DEFINICIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE INSITEL S.A. ALINEADO CON LA NORMATIVA DE LA FAMILIA ISO 27000.

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS

JONNY SANTIAGO PABON ALVAREZ
20171005103

MODALIDAD DE GRADO PASANTÍAS

BOGOTÁ D.C.

2023

Contenido

DEFINICIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DE INSITEL S.A. ALINEADO CON LA NORMATIVA DE LA FAMILIA ISO 27000.

1. PLANTEAMIENTO DE PROBLEMA 4
2. OBJETIVO GENERAL. 4
3. OBJETIVOS ESPECÍFICOS. 5
4. JUSTIFICACIÓN. 5
5. MARCO TEÓRICO. 6
5.1. Seguridad de la información. 6
5.2. Seguridad informática. 6
5.3. Estándar de seguridad de la información ISO/IEC27000 para implementación de SGSI. 7
5.4. Consideraciones para SGSI. 8
5.5. Integridad de la información. 9
5.6. Confidencialidad de la información. 9
5.7. Disponibilidad de la información. 9
5.8. Tipos de ataques a la red 10
5.8.1. Denegación de Servicios Distribuido (DDoS): 10
5.8.2. Phishing: 10
5.8.3. Ataques de Día Cero: 11
5.8.4. Malware: 11
5.9. Ciberseguridad. 12
5.10. Estrategias de defensa en ciberseguridad. 14
6. RESULTADOS. 16
6.1. DEFINICIÓN DEL ALCANCE, LOS LÍMITES Y LA POLÍTICA DEL SGSI. 16
6.1.1. CONTEXTO DE LA COMPAÑÍA. 16
6.1.2. ALCANCE. 17

6.1.3. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN. 17
6.2. REALIZAR EL ANÁLISIS DE LOS REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN. 18
6.2.1. PARÁMETROS PARA LA EJECUCIÓN. 18
6.3 REALIZAR LA VALORACIÓN DE RIESGOS Y PLANIFICAR EL TRATAMIENTO DE RIESGOS. 18
6.3.1 METODOLOGÍA DE EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN. 19
6.3.2 IDENTIFICACIÓN DE ACTIVOS Y TIPO. 19
6.3.3 CODIFICACIÓN DE LOS ACTIVOS. 21
6.3.4 CRITERIOS PARA LA VALORACIÓN DE ACTIVOS (IMPACTO). 22
6.3.6 IDENTIFICACIÓN DE LAS AMENAZAS. 24
6.3.7 IDENTIFICACIÓN DE LAS VULNERABILIDADES. 26
6.3.8 VALORACIÓN DE LOS RIESGOS EN LA SEGURIDAD DE LA INFORMACIÓN. 30
6.3.9 TRATAMIENTO DE RIESGOS MEDIANTE LA IMPLEMENTACIÓN DE CONTROLES. 31
6.3.10 DESARROLLO DE CONTROLES. 33
6.4 DISEÑAR EL SGSI ALINEADO A LA NORMATIVA DE LA SERIE ISO/IEC 27000. 33
6.4.1 CAPACITACIÓN DE AUDITORÍAS INTERNAS 34
6.4.2 AUDITORÍA INTERNA Y EXTERNA 34
7. CONCLUSIONES 34
8. REFERENCIAS. 35
9. ANEXOS 36

1. PLANTEAMIENTO DE PROBLEMA

El aumento de las tecnologías de la información en la mayoría de los sectores económicos, permite un crecimiento considerable de cada sector gracias a las diferentes bondades que ofrece la tecnología de la información, como pueden ser, la comunicación en instantes entre compañías separadas geográficamente, la posibilidad de realizar transacciones comerciales vía web, entre otras, facilitan el crecimiento cada vez más acelerado de las organizaciones.

No obstante, este uso masivo de tecnologías de la información ha generado ciertos problemas a las organizaciones, debido a que las amenazas presentes en el medio generan un continuo aumento de vulnerabilidades que pueden convertirse en un verdadero riesgo para las compañías, pues su funcionamiento puede verse afectado como consecuencia de algún percance en la tecnología utilizada.

Las compañías buscan combatir esta amenaza latente mediante la generación de un plan de acción frente a las diferentes situaciones que se pueden presentar en el día a día. Este plan de acción es llamado Sistema de Gestión de Seguridad de la Información (SGSI) y se define como el conjunto de directrices y/o lineamientos a seguir en las entidades, las personas responsables y la documentación requerida para garantizar su funcionamiento.

Por este motivo, las organizaciones buscan la implementación de unas normativas que se alineen con lo especificado en la norma ISO 27001, que consiste en determinados estándares y mejores prácticas que se deberían implementar en una compañía para obtener un SGSI enfocado en proteger el instrumento fundamental de cualquier compañía que es la información [1].

A partir de lo anterior, surge la siguiente pregunta problema ¿es posible realizar un proceso que permita diagnosticar, evaluar e implementar un sistema de gestión de la seguridad de la información basado en los lineamientos sugeridos por la serie de normas ISO 27000, garantizará la seguridad de la información de la compañía Insitel S.A?

2. OBJETIVO GENERAL.

Definir un sistema de gestión de la seguridad de la información de Insitel S.A. alineado con la normativa

de la familia ISO 27000.

3. OBJETIVOS ESPECÍFICOS.

- Definir el alcance, los límites y la política del SGSI.
- Realizar el análisis de los requisitos de seguridad de la información.
- Realizar la valoración de riesgos y planificar el tratamiento de riesgos.
- Diseñar el SGSI alineado a la normativa de la serie ISO/IEC 27000.

4. JUSTIFICACIÓN.

Este proyecto está enfocado en el ámbito académico y organizacional, se proporciona un contexto actual de la cantidad de información intercambiada a través de la red, que sigue en crecimiento y cada día integra nuevos campos de la vida cotidiana a la misma, un claro ejemplo de dicha afirmación es el internet de las cosas (IoT). Por medio de éste enfoque se busca proporcionar un punto de vista enfocado en la seguridad de la información, tanto las amenazas a las que se enfrenta, como las medidas que se toman en cada ámbito para solucionar.

Las conclusiones que se determinen a partir del estudio de las amenazas y la mejor forma de protegerse, enfocados en cada una de las diferentes técnicas de ataques presentes para una organización y los distintos métodos utilizados para proteger la red y los activos de una amenaza; adicionalmente se puede extender a otras organizaciones y/o ámbitos de investigación donde se busca la protección de la información tanto en medios electrónicos como en medios físicos.

La necesidad de preservar y proteger toda la información que circula en internet y físicamente en una organización, hace posible que se puedan desarrollar investigaciones y proyectos con el objetivo de asegurar un tráfico seguro en un entorno tan abstracto y tan utilizado en los últimos tiempos como lo es el ciberespacio. Anteriormente, las organizaciones debían preocuparse solamente por la seguridad física, proteger sus instalaciones, controlar el acceso a ciertos puntos en sus oficinas; pero con la evolución de internet ha causado que cada día las entidades estén más conectadas y por ende más involucradas con la navegación en el ciberespacio; en la internet actual esto se traduce en vulnerabilidades que ponen en peligro la integridad, disponibilidad y confidencialidad de la información de la empresa, debido a los diferentes ataques modernos que presentan riesgos en cada uno de los aspectos esenciales de la información.

Vale la pena aclarar que cualquier ataque exitoso dentro de organizaciones importantes se traducen en una cifra preocupante de pérdidas, según un estudio realizado por Olmedo, J et al 2018 [2] indica que más de un tercio de la población en Colombia reporta haber sido víctima de fraudes electrónicos y 6 de cada 10 personas pensaban que los defraudadores trabajaban en las mismas organizaciones. Adicionalmente, se asegura que en América Latina y el Caribe, el costo de ciberataques asciende a un promedio de US$90.000 millones al año debido a la falta de una política orientada a la respuesta oportuna a incidentes, lo que se traduce en fallas en su sistema de gestión de seguridad de la información que como consecuencia ocasiona pérdidas monetarias importantes para las organizaciones.

