DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA GINSAC COLOMBIA SAS

JHONATAN FABIAN CRUZ CONDE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUÉ
2023

DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA GINSAC COLOMBIA SAS

JHONATAN FABIAN CRUZ CONDE

Proyecto de Grado Aplicado–presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

EDUARD MANTILLA
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUÉ
2023

NOTA DE ACEPTACIÒN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Ibagué, 2023

DEDICATORIA

Esta dedicatoria es primero que todo para Dios y la Virgen que me han guiado por el buen camino de la vida y me han permitido llegar al éxito con su bendición.

A mis padres Flor Alba Conde, Gloria Arias Narváez, José Elver Cruz, que gracias a ellos y a su gran apoyo incondicional he podido cumplir mis sueños, forjando mi camino, han llenado mi vida de mucho amor y esperanza.

Mi esposa Nathalia Ducuara, por el amor y su alegría tan inmensa que me regala a diario, de su mano hemos podido cumplir muchos sueños y éxitos. Hoy más que nunca quiero desearle todos mis logros.

Mis hermanos, toda mi familia y amigos, por brindarme su apoyo, por su compañía y por desearme siempre lo mejor.

En especial mi dedicatoria es para Christopher Bermúdez y Yina Conde.

Por todos ustedes mi esfuerzo, amor y dedicación.

AGRADECIMIENTOS

Agradezco a mis tutores, directores y a todos mis compañeros, que, con su sabiduría, esfuerzo, acompañamiento, consejos me han brindado las mejores bases para mi formación, logrando importantes objetivos, culminar un proyecto de vida propuesto y sin su colaboración no hubiera sido posible.

A las directivas de la Universidad Nacional Abierta y a Distancia UNAD, que gracias a la gestión y oportunidades que brindan para acceder a una educación digna y con los mejores estándares de calidad, hoy somos miles de jóvenes que han podido cumplir el sueño de obtener un título profesional.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

Activos: Bienes, recursos, derechos, información, datos, etc. que forman y componen los sistemas de información y son esenciales para el funcionamiento de los proceso y actividades de la estructura informática de una compañía.

Amenaza: Es el evento que tiene el potencial de realizar el mayor daño posible a un sistema informático, dejando daños impredecibles.

Análisis de riesgos: Es el estudio e identificación de los activos de los sistemas de información que presenta un estado crítico, debilidades o posibles amenazas que puedan comprometer el funcionamiento del sistema de información.

Ataque: Acción no autorizada con fines delincuenciales y con objetivos de destruir, sabotear sistemas de información o estructuras informáticas.

Confidencialidad: Solo podrán acceder a los recursos de la información y tecnológicos, solo aquellos que integren elementos y accesos autorizados.

Disponibilidad: Los recursos y sistemas deben estar siempre activos y accesibles por elementos autorizados, con seguridad, privacidad y sin interrupciones.

Evaluación de riesgos: Identificados los riesgos que comprometen los sistemas de información, evaluándose frente a la medida de seguridad, de esta manera obtener el nivel de riesgo y el impacto para la seguridad de la información.
Formado por varias metodologías, documentos, software, hardware, que determinan que los accesos a recursos de un sistema sean llevados a cabo por elementos y accesos autorizados. Todo sin comprometer la confidencialidad, autenticidad e integridad de la infraestructura computacional, ya que se vería comprometidos en riesgos y amenazas
Garantiza la seguridad por cada mensaje transmitido o almacenado en el sistema, sólo podrá ser leído por el destinatario.

Gestión de riesgo: Actividades, controles y procesos coordinados para dirigir, administrar, controlar y mitigar el impacto de una amenaza de seguridad[1].
Identificación de activos: Es el proceso de identificación de los recursos que forman parte del sistema de información de una organización y que son necesarios para el desarrollo de actividades y el funcionamiento de una empresa. (Servidores, aplicaciones, instalaciones, datos, etc.)

[1] SYSTEM ADMINISTRADOR. Qué es el riesgo de Seguridad de información. LD GRUPO (blog) [EN LINEA]. (10, abril, 2019). [Consultado el 10, octubre, 2022]. Disponible en Internet: <https://www.ldgrupo.com.pe/que-es-el-riesgo-de-seguridad-de-informacion/>.

Integridad: Los recursos del sistema o estructuras tecnológicas solo podrán acceder con el personal y elementos autorizados.
Resguarda la información y asegura la confidencialidad, minimizando el riesgo de vulnerabilidad y amenazas.

Riesgo: Identificación de amenaza o vulnerabilidad de un activo informático siendo expuesto con una probabilidad de ocurrencia o impacto frente al activo.

Seguridad de la información: Conjunto de medidas y controles que permiten resguardar la información y protegerla. Además de evaluar los riesgos y amenazas que puedan estar expuestas.

Seguridad Informática: Conocida también como ciberseguridad, es la medida que impide la ejecución y acceso al sistema, red, procesos, recursos, etc. De manera No autorizada.

SGSI: Conjunto de políticas, procedimientos, normas, directrices que buscan proteger la información, preservando la confidencialidad, disponibilidad e integridad en el tratamiento y uso de la información.[2]

Vulnerabilidad: Son fallos o debilidades en un sistema de información que pueden ser aprovechados por exploint permitir a un atacante comprometer y poner en riesgo la seguridad de los sistemas de información de una organización.

[2] ¿QUÉ ES un sistema de Gestión de la Seguridad de la información (SGSI)? [Anónimo]. LISOT [EN LINEA]. (14, mayo, 2018). [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://www.lisot.com/que-es-un-sistema-de-gestion-de-la-seguridad-de-la-informacion-sgsi/>.

RESUMEN

El proyecto está orientado al diseño del sistema de gestión de la seguridad de la información (SGSI) para la organización Ginsac Colombia SAS, realizando un estudio de seguridad informática en la organización, identificando las fortalezas y las debilidades de seguridad en los procesos de las tecnologías de información, evaluando la efectividad que garantizará un mayor grado de eficiencia, eficacia, confidencialidad, integridad para la toma de decisiones de los sistemas de información.

Con la identificación, valoración y recolección de información se da inicio al sistema de gestión de seguridad de la información, que contará con los controles y acciones pertinentes en la gestión y tratamiento de riesgos, la preservación de los pilares de la seguridad (Confidencialidad, Integridad, Disponibilidad), permitirá monitorear y responder a incidentes o amenazas que pongan en riesgo la funcionalidad de los proceso y sistemas de Ginsac Colombia SAS.

El diseño del SGSI resalta la necesidad, el interés y la mayor responsabilidad de la alta dirección de GINSAC COLOMBIA para aprobar y mejorar la infraestructura y seguridad tecnológica. Se realiza un inventario de activos relacionados con el entorno informático, se realiza una evaluación de riesgos y se proponen estrategias, controles, proyectos y políticas para minimizar los riesgos que amenazan con la seguridad y continuidad de la compañía.

El diseño del sistema de gestión de la seguridad de la información y su buena implementación con los controles y políticas de seguridad, determinan el alcance y nivel de cumplimiento frente a la seguridad de la información que rige la ISO/27001, con las mejores prácticas de seguridad, apoyados a la metodología MAGERIT para obtener un análisis y gestión de riesgo acordes a las necesidades de GINSAC, adicional permite mejorar los planes de mitigación de riesgos. Las buenas prácticas de la ISO/IEC 27001 y MAGERIT Permitirán evaluar el impacto y proponer las recomendaciones necesarias para obtener un nivel superior en seguridad, madurez gestión y cumplimiento. Lo sistemas de información serán confiables y seguros dentro de la organización Ginsac Colombia SAS.

Palabras claves: Activos, Datos, ISO/IEC 27000, Seguridad de la información, Vulnerabilidad.

ABSTRACT

The project is oriented to the design of the information security management system (ISMS) for the organization Ginsac Colombia SAS, carrying out an information security study in the organization, identifying the security strengths and weaknesses in the technology processes. of information, evaluating the effectiveness that will guarantee a greater degree of efficiency, effectiveness, confidentiality, integrity for the decision making of the information systems.

With the identification, assessment and collection of information, the information security management system begins, which will have the pertinent controls and actions in the management and treatment of risks, the preservation of the pillars of security (Confidentiality, Integrity, Availability), will allow monitoring and responding to incidents or threats that put at risk the functionality of the processes and systems of Ginsac Colombia SAS.

The design of the ISMS highlights the need, interest and greater responsibility of GINSAC COLOMBIA's senior management to approve and improve infrastructure and technological security. An inventory of assets related to the IT environment is carried out, a risk assessment is carried out and strategies, controls, projects and policies are proposed to minimize the risks that threaten the security and continuity of the company.

The design of the information security management system and its proper implementation with security controls and policies, determine the scope and level of compliance with regard to information security governed by ISO/27001, with the best practices of security, supported by the MAGERIT methodology to obtain an analysis and risk management according to the needs of GINSAC, additionally allows improving risk mitigation plans. The good practices of ISO/IEC 27001 and MAGERIT will make it possible to assess the impact and propose the necessary recommendations to obtain a higher level of security, management maturity and compliance. The information systems will be reliable and secure within the Ginsac Colombia SAS organization.

Keywords: Assets, Data, ISO/IEC 27000, Information Security, Vulnerability.

INTRODUCCIÓN

En el desarrollo del sistema de gestión de la seguridad de la información para la organización Ginsac Colombia SAS, se podrá conocer la eficiencia en servicio de la compañía relacionada con su crecimiento en el agro Colombia. Se estable el alcance del SGSI, se realiza una evaluación y el estado de sus sistemas informáticos, se hace la identificación de activos, la medición en seguridad etc. Además del diseño para una política bases que serán parte fundamental para el SGSI y la confiabilidad de sus sistemas informáticos.

El diseño del SGSI resaltará la eficacia de los objetivos de la organización con las buenas prácticas y controles en seguridad que serán alineado con la norma ISO/IEC 27001:2013 y la metodología MAGERIT, con el objetivo principal de establecer análisis y estrategias de gestión más adecuadas para los requerimientos de la compañía.

Ginsac es una compañía que se ha convertido con el pasar del tiempo en un aliado estratégico para el sector agrícola de Colombia, durante los últimos años ha tomado fuerza y su crecimiento ha sido aceptable, pero ha dejado a un lado el crecimiento, innovación y sobre todo la seguridad de su entorno informático. El diseño del SGSI ayudará a identificar los riesgos a los que está expuesto, resaltará el activo más importante y al cual se le debe dar el mayor valor y seguridad como lo es los datos e información, le permitirá aumentar el nivel de madurez de los sistemas de información, contará con controles y proyectos en seguridad periódicas y administrables y sobre todo que podrá ser una empresa garante en seguridad informática y fiable en sus sistemas de información y servicios, todo relacionado con el compromiso de la alta gerencia de la compañía.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Ginsac Colombia SAS es una empresa legalmente constituida, actualmente con presencia en el territorio colombiano con 6 sedes, con aliados de marca en Perú y Ecuador, cuenta con una estructura tecnológica encargada de almacenar y gestionar toda clase de información y un sistema informático que centraliza el funcionamiento de la empresa con las aplicaciones necesarias en el desarrollo de las actividades.

En la auditoría realizada, se pudo evidenciar riesgos y problemas con alto nivel de madurez en la seguridad y tratamiento de los sistemas de información de la compañía. Se evidencia que solo el 40% de los datos cuentan con la seguridad adecuada para el manejo de los procesos de la compañía en los que se resalta el sistema contable y nómina de SIESA, HELISA y Servidor Local.

El 20% de los datos que están almacenados en servidores WEB para aplicaciones y plataformas basadas en la nube, cuentan con una seguridad intermedia, en las que se puede resaltar desarrollos propios como IRIS (Plataforma para gestión operativa) e INTRANET (Cotizador y Gestor para áreas comerciales).

El 30% de la información esta almacenada en equipos tecnológicos de la compañía que son asignados a sus colaboradores para el buen manejo de los procesos y operatividad de la compañía. Siendo este unos de los mayores problemas en fallas de seguridad en los sistemas de información por la perdida y mal uso de la información, la compañía y el área de las TI no tienen el control y la seguridad total para cada equipo tecnológico asignado, del mismo modo los equipos tecnológicos físicos están siendo vulnerados por software y navegaciones maliciosas y no autorizados, falla en seguridad por personal interno de la organización.

El 10% de la información almacenado por documentos físicos, no han sido digitalizados, su seguridad es mínima, con accesibilidad a personal no autorizado.

Por otra parte, los entornos y estructuras informáticas de cada una de las sedes de la organización presentan una seguridad básica sin gestión, control y administración total por parte del área de las TI. Siendo este un factor importante a mejorar y alinear en el diseño del SGSI para Ginsac.

La necesidad de evaluar y gestionar el estado de seguridad en los procesos de tecnología de información en el que se encuentra, hacen necesario el diseño de un sistema de gestión de la seguridad de la información, que permita optimizar los recursos informáticos, mitigar riesgo, amenazas, vulnerabilidades o incidentes de seguridad en los sistemas informáticos, hasta la fecha no cuenta con políticas y

controles de seguridad de la información, razones por las que aún existen riesgos sin controles y procedimientos sin gestión que se encarguen de mitigar los riesgos a un nivel aceptable dentro de la organización Ginsac Colombia SAS.

1.2 **FORMULACIÓN DEL PROBLEMA**

¿Cómo el diseño del sistema de gestión de la seguridad de la información (SGSI) alineados con la normativa del estándar de la ISO/IEC 27001:2013, ayudarán a minimizar riesgos, amenazas y vulnerabilidades, a proteger la información y garantizar sistemas confiables y seguros en la organización Ginsac Colombia SAS?

2 JUSTIFICACIÓN

Proteger y asegurar la información (Física y digital) y siendo los datos el activo más importante de cualquier organización, se ha convertido en una obligación y requisito para contar con sistemas confiables y eficientes. Con los controles y normativas de la ISO/27001 y la buena implementación en la organización Ginsac Colombia SAS, podrá contar con un mayor nivel de seguridad, mejor posicionamiento, mayor nivel de confianza con sus sistemas de información.

La implementación del sistema de gestión de la seguridad de la información es una decisión estratégica que permite garantizar un mayor nivel de protección de la información que asocia a toda la organización y que debe estar dirigida y apoyada por la alta dirección de Ginsac Colombia SAS[3].

El sistema de gestión de la seguridad de la información permite analizar y ordenar toda la estructura informática, facilita los procedimientos de trabajo, dispone de controles que permiten medir la eficiencia y eficacia de las medidas tomadas. Estas acciones de seguridad proporcionan un mayor nivel de competitividad, rentabilidad, prestigio, madurez, que permiten preservar la confidencialidad, integridad y la disponibilidad de la información, a su vez se asegura que los riesgos se encuentren en un nivel aceptable y asumible por la organización.

Ginsac Colombia SAS se posiciona como un aliado estratégico para el campo colombiano, procurando que sus clientes se sientan acompañados para sus labores de campo. Ginsac Colombia viene crecido en los últimos años, mejorando sus instalaciones, aumentando su productividad y servicios, pero no le han dado el valor que se merece el uso y tratamiento de la información, un mal uso o incidente pondrían en riesgo la funcionalidad e integridad de las actividades de operación en la organización.

El diseño de un sistema de gestión de seguridad de la información ayudará a fortalecer los procesos de las tecnologías de información, mejorar la calidad de los servicios y actividades dentro y fuera de Ginsac, mejorar el valor de importancia de las tecnologías de información, alinear objetivos con la dirección y garantizar una estructura informática garantes de la seguridad de la información.

Se pondrá en práctica los conocimientos obtenidos en la formación académica, se dará cumplimiento a las directrices de seguridad con la implementación de una valiosa herramienta como es la ISO/27001, se obtendrá experiencia, habilidades y un mayor conocimiento en los procesos de revisiones y evaluación de los sistemas informáticos relacionado con los procesos de seguridad de información.

[3] INCIBE. Guia_apoyo_SGSI.pdf. (30, mayo, 2022). [Consultado el 21, junio, 2022]. Disponible en Internet: <https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf>.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

- Diseñar un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001:2013, para la organización Ginsac Colombia SAS.

3.2 OBJETIVOS ESPECÍFICOS

- Analizar la situación actual de la organización Ginsac Colombia SAS, en cuanto a seguridad de la información para definir el alcance.

- Elaborar el inventario de activos que serán acobijados por el sistema de gestión de la seguridad de la información.

- Evaluar los riesgos informáticos del inventario de activos, a partir de la metodología Magerit.

- Proponer políticas de seguridad bases para el sistema de gestión de la seguridad de la información (SGSI), basado en el estándar de la ISO/IEC 27001.

4 MARCO REFERNCIAL

4.1 **MARCO TEÓRICO**

En el diseño del sistema de gestión de la seguridad de la información se referencian conceptos, que independientemente del tamaño o tipo de organización son esenciales para lograr los objetivos y contar con sistemas confiables.

4.1.1 Norma ISO/IEC 27001

Es la norma internacional permite implementar el sistema de gestión de seguridad de la información (SGSI) con una correcta evaluación de riesgos, alineados con controles necesarios para mitigar los riesgos, amenazas y vulnerabilidades de los sistemas de información. La ISO 27001 fomenta la seguridad de la triada de la información (Confidencialidad, Integridad y Disponibilidad) y de los sistemas que procesan la información[4], la ISO 27001 es certificable para cualquier organización que desee proteger sus activos, que influya en sus necesidades y objetivos de seguridad de la información, con la implementación, mejora y administración de un SGSI.

4.1.1.1 Alcance

La norma ISO/IEC 27001 establece los requisitos para implementar, mejorar, mantener y administrar un sistema de gestión de la seguridad de la información, la norma también establece los requisitos para la evaluación y el tratamiento adecuado en los riesgos de seguridad de la información y es aplicable para cualquier organización sin importar el tamaño, tipo, naturaleza, área, etc.

4.1.2 Sistema de Gestión de la Seguridad de la Información (SGSI)

El sistema de gestión de la seguridad de la información es el conjunto de normas, directrices y políticas de la administración de la información que busca proteger los activos de la información esenciales para una organización, también denominada (ISMS) Information Security Management System.[5]

---

[4] ISO 27001 - Software ISO 27001 de Sistemas de Gestión [Anónimo]. Software ISO [EN LINEA]. [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/>.

[5] FIRMA-E. ¿Qué es un SGSI – Sistema de Gestión de Seguridad de la Información? | Firma-e. Firma-e | Proyectos y formación [EN LINEA]. (19, febrero, 2013). [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://www.firma-e.com/blog/que-es-un-sgsi-sistema-de-gestion-de-seguridad-de-la-informacion/>.

El SGSI alineado con el estándar internacional ISO/IEC 27001, le permite implementar, monitorear, operar, gestionar, administrar, revisar, mejorar, mantener la seguridad de la información y lograr cumplir las metas y objetivos propuestas por una organización.

Es importante que el SGSI se emplee y se alinea con los procesos y sistemas de una organización, que la seguridad de la información se aplique y se tenga presente en todas las actividades, áreas de trabajo, datos, recursos, procesos, diseños, etc. y el crecimiento del SGSI sea correspondientes a las necesidades de la organización[6].

El SGSI resguarda los pilares de la información (Confidencialidad, Integridad, Disponibilidad) con buenas prácticas en la gestión de riesgo, los pilares son la clave para el buen uso y administración de la información, que garantizaran sistemas de información confiables.

4.1.2.1 Pilares de la seguridad de la información

- Confidencialidad: Es el pilar de seguridad que resguarda la información, garantiza la seguridad por cada mensaje transmitido o almacenado en el sistema, no se pone a disposición ni se revela, minimiza el riesgo de vulnerabilidad y amenazas, solo podrán acceder a los recursos de la información, aquellos que integren elementos y accesos autorizados.

- Integridad: Es el pilar de seguridad que permite mantener protegida la información y recursos del sistema de manera original sin modificaciones o alteraciones no autorizadas que busquen vulnerar y comprometer los sistemas de información de una organización.

- Disponibilidad: Es el pilar de seguridad que permite que los recursos y sistemas deben estar siempre activos y accesibles por el personal o procesos autorizados, con seguridad, privacidad y sin interrupciones.

[6] ISO/IEC 27001:2013(EN) Information technology — Security techniques — Information security management systems — Requirements [Anónimo]. Online Browsing Platform (OBP) [EN LINEA]. [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en>.

Figura 1. Pilares de la seguridad de la información

Fuente: Baja Consulting, «ISO 27000», accedido 15 de junio de 2022 https://www.bajacg.com/uncategorized/iso-27000/.[7]

4.1.2.2 Ciclo de mejora continua

La información de la organización debe mejorar de manera idónea y continua frente a las necesidades en seguridad de información que requiera la organización, con la implementación de la ISO/IEC 27001 implementará y se mejorará el SGSI con el ciclo de Deming o PDCA (Plan – Do – Check - Act) “Planificar – Hacer – Verificar - Actuar”, direccionados por un conjunto de fases que permite medir el grado de gestión de la seguridad alcanzado[8].

Planificar (Plan): Es la fase donde se planifica el Sistema de Gestión de la seguridad de la información y se llevarán a cabo análisis y contexto de la organización, definición de objetivos y políticas.

- Identificar los objetivos de la organización
- Establecer el alcance del SGSI
- Definir las políticas de seguridad de la información
- Identificar y evaluar los activos

[7] ISO 27000 [Anónimo]. Baja Consulting Group [EN LINEA]. (20, agosto, 2017). [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://www.bajacg.com/uncategorized/iso-27000/>.

[8] F. L. GÓMEZ Y. R. P. FERNÁNDEZ. Cómo implantar un SGSI según une-en ISO/IEC 27001 y su aplicación en el esquema nacional de seguridad. E-Libro [EN LINEA]. (2018). Disponible en Internet: <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/53624>.

- Realizar análisis y evaluación de riesgos

Hacer (Do): Es la fase donde se implementa y se pone en función el SGSI, tomando las políticas, controles que han sido identificados para hacerlas cumplir en el SGSI.

- Generar e implementar el plan para mitigación de riesgos
- Implantar el sistema de gestión de la seguridad de la información
- Establecer los controles de seguridad
- Formación y concienciación

Verificar (Check): Es la fase donde se revisa y se monitorea el SGSI, validando que los controles y procesos definidos se ejecuten de la manera prevista y que se estén cumpliendo con los objetivos realizados en el SGSI.

- Revisión del SGSI
- Monitoreo del SGSI
- Realizar auditoria internas

Actual (Act): Es la fase que mantiene y mejora el SGSI de acuerdo con los incidentes o fallas presentadas en los procesos detectados.

- Aplicación de mejoras continuas
- Acciones correctivas

Figura 2. Ciclo Deming o PDCA

Fuente: ARDANZA, Aitziber. Ciclo PDCA de gestión de la ISO 27001. GlobalSuite Solutions [EN LÍNEA]. (10, enero, 2022). [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://www.globalsuitesolutions.com/es/ciclo-pdca-iso-27001/>.

4.2 MARCO CONCEPTUAL

4.2.1 Activos

Los activos para el sistema de Gestión de la Seguridad de la Información (SGSI), Son los recursos para un sistema de información y son necesarios para el funcionamiento y alcance de los objetivos propuestos por la organización[9].
Para el sistema de gestión de la seguridad de la información podemos definir algunos de los activos más importantes y que serán necesarios para la funcionalidad del SGSI.

- Activos de información
- Activos de software
- Activos físicos
- Servicios
- Personas
- Activos intangibles

4.2.2 Inventario de activos

La norma ISO/IEC 27001 hace referencia que todos los activos de información deben Identificarse de forma clara y se debe de realizar un inventario y contar con periodicidad en el mismo en donde se reflejen todos los activos de información que hacen parte esenciales para el funcionamiento de la organización y que serán sujetas al Sistema de Gestión de la Seguridad de la Información (SGSI).

La empresa debe de tener identificados todos los activos y documentos en función a la importancia y labor. El inventario de activos debe acoger toda la información que sea importante para el funcionamiento de la empresa, además de poder recuperarse frente algún incidente informático o desastre natural.
En el inventario se debe alojar características importantes del activo como (Tipo de archivo, ubicación, peso, origen, funcionalidad, responsable, Información de licencia, respaldo, valor, compatibilidad, etc.).

Los inventarios de los activos deben de ser monitoreados y su responsable debe de aceptar y documentar la información que es fundamental para la empresa y que permitirá mejorar su valor, debido a esto se debe dar una clasificación de seguridad por el tipo de activo, por la importancia y el que juega para los procesos de la

[9] EXCELLENCE, ISOTools. ISO 27001: Los activos de información. PMG SSI - ISO 27001 [EN LINEA]. (30, marzo, 2015). [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://www.pmg-ssi.com/2015/03/iso-27001-los-activos-de-informacion/>.

empresa, para esto se clasifican por niveles de protección que ayudaran a cuidar la integridad del SGSI que será implementado en la empresa[10].

La importancia de realizar y mantener un inventario de activos ayudará a las tecnologías de información de la organización a contar con niveles superiores en seguridad y protección de la información, sistemas más eficientes, prevención laboral, mayor gestión en riesgos, etc. Beneficios obtenidos por una buena implementación y las buenas prácticas del SGSI basados en la norma ISO/IEC 27001.

4.2.3 Alcance del SGSI

El alcance para el sistema de gestión de la seguridad de la información aclara los límites, contexto, ubicación e importancia de los activos críticos que hacen parte del SGSI de la organización, además de los riesgos que son asociados a cada activo (Propios o externos), se debe de tener en cuenta todos los flujos de información que sobresalgan de los limiten y del alcance del SGSI.

4.2.4 Políticas del SGSI

Las políticas del sistema de gestión de la seguridad de la información establecen y confirman el compromiso que tiene la alta dirección de la organización frente a los objetivos y metas propuestos en seguridad de la información aplicados en el SGSI, además de contar con mejoras continuas frente aspectos e incidentes relevantes que puedan poner el riesgo los sistemas de información de una organización.
La alta dirección de la organización en el desarrollo de las políticas de seguridad puede optar por políticas de tipo gobierno únicas, de tipo sucinta, de tipo amplia-general, que sean alineados a las normas ISO u optar por políticas con enfoques diferentes.

4.2.5 Evaluación de riesgos

La evaluación de riesgos que son aplicados en el sistema de gestión de la seguridad de la información identifica los riesgos que comprometen los sistemas de información, evaluándose frente a la medida de seguridad, de esta manera obtener el nivel de riesgo y el impacto para la seguridad de la información.
Cada organización puede determinar cual deberá ser el proceso más adecuado aplicando ayudas de las normas ISO/IEC 27005, ISO/IEC 31000, factor importante para un proceso de auditoría donde se deberá evidenciar el proceso de evaluación,

[10] EXCELLENCE, ISOTools. ¿Cómo clasificar los activos de seguridad en un SGSI? PMG SSI - ISO 27001 [EN LINEA]. (6, mayo, 2015). [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://www.pmg-ssi.com/2015/05/como-clasificar-los-activos-de-seguridad-en-un-sgsi/>.

identificación y análisis de riesgos que ponen en peligro los activos de información de la organización. Una buena identificación y evaluación de riesgos priorizar los activos más relevantes y el alcance sobre estos.

El proceso de evaluación de riesgos se debe de realizar de manera periódica, contar con revisiones constantes requeridas frente a los cambios que se produzcan en la organización, le permitirá contar con un enfoque preventivo y aplicar acciones que permitan mitigar el impacto de nuevas amenazas.

4.2.6 Tratamiento de riesgos

Para el sistema de gestión de la seguridad de la información la evidencia y las políticas y procedimientos escritos, son necesarios para implementar planes y tratamientos de riesgos adecuados frente a incidentes, riesgos, amenazas, peligros, etc. Previamente identificados en la evaluación de los activos de la organización.

La presentación de un informe para el tratamiento de riesgo y convencer de cierta manera al auditor en el correcto funcionamiento de los procesos en reducción de riesgos se puede realizar con informes relevantes donde se presenten los planes, tratamiento, técnicas y la metodología utilizada para situaciones inaceptables en los sistemas de información.
Por otro lado, la presentación y la gestión se puede llevar a cabo mediante listas de chequeo, matriz, bases de datos, programación de control, donde se explique cómo están siendo controlados los riesgos, la eficacia en la reducción del impacto, la mitigación a posibles incidentes y como están siendo tratado los riesgos previamente identificados.

