionales. Debe notificar el ingreso, traslado y retiro de colocadores para la asignación, modificación, bloqueo y eliminación de usuarios y roles en los diferentes sistemas y/o aplicativos autorizados.

Proceso Gestión de Calidad.

El coordinador del sistema de gestión integrado es el responsable de garantizar la confidencialidad de la información, ya sea que se reciba de forma física o digital por parte de los usuarios o solicitantes de PQRS. Del mismo modo debe realizar la administración de la seguridad del sistema Binaps.

Proceso Tesorería y Contabilidad.

El director financiero debe garantizar el uso responsable y restringido de la base de datos de accionistas de la empresa y de cobradores de premios de la sede principal y los municipios del norte del valle en donde se tiene presencia.

Gestión Gerencial

Como proceso debe controlar la seguridad de la base de datos física y digital con la información personal de los accionistas, contratos de proveedores y los procesos judiciales de la empresa, labor que está bajo la responsabilidad de la Asistente de Gerencia.

Gestión de Riesgos

Dirigir y controlar la implementación de medidas de prevención y detección de situaciones que puedan generar riesgo en las actividades propias del objeto social de la empresa Súper Servicios del Valle como son el lavado de activos y la financiación del terrorismo, labor que realiza el Oficial de Cumplimiento.

Administrar la seguridad del sistema Compliance.

Protección de Datos

Garantizar el adecuado tratamiento de datos personales y/o sensibles de acuerdo con el marco legal vigente, con respecto a la información de carácter personal de empleados, accionistas, clientes y proveedores de la empresa Súper Servicios del Valle, labor que está bajo la responsabilidad de la Coordinadora de Protección de Datos.

- Cumplimiento

El cumplimiento de la política de control de acceso a la información es obligatorio. En Caso de presentarse alguna violación a la presente política dará lugar a un proceso disciplinario.

- Excepciones

Cualquier excepción en el cumplimiento de la política de control de acceso a la información debe ser autorizada por correo electrónico por la Gerencia. Todas las excepciones deben ser documentadas, registradas y revisadas para así garantizar la transparencia en el proceso.

Descripción de la política de control de acceso a la información.

- Control de acceso a la información física y digital

El acceso a las bases de datos físicas de los procesos de Gestión Humana, Logística, Comercial, Financiera, Calidad y Gestión Gerencial está autorizado únicamente al líder, coordinador y auxiliar de cada proceso. Estos funcionarios tienen la responsabilidad de velar por la confidencialidad, disponibilidad e integridad de la información almacenada.

Cada equipo de las estaciones de trabajo cuenta con 2 tipos de cuentas de usuario para ingresar. La cuenta de administrador es manejada por el proceso de T.I. quien

es el responsable de realizar cambios en la configuración de los equipos y hacer la instalación de aplicativos, la cuenta de usuario estándar no dispone de privilegios para realizar cambios o instalaciones en los equipos; la clave de acceso a esta cuenta de usuario la define cada empleado.

El uso de medios de almacenamiento removibles (CDs, DVDs, USBs, memorias flash, discos duros externos) para el procesamiento de la información de la empresa, estará autorizado para aquellos funcionarios cuyo perfil del cargo y funciones lo requiera. Estos medios de almacenamiento deben ser almacenados en lugares seguros y, se debe informar al proceso de T.I. y el Coordinador de Protección de Datos cualquier incidente de seguridad que se pueda presentar en el uso o pérdida de estos dispositivos.

Todas las aplicaciones utilizadas por el personal de Súper Servicios del Valle cuentan con requerimientos de seguridad (usuario y contraseña). Las contraseñas están implementadas con base en la Política de Contraseña Segura que establece los requerimientos necesarios para establecer las contraseñas.

La seguridad a nivel de contraseña en los sistemas de información utilizados en la empresa por los funcionarios administrativos se encuentra configurada así:

- Las contraseñas requieren mínimo 8 caracteres de longitud.
- El cambio de contraseña se solicita cada 30 días.
- La reutilización de las últimas 3 contraseñas se encuentra impedida.
- La clave del usuario se bloquea luego de 5 intentos utilizando una contraseña incorrecta. La habilitación deberá ser solicitada por correo electrónico dirigido a mesa de ayuda con copia al responsable del reinicio e incluyendo la cédula de ciudadanía del solicitante.
- Al iniciar sesión por primera vez se solicita el cambio de la contraseña.
- Se valida que las contraseñas incluyan al menos 3 de los siguientes grupos de caracteres:

Letras minúsculas (a … z).

Letras mayúsculas (A … Z).

Números (0 … 9).

Caracteres especiales, por ejemplo: #, $, %, &.

Cuando un colocador independiente de la empresa se va a ausentar o va a realizar un reemplazo o cuenta con un permiso, el administrador del Centro de Costo en el

Caso de los municipios o los supervisores de zona en el Caso de Cartago, deben informar al Proceso de Control Interno y al Coordinador de Giros para realizar el bloqueo en el acceso a los aplicativos de venta y de giros durante el tiempo que esté ausente.

Todos los funcionarios administrativos y colocadores independientes cuentan con un rol asignado que le permite el acceso al sistema y los diferentes aplicativos utilizados en la empresa para desarrollar sus funciones de acuerdo con su perfil. Todo cambio o activación debe ser solicitada por el líder de proceso.

El Coordinador de Protección de Datos Personales debe mantener un registro central de los derechos de acceso suministrados a cada rol de usuario para acceder a los aplicativos de la empresa que hacen tratamiento a los datos personales, los cuales deben ser revisados periódicamente con los administradores de los sistemas de información o servicios.

La información personal y sensible que se requiera por parte de la empresa SSVSA será tratada de acuerdo con las políticas de protección de acceso a bases de datos con información sensible y la política de consulta de bases de datos con información personal.

- Acuerdos de confidencialidad

Todos los empleados de Súper Servicios del Valle y terceros que tengan un contrato con la empresa deben aceptar la cláusula de confidencialidad definida por la empresa como parte del proceso de contratación, la cual refleja el compromiso de protección y buen uso de la información, de acuerdo con los criterios establecidos por ella.

- Seguridad física

Los procesos de Comunicaciones y T.I. deben solicitar por correo electrónico al Coordinador de auditoría la cancelación de la contraseña asignada al funcionario para acceder al cuarto inteligente en Caso de desvinculación o modificación de sus funciones, esta será redireccionada a la empresa de seguridad contratada. Adicionalmente, el Coordinador de Comunicaciones debe desenrolar a la persona que se retira de la empresa y solicitar la entrega de la tarjeta de proximidad asignada.

Todos los archivadores, armarios y demás elementos utilizados para el almacenamiento de información física por los funcionarios de la empresa, cuentan con mecanismos de seguridad que solo permiten el acceso a personal autorizado, siempre deben permanecer cerrados y bajo llave.

El personal externo que accede a las instalaciones de la empresa debe ser registrado en la recepción donde se le asignará el carné de visitante el cual debe portar en todo momento y de manera visible, con el fin de poder ser distinguido y controlar su acceso a las diferentes zonas no autorizadas.

La empresa Súper Servicios del Valle cuenta con personal de vigilancia permanente las 24 horas del día con turnos rotativos, y dispone de circuito cerrado de T.V. monitoreado periódicamente por muestreo por parte del proceso de Auditoría. Los registros de las grabaciones que requieran ser descargados deben tener autorización de gerencia.

El acceso a las áreas de Financiero y Tesorería, Logística, auxiliares de recaudo, caja principal y bóveda, se encuentran protegidos por un control biométrico que restringe y evita que personal no autorizado ingrese a esta zona. El ingreso a la oficina de Procesamiento de Datos es restringido, la puerta debe permanecer siempre con seguro.

Los funcionarios que requieran acceso a las instalaciones de la empresa un domingo o un festivo deben ser autorizados por el líder de cada proceso, el cual reporta por correo electrónico al Proceso de Control Interno para que las personas autorizadas sean incluidas en el listado de soporte que es entregado al guarda de seguridad, quien verifica al momento de ingreso que la persona esté autorizada para ingresar. En Caso de que no se haya diligenciado la autorización con anterioridad, el líder de proceso se debe comunicar con el Director de Control Interno quien dará la autorización al guarda de seguridad para que la persona pueda ingresar.

- Gestión de usuarios

Creación de Usuarios.

Los datos de acceso para los aplicativos utilizados por los empleados de la empresa están compuestos por un nombre de usuario y contraseña únicos para cada persona. Por ningún motivo deben ser compartidos ya que son de carácter confidencial e intransferible.

El proceso de Gestión Humana realiza el proceso de vinculación, licencia, vacaciones, suspensión, desvinculación o traslados de los funcionarios administrativos de la empresa y solicita la creación, modificación, bloqueo o eliminación de roles y usuarios al proceso de T.I.

El proceso de Gestión Comercial realiza el proceso de vinculación, desvinculación y cambio de roles de los colocadores independientes y solicita por medio de ticket a la mesa de ayuda con copia al auxiliar de T.I. la creación, retiro y traslado del rol utilizado por el usuario.

Todo requerimiento de creación, actualización, o eliminación de usuarios, debe ser efectuado a través de una solicitud por correo electrónico a la Mesa de Ayuda de la empresa por el líder del proceso del funcionario a quien se le hace el requerimiento.

- Equipos desatendidos en estaciones de trabajo

Cada empleado debe bloquear la sesión de usuario en el equipo de cómputo instalado en su estación de trabajo en el momento en que se retire del puesto, con el fin de evitar que otras personas puedan tener acceso a sus archivos o realicen cambios en la información o configuración del equipo al continuar con la sesión de usuario habilitada.

Para bloquear la sesión del equipo de cómputo, se deben presionar simultáneamente las teclas Windows – L, para ingresar nuevamente a la ventana de inicio de sesión se presiona la tecla Enter. Por ningún motivo se puede dejar el equipo de la estación de trabajo desbloqueado durante la ausencia del usuario.

Al finalizar la jornada laboral se deben apagar los equipos de cómputo de cada estación de trabajo, con el fin de proteger la seguridad, darle un buen uso de los recursos de la empresa, evitar pérdidas de información por cortes de energía y para garantizar aplicación de actualizaciones de sistema operativo que requieren reinicio.

- Uso del correo electrónico

El uso del correo electrónico facilita la comunicación entre los funcionarios de la empresa de forma interna y externa, el proceso de T.I. garantiza que este servicio cuente con la seguridad y la disponibilidad necesaria para la realización de las actividades que requieran su uso.

El proceso de T.I. es el encargado de administrar las cuentas de correo electrónico, así como de diseñar y socializar las normas para el uso de los servicios de correo electrónico entre los funcionarios de la empresa. De igual manera debe establecer los procedimientos y controles que permiten detectar y proteger la plataforma de correo electrónico contra código malicioso que pueda ser transmitido a través de los mensajes.

La cuenta de correo electrónico de cada funcionario de la empresa permanecerá activa durante el tiempo que dure su vinculación con la empresa, excepto en Casos de mal uso que eventualmente puedan causar la suspensión o cancelación de esta, en el Caso en que se produzca su desvinculación, la cuenta será dada de baja por el proceso de T.I.