5. MARCO TEÓRICO.

5.1. Seguridad de la información.

La seguridad de la información es la disciplina que se encarga de proteger la información y los diferentes sistemas de información contra acceso, uso, divulgación, alteración, modificación, lectura, inspección, registro o destrucción no autorizados. La seguridad de la información ha evolucionado en los últimos años, desde la seguridad física orientada a la protección de ordenadores y dispositivos de almacenamiento de información, pasando por la seguridad de sistemas y redes, a concentrarse en la gestión de alto nivel logrado a través de políticas, procedimientos y controles basados en las personas. [3]

5.2. Seguridad informática.

Consiste en la disciplina que se encarga de proteger los dispositivos y sistemas informáticos, mediante medidas técnicas que pretenden preservar la integridad, confidencialidad y disponibilidad de la información contenida en dichos sistemas; por ende, están enfocadas en infraestructura de comunicaciones que soportan la operación de una organización tanto el hardware como el software.
Adicionalmente, se podría definir la seguridad informática como la disciplina que se encarga de implementar de tecnologías que protegen la información almacenada en los diferentes dispositivos de red, algunas de éstas tecnologías son antivirus, firewalls, detección de intrusiones, detección de anomalías, correlación de eventos, atención de incidentes, entre otras soluciones que buscan la protección de la información que se encuentra en cada uno de los dispositivos. [4]

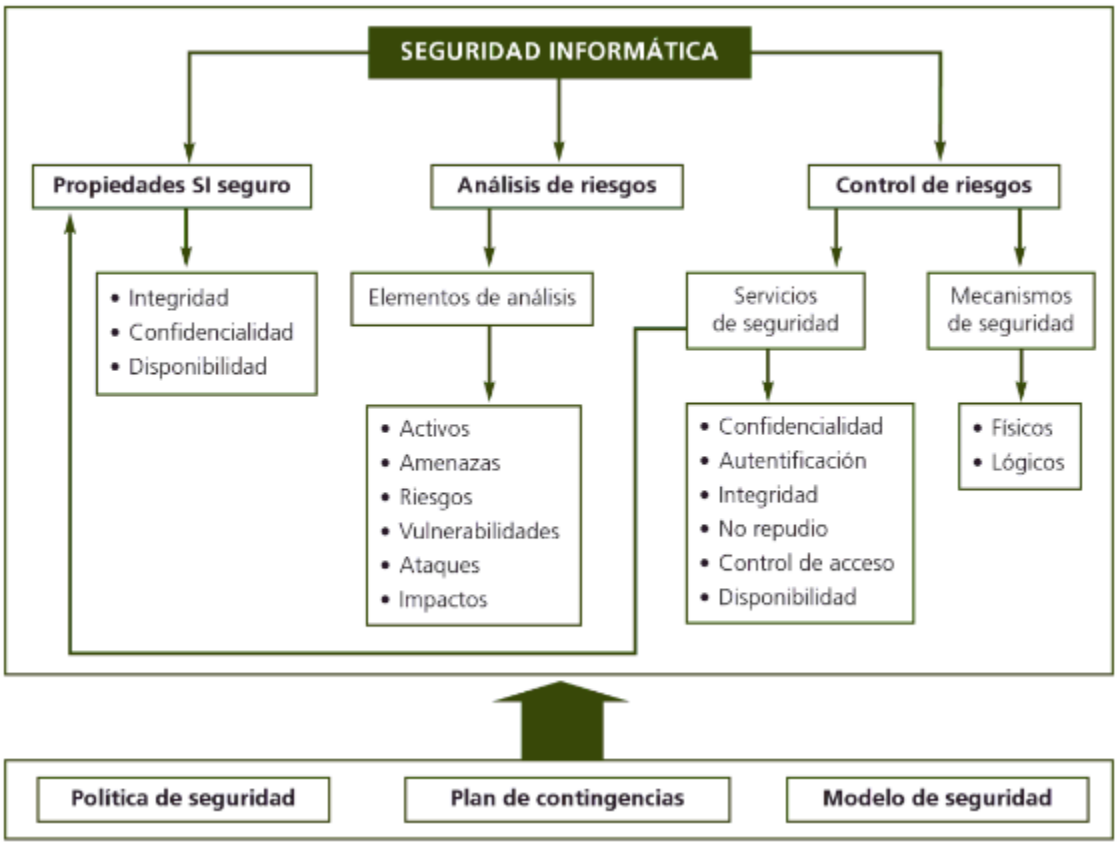


Figura 1, Estructura de seguridad informática. [5]

5.3. Estándar de seguridad de la información ISO/IEC27000 para implementación de SGSI.

Para llevar a cabo un sistema de gestión de seguridad de la información (SGSI) dentro de una organización es bastante importante conocer los requisitos que debe cumplir para que sea funcional, en éstos requisitos encontramos estándares, su estructura y la relación existente entre cada uno de ellos.

Los estándares más utilizados al momento de implementar un SGSI corresponden a la serie ISO/IEC 27000 publicadas por la ISO y la Comisión Electrotécnica Internacional (IEC), se subdivide en cuatro (4) categorías [6]:

- La categoría que contiene el léxico, que se encuentra en la norma ISO/IEC 27000.
- La categoría de los requerimientos, que se encuentra en la norma ISO/IEC 27001 y la norma ISO/IEC27006.
- La categoría que almacena las guías desarrolladas a través de 10 normas; ISO/IEC 27002,

ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005, ISO/IEC 27007, ISO/IEC 27008, ISO/IEC 27013, ISO/IEC 27014, ISO/IEC 27016 y ISO/IEC 27032.

- La categoría para sectores específicos, contenidas en las normas ISO/IEC 27010, ISO/IEC 27011, ISO/IEC 27015 y ISO/IEC 27017.

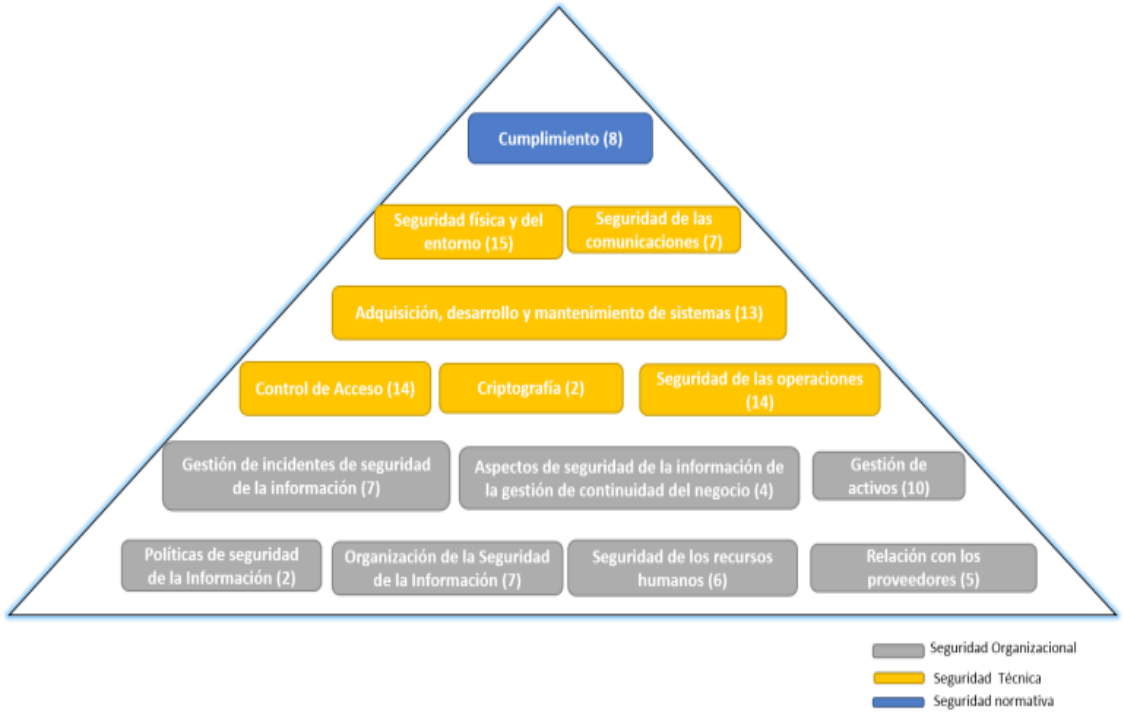


Figura 2, Estructura de controles. [6]

5.4. Consideraciones para SGSI.

Se recomienda tener en cuenta los siguientes elementos al momento de implementar un sistema de gestión de seguridad de la información:

- Objetivos estratégicos de la organización:

A través de estos objetivos se busca determinar como un SGSI puede aportar en diferentes ámbitos de la organización y ratificar aún más su necesidad como una parte esencial de la estrategia de la organización según lo comenta *Valencia-Duque et al [6]*.