4.2.7 MAGERIT

Es la metodología de análisis y gestión de riesgos, elaborada por el Consejo Superior de Administración Electrónica, la metodología se puede utilizar libremente y que no requiere autorización previa. Se utiliza principalmente para el principio de la gestión de seguridad que se basa en riesgos, análisis y gestión de riesgos, es considerando como parte de las tecnologías de la información que ayudan a cumplir y prestar servicios, para alcanzar los objetivos de la organización.

MAGERIT responde a los procesos de gestión de riesgos, implementación de riesgos, marco de gestión de riesgos, entre otras, siguiendo la normatividad de la ISO/IEC 31000. Permite alcanzar la toma de decisiones asociadas a los riesgos que se derivan del uso y manejo de las tecnologías de información de una organización.

4.3 ANTECEDENTES O ESTADO ACTUAL

En el 2017 la ingeniera Arlenys y Carolina Nieves como trabajo para optar el grado de especialista en seguridad de la información de la universidad Politécnico Gran Colombiano, realizado el diseño de un sistema de gestión de la seguridad de la información (SGSI) basado en la norma ISO/IEC 27001:2013 y siendo aplicado al Centro de Educación Técnica y Tecnológica del departamento del cesar[11], identificando que el desconocimiento de la seguridad de la información pone en riesgo los procesos que se desarrollan con los pilares de la información.

En el 2018 los ingenieros Maribel Jaqueline Pérez Mario Fernando Jurado realizaron como trabajo de grado para obtener el título de Especialistas en Seguridad Informática como trabajo de grado aplicado a la organización Ferretería Argentina de la ciudad de Pasto, presentado a la Universidad Nacional Abierta y a Distancia UNAD, concluye que la implementación del SGSI en la Ferretería Argentina le permitirá mitigar amenazas y actuar sobre los riesgos más críticos en los activos y con mejoras en los sistemas de información de la organización.

En el 2021 los ingenieros Sandra Paola Molina bravo Jack Dennis Quintero Torres, realizaron como trabajo de grado para obtener el título de Especialistas en Seguridad Informática de la Universidad Nacional Abierta y a Distancia UNAD, realizaron un diseño de un sistema de gestión de seguridad de la información (SGSI) para la empresa Bonos y Descuentos S.A.S, aplicó para el diseño controles para declaración de aplicabilidad SOA basado en la norma ISO/IEC 27001:2013 para mitigar los riesgos y aclara que es importante identificar e implementar los controles necesarios y adecuados para la organización, ayudará a optimizar la seguridad de los sistemas de información[12].

En el 2021 los ingenieros Jefferson Fabian Barbosa y Salinas David Alejandro González Vargas, realizaron el trabajo de grado para optar por el título de Especialistas en Seguridad Informática de la Universidad Piloto de Colombia, realizando el diseño del sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO/IEC 27001:2013 para la empresa Telemedicina en la IPS Colombiana de Trasplantes, concluyeron que la seguridad de la información es fundamental para todas las compañías, pero resalta que el personal de las empresas no le dan el valor adecuado e importancia a la seguridad de la

[11] NIEVES, ARLENYS CAROLINA. DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADOS EN LA NORMA. Principal [EN LINEA]. (2017). [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://alejandria.poligran.edu.co/bitstream/handle/10823/994/Trabajo%20Final.pdf?sequence=1&isAllowed=y>.

[12] SANDRA PAOLA MOLINA BRAVO Y. JACK DENNIS QUINTERO TORRES. DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA EMPRESA BONOS Y DESCUENTOS S.A.S, A PARTIR DE LA NORMA ISO 27001:2013. [s.l.]: [s.n.], 2022. 136 p.

información, además resaltan que el diseño del SGSI será la base para las buenas prácticas de todas las actividades que realice la compañía acompañado de seguridad en los procesos de información[13].

En el 2020 el ingeniero Cesar Daniel Rincón Brito, realizaron como trabajo de grado para obtener el título de Especialistas en Seguridad Informática de la Universidad Nacional Abierta y a Distancia UNAD, realizó el diseño del sistema de gestión de seguridad de la información SGSI basado en la norma internacional ISO/IEC 27001:2013 para la compañía ESSENSALE S.A.S, indicando que el diseño del SGSI le ofrecerá un mejor valor en protección de los activos de la compañía, permitirá mejorar la continuidad de los procesos de operación, estará atento a mitigar amenazas y generará confianza a los clientes de la compañía[14].

[13] JEFFERSON FABIAN BARBOSA SALINAS Y. DAVID ALEJANDRO GONZÁLEZ VARGAS. DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001:2013 PARA TELEMEDICINA EN LA IPS COLOMBIANA DE TRASPLANTES. [s.l.]: UNAD, 2021. 189 p.

[14] RINCON BRITO, Cesar Daniel. DISEÑO DE UN SGSI (SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN) BASADO EN LA NORMA INTERNACIONAL ISO/IEC 27001:2013 PARA LA COMPAÑÍA ESSENSALE S.A.S. [s.l.]: UNAD. 128 p.

4.4 MARCO LEGAL

Un buen sistema de gestión de seguridad de la información (SGSI) deberá estar alineado a las leyes, estándares, directrices, controles y regulaciones vigentes, que ayuden a Ginsac Colombia SAS en la correcta implementación de procesos en seguridad de la información y que a su vez se pueda proteger y salvaguardar la información como el activo más importante de la compañía.

Leyes en seguridad de la información colombiana necesarias para el SGSI de Ginsac Colombia SAS.[15]

Ley 1221 de 2008, Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
Esta ley apoya la interacción y la nueva oportunidad que brinda la organización Ginsac algunas áreas de trabajo (Contabilidad, Sistemas, Ejecutivos de ventas, social manager, Gerencia) a trabajar en condiciones óptimas desde lugares externos a la empresa y cumplir con sus obligaciones y actividades laborales, respetando los horarios establecidos por la organización, modalidad incluida a raíz de la Pandemia del COVID 19, la modalidad que se aplica en las áreas mencionadas es el teletrabajo suplementario, debido al tipo de contrato que se tiene con la organización y haciendo uso de las TIC para dar cumplimento a lo requerido en sus actividades diarias.

Ley 1266 de 2008, Por la cual se dictan disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.
La ley acoge a la organización a dar garantía, protección, privacidad de todos los datos personales, financieros o de cualquier naturaleza a que sean registrados, administrados y gestionados con la mayor confidencialidad y reserva que requiere la información.
La empresa al compilar la información informa a la persona (Natural, Jurídica) o empresa a que la información y el uso que se le va a dar es la correcta y corresponde a fines comerciales con la organización y de igual manera a que no será divulgada o vendida a entidades o servicios comerciales.

[15] MINTIC. Políticas de Operación Proceso de Tecnologías de la Información. Inicio - Función Pública [EN LINEA]. (marzo, 2020). [Consultado el 15, junio, 2022]. Disponible en Internet: <https://www.funcionpublica.gov.co/documents/418537/36701283/politica-de-seguridad-de-la-informacion.pdf.pdf/325019e5-a92f-0b44-3676-2356bd71240c?t=1586355315672>.

Ley 1273 de 2009[16]Por medio de la cual se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

.

Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad.

Artículo 269B. OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones.

Artículo 269C. INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático.

La ley y los artículos debe ser aplicables a los accesos a los sistemas informáticos de Ginsac que sin previa autorización accedan y violen la confidencialidad e integridad de la información que reposa en los sistemas y desarrollos de información, además si obstaculizan y vulneran los sistemas informático o telecomunicaciones poniendo en riesgo el funcionamiento normal de la estructura informática de la organización, Ginsac Colombia SAS, tomará las medidas pertinentes para hacer valer la ley 1273 del 2009 y los artículos que la conforman, que le permitan contar con sistemas fiables y que fortalezca el Sistema de Gestión de la Seguridad de la información con regulaciones a delincuentes informáticos que ocasionen daños a la organización y los sistemas de información que reposan en el SGSI de Ginsac.

Ley 1581 de 2012. 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.
La ley acoge al sistema de gestión de la seguridad de la información debido a que debe garantizar el buen uso y manejo de la información contenida y almacenada en los sistemas de información y las bases de datos de Ginsac.

[16] EL CONGRESO DE COLOMBIA. LEY 1273 DE 2009. Diario Oficial [EN LINEA]. (5, enero, 2009). [Consultado el 10, junio, 2022]. Disponible en Internet: <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf>.

Ley 1581 de 2012, art 3 Datos personales[17]Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Ley 1581 de 2012, art 3 Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento.

Ley 1581 de 2012, art 3 Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Para la aplicación de los sistemas de información que se acoge al SGSI se debe aplicar autorizaciones y consentimientos previos en el registro y recolección de información, tratamiento de información que es almacenada en las bases de datos, proteger la integridad de los datos personales que se vinculan a los sistemas de información de Ginsac, la empresa deberá designar responsables del tratamiento de los datos, responsables para el manejo y gestión de la información y ser acobijados por la ley 1581 y sus artículos .

Artículo 269D. DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos.
El SGSI será necesario la aplicación debido a que pondrían en riesgo la integridad y disponibilidad de los activos de la organización y que hacen parte del SGSI.

Artículo 269E. USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos.
El SGSI alineados con la ley contará con la facultad de implementar las técnicas y soluciones necesarias para mitigar riesgos e infección con software maliciosos que pongan en riesgo los sistemas de información acobijados por el SGSI de Ginsac.
Será necesario realizar las mayores estrategias que rija la ley para mitigar riesgos y sobre todo contar con software antimalware legal que ayude a prevenir este tipo de incidentes.

Artículo 269F. VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee

[17] MINTIC. Elaboración de la política general de seguridad y privacidad de la información. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN [EN LINEA]. [Consultado el 23, mayo, 2022]. Disponible en Internet: <https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf>.

códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.
Así compensara y brindara mayor protección y garantía al SGSI, debido a que se velará por la seguridad de los pilares de la seguridad de la información (Confidencialidad, Integridad y Disponibilidad) de los activos de información de Ginsac que se acogen al SGSI y necesarios para las actividades de los sistemas informáticos.

Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes.
La ley en suplantación de datos brindara al SGSI garantía de los desarrollos y sitios web que aloja en la internet la organización, ayudará a que los sitios sean empleadas de manera segura, que utilicen las licencias y servicios legales y pertinentes para el buen uso de la información e interacción que se emplea en la internet. Evitando plagiados por delincuentes.

Artículo 2691. HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informática, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos.
La protección de los sistemas de información acobijados por el SGSI deberá garantizar el buen uso de los recursos informáticos que Ginsac dispone para las actividades, teniendo con el control y tomando las medidas pertinentes que eviten el hurto del activo más importante de la organización como lo es la información.

Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero.
Para el SGSI es importante tener el control de los sistemas de información, contar con el mayor nivel de seguridad que se le pueda dar a un activo, calificando las vulnerabilidades y riesgos a los que están sometidos, actuando sobre esto para evitar vulneración en integridad de los sistemas de información de la organización.
Las políticas y controles que forman parte del SGSI ayudarán a reconocer el perfil y rol que un usuario juega en los sistemas de información, además del alcance que se le puede dar, revisiones y auditorias periódicas ayudarán a fortalecer la transparencia y buen uso de la información.

Decreto 1377 de 2013, art 3 Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación.

El SGSI y sus activos cuentan con niveles de sensibilidad frente a los sistemas de información de la empresa, para esto se debe trabajar y dar prioridad a las necesidades y tipo de información con la que se debe resguardar, la seguridad deberá ser la pertinente para cada nivel identificado en el SGSI.

DISEÑO METODOLÓGICO

La metodología que se utilizará para el desarrollo de los objetivos del proyecto del Sistema de Gestión de Seguridad de la Información, para la organización Ginsac Colombia SAS. Consiste en la aplicación de la fase planear y parte del hacer del ciclo de Deming o PDCA (Plan – Do – Check – Act), alineados con la norma ISO/IEC 27001 que será fundamental para el desarrollo y dirección del SGSI.

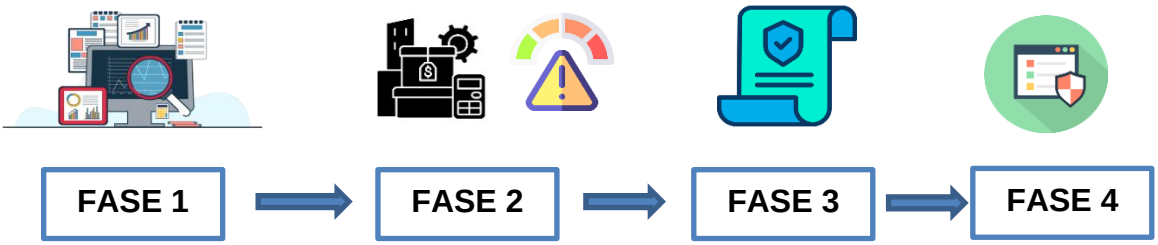
Fase 1. Diagnóstico situación actual de la seguridad de la información de Ginsac.

Fase 2. Identificación de activos y evaluación de riesgos asociados.

Fase 3. Diseño de políticas y controles de seguridad de la información.

Fase 4. Diseño de controles necesarios y aplicables para mitigación de riesgos

Figura 3. Fases desarrollo del proyecto



Fuente: Elaboración Propia

4.5 DIAGNÓSTICO SITUACIÓN ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN DE GINSAC

Es necesario reconocer e identificar el estado actual de la organización Ginsac Colombia SAS en materia de seguridad de la información, de esta manera se evidencia el nivel de madurez, la efectividad en los controles actuales y el nivel de riesgo al que están expuestos, se obtendrá un diagnóstico actual que ayudarán a determinar el alcance en seguridad y manejo de la información necesarias para el diseño del SGSI.

4.6 IDENTIFICACIÓN DE ACTIVOS Y EVALUACIÓN DE RIESGOS ASOCIADOS

Se realizará un inventario de activos de la información que será importante para la implementación del SGSI y la aplicación de los dominios de la norma ISO/IEC 27001, siendo la información el activo más importante para Ginsac Colombia SAS, de esta manera permita asegurar la integridad de la información, iniciar una evaluación de riesgos necesarios, minimizar el impacto de amenazas y mejorar el nivel en seguridad de la información de las tecnologías de información de la empresa.
Se realizará un recorrido por las instalaciones de Ginsac Colombia, entrevista e interacción con el Ingeniero de sistemas y encargado de las tecnologías de información.

4.7 DISEÑO DE POLÍTICAS Y CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

Es importante la definición de las reglas en seguridad de la información y que estén acorde con los objetivos y necesidades de la organización y del SGSI, así se podrá medir la efectividad del SGSI y mejorar con periodicidad la seguridad de los sistemas de información de Ginsac Colombia SAS.
Para el diseño de la política es necesario tener en cuenta[18]:

- Definir los objetivos, alcance y vigencia
- Definir los responsables
- Definir la autoridad en Ginsac Colombia que se encargará de la revisión, emisión, aprobación y publicación.
- Definir las bases o reglas del SGSI
- Actualización, revisión y mejoras de políticas de seguridad.

4.8 DISEÑO DE CONTROLES NECESARIOS Y APLICABLES PARA MITIGACIÓN DE RIESGOS

Determinar la aplicabilidad de controles alineados con los dominios de anexo (A) de la norma ISO/27001, para diseñar un plan de mitigación de riesgos que permita a los sistemas de información de Ginsac Colombia SAS contar con medidas de seguridad, velar por la integridad y buenas prácticas de la información, mejorar la calidad de los sistemas informáticos y ser garantes de sistemas de información fiables y confiables.

[18] ARAUJO, Adriel. ISO 27001: Cómo hacer tu política del SGSI - Hackmetrix Blog. Hackmetrix Blog [EN LINEA]. (9, septiembre, 2021). [Consultado el 9, abril, 2022]. Disponible en Internet: https://blog.hackmetrix.com/politica-del-sgsi/.

Los controles que se desean proponer se determinan con relación a los riesgos que sean identificados en la evaluación de los activos de la información, buscando disminuir probabilidades de que sucedan eventos, acciones, incidentes, riesgos o amenazas, además de reducir los impactos que se puedan originar en los sistemas de información de Ginsac Colombia SAS.

En el diseño de los controles que ayuden a mitigar los riesgos y su impacto, se podrá hacer usos de técnicas de tratamiento como:

- Medidas para reducir el riesgo
- Medidas para evitar el riesgo
- Medidas que permitan compartir el riesgo a entidades aseguradoras[19]

4.9 ESTRUCTURA ORGANIZACIONAL

La estructura organizacional de la compañía GINSAC identificada para el diseño del Sistema de Gestión de la Seguridad de la Información (SGSI), hace referencia a todos los usuarios, colaboradores (Internos y Externos), Alta dirección, que hace uso e interactúan con los sistemas de información de Ginsac Colombia SAS, en cada una de sus sedes.

Tabla 1. Estructura organizacional - Ginsac Colombia SAS

Cargo	Personal
Revisoría Fiscal	1
Gerente General	1
Gestores de conocimiento	2
Ingeniero de sistemas	1
Social Media Manager	1
Jefe administrativa y contable	1
Analista comercio exterior, compras e inventarios	1
Auxiliar contable	1
Auxiliar de tesorería	1
Auxiliar administrativo	1
Analista de gestión humana	1

[19] CÓMO MITIGAR riesgos en ISO 27001: opciones disponibles [Anónimo]. Software 45001 - ISOTools Chile [EN LINEA]. [Consultado el 25, junio, 2022]. Disponible en Internet: <https://www.isotools.cl/mitigar-riesgos-iso-27001/>.

Aprendiz SENA		2
Auxiliares servicios generales		3
Jefe de almacenes, compras y logística		1
Administrador de almacén		5
Jefe de planta		1
Analista de operaciones		1
Técnicos mecánicos Máster		2
Técnicos mecánicos Senior		7
Técnicos mecánicos Junior		6
Técnicos mecánicos auxiliares		2
Ejecutivo comercial molinería		1
Ejecutivos comerciales Senior		4
Ejecutivos comerciales Junior		4
	TOTAL	**51**

Fuente: Propia

Se pretende trabajar desde el área de las tecnologías de información con su alto grado de experiencia y conocimiento de los sistemas de información de la empresa, obtener información veraz, confiable, precisa, con criterios y necesidades específicas que permita diseñar de manera eficiente el SGSI para Ginsac Colombia SAS.

4.10 INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

Para el levantamiento de información necesaria para el diseño del Sistema de Gestión de la Seguridad de la Información (SGSI), se recopilaron a través de los siguientes métodos.

- Entrevistas
- Listas de chequeo
- Herramientas de encuestas de análisis (INCIBE)
- Magerit[20]

[20] MAGERIT V.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información [Anónimo]. PAe - MAGERIT v.3 [EN LINEA]. (octubre, 2012). [Consultado el 22, junio, 2022]. Disponible en Internet: <https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.YrdL9XbMKUk>.

5 ESTABLECER EL SGSI GINSAC COLOMBIA SAS

5.1 ALCANCE

El alcance del sistema de gestión de la seguridad de la información se realizará principalmente al conjunto de componentes que hacen parte de las tecnologías de información (TIC) de la compañía, los procesos y servicios tecnológicos más críticos y específicos en los departamentos y áreas que conforman la organización. Seguridad que será necesaria para garantizar la continuidad del negocio y buen uso de las tecnologías de información.

5.2 IDENTIFICACIÓN DE ACTIVOS

Se realiza un levantamiento de los activos que serán acobijados bajo la norma ISO/IEC 27001, alineados con una descripción de los procesos internos. La lista de inventarios de activos será evidencia por un análisis de relación del negocio y los activos de la compañía Ginsac Colombia SAS.
El desarrollo en la identificación de activos se realizó con la colaboración y aprobación de la alta dirección de Ginsac, asociados con los encuentros realizados con el responsable de las tecnologías de información TIC y las visitas realizadas en la compañía

5.3 IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES

Identificados la lista de activos acobijados para el diseño del SGSI y mejorar la calidad, eficiencia y seguridad de los sistemas de información, servicios y procesos de la compañía, se procede a realiza una eficiente evaluación de riesgos y conocer las existencias de vulnerabilidades y amenazas, el estado de cada activo y las medidas de seguridad que se deben tomar para minimizar los riesgos a niveles aceptable. La prioridad es contar con sistemas confiables y eficientes.
Se identifican las amenazas y vulnerabilidades asociadas a los activos y se resalta el nivel de impacto sobre cada activo de información acobijado en el diseño del SGSI.

5.4 CONTROLES Y POLÍTICAS DE SEGURIDAD

Establecer políticas de seguridad de la información para la protección, cuidado y el buen uso de los activos recolectados, procesados, resguardados en todos los sistemas informáticos de la compañía, relacionados con el cumplimiento eficiente de los principios de la seguridad de la información (Confidencialidad, Integridad y Disponibilidad). Consiste en gestionar y proteger los activos más importantes de Ginsac Colombia SAS, alineados con el cumplimiento y aplicación de controles de seguridad legales vigentes ISO/27000.

6 ANÁLISIS EN SEGURIDAD DE LA INFORMACIÓN ACTUAL

6.1 NECESIDAD

El SGSI para la compañía GINSAC COLOMBIA S.A.S será necesario para aumentar su nivel de madurez tecnológica y sobre todo implementar seguridad en su infraestructura informática que ha sido demasiado básica. GINSAC COLOMBIA S.A.S. es una empresa dedicada a la comercialización de maquinaria agrícola. Actualmente cuenta con presencia a lo largo del territorio nacional y tienen la representación exclusiva para Colombia de la Marca ZUKAI. Cuenta con el respaldo y servicio técnico de GINSAC IMPORT SAC, empresa líder en el mercado de Cosechadoras de Arroz en Perú, con experiencia mayor a 20 años y más de 1.500 máquinas vendidas en ese País.

Con el diseño del Sistema de Gestión de seguridad de la información y alineados con las buenas prácticas de la ISO/IEC 27001, la compañía podrá identificar que su activo más importante son los datos e información, que cada uno de sus activos de información están en constante amenaza con el auge y avances tecnológicos, identificara cada uno de sus activos y lo valiosos que son para la operatividad de sus servicios, resaltara los riesgos a los que están expuestos actualmente los procesos y actividades de su organización y podrá entender que es muy importante el apoyo e interés de la alta dirección al área de TI de la compañía. Que la seguridad y continuidad de los objetivos de la organización deberán estar alineados con las buenas prácticas de un SGSI.

La compañía no cuenta con normas y controles de seguridad para el manejo de cada uno de sus sistemas de información, cuenta con pronósticos favorables de ser víctimas de ataques cibernéticos, perdidas de información, manipulación errada de dispositivos tecnológicos, riesgos que se podrán minimizar con el diseño y gestión de políticas y normas en seguridad informática asociadas con el diseño del SGSI, los controles ayudaran a la organización a crear proyectos y estrategias en seguridad, a proteger, controlar y administrar los sistemas de información, prevenir amenazas internas y externas, sobre todo asegurar la continuidad de los procesos de GINSAC.

El Sistema de gestión de seguridad de la información velara por la seguridad de los tres pilares de la seguridad de la información (Confidencialidad, Integridad y Disponibilidad) sensibles y fundamentales para su competitividad comercial en el territorio agrícola. Sus buenas prácticas enmarcaran una buena imagen empresarial con objetivos seguros, con estrategias eficientes y como garantes de sistemas de información confiable.

El diseño del sistema de gestión de la seguridad de la información será la mejor herramienta en gestión de riesgos tecnológicos, será la mejora estrategia para

proyectos de altos niveles en seguridad informática y sobre todo será la mejor manera de alcanzar niveles de madurez tecnológicos muy altos. Su eficacia será alineada con el compromiso e interés de la alta dirección de GINSAC COLOMBIAS SAS.

6.2 GINSAC COLOMBIA

La compañía trabaja para crear una cultura diferente en el proceso de la cosecha de arroz, importado desde ASIA cosechadoras de diferentes capacidades y menor peso, selectoras por color, sembradoras de arroz y otros granos, torres de secamiento y molinos; brindándole soluciones a los agricultores que hasta hace poco tiempo no consideraban la opción de adquirir máquinas destinadas a este fin. Su entorno tecnológico es muy básico por falta de proyectos e interés de la alta dirección en tecnologías de información. Lleva más de ocho años en el país, ofreciendo productos con atributos diferenciadores a los que tradicionalmente se comercializaban, entregando equipos con adaptaciones que cumplen con el objetivo esperado, minimizando las pérdidas de granos y mejorando el rendimiento por hectárea y han dejado a un lado la seguridad de los sistemas de información de su estructura organizacional.

La empresa con el pasar de los años ha tomado cada vez más fuerza en el agro colombiano, ya son más de 6 sedes distribuidas en el territorio y con indicadores de tomar fuerza al ser uno de los aliados principales de los agricultores. Su infraestructura y plantas de operaciones han crecido con el tiempo, pero no se han tomado las medidas realmente necesarias para evitar ser víctimas de ataques o amenazas cibernéticas. Amenazas que podrían afectar gravemente la continuidad operacional de la organización.

Los servicios que presta GINSAC para el agro colombiano es amplio, podemos detallar el respaldo en servicio técnico, capacitación y disponibilidad de repuestos, convirtiéndolos así durante los últimos años, en el principal aliado de agricultores[21]. Mencionando las capacidades de servicios, pero con bastantes inseguridades informáticos en su entorno tecnológico, se plantea la necesidad de diseñar un SGSI que les permita mejorar y fortalecer los sistemas de información, su infraestructura informática, los entornos de red y tecnológicos distribuidos en cada una de sus sedes.

A continuación, podemos conocer un poco de la compañía su misión y visión, su estructura organizacional y sobre todo como poder involucrar cada proceso operacional con los objetivos propuestos en el diseño del SGSI para mejorar la

[21] GINSAC COLOMBIA | Maquinaria Agrícola [Anónimo]. Ginsac Colombia | Maquinaria Agrícola [EN LINEA]. (2022). [Consultado el 25, junio, 2022]. Disponible en Internet: <https://www.ginsac.com.co/nosotros.php>.

seguridad de la infraestructura informática de la compañía y ser garantes en la seguridad de los sistemas de información.

6.2.1 Misión

Ofrecer maquinaria y equipos de alto beneficio, garantizando un óptimo desarrollo y excelente servicio que contribuyan al mejoramiento de la calidad de vida de los clientes, colaboradores y accionistas.

6.2.2 Visión

En cinco años será la mejor opción en el uso de maquinaria agrícola y equipos eficientes, reconocidos por ser una empresa de calidad humana y profesional con responsabilidad social.

6.2.3 Eficiencia

Para desarrollar las actividades, se generan procesos prestando atención a la calidad, implementando hábitos de productividad, contratando las personas y la tecnología adecuados, y formalizando un sistema logístico innovador y flexible.

Ginsac Colombia SAS cuenta con 10 áreas de trabajo, con aplicaciones y desarrollos propios que almacenan y recopilan información para la gestión de proceso y desarrollos de actividades operativas, almacena información con ERP contables como SIESA, que permiten realizar los procesos fiscales, inventarios, facturación, Kardex, etc. Suscripciones corporativas para correos, almacenamiento en la nube de copias de seguridad, rastreo digital de flota vehicular, etc., que serán necesarios para el diseño e implementación del sistema de gestión de la seguridad de la información.

Áreas o departamentos de trabajo

- Ejecutivos de ventas internos y externos
- Contabilidad y Finanzas
- Compras y Logística
- Inventarios y compras e importaciones
- Almacenes de repuestos
- Planta y taller
- Gestor de sistemas
- Social media manager
- Gerencia
- Recursos Humanos

A continuación, se realiza una breve descripción de los procesos y departamentos de la compañía, actividades y responsabilidades para el diseño del SGSI.