La cuenta de correo electrónico asignada a cada funcionario de la empresa es de carácter individual, por lo que en ninguna circunstancia se debe utilizar una cuenta de correo que no sea la asignada para enviar o solicitar información de carácter corporativo.

El correo electrónico asignado por la empresa no debe ser utilizado por los funcionarios de la empresa para registrarlo en actividades personales. Cada que se realice el envío de información por este medio se debe adjuntar el pie de firma asignado y configurado por el auxiliar de T.I.

La opción de CCO (Copia Oculta) debe ser usada cuando se envíen mensajes a más de un destinatario externo o por envío de correos internos para la difusión masiva de información de interés para la empresa, así se evita que las direcciones de correo sean claras para desconocidos o spammers. Además, cuando se solicite notificación de recibido, dicha confirmación no debe ser enviada a todos los destinatarios iniciales, es decir, únicamente le llegará a quien lo solicito.

Los funcionarios de la empresa deben tener precaución al abrir archivos adjuntos de correo electrónico recibidos de remitentes desconocidos, estos pueden contener virus. Tampoco se deben abrir mensajes sospechosos, en Caso de recibir algún mensaje con características extrañas debe comunicarlo de forma inmediata y directa al proceso de T.I.

Se debe tener extremo cuidado con la información que es compartida por este medio, teniendo en cuenta el tipo de datos personales, sensibles o confidenciales que contenga, garantizando que solo sea recibida por personal autorizado para manejarla adecuadamente.

- Seguridad en las oficinas

Los escritorios de las estaciones de trabajo de cada empleado deben mantenerse limpios y sin documentos fuera del horario de trabajo o en ausencia prolongada del sitio, para evitar el acceso no autorizado a la información.

Las pantallas de los equipos en las estaciones de trabajo del personal administrativo se deben colocar en una posición en la que se evite que personal no autorizado pueda ver la información que se encuentre en ellas.

No se debe dejar abandonada en las impresoras información confidencial una vez se haya impreso.

Guarde bajo llave la información crítica o confidencial, preferentemente en una caja fuerte, gabinete o archivador, asegurándose de que la llave no quede en un lugar de fácil acceso por personal no autorizado.

No se deben dejar CD´s, memorias USB, discos externos, u otro elemento removible con información en lugares visibles y accesibles por personas no autorizadas, esto

incluye no dejar los diferentes dispositivos conectados en los puertos de los computadores cuando no sea necesario.

Cada empleado debe bloquear el equipo de cómputo instalado en su estación de trabajo en el momento en que se retire del puesto, así sea por poco tiempo, con el fin de evitar que otras personas puedan tener acceso a sus archivos o realicen cambios en la información o configuración del equipo al continuar con la sesión de usuario habilitada. Para bloquear la sesión del equipo de cómputo, se deben presionar simultáneamente las teclas Windows - L, para ingresar nuevamente a la ventana de inicio de sesión se presiona la tecla Enter.

Al finalizar la jornada laboral se deben apagar los equipos de cómputo de cada estación de trabajo, con el fin de darle seguridad a la información y un buen uso a los recursos de la empresa.

Sí utiliza un computador portátil dentro de la empresa, manténgalo en un lugar seguro para evitar hurtos o robos. Se recomienda el uso de guayas para proteger los portátiles cuando se encuentren desatendidos o sin la supervisión de alguien.

El usuario autorizado para usar un equipo de cómputo por fuera de la empresa debe tener el mismo nivel de protección de la información como si estuviese en las instalaciones de la empresa y aplicar la totalidad de recomendaciones.

Se debe tener sumo cuidado con la custodia de las colillas de chance que han sido previamente diligenciadas, es recomendable que estas permanezcan en un lugar que sea confidencial y al cual no pueda acceder cualquier persona que no esté autorizada para ello.

Registrar en la bitácora de la recepción el ingreso de equipos de carácter personal como portátiles, equipos fotográficos, de vídeo, audio o cualquier otro tipo de equipo que registre información, en Caso de ausencia de la persona encargada del área de Recepción esta labor será desempeñada por el vigilante de la puerta principal, indicando el número de serie del equipo a ingresar y la persona responsable de su uso. A la salida se debe verificar que el equipo corresponda con los datos inicialmente consignados en la bitácora.

- Seguridad de equipos por fuera de la empresa

El uso de equipos de cómputo portátiles destinados al procesamiento de información por fuera de las instalaciones de la empresa, debe ser autorizado por el responsable del proceso al que pertenezca el empleado. Además, debe registrar la salida en el formato de salida permanente. Si el equipo que sale está asignado a otra persona y se ha recibido en préstamo, se debe hacer el registro en el formato de salida general.

El uso de discos duros externos con información correspondiente a los procesos de la empresa por fuera de sus instalaciones debe ser autorizado por el líder de proceso mediante el formato de orden de salida general. Se debe verificar que el disco se encuentre cifrado y en Caso contrario solicitar este proceso a T.I.

El usuario autorizado para usar un equipo de cómputo por fuera de la empresa debe tener el mismo nivel de protección de la información como si estuviese en las instalaciones de la empresa, evitando así cualquier posible fuga de la información almacenada, o daño físico.

En el uso de dispositivos extraíbles como memorias o discos duros se debe adoptar todas las medidas que se encuentren al alcance del funcionario para asegurar que los archivos contenidos se encuentren libres de virus, malware o código malicioso, que puedan poner en riesgo su confidencialidad, integridad y disponibilidad o infección de los equipos informáticos de la empresa.

Con el fin de minimizar el riesgo de pérdida de información confidencial, durante el uso de los equipos portátiles en lugares diferentes a las instalaciones de la empresa, no se debe almacenar este tipo de información de forma permanente en el disco duro del equipo, en ese Caso se debe hacer uso de dispositivos de almacenamiento extraíble que permitan una mayor facilidad de custodia y resguardo en un lugar seguro por el funcionario.

- Estándares para desarrollo de aplicaciones

Los desarrollos de aplicaciones informáticas para la empresa Super Servicios del Valle S.A. en todos los Casos, deben incluir los siguientes controles de seguridad para la autenticación de los usuarios que garanticen el control de acceso a la información:

Soportar autenticación de usuarios individuales.

No almacenar contraseñas en texto plano.

Incluir mecanismos que permitan la asignación de roles por usuario.

Expirar las contraseñas y obligar a los usuarios a realizar el cambio.

Limitar el número de intentos de acceso sin éxito consecutivos.

Validar la utilización de diferentes grupos de caracteres. (a … z, A … Z, 0 … 9, símbolos entre otros.)

Cumplir con la Política de Contraseña Segura.

- Uso de dispositivos móviles

Súper Servicios del Valle proveerá las condiciones para el manejo de los dispositivos móviles asignados por la empresa. Así mismo, velará porque los funcionarios hagan uso responsable de los servicios y equipos proporcionados por la entidad.

En el Caso de equipos de telefonía celular, el usuario a quien se le asigna el equipo debe establecer un método de bloqueo automático de seguridad para la pantalla que impida el acceso a las aplicaciones o información almacenada a personas no autorizadas o familiares. Por ningún motivo se debe dar a conocer a otras personas las contraseñas o patrón de acceso configurados.

El proceso de T.I. debe configurar la opción de borrado remoto de información en los celulares entregados a los usuarios por la empresa, con el fin de eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica de forma remota, evitando así divulgación no autorizada de información en Caso de pérdida o hurto, o cualquier incumplimiento de la presente política.

Los usuarios deben evitar usar los dispositivos móviles entregados por la empresa en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar la pérdida o robo de estos. Así mismo evitar hacer uso de redes inalámbricas de uso público y desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles corporativos asignados cuando no se estén utilizando.

Los usuarios no deben modificar las configuraciones de seguridad de los dispositivos móviles corporativos bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega o realizar instalaciones de aplicaciones que no sean para uso corporativo como juegos entre otros. Cuando el dispositivo móvil notifique la disponibilidad de una actualización de aplicaciones o sistema operativo, el usuario debe aceptar y aplicar la nueva versión.

Los usuarios deben evitar la instalación de aplicaciones desde fuentes desconocidas; en el Caso de los celulares las aplicaciones se deben instalar únicamente desde las tiendas oficiales de los dispositivos móviles entregados por la empresa.

El dispositivo móvil corporativo nunca se debe dejar desatendido, aunque sea por un periodo corto de tiempo y sin importar el sitio donde se encuentre. Se debe evitar conectar el equipo en puertos USB de cualquier computador público y durante los viajes deben ser cargados como equipaje de mano.

Solo está permitido copiar información sensible o confidencial al dispositivo móvil o de almacenamiento extraíble cuando sea requerida para funciones propias dentro de su perfil en la empresa y el desarrollo de sus funciones. Sí la información que se muestra en la pantalla es de carácter sensible, se debe posicionar de tal manera de que la información no pueda ser vista por otros.

9.7.2 POLITICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

- Objetivo

Establecer los lineamientos generales para la gestión de incidentes de seguridad de la información para así prevenir y limitar su impacto.

- Alcance

La política de gestión de incidentes de seguridad de la información está dirigida a todo empleado de la empresa Súper Servicios del Valle que tenga acceso a información interna, confidencial o sensible durante el desarrollo de sus actividades dentro y fuera de la empresa.

- Responsabilidades

Todo funcionario debe informar cualquier incidente que observe que pueda afectar la seguridad de la información de la empresa.

La notificación de los incidentes deberá hacerse de forma inmediata, incluso durante días no hábiles, a los Coordinadores de Protección de Datos, de Comunicaciones, de TI y al oficial de Cumplimiento y Riesgos. Ellos deberán responder oportunamente ante notificaciones de incidentes y/o amenazas por parte de los funcionarios de la empresa, y verificando la implementación de mejoras que correspondan para prevenirlos.

Los coordinadores y el oficial deben guardar los registros de los incidentes reportados por los funcionarios de la empresa, para su seguimiento y control.

El conocimiento y la no notificación de una incidencia por parte de un usuario será considerado como una falta contra la seguridad de la información por parte de ese usuario y puede desencadenar un proceso disciplinario.

- Activos de información que deberán ser protegidos ante incidentes:
- Cuarto inteligente.
- Equipos de comunicación y servidores.
- Computadores asignados en las estaciones de trabajo.
- Discos duros externos, memorias USB y dispositivos móviles asignados por la empresa a los funcionarios.
- Aplicaciones, bases de datos, repositorios de software en general.
- Archivadores o sitios donde se almacenen documentos físicos

En la tabla 20 se relaciona la clasificación de los incidentes de seguridad identificados y agrupados de acuerdo con sus características para la empresa SSVSA, además se especifica su probabilidad de ocurrencia y el nivel de impacto que pueden generar en los activos.

Tabla 20. Clasificación de incidentes de seguridad.