- Requisitos normativos o de terceros relacionados con la seguridad de la información:

Adicionalmente a los requerimientos de la normativa ISO/IEC 27000, es necesario identificar los requerimientos normativos que se deben implementar para la entidad, por ejemplo, leyes nacionales enfocadas en la protección de la información o los requerimientos que se tengan con terceros para asegurar con criterios de confidencialidad, integridad y disponibilidad de la información como lo menciona *Valencia-Duque et al [6]*.

- Sistema de gestión existentes:

Para aprovechar la base ejecutada por cuenta de la organización en relación con otras normas para la gestión de la seguridad de la información, se hace necesario identificar y evaluar si se tiene en cuenta, aunque por lo general todas las normas de gestión basadas en las normas ISO cuentan con algunos elementos estructurales idénticos y pueden ser compatibles con los requerimientos establecidos en la norma ISO/IEC 27001:2013 como lo asegura *Valencia-Duque et al [6]*.

5.5. Integridad de la información.

Consiste en la protección de datos frente a la modificación, supresión, duplicación o reordenación realizada por entidades o terceros no autorizados. Es decir, la integridad de la información se refiere a la fiabilidad de los recursos de información, la garantía de la no alteración. [7]

5.6. Confidencialidad de la información.

Se llama confidencialidad a la protección de la información contra la divulgación a entidades o individuos no autorizados, es decir, la información debe ser conocida sólo por las personas y/o entidades previstas. [7]

5.7. Disponibilidad de la información.

La disponibilidad consiste en tener acceso a la información cuando se requiere. En perspectiva, sí la información no está disponible cuando se necesita es, como mínimo, tan malo como no disponer del sistema donde se almacena la información. [7]



Figura 3, Principios fundamentales de la seguridad de la información. [8]

5.8. Tipos de ataques a la red

5.8.1. Denegación de Servicios Distribuido (DDoS):

Se define como denegación de servicios distribuido a la actividad que niega parcial o totalmente el acceso de usuarios legítimos a los recursos o redes mediante la saturación de tráfico enviado a dicho recurso o red para crear un efecto de hacinamiento, de forma que colapsan los recursos informáticos disponibles. A diferencia de un ataque de denegación de servicio (DoS), que desde una única fuente genera todo el tráfico malicioso; el ataque de denegación de servicio distribuido genera tráfico desde varios nodos comprometidos distribuidos geográficamente conocidos como botnets acorde a lo mencionado por Krishna Kishore, P. et al 2023 [9].

5.8.2. Phishing:

Los ataques phishing son aquellos ataques que mediante el engaño buscan extraer datos confidenciales de cualquier persona u organización, usualmente usan páginas web falsas para que la víctima ingrese sus datos confidenciales, por ejemplo, número de documento, tarjetas de crédito, usuario y contraseña del correo, entre otras. Para luego, utilizar estos datos para realizar cualquier tipo de actividad ilegal según el estudio realizado por Basit, A et al 2021 [10].



Figura 4, Phishing simulando ser el gobierno de Estados Unidos. [11]

5.8.3. Ataques de Día Cero:

Se categorizan como ataques de día cero a los ataques que se originan a través de vulnerabilidades desconocidas en el sistema para la comunidad pública, con el fin de evitar la detección de herramientas de ciberseguridad, al basarse en el hecho de que es una vulnerabilidad desconocida para las identidades se convierte en una de las principales amenazas para la seguridad informática como lo menciona Yang Guo et al 2023 [12].

5.8.4. Malware:

Se define como malware a cualquier software que ejecuta intencionalmente cargas maliciosas en cualquier máquina víctima. Cabe aclarar que, existen varios tipos de malware como lo puede ser virus, gusanos, ransomware, caballos de troya, spyware, entre otros como lo menciona Aslan, Ö. A. et al 2020 [13].

Para proteger a un dispositivo contra esta amenaza, se utiliza generalmente un software que detecta malware que ha evolucionado a medida que los ataques por malware se vuelven más sofisticados, como en la complejidad de su código, las técnicas de ofuscación o los vectores de distribución. Las técnicas de detección se pueden categorizar desde diferentes perspectivas, que depende del enfoque utilizado para su detección.

La técnica basada en firmas consiste en comparar el archivo con una base de datos de firmas de malware conocidos, las firmas pueden ser de Hash o Bytes; esta técnica es bastante rápida y funcional para ataques conocidos. No obstante, su desventaja radica en la incapacidad de detectar ataques desconocidos o nuevos, ya que sí un ataque no se encuentra almacenado en la base de datos de firmas del software no podrá ser detectado.

En cuanto a la técnica basada en heurística, el software utiliza reglas y/o algoritmos que indiquen comportamiento malicioso, como lo puede ser, comandos que llamen APIs, relaciones entre archivos, comunicación con servidores de reputación dudosa, entre otros. Al utilizar esta técnica, los software son capaces de detectar ataques que no estén disponibles en las firmas; puede ser bastante rápida y efectiva pero requiere mejoras constantes en las reglas para mantener el sistema actualizado evitando falsos positivos.

Por último, para la técnica basada en comportamiento, el software analiza el comportamiento e interacción del archivo en un entorno controlado, de esta forma, puede conocer todas las acciones que ejecutará el archivo en el sistema y recolectar información para clasificar el archivo. La principal desventaja de esta técnica, es que requiere más recursos del dispositivo y toma más tiempo que las otras técnicas. [14]

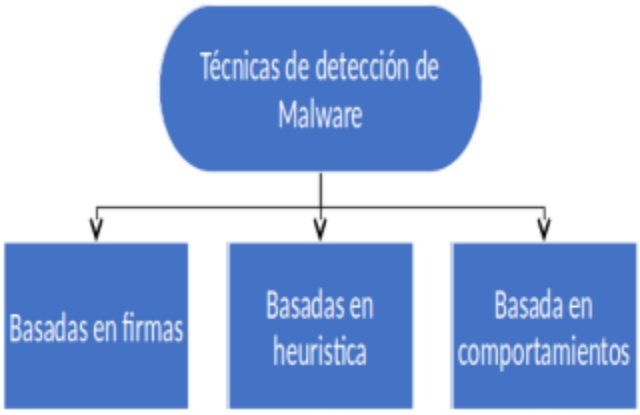


Figura 4, técnicas de detección de malware. [14]

5.9. Ciberseguridad.

La ciberseguridad se define como el conjunto de tecnologías, prácticas y procesos diseñados para ayudar a proteger la red, dispositivos, información y programas de cualquier tipo de ataque cibernético, como

denegación de servicios (DoS), Ataques de día cero, puertas traseras, phishing o acceso no autorizado. A menudo, la ciberseguridad se asocia a la seguridad de la tecnología de la información (IT). No obstante, el creciente número de dispositivos asociados a internet ocasiona que la superficie de ataque de una organización sea cada vez mayor, como lo puede ser las tecnologías operativas (OT) y el internet de las cosas (IoT) como lo aseguró *Ordieres, J et al 2022* [15].