Procesos de la compañía:

Gerencia General: Representante de Ginsac Colombia SAS, Accionista, jefe comercial, jefe administrativo.

Gestores de conocimiento: Encargados de estrategias y capacitaciones del campo y maquinaria agrícola, con el objetivo de fortalecer el conocimiento investigativo en maquinaria agrícola y sus beneficios.

Comercial: Ejecutivos comerciales (junior, senior y master) en área de maquinaria agrícola, plantas de trilla y secado. Encargados de la gestión, vinculación y acompañamientos de clientes y venta y leasing de maquinaria.

Administrativo y contable: Encargados del funcionamiento administrativo, financiero, contable, contratos, garantías, legalizaciones, viáticos, pagos, obligaciones fiscales y societarias.

Comercio exterior, compras nacional e inventario: Analista de inventarios, stock, Kardex y precios que requiere la empresa para venta de maquinaria y repuestos.

Recursos Humanos: Gestión de nóminas y personal.

Operaciones y alistamiento: Planta y grupo de expertos en mecánica agrícola que son los encargados del alistamiento, entrega y reparación de las maquinarias y plantas de molinería que importa y vende Ginsac Colombia SAS.

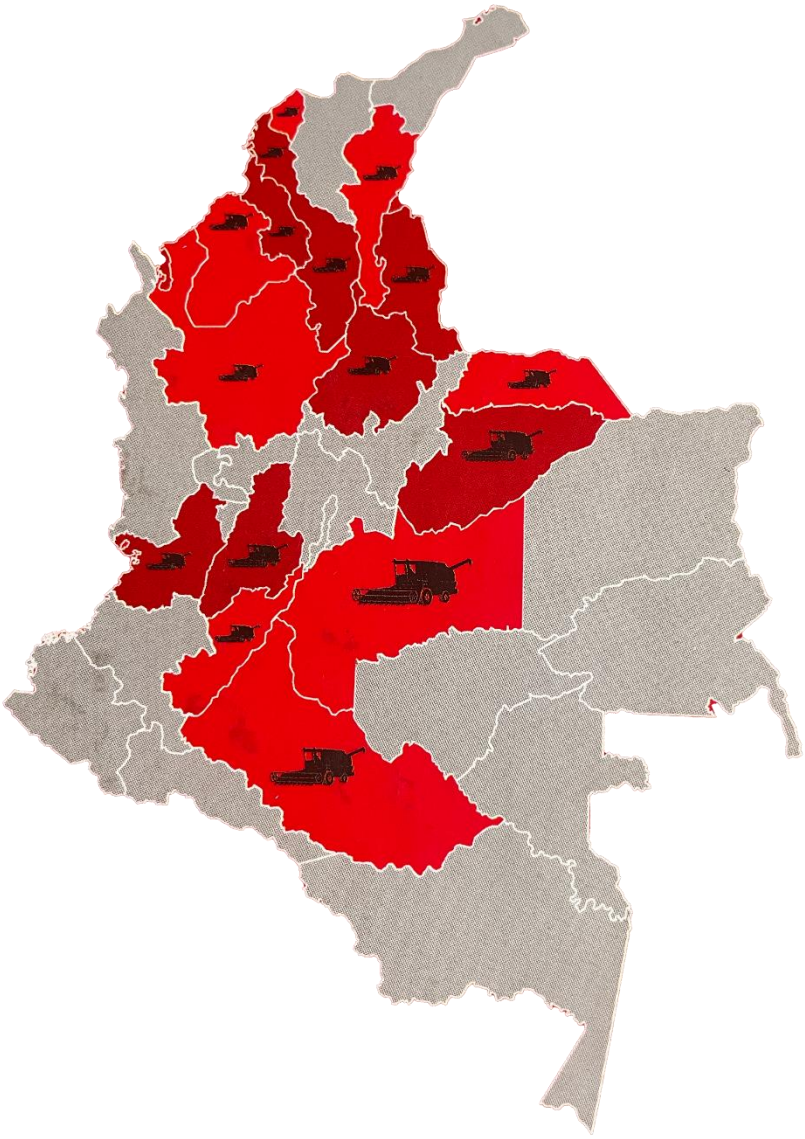
Almacenes compras y logística: Administradores de los puntos de ventas de repuestos originales de la maquinaria importada por Ginsac Colombia SAS.

Gestión administrativa: Gestión informática, Desarrollo web, soporte técnico, manejo y administración de bases datos, asesoramiento tecnológico, administrador de red.

Social Media: Manejo de redes sociales, publicidad, marketing digital.

Como se visualiza dentro del proceso operativo y administrativo y diseño del organigrama, no se tiene definido un área o departamento de tecnologías de información, se implementa un cargo administrativo en gestión de sistemas de información, para el apoyo, manejo y responsabilidad de las TIC, pero no se encuentra definido por la alta gerencia. La importancia de un departamento de TIC y de seguridad informática, será un proceso necesario en el diseño del SGSI de Ginsac Colombia SAS.

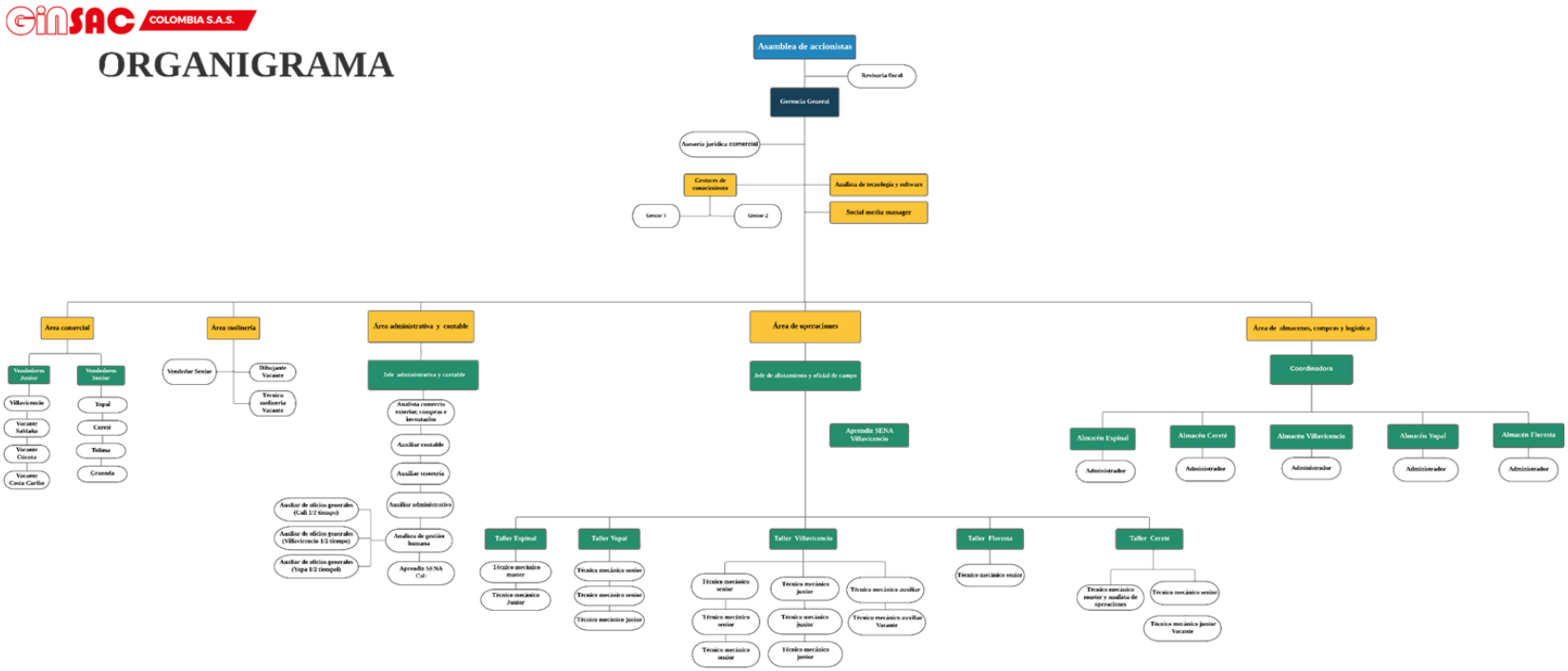
Figura 4. Presencia en Colombia



Fuente: GINSAC COLOMBIA SAS.

6.2.4 Organigrama Ginsac Colombia

Figura 5. Organigrama Ginsac



Fuente: GINSAC COLOMBIA SAS

6.3 ANÁLISIS EN SEGURIDAD ACTUAL

La información es el recurso más importante para el funcionamiento de los sistemas tecnológicos de una organización, es por esto por lo que la seguridad de la información se le debe dar el valor que se merece, que permita la efectividad y el cumplimiento de los pilares de la seguridad de la información (Confidencialidad, Integridad y Disponibilidad), mejorar y contar con sistemas de información fiables y eficientes.

Para el análisis en seguridad de la información de Ginsac Colombia SAS y que ayudará a evaluar el estado de riesgos y amenazas a los que se encuentra expuestos actualmente; como primer contacto con la compañía y como primer método para el levantamiento de información desde el área de tecnologías de información de Ginsac y con ayuda de herramientas del Instituto Nacional en Ciberseguridad (INCIBE)[22] de España, se realiza un diagnóstico contestado por el encargado de las TIC de la compañía, encuesta que es utilizada como inicio especialmente para dimensionar y comprender el estado en que se encuentra las tecnologías de información, determinar el estado en seguridad de la información, los riesgos que amenazan el funcionamiento de los procesos de la empresa y sobre todo resaltar los aspectos y mejoras que se deberán realizar y aplicar en el diseño del Sistemas de Gestión de Seguridad de la Información (SGSI).

Como inicio del análisis realizado en Ginsac Colombia SAS y calificado por Instituto Nacional en Ciberseguridad (INCIBE), se obtuvo los siguientes resultados en seguridad correlacionados con la implementación y el uso de los sistemas de información[23], encuesta que se puede evidencia el anexo (A) análisis de riesgo de información Ginsac Colombia SAS:

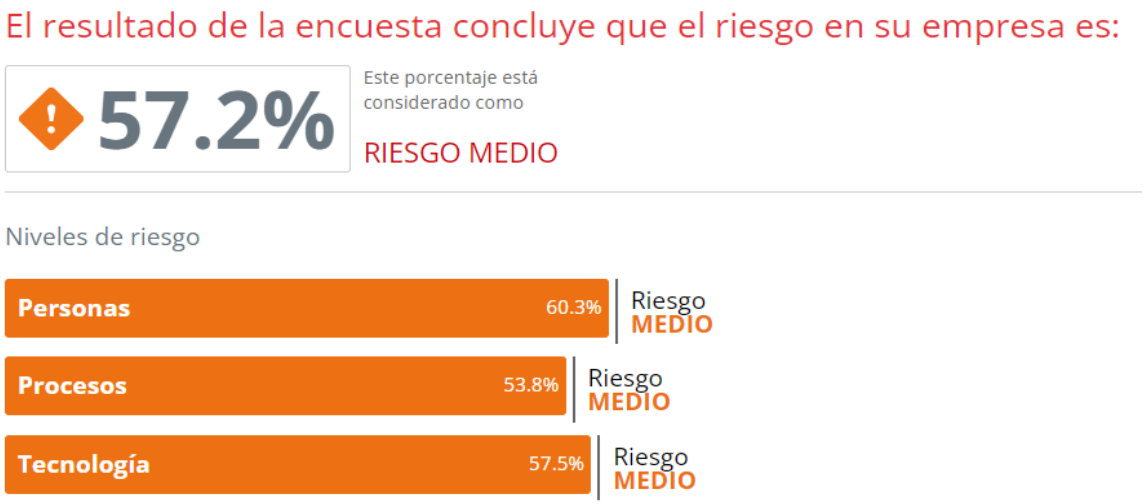
El nivel de seguridad con el que cuente los sistemas de información de Ginsac Colombia SAS es adecuado, pero se deberá mejorar, con un **57.2%** es considerado por INCIBE Riesgo Medio, distribuido en 3 niveles de riesgos claves para las buenas prácticas en seguridad de la información:

- Nivel de riesgo en personas 60.3%
- Nivel de riesgo en procesos 53.8%
- Nivel de riesgo en tecnología 57.5%

[22] ¿CONOCES TUS riesgos? [Anónimo]. INCIBE [EN LIENA] (27, enero, 2016). [Consultado el 3, octubre, 2022]. Disponible en Internet: <https://www.incibe.es/protege-tu-empresa/conoces-tus-riesgos>.

[23] AUTODIAGNÓSTICO LIGERO, INCIBE - Instituto Nacional de Ciberseguridad [Anónimo]. Autodiagnóstico ligero, INCIBE - Instituto Nacional de Ciberseguridad [EN LINEA]. [Consultado el 25, junio, 2022]. Disponible en Internet: <https://adl.incibe.es/questions.php#resultado>.

Figura 6. Resultado análisis de seguridad Ginsac Colombia SAS



Fuente: Instituto Nacional en Ciberseguridad (INCIBE)

6.3.1 Nivel de riesgo en personas

El primer nivel de riesgo de Ginsac Colombia SAS con relación al personal o colaboradores se ha considerado Nivel de riesgo Medio, siendo calificado por INCIBE con un 60.3% en manejo de seguridad, Indica que Ginsac Colombia SAS y sus empleados tienen una base de concienciación en seguridad de la información y además la importancia de buen uso y la responsabilidad que tienen con los sistemas de información de la empresa[24].

Es necesario el diseño de políticas de seguridad y socializarlas, de esta manera se mejorará el nivel de concienciación y las buenas prácticas en la seguridad de la información.

Es muy recomendable realizar políticas para el control de copias de seguridad y que se realicen con bastante frecuencia, además que esté acorde con el volumen de cambios que se realizan. Así, en caso de incidente, no se perderá demasiada

[24] HERRAMIENTA DE autodiagnóstico [Anónimo]. Autodiagnóstico ligero, INCIBE - Instituto Nacional de Ciberseguridad [EN LINEA]. [Consultado el 25, junio, 2022]. Disponible en Internet: <https://adl.incibe.es/pdfs/Personas_medio.pdf>.

información y la respuesta se hará más efectiva y la continuidad de la empresa no tardará.

Carece de control y responsabilidad por parte de los colaboradores para la actualización de dispositivos móviles con frecuencia, no notificarme puede causar al ingeniero de sistemas de Ginsac Colombia SAS, podrá ser parte de complicidad de riesgo a los sistemas de información que maneja la empresa, por esto será necesario automatizar esta acción. Hoy en día los dispositivos móviles suponen un objetivo primario de los delincuentes informáticos.

6.3.2 Nivel de riesgo en procesos

El primer nivel de riesgo de Ginsac Colombia SAS, en relación con la seguridad de la información de sus procesos y actividades de negocio ha sido considerado como nivel de riesgo medio, siendo calificado por INCIBE con un 53.8% en manejo de seguridad, indicando que los procesos de Ginsac y el uso de la información de parte de sus colaboradores, presentan una base que debe ser mejorada para fortalecer el nivel de fiabilidad de los sistemas de información[25].

Es necesario contar con políticas de contraseñas y mejorar el nivel de seguridad con normativas en la que indique el nivel, calidad y robustez de las contraseñas, garantizando que sean difíciles de adivinar y se cambien con frecuencia.
Además, se evidencia que la empresa no cuenta con el control para la destrucción de información (Confidencial u ordinaria), siendo necesario para la protección de la confidencialidad e integridad de la información que maneja Ginsac Colombia SAS, de esta manera cumplir con la legislación que rige por ley.

Cuenta con página web y desarrollos web, aunque se evidencia que se realizan copias de seguridad (Código y bases de datos), es necesario fortalecer los Backup, realizarlos con mayor periodicidad, probar los respaldos que permitan estar listos a incidentes que vulneren la integridad y disponibilidad de la información alojada en la web.

Aunque se evidencia que cuenta su servidor y la red de la sede principal (Cali – Valle del Cauca) en un espacio individual y restringido al personal de trabajo, es necesario que se reestructura y se mejore las condiciones de red de las demás sedes, ya que su implementación es básica y esto podría ayudar aumentar algún riesgo en seguridad informática.

Ginsac Colombia cuenta con un Plan de Contingencia y Continuidad de Negocio (lo que comúnmente se conoce como un plan B) y almacenar copias de seguridad

[25] HERRAMIENTA DE autodiagnóstico [Anónimo]. Autodiagnóstico ligero, INCIBE - Instituto Nacional de Ciberseguridad [EN LINEA]. [Consultado el 5, junio, 2022]. Disponible en Internet: <https://adl.incibe.es/pdfs/Procesos_medio.pdf>.

diarias en la nube (proveedor externo **Acronis Backup Cloud**), pero se recomienda revisar el plan de forma periódica la actividad y la eficiencia de las copias que se almacenan en la nube y que van a hacer parte del plan de contingencia y continuidad de los procesos y actividades de Ginsac Colombia SAS.
Ginsac Colombia, aplica para alguna parte del área administrativa, la modalidad de teletrabajo, pero es necesario monitorizar la red, mejorar las herramientas tecnológicas que permitan filtrar el tráfico y permitir las conexiones autorizadas por el ingeniero de las tecnologías de información de la empresa, que les permitirá acceder a los recursos alojados en el servidor local. Importante resaltar que una mala acción en las conexiones y en sus actividades, supone pérdidas para la empresa y pondrá en riesgo los sistemas informáticos de Ginsac Colombia SAS.

6.3.3 Nivel de riesgo en tecnología

El primer nivel de riesgo de Ginsac Colombia SAS con relación a la seguridad de la información y los componentes tecnológicos de la empresa, han sido considerado como nivel de riesgo medio, siendo calificado por INCIBE con un **57.5%** en manejo de seguridad de la información en las tecnologías de información de Ginsac, indica que la empresa, sus estructura informática y el manejo que le dan su colaboradores a la información cuentan con una base en el manejo y seguridad de los sistemas de información de la empresa[26].

La empresa no cuenta con tecnología cortafuegos, pero si con software antimalware en cada equipo de cómputo, servidor, pero no se puede olvidar en actualizar los recursos tecnológicos y configurarlos para que sean realmente útiles y mucho más seguros. Además, considere implementar algún tipo de cifrado a sus archivos e información, para proteger la confidencialidad e integridad de los sistemas de información de la empresa.

Continuando con el análisis actual en seguridad de las tecnologías de información por parte de la compañía y que será fundamental para la implementación de controles y proyectos en seguridad que permitirán contrarrestar los riesgos en seguridad encontrados y evaluados desde el estándar de la ISO/IEC 27002:2017 y la Declaración de Aplicabilidad (SOA) alineadas con el modelo de madurez de capacidades (CMM).

Realizamos un levantamiento de información con los responsables de la seguridad de la información, se hicieron visitas a la sede principal de Villavicencio y Cali, se evidencio las mejoras que se han podido realizar con el crecimiento del negocio, etc. Pero, para dimensionar el nivel de madurez del modelo de seguridad informática

[26] INCIBE. Herramienta de autodiagnóstico. Autodiagnóstico ligero, INCIBE - Instituto Nacional de Ciberseguridad [EN LINEA]. [Consultado el 25, junio, 2022]. Disponible en Internet: <https://adl.incibe.es/pdfs/Tecnologia_medio.pdf>.

y el nivel de privacidad de la información en la organización Ginsac Colombia SAS se realizó un diagnóstico basado en el estándar de la ISO/IEC 27001:2013 y 27002:2017 (SOA) y se realizó una evaluación de efectividad de controles, procesos que se pueden evidenciar en los anexos (b) Modelo de madurez y (c) en la evaluación de efectividad de controles.

Permitiendo de esta manera obtener los siguientes resultados.

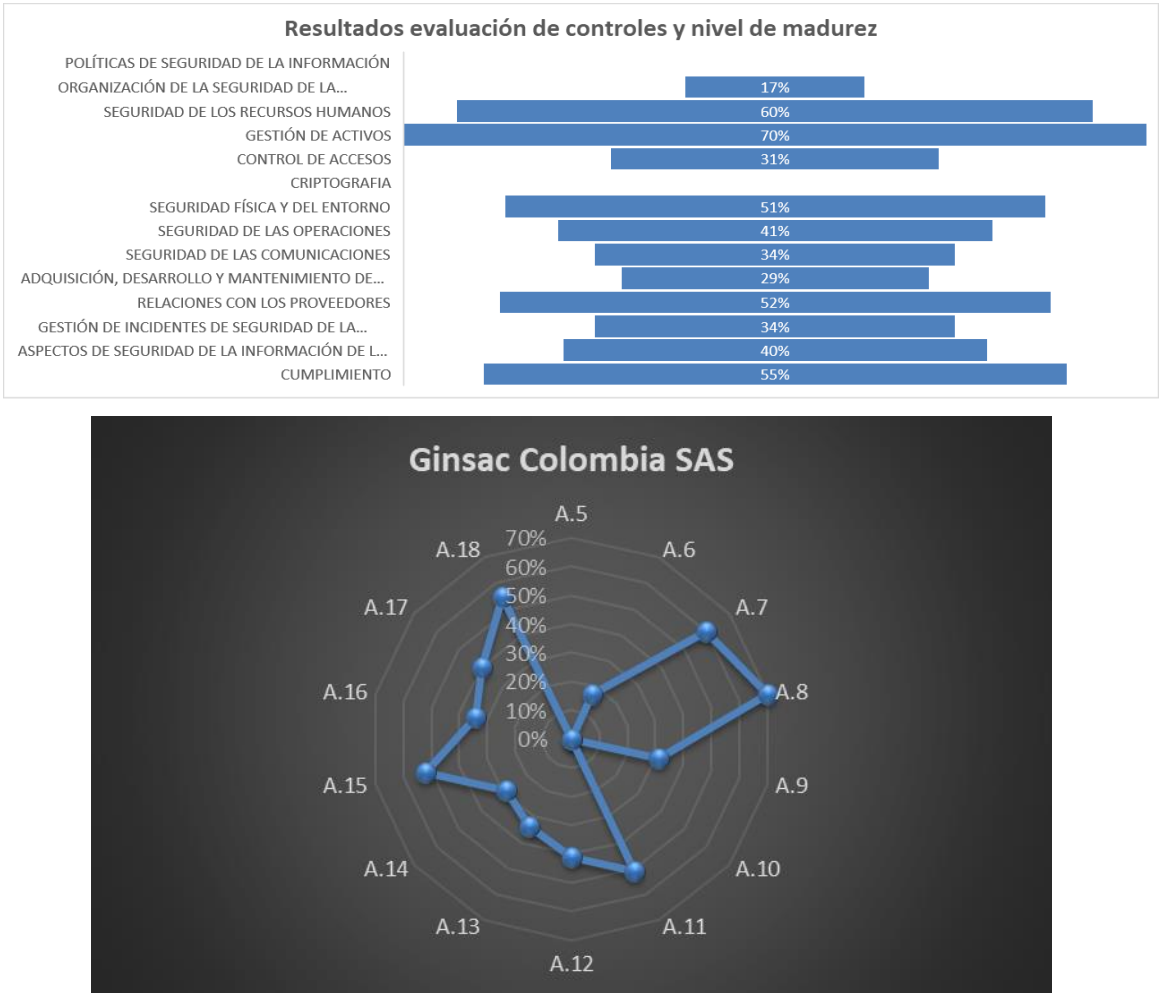
Tabla 2. Resultados evaluación de controles

Resultados evaluación de controles y nivel de madurez			
N° del Control	**Dominio**	**Puntuación**	**Nivel Efectividad**
A.5	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	0%	Inexistente
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	17%	Inicial
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	60%	Definido
A.8	GESTIÓN DE ACTIVOS	70%	Definido
A.9	CONTROL DE ACCESOS	31%	Repetible
A.10	CRIPTOGRAFIA	0%	Inexistente
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	51%	Definido
A.12	SEGURIDAD DE LAS OPERACIONES	41%	Definido

A.13	SEGURIDAD DE LAS COMUNICACIONES	34%	Repetible
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	29%	Repetible
A.15	RELACIONES CON LOS PROVEEDORES	52%	Definido
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	34%	Repetible
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO	40%	Repetible
A.18	CUMPLIMIENTO	55%	Definido
Promedio		**37%**	**Repetible**

Fuente: Elaboración propia.

Figura 7. Grafica resultado de controles de seguridad



Fuente: Elaboración propia.

Finalizada la evaluación de controles de seguridad otorgados por la ISO/IEC 27001:2013 se puede evidenciar el nivel de madurez en seguridad de las tecnologías de información en la organización Ginsac Colombia SAS, con un **promedio de 37%** de cumplimiento y posicionándola en un nivel de madurez **REPETIBLE**. Lo que quiere decir que desde las tecnologías de información de Ginsac deben de ser tratadas, documentadas y mejoradas en la mayor brevedad posible, evitando incidentes de seguridad informática y evitando perjudicar la continuidad de operación de la organización.

Gracias al resultado obtenido en el manejo de la seguridad de los sistemas informáticos y su gestión desde las tecnologías de información (TIC) de la compañía, se define un punto de partida para el diseño del SGSI y poder evidenciar las mayores falencias en seguridad que se deberá trabajar y mejorar.

7 INVENTARIOS DE ACTIVOS

Para la implementación del sistema de gestión de seguridad de la información en la empresa Ginsac Colombia SAS, se realiza la identificación de los activos alineados con la normativa de la ISO/27001, permitirá realizar una eficiente evaluación de riesgos y conocer las existencias de vulnerabilidades y amenazas, el estado de cada activo y las medidas de seguridad que se deben tomar para minimizar los riesgos a niveles aceptable. La prioridad es contar con sistemas confiables y eficientes.

En el levantamiento de información que permitió la recolección y elaboración del inventario de activos se implementó bajo la metodología Magerit, que se alineo con la aplicación de sus técnicas y se organizó cada activo relacionado con el tipo de activo correspondiente, clasificación que permite de manera ordenada realizar un criterio de evaluación de amenazas y sus posibles salvaguardas de manera jerárquica y simultánea.

Se realizo una descripción de los procesos internos, se presenta una lista de inventarios de activos y se evidencia un análisis de relación del negocio y los activos de la compañía Ginsac Colombia SAS. El desarrollo se realizó con la colaboración y aprobación de la alta dirección de Ginsac, asociados con los encuentros realizados con el responsable de las tecnologías de información TIC y las visitas realizadas en la compañía.

7.1 PROCESOS DE NEGOCIO

Tabla 3. Procesos de negocio

Procesos del negocio	Descripción
Gerencia General	Representante de Ginsac Colombia SAS, Accionista, jefe comercial, jefe administrativo.
Gestores de conocimiento	Encargados de estrategias y capacitaciones del campo y maquinaria agrícola, con el objetivo de fortalecer el conocimiento investigativo en maquinaria agrícola y sus beneficios.
Comercial	Ejecutivos comerciales (junior, senior y master) en área de maquinaria agrícola, plantas de trilla y secado. Encargados de la gestión, vinculación y acompañamientos de clientes y venta y leasing de maquinaria.
Administrativo y contable	Encargados del funcionamiento administrativo, financiero, contable, contratos, garantías, legalizaciones, viáticos, pagos, obligaciones fiscales y societarias.
Comercio exterior, compras nacional e inventario	Analista de inventarios, stock, Kardex y precios que requiere la empresa para venta de maquinaria y repuestos.
Recursos Humanos	Gestión de nóminas y personal.
Operaciones y alistamiento	Planta y grupo de expertos en mecánica agrícola que son los encargados del alistamiento, entrega y reparación de las maquinarias que importa y vende Ginsac Colombia SAS.
Almacenes compras y logística	Administradores de los puntos de ventas de repuestos originales de la maquinaria importada por Ginsac Colombia SAS.

Gestión administrativa	Gestión informática, Desarrollo web, soporte técnico, manejo y administración de bases datos, asesoramiento tecnológico, administrador de red.
Social Media	Manejo de redes sociales, publicidad, marketing digital.

Fuente: Elaboración propia.