Código	Amenazas naturales o ambientales	Probabilidad	Impacto
ISI01	Apagón o corto circuito por tormenta eléctrica.	Baja	Medio
ISI02	Inundación (por daño en tubería o fenómeno natural).	Baja	Alto
ISI03	Incendio accidental o provocado.	Baja	Alto

ISI04	Bio-deterioro (bacterias, hongos, insectos y roedores) en los archivadores o bodegas utilizados para almacenar las bases de datos manuales de la empresa.	Baja	Alto
ISI05	Oxidación de clips, ganchos de cosedora, legajadores de los documentos almacenados en las bases de datos físicas de la empresa o de documentos guardados en las estaciones de trabajo.	Baja	Alto
ISI06	Rotura de cajas o documentos de forma malintencionada de información física de bases de datos o estaciones de trabajo.	Baja	Alto
ISI07	Temblor o terremoto	Baja	Alto

Código	Amenazas humanas o accidentales	Probabilidad	Impacto
ISI08	Robo o pérdida accidental de hardware (computador, disco duro externo, memoria USB, celular corporativo) dentro y fuera de las instalaciones de la empresa.	Media	Alto
ISI09	Robo, alteración o pérdida accidental de información dentro y fuera de las instalaciones de la empresa,	Media	Alto
ISI10	Destrucción no autorizada de información.	Media	Alto
ISI11	Uso no autorizado de la información en formato físico o digital.	Bajo	Alto
ISI12	Fraude por personal interno o externo de la compañía.	Bajo	Alto
ISI13	Ingreso de personal no autorizado al cuarto inteligente, estaciones de trabajo de funcionarios o en la zona en donde se encuentran los archivadores que almacenan las bases de datos manuales.	Bajo	Alto
ISI14	Modificación o eliminación no autorizada de datos.	Bajo	Alto
ISI15	Amenaza o acoso por correo electrónico o uso indebido del mismo.	Bajo	Medio
ISI16	Incumplimiento de políticas de seguridad de la información.	Media	Alto
ISI17	Tratamiento no autorizado de datos personales (Ley 1581 del 2012).	Bajo	Alto

Código	Amenazas técnicas	Probabilidad	Impacto
ISI18	Malware o virus informáticos.	Media	Alto

ISI19	Daño de un equipo de cómputo, de comunicaciones, servidor, o almacenamiento externo	Bajo	Alto
ISI20	Mal funcionamiento de los controles de acceso como biométricos o alarmas que alteren la protección de la información.	Bajo	Alto
ISI21	Cambio de contraseñas de acceso a la sesión de usuario en los aplicativos de la empresa	Bajo	Alto
ISI22	Sistemas operativos y software desactualizado	Media	Alto
ISI23	Respaldos de la información no realizados	Baja	Alto

Fuente: El autor.

- Reporte de incidentes, amenazas y debilidades de seguridad

El primer medio formal para el reporte de incidentes es el envío de correo electrónico a las cuentas de los responsables de gestionarlos colocando en el asunto del correo “Incidente de seguridad de información”. Se debe especificar el incidente o amenaza detectada y a qué proceso, recurso tecnológico o físico puede estar afectando.

En Caso de que el incidente requiera una intervención urgente se debe contactar a los responsables personalmente o vía telefónica, sin necesidad de enviar un correo electrónico.

- Respuesta ante incidentes, amenazas y debilidades de seguridad

Después de ser informado el incidente a los responsables, se debe diligenciar el formato de registro de incidentes con el funcionario que lo reporta y clasificar el hecho de la siguiente forma:

El evento no corresponde a una amenaza: el proceso se da por terminado, informando a la persona que lo reportó.

El evento es una amenaza: se deben gestionar las actividades para solucionar el incidente a la persona afectada.

Una vez definido el incidente, los responsables deben atender la solicitud de la siguiente forma:

- Coordinador de T.I.:

Fallas en aplicativos.

Virus en los equipos.

Accesos no autorizados a las bases de datos.

Acceso no autorizado a los equipos de las estaciones de trabajo.

Pérdida de información almacenada en los equipos de las estaciones de trabajo.

Cambios de contraseña no autorizada o informada en aplicativos o equipos.

Pérdida de equipos móviles y dispositivos de almacenamiento externo asignados a los funcionarios de la empresa.

- Coordinador de Comunicaciones

Violación de políticas de acceso a la red.

Ataques o tentativas de acceso no autorizado a la red corporativa, interna o externamente.

Coordinador de Logística.

Incidentes eléctricos, inundaciones, incendios o eventos de bio-deterioro.

Robo o pérdida de hardware.

- Coordinador de auditoria y Coordinador de Comunicaciones

Fallas en el sistema de seguridad física.

Coordinador de Protección de datos.

Relacionado con pérdida o robo de información personal y/o sensible.

Cada proceso responsable de dar solución a un incidente debe clasificar el nivel de atención que se requiere de la siguiente forma:

Crítico: No admite demora en ser solucionado. En Caso de que se presenten varios incidentes de este nivel, deben ser solucionados en paralelo.

Alto: El incidente requiere ser atendido antes que otros, aunque se haya detectado posteriormente.

Medio: Los incidentes son atendidos por orden de llegada, un incidente de este tipo puede pasar a nivel alto si no es solucionado en un tiempo prolongado.

Detectadas las causas del problema y los elementos afectados, el proceso responsable debe dar a conocer la solución, el tiempo de respuesta y los recursos necesarios dependiendo del grado de complejidad y magnitud del problema.

Sí después de un incidente de seguridad se debe iniciar una acción en contra de una persona u organización que implique medidas legales, se deberán recopilar y proteger las pruebas evitando su destrucción (videos, registros de acceso no autorizado o testigos de ataques) para poder ser presentadas ante los organismos correspondientes.

La Gerencia o en su caso a quien delegue, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas.

Sí el incidente de seguridad que se presenta está relacionado con pérdida o robo de información personal y/o sensible el Coordinador de Protección de Datos debe informar por escrito al (los) titular (es) de la información solicitando tomar las precauciones para enfrentar el uso ilegal de su identidad.

- Registro y Control

Se debe mantener un registro actualizado de incidentes y a su vez de las lecciones aprendidas como resultado de las acciones o medidas que se implementen para solucionarlos, ya sea de forma total o parcial.

El formato diseñado para el reporte de registro de incidentes de seguridad se encuentra disponible y habilitado para descargar para todos los funcionarios de la empresa en el sistema de gestión de la calidad, en cualquier Caso, se puede apoyar en el coordinador del SIG para según el Caso se habilité en el perfil del usuario.

Los responsables asignados según el Caso reportado deberán realizar la revisión de los reportes realizados, al menos una vez al año y garantizar que se ha dado seguimiento y solución a todos los incidentes reportados. Adicionalmente trimestralmente se deberá generar un reporte de incidentes, con objeto de identificar categorías de incidentes más reportados y luego tomar las medidas que correspondan para prevenirlos.

Es importante que después de identificarse cualquier incidente, en un proceso de mejora continua se evalúe la eficacia de los tratamientos dados, qué incidentes son recurrentes o han sido de alto impacto, y finalmente la necesidad de implementar nuevos controles para limitar la frecuencia del daño o problemas subyacentes.

Cuando los incidentes de seguridad han sido atendidos, solucionados y cerrados, se debe crear una base de conocimiento sobre cómo fueron manejados, que permita a la empresa enfrentar un evento similar con mayor rapidez y a su vez implementar un modelo de mejora continua para gestión de incidentes de seguridad de la información.

Los procedimientos disciplinarios aplicables a infracciones o violaciones de políticas de seguridad de la información y de la protección de datos personales, sensibles e información confidencial se establecerán de acuerdo con el Reglamento Interno de Trabajo, contemplado en el capítulo XV.

9.7.3 POLITICA DE CONTRASEÑA SEGURA

- Objetivos

Indicar a los funcionarios, colocadores independientes y/o terceros los parámetros mínimos que deben utilizar para crear contraseñas de seguridad fuertes.

Determinar que los accesos a la red, los aplicativos corporativos y los sistemas de información deben requerir un usuario y una contraseña fuerte para la autenticación y acceso a la información de forma segura.

- Alcance

Todos los funcionarios de la empresa, colocadores independientes y terceros.

- Responsabilidades

- Proceso de T.I.

Aplicar las configuraciones de seguridad en los aplicativos corporativos utilizados por el personal administrativo de la empresa, para que realice las validaciones correspondientes y verifique que el usuario cumpla con los requerimientos planteados.

- Proceso de Protección de Datos

Realizar revisiones periódicas a los aplicativos corporativos y a la gestión de usuarios y contraseñas, que permitan verificar el cumplimiento de las normas establecidas en la presente política.

- Gestión Gerencial

Gestionar recursos y/o espacios para la sensibilización del recurso humano en cuanto a la implementación de técnicas y aplicación de las normas de seguridad en la empresa.

- Funcionarios administrativos

Asistir a capacitaciones programadas y dar cumplimiento de las normas establecidas en la presente política.

- Excepciones

Cualquier excepción en el cumplimiento de la política de control de acceso a la información debe ser autorizada por la Gerencia. Todas las excepciones deben ser documentadas, registradas y revisadas para garantizar que el requerimiento si amerita crear una excepción en el cumplimiento de la política.

- Descripción de la política

La asignación de contraseñas no se debe comunicar a los funcionarios por medio de llamada telefónica, la única herramienta permitida para este proceso será el envío por correo electrónico de un archivo que contenga dichos datos.

Cada usuario deberá cambiar la contraseña inicial que se le asigne, en el primer acceso que realice al sistema o tras el desbloqueo de su contraseña cuando haya sido necesaria la intervención de los administradores de la seguridad de los aplicativos.

Los funcionarios de la empresa deben establecer contraseñas de seguridad para los equipos o los aplicativos que utilicen teniendo en cuenta las siguientes instrucciones: longitud mínima de 8 caracteres, debe contener al menos 3 de los siguientes 4 grupos o categorías de caracteres disponibles: letras minúsculas

(a…z), letras mayúsculas (A…Z), números (0...9) y caracteres especiales como, por ejemplo: #, $, %, &. En la contraseña estos caracteres no se deben repetir de forma contigua.

El tiempo de vida útil para las contraseñas utilizadas para acceder a los aplicativos corporativos es de 30 días, al finalizar este plazo el aplicativo solicitará el cambio dejando en desuso las 3 últimas contraseñas ya registradas. Para los aplicativos que no soliciten cambio de contraseña, esta se deberá cambiar máximo cada mes.

Los aplicativos corporativos están configurados para que el límite de intentos fallidos al ingresar una contraseña sea de 5 intentos, luego esta se bloqueará y se deberá solicitar el desbloqueo de la contraseña y reinicio para poder acceder.

Los responsables para los reinicios de las contraseñas son:

- Proceso de T.I:

Bnet.

Mesa de ayuda.

Portal corporativo.

Spark.

Módulo de reportes en Jasper.

Desarrollos internos. (Papyro, simcracia, inventory, recaudo giros, Qualisk, Hera).

- Proceso de Gestión de Riesgos:

Compliance.

- Proceso de Calidad:

Binaps.

- Proceso Giros:

Aplicativo SIMS.

El proceso de T.I. configura desde el dominio la instrucción para que el sistema operativo bloquee la sesión del usuario después de 15 minutos de inactividad, hasta que el usuario solicite el desbloqueo.

Si se requiere obtener información de un equipo de escritorio o portátil de un funcionario que se encuentre ausente de forma temporal o definitiva, la solicitud debe ser enviada únicamente por el líder del proceso a T.I. a través de la mesa de ayuda.

Las contraseñas que se encuentren almacenadas en archivos en los equipos, o cuando sean transmitidas a través de redes, deben estar siempre protegidas por mecanismos como asignación de claves a los archivos o cifrado de información para evitar que sean visualizadas por otros usuarios.