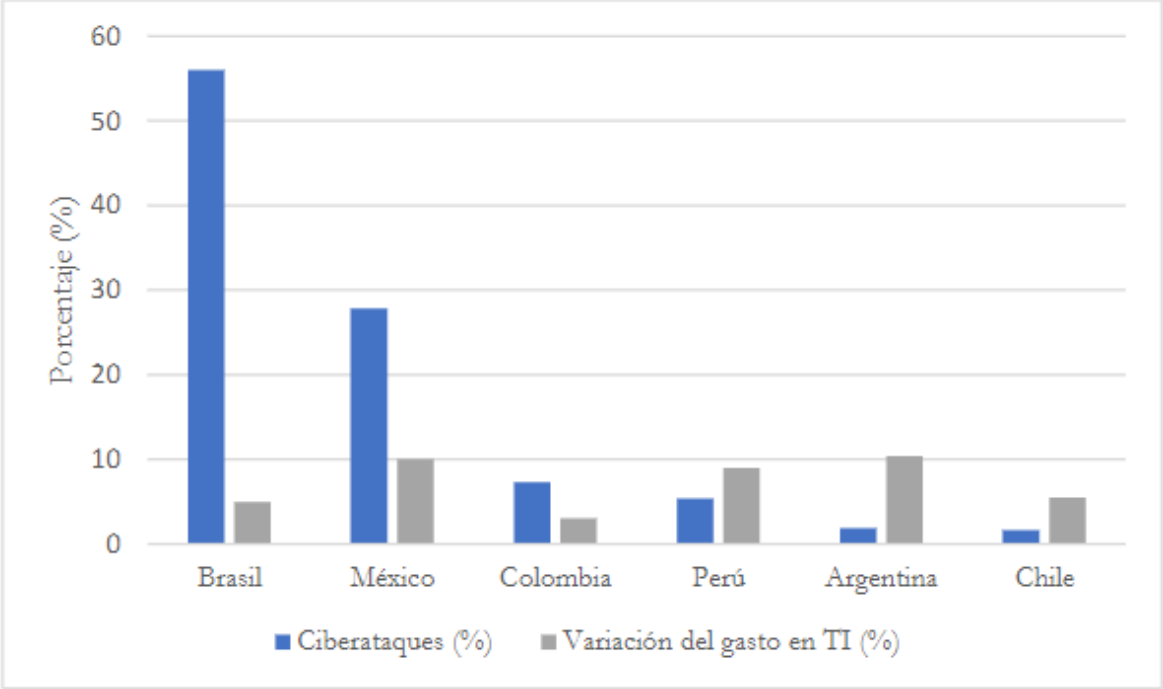


Figura 5, Proporción de ciberataques (en %) y variación en el gasto en TI (en %). [16]

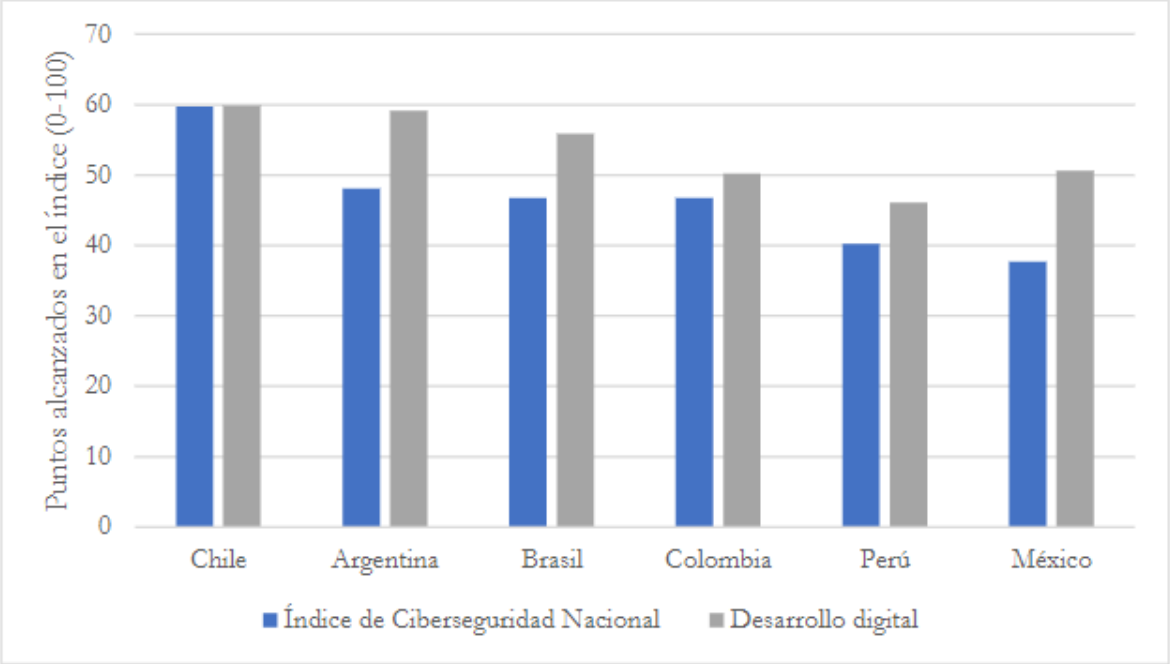


Figura 6, Puntuaciones obtenidas en el Índice Nacional de Ciberseguridad y el Índice de Desarrollo Digital. [16]

5.10. Estrategias de defensa en ciberseguridad.

En el campo de la ciberseguridad, se requieren estrategias de defensa para proteger los datos, sistemas de información y redes contra ciberataques o intrusiones. Estas estrategias tienen como objetivo prevenir brechas de datos o incidentes de seguridad, así como monitorear y reaccionar ante intrusiones, las cuales se definen como cualquier tipo de actividad no autorizada que cause daño a un sistema de información.

Un sistema de detección de intrusiones (IDS, por sus siglas en inglés) se representa típicamente como "un dispositivo o aplicación de software que monitorea una red de computadoras o sistemas en busca de actividad maliciosa o violaciones de políticas" . Las soluciones de seguridad tradicionales conocidas, como antivirus, firewalls, autenticación de usuarios, control de acceso, cifrado de datos y sistemas de criptografía, podrían no ser efectivas según las necesidades actuales de la industria cibernética. Por otro lado, los IDS resuelven estos problemas al analizar datos de seguridad desde varios puntos clave en una red de computadoras o sistemas.
Además, los sistemas de detección de intrusiones pueden usarse para detectar ataques tanto internos como externos. Existen diferentes categorías de sistemas de detección de intrusiones según el alcance de uso. Por ejemplo, un sistema de detección de intrusiones basado en host (HIDS, por sus siglas en inglés) y un sistema de detección de intrusiones de red (NIDS, por sus siglas en inglés) son los tipos más comunes,

basados en el alcance de sistemas individuales a grandes redes. En un HIDS, el sistema monitorea archivos importantes en un sistema individual, mientras que en un NIDS analiza y monitorea las conexiones de red en busca de tráfico sospechoso. De manera similar, según las metodologías, los IDS basados en firmas y los IDS basados en anomalías son las variantes más conocidas.

- Los IDS basados en firmas: Utilizan una firma predefinida que corresponde a un ataque conocido. Se identifica una determinada secuencia o patrón como la detección de ataques correspondientes en un IDS basado en firmas. Este enfoque puede ser eficiente para procesar un alto volumen de tráfico de red, pero está estrictamente limitado a los ataques conocidos. Por lo tanto, la detección de ataques nuevos o no vistos es uno de los mayores desafíos de este sistema basado en firmas.
- Los IDS basados en anomalías: Este enfoque supera las limitaciones de los IDS basados en firmas mencionados anteriormente. En un sistema de detección de intrusiones basado en anomalías, primero se examina el comportamiento de la red para encontrar patrones dinámicos y crear automáticamente un modelo basado en datos que perfila el comportamiento normal. Así, se detectan desviaciones en caso de cualquier anomalía. El IDS basado en anomalías se considera un enfoque dinámico que sigue una detección orientada al comportamiento. Su ventaja principal es la capacidad para identificar ataques desconocidos o ataques de día cero.

Además de estos enfoques, se puede utilizar un enfoque de detección híbrida que combina tanto las técnicas basadas en el uso de firmas como las basadas en anomalías. En un sistema híbrido, se utiliza el sistema de detección de uso indebido para detectar tipos conocidos de intrusiones y el sistema de detección de anomalías para detectar ataques novedosos.