7.2 LISTADO DE ACTIVOS

Tabla 4. Inventario de activos

Listado de activos		
Activo	**Cantidad**	**Responsable**
[D] Datos / Información		
DB sistema contable		Jefe administrativa
DB usuarios de red		Gestor administrativo
BD Personal		Jefe administrativa
Copias de seguridad		Gestor administrativo y jefe administrativa
BD Lista de precios		Gestor administrativo y jefe administrativa
BD RRHH		Jefe administrativa
[K] Claves criptográficas		
Firma electrónica Gerencia y tesorería [encrypt]	1	Gerencia
Matricula RUNT [com]	1	Tesorería
[S] Servicios		

Página Web [www]	1	Gestor administrativo
Work Space - Cuentas de correos [email]	32	Gestor administrativo
Acronix Protect - Copias en la nube [file]	1	Gestor administrativo
Cuentas de Google Drive [file]	32	Gestor administrativo
SIESA CONTABLE CLOUD	1	Jefe administrativa
Rastreo de flotas	1	Gestor administrativo y jefe administrativa
Hosting, Dominio [www]	1	Gestor administrativo
Tiene virtual Agrofy [www]	1	Gerencia
[SW] Software - Aplicaciones informáticas		
Sistema operativo Windows 10 - Windows 11 [os]	28	Gestor administrativo
S.O. Windows Server 2016 [os]	1	Gestor administrativo
Antivirus ESET Endpoint Security [av]	17	Gestor administrativo
Microsoft Office Empresa 2016 – 2019 [office]	28	Gestor administrativo
Software contable Helisa [sub]	1	Gestor administrativo y jefe administrativa

Software de copias de seguridad ACRONIS PROTECT [backup]	1	Gestor administrativo
Antivirus Norton 360 Premium [av]	20	Gestor administrativo
Desarrollos de intranet a la medida [prp]	1	Gestor administrativo
[HW] Equipamiento informático (hardware)		
Computadores All in One [pc]	12	Área administrativa
Servidor [pc]	1	Gestor administrativo
Impresora Epson [print]	7	Área administrativa
Router [router]	4	Gestor administrativo
Rack	2	Gestor administrativo
Modem [modem]	6	Gestor administrativo
Switch	2	Gestor administrativo
Teléfonos fijos [pabx]	3	Área administrativa
Cámaras de vigilancias x Sede [mid]	4	Área administrativa
Computador de mesa DELL [pc]	1	Gestor administrativo
Equipos portátiles [pc]	15	Gestor administrativo y jefe administrativa

Tablet Lenovo Yoga [mid]	6	Gestor administrativo, jefe administrativa y equipo comercial
Equipo Móviles [mobile]	10	Gestor administrativo
[COM] Redes de comunicaciones		
Infraestructura de RED LAN [LAN]	6	Gestor administrativo
Redes wifi [wifi]	8	Gestor administrativo
Internet [Internet]	6	Gestor administrativo y jefe administrativa
Telefonía móvil [Mobile]	10	Jefe administrativa
[Media] Soportes de información		
Discos duros externos SSD 1T [disk]	2	Gestor administrativo y jefe administrativa
Memorias USB 64 GB [usb]	2	Gerencia
[AUX] Equipamiento auxiliar		
UPS [ups]	6	Gestor administrativo
Cable estructurado por sede [cabling]	2	Gestor administrativo
[L] Instalaciones		

Oficinas / Sedes [site]	6	Gerencia
Vitrinas comerciales [local]	2	Gerencia
Puntos de teletrabajo [site]	10	Gerencia y jefe administrativa
Plantas de operaciones [site]	2	Gerencia y jefe administrativa
[P] Personal		
Área administrativa [ui]		Jefe administrativa y RRHH
Área Operativa [op]		Jefe administrativa y RRHH
Servicios generales [ui]		Jefe administrativa y RRHH
Área comercial [prov]		Gerencia y RRHH

Fuente: Elaboración propia alineados con la metodología Magerit V3.

7.3 RELACIÓN PROCESO DE NEGOCIO / ACTIVOS

Tabla 5. Inventarios de activos – Relación Procesos/Activos

Activos	Gerencia General	Gestores de conocimiento	Comercial	Administrativo y contable	Comercio exterior, compras	Recursos Humanos	Operaciones y alistamiento	Almacenes compras y logística	Gestión administrativa	Social Media
[D] Datos / Información										
DB sistema contable	X		X	X						
DB usuarios de red									X	
BD Personal	X			X		X			X	
Copias de seguridad	X			X		X		X	X	
BD Lista de precios	X		X	X	X		X	X	X	
BD RRHH	X			X		X			X	
[K] Claves criptográficas										
Firma electrónica Gerencia y tesorería [encrypt]	X			X						
Matricula RUNT [com]	X			X						
[S] Servicios										

Página Web [www]	X	X	X	X	X			X	X	X
Work Space - Cuentas de correos [email]	X	X	X	X	X	X	X	X	X	X
Acronix Protect - Copias en la nube [file]	X			X					X	
Cuentas de Google Drive [file]	X	X	X	X	X	X	X	X	X	X
SIESA CONTABLE CLOUD				X		X		X		
Rastreo de flotas									X	
Hosting, Dominio [www]									X	
Tiene virtual Agrofy [www]	X		X	X					X	X
[SW] Software - Aplicaciones informáticas										
Sistema operativo Windows 10 - Windows 11 [os]	X	X	X	X	X	X	X	X	X	X
S.O. Windows Server 2016 [os]				X					X	
Antivirus ESET Endpoint Security [av]	X	X	X	X	X	X	X	X	X	X

Microsoft Office Empresa 2016 – 2019 [office]	X	X	X	X	X	X	X	X	X	X
Software contable Helisa [sub]				X		X		X		
Software de copias de seguridad ACRONIS PROTECT [backup]									X	
Antivirus Norton 360 Premium [av]		X	X	X	X	X	X	X	X	X
Desarrollos de intranet a la medida [prp]	X		X	X		X	X	X	X	
[HW] Equipamiento informático (hardware)										
Computadores All in One [pc]			X	X	X	X	X	X	X	
Servidor [pc]				X					X	
Impresora Epson [print]	X	X	X	X	X	X	X	X	X	
Router [router]									X	
Rack									X	
Modem [modem]									X	
Switch									X	
Teléfonos fijos [pabx]	X		X	X				X		

Cámaras de vigilancias x Sede [mid]	X			X				X	X	
Computador de mesa DELL [pc]									X	
Equipos portátiles [pc]	X	X	X	X			X	X		X
Tablet Lenovo Yoga [mid]	X		X				X		X	
Equipo Móviles [mobile]	X		X	X	X	X		X		X
[COM] Redes de comunicaciones										
Infraestructura de RED LAN [LAN]	X			X					X	
Redes wifi [wifi]	X			X				X	X	
Internet [Internet]				X					X	
Telefonía móvil [Mobile]			X	X	X	X		X		X
[Media] Soportes de información										
Discos duros externos SSD 1T [disk]				X					X	
Memorias USB 64 GB [usb]	X									
[AUX] Equipamiento auxiliar										
UPS [ups]									X	
Cable estructurado por sede [cabling]									X	

[L] Instalaciones										
Oficinas / Sedes [site]	X			X				X		
Vitrinas comerciales [local]	X		X	X						
Puntos de teletrabajo [site]	X	X	X	X					X	
Plantas de operaciones [site]	X	X	X	X	X		X			
[P] Personal										
Área administrativa [ui]	X			X		X				
Área Operativa [op]	X	X		X		X	X			
Servicios generales [ui]	X			X		X				
Área comercial [prov]	X		X	X		X				

Fuente: Elaboración propia.

8 VALORACIÓN DEL ACTIVO

La valoración y clasificación de los activos tiene como objetivo asegurar que el nivel de seguridad sea el adecuado, cumpliendo los requerimientos que se estipulan en la gestión de activos de la ISO/27000.
En la valoración de activos se toman los parámetros de seguridad (Confidencialidad, Integridad y Disponibilidad). Determinaremos la importancia en Ginsac Colombia SAS.

Para realizar una valoración de los activos identificados en la compañía se alinean con la metodología Magerit proporcionando las técnicas y procedimientos para identificar de manera más precisa los activos con mayor criticidad y sus posibles amenazas a las que están expuestas.

A continuación, se ilustra el listado de amenazas relacionados por la metodología Magerit, necesarios para la evaluación de los riesgos[27].

8.1 AMENAZAS/ACTIVOS

Se realiza una matriz para representar las amenazas relacionadas con cada activo que hace parte del inventario de activos y forman parte del diseño del Sistema de Gestión de la seguridad de la información (SGSI) realizado para Ginsac Colombia SAS. Relación que se podrá observar en el anexo (d) la lista de amenazas MAGERIT. Listado de amenazas que nos permitirá identificar el grado o nivel de riesgo que se encuentran expuesto cada componente del inventario de activos.

8.1.1 Criterios de valoración

Se realiza la comparación de riesgos utilizando una escala común de todas las dimensiones, escalas algorítmicas y criterios homogéneo permitiendo realizar un análisis separado y relacionado con cada tipo de activo, obteniendo resultados de la probabilidad de impacto con su respectiva valoración, fundamental para priorizar en los controles y salvaguardas en seguridad de los sistemas informáticos y tecnológicos de Ginsac Colombia SAS.

8.1.1.1 Valoración de activos cualitativos

Se pueden evidenciar en la tabla de lista de inventario de activos, siendo clasificados de forma correcta, según el criterio y las buenas prácticas de la

[27] CALDERON, Marco. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III -Guía de Técnicas. Academia.edu - Share research [EN LINEA]. [Consultado el 10, diciembre, 2022]. Disponible en Internet: <https://www.academia.edu/27331595/MAGERIT_versión_3_0_Metodología_de_Análisis_y_Gestión_de_Riesgos_de_los_Sistemas_de_Información_Libro_III_Guía_de_Técnicas>.

metodología MAGERIT. Buscando saber qué es lo que hay dentro de la organización sin cuantificarlo y sobre todo que formara parte del SGSI. Permitiendo valorar relativamente los activos relacionados con posibles amenazas, riesgos que corren y el impacto de un posible incidente informático, informe que puede observarse en el anexo (E) la metodología para la valoración del riesgo en los activos de información MAGERIT.
Resaltando factores de análisis como degradación de un activo, impactos de amenazas, probabilidad de amenazas, riesgos, salvaguardas, etc.

8.1.1.2 Valoración de activos cuantitativos

Es relaciona con el listado y la categoría de cada activo, permitiendo realizar una valoración cuantitativa, relacionada con las buenas prácticas de la metodología MAGERIT, que busca saber que hay y cuanto hay, siendo cuantificados todos los posibles aspectos, evaluados por números reales, determinando un posible valor de riesgo alineados a cada activo. Procesos que pueden ser observados en el anexo (F) la metodología para la valoración del riesgo en los activos de información MAGERIT.

Metodología para la valoración del riesgo en los activos de información MAGERIT

Tabla 6. Probabilidad del riesgo

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

Fuente: Elaboración propia.

Tabla 7. Impacto del riesgo

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

Fuente: Elaboración propia.

Tabla 8. Valoración del riesgo

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

Fuente: Elaboración propia.

Tabla 9. Matriz valoración de riesgos

		Probabilidad				
Impacto	***Riesgo***	MB	B	M	A	MA
	MA					
	A					
	M					
	B					
	MB					

Fuente: Elaboración propia.

8.1.2 Análisis de los resultados de la matriz de riesgos

Tabla 10. Resultado valoración análisis del riesgo

Nombre	Riesgo	AUTENTICIDAD	TRAZABILIDAD	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	VALOR
UPS	APRECIABLE	9	9	9	9	25	12
Cable estructurado por sede	APRECIABLE	9	9	9	9	25	12
Infraestructura de RED LAN	APRECIABLE	9	9	25	9	9	12
REDES WIFI	APRECIABLE	9	25	25	9	9	15
INTERNET	APRECIABLE	9	9	25	15	15	15
Firma electrónica Gerencia y tesorería	APRECIABLE	9	9	25	15	15	15
DB sistema contable	APRECIABLE	9	9	9	25	9	12
DB usuarios de red	APRECIABLE	9	25	9	15	9	13
BD Personal	APRECIABLE	9	9	9	9	25	12
Copias de seguridad	APRECIABLE	9	9	25	9	9	12
BD Lista de precios	APRECIABLE	9	9	9	9	25	12
Computadores All in One	APRECIABLE	9	9	9	9	25	12
Servidor	APRECIABLE	9	9	25	9	9	12
Impresora Epson	APRECIABLE	9	9	15	9	25	13
Router	APRECIABLE	9	9	9	9	25	12
Modem	CRITICO	25	15	20	20	25	21
Switch	APRECIABLE	9	25	25	9	9	15
Teléfonos fijos	APRECIABLE	9	9	9	9	25	12
Cámaras	APRECIABLE	9	9	9	9	25	12
Computador de mesa DELL	APRECIABLE	9	9	25	9	25	15
Equipos portátiles	APRECIABLE	9	9	25	9	25	15
Tablet Lenovo Yoga	APRECIABLE	9	25	25	9	9	15
Equipo Móviles	APRECIABLE	9	9	25	9	25	15
Oficinas / Sedes	APRECIABLE	9	9	25	9	9	12
Vitrinas comerciales	APRECIABLE	9	9	9	25	9	12
Puntos de teletrabajo	APRECIABLE	9	9	9	9	25	12
Plantas de operaciones	CRITICO	20	15	25	20	25	21

Área administrativa	APRECIABLE	9	9	9	9	25	12
Área Operativa	APRECIABLE	9	9	25	20	9	14
Servicios generales	APRECIABLE	9	9	9	9	25	12
Área comercial	BAJO	9	9	9	9	9	9
Proveedores	APRECIABLE	9	9	9	9	25	12
Desarrollos de intranet a la medida	APRECIABLE	9	9	9	25	15	13
Work Space - Cuentas de correos	APRECIABLE	9	9	9	25	9	12
Acronix Protect - Copias en la nube	APRECIABLE	9	9	15	15	25	15
Cuentas de Google Drive	APRECIABLE	9	9	9	25	15	13
SIESA CONTABLE CLOUD	APRECIABLE	9	9	9	25	9	12
Rastreo de flotas	APRECIABLE	9	9	25	15	9	13
Hosting, Dominio	APRECIABLE	9	9	25	9	9	12
Tiene virtual Agrofy	APRECIABLE	9	9	9	25	25	15
Sistema operativo Windows 10 - Windows 11	IMPORTANTE	9	9	25	15	25	17
S.O. Windows Server 2016	IMPORTANTE	9	9	25	25	25	19
Antivirus ESET Endpoint Security	APRECIABLE	9	9	9	9	25	12
Microsoft Office Empresa 2016 - 2019	APRECIABLE	9	9	20	9	25	14
Software contable Helisa	APRECIABLE	9	9	25	9	9	12
Software de copias e seguridad ACRONIS PROTECT	IMPORTANTE	9	9	25	25	25	19
Discos duros externos SSD 1T	APRECIABLE	9	9	9	25	25	15
Memorias USB 64 GB	APRECIABLE	9	9	9	25	25	15
SIESA NOMINA CLOUD	BAJO	9	9	9	9	9	9

Fuente: Elaboración propia.

Tabla 11. Matriz valoración de riesgo - Promedio por tipo de activo

Impacto de riesgo	Valoración	Categoría
[D] Datos / Información	15	APRECIABLE
[K] Claves criptográficas	15	APRECIABLE
[S] Servicios	14	APRECIABLE
[SW] Software - Aplicaciones informáticas	15	APRECIABLE
[HW] Equipamiento informático (hardware)	15	APRECIABLE
[COM] Redes de comunicaciones	14	APRECIABLE
[Media] Soportes de información	13	APRECIABLE
[AUX] Equipamiento auxiliar	13	APRECIABLE
[L] Instalaciones	13	APRECIABLE
[P] Personal	16	IMPORTANTE

Fuente: Elaboración propia.

En la tabla 24 se hace énfasis del total del riesgo y su impacto, relacionados en los niveles más críticos de la compañía.

Tabla 12. Resultado apetito por el riesgo y zonas de admisibilidad

		Probabilidad				
Impacto	***Riesgo***	MB	B	M	A	MA
	MA	3	37	11	11	**4**
	A	0	16	20	12	13
	M	0	46	3	12	9
	B	0	0	0	0	0
	MB	0	0	0	0	0

Fuente: Elaboración propia.

Finalizado el resultado de riesgos y el impacto dentro de los sistemas de información y acobijado por la metodología Magerit, resume lo siguiente que podrá ser observado en el anexo (f) la matriz de análisis de riesgos GINSAC COLOMBIA SAS:

Todas las categorías de los tipos de activos acobijados por el diseño del sistema de gestión de seguridad de la información se deben tratar y alinear con proyectos de seguridad, para mejorar y maximizar la madurez y seguridad de la infraestructura informática de Ginsac Colombia SAS, estando sus sistemas de información en niveles de riesgos apreciables e importantes.

El resultado presenta 4 Riesgos con mayor probabilidad de impacto a los activos de información de la compañía resaltados principalmente en la fuga de información, carencia de políticas y controles para el manejo de las tecnologías de información, abuso de privilegios, robo o alteración de datos, ya que no se establece un control con niveles de seguridad eficaces, engaños e ingeniería social, almacenamiento y

tratamiento inadecuado de la información por parte de algunas áreas de la compañía, etc.

Se presentan un promedio de 36 riesgos de amenazas importantes dentro de los sistemas de Ginsac, riesgos en lo que se deberá generar y enfatizar proyectos que ayuden a llevar a niveles aceptables lo más rápido posible para no perder el control y subir a un nivel de seguridad crítico.

Riesgos que podemos resumir a continuación error por mal manejo de los sistemas los usuarios, errores por una mala configuración por parte del administrador, manipulación de datos, abuso de privilegios por parte de algunos colaboradores de la compañía, suplantación de identidad, etc. Son riesgos que afectan a varias categorías de activos que fueron clasificadas bajo la metodología de Magerit.

Se evidencia en la calificación de riesgo que la implementación de tecnologías de seguridad y para contrarrestar amenazas son muy básicas, para el nivel de riesgo en que se encuentran varias de las categorías de activos valorados. Es necesarios la implementación de herramientas y tecnologías para el monitoreo, gestión y administración del tráfico, tecnología para bloqueo de posibles intrusiones a los sistemas, comunicaciones y canales seguros por VPN, etc.

Aunque no hay sistemas 100% seguros, lo que, si podrá Ginsac Colombia SAS alineados con un SGSI, es minimizar a niveles aceptables cualquier tipo de incidentes de seguridad con la integración de herramientas especializadas y sobre todo a nuestro alcance para mejorar y asegurar los 3 pilares de la seguridad de la información y sobre todo tener siempre el control de sistemas eficientes y fiables.

La importancia de implementar un diseño del SGSI bajo técnicas y estándar de la ISO/IEC 27001:2013, garantizará a las tecnologías de información el endurecimiento tecnológico en ambientes e infraestructuras informáticas, ayudaran a maximizar la seguridad, reducir amenazas, evitar explotación de vulnerabilidades y sobre todo garantizar la continuidad de las aplicaciones, servicios y procesos del negocio. Su correcta implementación y monitoreo continuo preparara al entorno informático ante posibles ataques cibernéticos con defensas en seguridad eficientes y robustas.

Con los resultados obtenidos con la buena implementación de la metodología Magerit y las tecnologías de la compañía GINSAC, se procede a proponer proyectos controles y políticas que ayuden a minimizar y a priorizar a niveles aceptables la mayor cantidad de riesgos a los que se enfrenta actualmente la compañía.

En el anexo (f) la matriz de análisis de riesgos GINSAC COLOMBIA SAS, se evidencia la calificación de riesgos importantes con nivel de criticidad alta, resaltado en servicios y configuración de los entornos informáticos en cada una de las sedes, manejo de copias de seguridad, equipos tecnológicos asignados al personal de la

compañía, seguridad en los sistemas de información, gestión de sistemas comerciales, etc.
Se evidencia que la compañía cuenta con personal poco capacitado en el manejo básico de seguridad de los sistemas de información y equipos tecnológicos asignados para sus labores diarias dentro de la organización. Se hace énfasis y es notificado al encargado de las TI de la compañía de los riesgos encontrados durante el levantamiento de información y el proceso realizado para el diseño del SGSI.

Se presentan a continuación algunas políticas y controles en seguridad que podrán ser de ayuda para el área de TI para aumentar el nivel en seguridad y sobre todo aumentar el control de la infraestructura informática y el uso adecuado de los recursos de Ginsac Colombia SAS.

9 POLÍTICA DE SEGURIDAD

Ginsac Colombia SAS comprometidos con el sistema de gestión de la seguridad de la información, y en el fortalecer la seguridad de la estructura tecnológica, direccionados con las buenas prácticas de los controles de seguridad vigentes y dispuestos por la ISO/27000, se procede al desarrollo y diseño de una política de seguridad que alineados con buenas prácticas, proporcionan un mayor nivel de madurez, continuidad, minimización de riesgos, fortalecerá los objetivos establecidos y los propuestos, incrementará en el cumplimiento de los principios de la seguridad (Confidencialidad, Integridad y Disponibilidad), eficiencia y rapidez en la gestión de incidentes o amenazas, relacionados con los sistemas informáticos de la organización Ginsac Colombia SAS, y contará con sistemas y servicios eficientes y confiables.

9.1 OBJETIVO POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN[28]

El objetivo de la política de seguridad de la información consiste en gestionar y proteger los activos más importantes de Ginsac Colombia SAS, alineados con el [29]cumplimiento y aplicación de controles de seguridad legales vigentes ISO/27000.

- Establecer políticas de seguridad de la información para la protección, cuidado y el buen uso de los activos recolectados, procesados, resguardados en todos los sistemas informáticos de la compañía, relacionados con el cumplimiento eficiente de los principios de la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).

- Maximizar el mayor nivel de madurez en la integridad y disponibilidad de la información y la calidad de los servicios que se prestan para los clientes, proveedores y aliados, proyectando disminución del impacto frente a incidentes, riesgos, vulnerabilidades o brechas de seguridad identificados.

- Atribuir en el cumplimiento con las obligaciones legales, regulatorias y vigentes referente con la seguridad de la información, en las actividades, procesos, operaciones, innovación e investigación de los sistemas tecnológicos que tiene y desarrollará Ginsac Colombia SAS con el apoyo y respaldo de la alta dirección.

---

[28] PEDRO PABLO FERNÁNDEZ RIVERO Y. LUIS GÓMEZ FERNÁNDEZ. https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/53624/?page=86. E-Libro [EN LINEA]. (2018). [Consultado el 25, junio, 2022]. Disponible en Internet: <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/53624/?page=86>.

[29] GERENCIA. Política de seguridad. FIDETIA [EN LINEA]. (30, abril, 2015). [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://www.fidetia.es/politica_seguridad.php>.

- Diseñar estrategias de cultura, capacitaciones y sensibilización a los colaboradores, directivos, clientes, aliados, proveedores, etc. La responsabilidad y el cumplimento de las políticas dispuestas en el tratamiento y uso de la seguridad de la información, fortaleciendo la cultura de la seguridad de la información dentro y fuera de la compañía, adicional del seguimiento e implementación del sistema de gestión de la seguridad de la información con mejoras y actualizaciones periódicas alineadas con planes de contingencia sin afectar la continuidad de operación de Ginsac Colombia SAS[30].

9.1.1 Alcance en el sistema de gestión de la seguridad de la información

- Sistemas de información que controlan los procesos de los servicios de la organización Ginsac Colombia SAS (venta de maquinaria agrícola, equipos de molinería y secado, respuestas, servicio de planta y taller, dirección técnica, asesoría agrícola, alianzas estratégicas, acompañamiento técnico), servicio comercial, financieros y contable, Recursos humanos, inventarios y compras nacionales e internacionales, gestor de sistemas de información, Logística e importaciones, etc. que la organización Ginsac Colombia SAS aplica.

- Las directrices expuestas serán efectivas y gestionadas en la estructura, recursos y activos de información.

- La política de seguridad diseñada será aplicable para todos los colaboradores y que serán guiados a la medida como afecten sus áreas y actividades de trabajo. Será aplicable para proveedores, clientes, aliados estratégicos y aquellos que hagan parte del manejo de la información de la organización Ginsac Colombia SAS.

9.2 ALCANCE

La política de seguridad diseñada será aplicable para todos los colaboradores y que serán guiados a la medida como afecten sus áreas y actividades de trabajo. Será aplicable para proveedores, clientes, aliados estratégicos y aquellos que hagan parte del manejo de la información de la organización Ginsac Colombia SAS.

[30] ELABORACIÓN DE la política general de seguridad y privacidad de la información [Anónimo]. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN [EN LINEA]. [Consultado el 25, junio, 2022]. Disponible en Internet: <https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf>.

9.3 REQUISITOS LEGALES EN EL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información [31]

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal[32]

- Real Decreto 1720/2007, de 21 de diciembre, protección de datos de carácter personal.

- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico

- [33]Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual.
- Decisión (UE) 2021/1075 del Consejo de 21 de junio de 2021 por la que se modifica la Decisión 2013/488/UE sobre las normas de seguridad para la protección de la información clasificada de la UE.

- Ley 32/2003, General de telecomunicaciones[34], regulación de las telecomunicaciones.

9.4 REVISIONES Y AUDITORÍAS

- Los responsables de la gestión y cumplimiento de las políticas de seguridad tendrán la responsabilidad de mantener actualizadas las directrices. Los cambios deben ser revisados y aprobados por la alta dirección de Ginsac Colombia SAS. Cada nuevo requerimiento debe mostrar la efectividad de la política y el nivel de cambio que afecta al entorno tecnológico y servicios sea valorado.

---

[31] JEFATURA DEL ESTADO. BOE.es - BOE-A-2018-12257 Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. BOE.es - Agencia Estatal Boletín Oficial del Estado [EN LINEA]. (7, septiembre, 2018). [Consultado el 24, julio, 2022]. Disponible en Internet: <https://www.boe.es/eli/es/rdl/2018/09/07/12>.

[32] NOTICIAS JURÍDICAS [Anónimo]. Noticias Jurídicas [EN LINEA]. (30, julio, 2018). [Consultado el 25, junio, 2022]. Disponible en Internet: <https://noticias.juridicas.com/base_datos/Anterior/r3-lo15-1999.html>.

[33] «Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.», s. f., 100.

[34] INCIBE. Guia_apoyo_SGSI.pdf. (24, mayo, 22). [Consultado el 12, octubre, 2022]. Disponible en Internet: <https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf>.

- En el plan del sistema de gestión de seguridad, se llevará a cabo una auditoría completa cada año y será desarrollado por el responsable de la gestión y seguridad de Ginsac Colombia SAS.

- La alta dirección de la organización Ginsac Colombia SAS serán los responsables de revisar y aprobar actualizaciones o modificaciones que se realicen y ésta produzca cambios frente a los riesgos establecidos.

- Los responsables de seguridad en la organización Ginsac Colombia SAS garantizarán el almacenamiento de los registros, copias de las bases de datos, datos, información, etc. que hagan parte de la funcionalidad de los sistemas y actividades dentro y fuera de la organización. Se deberán gestionar y realizar seguimiento y monitoreo a eventos de seguridad que se presenten.

- Los responsables de seguridad en la organización Ginsac Colombia SAS deben garantizar la evaluación de los controles, eficiencia y funcionalidad de los sistemas, el cumplimiento en las operaciones, procedimientos y las políticas establecidas, además del reporte de deficiencias o vulnerabilidades detectadas.

9.5 COMPROMISO DE LA DIRECCIÓN DE GINSAC COLOMBIA SAS

La alta dirección de Ginsac Colombia SAS, manifiesta su compromiso y relación con las políticas de seguridad establecidas alineadas y aceptadas para la implementación, monitoreo, operación, mantenimiento, revisión y todas las mejoras que se requieran y con la disponibilidad de facilitar y proporcionar los recursos necesarios para el desarrollo y cumplimiento del presente documento.
Ginsac Colombia SAS realizará la publicación, capacitación, sensibilización y socialización al personal, clientes, proveedores y aliados de las directrices, normas, objetivos, leyes, políticas, controles, adoptadas y encaminadas para la seguridad de la organización Ginsac Colombia SAS. La dirección manifiesta el respaldo a los responsables de la seguridad.