- Uso de Contraseñas

Cada empleado de Súper Servicios del Valle debe cumplir las siguientes normas:

La contraseña es personal e intransferible y se debe mantener en secreto, cualquier evento o incidente que suceda por el préstamo de la contraseña será responsabilidad de la persona dueña de la contraseña. Se debe evitar escribirlas en papel o almacenarlas en medios digitales no encriptados.

Se recomienda que las contraseñas sean fáciles de recordar, pero no fácil de adivinar, se debe evitar que estén basadas en algún dato que otra persona pueda obtener fácilmente mediante información relacionada de la persona, por ejemplo, nombres, fecha de nacimiento, o teléfonos.

Cada usuario debe hacer uso de diferentes contraseñas para cada aplicativo al que tenga acceso, para así impedir la intrusión a múltiples recursos con información. Evitar utilizar secuencias de teclado como, por ejemplo: “qwerty”, “asdf” o de numeración como: “1234” ó “98765” o palabras que puedan estar incluidas en diccionarios (cualquier idioma) con el propósito de evitar la ruptura de claves mediante un ataque por diccionario.

Cuando la contraseña es olvidada por el usuario o esta es bloqueada después de 5 intentos errados, debe solicitar por medio de ticket a mesa de ayuda su reinicio y no puede ser solicitada por otra persona.

La opción de autoguardado de contraseñas en los diferentes navegadores web y aplicativos utilizados por cada empleado de la empresa no debe ser activada por los usuarios.

Se debe notificar al proceso de T.I cualquier incidente o sospecha de cualquier acto que viole la seguridad relacionado con sus contraseñas, ya sea: pérdida, robo o indicio de pérdida de confidencialidad. Se recomienda no compartir las contraseñas entre compañeros, mucho menos divulgarlas en conversaciones directas o telefónicas o mensajes de correo electrónico.

El uso de usuarios y contraseñas individuales permite determinar responsabilidades en el uso de los aplicativos y estaciones de trabajo por parte de los empleados de Súper Servicios del Valle.

9.7.4. PLAN DE CONTINGENCIA INFORMÁTICO

Para Super Servicios Del Valle S.A. es indispensable recurrir a los recursos de cómputo como un medio de proveer información a todos los niveles de la organización, y es de vital importancia que dicha información sea lo más exacta posible.

Es importante resaltar que para que la organización logre sus objetivos necesita garantizar tiempos de indisponibilidad mínimos, tanto en sus recursos informáticos como en las comunicaciones; de este modo debe contar con una contingencia eficiente en todas las áreas operativas.

Por todo lo anteriormente dicho, el estar sin el servicio del punto de venta por un lapso mayor de 3 horas origina distorsiones al funcionamiento normal de nuestros servicios y mayores costos de operación. De continuar esta situación por un mayor tiempo nos exponemos al riesgo de paralizar las operaciones por falta de información para el control y toma de decisiones de la Institución. Por tanto, es necesario prever cómo actuar y qué recursos necesitamos ante una situación de contingencia con el objeto de que su impacto en las actividades sea lo menor posible.

Cabe señalar que Super Servicios Del Valle S.A. ingresa en una situación de contingencia cuando en cualquiera de sus 19 centros de costos el punto de venta

sale de servicio por más de 1 horas y termina cuando se restablece el ambiente de trabajo original y el procesamiento normal de sus actividades.

- Introducción

El presente documento es el Plan de Contingencia Informático de Super Servicios Del Valle S.A en materia de Riesgos de Tecnología de Información y Comunicaciones (TIC).

Establece el objetivo, alcance y metodología desarrollada. Incluye, además las definiciones utilizadas, las políticas de seguridad, el análisis de la situación, el análisis de sensibilidad de la información manejada, la identificación de los riesgos y controles, y la clasificación de activos de TI.

La metodología práctica comprende: la identificación de riesgos, calificación de la probabilidad de que ocurra un riesgo, evaluación del impacto en los procesos críticos, la creación de estrategias de contingencias y la planeación de oportunidades de mejora.

Permitirá mantener la contingencia operativa frente a eventos críticos de la organización y minimizar el impacto negativo sobre la misma, los usuarios y clientes, deben ser parte integral para evitar interrupciones, estar preparado para fallas potenciales y guiar hacia una solución.

- Definiciones

Contingencia: Interrupción, no planificada, de la disponibilidad de recursos Informáticos.

Plan de contingencia: Conjunto de medidas (de detección y de reacción) a poner en marcha ante la presencia de una contingencia en la empresa Super Servicios del Valle S.A.

Emergencia

Restauración (backup).

Recuperación.

En la tabla 21 se muestra la clasificación de los estados en los que se puede llegar a encontrar la empresa y en los cuales se deberá realizar la activación del plan de Contingencia.

Tabla 21. Plan de contingencia informático.

	Emergencia	Restauración	Recuperación
Objetivo	Limitar el daño	Continuar Procesos Vitales	Recuperar proceso total
Actuación	Inmediata	A corto plazo	A medio plazo
Contenido	Valoración de daños Arranque de acciones	Alternativas para los procesos vitales	Estrategias para la recuperación de todos los recursos
Responsabilidad principal	Comunicaciones / TI	Comunicaciones / TI	Comunicaciones / TI

Fuente: Coordinador comunicaciones SSVSA.

- Elementos esenciales de los planes

Planes aprobados por la Gerencia elaborados con el apoyo de los todos los procesos, para la eventual reasignación de las prioridades que debe haber sido pactada con anterioridad por las tres partes implicadas (Gerencia, Comunicaciones-TI y Usuarios).

- Recursos

Diferentes equipos de hardware, software e infraestructura tecnológica, además copias de respaldo actualizadas que permitan reestablecer el funcionamiento de los servicios y los aplicativos corporativos para que el personal pueda retornar rápida y eficazmente al desempeño de sus funciones.

- Pruebas

Validez de las copias de seguridad, que garantice que la información que se encuentra respaldada es actual, y conserva sus propiedades de integridad y confiabilidad. Formación y verificación del buen estado de los diferentes dispositivos.

- Seguros

Aseguramiento de los equipos informáticos, que garantice alta disponibilidad como contingencia de elementos de hardware, software o infraestructura tecnológica ya sea para reemplazo inmediato o como abastecimiento para backup para un futuro evento.

- Objetivos

Definir las actividades de planeamiento, preparación, entrenamiento y ejecución de tareas destinadas a proteger la información contra los daños y perjuicios producidos por corte de servicios, fenómenos naturales o humanos.

Establecer un plan de contingencia, formación de equipos y entrenamiento para restablecer la operatividad del sistema en el menor tiempo posible.

Establecer actividades que permitan evaluar los resultados y retroalimentación del plan general.

- Organización

Para el desarrollo e implementación, se ha diseñado la siguiente estructura, definiendo las responsabilidades por cada una de las áreas de la organización participantes.

Líder de plan: gerente.

Administrador del plan: coordinador de comunicaciones / coordinador de T.I.

Equipo de trabajo: técnico en sistemas, personal de logística, departamento

comercial.

- Definiciones

Proceso crítico: Proceso considerado indispensable para la continuidad de las operaciones y servicios de la organización, y cuya falta o ejecución deficiente puede tener un impacto negativo para la organización y por ende para la ciudadanía.

Impacto: El impacto de una actividad crítica se encuentra clasificado, dependiendo de la importancia de los servicios que afecta dentro de los procesos TI y comunicaciones, en:

Impacto Alto: se considera que una actividad crítica tiene impacto alto sobre las operaciones de SUPER SERVICIOS DEL VALLE S.A cuando ante una eventualidad en ésta se encuentran imposibilitadas para realizar sus funciones normalmente.

Impacto Medio: se considera que una actividad crítica tiene un impacto medio cuando la falla de esta ocasiona una interrupción en las operaciones de SUPER SERVICIOS DEL VALLE S.A por un tiempo mínimo de tolerancia.

Impacto Bajo: se considera que una actividad crítica tiene un impacto bajo, cuando la falla de ésta no tiene un impacto en la continuidad de las operaciones.

- Plan de Contingencia:

Son procedimientos que definen cómo una organización continuará o recuperará sus funciones críticas en Caso de una interrupción no planeada de los servicios, ya sea por un evento causado por errores del personal de la empresa o fenómenos naturales.

Los sistemas de T.I. son vulnerables a diversas interrupciones.

Leves: Caídas de energía de corta duración, fallas en disco duro, daño en impresora, etc.

Severa: Destrucción de equipos, incendios, daño en equipo de comunicación, etc.

Asegura que se dé una interrupción mínima a los procesos de atención al usuario en Caso de una interrupción significativa de los servicios que normalmente soportan esos procesos.

- Análisis y evaluación de riesgos

Los desastres causados por un evento natural o humano pueden ocurrir, en cualquier parte, hora y actividad. Existen diferentes tipos de contingencias que se pueden presentar y que pueden afectar la normal prestación de los servicios que ofrece la empresa, como, por ejemplo:

Riesgos Naturales: tales como mal tiempo, terremotos, erupción volcánica, etc.

Riesgos Tecnológicos: tales como incendios eléctricos, fallas de energía, daño en componentes y accidentes de transmisión, transporte, ataque de virus, etc.

Riesgos Sociales: como actos terroristas y desordenes.

Las causas de fallas más representativas que originarían cada uno de los escenarios propuestos en el plan de contingencia y seguridad de la información se presentan en la tabla 22.

Tabla 22. Escenarios de riesgos en la empresa SSVSA.

Escenario	Casos
Falla en el punto de venta PC	Falla en la CPU. Falla en el monitor. Falla en la impresora. Falla en la UPS. Falla en Mouse. Falla en Teclado. Falla en lector biométrico. Falla en Lector de barras. Falla en Radio de comunicación.
Falla en el punto de venta Móvil	Falla en terminal Móvil
Falla en el servidor	Falla en hardware Falla en Software
Ausencia parcial o permanente del personal de TI	Accidente. Renuncia intempestiva.
Perdida de servicios de red	Falla de switch. Falla en router Falla en Radio de Comunicación. Falla en cable de red.

Fallos prolongados en el servicio eléctrico.	Falla en el servicio energético.
Indisponibilidad del centro de servidores	Falla ups Falla planta eléctrica. Incendio Terremoto Sabotaje Cortocircuito Inundación.
Falla servicio de comunicación	Falla de Internet Falla de canales MPLS

Fuente: Coordinador de comunicaciones SSVSA.

9.7.5. PLAN DE CONTINGENCIA INFORMATICO PARA CENTROS DE COSTOS
Se debe activar en los municipios de Águila, Alcalá, Anserma, Argelia, Bolívar, Caicedonia, Cairo, Cartago, Dovio, Obando, paila, Roldanillo, Sevilla, toro, Ulloa, Unión, Versalles, victoria, zarzal.

Diseño de estrategia de contingencia de los procesos y servicios que brinda super servicios del valle S.A. contemplando que la asistencia inicial la debe realizar la auxiliar del centro de costos, teniendo en cuenta que son el primer contacto con la colocadora independiente.