También se puede emplear el análisis de protocolos estatales para detectar intrusiones. Este método identifica desviaciones en el estado del protocolo de manera similar al método basado en anomalías, pero utiliza perfiles universales predefinidos basados en definiciones aceptadas de actividad benigna. Sin embargo, este enfoque tiene sus propias limitaciones y depende de la definición precisa de actividad normal.

Una vez que se ha completado la detección, se puede utilizar un sistema de prevención de intrusiones (IPS, por sus siglas en inglés) para mitigar los riesgos de diferentes maneras, ya sea de forma manual, proporcionando notificaciones o a través de procesos automáticos. Se considera que un sistema de respuesta automática es más efectivo, ya que no requiere una interfaz humana entre los sistemas de detección y respuesta.

En resumen, los sistemas de defensa y detección de intrusiones son fundamentales para proteger los datos, sistemas de información y redes contra ciberataques. Los IDS son herramientas clave en esta tarea, permitiendo detectar actividades maliciosas o violaciones de políticas. Los enfoques más comunes de IDS son los basados en firmas y los basados en anomalías, cada uno con sus ventajas y desafíos. La combinación de ambos enfoques en sistemas híbridos y el uso de análisis de protocolos estatales pueden mejorar la capacidad de detección de intrusiones. Además, se puede utilizar un sistema de prevención de

intrusiones para responder automáticamente a las amenazas detectadas y mitigar los riesgos [17].

6. RESULTADOS.

Para llevar a cabo el proyecto planteado del sistema de gestión de seguridad de la información, se realiza un plan de trabajo secuencial para cumplir con los objetivos planteados anteriormente, de esta forma se detalla el desarrollo a continuación.

6.1. DEFINICIÓN DEL ALCANCE, LOS LÍMITES Y LA POLÍTICA DEL SGSI.

6.1.1. CONTEXTO DE LA COMPAÑÍA.

Para llevar a cabo el contexto de la compañía, es importante entender las actividades que realiza INSITEL S.A. Es una compañía de más de veinte (20) años de experiencia dedicada a la prestación de servicios en telecomunicaciones, ciberseguridad, automatización, desarrollo de hardware y software de propósito específico. Luego para llevar a cabo el proyecto es entender el contexto de la compañía, de este modo establecer el punto de partida, comprender las necesidades de la organización y acoplar el sistema de gestión de seguridad de la información para que no impacte negativamente en el desarrollo de las actividades principales de la empresa. Para entender este contexto, es importante identificar las partes interesadas y las necesidades de ellas para la implementación del SGSI.

Se establecen las siguientes partes interesadas y sus principales necesidades con respecto al sistema de seguridad de la información:

- **Clientes**: Protección de la confidencialidad de información sensible, garantizar disponibilidad de la información pertinente e intercambio de información seguro.
- **Proveedores:** Protección de la confidencialidad de información sensible, garantizar disponibilidad de la información pertinente e intercambio de información de manera segura.
- **Vecinos:** Seguridad física en su entorno.
- **Directivos:** Protección de la confidencialidad en información reservada y garantizar la continuidad del negocio.
- **Empleados:** Protección de la confidencialidad de la información personal privada y facilitar las herramientas necesarias para la seguridad de la información en el desarrollo sus actividades laborales.

Los procesos que disminuyen el impacto y protegen la información se conocen como gestión de riesgos de seguridad de la información, se enfocan en descubrir los puntos débiles y brindar controles o complementos que permitan fortalecer dichos puntos en todo el ciclo de vida del servicio prestado por una organización específica.

Cabe resaltar que las organizaciones deberían diseñar y ejecutar un plan de gestión de riesgos que les permita garantizar la continuidad de su negocio cuando se presenten incidentes de seguridad de la información. Debido a lo anterior, se genera la necesidad de implementar un análisis de riesgos de seguridad de la información aplicado a los procesos previstos en el alcance del SGSI de INSITEL S.A, para llevar a cabo lo menciona, es crucial entender la situación actual de INSITEL y realizar un inventario de activos con sus respectivas amenazas; de este modo, se podrá desarrollar la medición de riesgos existente e implementar los controles y/o políticas necesarias que garanticen la seguridad de dichos activos.

Los diferentes tipos de riesgos identificados de distintos indoles como los desastres naturales, desconocimiento de normas, fallas en el tratamiento de la información entre otros; a menudo son los riesgos más frecuentes y que generan mayor impacto para la organización. Como consecuencia, sí la organización no cuenta con un plan de tratamiento para los riesgos estará expuesta a que su información pueda ser corrompida.

La principal ventaja del plan es que ayuda a identificar el nivel de riesgo de los activos a través del nivel de madurez de la protección brindada a cada activo, adicionalmente le brinda herramientas al personal de INSITEL para seguir los procedimientos y normas asociadas a la seguridad de la información.

6.1.2. ALCANCE.

El alcance del SGSI se determina en todos los procesos internos involucrados en el desarrollo de las actividades principales de la compañía involucrando los procesos secundarios de apoyo para garantizar tanto la continuidad del negocio como la calidad del servicio. Como se evidencia en el anexo *ALCANCE SGSI,* donde se incluyen procesos vitales como los **“Proceso Directivos”** y **“Procesos Misionales Operativos”**; también vale la pena resaltar numeral 4 de exclusiones, donde se definen tanto procesos, ubicaciones e infraestructura que no es incluida en el alcance a partir del contexto de la compañía definido inicialmente.

6.1.3. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

Una vez se establece el alcance que tendrá el SGSI, se procede a redactar una política de seguridad de la información que cumpla con las siguientes características:

- Satisfaga las necesidades de la organización.

- Garantice la continuidad del negocio.
- Busque la protección de los tres pilares fundamentales de la información, los cuales son; integridad, disponibilidad y confidencialidad.
- Sea fácil de comprender por cualquier colaborador interno de INSITEL S.A.

Tomando en cuenta los parámetros anteriormente mencionados, se redacta y aprueba una política general de seguridad de la información que se enfoca en la protección de la confidencialidad, disponibilidad e integridad de la información tanto interna como de terceras partes que se pueda ver involucrado en el desarrollo de sus actividades principales (revisar anexo *Política de Seguridad de la Información)* y la continuidad del negocio.

6.2. REALIZAR EL ANÁLISIS DE LOS REQUISITOS DE SEGURIDAD DE LA INFORMACIÓN.

6.2.1. PARÁMETROS PARA LA EJECUCIÓN.

Con base en el alcance determinado y el contexto de la compañía, se establecen los objetivos del SGSI (revisar anexo *Objetivos del SGSI 2023)* e indicadores que permitan evaluar el cumplimiento de los objetivos del SGSI; dichos objetivos están alineados a los siguientes requisitos de seguridad de la información:

- ✓ La valoración de riesgos se debe involucrar el inventario de todos los activos que contienen información tanto físicos como tecnológicos, la persona responsable del activo, líder de cada proceso a evaluar, el personal de ciberseguridad y tecnologías de la información en apoyo a la valoración de éste.
- ✓ Cumplimiento del marco legal con respecto a seguridad de la información y seguridad informática de la compañía.
- ✓ Garantizar la continuidad del negocio con la implementación de políticas tomando en cuenta las actividades de la organización.
- ✓ Fomentar la concientización del personal de INSITEL S.A. a través de capacitaciones que mitiguen posibles riesgos asociados a las personas.
- ✓ Cumplimiento contractual en temas de seguridad de la información y seguridad informática.
- ✓ Establecer acciones de mejora cuando sea necesario para cerrar la brecha de seguridad de la información.
- ✓ Análisis de riesgos con frecuencia anual o cuando los cambios en la operación de la organización lo requieran con el fin de buscar la mejora continua de la seguridad de la información.

6.3 REALIZAR LA VALORACIÓN DE RIESGOS Y PLANIFICAR EL TRATAMIENTO DE

RIESGOS.