9.6 MARCO ORGANIZATIVO DE LA SEGURIDAD DE LA INFORMACIÓN

9.6.1 Responsabilidades de la dirección

- Facilitar y proporcionar los recursos necesarios para el desarrollo del sistema de gestión de la seguridad de la información.

- Asignación de los responsables y gestión de la seguridad de la información.

- Revisión y aceptación en las directrices que componen los controles de seguridad.

- Proporcionar el tiempo y espacio para la publicación, socialización de las directrices adoptadas para la seguridad de la información al personal, clientes, proveedores, aliados que forman parte del manejo de la información.

9.6.2 Responsabilidades del responsable de la seguridad[35]

- Aplicación de conocimientos, habilidades, técnicas para el desarrollo del proyecto que cumpla con las necesidades y expectativas de la organización Ginsac Colombia SAS.

- Identificar vulnerabilidades, brechas o puertas traseras para contrarrestarlos.

- Diseñar un plan de trabajo para la implementación del modelo y políticas de seguridad de la información.

- Seguimiento al cronograma de actividades, tareas, presupuesto, objetivos, etc. previstos en el marco del modelo de seguridad.
- Designación de responsabilidades dentro del marco de seguridad, roles, privilegios, fechas de entregas, tiempos de socialización, etc.

- Coordinación en las actividades diarias y contar con el apoyo administrativo.
- Alinear el marco de seguridad al cumplimiento propuesto para la organización Ginsac Colombia SAS.

- Seguimiento permanente en la ejecución del cronograma de trabajo, monitorear los riesgos, rapidez en soporte a soluciones de seguridad y reportar al comité de seguridad las novedades o incidentes identificados.

- Trabajo en equipo con las áreas designadas.

- Garantizar calidad en el desarrollo y entregas del proyecto de seguridad.

- Velar el mantenimiento, custodia y protección de la documentación del proyecto de seguridad.

[35] ROLES Y Responsabilidades [Anónimo]. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN [EN LINEA]. (26, abril, 2016). [Consultado el 10, noviembre, 2022]. Disponible en Internet: <https://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf>.

- Capacitación y contribución en el fortalecimiento y retroalimentación en la gestión y sensibilización del proyecto de seguridad presentado.

- Liderar y velar por la gestión y seguimiento del cronograma de reuniones de gestión con indicadores actualizados

9.6.3 Responsabilidades del propietario de los riesgos

- Aprobación de los niveles de riesgo residuales, identificados en la evaluación de riesgos.

- Aprobar las estrategias para el tratamiento y mitigación de riesgos a niveles aceptables.

- Conocer de manera detallada la exposición y los riesgos identificados en el análisis de riesgos.

- Garantizar y elaborar propuestas apropiadas para la evaluación de los riesgos[36].

- Informar al grupo de trabajo de gestión de riesgos la socialización periódica de objetivos y conceptos necesarios que les permita tener una visión general de las metas propuestas.

- Informar los resultados obtenidos y relacionados con los riesgos asumidos, presentados en informes de monitoreo y gestión de riesgos.

- Evaluación de la efectividad en las técnicas de administración en gestión de riesgos.

- Capacitar y fortalecer el conocimiento referente a los riesgos a toda la estructura de Ginsac Colombia SAS.

9.6.4 Responsabilidades del responsable de sistemas

- Implementar las medidas y metodologías de seguridad para mitigar y reducir los riesgos.

- Velar por el óptimo funcionamiento de los sistemas y componentes tecnológicos que hacen parte de la organización Ginsac Colombia SAS, el

[36] ROLES Y responsabilidades de la Gestión de Riesgos en PRAM [Anónimo]. 1Library.Co - plataforma para compartir documentos [EN LINEA]. [Consultado el 2, noviembre, 2022]. Disponible en Internet: <https://1library.co/article/roles-responsabilidades-gestión-riesgos-pram.z1e0rrey>.

manejo y uso de la información, activos, recursos, y disponer de las técnicas de seguridad aplicadas en toda la organización.

- Seguimiento y control de las tecnologías de información que le permitan a Ginsac Colombia SAS alcanzar los objetivos y minimizar los riesgos en los dispositivos TI.

- Monitorear, gestionar y garantizar seguridad en los sistemas de información, desarrollos, aplicativos, etc.

- Gestionar e implementación de las directrices de seguridad de gestión de las TI e información.

- Monitorear el control y seguimiento para medir los niveles de cumplimiento en de las medidas de seguridad implementadas en Ginsac Colombia SAS.

- Supervisar incidentes de seguridad, violaciones de acceso, amenazas o riesgos que afecten a la organización.

- Identificar y evaluar pruebas de vulnerabilidad sobre los servicios y dispositivos tecnológicos con los que cuenta Ginsac Colombia SAS, de esta manera mejorar los niveles de seguridad de la organización.

9.6.5 Responsabilidades del personal

- Conocer, cumplir y responsabilizarse de las directrices establecidas en la política de seguridad de Ginsac Colombia SAS.

- Informar incidentes o vulnerabilidades de seguridad identificadas.

- Responsabilidad y confidencialidad de los métodos de accesos a las aplicaciones y sistemas o recursos informáticos y de la información de la organización Ginsac Colombia SAS [37].
- Participación en las presentaciones, publicaciones, capacitaciones, entrenamiento y programas de sensibilización con temas de seguridad informática y seguridad de la información, dispuestos por Ginsac Colombia SAS.

- Confidencialidad con la información almacenada y captada por los sistemas, aplicativos, desarrollos, móviles, etc. de la organización Ginsac Colombia

[37] RM 298-2020-DM-MC. ROLES Y RESPONSABILIDADES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI. (2020). [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://cdn.www.gob.pe/uploads/document/file/1464568/RM%20298-2020-DM-MC%20-%20ANEXO%202.pdf.pdf>.

SAS. Recursos que son necesarios para el desarrollo de actividades y procesos, que una exposición o un mal uso pondría en riesgo la seguridad de la organización.

- Hacer buen uso de los sistemas tecnológicos y recursos con la protección y calidad necesaria.

- Todas las personas y personal que hagan parte de las directrices expuestas en el proyecto de seguridad deberán dar cumplimiento al 100% de los controles expuestos.

9.7 CLASIFICACIÓN DE LAS POLÍTICAS DE SEGURIDAD

Cumpliendo con los estándares de seguridad regulados por la ISO/IEC 27000 y alineados con los 3 pilares de la seguridad de la información, se realiza la siguiente clasificación de políticas que ayudaran a fortalecer y mejorar la seguridad de los sistemas informáticos de Ginsac Colombia SAS.

9.7.1 Política para gestión de activos

Objetivo: Gestionar el manejo, procesamiento, mantenimiento, administración y la protección adecuada para cada uno de los activos de información que hacen parte del SGSI para GINSAC COLOMBIA SAS.

Control:

- Cada equipo tecnológico que formen parte de la infraestructura informática de la compañía, sin importar las sedes o lugar de trabajo remoto; deberán contar con su respectiva hoja de vida alineados con el acta de entrega al colaborar y responsable del activo, documentos que serán anexados a la carpeta de inventarios de activos de la compañía y copia a la hoja de vida del colaborar y responsables asignado.

- Todos los dispositivos tecnológicos conectados e interconectados con la infraestructura de GINSAC deberán contar con los estándares y normas mínimos en seguridad, cumpliendo con lo que rige la ley y controles internos desde el área de tecnología de información. (Antivirus, S.O Original, Licencias o suscripciones activas y vigentes). De no ser así, no tendrán el aval por el área de TI de la compañía para ser conectados e interactuar con los sistemas de información de la organización.

- El equipo de cómputo asignado será de uso corporativo y no personal, todos los dispositivos tecnológicos son revisados, configurados desde el área de TI, los programas instalados sin autorización de GINSAC COLOMBIA SAS, será responsabilidad del colaborador y encargado del equipo de cómputo, será causa de finalización de contrato laboral.

- Asegurar la integridad del equipo asignado y hacer un uso adecuado del mismo, no podrá realizar modificación alguna a la configuración del equipo sin previa autorización de GINSAC COLOMBIA SAS, Usará diligentemente el equipo e introducirá exclusivamente programas computacionales debidamente licenciados otorgados por GINSAC COLOMBIA SAS o con autorización expresa y por escrito del titular de los derechos de carácter intelectual de los mismos.

Funciones de los responsables:

- Todos los colaboradores y responsables de equipos tecnológicos o en su caso que interactúen con los sistemas de información de la compañía, deberán cumplir con los reglamentos, normas y las buenas prácticas exigidas y socializadas por el área de la TI, entre ellas evitaran exponer la máquina al polvo, líquidos, objetos que se puedan introducir, a las vibraciones mecánicas, a temperaturas superiores de 35° C, a los rayos directos del sol y a la humedad y a cualquier otra condición anormal que pueda dañarlo.

- Cada colaborador e integrante de la organización tiene prohibido consumir alimentos o bebidas en espacios con infraestructura informática, que pongan en riesgo los sistemas de información o continuidad de las actividades de la compañía, adicional cada responsable asignado deberá custodiar y proteger los equipos tecnológicos que dispone GINSAC COLOMBIA SAS para cada uno de los colaboradores.

- Reportar cualquier desperfecto, avería o pérdida en el equipo de forma inmediata a GINSAC COLOMBIA SAS, cada responsable se compromete a responder por la pérdida o extravío y daños de los equipos y para lo cual autoriza a GINSAC COLOMBIA SAS a descontar de los pagos adeudados relacionados con el contrato laboral el valor del elemento que se indique.

- No reproducir, copiar, transmitir o disponer del disco duro del equipo de cómputo y la información y datos contenidos en el mismo sin previa autorización de GINSAC COLOMBIA SAS.

- Los responsables y/o encargados de los equipos tecnológicos No concederá a un tercero el uso del equipo asignado, devolverán el equipo asignado en cualquier tiempo que se le solicite, éstos deben estar en las mismas

condiciones que fueron recibidos o con desgastes por sus labores, de no ser así estarían incumpliendo con sanciones establecidas por normativas de GINSAC.

- El área de TI velará por la seguridad de la infraestructura informática entre las podemos resaltar: Ambientes y condiciones apropiados, seguridad física y control de acceso, conexiones y estabilidad con sistemas eléctricos, mantenimientos periódicos, escritorios limpios, socialización del uso adecuado en sistemas de información, etc.

- El área de tecnología de información cada año presentará planes de trabajos y gestiones informáticos para mejorar y maximizar el nivel de madures de las TI dentro y fuera de la compañía. Plan de trabajo revisado y aprobado por la alta dirección.

- Las mejoras en infraestructura informática y equipos tecnológicos se llevarán a cabo por parte del área de TI, jefe administrativa y la alta dirección.

- El área de TI realizara copias de seguridad de cada activo de información de manera periódica, cumpliendo con el cronograma estipulado, resaltado el buen uso y manejo de la copia, funcionalidad y pruebas eficientes. A su vez encriptará las copias de seguridad y protegerá la integridad de las mismas.

9.7.2 Política para el control de acceso

Objetivo: Establecer las reglas y parámetros para proporcionar privilegios dentro de los sistemas de información e infraestructura informática acobijada por la organización. Desde las TI se administrará, gestionará y controlará los permisos a los sistemas y equipos de tecnologías de GINSAC COLOMBIA SAS.

Control:

- Los servidores, infraestructura informática y sistemas de información deberán tener acceso únicamente a roles y perfiles específicamente autorizados por la alta dirección de GINSAC para el desempeño de cada actividades y funciones asignados.

- Los accesos a sistemas de información y plataformas de gestión deberán ser controlados, administrados y centralizados por autenticación y con autorización e implementación de servicios de Windows de Active Directory previa por la jefe administrativa de la compañía.

- El área de tecnologías de información deberá realizar seguimiento periódicamente a las conexiones que se establezcan dentro y fuera de los sistemas de información y plataformas habilitadas por la compañía solo y exclusivamente a personal autorizado.

- El área de TI junto a la alta dirección establecerá cronogramas de auditorías y salvaguardas de información, escritas y autorizadas por gerencia, permitiendo identificar el tráfico y conexiones activas por cada uno de sus usuarios e identificar conexiones y accesos no autorizados.

- Las asignaciones de permisos y accesos para los sistemas de información, plataformas, equipos, correos y demás herramientas tecnológicas deberán ser solicitadas por los jefes inmediatos relacionados con acta de funciones, adjuntados por correo electrónico interno a Gerencia, jefe administrativa y área de TI. Una vez sea aprobado la solicitud por la alta dirección, el colaborador será notificado, capacitado en el acceso y manejo correcto de los sistemas de información de la compañía. Las actas de solicitud serán firmadas y archivadas en las hojas de vida de procesos de la compañía.

- Las conexiones remotas al servidor deberán ser aprobadas por la alta dirección y deberán ser supervisadas de manera continua. Su configuración y conectividad deberá realizarse con los estándares de seguridad exigidos. El área de TI deberá asegurar la conectividad de manera privada y cifrada (VPN).

- Las conexiones a la red, plataformas, sistemas de información y entorno tecnológico e informático de Ginsac, deberá realizarse con dispositivos previamente asignados y autorizados por la alta dirección y TI.

- La seguridad de acceso a recursos de la compañía, solo serán asequibles por personal, dispositivos y roles autorizados. La seguridad de contraseñas o claves de accesos serán procesadas por algoritmos de encriptación. Adicional él envió de documentos confidenciales se realizará por canales seguros, alineados con certificado digitales, evitando ser vulnerados.

- Las conexiones a las plataformas o desarrollos web otorgados por GINSAC a cada colaborador se realizará por accesos basados en ROLES (RBAC), siendo el administrador de TI quien vinculará los permisos necesarios y el alcance de cada rol predefinidos y estandarizados en los sistemas de información y desarrollos de la compañía.

Función del responsable:

- El área de RRHH deberá notificar la desvinculación o finalización de contrato del personal de trabajo en tiempos oportunos a la alta dirección y al área de TI, se realizará la desactivación de acceso y desvinculación de permisos dentro de la infraestructura informática de GINSAC.

- El área de TI deberá supervisar las conexiones y accesos de terceros que han sido autorizados por la alta dirección (Proveedores, nuevos servicios, actualizaciones, etc.).

- Se establecerá control y endurecimiento en la creación de contraseñas o sistemas de autenticación con altos estándares de seguridad.

- Se implementará monitoreo, supervisión y autorías de control de eventos en distintos sectores de la infraestructura informática, que permitan identificar el uso y accesos de cada colaborador con el objetivo de minimizar posibles impactos, riesgo o amenazas y sobre todo asegurar el uso adecuado de los pilares de la seguridad de los sistemas de información (Confidencialidad, Integridad y Disponibilidad).

- Cada colaborador de la compañía tendrá el compromiso de navegar por la internet de manera segura, validar direcciones IP o URL veraces, evitar realizar compras en canales no autorizado o no seguros (sin certificados o protocolos SSL), revisaran que sus programas de protección local (Antivirus) estén activos, realizaran transacciones o procesos bancarios en páginas incognitos, no guardaran contraseñas en los navegadores, etc. cada colaborar contará con el respaldo del área de TI por si tienen alguna inquietud u observan algo anormal en un sitio web.

9.7.3 Política para el buen uso de dispositivos móviles

Objetivo: Promover y asegurara el buen uso de los dispositivos móviles corporativos o de uso personal.

Control:

- Todos los dispositivos móviles deben ser entregados por actas de activos a colaboradores asignados por la alta dirección de Ginsac.

- Cada dispositivo móvil es configurado por el área de TI, quien realizara las entregas con controles de seguridad pertinentes para la preservación y

durabilidad del equipo móvil. (Protector de vidrio, Case, manos libres) de igual manera su IMEI será almacenado en el inventario de activos de GINSAC.

- Cada dispositivo móvil asignado estará enlazado con una SIMCARD corporativa entregada por la alta dirección para sus labores y actividades corporativas.

- Las conexiones móviles a la red inalámbrica y consumo de recursos informáticos deberán ser monitoreadas y administradas por el área de TI, que garantizará una conectividad eficiente, estable y sobre todo segura.

Función del responsable:

- El uso de celulares No CORPORATIVOS dentro de la infraestructura informática de la organización GINSAC, será en horarios de descansos y no interfiera con las actividades y procesos internos de la compañía, de no ser así deberán ser autorizados por la alta dirección y abstenerse a un llamado de atención o finalización de contrato.

9.7.4 Política de seguridad Física y del entorno

Objetivo: Promover controles que permitan minimizar y prevenir accesos físicos no autorizados, daños, manipulación de equipos, conexiones no controladas, etc. poniendo en riesgo la infraestructura y entorno informático de la compañía.

Control:

- Los accesos al servidor físicos y virtuales deberán ser denegados a personal no autorizado. Solo la alta dirección y el área de TI tendrán acceso directo a los ambientes informáticos de la compañía.

- Los equipos de comunicaciones, de seguridad, de RED, informáticos, deberán estar protegidos y aislados de personal no autorizado y capacitado. Cada equipo tecnológico para la administración de la estructura informática deberá estar bajo llave, en ambientes de datos seguros y con la calidad de temperatura adecuado.

Función del responsable:

- El área de TI junto a la alta dirección deberá velar por el respaldo de datos, copias de seguridad, códigos fuentes, activos en peligro, documentos confidenciales, etc. resguardo que deberá contar con la mayor seguridad física y lógica, adicional deberá ser resguardada en sitios extornos al entorno informático.

- La compañía junto a la alta dirección establecerá parámetros de seguridad física (Seguridad biométrica) para el registro de entrada y salida del personal de trabajo, les permitirá obtener monitoreo continuo del personal que permanece en cada una de sus sedes a nivel nacional.

- La compañía contara con una infraestructura adecuada y segura que permita la distribución por separado de las distintas líneas eléctricas, de comunicaciones y de datos que hagan parte fundamental para el entorno de sistemas de información e informáticos de Ginsac.

- El área de TI deberá contar con inventarios de activos físicos actualizados y organizados en cada distribución de las sedes de la compañía, tendrá la facultad de identificar si un equipo ha sido retirado de su sitio asignado y puntualizar algún cambio físico de manera inmediata.

- Todos los colaboradores deberán informar si observan alguna eventualidad, daño o personal sospechosos dentro de las instalaciones de GINSAC.

9.7.5 Política para la seguridad de la red y dispositivos de almacenamiento

Objetivo: Implementar seguridad en los entornos de red fundamentales para la infraestructura informática y operatividad de la compañía, promocionará controles importantes para el óptimo manejo, gestión y administración de los entornos de red y medios de almacenamiento de Ginsac.

Control:

- Se deben tener diseñadas diagramas o planos de las distribuciones eléctricas y líneas de datos de los entornos de red de cada una de las sedes. Siendo estos documentos custodiados junto a la distribución y topologías previamente configuradas y asequible por personal autorizado.

- Las bases de datos que alojan la integración de los desarrollos web y locales de los sistemas de información, serán acobijados con un Firewall de bases de datos, maximizando la seguridad, integridad, confiabilidad y disponibilidad de la información que resguarda.

- Los medios o dispositivos de almacenamiento dispuestos por la alta dirección al área de TI para el desarrollo de copias de seguridad deberán ser transportados y manipulados por personal autorizado, deberán estar alineados con actas y monitoreo de gerencia.

- El manejo de medios extraíbles o unidades de almacenamiento externas a las corporativas deberán ser analizadas, autorizo y monitoreado por el área de TI, el uso de los dispositivos de almacenamiento deberá cumplir con controles mínimos de seguridad y estar libres de malware o software malicioso que pueda contaminar la infraestructura informática y los sistemas de información.

- El almacenamiento y traslado de información por medios de almacenamiento deberán estar autorizados por la alta dirección y el área de TI de GINSAC. Se aplicará algoritmos de encriptación y métodos HASH para validar la integridad de la información que reposa allí.

- Cada dispositivo tecnológico que forma parte del entorno informáticos de la compañía deberá contar con antivirus y licencias originales. Estas serán evaluadas y administras desde el área de TI.

- Todos los equipos tecnológicos y sistemas de seguridad deberán estar actualizados, los responsables de TI deberán documentar y velar periódicamente que cada punto se encuentre en óptimas condiciones y con las actualizaciones más recientes.

Función del responsable:

- El área de TI alinea la seguridad de la red mediante claves encriptadas (WPA2 Y WPA3) que restringe el acceso a la red WIFI con altos estándares de seguridad. Cambiando periódicamente las claves de acceso a la red WIFI de las sedes de la compañía.

- La alta dirección y TI, tendrán la responsabilidad del flujo de tráfico y monitoreo de la red en tiempo real, reforzara la seguridad de la red con Firewall de nuevas generaciones y sistemas de detección (IDS/IPS),

previniendo posibles intrusiones, actividades maliciosas e inclusive filtraciones o accesos no autorizadas.

- El área de tecnologías de información deberá mejorar el nivel de seguridad en los desarrollos web que tienen actualmente y futuras aplicaciones. Será implementado WAF un Firewall para aplicaciones web que supervise, filtre y bloquee posibles intrusiones, su administración será responsabilidad del área de TI o de terceros si es proveedor.

- El área de TI velará por la mejor distribución y optimización de los recursos de internet de cada sede, permitirá acceso a navegaciones autorizadas por la alta dirección, limitará el acceso a personal no autorizado, filtrará páginas con malware, prohibirá descarga de aplicaciones o archivos de internet sin previa autorización.

9.7.6 Política para el manejo y gestión de contraseñas

Objetivo: Proponer de manera adecuada con estándares altos en seguridad el manejo y asignación de contraseñas.

Control:

- El uso correcto y la seguridad de cada licencia dispuesta por la alta dirección a los colaboradores de la compañía será para uso corporativo y laboral, no se permitirá para actividades personales o externas, ni mucho menos transferir o compartir su licencia. Cabe resaltar que serán monitoreados por la alta dirección y el área de TI el uso que se le dé.

- La asignación y creación de contraseña deberá contar con parámetros de seguridad como: Longitud mínima de 8 dígitos, contar con al menos un número, una mayúscula, una minúscula, una letra, un carácter especial.

- No se permitirá la asignación de la misma contraseña en varias plataformas o sistemas de información de la compañía, deberán ser diferentes para cada aplicativo, actividad y procesos.

- El cambio de contraseña será vigilado y auditado por el área de TI de manera periódica, cada 60 días se deberá realizar el cambio de contraseña en cada aplicativo y sistema de información bajo los parámetros permitidos en la creación de contraseñas.

- El almacenamiento de contraseña será acobijado por algoritmos de cifrados que maximizan las seguridad e integridad de esta.

Función del responsable:

- Cada colaborador tendrá asignado un usuario y una contraseña para interactuar con los sistemas de información de la compañía y será responsabilidad de cada colaborador el buen uso de su cuenta frente algún incidente de seguridad.

9.7.7 Política para los controles y métodos criptográficos

Objetivo: Integrar controles y metodologías para el cifrado de contraseñas, documentos y sistemas de información.

Control:

- El resguardo e implementación de seguridad de documentos confidenciales se realizará con métodos de algoritmos criptográficos simétricos y asimétricos, sea el caso y el uso adecuado para cada proceso.

- Las copias de seguridad generadas en cada aplicativo o sistemas de información serán encriptadas y resguardadas por personal autorizado y la alta dirección de la compañía, adicional contara con un acta que soporte la extracción y creación de las copias, estarán alineados con métodos HASH para validar la integridad y seguridad de la información.

Función del responsable:

- Las claves de encriptación y desencriptación serán creadas por el área de TI y serán administradas y asignadas solo por la alta dirección de GINSAC.

- La documentación confidencial será protegida mediante firmas digitales, que serán legibles y manipulados solo por el personal autorizado y responsables asignados por la alta dirección.

10 CONCLUSIONES

Se realizó un buen diseño del SGSI, utilizando herramientas y las buenas prácticas avaladas por normas internacionales, que fueron esenciales para obtener el resultado del diagnóstico del estado actual de las tecnologías de información y el nivel de madurez, funcionalidad y seguridad de cada proceso y sistema informático. Resultados considerables para el mejoramiento en seguridad de la información y factores claves e importantes que se encuentran en riesgo como lo es las tecnologías, procesos y sobre todo el personal que interactúa con los sistemas informáticos de la compañía.

El análisis que hizo a la compañía con ayuda de herramientas del Instituto Nacional en Ciberseguridad (INCIBE), se pudo obtener un resultado del riesgo actual y su nivel de madurez en seguridad de las tecnologías de información, con una calificación que es básica y con necesidades en mejoramiento de seguridad, concienciación, gestión, administración y efectividad que serán acobijados en el diseño del SGSI fundamental para la continuidad de los procesos del negocio.

Durante el levantamiento de información del inventario de activos de la infraestructura informática y sistemas de información de la compañía, se realizó por las buenas prácticas de la norma ISO/IEC 27001, que indica un paso a paso del buen diseño de un sistema de gestión para la seguridad de la información que acobija y mejora la seguridad de los sistemas y procesos de la compañía.

Se implementó técnicas relacionadas con la metodología de MAGERIT, que fueron esenciales para clasificar cada activo de información, dimensionar el impacto del riesgo al que está expuesto, y mejorar de manera oportuna los niveles en seguridad de cada activo.

Se realizó la valoración, evaluación y clasificación de los activos de información cumpliendo los requerimientos que indica la norma ISO/IEC 27000, preservando los 3 pilares de la seguridad de la información (Confidencialidad, Integridad y Disponibilidad), que fueron de ayuda para determinar la importancia y el nivel de vulnerabilidad al que estaba expuesto y la amenaza que presentaba a los sistemas informáticos de la compañía.

Se diseñó un sistema de gestión de la seguridad de la información que se basó en el resultado del análisis actual en seguridad y la evaluación de los riesgos, amenazas y vulnerabilidades relacionadas con cada activo. Cada activo es clasificado sobre el nivel de aceptación del riesgo que es asociado por su impacto y la prioridad de ocurrencia. Se determino los métodos, controles y prioridades necesarios para fortalecer los sistemas de información y mejorar la seguridad del entorno informático de la compañía, a partir de la norma ISO/IEC 27001:2013.

Se presentó propuestas de políticas en seguridad de la información, relacionadas con la situación actual de los sistemas de información de la compañía, que ayudarán desde las tecnologías de información a fortalecer y aumentar el nivel de seguridad de la infraestructura tecnológica y estarán alineados a la norma ISO/IEC 27001:2013. Sera ideal para que la alta gerencia de Ginsac Colombia SAS, evalué y apruebe controles y políticas en seguridad y mejoramiento de los sistemas de información de la compañía.

Las propuesta que se presentó a la alta gerencia de Ginsac Colombia SAS de controles y políticas que ayudarán a mitigar riesgos y a mejorar la seguridad informática de compañía, debió ser evaluado y gestionada para resaltar la eficiencia de los procesos internos, garantizar el tratamiento de datos, mejorar el cumplimiento de normativas legales y sobre todo garantizar a sus clientes confiablidad de su información, eficacia de sus procesos y garantes de sistemas de información fiables y confiables.

11 RECOMENDACIONES

Se debe asignar un responsable para el manejo del sistema de gestión de la seguridad de la información diseñado para la empresa Ginsac Colombia SAS, quien velara por la correcta administración, gestión e implementación de los procesos que ayudaran a mejorar y aumentar el nivel de madurez y seguridad de los sistemas informáticos y sistemas de información, que será avalado y vigilado por la alta gerencia de la compañía.

Ginsac Colombia SAS deberá realizar seguimiento e implementación de mejoras periódicas al sistema de gestión de la seguridad de la información, con apoyo de nuevas tecnologías, con planes de contingencia y continuidad del negocio, con compromiso y relación de nuevas políticas de seguridad establecidas y aceptadas, también facilitar y proporcionar recursos necesarios para la implementación y cumplimiento del presente SGSI diseñado.