Los equipos de soporte con los que cuentan como mínimo los centros de costos son:

1 CPU (torre)
1 monitor LCD
1 mouse USB o PS2
1 teclado USB o PS2
1 impresora TMU-220 PD
1 cable de impresora USB a Paralelo
1 cable de red
1 fuente de poder para computador

- Procedimiento para el reemplazo de algunos equipos de soporte:

Cuando se presenta una falla en el hardware en cualquiera de los puntos de venta de los centros de costos, inicialmente se debe solicitar soporte técnico ya sea a la mesa de ayuda por chat corporativo, celular o al funcionario de soporte encargado para ese día.

Luego de recibir el soporte, y se determine que debe reemplazar algún componente, la auxiliar de la oficina, debe desplazarse al punto de venta con fallas y llevarle la parte de reemplazo. Luego de este procedimiento se debe generar el ticket de servicio en la mesa de ayuda para que sea enviada la parte afectada y queden nuevamente completo los equipos de soporte.

Como cambiar alguna parte afectada:

Llevar la parte afectada al punto de venta.
Apagar el equipo correctamente.
Desconectar la parte afectada.
Conectar el equipo de respaldo.
Encender nuevamente y probar su funcionamiento.

A continuación, en la tabla 23 se describe cada uno de los posibles Casos que se pueden presentar en los puntos de venta sistematizados de los centros de costos asociados a la empresa y que generan afectación al proceso comercial:

Tabla 23. Falla en el punto de venta P.C

Impacto Punto de venta (PC)	Procesos afectados	Recurso	Prioridad de Recuperación
No se pueden prestar los servicios de Super Servicios Del Valle S.A**.**	Proceso Comercial	Partes del computador.	ALTA
		Partes de la estación de trabajo.	ALTA
		Software Sistema Operativo y aplicación	ALTA

Fuente: Coordinador de comunicaciones.

- Recurso de Contingencia:

CPU, Disco duro, memoria RAM, teclado, monitor, UPS, mouse, impresora, cable USB a Paralelo, lector biométrico, lector de barras, radio de comunicación, planta eléctrica, tarjetas de red, patch cord.

- Escenario 1. Falla en el punto de venta de PC:

Caso 1: El computador no enciende por fallas en la fuente.

En este Caso se debe llamar a la auxiliar del centro de costo para que apoye en los siguientes pasos:

- Verificar que la UPS este encendida.
- Verificar que la CPU tenga conectado el cable de poder.
- Revisar que el botón de encendido de la fuente de poder este en encendido.
- Ensayar que encienda de un botón de encendido diferente al tradicional.
- Encender la torre nuevamente.
- Si la falla continua, instalar la torre de soporte.

Caso 2: El computador no inicia (prende, pero no da imagen)

En este Caso se debe llamar a la auxiliar del centro de costo para que apoye en los siguientes pasos:

- Apague la CPU para prevenir choques eléctricos.
- Destape la torre, por un lado.
- Retire el banco de memoria RAM y colóquelo en el banco disponible.
- Encienda la torre nuevamente.
- Si la falla continua, debe instalar la torre de soporte.

Caso 3: El computador inicia, pero se queda pegado en unas letras blancas que dicen Ctrl + D.

- Solicite soporte técnico al funcionario de soporte encargado para ese día.
- Ingrese la contraseña de restauración que le indiquen.
- Cuando aparezca la línea de comandos, teclee lo siguiente en minúscula:
- fsck – y, espere que realice los 5 pasos, cuando termine reinicie el computador

para que inicie con normalidad.
- Si la falla continua, debe instalar la torre de soporte.

Caso 4: El monitor no enciende.

- Verifique que se encuentre conectado a la energía eléctrica.
- Revise que encienda del botón correspondiente.
- Si la falla continua, debe instalar el monitor de soporte.

Caso 5: El monitor enciende, pero no muestra imagen o sale un mensaje de fuera de línea moviéndose por la pantalla.

- Verifique que se encuentre conectado a la CPU.
- Revise que la CPU este iniciando normalmente de lo contrario remítase al caso 2.
- Si la falla continua, debe instalar el monitor de soporte.

Caso 6: La impresora no imprime (1).

- Revise que se encuentre conectado a la energía y al adaptador.
- Verifique que este encendida.
- Verifique que la tapa está cerrada correctamente.
- Si el botón de “error” se encuentra encendido o parpadeando debe reemplazar la impresora.
- Si la falla continua, debe instalar la impresora de soporte.

Caso 7: La impresora no imprime (2), se le da la orden de imprimir, pero no lo hace

- Verifique que la impresora este encendida.
- Revise que se encuentre conectada a la CPU, mediante el cable USB a Paralelo.

Caso 8: La UPS no enciende o está pitando repetidamente.

- Verifique que se encuentre conectada a la toma de la pared.
- Revise los breakers del local pueden estar disparados o en posición apagado.
- Si la falla continua, debe instalar la UPS de soporte.

Caso 9: La UPS no funciona cuando hay un corte de energía.

- La UPS tiene una falla, debe instalar la UPS de soporte.

Caso 10: El Teclado no funciona.

- Revise que el teclado se encuentre conectado correctamente a la CPU.
- Verifique que el bloque numérico este encendido.
- Reinicie el PC para eliminar el bloqueo.
- Si la falla continua, debe instalar el teclado de soporte.

Caso 11: El mouse no funciona.

- Verifique que esté conectado a la CPU.
- Revise la superficie donde lo están operando.
- Reinicie el PC para eliminar el bloqueo.
- Si la falla continua, debe instalar el mouse de soporte.

Caso 12: El Lector Biométrico no funciona.

- Verifique que esté conectado a la CPU.
- Revise que el lector este enrolado correctamente con SuperGIROS.
- Reinicie el PC para eliminar el bloqueo.

Caso 13: El Lector de Barras no funciona.

- Verifique que esté conectado a la CPU.
- Verifique el estado del código que va a leer, que sea soportado por el lector.
- Reinicie el PC para eliminar el bloqueo.

Caso 14: El radio de comunicación no funciona.

- Revise que la unidad indoor este encendida.
- Verifique que esté conectado a la CPU.
- Reinicie el PC para eliminar el bloqueo de la tarjeta de red

Si la falla continua o se requirió cambiar una parte (impresora – mouse – disco duro - ups), por favor comunicarse con la mesa de ayuda, y reportar el incidente para que el componente sea verificado por el área de comunicaciones o reemplazado.

- Escenario 2: Falla en el punto de venta Móvil.

A continuación, en la tabla 24 se describe cada uno de los posibles Casos que se pueden presentar en los puntos de venta móvil de los centros de costos asociados a la empresa y que generan afectación al proceso comercial:

Tabla 24. Fallas en el punto de venta Móvil.

Impacto Punto de venta (PC)	Procesos afectados	Recurso	Prioridad de Recuperación
No se pueden prestar los servicios de Super Servicios Del Valle S.A.	Departamento Comercial	Partes de Maquinas.	ALTA
		Software Sistema Operativo y aplicación	ALTA

Fuente: Coordinador de comunicaciones SSVSA.

Caso 1: La terminal móvil no enciende.

- Revise que la terminal este correctamente cargada y con la pila puesta.
- Intente encenderla sin la batería puesta, solamente conectada al cargador.

Caso 2: La terminal móvil enciende, pero no conecta**.**

- Se debe revisar que la tarjeta SIM se encuentre correctamente instalada.
- Reiniciar la terminal, para descartar problemas de conexión con el operador o fallas de cobertura.
- Si la falla continua, debe instalar la terminal de soporte.

Caso 3: La terminal móvil muestra diferentes errores al momento de ingreso

- Cuando realizamos el proceso de ingreso la terminal puede mostrar diferentes mensajes de error, cuando estos aparecen debe comunicarse con la mesa de ayuda, y reportar el incidente:

E0: No tiene código de Punto de venta

E3: No tiene papelería asignada.

E5: No tiene horario asignado.

- Si la falla continua, debe instalar la terminal de soporte.

Caso 4: La terminal móvil presenta daño en alguno de sus componentes (tapa, Impresora, Batería, etc.).

Instalar la terminal de soporte.

Si la falla continua o se requirió cambiar un componente de la terminal móvil (tapa – impresora – batería), por favor comunicarse con la mesa de ayuda, y reportar el incidente para que el componente sea verificado por el área de comunicaciones o reemplazado.

- Escenario 3: Falla en el Servidor.

A continuación, en la tabla 25 se describen los casos que se pueden presentar durante una falla en el servidor y que generaría afectación en todos los procesos de la empresa:

Tabla 25. Fallas en el servidor.

Impacto Punto de venta (PC)	Procesos afectados	Recurso	Prioridad de Recuperación
No se pueden prestar los servicios de Super Servicios Del Valle S.A.	Todas las Áreas	Partes de Servidor.	ALTA
		Software Sistema Operativo y	ALTA

aplicación

Fuente: Coordinador de comunicaciones SSVSA.

Caso 1: Fallas de Hardware

- Identificar el servidor que presenta la falla.
- Identificar la parte que está afectando el funcionamiento del servidor.
- Solicitar la parte al área de logística ya sea fuente de poder, disco duro.
- Apague el servidor si se requiere.
- Luego que la parte sea entregada debe ser instalada en el servidor que está presentando falla para restablecer el servicio.
- Si la falla es mayor (board, procesador) debe solicitarse soporte técnico al fabricante para que reemplace la parte dañada (si el contrato de Garantía está vigente).
- Encienda el Servidor.
- Verifique que funcione correctamente.

Caso 2: Fallas de Software

El DBA analiza la falla presentada a nivel de la base de datos o el sistema operativo.

El DBA Soluciona la falla presentada si está en sus conocimientos.

Si la falla no se soluciona con los conocimientos del DBA, se procede a generar un ticket de servicio a la empresa CODESA (soporte@codesa.com.co), donde se indica el incidente y se asigna un consultor.

Cuando la falla sea solucionada, se envía una difusión por medio de la herramienta SPARK indicando el reingreso al aplicativo.

- Escenario 4: Ausencia parcial o permanente del personal de TI o Comunicaciones.

A continuación, en la tabla 26 se describen los casos que se pueden presentar durante la ausencia parcial o permanente del personal de T.I. o comunicaciones y que generaría afectación en todos los procesos de la empresa:

Tabla 26. Ausencia parcial o permanente del personal de T.I. o Comunicaciones.

Impacto Punto de venta (PC)	Procesos afectados	Recurso	Prioridad de Recuperación
No se puede brindar soporte técnico a Super Servicios Del Valle S.A.	Todos	Personal de soporte de las áreas	MEDIA
		Personal de la mesa de ayuda	MEDIA

Fuente: Coordinador de comunicaciones SSVSA.

Caso 1: Accidente:

- Verificar que soporte estaba realizando en el momento del accidente.
- Cubrir el soporte y dejar funcionando correctamente la estación solicitante.
- Durante la incapacidad del compañero los demás compañeros de área realizaran sus actividades.

Caso 2: Renuncia intempestiva.

- Procedemos a cubrir el soporte y dejar funcionando correctamente la estación solicitante.
- Durante la incapacidad del compañero los demás compañeros de área realizaran sus actividades
- Realizamos la solicitud por escrito al Proceso de Gestión Humana, mediante el formato de requisición de personal donde indicamos el perfil de la persona que necesitamos para cubrir la vacante que queda después de la renuncia.
- Realizamos entrevistas a las personas que envían su hoja de vida y cumplen con el perfil solicitado.
- Una vez seleccionado e ingresado al sistema, procedemos a la capacitación necesaria para que cumpla totalmente con sus labores.