6.3.1 METODOLOGÍA DE EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

Ingeniería de Sistemas Telemáticos S.A – INSITEL, se apoya en la norma ISO 27005:2008 para desarrollar una metodología de Gestión de Riesgos de Seguridad de la Información. Las etapas de la metodología es la siguiente:

I. Identificación de activos y tipo.
II. Codificación de los activos.
III. Criterios para la valoración de activos.
IV. Valoración del impacto.
V. Identificación de las amenazas.
VI. Identificación de las vulnerabilidades.
VII. Valoración de los riesgos en la seguridad de la información.
VIII. Tratamiento de los riesgos críticos.

Se establece que el plan de tratamiento de riesgos se dará por cumplido una vez se culminen todas las fases del ciclo de la metodología anteriormente planteada y el tiempo empezará a contar una vez se dé inicio a la primera fase del ciclo.

A continuación, se explican a profundidad cada una de las etapas de la metodología de riesgos:

6.3.2 IDENTIFICACIÓN DE ACTIVOS Y TIPO.

Esta etapa consiste en determinar todos los elementos propiedad de una organización para la manipulación, intercambio y demás actividades relacionadas con la información. Cabe resaltar, que los activos se deben agrupar en tipos acorde a la función que realizan con la información, es por este motivo, que se desarrolla un inventario de activos importantes para la gestión de la seguridad de la información donde se obtiene los siguientes activos, para más información se recomienda revisar el documento de gestión de activos:

6.3.2.1 Hardware:

- Servidores.
- Computadores de escritorio.
- Portátiles.

- Impresoras.
- Firewall.
- Switches.
- Access Point.
- Teléfonos IP.
- Líneas Móviles.
- Cámaras de seguridad.
- NVR.
- Smart TV.
- Alarmas de monitoreo.
- Discos Duros de respaldo.

6.3.2.2 Software:

- Backup Cloud.
- CRM.
- Workspace.
- Sistema contable.
- Office 365.
- Páginas Web.
- Antivirus.
- Sistemas operativos.
- Máquinas virtuales.

6.3.2.3 Activo de Información:

- Archivos de datos.
- Manuales de funciones.
- Hojas de vida.
- Documentos internos.
- Material físico.
- Formatos.
- Información en carpetas compartidas en red.

6.3.2.4 Recurso Humano:

- Gerentes.
- Directores.
- Coordinadores.
- Desarrolladores.
- Personal administrativo.
- Ingenieros comerciales.
- Ingenieros operacionales.
- Técnicos.
- Clientes.
- Proveedores.

6.3.2.5 Infraestructura:

- Sedes de la organización.
- Canalización de red eléctrica.
- Canalización de red de datos.

6.3.2.6 Servicios:

- Internet.
- Fluido eléctrico.

6.3.2.7 Propiedad intelectual:

- Marcas.
- Desarrollo de software y hardware.
- Sistemas de gestión de calidad y seguridad y salud en el trabajo.
- RUP.

6.3.3 CODIFICACIÓN DE LOS ACTIVOS.

Se establece una codificación para cada activo de la lista de activos identificados, acorde a su tipo, como se evidencia a continuación:

Activo	**Codificación**

Hardware	HW-##
Software	SW-##
Información	IF-##
Recurso Humano	RH-##
Infraestructura	ES-##
Servicios	SE-##
Propiedad Intelectual	PI-##

Tabla 1, codificación de activos.

6.3.4 CRITERIOS PARA LA VALORACIÓN DE ACTIVOS (IMPACTO).

Basados en la norma ISO/IEC 27005:2008, se requiere establecer una escala que se utilizará y los criterios para la asignación de los valores para cada activo, con base en la importancia para la seguridad de la información, el valor del daño de perder la información contenida en el activo y su valor monetario juegan papeles importantes al momento de definir su valoración. A continuación, se muestra la escala de valoración de acuerdo a lo planteado anteriormente:

Valor Cuantitativo	**Valor Cualitativo**	**Criterio**
4	Crítico	Las consecuencias del daño son extremadamente graves, afectación a toda la organización u obligaciones contractuales.
3	Alto	Las consecuencias del daño son graves, afectación alguna área o sede de la empresa.
2	Medio	Las consecuencias del daño son considerables, afectación a un cargo específico no crítico o a un proceso que puede dar espera.
1	Bajo	Las consecuencias del daño son menores, no interrumpen las actividades de la organización.

Tabla 2, criterios de evaluación de activos.

6.3.5 Valoración de Activos por tipo.

De acuerdo con la tabla anterior y a los parámetros definidos, se asigna valores a los diferentes activos de la organización a continuación:

Tipo de Activo	Descripción del Activo	Valoración del Activo

Hardware	Servidores Principales	4
	Servidores Secundarios	3
	Computadores de escritorio	3
	Portátiles críticos	4
	Portátiles	3
	Impresoras	2
	Firewall	4
	Switches	4
	Access Point	4
	Teléfonos IP	2
	Líneas móviles	2
	Cámaras de seguridad	4
	NVR	4
	Smart Tv	1
	Alarmas de monitoreo	4
	Discos Duros de respaldo	3
Software	Backup Cloud	3
	CRM	4
	Workspace (Google)	4
	Sistema Contable	4
	Office 365	3
	Páginas Web	3
	Antivirus	4
	Sistemas Operativos	4
	Máquinas Virtuales	3
Archivos de In-formación	Archivos de datos	4
	Manuales de funciones	4
	Hojas de vida	4
	Documentos Internos	4
	Material físico	4
	Formatos	4
	Información en carpetas compartidas en red	4
	Gerentes	4

Recursos Humanos	Directores	4
	Coordinadores	4
	Desarrolladores	3
	Personal administrativo	3
	Ingenieros comerciales	3
	Ingenieros operacionales	3
	Técnicos	3
	Clientes	4
	Proveedores Críticos	4
	Proveedores No Críticos	3
Infraestructura	Sedes de la organización	4
	Canalización de red eléctrica	4
	Canalización de red de datos	4
Servicios	Internet	4
	Fluido eléctrico	4
Propiedad intelectual	Marcas	4
	Desarrollo de software y hardware	4
	Sistemas de gestión de calidad y seguridad y salud en el trabajo	4
	RUP	4

Tabla 3, identificación y valoración de activos.

6.3.6 IDENTIFICACIÓN DE LAS AMENAZAS.

Se listan las amenazas, que son las situaciones o fuentes a las que se exponen los activos de información anteriormente mencionados y pueden ocasionar fallas en los tres componentes claves de la información integridad, confidencialidad y disponibilidad:

Accidental (A), deliberada (D) o ambientales (E)

Tipo	Amenaza	Origen
Daño Físico	Incendio	A,D,E
	Daño por agua	A,D,E
	Accidente importante	A,D,E
	Destrucción del equipo	A,D,E

	Polvo, corrosión	A,D,E
Eventos Naturales	Fenómenos sísmicos	E
	Fenómenos climáticos	E
	Fenómenos meteorológicos	E
	Inundación	E
Pérdida de los servicios esenciales	Falla en el sistema de suministro de energía	A,D,E
	Falla en el equipo de telecomunicaciones	A,D
Perturbación debida a la radiación	Radiación electromagnética	A,D,E
	Radiación térmica	A,D,E
	Impulsos electromagnéticos	A,D,E
Compromiso de la información	Interceptación de señales de interferencia comprometedores	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	A,D
	Datos provenientes de fuentes no confiables	A,D
	Manipulación de hardware	D
	Manipulación de software	A,D
	Detección de posición	D
Fallas técnicas	Falla del equipo	A
	Mal funcionamiento del equipo	A
	Saturación del sistema de información	A,D
	Mal funcionamiento del software	A
	Incumplimiento en el mantenimiento del sistema de información	A,D
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso del software falso o copiado	A,D
	Corrupción de los datos	D
	Procesamiento ilegal de los datos	D
Compromiso de las funciones	Error en el uso	A
	Abuso de derechos	A,D