Ginsac Colombia SAS una vez apruebe la implementación del diseño del sistema de gestión de la seguridad de la información, deberá realizar la publicación, capacitación, sensibilización y socialización al personal, proveedores, clientes y demás participantes. Manifestara su respaldo y responsabilidad frente al mejoramiento en seguridad de sus sistemas de información, calidad de sus procesos y servicios.

Los responsables de las tecnologías de información y del SGSI, deberán realizar periódicamente o en periodos cortos de tiempo estipulados en políticas de seguridad, el inventario de activos actuales, evaluación de riesgos, seguimiento y fortalecimiento de nuevas políticas y controles de seguridad. Que les permita protegerse de nuevas amenazas tecnológicas y sobre todo que les permitan evidenciar el resultado de las buenas prácticas del SGSI propuesto para la Ginsac Colombia SAS.

La alta dirección de Ginsac Colombia SAS deberá monitorear el manejo del SGSI por el responsable asignado, evaluando la criticidad residual por periodos de tiempos, controles aplicados, la probabilidad de impacto y el seguimiento de los niveles de aceptación estipulados en SGSI bajo su aprobación. Sus resultados serán fundamentales para contar con sistemas de información confiables y seguros, además de ser garantes de sistemas de informáticos eficaces.

El fortalecimiento del SGSI diseñado para Ginsac Colombia SAS deberá realizarse continuamente, le permitirá contar con información de nuevos riesgos a los que está expuesto su entorno tecnológico, calificar las estrategias actuales y endurecerlas, implementar nuevas tecnologías en seguridad física y digital, sobre todo mejorar la administración y gestión de los sistemas de la información.

Es necesario contar con la ayuda de especialistas en seguridad de los sistemas informáticos, para que realicen pruebas de Pentesting o pruebas de penetración a los sistemas de información, evaluando la efectividad de soluciones en seguridad implementadas actualmente y sobre todo priorizar y tomar las medidas necesarias e indispensables para asegurar los procesos, tecnologías y servicios expuestos por la compañía en ambientes informáticos.

Para la implementación del SGSI se deberán diseñar y definir las estrategias en seguridad que serán alineadas al diseño del SGSI propuesto, asegurará los activos de información, será controlado y aplicado con las políticas propuestas fundamentales para contar con tecnología eficiente, procesos activos y seguros, eficacia en las actividades y servicios de la compañía y vigilados por normativas de la ISO/IEC 27000.

BIBLIOGRAFÍA

ADMINISTRADOR SYSTEM. Qué es el riesgo de Seguridad de información. LD GRUPO (blog) [EN LINEA]. (19, abril, 2019). [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://www.ldgrupo.com.pe/que-es-el-riesgo-de-seguridad-de-informacion/>.

ADMINISTRADOR. Qué es el riesgo de Seguridad de información». LD GRUPO (blog). System [EN LINEA]. (10, abril, 2019). [Consultado el 25, junio, 2022]. Disponible en Internet: <https://www.ldgrupo.com.pe/que-es-el-riesgo-de-seguridad-de-informacion/>.

ADRIEL, Araujo. ISO 27001: Cómo hacer tu política del SGSI - Hackmetrix Blog. Hackmetrix Blog [EN LINEA]. (9, septiembre, 2021). [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://blog.hackmetrix.com/politica-del-sgsi/>.

ARAUJO, Adriel. ISO 27001: Cómo hacer tu política del SGSI - Hackmetrix Blog. Hackmetrix Blog [EN LINEA]. (9, septiembre, 2021). [Consultado el 9, abril, 2022]. Disponible en Internet: <https://blog.hackmetrix.com/politica-del-sgsi/>.

ARAUJO, Adriel. ISO 27001: Cómo hacer tu política del SGSI - Hackmetrix Blog. Hackmetrix Blog [EN LINEA]. (9, septiembre, 2021). [Consultado el 25, junio, 2022]. Disponible en Internet: <https://blog.hackmetrix.com/politica-del-sgsi/>.

ARDANZA, Aitziber. Ciclo PDCA de gestión de la ISO 27001. GlobalSuite Solutions [EN LINEA]. (10, enero, 2022). [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://www.globalsuitesolutions.com/es/ciclo-pdca-iso-27001/>.

ARDANZA, Aitziber. Ciclo PDCA de gestión de la ISO 27001. GlobalSuite Solutions [EN LINEA]. (10, enero, 2022). [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://www.globalsuitesolutions.com/es/ciclo-pdca-iso-27001/>.

AUTODIAGNÓSTICO LIGERO, INCIBE - Instituto Nacional de Ciberseguridad [Anónimo]. Autodiagnóstico ligero, INCIBE - Instituto Nacional de Ciberseguridad [EN LINEA]. [Consultado el 25, junio, 2022]. Disponible en Internet: <https://adl.incibe.es/questions.php#resultado>.

CALDERON, Marco. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III -Guía de Técnicas. Academia.edu - Share research [EN LINEA]. [Consultado el 10, diciembre, 2022]. Disponible en Internet: <https://www.academia.edu/27331595/MAGERIT_versión_3_0_Metodología_de_Análisis_y_Gestión_de_Riesgos_de_los_Sistemas_de_Información_Libro_III_Guía_de_Técnicas>.

CÓMO MITIGAR riesgos en ISO 27001: opciones disponibles [Anónimo]. Software 45001 - ISOTools Chile [EN LINEA]. [Consultado el 25, junio, 2022]. Disponible en Internet: <https://www.isotools.cl/mitigar-riesgos-iso-27001/>.

CÓMO MITIGAR riesgos en ISO 27001: opciones disponibles [Anónimo]. Software 45001 - ISOTools Chile [EN LINEA]. (2022). [Consultado el 25, junio, 2022]. Disponible en Internet: <https://www.isotools.cl/mitigar-riesgos-iso-27001/>.

CONOCES TUS riesgos [Anónimo]. INCIBE [EN LINEA]. (27, enero, 2016). [Consultado el 3, octubre, 2022]. Disponible en Internet: <https://www.incibe.es/protege-tu-empresa/conoces-tus-riesgos>.

CONOCES TUS riesgos [Anónimo]. INCIBE [EN LINEA]. (27, enero, 2016). [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://www.incibe.es/protege-tu-empresa/conoces-tus-riesgos>.

DIARIO OFICIA. El CONGRESO DE COLOMBIA. LEY 1273 DE 2009 [EN LINEA]. [Consultado el 15, junio, 2022]. Disponible en Internet: <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf>.

EL CONGRESO DE COLOMBIA. LEY 1273 DE 2009. Diario Oficial [EN LINEA]. (5, enero, 2009). [Consultado el 10, junio, 2022]. Disponible en Internet: <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf>.

ELABORACIÓN DE la política general de seguridad y privacidad de la información [Anónimo]. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN [EN LINEA]. [Consultado el 25, junio, 2022]. Disponible en Internet: <https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf>.

ELABORACIÓN DE la política general de seguridad y privacidad de la información [Anónimo]. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN LINEA]. [Consultado el 23, mayo, 2022]. Disponible en Internet: <https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf>.

EMPRESARIAL LISOT INFORMÁTICA. ¿Qué es un sistema de Gestión de la Seguridad de la información (SGSI)? LISOT EN LINEA]. (14, mayo, 2018). [Consultado el 2, noviembre, 2022]. Disponible en Internet: <https://www.lisot.com/que-es-un-sistema-de-gestion-de-la-seguridad-de-la-informacion-sgsi/>.

EXCELLENCE, ISOTools. ¿Cómo clasificar los activos de seguridad en un SGSI? PMG SSI - ISO 27001 [EN LINEA]. (6, mayo, 2015). [Consultado el 2, diciembre,

2022]. Disponible en Internet: <https://www.pmg-ssi.com/2015/05/como-clasificar-los-activos-de-seguridad-en-un-sgsi/>.

F. L. GÓMEZ Y. R. P. FERNÁNDEZ. Cómo implantar un SGSI según une-en ISO/IEC 27001 y su aplicación en el esquema nacional de seguridad. E-Libro [EN LINEA]. (2018). Disponible en Internet: <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/53624>.

FERNÁNDEZ RIVERO PEDRO PABLO Y. LUIS GÓMEZ FERNÁNDEZ. https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/53624?page=86. E-Libro [EN LINEA]. (2018). [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/53624?page=86>.

FIRMA-E. ¿Qué es un SGSI – Sistema de Gestión de Seguridad de la Información? | Firma-e. Firma-e | Proyectos y formación [EN LINEA]. (19, febrero, 2013). [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://www.firma-e.com/blog/que-es-un-sgsi-sistema-de-gestion-de-seguridad-de-la-informacion/>.

FIRMA-E. ¿Qué es un SGSI – Sistema de Gestión de Seguridad de la Información? | Firma-e. Firma-e | Proyectos y formación [EN LINEA]. [Consultado el 8, junio, 2022]. Disponible en Internet: <https://www.firma-e.com/blog/que-es-un-sgsi-sistema-de-gestion-de-seguridad-de-la-informacion/>.

GERENCIA. Política de seguridad. FIDETIA [EN LINEA]. (30, abril, 2015). [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://www.fidetia.es/politica_seguridad.php>.

GINSAC COLOMBIA | Maquinaria Agrícola [Anónimo]. Ginsac Colombia | Maquinaria Agrícola [EN LINEA]. (2022). [Consultado el 25, junio, 2022]. Disponible en Internet: <https://www.ginsac.com.co/nosotros.php>.

GÓMEZ F. L. Y. R. P. FERNÁNDEZ. Cómo implantar un SGSI según une-en ISO/IEC 27001 y su aplicación en el esquema nacional de seguridad. [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/53624>.

HERRAMIENTA DE autodiagnóstico [Anónimo]. Autodiagnóstico ligero, INCIBE - Instituto Nacional de Ciberseguridad [EN LINEA]. [Consultado el 25, junio, 2022]. Disponible en Internet: <https://adl.incibe.es/pdfs/Personas_medio.pdf>.

INCIBE. ¿Conoces tus riesgos? INCIBE [EN LINEA]. (27, enero, 2016). [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://www.incibe.es/protege-tu-empresa/conoces-tus-riesgos>.

INCIBE. Autodiagnóstico ligero, INCIBE - Instituto Nacional de Ciberseguridad. Autodiagnóstico ligero, INCIBE - Instituto Nacional de Ciberseguridad [EN LINEA]. [Consultado el 25, junio, 2022]. Disponible en Internet: <https://adl.incibe.es/questions.php#resultado>.

INCIBE. Autodiagnóstico ligero, INCIBE - Instituto Nacional de Ciberseguridad. [Consultado el 5, junio, 2022]. Disponible en Internet: <https://adl.incibe.es/pdfs/Procesos_medio.pdf>.

INCIBE. Guia_apoyo_SGSI.pdf. (30, mayo, 2022). [Consultado el 21, junio, 2022]. Disponible en Internet: <https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf>.

INCIBE. Herramienta de autodiagnóstico. Autodiagnóstico ligero, INCIBE - Instituto Nacional de Ciberseguridad [EN LINEA]. [Consultado el 25, junio, 2022]. Disponible en Internet: <https://adl.incibe.es/pdfs/Tecnologia_medio.pdf>.

INCIBE. Herramienta de autodiagnóstico. Autodiagnóstico ligero, INCIBE - Instituto Nacional de Ciberseguridad [EN LINEA]. [Consultado el 25, junio, 2022]. Disponible en Internet: <https://adl.incibe.es/pdfs/Tecnologia_medio.pdf>.

INCIBE. PLAN DIRECTOR DE SEGURIDAD. PROTEGE TU EMPRESA [EN LINEA]. [Consultado el 25, junio, 2022]. Disponible en Internet: <https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf>.

ISO 27000 [Anónimo]. Baja Consulting Group [EN LINEA]. (20, agosto, 2017). [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://www.bajacg.com/uncategorized/iso-27000/>.

ISO 27001 - Software ISO 27001 de Sistemas de Gestión [Anónimo]. Software ISO [EN LINEA]. [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/>.

ISO 27001. ISO 27001 - Software ISO 27001 de Sistemas de Gestión. Software ISO [EN LINEA]. [Consultado el 8, junio, 2022]. Disponible en Internet: <https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/>.

ISO 27001: Los activos de información [Anónimo]. PMG SSI - ISO 27001 [EN LINEA] (30, mayo, 2015). [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://www.pmg-ssi.com/2015/03/iso-27001-los-activos-de-informacion/>.

ISO 27001: Los activos de información. PMG SSI - ISO 27001 [EN LINEA]. (30, marzo, 2015). [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://www.pmg-ssi.com/2015/03/iso-27001-los-activos-de-informacion/>.

ISO/IEC 27001:2013(EN) Information technology — Security techniques — Information security management systems — Requirements [Anónimo]. Online Browsing Platform (OBP) [EN LINEA]. [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en>.

ISOTOOLS. Cómo mitigar riesgos en ISO 27001: opciones disponibles. Software 45001 - ISOTools Chile [EN LINEA]. [Consultado el 25, junio, 2022]. Disponible en Internet: <https://www.isotools.cl/mitigar-riesgos-iso-27001/>.

JEFATURA DEL ESTADO. BOE.es - BOE-A-2018-12257 Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. BOE.es - Agencia Estatal Boletín Oficial del Estado [EN LINEA]. (7, septiembre, 2018). [Consultado el 24, julio, 2022]. Disponible en Internet: <https://www.boe.es/eli/es/rdl/2018/09/07/12>.

JEFATURA DEL ESTADO. BOE.es - BOE-A-2018-12257 Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. BOE.es - Agencia Estatal Boletín Oficial del Estado [EN LINEA]. (7, septiembre, 2018). [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://www.boe.es/eli/es/rdl/2018/09/07/12>.

JEFATURA DEL ESTADO. BOE.es - BOE-A-2018-12257 Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. BOE.es - Agencia Estatal Boletín Oficial del Estado [EN LINEA]. (2018). [Consultado el 15, junio, 2022]. Disponible en Internet: <https://www.boe.es/eli/es/rdl/2018/09/07/12>.

JEFFERSON FABIAN BARBOSA SALINAS Y. DAVID ALEJANDRO GONZÁLEZ VARGAS. DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001:2013 PARA TELEMEDICINA EN LA IPS COLOMBIANA DE TRASPLANTES. [s.l.]: UNAD, 2021. 189 p.

LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal [Anónimo]. Noticias Jurídicas [EN LINEA]. [Consultado el 24, mayo, 2022]. Disponible en Internet: <https://noticias.juridicas.com/base_datos/Anterior/r3-lo15-1999.html>.

LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal [Anónimo]. Noticias Jurídicas [EN LINEA]. [Consultado el 24, mayo, 2022]. Disponible en Internet: <https://noticias.juridicas.com/base_datos/Anterior/r3-lo15-1999.html>.

LIBRARY.CO. Roles y responsabilidades de la Gestión de Riesgos en PRAM. 1Library.Co - plataforma para compartir documentos [EN LINEA]. [Consultado el 4, mayo, 2022]. Disponible en Internet: <https://1library.co/article/roles-responsabilidades-gestión-riesgos-pram.z1e0rrey>.

MAGERIT V.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información [Anónimo]. PAe - MAGERIT v.3 [EN LINEA]. (octubre, 2012). [Consultado el 22, junio, 2022]. Disponible en Internet: <https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.YrdL9XbMKUk>.

MINTIC. Elaboración de la política general de seguridad y privacidad de la información. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN [EN LINEA]. [Consultado el 23, mayo, 2022]. Disponible en Internet: <https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf>.

MINTIC. Elaboración de la política general de seguridad y privacidad de la información. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN [EN LINEA]. [Consultado el 23, mayo, 2022]. Disponible en Internet: <https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf>.

MINTIC. Políticas de Operación Proceso de Tecnologías de la Información. Inicio - Función Pública [EN LINEA]. (marzo, 2020). [Consultado el 15, junio, 2022]. Disponible en Internet: <https://www.funcionpublica.gov.co/documents/418537/36701283/politica-de-seguridad-de-la-informacion.pdf.pdf/325019e5-a92f-0b44-3676-2356bd71240c?t=1586355315672>.

MINTIC. Políticas de Operación Proceso de Tecnologías de la Información. Seguridad de la Información Documento Técnico [EN LINEA]. (marzo, 2020). [Consultado el 15, junio, 2022]. Disponible en Internet: <https://www.funcionpublica.gov.co/documents/418537/36701283/politica-de-seguridad-de-la-informacion.pdf.pdf/325019e5-a92f-0b44-3676-2356bd71240c?t=1586355315672>.

MINTIC. Roles y Responsabilidades. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN [EN LINEA]. [Consultado el 24, mayo, 2022]. Disponible en Internet: <https://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf>.

MINTIC. Roles y Responsabilidades. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN [EN LINEA]. [Consultado el 24, mayo, 2022]. Disponible en Internet: <https://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf>.

NIEVES, ARLENYS CAROLINA. DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADOS EN LA NORMA. Principal [EN LINEA]. (2017). [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://alejandria.poligran.edu.co/bitstream/handle/10823/994/Trabajo%20Final.pdf?sequence=1&isAllowed=y>.

NOTICIAS JURÍDICAS [Anónimo]. Noticias Jurídicas [EN LINEA]. (30, julio, 2018). [Consultado el 25, junio, 2022]. Disponible en Internet: <https://noticias.juridicas.com/base_datos/Anterior/r3-lo15-1999.html>.

PEDRO PABLO FERNÁNDEZ RIVERO Y. LUIS GÓMEZ FERNÁNDEZ. https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/53624/?page=86. E-Libro [EN LINEA]. (2018). [Consultado el 25, junio, 2022]. Disponible en Internet: <https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/53624/?page=86>.

PMG SSI ISO 27001. ISO 27001: Los activos de información. Blog especializado en Seguridad de la Información y Ciberseguridad [EN LINEA]. (30, marzo, 2015). [Consultado el 18, junio, 2022]. Disponible en Internet: <https://www.pmg-ssi.com/2015/03/iso-27001-los-activos-de-informacion/>.

PMG SSI. ¿Cómo clasificar los activos de seguridad en un SGSI? PMG SSI - ISO 27001 [EN LINEA]. (mayo, 2015). [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://www.pmg-ssi.com/2015/05/como-clasificar-los-activos-de-seguridad-en-un-sgsi/>.

POLÍTICAS DE Operación Proceso de Tecnologías de la Información [Anónimo]. Inicio - Función Pública [EN LINEA]. (marzo, 2020). [Consultado el 10, octubre, 2022]. Disponible en Internet: <https://www.funcionpublica.gov.co/documents/418537/36701283/politica-de-seguridad-de-la-informacion.pdf.pdf/325019e5-a92f-0b44-3676-2356bd71240c?t=1586355315672>.

QUÉ ES un SGSI – Sistema de Gestión de Seguridad de la Información | Firma-e [Anónimo]. Firma-e | Proyectos y formación [EN LINEA]. [Consultado el 8, junio, 2022]. Disponible en Internet: <https://www.firma-e.com/blog/que-es-un-sgsi-sistema-de-gestion-de-seguridad-de-la-informacion/>.

QUÉ ES un sistema de Gestión de la Seguridad de la información (SGSI) [Anónimo]. LISOT [EN LINEA]. (14, mayo, 2018). [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://www.lisot.com/que-es-un-sistema-de-gestion-de-la-seguridad-de-la-informacion-sgsi/>.

QUÉ ES un sistema de Gestión de la Seguridad de la información (SGSI) [Anónimo]. LISOT [EN LINEA]. (14, abril, 2018). [Consultado el 2, diciembre, 2022]. Disponible

en Internet: <https://www.lisot.com/que-es-un-sistema-de-gestion-de-la-seguridad-de-la-informacion-sgsi/>.

RINCON BRITO, Cesar Daniel. DISEÑO DE UN SGSI (SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN) BASADO EN LA NORMA INTERNACIONAL ISO/IEC 27001:2013 PARA LA COMPAÑÍA ESSENSALE S.A.S. [s.l.]: UNAD. 128 p.

RINCON, Brito Cesar Daniel. ¿Cómo clasificar los activos de seguridad en un SGSI? PMG SSI - ISO 27001 [EN LINEA]. (6, mayo, 2015). [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://www.pmg-ssi.com/2015/05/como-clasificar-los-activos-de-seguridad-en-un-sgsi/>.

RM 298-2020-DM-MC. ROLES Y RESPONSABILIDADES DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – SGSI. (2020). [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://cdn.www.gob.pe/uploads/document/file/1464568/RM%20298-2020-DM-MC%20-%20ANEXO%202.pdf.pdf>.

ROLES Y Responsabilidades [Anónimo]. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN [EN LINEA]. (26, abril, 2016). [Consultado el 10, noviembre, 2022]. Disponible en Internet: <https://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf>.

ROLES Y responsabilidades de la Gestión de Riesgos en PRAM [Anónimo]. 1Library.Co - plataforma para compartir documentos [EN LINEA]. [Consultado el 2, noviembre, 2022]. Disponible en Internet: https://1library.co/article/roles-responsabilidades-gestión-riesgos-pram.z1e0rrey>
.

ROLES Y responsabilidades de la Gestión de Riesgos en PRAM [Anónimo]. 1Library.Co - plataforma para compartir documentos [EN LINEA]. [Consultado el 24, mayo, 2022]. Disponible en Internet: <https://1library.co/article/roles-responsabilidades-gestión-riesgos-pram.z1e0rrey>.

SALINAS JEFFERSON FABIAN BARBOSA Y. DAVID ALEJANDRO GONZÁLEZ VARGAS. DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001:2013 PARA TELEMEDICINA EN LA IPS COLOMBIANA DE TRASPLANTES. SGSI [página web]. [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://www.iso27000.es/sgsi.html>.

SANDRA PAOLA MOLINA BRAVO Y. JACK DENNIS QUINTERO TORRES. DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA EMPRESA BONOS Y DESCUENTOS S.A.S, A PARTIR DE LA NORMA ISO 27001:2013. [s.l.]: [s.n.], 2022. 136 p.

SOFTWARE ISO. ISO 27001 - Software ISO 27001 de Sistemas de Gestión. Sistemas de Gestión la Seguridad de la Información [EN LINEA]. [Consultado el 8, junio, 2022]. Disponible en Internet: <https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/>.

SYSTEM ADMINISTRADOR. Qué es el riesgo de Seguridad de información. LD GRUPO (blog) [EN LINEA]. (10, abril, 2019). [Consultado el 10, octubre, 2022]. Disponible en Internet: <https://www.ldgrupo.com.pe/que-es-el-riesgo-de-seguridad-de-informacion/>.

ANEXOS

Anexo A. Encuentra análisis de riesgo de información Ginsac Colombia SAS

Encuesta de análisis de riesgo de información Ginsac Colombia SAS

¿Controla el acceso a sus dependencias?

- ☐ No, el acceso es libre
- ☐ Usamos tarjetas de acceso / llaves
- ☑ Tenemos elementos físicos que bloquean la entrada (por ejemplo, tornos o puertas con control de acceso); solo se permite el acceso identificado
- ☑ Tenemos cámaras de seguridad
- ☑ Tenemos un guardia de seguridad que controla los accesos

¿Tiene definida algún tipo de política de gestión de contraseñas?

- ○ No
- ◉ Sí, el usuario escoge su contraseña
- ○ Nuestro servidor central nos obliga a cambiar la contraseña cada cierto tiempo
- ○ Sí, tenemos una política de gestión de contraseñas, bien definida y de obligado cumplimiento

¿Cómo se deshace de la información, los soportes y sistemas que no va a utilizar?

- ◉ Los tiramos a la basura
- ○ Tenemos, una destructora de papel, el resto a la basura
- ○ Subcontratamos su destrucción
- ○ Disponemos de una política de destrucción de papeles y soportes; formateamos los soportes y destruimos los papeles según la normativa vigente

¿Tiene presencia su empresa en las redes sociales?

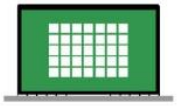
- ○ Sí, tenemos una cuenta de Twitter o Facebook... creo
- ○ Tenemos cuenta en un par de redes sociales, pero las actualizamos sólo cuando hay algo importante
- ◉ Tenemos presencia en varias redes sociales y una persona que las mantiene actualizadas (Community Manager)
- ○ No, en ninguna

¿Cuánto tiempo podría estar su empresa sin acceso al correo electrónico sin que esto le supusiera un problema?

- ○ Menos de 4 horas
- ◉ Más de 4 horas pero menos de un día
- ○ Entre 1 y 5 días
- ○ Más de 5 días, no es fundamental para mi actividad o tengo prevista una alternativa

¿Con qué frecuencia realiza copias de seguridad de sus equipos y del correo electrónico?

- ○ Cuando me acuerdo
- ○ Nunca / No lo sé
- ○ Una vez al mes
- ○ Cada semana
- ◉ Todos los días



¿Qué servicio de correo electrónico utilizan?

- ○ Usamos un correo gratuito (Gmail, Yahoo, etc.)
- ○ Mantenemos nuestro propio servidor de correo electrónico
- ○ Tenemos nuestro propio servidor de correo, lo mantiene un técnico externo
- ◉ Lo tenemos contratado a una empresa de servicios

¿Quién crea y elimina las cuentas de correo electrónico de su empresa?

- ○ Todos los usuarios
- ○ Algunos usuarios autorizados
- ◉ Nuestro informático en plantilla
- ○ La empresa de servicios que nos gestiona el correo

¿Cuánto tiempo podría estar su empresa con la página web caída sin que las pérdidas sean considerables?

- ○ Menos de 4 horas
- ○ Más de 4 horas pero menos de un día
- ◉ Entre 1 y 5 días
- ○ Más de 5 días, no es fundamental para mi actividad o tengo prevista una alternativa

¿Con qué frecuencia realiza copias de seguridad de los contenidos de su página web?

¿Quién tiene acceso a la carga de los contenidos de su página web?

- ○ Todos los usuarios
- ○ Algunos usuarios autorizados
- ◉ Nuestro informático en plantilla
- ○ La empresa de mantenimiento informático que tenemos contratada

¿Con qué frecuencia actualiza la herramienta que gestiona los contenidos de su página web?

- ○ Nunca / No lo sé
- ○ Cuando me acuerdo
- ◉ Una vez al mes
- ○ Cada vez que sale una actualización

¿Con qué frecuencia realiza copias de seguridad de sus sistemas?

Cuando me acuerdo | Nunca / No lo sé | Una vez al mes | Cada semana | Todos los días

¿Considera que cumple la legislación en materia de seguridad?

No / No lo necesito | No estoy segur@ | No estoy al día de todo | Cumplo casi todo | Por completo

¿Cuánto tiempo podría estar su empresa con sus sistemas caídos sin que las pérdidas sean considerables?

- ◉ Menos de 4 horas
- ○ Más de 4 horas pero menos de un día
- ○ Entre 1 y 5 días
- ○ Más de 5 días, no es fundamental para mi actividad o tengo prevista una alternativa

¿Se realizan conexiones remotas a sus sistemas?

- ○ Empleados y clientes a través de la página web
- ◉ Los empleados accediendo a través de una aplicación web / intranet
- ○ Solo yo, de forma segura
- ○ Los empleados pueden acceder a aplicaciones internas en remoto y usar escritorio remoto
- ○ No, nunca

¿Dónde se encuentran los servidores y routers de su organización?

- ○ Están en una zona de paso
- ○ En un cuarto compartido
- ◉ En un espacio con acceso restringido
- ○ En las instalaciones del proveedor

¿Quién tiene privilegios para administrar las aplicaciones internas de la empresa?

- ○ Todos los usuarios
- ○ Algunos usuarios autorizados
- ○ Solo yo
- ◉ Nuestro informático en plantilla
- ○ La empresa de mantenimiento informático que tenemos contratada

¿Tiene un plan B por si ocurre algún desastre que le impida utilizar sus sistemas de información?

- ○ No
- ○ Algo pero no lo he probado
- ◉ Sí, está definido pero no lo hemos comprobado
- ○ Sí, bien definido y comprobado; con copias de seguridad en local
- ○ Sí, bien definido y comprobado; con copias de seguridad en otra ubicación fuera de la empresa
- ○ Sí, tenemos incluso servidores redundantes

¿Cuánto tiempo podría estar su empresa sin que sus trabajadores puedan trabajar en remoto?