- Escenario 5: Perdida de servicios de red

A continuación, en la tabla 27 se describen los casos que se pueden presentar durante la ausencia parcial o permanente del personal de T.I. o comunicaciones y que generaría afectación en todos los procesos de la empresa:

Tabla 27. Pérdida de servicios| de red.

Impacto Punto de venta (PC)	Procesos afectados	Recurso	Prioridad de Recuperación
No se pueden prestar los servicios de Super Servicios Del Valle S.A.	Todos.	Hardware de respaldo	ALTA
		Actualizaciones y copias de seguridad de la configuración.	ALTA

Fuente: Coordinador de comunicaciones SSVSA.

Caso 1: Falla de Switch / Router:

- Verificar el estado del equipo, si es falla del equipo en general o solamente es un puerto:

Falla total del equipo:

Solicitar al área de logística el dispositivo.

Realizar el cambio del equipo que presenta fallas, si es necesario actualizar los parámetros de configuración mediante el software propietario y habilitar el servicio.

Hacer pruebas de conectividad mediante Ping hacia un Host Vecino.

Notificar a los afectados que ya pueden continuar con sus funciones normales.

Falla en un puerto especifico:

Al identificar el puerto que presenta fallas, validar los que tenemos disponibles en el mismo equipo y cambiarlo normalmente, teniendo en cuenta los parámetros de seguridad.

Hacer pruebas de conectividad mediante Ping hacia un Host Vecino.

Notificar a los afectados que ya pueden continuar con sus funciones normales.

Revisar que el equipo esté conectado adecuadamente a la energía y que este encendido.

Caso 2. Falla en Radio de Comunicación:

- Verificar si la falla fue alámbrica o inalámbrica.
- Solicitar el equipo a Logística para su configuración.
- Una vez tengamos el equipo lo configuramos con el software propietario y los parámetros correspondientes al punto de venta que presenta la falla (esta información la podemos obtener del archivo WLAN 15.xlsx.
- Reemplazamos el equipo dañado.
- Realizar pruebas de conectividad.
- Notificar al usuario que ya puede continuar trabajando.

Caso 3. Falla en cable de red:

Verificar el estado del cableado, si esta malo o deficiente se debe cambiar completamente.

Si alguno de los terminales presenta deterioro en sus componentes, se debe reponchar con un terminal RJ-45 Nuevo.

Si el patch cord presenta deterioro se debe cambiar.

Realizar pruebas de conectividad.

Notificar al usuario que ya puede continuar trabajando.

- Escenario 6: Fallos prolongados en el servicio eléctrico.

A continuación, en la tabla 28 se describen los casos que se pueden presentar durante una falla en el servicio eléctrico y que generaría afectación en todos los procesos de la empresa:

Tabla 28. Fallas en el servicio eléctrico.

Impacto Punto de venta (PC)	Procesos afectados	Recurso	Prioridad de Recuperación
No se pueden prestar los servicios de Super Servicios Del Valle S.A.	Todos.	Hardware de respaldo	MEDIA

Fuente: Coordinador de comunicaciones SSVSA.

Caso 1: Falla en el servicio energético de la cuidad.

Consultar con la empresa de energía si la falla es prolongada o solo es pasajera.

Si la falla es prolongada se debe consultar al Proceso comercial a cuáles puntos de venta se les instalara una de las 5 plantas generadoras de emergencia con las que cuenta la empresa (Cartago).

Si la falla es en municipios, se debe llevar la planta de soporte al punto de venta que presenta el corte energético.

- Escenario 7: Indisponibilidad del centro de datos.

A continuación, en la tabla 29 se describen los casos que se pueden presentar si se presenta indisponibilidad del centro de datos ubicado en la oficina principal y que generaría afectación en todos los procesos de la empresa:

Tabla 29. Indisponibilidad del centro de datos.

Impacto punto de venta (pc)	Afectada	Recurso	Prioridad de recuperación
No se pueden prestar los servicios de SSVSA	Todas las Áreas.	Hardware de respaldo	ALTA

Fuente: Coordinador de comunicaciones SSVSA.

Caso 1: Falla en la UPS.

- Aunque el centro de servidores cuenta con sistema redundante de UPS, contamos con una tercera UPS de marca POWERCOM de 4,5 kVA, para realizar el cambio en caso de que llegue a fallar alguna de las UPS´s de cuarto de servidores.
- Desconecte de la energía eléctrica la UPS que presenta falla.
- Conecte de la clavija que alimenta los circuitos regulados y conecte a la energía la UPS de respaldo.
- Encienda la UPS.

- Verifique el funcionamiento.
- Llame al servicio técnico para que repare la UPS dañada.
- Reinstale la UPS reparada cuando sea devuelta.

Caso 2: Falla en la planta eléctrica.

- El edificio cuenta con dos plantas que se respaldan automáticamente en Caso de que falle la planta principal.
- En Caso de que no encienda automáticamente, se debe encender con el botón de encendido manual.
- Si definitivamente no encienden, deben iniciar con el proceso de apagado de los servidores para prevenir daños en la información.

Caso 3: Incendio

- Activar el sistema de evacuación de la empresa para salvaguardar vidas.
- Informar a los bomberos.
- Emplear los extintores ubicados en cada área.
- Salva guardar la información.
- Hacer un inventario posterior de los daños.
- Solicitar a logística las partes afectadas.
- Cuando se halla solucionado los inconvenientes reanudar las actividades.
- En caso de que se presente terremoto, actos de sabotaje o inundación se debe iniciar con el BCP diseñado para Super Servicios Del Valle S.A

Caso 4: Cortocircuito

- Verificar el sitio que está generando la falla.
- Retirar de la conexión el dispositivo causante.
- Llamar al contratista encargado de la electricidad.
- Reemplazar el equipo con conexión dañada.
- Restablecer los Breakers disparados durante el cortocircuito.
- Verificar su funcionamiento.
- Iniciar actividades normales.

- Escenario 8: Falla en el servicio de comunicación.

A continuación, en la tabla 30 se describen los casos que se pueden presentar si se presenta fallas en el servicio de comunicaciones y que generaría afectación en

todos los procesos de la empresa:

Tabla 30. Fallas en el servicio de comunicaciones.

Impacto Punto de venta (PC)	Afectada	Recurso	Prioridad de Recuperación
No se pueden prestar algunos de los servicios de Super Servicios Del Valle S.A.	Todas las Áreas.	Hardware de respaldo	MEDIA

Fuente: Coordinador de comunicaciones SSVSA.

Caso 1 Falla de Internet

- Automáticamente se habilita el segundo canal de internet UNE.
- Verificar su funcionamiento, si falla se debe habilitar el canal 3G de Movistar.
- Reportar al operador que presenta la falla para que valide y genere la reparación respectiva.
- Cuando se haya restablecido el servicio el router automáticamente habilita el servicio.

Caso 2 Falla en el Canal MPLS:

- Verificar mediante ping la conectividad del enlace con CODESA.
- Apagar el router MPLS por 2 minutos, los prendemos y verificamos nuevamente el funcionamiento
- Reportar el incidente al operador Movistar, los cuales solucionan durante las próximas 8 horas.
- Verificar que funcione correctamente.

10. PROPONENTES O PERSONA QUE PARTICIPA EN EL PROYECTO

10.1. PROPONENTES PRIMARIOS

En la tabla 31 se presenta la información del estudiante responsable del proyecto y aspirante al título

Tabla 31. Datos del responsable del proyecto.

Datos del responsable del proyecto				
Nombre del estudiante: Claudia Marcela Narváez Vélez				
Identificado con	C.C. x	C.E	Otro	Número: 1094892429
Programa Académico	Especialización en Seguridad informática		Correo Electrónico	cmnarvaezv@hotmail.com
No. de Créditos Aprobados del plan de estudios:	12		Promedio Acumulado:	4.8
Dirección residencia: Carrera 10 No. 20-24				Municipio / Departamento Cartago / Valle
Teléfono / Celular 3006656087			Zona Occidente	CEAD Dosquebradas

Fuente: El Autor.

10.2. PROPONENTES SECUNDARIOS

- Empresa Super Servicios del Valle.
- Director del proyecto

Martín Camilo Cancelado**.**

Ingeniero de sistemas con énfasis en telecomunicaciones de la UCC de Bucaramanga.

Especialista en seguridad informática de la Universidad Pontificia Bolivariana de Bucaramanga.

11. RECURSOS DISPONIBLES

11.1. RECURSOS MATERIALES

Los recursos físicos y digitales utilizados para el desarrollo del proyecto de grado son relacionados en la tabla 32.

Tabla 32. Recursos físicos y digitales.

Recurso	Descripción	Presupuesto
Equipos y Software	Computador personal Samsung Intel® Core ™ i5-3337u, RAM 8G, DD 400G, S.O Windows. Suite Office 365 Pro Plus. Herramientas para análisis de riesgos.	$900.000 Servicios para estudiantes UNAD.
Total		$900.000

Fuente: El autor.

11.2. RECURSOS INSTITUCIONALES

Se relacionan en la tabla 33 los recursos financieros requeridos para desarrollar el proyecto.

Tabla 33. Recursos financieros.

Recurso	Descripción	Presupuesto
Viajes y Salidas de Campo	Desplazamientos a la oficina. Tutorías.	$100.000
Materiales y suministros	Conexión a Internet. Resma de papel.	$70.000 mensuales $35.000
TOTAL		$205.000

Fuente: El autor.

12. RESULTADOS O PRODUCTOS ESPERADOS

Los resultados que se esperan durante el desarrollo del SGSI para la empresa Super Servicios del Valle S.A. permitirán mediante la identificación de sus activos, implementar controles y políticas de seguridad que mejoren los niveles de seguridad en la empresa y sensibilicen los funcionarios en temas de seguridad de la información. En la tabla 34 se muestra cómo se relaciona el resultado esperado con el usuario final.

Tabla 34. Resultados o productos esperados.

Resultado/producto esperado	Indicador	Beneficiarios
Diagnóstico inicial	Determinar el nivel de la empresa con respecto a la seguridad de la información.	Usuarios internos.
Inventario de activos	Cubrimiento del SGSI a los activos de información de la empresa.	Usuarios internos.
Análisis de vulnerabilidades	Identificar que amenazas se puedan estar presentado en la empresa, para activar controles de acuerdo con su nivel de riesgo.	Usuarios internos. Clientes. Proveedores.
Identificación y valoración de riesgos	Nivel de seguridad en las aplicaciones de la empresa.	Usuarios internos. Clientes. Proveedores. Arrendatarios.
Políticas y controles de seguridad	Nivel de implementación de controles (controles implementados / controles planeados a implementar)	Usuarios internos. Clientes. Proveedores.

		Arrendatarios.
Plan de sensibilización	Sensibilidad de los funcionarios frente al SGSI (capacitaciones ejecutadas/capacitaciones programadas)	Usuarios internos. Clientes. Proveedores. Arrendatarios.
Auditorias	Nivel de compromiso de la alta gerencia. Gestión de incidentes de seguridad (incidentes reportados / incidentes gestionados) Verificación periódica de las políticas y controles de seguridad planteadas.	Usuarios internos.