	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	A,D,E
Dirigidas por el hombre	Piratería	D
	Ingeniería social	D
	Crimen por computador	D
	Acto fraudulento	D
	Ataques contra el sistema	D
	DDoS	D
	Penetración en el sistema	D
	Ventaja de defensa	D
	Hurto de información	D
	Asalto a un empleado	D
	Chantaje	D

Tabla 4, amenazas identificadas acorde a la norma ISO/IEC 27005

6.3.7 IDENTIFICACIÓN DE LAS VULNERABILIDADES.

Se listan las vulnerabilidades o debilidades de acuerdo con el tipo de activo asociado:

Tipo	Vulnerabilidad	Ejemplos de amenazas
Hardware	Mantenimiento insuficiente	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de esquemas de reemplazo periódico	Destrucción de equipos o de medios
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Susceptibilidad a las variaciones de voltaje	Pérdida del suministro de energía
	Almacenamiento sin protección	Hurto de medios o documentos
	Falta de cuidado en la disposición final	Hurto de medios o documentos
	Copia no controlada	Hurto de medios o documentos

Software	Ausencia o insuficiencia de pruebas de software	Abuso de derechos
	Defectos bien conocidos en el software	Abuso de derechos
	Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	Abuso de derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de derechos
	Ausencia de pistas de auditoria	Abuso de derechos
	Asignación errada de los derechos de acceso	Abuso de derechos
	Software ampliamente distribuido	Corrupción de datos
	En términos de tiempo utilización de datos errados en los programas de aplicación	Corrupción de datos
	Interfaz de usuario compleja	Error en el uso
	Ausencia de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Ausencia de mecanismos de identificación y autentificación	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
	Ausencia de control de cambios eficaz	Mal funcionamiento del software
	Descarga y uso no controlado de software	Manipulación del software
	Ausencia de copias de respaldo	Manipulación del software
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de medios o documentos
	Falla de la producción de informes de gestión	Uso no autorizado del equipo
Red	Ausencia de pruebas de envío o recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha encubierta
	Tráfico sensible sin protección	Escucha encubierta

	Conexión deficiente de los cables	Falla del equipo de telecomunicaciones
	Punto único de falla	Falla del equipo de telecomunicaciones
	Ausencia de identificación y autenticación de emisor y receptor	Falsificación de derechos
	Transferencias de contraseñas en claro	Espionaje remoto
	Arquitectura insegura de la red	Espionaje remoto
	Gestión inadecuada de la red	Saturación del sistema de información
	Conexiones de red pública sin protección	Uso no autorizado del equipo
Personal	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos o de medios
	Entrenamiento insuficiente en seguridad	Error en el uso
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Ausencia de mecanismos de monitoreo	Procesamiento ilegal de datos
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documentos
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo
Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Destrucción de equipos o de medios
	Ubicación en un área susceptible a inundación	Inundación
	Red energética inestable	Pérdida del suministro de energía
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de equipos
Organización	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de derechos
	Ausencia de procedimiento formal para la revisión de los derechos de acceso	Abuso de derechos
	Ausencia o insuficiencia de disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes	Abuso de derechos

	Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información	Abuso de derechos
	Ausencia de auditorías regulares	Abuso de derechos
	Ausencia de procedimiento de identificación y valoración de riesgos	Abuso de derechos
	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de derechos
	Respuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de acuerdos de nivel de servicio, o insuficiencia de los mismos	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimiento de control de cambios	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimiento formal para el control de documentación del SGSI	Corrupción de datos
	Ausencia de procedimiento formal para la supervisión del registro del SGSI	Corrupción de datos
	Ausencia de procedimiento formal para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables
	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información	Negación de acciones
	Ausencia de planes de continuidad	Falla del equipo
	Ausencia de políticas sobre el uso del correo electrónico	Error en el uso
	Ausencia de procedimientos para la introducción del software en los sistemas operativos	Error en el uso
	Ausencia de registros en las bitácoras (logs) de administrador y operario	Error en el uso
	Ausencia de procedimientos para el manejo de información clasificada	Error en el uso
	Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos	Error en el uso

	Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Procesamiento ilegal de datos
	Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Hurto de equipo

Tabla 5, identificación de vulnerabilidades acorde a la norma ISO/IEC 27005.

6.3.8 VALORACIÓN DE LOS RIESGOS EN LA SEGURIDAD DE LA INFORMACIÓN.

Se lleva a cabo la valoración de riesgos con el objetivo de identificar y evaluar los riesgos a los cuales se enfrenta la organización para la continuidad y seguridad de su negocio. El análisis se realiza a través de la valoración de cada activo, amenaza y vulnerabilidad identificada; el resultado de estas tareas permitirá evaluar los riesgos y establecer los controles y/o tratamiento para minimizar los riesgos a los que se expone la organización.

En esta etapa, se definen los criterios que se tendrán en cuenta para realizar la importancia y la gestión de cada uno de los riesgos que se identifiquen. Los criterios van acorde a la continuidad del negocio, la imagen de la compañía, los objetivos y los recursos existentes para tal fin. Cabe resaltar, que los criterios de riesgo serán revisados constantemente para obtener la visión más acertada hacia las necesidades del negocio y los continuos cambios.

Para definir los criterios del riesgo, se tendrá en cuenta:

- La naturaleza, los tipos de causas y consecuencias que pueden ocurrir.
- Lo atractivo del activo, o el impacto posible aplicable cuando se toma en consideración una amenaza humana deliberada.
- La susceptibilidad de la vulnerabilidad a la explotación, aplicable tanto a vulnerabilidades técnica como no técnicas.

Acorde a los criterios anteriormente planteados, y los activos de información que se involucran en cada uno de los riesgos, se obtiene la siguiente tabla:

			Análisis de Riesgos Inherente			
Amenaza	**Vulnerabilidad**	**Riesgo**	**Impacto**	**Probabilidad**	**Riesgo**	**Nivel de Riesgo**

Incendio	Falta de elementos contra incendios	Quemado de dispositivos, haciendo que toda la información se pueda perder afectando la continuidad del negocio	4	4	16	**Crítico**
Daño por agua	Ausencia de buen uso de activos	Daño de dispositivos por agua, haciendo que la información contenida en ellos se pueda perder parcial o totalmente afectando la continuidad del negocio	3	5	15	**Severo**

Tabla 6, valoración de riesgos (Anexo Gestión de Riesgos).

Para información más detallada sobre la valoración de riesgos, revisar anexo *GESTIÓN DE RIESGO*.

6.3.9 TRATAMIENTO DE RIESGOS MEDIANTE LA IMPLEMENTACIÓN DE CONTROLES.

Para gestionar las amenazas identificadas, se procede a determinar la acción a realizar con el riesgo sí será reducido, transferido, eliminado o aceptado. A partir de esto, se implementan los controles necesarios del anexo A de la norma ISO/IEC 27001 que permitirán reducir los riesgos plasmados en el documento de análisis de riesgos.

En la tabla de declaración de aplicabilidad se determinan los controles necesarios para fortalecer la seguridad de la información de la organización, como se plasma en la siguiente tabla:

ISO 27001:2022 CONTROLES DE SEGURIDAD	NUM	DESCRIPCIÓN	EXCLUSIÓN (SI/NO)	JUSTIFICACIÓN DE EXCLUSIÓN	¿QUÉ?	¿CÓMO?	RESPONSABLE

DE LA INFORMACIÓN							
Controles Tecnológicos	A8,8	Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a tales vulnerabilidades y se deben tomar las medidas apropiadas.	NO		GARANTIZAR LA CONTINUA GESTIÓN DE VULNERABILIDADES TÉCNICAS	INFORMES DE VULNERABILIDADES MENSUALES	SANTIAGO PABON
Controles Tecnológicos	A8,12	Las medidas de prevención de fuga de datos se aplicarán a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.	NO		ESTABLECER HERRAMIENTAS QUE NO PERMITAN LA FUGA DE DATOS	PROTECCIÓN ENDPOINT	SANTIAGO PABON
Controles Tecnológicos	A8,20	Las redes y los dispositivos de red se asegurarán, administrarán y controlarán para proteger la información en los sistemas y aplicaciones.	NO		GARANTIZAR EL FUNCIONAMIENTO SEGURO DE LA RED	FIREWALL	SANTIAGO PABON

Tabla 7, controles definidos para gestionar riesgos y asignación de responsable (Anexo Declaración de aplicabilidad).