- ○ Menos de 4 horas
- ○ Más de 4 horas pero menos de un día
- ◉ Entre 1 y 5 días
- ○ Más de 5 días, no es fundamental para mi actividad o tengo prevista una alternativa

¿Quién realiza conexiones remotas a sus sistemas?

- ○ Empleados accediendo a una aplicación web / intranet sin usar HTTPS
- ◉ Los empleados accediendo de forma segura a una aplicación web / intranet (HTTPS)
- ○ Los empleados pueden acceder a aplicaciones internas en remoto y usar escritorio remoto
- ○ Solo yo, de forma segura

¿Quién autoriza a qué aplicaciones internas acceden los teletrabajadores?

- ○ Todos los usuarios
- ○ Algunos usuarios autorizados
- ○ Solo yo
- ◉ Nuestro informático de plantilla
- ○ La empresa de mantenimiento informático que tenemos contratada

¿Tiene un plan B por si ocurre algún desastre que le impida acceder a los trabajadores remotos?

- ○ No, se quedarían sin trabajar
- ◉ No, tendrían que acudir a las instalaciones de la empresa
- ○ Sí, tengo una segunda línea de comunicaciones

¿Cuánto tiempo podrían estar sus empleados sin acceso a los dispositivos móviles de empresa?

- ○ Menos de 4 horas
- ○ Más de 4 horas pero menos de un día
- ◉ Entre 1 y 5 días
- ○ Más de 5 días, no es fundamental para mi actividad o tengo prevista una alternativa

¿Sus empleados utilizan el mismo dispositivo (móvil, tableta, portátil,...) para uso personal y de empresa?

- ○ Sí, todos
- ○ Solo algunos empleados
- ○ No, solo los directores
- ◉ No, únicamente se permite el uso de dispositivos de empresa

¿Los dispositivos móviles de empresa que usan sus empleados están debidamente actualizados?

- ○ No / No lo sé
- ○ Se actualizan de vez en cuando
- ◉ Se actualizan cuando me avisa el informático o el fabricante
- ○ Estamos completamente actualizados

¿Con qué frecuencia realiza copias de seguridad de sus dispositivos?

Cuando me acuerdo | Nunca / No lo sé | Una vez al mes | Cada semana | Todos los días

¿Tiene su personal informático conocimientos específicos en ciberseguridad?

- ○ No / No estoy seguro
- ○ Creo que sí, pero son conocimientos básicos
- ◉ Sí, ha recibido formación técnica en ciberseguridad
- ○ Sí, nuestro personal está certificado en ciberseguridad

¿Con qué frecuencia actualiza el software de sus equipos y sistemas?

- ○ Nunca
- ○ De vez en cuando
- ◉ Se actualizan cuando me avisa el informático o el fabricante
- ○ Estamos al día en todas las actualizaciones disponibles

La encuesta fue desarrollada con la herramienta de análisis de riesgo del Instituto Nacional en Ciberseguridad (INCIBE) y a su vez fue contestada por el Ingeniero de sistemas de Ginsac Colombia SAS.

Anexo B. Modelo de madurez

Tabla 13. Modelo de madurez

Modelo de madurez		
Nivel de madurez	**Descripción**	**Porcentaje**
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.	0
Inicial	Las salvaguardas existen, pero no se gestionan	1-20
Repetible	La medida de seguridad se realiza de un modo totalmente informal, La responsabilidad es individual. No hay formación	21-40
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el responsable de Seguridad ni el Comité de Dirección	41-60
Administrado	El control se lleva a cabo de acuerdo con un procedimiento documentado, aprobado y formalizado	61 – 80
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.	81 - 100

Fuente: INCIBE. PLAN DIRECTOR DE SEGURIDAD. PROTEGE TU EMPRESA [EN LINEA]. [Consultado el 25, junio, 2022]. Disponible en Internet: <https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan-director-seguridad.pdf>

Anexo C. Evaluación de efectividad de controles

Tabla 14. Cumplimiento de controles y nivel de madurez

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES			
No del Control	**Dominio/Objetivo Control**	**Nivel de Aplicabilidad del control**	**Nivel de madurez %**
A.5	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**		
A.5.1	Orientación de la dirección para la gestión de la seguridad de la información.		
A.5.1.1	Políticas para la seguridad de la información.	Inexistente	0%
A.5.1.2	Revisión de las políticas para la seguridad de la información.	Inexistente	0%
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**		
A.6.1	Organización interna		
A.6.1.1	Roles y responsabilidades para la seguridad de la información	Repetible	40%
A.6.1.2	Separación de deberes	Repetible	40%
A.6.1.3	Contacto con las autoridades	Inexistente	0%

A.6.1.4	Contacto con grupos de interés especial	Inexistente	0%
A.6.1.5	Seguridad de la información en la gestión de proyectos	Inexistente	0%
A.6.2	Dispositivos móviles y teletrabajo		
A.6.2.1	Política de dispositivos móviles	Inexistente	0%
A.6.2.2	Teletrabajo	Repetible	40%
A.7	**Seguridad de los recursos humanos**		
A.7.1	Previo al Empleo		
A.7.1.1	Verificación de antecedentes	Definido	60%
A.7.1.2	Términos y condiciones del empleo	Definido	60%
A.7.2	Durante el Empleo		
A.7.2.1	Responsabilidades de la Alta Gerencia	Administrado	80%
A.7.2.2	Conciencia, educación y entrenamiento de Seguridad de la Información	Repetible	40%
A.7.2.3	Proceso disciplinario	Definido	60%
A.7.3	Terminación y Cambio de Empleo		

A.7.3.1	Terminación o cambio de responsabilidades de empleo	Definido	60%
A.8	**GESTIÓN DE ACTIVOS**		
A.8.1	Responsabilidad por los activos		
A.8.1.1	Inventario de activos	Administrado	80%
A.8.1.2	Propiedad de los activos	Administrado	80%
A.8.1.3	Uso aceptable de los activos	Administrado	80%
A.8.1.4	Devolución de activos	Administrado	80%
A.8.2	Clasificación de la información		
A.8.2.1	Clasificación de la información	Administrado	80%
A.8.2.2	Etiquetado de la información	Administrado	80%
A.8.2.3	Manejo de activos	Administrado	80%
A.8.3	Manejo de medios		
A.8.3.1	Gestión de medios removibles	Repetible	40%
A.8.3.2	Disposición de los medios	Repetible	40%
A.8.3.3	Transferencia de medios físicos	Definido	60%

A.9	CONTROL DE ACCESOS		
A.9.1	Requisitos del negocio para control de accesos		
A.9.1.1	Política de control de acceso	Inicial	20%
A.9.1.2	Acceso a redes y a servicios en red	Inicial	20%
A.9.2	Gestión de acceso de usuarios		
A.9.2.1	Registro y cancelación del registro de usuarios	Repetible	40%
A.9.2.2	Suministro de acceso de usuarios	Repetible	40%
A.9.2.3	Gestión de derechos de acceso privilegiado	Repetible	40%
A.9.2.4	Gestión de información de autenticación secreta de usuarios	Repetible	40%
A.9.2.5	Revisión de los derechos de acceso de usuarios	Repetible	40%
A.9.2.6	Retiro o ajuste de los derechos de acceso	Repetible	40%
A.9.3	Responsabilidades de los usuarios		

A.9.3.1	Uso de información de autenticación secreta	Inexistente	0%
A.9.4	Control de acceso a sistemas y aplicaciones		
A.9.4.1	Restricción de acceso a la información	Inicial	20%
A.9.4.2	Procedimiento de ingreso seguro	Inicial	20%
A.9.4.3	Sistema de gestión de contraseñas	Repetible	40%
A.9.4.4	Uso de programas utilitarios privilegiados	Repetible	40%
A.9.4.5	Control de acceso a códigos fuente de programas	Repetible	40%
A.10	**CRIPTOGRAFIA**		
A.10.1	Controles criptográficos		
A.10.1.1	Política sobre el uso de controles criptográficos	Inexistente	0%
A.10.1.2	Gestión de llaves	Inexistente	0%
A.11	**SEGURIDAD FÍSICA Y DEL ENTORNO**		
A.11.1	Áreas seguras		

A.11.1.1	Perímetro de seguridad física	Inexistente	0%
A.11.1.2	Control de accesos físicos	Inexistente	0%
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Definido	60%
A.11.1.4	Protección contra amenazas externas y ambientales	Repetible	40%
A.11.1.5	"Trabajo en áreas seguras	Definido	60%
A.11.1.6	Áreas de despacho y carga	Definido	60%
A.11.2	Equipos		
A.11.2.1	Ubicación y protección de los equipos	Administrado	80%
A.11.2.2	Servicios de suministro	Administrado	80%
A.11.2.3	Seguridad del cableado	Administrado	80%
A.11.2.4	Mantenimiento de equipos	Administrado	80%
A.11.2.5	Retiro de activos	Definido	60%
A.11.2.6	Seguridad de activos y equipos fuera de la oficina	Definido	60%
A.11.2.7	Disposición segura o reutilización de equipos	Definido	60%

A.11.2.8	Equipos de usuario desatendido	Repetible	40%
A.11.2.9	Políticas de escritorio limpio y pantalla limpia	Inexistente	0%
A.12	**SEGURIDAD DE LAS OPERACIONES**		
A.12.1	Procedimientos operacionales y responsabilidades		
A.12.1.1	Procedimientos de operación documentados	Inicial	20%
A.12.1.2	Gestión de cambios	Inicial	20%
A.12.1.3	Gestión de capacidad	Inicial	20%
A.12.1.4	Separación de los ambientes de desarrollo, pruebas, y operación	Inicial	20%
A.12.2	Protección contra códigos maliciosos		
A.12.2.1	Controles contra códigos maliciosos	Definido	60%
A.12.3	Proteger contra la perdida de datos		
A.12.3.1	Respaldo de la información	Definido	60%
A.12.4	Registro y seguimiento		
A.12.4.1	Registro de eventos	Repetible	40%

A.12.4.2	Protección de la información de registro	Repetible	40%
A.12.4.3	Registros del administrador y del operador	Repetible	40%
A.12.4.4	Sincronización de reloj	Definido	60%
A.12.5	Control de software operacional		
A.12.5.1	Instalación de software en sistemas operativos	Administrado	80%
A.12.6	Gestión de la vulnerabilidad técnica		
A.12.6.1	Gestión de las vulnerabilidades técnicas	Administrado	80%
A.12.6.2	Restricciones sobre la instalación de software	Repetible	40%
A.12.7	Consideraciones sobre auditorías de sistemas de información		
A.12.7.1	Controles de auditorías de sistemas de información	Inexistente	0%
A.13	**SEGURIDAD DE LAS COMUNICACIONES**		
A.13.1	Gestión de la seguridad de las redes		
A.13.1.1	Controles de redes	Repetible	40%

A.13.1.2	Seguridad de los servicios de red	Repetible	40%
A.13.1.3	Separación en las redes	Repetible	40%
A.13.2	Transferencia de información		
A.13.2.1	Políticas y procedimientos de transferencia de información	Inexistente	0%
A.13.2.2	Acuerdos sobre transferencia de información	Inexistente	0%
A.13.2.3	Mensajería electrónica	Definido	60%
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	Definido	60%
A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**		
A.14.1	Requisitos de seguridad de los sistemas de información	Repetible	40%
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Repetible	40%
A.14.1.2	Seguridad de servicio de las aplicaciones en redes publicas	Repetible	40%
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	Repetible	40%

A.14.2	Seguridad en los procesos de desarrollo y soporte		
A.14.2.1	Políticas de desarrollo seguro	Inexistente	0%
A.14.2.2	Procedimiento de control de cambios en sistemas	Inexistente	0%
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Repetible	40%
A.14.2.4	Restricción en los cambios a los paquetes de software	Repetible	40%
A.14.2.5	Principios de construcción de los sistemas seguros	Repetible	40%
A.14.2.6	Ambiente seguro de desarrollo	Repetible	40%
A.14.2.7	Desarrollo externamente contratado	Inexistente	0%
A.14.2.8	Pruebas de seguridad de sistemas	Inexistente	0%
A.14.2.9	Prueba de aceptación de sistemas	Repetible	40%
A.14.3	Datos de pruebas		
A.14.3.1	Protección de datos de pruebas	Repetible	40%

A.15	**RELACIONES CON LOS PROVEEDORES**		
A.15.1	Seguridad de la información en las relaciones con los proveedores		
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	Definido	60%
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Definido	60%
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Definido	60%
A.15.2	Gestión de la prestación de servicios de proveedores		
A.15.2.1	Seguimiento y revisión a los servicios proveedores	Repetible	40%
A.15.2.2	Gestión de cambios en los servicios de los proveedores	Repetible	40%
A.16	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**		
A.16.1	Gestión de incidentes y mejoras en la seguridad de la información		
A.16.1.1	Responsabilidades y procedimientos	Repetible	40%

A.16.1.2	Reporte de eventos de seguridad de la información	Repetible	40%
A.16.1.3	Reporte de debilidades de seguridad de la información	Repetible	40%
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Inicial	20%
A.16.1.5	Respuesta a incidentes de seguridad de la información	Repetible	40%
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Repetible	40%
A.16.1.7	Recolección de evidencia	Inicial	20%
A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO**		
A.17.1	Continuidad de seguridad de la información		
A.17.1.1	Planificación de la continuidad de la seguridad de la información	Repetible	40%
A.17.1.2	Implementación de la continuidad de la seguridad de la información	Repetible	40%
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Repetible	40%

A.17.2	Redundancia		
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Repetible	40%
A.18	**CUMPLIMIENTO**		
A.18.1	Cumplimiento de requisitos legales y contractuales		
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Optimizado	100%
A.18.1.2	Derechos de propiedad intelectual	Optimizado	100%
A.18.1.3	Protección de registros	Repetible	40%
A.18.1.4	Privacidad y protección de información de datos personales	Administrado	80%
A.18.1.5	Reglamentación de controles criptográficos	Inexistente	0%
A.18.2	Revisiones de seguridad de la información		
A.18.2.1	Revisión independiente de la seguridad de la información	Repetible	40%
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	Repetible	40%

A.18.2.3	Revisión del cumplimiento técnico	Repetible	40%

Fuente: Elaboración propia, alineados con el Anexo de la norma ISO/IEC 27001:2013.

Anexo D. Lista de amenazas MAGERIT

Tabla 15. Listado de amenazas MAGERIT

LISTA DE AMENAZAS MAGERIT		
[N] Desastres naturales		
[N.1]	Fuego	[D] disponibilidad
[N.2]	Daños por agua	[D] disponibilidad
[N.*]	Desastres naturales	[D] disponibilidad
[I] De origen industrial		
[I.1]	Fuego	D] disponibilidad
[I.2]	Daños por agua	D] disponibilidad
[I.*]	Desastres industriales	D] disponibilidad
[I.3]	Contaminación mecánica	D] disponibilidad
[I.4]	Contaminación electromagnética	D] disponibilidad

[I.5]	Avería de origen físico o lógico	D] disponibilidad
[I.6]	Corte del suministro eléctrico	D] disponibilidad
[I.7]	Condiciones inadecuadas de temperatura o humedad	D] disponibilidad
[I.8]	Fallo de servicios de comunicaciones	D] disponibilidad
[I.9]	Interrupción de otros servicios y suministros esenciales	D] disponibilidad
[I.10]	Degradación de los soportes de almacenamiento de la información	D] disponibilidad
[I.11]	Emanaciones electromagnéticas	[C] confidencialidad
[E] Errores y fallos no intencionados		
[E.1]	Errores de los usuarios	[D] disponibilidad [I] integridad [C] confidencialidad
[E.2]	Errores del administrador	[D] disponibilidad [I] integridad [C] confidencialidad
[E.3]	Errores de monitorización (log)	[I] integridad (trazabilidad)
[E.4]	Errores de configuración	[I] integridad
[E.7]	Deficiencias en la organización	[D] disponibilidad

[E.8]	Difusión de software dañino	[D] disponibilidad [I] integridad [C] confidencialidad
[E.9]	Errores de [re-]encaminamiento	[C] confidencialidad
[E.10]	Errores de secuencia	[I] integridad
[E.14]	Escapes de información	[C] confidencialidad
[E.15]	Alteración accidental de la información	[I] integridad
[E.18]	Destrucción de información	[D] disponibilidad
[E.19]	Fugas de información	[C] confidencialidad
[E.20]	Vulnerabilidades de los programas (software)	[I] integridad [D] disponibilidad [C] confidencialidad
[E.21]	Errores de mantenimiento / actualización de programas (software)	[I] integridad [D] disponibilidad
[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	[D] disponibilidad
[E.24]	Caída del sistema por agotamiento de recursos	[D] disponibilidad
[E.25]	Pérdida de equipos	[D] disponibilidad [C] confidencialidad
[E.28]	Indisponibilidad del personal	[D] disponibilidad

[A] Ataques intencionados		
[A.3]	Manipulación de los registros de actividad (log)	[I] integridad (trazabilidad)
[A.4]	Manipulación de la configuración	[I] integridad [C] confidencialidad [D] disponibilidad
[A.5]	Suplantación de la identidad del usuario	[C] confidencialidad [A] autenticidad [I] integridad
[A.6]	Abuso de privilegios de acceso	[C] confidencialidad [I] integridad [D] disponibilidad
[A.7]	Uso no previsto	[D] disponibilidad [C] confidencialidad [I] integridad
[A.8]	Difusión de software dañino	[D] disponibilidad [I] integridad [C] confidencialidad
[A.9]	[Re-]encaminamiento de mensajes	C] confidencialidad
[A.10]	Alteración de secuencia	[I] integridad
[A.11]	Acceso no autorizado	[C] confidencialidad [I] integridad
[A.12]	Análisis de tráfico	[C] confidencialidad

[A.13]	Repudio	I] integridad (trazabilidad)
[A.14]	Interceptación de información (escucha)	[C] confidencialidad
[A.15]	Modificación deliberada de la información	[I] integridad
[A.18]	Destrucción de información	D] disponibilidad
[A.19]	Divulgación de información	[C] confidencialidad
[A.22]	Manipulación de programas	[C] confidencialidad [I] integridad [D] disponibilidad
[A.23]	Manipulación de los equipos	[C] confidencialidad [D] disponibilidad
[A.24]	Denegación de servicio	[D] disponibilidad
[A.25]	Robo	[D] disponibilidad [C] confidencialidad
[A.26]	Ataque destructivo	[D] disponibilidad
[A.27]	Ocupación enemiga	[D] disponibilidad [C] confidencialidad
[A.28]	Indisponibilidad del personal	[D] disponibilidad

[A.29]	Extorsión	[C] confidencialidad [I] integridad [D] disponibilidad
[A.30]	Ingeniería social (picaresca)	[C] confidencialidad [I] integridad [D] disponibilidad

Fuente: CALDERON, Marco. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III -Guía de Técnicas. Academia.edu - Share research [EN LINEA]. [Consultado el 10, diciembre, 2022]. Disponible en Internet: <https://www.academia.edu/27331595/MAGERIT_versión_3_0_Metodología_de_Análisis_y_Gestión_de_Riesgos_de_los_Sistemas_de_Información_Libro_III_Guía_de_Técnicas>.

Anexo E. Metodología para la valoración del riesgo en los activos de información MAGERIT

Tabla 16. Matriz valoración de riesgo - [D] Datos/Información

Activo	Amenazas	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Valoración	Nivel riesgo
[D] Datos / Información								
DB sistema contable DB usuarios de red BD Personal Copias de seguridad BD Lista de precios BD RRHH	[E1] Errores de los usuarios	B	B	MA	MA	MA	19	IMPORTANTE
	[E2] Errores del administrador	B	B	MA	MA	MA	19	IMPORTANTE
	[E3] Errores de monitorización (log)	B	MA	B	MA	B	15	APRECIABLE
	[E4] Errores de configuración	B	B	B	MA	B	12	APRECIABLE
	[E15] Alteración accidental de la información	B	B	B	MA	B	12	APRECIABLE
	[E18] Destrucción de información	B	B	B	B	MA	12	APRECIABLE

	[E19] Fugas de información	B	B	MA	B	B	12	APRECIABLE
	[A3] Manipulación de los registros de actividad (log)	B	MA	B	MA	B	15	APRECIABLE
	[A4] Manipulación de la configuración	B	B	MA	MA	MA	19	IMPORTANTE
	[A5] Suplantación de la identidad del usuario	MA	B	MA	MA	B	19	IMPORTANTE
	[A6] Abuso de privilegios de acceso	B	B	MA	MA	MA	19	IMPORTANTE
	[A11] Acceso no autorizado	B	B	MA	MA	B	15	APRECIABLE
	[A13] Repudio	B	MA	B	MA	B	15	APRECIABLE
	[A15] Modificación deliberada de la información	B	B	B	MA	B	12	APRECIABLE
	[A18] Destrucción de información	B	B	B	B	MA	12	APRECIABLE
	[A19] Divulgación de información	B	B	MA	B	B	12	APRECIABLE

Fuente: Elaboración propia.

Tabla 17. Matriz valoración de riesgo - [K] Claves criptográficas

Activo	Amenazas	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Valoración	Nivel riesgo
[K] Claves criptográficas								
Firma electrónica Gerencia y tesorería [encrypt] Matricula RUNT [com]	[E1] Errores de los usuarios	B	B	MA	MA	MA	19	IMPORTANTE
	[E2] Errores del administrador	B	B	MA	MA	MA	19	IMPORTANTE
	[E15] Alteración accidental de la información	B	B	B	MA	B	12	APRECIABLE
	[E18] Destrucción de información	B	B	B	B	MA	12	APRECIABLE
	[E19] Fugas de información	B	B	MA	B	B	12	APRECIABLE
	[A5] Suplantación de la identidad del usuario	MA	B	MA	MA	B	19	IMPORTANTE
	[A6] Abuso de privilegios de acceso	B	B	MA	MA	MA	19	IMPORTANTE

	[A11] Acceso no autorizado	B	B	MA	MA	B	15	APRECIABLE
	[A15] Modificación deliberada de la información	B	B	B	MA	B	12	APRECIABLE
	[A18] Destrucción de información	B	B	B	B	MA	12	APRECIABLE
	[A19] Divulgación de información	B	B	MA	B	B	12	APRECIABLE

Fuente: Elaboración propia.

Tabla 18. Matriz valoración de riesgo - [S] Servicios

Activo	Amenazas	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Valoración	Nivel riesgo
[S] Servicios								
Página Web [www] Work Space – Cuentas de correos [email] Acronix Protect – Copias en la nube [file] Cuentas de Google Drive [file] SIESA CONTABLE CLOUD Rastreo de flotas	[E1] Errores de los usuarios	B	B	MA	MA	MA	19	IMPORTANTE
	[E2] Errores del administrador	B	B	MA	MA	MA	19	IMPORTANTE
	[E9] Errores de [re-]encaminamiento	B	B	MA	B	B	12	APRECIABLE
	[E10] Errores de secuencia	B	B	B	MA	B	12	APRECIABLE
	[E15] Alteración accidental de la información	B	B	B	MA	B	12	APRECIABLE
	[E18] Destrucción de información	B	B	B	B	MA	12	APRECIABLE
	[E19] Fugas de información	B	B	MA	B	B	12	APRECIABLE

Hosting, Dominio [www] Tiene virtual Agrofy [www]	[E24] Caída del sistema por agotamiento de recursos	B	B	B	B	MA	12	APRECIABLE
	[A5] Suplantación de la identidad del usuario	MA	B	MA	MA	B	19	IMPORTANTE
	[A6] Abuso de privilegios de acceso	B	B	MA	MA	MA	19	IMPORTANTE
	[A7] Uso no previsto	B	B	MA	MA	MA	19	IMPORTANTE
	[A9] [Re-]encaminamiento de mensajes	B	MA	MA	B	B	15	APRECIABLE
	[A10] Alteración de secuencia	B	B	B	MA	B	12	APRECIABLE
	[A11] Acceso no autorizado	B	B	MA	MA	B	15	APRECIABLE
	[A13] Repudio	B	MA	B	MA	B	15	APRECIABLE
	[A15] Modificación deliberada de la información	B	B	B	MA	B	12	APRECIABLE
	[A18] Destrucción de información	B	B	B	B	MA	12	APRECIABLE
	[A19] Divulgación de información	B	B	MA	B	B	12	APRECIABLE

	[A24] Denegación de servicio	B	B	B	B	MA	12	APRECIABLE

Fuente: Elaboración propia.

Tabla 19. Matriz valoración de riesgo - [SW] Software - Aplicaciones informáticas

Activo	Amenazas	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Valoración	Nivel riesgo
[SW] Software - Aplicaciones informáticas								
Sistema operativo Windows 10 Windows 11 [os] S.O. Windows Server 2016 [os] Antivirus ESET Endpoint Security [av] Microsoft Office Empresa 2016 – 2019 [office] Software contable Helisa [sub]	[I5] Avería de origen físico o lógico	B	B	B	B	MA	12	APRECIABLE
	[E1] Errores de los usuarios	B	B	MA	MA	MA	19	IMPORTANTE
	[E2] Errores del administrador	B	B	MA	B	MA	15	APRECIABLE
	[E8] Difusión de software dañino	B	B	MA	MA	MA	19	IMPORTANTE
	[E9] Errores de [re-]encaminamiento	B	B	MA	B	B	12	APRECIABLE
	[E10] Errores de secuencia	B	B	B	MA	B	12	APRECIABLE
	[E15] Alteración accidental de la información	B	B	B	MA	B	12	APRECIABLE

Software de copias de seguridad ACRONIS PROTECT [backup] Antivirus Norton 360 Premium [av] Desarrollos de intranet a la medida [prp]	[E18] Destrucción de información	B	B	B	B	MA	12	APRECIABLE
	[E19] Fugas de información	B	B	MA	B	B	12	APRECIABLE
	[E20] Vulnerabilidades de los programas (software)	B	B	MA	MA	MA	19	IMPORTANTE
	[E21] Errores de mantenimiento / actualización de programas (software)	B	B	B	MA	MA	15	APRECIABLE
	[A5] Suplantación de la identidad del usuario	MA	B	MA	MA	B	19	IMPORTANTE
	[A6] Abuso de privilegios de acceso	B	B	MA	MA	MA	19	IMPORTANTE
	[A7] Uso no previsto	B	B	MA	MA	MA	19	IMPORTANTE
	[A8] Difusión de software dañino	B	B	MA	MA	MA	19	IMPORTANTE
	[A9] [Re-]encaminamiento de mensajes	B	B	MA	B	B	12	APRECIABLE
	[A10] Alteración de secuencia	B	B	M	MA	B	13	APRECIABLE

	[A11] Acceso no autorizado	B	B	MA	MA	B	15	APRECIABLE
	[A15] Modificación deliberada de la información	B	B	B	MA	B	12	APRECIABLE
	[A18] Destrucción de información	B	B	B	B	MA	12	APRECIABLE
	[A19] Divulgación de información	B	B	MA	B	B	12	APRECIABLE
	[A22] Manipulación de programas	B	B	MA	MA	MA	19	IMPORTANTE

Fuente: Elaboración propia.