Fuente: el autor.

CONCLUSIONES

Para el diseño del SGSI de la empresa Super Servicios del Valle S.A se hizo uso de herramientas de observación directa, aplicación de encuestas, entre otros para poder realizar el análisis necesario y la recolección de información para tener una mayor claridad y definir e iniciar el desarrollo de cada una de las fases del SGSI. Posteriormente utilizando la metodología MAGERIT se realiza el análisis de riesgos, el cual se inició realizando el levantamiento del inventario de activos de acuerdo con la clasificación sugerida, se asignó su valoración cualitativa, se identificaron las posibles amenazas a los que la organización se vería expuesta, el uso de salvaguardas, y la documentación detallada de los riesgos encontrados.

Se realiza con la colaboración del personal administrativo la revisión e identificación de posibles vulnerabilidades en los procesos que se realizan a diario en la empresa, lo que permitió encontrar fallas de seguridad no registradas para las cuales se dio prioridad y se solucionaron por el personal del proceso de T.I. y fueron incluidas en las políticas de seguridad para continuar con su vigilancia y como mejora continua del SGSI implementado.

Seguidamente, se establecen y se publican en el SIG las políticas de seguridad y se aplican los controles de seguridad propuestos para disminuir los riesgos identificados. Además, se convoca el personal administrativo para participar en campañas de sensibilización para promover la seguridad de la información entre todos los funcionarios y terceros relacionados con la empresa. De esta forma se generará sentido de pertenencia y concientización de los riesgos que pueden afectar la seguridad de la información y las consecuencias incluso legales que se pueden desencadenar a partir de un ataque para la empresa.

Finalmente, en conjunto con la alta gerencia se realiza la asignación de responsables quienes participan tanto como para reportar cualquier posible incidente como para dar solución final y tratamiento, y a su vez liderar el proceso de mejora continua del SGSI.

BIBLIOGRAFIA

Administración electrónica. (2018). PAe - MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [en línea] Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WvPMV4gvwdU [Consultada el 9 mayo 2018].

Alcaldía Bogotá. Consulta de la Norma: Ley 1581 de 2012. (2018). {En línea}. {13 febrero de 2018}. Disponible en: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981)

Congreso de la república. “Ley 1273 de 2009”. {En línea}. {14 de marzo de 2018}. Disponible en: Ministerio de Tecnologías de la Información y las Comunicaciones: http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf.

Córdoba, Alba. Diseño e implementación de un SGSI para el área de informática de la curaduría urbana segunda de Pasto bajo la norma ISO/IEC 27001. Pasto. 2015. UNAD. Facultad de ciencias básicas e ingeniería.

El ciclo de Deming. La gestión y mejora de procesos. {en línea}. {17 febrero de 2018}. Disponible en: (http://equipo.altran.es/el-ciclo-de-deming-la-gestion-y-mejora-de-procesos/).

ESET Security Report Latinoamérica 2017. {en línea}. {13 febrero de 2018}. Disponible en: (https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf).

Gane Super Servicios. (2018). Nosotros | Gane Super Servicios. [en línea] Disponible en: https://ganesuperservicios.co/nosotros/ [Consultado el 4 mayo 2018].

GTC–ISO/IEC 27002. {en línea}. {13 febrero de 2018}. Disponible en: (https://tienda.icontec.org/wp-content/uploads/pdfs/GTC-ISO-IEC27002.pdf).

Guía para la implementación de seguridad de la información en una MIPYME. {en línea}. {23 febrero de 2018}. Disponible en: (https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf).

ICONTEC. (02 febrero de 2018). NTC-ISO-IEC 27001. Recuperado el 03 de diciembre de 2019 de https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-ISO-IEC27001.pdf

ICONTEC. (02 febrero de 2018). NTC 1486. Recuperado el 3 de diciembre de 2019 de http://www.unipamplona.edu.co/unipamplona/portalIG/home_15/recursos/01_general/09062014/n_icontec.pdf

ISO 27000. (2018). ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información. (2018) {En línea}. {25 febrero 2018}. Disponible en: http://www.iso27000.es/iso27002.html

ISO27001: La seguridad de la información en la Gestión de la continuidad del negocio. {en línea}. {03 marzo de 2018}. Disponible en: (http://www.pmg-ssi.com/2014/11/iso-27001-la-seguridad-de-la-informacion-en-la-gestion-de-la-continuidad-de-negocio/)

La seguridad como rehén. Tendencias 2017. {en línea}. {08 febrero de 2018}. Disponible en: (https://www.welivesecurity.com/wp-content/uploads/2016/12/Tendencias-2017-eset.pdf).

MAGERIT – versión 3.0. Libro I. Método. Recuperado el 06 febrero de 2018 de https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html).

MAGERIT – versión 3.0. Libro II. Catálogo de elementos. Recuperado el 13 febrero de 2018 de https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html

MAGERIT – versión 3.0. Libro III. Guía de Técnicas. {en línea}. {13 febrero de 2018}. Disponible en (https://www.ccn-cert.cni.es/documentos-publicos/1793-magerit-libro-iii-tecnicas/file.html).

Mintic. Ley 1273 de 2009 - Ministerio de Tecnologías de la Información y las Comunicaciones. (2018). {En línea}. {12 febrero 2018}. Disponible en: http://www.mintic.gov.co/portal/604/w3-article-3705.html

NTC-5722. Continuidad del negocio. {en línea}. {07 marzo de 2018}. Disponible en: (https://tienda.icontec.org/wp-content/uploads/pdfs/NTC5722.pdf).

Sistema de Gestión de Seguridad de la Información. {en línea}. {15 febrero de 2018}. Disponible en: (http://www.iso27000.es/download/doc_sgsi_all.pdf).

Reality Vs. Delusion: A Guide to a Modern Threat Landscape. {en línea}. {09 marzo de 2018}. Disponible en: (https://media.kaspersky.com/en/business-security/reality-vs-delusion-guide-to-modern-threat-landscape.pdf).

ANEXOS

Anexo A. Identificación y valoración de amenazas.

Tabla 35. Identificación y valoración de amenazas.

ID Riesgo	Activo	Riesgo	Nivel del riesgo	Responsable	Opción de tratamiento			Control	
					Evitar	Reducir	Transferir		
RSI-01	Datos [D]	Degradación de los soportes de almacenamiento de información.	Muy grave	Coordinador T.I.		x		A.9.2.6	Se deben verificar todos los elementos del equipo que contengan medios de almacenamiento para asegurar que se haya eliminado cualquier software licenciado y datos sensibles o asegurar que se hayan sobrescrito de forma segura, antes de la eliminación.
		Errores de los usuarios.	Muy grave			x		A12.4.3	Las actividades del administrador y del operador del sistema se deben

							registrar, y los registros se deben proteger y revisar con regularidad.
RSI-02		Escape, alteración y destrucción de información.	Muy grave	Auxiliar de T.I.	x	A.11.3.2	Los usuarios deben asegurarse de que a los equipos desatendidos se les da protección apropiada.
RSI-03	Servicios [S]	Avería de tipo lógico o físico. Agotamiento de recursos.	Muy grave	Coordina-dor T.I.	x	A.10.3.1	Se debe hacer seguimiento y adaptación del uso de los recursos, así como proyecciones de los requisitos de la capacidad futura para asegurar el desempeño requerido del sistema.
RSI-04		Error de monitorización al proceso de copia de respaldo automático.	Muy grave	Auxiliar de T.I.	x	A.10.5.1	Se deben hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada.
RSI-05	Software [SW]	Avería lógica o física en el proceso de generación de backups	Muy grave	Auxiliar de T.I.	x	A.10.5.1	Se deben hacer copias de respaldo de la información y

		de seguridad de las estaciones de trabajo.						del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada.
RSI-06		Errores en actualizaciones de S.O.	Muy grave	Auxiliar de T.I.	x		A.10.3.2	Se deben establecer criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones y llevar a cabo los ensayos adecuados del sistema durante el desarrollo y antes de la aceptación.
RSI-07		Denegación del servicio de los sistemas de información de la empresa.	Muy grave	Coordinador T.I.	x		A.10.10.2	Se deben establecer procedimientos para el monitoreo del uso de los servicios de procesamiento de información, y los resultados de las actividades de monitoreo se deben revisar con regularidad
RSI-08		Vulnerabilidades de los programas.	Muy grave	Auxiliar de T.I.	x		A.10.10.5	Las fallas se deben registrar y

						analizar, y se deben tomar las acciones adecuadas.
RSI-09	Errores del administrador.	Muy grave	Coordinador T.I.	x	A.10.10.4	Se deben registrar las actividades tanto del operador como del administrador del sistema.
RSI-10	Difusión de software dañino.	Muy grave	Auxiliar de T.I.	x	A.10.4.1	Se deben implementar controles de detección, prevención y recuperación para proteger contra códigos maliciosos, así como procedimientos apropiados de concientización de los usuarios.
RSI-11	Fugas de información.	Muy grave	Coordinador T.I.	x	A.11.2.4	La dirección debe establecer un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios.
RSI-12	Abuso de privilegios de acceso.	Muy grave	Coordinador T.I.	x	A.11.2.2	Se debe restringir y controlar la asignación y uso de privilegios.
RSI-13	Uso no previsto.	Muy grave	Coordinador T.I.	x	A.11.2.1	Debe existir un procedimiento formal para

							el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información.
RSI-14		Errores de configuración.	Muy grave	Coordinador T.I.	x	A.15.2.2	Los sistemas de información se deben verificar periódicamente para determinar el cumplimiento con las normas de implementación de la seguridad.
RSI-15		Errores de mantenimiento / actualización de programas (software)	Muy grave	Coordinador T.I.	x	A.10.3.2	Se deben establecer criterios de aceptación para sistemas de información nuevos, actualizaciones y nuevas versiones y llevar a cabo los ensayos adecuados del sistema durante el desarrollo y antes de la aceptación.
RSI-16	Hardware [HW]	Avería de origen Físico.	Muy grave	Coordinador T.I.	x	A.9.2.4	Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilida

						d e integridad.
RSI-17	Abuso de privilegios de acceso.	Muy grave	Coordinador T.I.	x	A.11.2.2	Se debe restringir y controlar la asignación y uso de privilegios.
RSI-18	Destrucción - alteración de información.	Muy grave	Coordinador T.I.	x	A.10.7.3	Se deben establecer procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información contra divulgación no autorizada o uso inadecuado.
RSI-19	Errores de mantenimiento / actualización.	Muy grave	Coordinador T.I.	x	A.9.2.4	Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad.
RSI-20	Robo	Muy grave	Coordinador T.I.	x	A.9.2.1	Los equipos deben estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno, y las oportunidades de acceso no autorizado.
RSI-21	Manipulación del hardware.	Muy grave	Coordinador T.I.	x	A.9.2.7	Ningún equipo, información