Para más información sobre los controles implementados y su responsable. Consultar el anexo de declaración de aplicabilidad.

De esta forma, se asigna responsables que permitan garantizar la implementación, comunicación y medición de cumplimiento de cada uno de los controles aplicables para INSITEL S.A.

6.3.10 DESARROLLO DE CONTROLES.

Para los controles mencionados anteriormente, se utilizan las siguientes herramientas:

NUM DE CONTROL	HERRAMIENTA
A8.8	Nessus
A8.12	Sophos
A8.20	Sophos

Tabla 7, herramientas utilizadas para los controles.

En el caso del control A8.8, se implementa la herramienta Nessus, la cual consiste en un agente desplegado en un equipo que comprueba diferentes plugins relacionados con las vulnerabilidades de bases de datos como CVE (Common Vulnerabilites and Explosure) a diferentes IPs de la compañía, se establece una frecuencia mensual para el análisis de vulnerabilidades, entrega de informe sobre las vulnerabilidades encontradas en cada activo analizado y período de mitigación de vulnerabilidades.

En cuanto a la protección de fuga de información, se implementa en cada dispositivo portátil registrado en el inventario de activos, agendes endpoint con varias funcionalidades, entre ellas, se incluye la protección contra malware, la prevención de fuga de información, control de periféricos, control de aplicaciones; entre otros.

Por último, se garantiza una segmentación de la red interna de INSITEL S.A. mediante el uso de un Next Generation Firewall, que permite establecer políticas de comunicación entre las diferentes Vlans que separan los ambientes de la red de la organización. Por ejemplo, la red de invitados, está totalmente aislada de la red utilizada por los colaboradores internos de la organización; con el fin de evitar posibles ataques desde la red abierta que se entrega a los invitados, así mismo, se aísla el segmento asignado a los servidores de la compañía.

6.4 DISEÑAR EL SGSI ALINEADO A LA NORMATIVA DE LA SERIE ISO/IEC 27000.

Para la búsqueda de la mejora continua y establecer acciones de mejorada que permitan fortalecer el

SGSI, se implementaron las siguientes acciones:

6.4.1 CAPACITACIÓN DE AUDITORÍAS INTERNAS

Se realiza un programa de doce (12) horas de capacitación con certificación de auditores internos para diez (10) empleados de INSITEL S.A. que facilita la evaluación autónoma del Sistema de Gestión de Seguridad de la Información (SGSI) y establecer acciones de mejora que fortalezcan la postura de seguridad de la información y ciberseguridad de la organización.

6.4.2 AUDITORÍA INTERNA Y EXTERNA

En un lapso de tres (3) meses posteriores a la implementación de los controles aplicados a la organización, se realizará una auditoría interna que permita establecer observaciones, acciones de mejora y/o no conformidades cada una de las cláusulas y los controles relacionados con el Sistema de Gestión de Seguridad de la Información enfocado en la norma ISO/IEC 270001:2022; lo que permitirá medir la efectividad de los controles implementados y calcular el porcentaje completado de los objetivos definidos. Acorde a los resultados de la auditoría interna, se realizarán las mejoras pertinentes para fortalecer el SGSI, garantizando así, la mejora continua del sistema para proteger la información de INSITEL S.A.

7. CONCLUSIONES

A lo largo del tiempo de ejecución del proyecto, se ha destacado la importancia de un enfoque sistemático y estructurado para proteger tanto los activos de información como la propia información, por lo que se concluyen los siguientes puntos:

- La implementación de un sistema de gestión de seguridad de la información tiene como objetivo identificar, valorar, gestionar y disminuir tanto el impacto como la probabilidad de que se presente incidentes que puedan afectar la seguridad de la información.
- Los controles tecnológicos fortalecen los conocimientos telemáticos y de redes debido a que su implementación debe alinearse a las necesidades de la organización para garantizar la seguridad de la información en cada una de las capas del modelo OSI y minimizar el impacto para el desarrollo de las actividades de la empresa.
- La correcta valoración y tratamiento de riesgos facilitan gestionar un plan de acción para mejorar la postura de seguridad de la información, debido a que brinda herramientas y análisis para entender el contexto de la compañía.
- Se ha fortalecido la cultura de seguridad en la organización, fomentando la responsabilidad y el

compromiso de todos los miembros del equipo.

8. REFERENCIAS.

[1] Ladino, M. I., Villa, P. A., & López, A. M. (2011). Fundamentos de ISO 27001 y su aplicación en las empresas. Scientia et technica, 17(47), 334-339.

[2] Olmedo, J. I., & Gavilánez, F. L. (2018). Análisis de los ciberataques realizados en América Latina. INNOVA Research Journal, 3(9), 172-181.

[3] Cárdenas-Solano, L. J., Martínez-Ardila, H., & Becerra-Ardila, L. E. (2016). Gestión de seguridad de la información: revisión bibliográfica. Profesional de la información, 25(6), 931-948.

[4] Figueroa-Suárez,J. A., Rodríguez-Andrade, R. F., Bone-Obando, C. C., & Saltos-Gómez, J. A. (2018). La seguridad informática y la seguridad de la información. Polo del conocimiento, 2(12), 145-155.

[5] López, P. A. (2010). Seguridad informática. Editex.

[6] Valencia-Duque, F. J., & Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. Revista Ibérica de Sistemas e tecnologías de Informação, (22), 73.

[7] Soriano, M. (2014). Seguridad en redes y seguridad de la información. Obtenido de http://improvet. cvut. cz/project/download/C2ES/Seguridad_de_Red_e_Informacion. pdf.

[8] Santiago, E. J., & Allende, J. S. (2017). Riesgos de ciberseguridad en las empresas. Tecnología y desarrollo, (15), 10.

[9] Krishna Kishore, P., Ramamoorthy, S., Rajavarman, V.N. (2023). ARTP: Anomaly based real time prevention of Distributed Denial of Service attacks on the web using machine learning approach. International Journal of Intelligent Networks, Volume 4, 38-45.

[10] Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z., & Kifayat, K. (2021). A comprehensive survey of AI-enabled phishing attacks detection techniques. Telecommunication Systems, 76, 139-154.

[11] Doig Díaz, D. F., Mendoza Blanco, J. C., Mendoza Pasco, J. L., & Yañez Herrera, D. A. (2019). Escenarios de aprendizaje competitivo a través de uso de elementos lúdicos para estrenamiento en ciberseguridad.

[12]Yang, G. (2023) A review of Machine Learning-based zero-day attack detection: Challenges and future directions. Computer Communications, Volume 198, 175-185. DOI: https://doi.org/10.1016/j.comcom.2022.11.001

[13] Aslan, Ö. A., & Samet, R. (2020). A comprehensive review on malware detection approaches. IEEE Access, 8, 6249-6271. DOI:10.1109/ACCESS.2019.2963724.

[14] Rivera-Guevara, R. P. (2018). Deteccion y Clasificacion de Malware con el Sistema de Análisis de Malware Cuckoo (Master's thesis).

[15] Ordieres, J,. Wolff, A., Pacios, A,. Bello, A. (2022). Cybersecurity challenges in downstream steel production processes. IFAC-PapersOnLine. No 40(55), 283-288. DOI:

https://doi.org/10.1016/j.ifacol.2023.01.086.
[16] Urbanovics, A., & Guajardo, R. (2022). Estrategias de ciberseguridad en los paises latinoamericanos–un análisis comparativo. Acta Hispanica, (IV), 89-104.
[17] Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: an overview from machine learning perspective. Journal of Big data, 7, 1-29.

9. ANEXOS.

- Norma ISO/IEC 27001:2022.
- Norma ISO/IEC 27002:2022.
- Norma ISO/IEC 27005:2008.
- Política general de seguridad de la información.
- Alcance SGSI.
- Objetivos SGSI.
- Gestión de riesgos.
- Declaración de aplicabilidad.