Tabla 20. Matriz valoración de riesgo - [HW] Equipamiento informático (hardware)

Activo	Amenazas	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Valoración	Nivel riesgo
[HW] Equipamiento informático (hardware)								
Computadores All in One [pc] Servidor [pc] Impresora Epson [print] Router [router] Rack Modem [modem] Switch Teléfonos fijos [pabx] Cámaras de vigilancias x Sede [mid]	[N1] Fuego	B	B	B	B	MA	12	APRECIABLE
	[N2] Daños por agua	B	B	B	B	MA	12	APRECIABLE
	[N*] Desastres naturales	B	MA	B	B	MA	15	APRECIABLE
	[I1] Fuego	B	B	B	B	MA	12	APRECIABLE
	[I2] Daños por agua	B	B	B	B	MA	12	APRECIABLE
	[I*] Desastres industriales	B	B	B	B	MA	12	APRECIABLE
	[I3] Contaminación mecánica	B	B	B	B	MA	12	APRECIABLE

Computador de mesa DELL [pc] Equipos portátiles [pc] Tablet Lenovo Yoga [mid] Equipo Móviles [mobile]	[I4] Contaminación electromagnética	B	B	B	B	MA	12	APRECIABLE
	[I5] Avería de origen físico o lógico	B	B	B	B	MA	12	APRECIABLE
	[I6] Corte del suministro eléctrico	B	B	B	B	MA	12	APRECIABLE
	[I7] Condiciones inadecuadas de temperatura o humedad	B	B	B	B	MA	12	APRECIABLE
	[I11] Emanaciones electromagnéticas	A	B	MA	A	A	19	IMPORTANTE
	[E2] Errores del administrador	B	B	MA	MA	MA	19	IMPORTANTE
	[E23] Errores de mantenimiento / actualización de equipos (hardware)	B	B	B	B	MA	12	APRECIABLE
	[E24] Caída del sistema por agotamiento de recursos	B	MA	B	B	MA	15	APRECIABLE
	[E25] Pérdida de equipos	B	B	MA	B	MA	15	APRECIABLE

	[A6] Abuso de privilegios de acceso	A	B	MA	MA	MA	21	CRITICO
	[A7] Uso no previsto	B	B	MA	MA	MA	19	IMPORTANTE
	[A11] Acceso no autorizado	B	B	MA	MA	B	15	APRECIABLE
	[A23] Manipulación de los equipos		B	MA	A	MA	20	IMPORTANTE
	[A24] Denegación de servicio	B	B	B	B	MA	12	APRECIABLE
	[A25] Robo	MA	M	MA	A	MA	22	CRITICO
	[A26] Ataque destructivo	B	B	B	B	MA	12	APRECIABLE

Fuente: Elaboración propia.

Tabla 21. Matriz valoración de riesgo - [COM] Redes de comunicaciones

Activo	Amenazas	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Valoración	Nivel riesgo
[COM] Redes de comunicaciones								
Infraestructura de RED LAN [LAN] Redes wifi [wifi] Internet [Internet] Telefonía móvil [Mobile]	[I8] Fallo de servicios de comunicaciones	B	B	B	B	MA	12	APRECIABLE
	[E2] Errores del administrador	B	B	MA	MA	MA	19	IMPORTANTE
	[E9] Errores de [re-]encaminamiento	B	B	MA	B	B	12	APRECIABLE
	[E10] Errores de secuencia	B	B	B	MA	B	12	APRECIABLE
	[E15] Alteración accidental de la información	B	B	M	MA	B	13	APRECIABLE
	[E18] Destrucción de información	B	B	B	B	MA	12	APRECIABLE
	[E19] Fugas de información	B	B	MA	B	B	12	APRECIABLE

[E24] Caída del sistema por agotamiento de recursos	B	B	B	B	MA	12	APRECIABLE
[A5] Suplantación de la identidad del usuario	MA	B	MA	MA	B	19	IMPORTANTE
[A6] Abuso de privilegios de acceso	B	B	MA	MA	MA	19	IMPORTANTE
[A7] Uso no previsto	B	B	MA	MA	MA	19	IMPORTANTE
[A9] [Re-]encaminamiento de mensajes	B	B	MA	B	B	12	APRECIABLE
[A10] Alteración de secuencia	B	B	B	MA	B	12	APRECIABLE
[A11] Acceso no autorizado	B	B	MA	MA	B	15	APRECIABLE
[A12] Análisis de tráfico	B	B	MA	B	B	12	APRECIABLE
[A14] Interceptación de información (escucha)	B	MA	MA	B	B	15	APRECIABLE
[A15] Modificación deliberada de la información	B	B	B	MA	B	12	APRECIABLE
[A19] Divulgación de información	B	B	MA	B	B	12	APRECIABLE

	[A24] Denegación de servicio	B	MA	B	B	MA	15	APRECIABLE

Fuente: Elaboración propia.

Tabla 22. Matriz valoración de riesgo - [Media] Soportes de información

Activo	Amenazas	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Valoración	Nivel riesgo
[Media] Soportes de información								
Discos duros externos SSD 1T [disk] Memorias USB 64 GB [usb]	[N1] Fuego	B	B	B	B	MA	12	APRECIABLE
	[N2] Daños por agua	B	B	B	B	MA	12	APRECIABLE
	[N*] Desastres naturales	B	B	B	B	MA	12	APRECIABLE
	[I1] Fuego	B	B	B	B	MA	12	APRECIABLE
	[I2] Daños por agua	B	B	B	B	MA	12	APRECIABLE
	[I*] Desastres industriales	B	B	B	B	MA	12	APRECIABLE
	[I3] Contaminación mecánica	B	B	B	B	MA	12	APRECIABLE

[I4] Contaminación electromagnética	B	B	B	B	MA	12	APRECIABLE
[I5] Avería de origen físico o lógico	B	B	B	B	MA	12	APRECIABLE
[I6] Corte del suministro eléctrico	B	MA	B	B	MA	15	APRECIABLE
[I7] Condiciones inadecuadas de temperatura o humedad	B	B	B	B	MA	12	APRECIABLE
[I10] Degradación de los soportes de almacenamiento de la información	B	B	B	B	MA	12	APRECIABLE
[I11] Emanaciones electromagnéticas	B	B	MA	B	B	12	APRECIABLE
[E1] Errores de los usuarios	B	B	MA	MA	MA	19	IMPORTANTE
[E2] Errores del administrador	B	B	MA	MA	MA	19	IMPORTANTE
[E15] Alteración accidental de la información	B	B	B	MA	B	12	APRECIABLE
[E18] Destrucción de información	B	B	B	B	MA	12	APRECIABLE
[E19] Fugas de información	B	B	MA	B	B	12	APRECIABLE

	[E23] Errores de mantenimiento / actualización de equipos (hardware)	B	B	B	B	MA	12	APRECIABLE
	[E25] Pérdida de equipos	B	B	MA	B	MA	15	APRECIABLE
	[A7] Uso no previsto	B	B	MA	MA	MA	19	IMPORTANTE
	[A11] Acceso no autorizado	B	B	MA	MA	B	15	APRECIABLE
	[A15] Modificación deliberada de la información	B	B	B	MA	B	12	APRECIABLE
	[A18] Destrucción de información	B	B	B	B	MA	12	APRECIABLE
	[A19] Divulgación de información	B	B	MA	B	B	12	APRECIABLE
	[A23] Manipulación de los equipos	B	B	MA	B	MA	15	APRECIABLE
	[A25] Robo	B	B	MA	B	MA	15	APRECIABLE
	[A26] Ataque destructivo	B	B	B	B	MA	12	APRECIABLE

Fuente: Elaboración propia.

Tabla 23. Matriz valoración de riesgo - [AUX] Equipamiento auxiliar

Activo	Amenazas	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Valoración	Nivel riesgo
[AUX] Equipamiento auxiliar								
UPS [ups] Cable estructurado por sede [cabling]	[N1] Fuego	B	B	B	B	MA	12	APRECIABLE
	[N2] Daños por agua	B	B	B	B	MA	12	APRECIABLE
	[N*] Desastres naturales	B	B	B	B	MA	12	APRECIABLE
	[I1] Fuego	B	B	B	B	MA	12	APRECIABLE
	[I2] Daños por agua	B	B	B	B	MA	12	APRECIABLE
	[I*] Desastres industriales	B	B	B	B	MA	12	APRECIABLE
	[I3] Contaminación mecánica	B	B	B	B	MA	12	APRECIABLE

[I4] Contaminación electromagnética	B	B	B	B	MA	12	APRECIABLE
[I5] Avería de origen físico o lógico	B	B	B	B	MA	12	APRECIABLE
[I6] Corte del suministro eléctrico	B	MA	B	B	MA	15	APRECIABLE
[I7] Condiciones inadecuadas de temperatura o humedad	B	B	B	B	MA	12	APRECIABLE
[I9] Interrupción de otros servicios y suministros esenciales	B	B	B	B	MA	12	APRECIABLE
[I11] Emanaciones electromagnéticas	B	B	MA	B	B	12	APRECIABLE
[E23] Errores de mantenimiento / actualización de equipos (hardware)	B	B	B	B	MA	12	APRECIABLE
[E25] Pérdida de equipos	B	B	MA	B	MA	15	APRECIABLE
[A7] Uso no previsto	B	B	MA	MA	MA	19	IMPORTANTE
[A11] Acceso no autorizado	B	B	MA	B	MA	15	APRECIABLE

	[A23] Manipulación de los equipos	B	B	MA	B	MA	15	APRECIABLE
	[A25] Robo	B	B	MA	B	MA	15	APRECIABLE
	[A26] Ataque destructivo	B	B	B	B	MA	12	APRECIABLE

Fuente: Elaboración propia.

Tabla 24. Matriz valoración de riesgo - [L] Instalaciones

Activo	Amenazas	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Valoración	Nivel riesgo
[L] Instalaciones								
Oficinas / Sedes [site] Vitrinas comerciales [local] Puntos de teletrabajo [site] Plantas de operaciones [site]	[N1] Fuego	B	B	B	B	MA	12	APRECIABLE
	[N2] Daños por agua	B	B	B	B	MA	12	APRECIABLE
	[N*] Desastres naturales	B	B	B	B	MA	12	APRECIABLE
	[I1] Fuego	B	B	B	B	MA	12	APRECIABLE
	[I2] Daños por agua	B	B	B	B	MA	12	APRECIABLE
	[I*] Desastres industriales	B	B	B	B	MA	12	APRECIABLE

[I11] Emanaciones electromagnéticas	B	B	MA	B	B	12	APRECIABLE
[E15] Alteración accidental de la información	B	B	B	MA	B	12	APRECIABLE
[E18] Destrucción de información	B	B	B	B	MA	12	APRECIABLE
[E19] Fugas de información	B	B	MA	A	B	14	APRECIABLE
[A7] Uso no previsto	B	B	MA	MA	MA	19	IMPORTANTE
[A11] Acceso no autorizado	B	B	MA	B	MA	15	APRECIABLE
[A15] Modificación deliberada de la información	B	B	B	MA	B	12	APRECIABLE
[A18] Destrucción de información	B	B	B	B	MA	12	APRECIABLE
[A19] Divulgación de información	B	B	MA	B	B	12	APRECIABLE
[A26] Ataque destructivo	B	B	B	B	MA	12	APRECIABLE
[A27] Ocupación enemiga	B	B	MA	B	MA	15	APRECIABLE

Fuente: Elaboración propia.

Tabla 25. Matriz valoración de riesgo - [P] Personal

Activo	Amenazas	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Valoración	Nivel riesgo
[P] Personal								
Área administrativa [ui] Área Operativa [op] Servicios generales [ui] Área comercial [prov]	[E7] Deficiencias en la organización	B	B	B	B	MA	12	APRECIABLE
	[E19] Fugas de información	B	B	MA	A	B	14	APRECIABLE
	[E28] Indisponibilidad del personal	B	B	B	B	MA	12	APRECIABLE
	[A29] Extorsión	M	M	MA	A	MA	20	IMPORTANTE
	[A30] Ingeniería social (picaresca)	A	M	MA	A	MA	21	CRITICO

Fuente: Elaboración propia

Anexo F. Matriz de análisis de riesgos GINSAC COLOMBIA SAS.

Tabla 26. Matriz de análisis y tratamiento de riesgos

Activos de Información	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS	Amenazas Metodología Magerit	Niveles de aceptación del riesgo	Probabilidad de vulneración	Cálculo del riesgo neto	Criticidad neta	Calificación de Gestión	Si la opción es 2 - 3 o 4 Indique el Control aplicado actual	Riesgo residual	Criticidad residual
AUXILIAR	UPS	12	[I5] Avería de origen físico o lógico	M	2	24	C	3	Cuenta con mantenimientos periódicos por parte de la compañía.	8	B
AUXILIAR	Cable estructurado por sede	12	[I6] Corte del suministro eléctrico	I	4	48	C	2	Solo 1 sede cuenta con infraestructura certificada.	24	C
COMUNICACIONES	Infraestructura de RED LAN	12	[I8] Fallo de servicios de comunicaciones	M	3	36	C	3	Se han gestionado configuraciones internas a la medida.	12	A
COMUNICACIONES	REDES WIFI	15	[E2] Errores del administrador	I	4	60	C	2	Se cuenta con 2 Routers en 2 de las 6 sedes de la compañía, no se tiene el control de las conexiones.	30	C
COMUNICACIONES	INTERNET	15	[A12] Análisis de tráfico	I	4	60	C	2	Servicios inestables en las zonas donde están ubicadas las sedes.	30	C
CRIPTOGRAFICAS	Firma electrónica Gerencia y tesorería	15	[E2] Errores del administrador	A	1	15	A	4	Solo 1 persona es la encargada del manejo de las llaves criptográficas, adicional desde	4	D

									el área de TI. Se tienen copias de seguridad		
DATOS	DB sistema contable	12	[E2] Errores del administrador	I	3	36	C	2	Solo la jefe administrativa tiene acceso a las BD de SIESA. El área de TI no tiene el control directo de las copias.	18	I
DATOS	DB usuarios de red	13	[E4] Errores de configuración	M	3	39	C	3	Se cuentan con Copias por parte de TI, pero la administración desde RRHH es muy básica.	13	A
DATOS	BD Personal	12	[E19] Fugas de información	I	5	60	C	1	No se tiene el control de la información con la que interactúa los colaboradores de la compañía. No hay forma de hacerle seguimiento.	60	C
DATOS	Copias de seguridad	12	[E18] Destrucción de información	A	1	12	A	4	Desde el área de TI se tienen copias de seguridad al día y almacenadas en distintos lugares. Probadas	3	D
DATOS	BD Lista de precios	12	[E19] Fugas de información	M	2	24	C	4	Se tiene el control desde Contabilidad y TI de las listas expuestas al mercado.	6	B

HARDWARE	Computadores All in One	12	[I5] Avería de origen físico o lógico	I	4	48	C	3	Son muchos los equipos que cuentan con modificaciones y arregles para optimizar su funcionamiento y seguridad. Pero no se tiene el control del 100%.	16	I
HARDWARE	Servidor	12	[I7] Condiciones inadecuadas de temperatura o humedad	A	1	12	A	4	Se cuenta desde TI con restricción y ventilación del servidor en la sede principal	3	D
HARDWARE	Impresora Epson	13	[A7] Uso no previsto	M	2	26	C	4	Aunque cada impresora cuenta con su responsable, no se tiene el control del uso apropiado.	7	B
HARDWARE	Router	12	[E24] Caída del sistema por agotamiento de recursos	A	1	12	A	3	Aunque no se tienen en todas las sedes, las sedes que cuentan, tienen configuraciones y accesos con seguridad. Control desde TI.	4	D
HARDWARE	Modem	21	[A6] Abuso de privilegios de acceso	I	4	84	C	2	La gran mayoría de las sedes cuentan con configuraciones básicas por modem, propuestas y definidas por el proveedor de servicio.	42	C
HARDWARE	Switch	15	[A25] Robo	A	1	15	A	4	El dispositivo tecnológico ubicado en la sede principal,	4	D

									ubicado en una zona familiar.		
HARDWARE	Teléfonos fijos	12	[E25] Pérdida de equipos	A	1	12	A	4	Se encuentran aislados de personal no autorizado	3	D
HARDWARE	Cámaras	12	[I6] Corte del suministro eléctrico	I	3	36	C	2	No se cuenta con plantas eléctricas de apoyo.	18	I
HARDWARE	Computador de mesa DELL	15	[A11] Acceso no autorizado	I	4	60	C	3	Se tiene seguridad en los equipos de cómputo, pero desde el área de TI no cuenta con el control de acceso a usuarios para el uso de los equipos tecnológicos.	20	I
HARDWARE	Equipos portátiles	15	[A25] Robo	I	4	60	C	1	Se cuentan con actas de entrega y responsabilidad del usuario responsable, pero no se cuenta con la seguridad física y el uso que le de el personal.	60	C
HARDWARE	Tablet Lenovo Yoga	15	[A23] Manipulación de los equipos	I	4	60	C	2	Se tiene seguridad en los implementos tecnológicos en cuanto a Software, pero no se tiene el control de quien lo utilice.	30	C
HARDWARE	Equipo Móviles	15	[E25] Pérdida de equipos	M	2	30	C	3	Se tienen actas de responsabilidad al personal asignado.	10	B

HARDWARE	Oficinas / Sedes	12	[N*] Desastres naturales	A	1	12	A	4	Los sitios donde se encuentran las sedes, están en zonas seguras.	3	D
INSTALACIONES	Vitrinas comerciales	12	[N1] Fuego	A	1	12	A	4	Se tienen asegurados equipos tecnológicos.	3	D
INSTALACIONES	Puntos de teletrabajo	12	[E15] Alteración accidental de la información	M	2	24	C	4	Se implementan desde las TI, accesos solo autorizados y con niveles de seguridad mínimos.	6	B
INSTALACIONES	Plantas de operaciones	21	[E19] Fugas de información	I	4	84	C	3	Aunque se tiene actas de confidencialidad, son vulnerables a manipular información y elementos confidenciales.	28	C
INSTALACIONES	Área administrativa	12	[A19] Divulgación de información	M	2	24	C	4	Personal calificado y con contratos de exclusividad y confidencialidad	6	B
PERSONAL	Área Operativa	14	[A11] Acceso no autorizado	M	2	28	C	4	Los sistemas de información cuentan con estándares mínimos en seguridad.	7	B
PERSONAL	Servicios generales	12	[A30] Ingeniería social (picaresca)	M	2	24	C	3	No se cuenta con continuidad del personal y no tienen acceso a los sistemas de información.	8	B
PERSONAL	Área comercial	9	[E19] Fugas de información	M	2	18	I	3	Trabajan en desarrollos propios administrados por las TI. Pero	6	B

									no se tiene el control y relaciones con terceros.		
PERSONAL	Proveedores	12	[E7] Deficiencias en la organización	A	1	12	A	4	Sistemas de información custodiadas por la jefe administrativa y personal calificado.	3	D
SERVICIOS	Desarrollos de intranet a la medida	13	[E2] Errores del administrador	M	2	26	C	3	Se cuenta con desarrollos y control total por parte del área de TI.	9	B
SERVICIOS	Work Space - Cuentas de correos	12	[E24] Caída del sistema por agotamiento de recursos	M	2	24	C	4	Es administrado por el área de TI, con el control de acceso a personal autorizado.	6	B
SERVICIOS	Acronix Protect - Copias en la nube	15	[A6] Abuso de privilegios de acceso	A	1	15	A	4	Suscripción activa y administrada por la TI.	4	D
SERVICIOS	Cuentas de Google Drive	13	[A7] Uso no previsto	M	2	26	C	4	Control desde las TI. Pero con garantías de compromiso del buen uso del personal responsable.	7	B
SERVICIOS	SIESA CONTABLE CLOUD	12	[E2] Errores del administrador	M	2	24	C	4	Solo la jefe administrativa cuenta con el control total del sistema SIESA.	6	B
SERVICIOS	Rastreo de flotas	13	[A11] Acceso no autorizado	A	1	13	A	3	Se tiene personal encargado del uso y seguimiento de la plataforma, pero no se tiene control y	4	D

									seguimiento de accesos.		
SERVICIOS	Hosting, Dominio	12	[A24] Denegación de servicio	M	2	24	C	4	Servicios administrado y gestionado por proveedores externos.	6	B
SERVICIOS	Tiene virtual Agrofy	15	[A10] Alteración de secuencia	A	1	15	A	4	Se tiene control desde las TI. Y personal asignado para su gestión.	4	D
SOFTWARE	Sistema operativo Windows 10 - Windows 11	17	[I5] Avería de origen físico o lógico	M	3	51	C	4	Sistemas originales y seguridad mínima requerida, pero no exentos a daños lógicos.	13	A
SOFTWARE	S.O. Windows Server 2016	19	[A6] Abuso de privilegios de acceso	M	1	19	I	4	Se tiene el control por parte de las TI. Pero no el uso inadecuado que le dé el personal de la compañía.	5	B
SOFTWARE	Antivirus ESET Endpoint Security	12	[E19] Fugas de información	M	2	24	C	4	Servicios corporativos y activos.	6	B
SOFTWARE	Microsoft Office Empresa 2016 - 2019	14	[E21] Errores de mantenimiento / actualización de programas (software)	A	1	14	A	4	Licencias originales y administradas por las TI.	4	D
SOFTWARE	Software contable Helisa	12	[A7] Uso no previsto	M	2	24	C	3	Administración y gestión por parte del área contable.	8	B

SOFTWARE	Software de copias e seguridad ACRONIS PROTECT	19	[A18] Destrucción de información	M	2	38	C	4	Suscripción en la nube activa y administrada por las TI.	10	B
SOPORTE	Discos duros externos SSD 1T	15	[I5] Avería de origen físico o lógico	M	3	45	C	4	Se tienen discos externos confiables y designados a TI y Contabilidad.	11	A
SOPORTE	Memorias USB 64 GB	15	[E18] Destrucción de información	M	3	45	C	4	Dispositivos no administrados y contralados por las TI.	11	A
SERVICIOS	SIESA NOMINA CLOUD	9	[E2] Errores del administrador	M	2	18	I	4	Solo la jefe administrativa cuenta con el control total del sistema SIESA.	5	B

Fuente: Elaboración propia.

Anexo G. Resumen Analítico Especializado RAE

Tabla 27. Resumen Analítico Especializado RAE

Fecha de Realización:	31/07/2023
Programa:	Especialización en Seguridad informática
Línea de Investigación:	Proyecto de Desarrollo tecnológico
Título:	Diseño de un sistema de gestión de la seguridad de la información para Ginsac Colombia SAS
Autor(es):	Jhonatan Fabian Cruz Conde

Fuentes bibliográficas destacadas:

ADMINISTRADOR. Qué es el riesgo de Seguridad de información». LD GRUPO (blog). System [EN LINEA]. (10, abril, 2019). [Consultado el 25, junio, 2022]. Disponible en Internet: <https://www.ldgrupo.com.pe/que-es-el-riesgo-de-seguridad-de-informacion/>.

ADRIEL, Araujo. ISO 27001: Cómo hacer tu política del SGSI - Hackmetrix Blog. Hackmetrix Blog [EN LINEA]. (9, septiembre, 2021). [Consultado el 2, diciembre, 2022]. Disponible en Internet: <https://blog.hackmetrix.com/politica-del-sgsi/>.

CÓMO MITIGAR riesgos en ISO 27001: opciones disponibles [Anónimo]. Software 45001 - ISOTools Chile [EN LINEA]. [Consultado el 25, junio, 2022]. Disponible en Internet: <https://www.isotools.cl/mitigar-riesgos-iso-27001/>.

CÓMO MITIGAR riesgos en ISO 27001: opciones disponibles [Anónimo]. Software 45001 - ISOTools Chile [EN LINEA]. (2022). [Consultado el 25, junio, 2022]. Disponible en Internet: <https://www.isotools.cl/mitigar-riesgos-iso-27001/>.

DIARIO OFICIA. El CONGRESO DE COLOMBIA. LEY 1273 DE 2009 [EN LINEA]. [Consultado el 15, junio, 2022]. Disponible en Internet: <https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf>.

INCIBE. Autodiagnóstico ligero, INCIBE - Instituto Nacional de Ciberseguridad. Autodiagnóstico ligero, INCIBE - Instituto Nacional de Ciberseguridad [EN LINEA]. [Consultado el 25, junio, 2022]. Disponible en Internet: <https://adl.incibe.es/questions.php#resultado>.

INCIBE. Guia_apoyo_SGSI.pdf. (30, mayo, 2022). [Consultado el 21, junio, 2022]. Disponible en Internet: <https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf>.

INCIBE. Autodiagnóstico ligero, INCIBE - Instituto Nacional de Ciberseguridad. [Consultado el 5, junio, 2022]. Disponible en Internet: <https://adl.incibe.es/pdfs/Procesos_medio.pdf>.

ISO 27001. ISO 27001 - Software ISO 27001 de Sistemas de Gestión. Software ISO [EN LINEA]. [Consultado el 8, junio, 2022]. Disponible en Internet: <https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/>.

MINTIC. Elaboración de la política general de seguridad y privacidad de la información. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN [EN LINEA]. [Consultado el 23, mayo, 2022]. Disponible en Internet: <https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf>.

PMG SSI ISO 27001. ISO 27001: Los activos de información. Blog especializado en Seguridad de la Información y Ciberseguridad [EN LINEA]. (30, marzo, 2015). [Consultado el 18, junio, 2022]. Disponible en Internet: <https://www.pmg-ssi.com/2015/03/iso-27001-los-activos-de-informacion/>.

Resumen:

El proyecto está orientado al diseño del sistema de gestión de la seguridad de la información (SGSI) para la organización Ginsac Colombia SAS, realizando un estudio de seguridad informática en la organización, identificando las fortalezas y las debilidades de seguridad en los procesos de las tecnologías de información, evaluando la efectividad que garantizará un mayor grado de eficiencia, eficacia, confidencialidad, integridad para la toma de decisiones de los sistemas de información.

El diseño del SGSI resalta la necesidad, el interés y la mayor responsabilidad de la alta dirección de GINSAC COLOMBIA para aprobar y mejorar la infraestructura y seguridad tecnológica. Se realiza un inventario de activos relacionados con el entorno informático, se realiza una evaluación de riesgos y se proponen estrategias, controles, proyectos y políticas para minimizar los riesgos que amenazan con la seguridad y continuidad de la compañía.

Palabras claves:	Activos, Datos, ISO/IEC 27000, Seguridad de la información, Vulnerabilidad.
Contenido del documento:	• Introducción • Definición del problema • Justificación • Objetivos • Marco Referencial • Diseño Metodológico • Desarrollo de los Objetivos • Conclusiones • Recomendaciones
Descripción del problema de investigación:	¿Cómo el diseño del sistema de gestión de la seguridad de la información (SGSI) alineados con la normativa del estándar de la ISO/IEC 27001:2013, ayudarán a minimizar riesgos, amenazas y vulnerabilidades, a proteger la información y garantizar sistemas confiables y seguros en la organización Ginsac Colombia SAS?
Objetivo general:	Diseñar un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001:2013, para la organización Ginsac Colombia SAS
Objetivos específicos:	• Analizar la situación actual de la organización Ginsac Colombia SAS, en cuanto a seguridad de la información para definir el alcance. • Elaborar el inventario de activos que serán acobijados por el sistema de gestión de la seguridad de la información. • Evaluar los riesgos informáticos del inventario de activos, a partir de la metodología Magerit. • Proponer políticas de seguridad bases para el sistema de gestión de la seguridad de la información (SGSI), basado en el estándar de la ISO/IEC 27001.

Metodología:	El proyecto se realizó bajo los lineamientos de MINTIC y la metodología MAGERIT.
Principales referentes teóricos y conceptuales: INCIBE. Autodiagnóstico ligero, MAGERIT V.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, MINTIC. Elaboración de la política general de seguridad y privacidad de la información. SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.	
Resultados:	El fortalecimiento del SGSI diseñado para Ginsac Colombia SAS deberá realizarse continuamente, le permitirá contar con información de nuevos riesgos a los que está expuesto su entorno tecnológico, calificar las estrategias actuales y endurecerlas, implementar nuevas tecnologías en seguridad física y digital, sobre todo mejorar la administración y gestión de los sistemas de la información.
Conclusiones:	Se realizó un buen diseño del SGSI, utilizando herramientas y las buenas prácticas avaladas por normas internacionales, que fueron esenciales para obtener el resultado del diagnóstico del estado actual de las tecnologías de información y el nivel de madurez, funcionalidad y seguridad de cada proceso y sistema informático. Resultados considerables para el mejoramiento en seguridad de la información y factores claves e importantes que se encuentran en riesgo como lo es las tecnologías, procesos y sobre todo el personal que interactúa con los sistemas informáticos de la compañía.