							ni software se deben retirar sin autorización previa.
RSI-22		Fuego.	Muy grave	Coordinador Com.	x		Diseñar y aplicar protecciones físicas contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial.
RSI-23		Daños por agua.	Muy grave	Coordinador Com.	x		
RSI-24		Desastres naturales.	Muy grave	Coordinador Com.	x	A.9.1.4	
RSI-25	Comunicaciones [COM]	Avería de origen físico o lógico.	Muy grave	Coordinador Com.	x	A.11.4.4	El acceso lógico y físico a los puertos de configuración y de diagnóstico debe estar controlado
RSI-26		Alteración de secuencia.	Muy grave	Coordinador Com.	x	A.12.5.4	Se deben evitar las oportunidades para que se produzca fuga de información.
RSI-27		Fallo de servicios de comunicaciones.	Muy grave	Coordinador Com.	x	A.10.1.2	Se deben controlar los cambios en los servicios y los sistemas de procesamiento de información.
RSI-28		Acceso no autorizado.	Muy grave	Coordinador Com.	x	A.11.4.1	Los usuarios sólo deben tener acceso a los servicios para cuyo uso están

							específicamente autorizados.
RSI-29		Interceptación de información. (escucha)	Muy grave	Coordinador Com.	x	A.11.4.3	La identificación automática de los equipos s e debe considerar un medio para autenticar conexiones de equipos y ubicaciones específicas.
RSI-30	Equipamiento auxiliar [AUX]	Fuego.	Muy grave	Coordinador Logística	x	A.9.1.4	Diseñar y aplicar protecciones físicas contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial.
RSI-31		Daños por agua.	Muy grave	Coordinador Logística	x		
RSI-32		Desastre natural.	Muy grave	Coordinador Logística	x		
RSI-33	Instalaciones [L]	Fuego.	Muy grave	Coordinador Logística	x	A.9.1.4	Diseñar y aplicar protecciones físicas contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial.
RSI-34		Daños por agua.	Muy grave	Coordinador Logística	x		
RSI-35		Desastre natural.	Muy grave	Coordinador Logística	x		
RSI-36	Personal [P]	Indisponibilidad del personal.	Muy grave		x	A.8.1.1	Se deben definir y documentar los roles y

						responsabilidades de los empleados, contratistas y usuarios de terceras partes por la seguridad, de acuerdo con la política de seguridad de la información de la organización
RSI-37	Extorsión.	Muy grave		x	A.6.1.5	Identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no-divulgación que reflejan las necesidades de la organización para la protección de la información.
RSI-38	Fuga de información.	Muy grave		x	A.8.1.3	Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes deben estar de acuerdo y firmar los términos y condiciones de su

					contrato laboral, el cual debe establecer sus responsabilidades y las de la organización con relación a la seguridad de la información.
RSI-39	Ingeniería social.	Muy grave	x	A.8.2.2	Todos los empleados de la organización y, cuando sea pertinente, los contratistas y los usuarios de terceras partes deben recibir formación adecuada en concientización y actualizaciones regulares sobre las políticas y los procedimientos de la organización, según sea pertinente para sus funciones laborales.

Fuente: el autor.

RESUMEN ANALÍTICO ESPECIALIZADO - RAE

1. Información General	
Tema	Controles y políticas de seguridad para resguardar la información de la empresa Super Servicios del Valle S.A. definidos en un SGSI.
Titulo	Diseño de un Sistema de Gestión de Seguridad de la Información para la empresa Super Servicios del Valle S.A. basado en la norma ISO 27001:2013.
Tipo de proyecto	Aplicado
Autor (es)	Claudia Marcela Narváez Vélez
Director	Martín Cancelado
Fuente Bibliográfica	Guía para la implementación de seguridad de la información en una MIPYME. (en línea). Consultada el 23 de febrero de 2020. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-482_Guia_Seguridad_informacion_Mypimes.pdf El ciclo de Deming. La gestión y mejora de procesos. (en línea). Consultado el 17 de febrero de 2020. Disponible en: http://equipo.altran.es/el-ciclo-de-deming-la-gestion-y-mejora-de-procesos/ ESET Security Report Latinoamérica 2017. (en línea). Consultado el 13 de noviembre de 2019. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf ICONTEC. NTC 1486. (en línea) Consultado el 3 de marzo de 2020. Disponible en: http://www.unipamplona.edu.co/unipamplona/portalIG/home_15/recursos/01_general/09062014/n_icontec.pdf MAGERIT – versión 3.0. Libro I. Método. (en línea) Consultado el 06 de marzo de 2020. Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html MAGERIT – versión 3.0. Libro II. Catálogo de elementos. (en línea) Consultado el 13 marzo de 2020. Disponible de: https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html MAGERIT – versión 3.0. Libro III. Guía de Técnicas. (en línea). Consultado el 13 de febrero de 2020. Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1793-magerit-libro-iii-tecnicas/file.html.
Año	2020
Resumen	El desarrollo del SGSI para la empresa Super Servicios del Valle se propone para suplir la necesidad que presenta la empresa para realizar una adecuada gestión del riesgo. En la fase de diseño se realiza el inventario de activos de la empresa, incluyendo en el aquellos que son fundamentales para el desarrollo de los procedimientos dentro de la organización. Seguidamente se realiza la valoración de los activos bajo los criterios y dimensiones señaladas en la metodología MAGERIT, y así identificar y valor las vulnerabilidades y amenazas que pueden ser explotadas en los activos. Finalmente se evalúan los riesgos encontrados para así sobre estos resultados identificar cuáles se deben tratar con mayor prioridad, qué tipo de controles y/o políticas son necesarias para mitigar su impacto o lograr la corrección y disminuir la probabilidad de ocurrencia.

Palabras Claves	Activos, amenaza, auditoría, controles, disponibilidad, información, integridad, ISO 27001, ISO 27002, políticas, riesgo, seguridad, vulnerabilidad.
Contenidos	Inventario de activos: Se identifican todos los activos que son fundamentales en la organización para el desarrollo de sus procesos. Valoración de activos – Escalas de valoración: De acuerdo con la función que cumple cada uno de los activos se le otorga una valoración cualitativa y cuantitativa, conforme al impacto que generará su daño o pérdida. [4] Identificación y valoración de vulnerabilidades. Valoración de amenazas sobre activos: Determinar la degradación que puede sufrir un activo en el caso de materializarse una amenaza. [5] Identificación y análisis de riesgos: Permite establecer todos los riesgos que pueden afectar la operatividad de la empresa. Evaluación del riesgo: Identificar cómo debe ser el tratamiento de los riesgos y su prioridad. Tratamiento del riesgo: definir controles y políticas de seguridad de la información.

2. Descripción del Problema de Investigación

Actualmente, la empresa no cuenta con un modelo o proceso que permita la adecuada gestión del riesgo, por lo que al presentarse algún tipo de materialización o sospecha que pueda afectar la seguridad muy probablemente se puedan presentar fugas o vacíos tanto en el procedimiento de contención como en el de control.

Es por esto por lo que se requiere la implementación del SGSI, en el cual se establezcan procesos ordenados que le permitan a la empresa SSV S.A identificar, analizar y ejecutar controles para salvaguardar sus activos de información y a sí mismo realizar una gestión continua durante el ciclo de vida de la ejecución de los procesos dentro de la empresa.

3. Objetivos

Objetivo general:

Diseñar un Sistema de Gestión de la Seguridad de la Información para la empresa Super Servicios del Valle, que garantice la confidencialidad, integridad y disponibilidad de la información.

Objetivos específicos:

- Clasificar los activos de información de la empresa Super Servicios del Valle.
- Analizar las vulnerabilidades, amenazas y riesgos presentes.
- Establecer políticas y controles de seguridad basados en la norma ISO 27001:2013 para mitigar y reducir los riesgos detectados.
- Definir la estructura organizacional, roles y responsabilidades de los funcionarios en cuanto a la Seguridad de la Información en la empresa Super Servicios del Valle.

4. Referentes Teóricos y Conceptuales

Referentes teóricos:

- SGSI:

Permite la gestión de la seguridad de la información mediante procesos sistemáticos, documentados y de conocimiento por parte de toda la organización. Su propósito principal es garantizar que los sistemas de información en las empresas estén protegidos por mecanismos de control físicos y lógicos que protejan estos activos frente a cualquier vulnerabilidad o amenaza. Entre los ejemplos más comunes están: modalidades de fraude, espionaje, sabotaje o vandalismo, virus informáticos, el “hacking” o ataques cibernéticos o incluso incidentes de seguridad causados voluntaria o involuntariamente en la empresa o aquellos que surgen accidentalmente por catástrofes naturales y fallas técnicos.

Las practicas más utilizadas para la gestión de la seguridad en Latinoamérica son:
políticas de seguridad (74%).
Auditorías internas y/o externas (38%) y la clasificación de la información (31%).

- ISO 27001

Busca minimizar el riesgo en los sistemas de información de las empresas mediante la especificación de requisitos para establecer, implementar, mantener y mejorar continuamente un SGSI. Permite que una empresa sea certificada confirmando el cumplimiento de esta norma en la organización.

- ISO 27002

Proporciona directrices detalladas para la implantación de controles y el uso de buenas prácticas dentro de una organización.

Referentes conceptuales:

- Amenaza: Causa potencial de un incidente no deseado, que podría dañar uno o más activos de un sistema u organización.
- Vulnerabilidad: Es una debilidad del sistema informático que puede ser utilizada para causar daño.
- Riesgo: Grado de exposición de un activo que permite la materialización de una amenaza.

5. Resultados y Conclusiones

Resultado/producto esperado	Indicador	Beneficiarios
Diagnóstico inicial	Determinar el nivel de la empresa con respecto a la seguridad de la información.	Usuarios internos.
Inventario de activos	Cubrimiento del SGSI a los activos de información de la empresa.	Usuarios internos.
Análisis de vulnerabilidades	Identificar que amenazas se puedan estar presentado en la empresa, para activar controles de acuerdo con su nivel de riesgo.	Usuarios internos. Clientes. Proveedores.
Identificación y valoración de riesgos	Nivel de seguridad en las aplicaciones de la empresa.	Usuarios internos. Clientes. Proveedores. Arrendatarios.
Políticas y controles de seguridad	Nivel de implementación de controles (controles implementados / controles planeados a implementar)	Usuarios internos. Clientes. Proveedores. Arrendatarios.

Plan de sensibilización	Sensibilidad de los funcionarios frente al SGSI (capacitaciones ejecutadas/capacitaciones programadas)	Usuarios internos. Clientes. Proveedores. Arrendatarios.
Auditorias	Nivel de compromiso de la alta gerencia. Gestión de incidentes de seguridad (incidentes reportados / incidentes gestionados) Verificación periódica de las políticas y controles de seguridad planteadas.	Usuarios internos.

Fuente: el autor.

CONCLUSIONES

Al implementar un SGSI en la empresa se busca certificar las buenas prácticas que son implementadas con el fin de fin de proteger la organización y sus activos de información, mediante la asignación de controles necesarios ya sean de tipo físico, lógico e incluyendo a todos los colaboradores y/o

Se incluye el personal administrativo para realizar la revisión e identificación de posibles vulnerabilidades en los procesos que se realizan a diario en la empresa, esto permite encontrar fallas de seguridad no registradas para las cuales se dio prioridad y se solucionaron por el personal del proceso de T.I. y fueron incluidas en las políticas de seguridad para continuar con su vigilancia y como mejora continua del SGSI implementado. Además de concientizar a cada funcionario sobre la existencia de riesgos y la necesidad de contenerlos a tiempo haciendo uso de buenas prácticas de seguridad.