UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE INGENIERIA
CARRERA DE INGENIERIA EN SISTEMAS COMPUTACIONALES

TEMA:

Propuesta metodológica para la implementación de SGSI basado en ISO 27001:2022 aplicada al proceso “Gestión de Cobranzas” de la empresa Novacobranzas S.A.

AUTOR:
Mora Henríquez, Álvaro Fernando

Componente práctico de examen complexivo previo a la obtención del título de
INGENIERO EN SISTEMAS COMPUTACIONALES

TUTOR:
Ing. Toala Quimí, Edison José

Guayaquil - Ecuador
04 de septiembre de 2025

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE INGENIERIA

CARRERA DE INGENIERIA EN SISTEMAS COMPUTACIONALES

CERTIFICACIÓN

Certificamos que el presente Componente Práctico de Examen Complexivo fue realizado en su totalidad por el Sr. **Mora Henríquez, Álvaro Fernando,** como requerimiento para la obtención del título de **INGENIERO EN SISTEMAS COMPUTACIONALES.**

TUTOR (A)

f. _____

Toala Quimí, Edison José

Guayaquil, a los 4 días del mes de septiembre del año 2025

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE INGENIERIA

CARRERA DE INGENIERIA EN SISTEMAS COMPUTACIONALES

DECLARACIÓN DE RESPONSABILIDAD

Yo, Mora Henríquez, Álvaro Fernando

DECLARO QUE:

El Componente Práctico de Examen Complexivo, "**Propuesta metodológica para la implementación de SGSI basado en ISO 27001:2022 aplicada al proceso "Gestión de Cobranzas" de la empresa Novacobranzas S.A.**" previo a la obtención del título de **INGENIERO EN SISTEMAS COMPUTACIONALES** ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Integración Curricular referido.

Guayaquil, a los 4 días del mes de septiembre del año 2025

f. 

_____

Mora Henríquez, Álvaro Fernando

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE INGENIERIA

CARRERA DE INGENIERIA EN SISTEMAS COMPUTACIONALES

AUTORIZACIÓN

Yo, **Mora Henríquez, Álvaro Fernando**

Autorizo a la Universidad Católica de Santiago de Guayaquil a la **publicación** en la biblioteca de la institución del Componente Práctico de Examen Complexivo, "**Propuesta metodológica para la implementación de SGSI basado en ISO 27001:2022 aplicada al proceso "Gestión de Cobranzas" de la empresa Novacobranzas S.A.**", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 4 días del mes de septiembre del año 2025

EL AUTOR:

f. 

_____

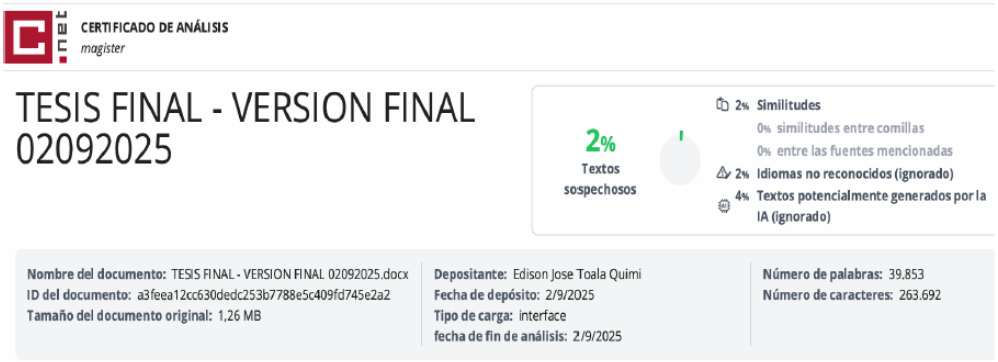
Mora Henríquez, Álvaro Fernando

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE INGENIERIA

CARRERA DE INGENIERIA EN SISTEMAS COMPUTACIONALES

REPORTE ANTIPLAGIO



CERTIFICADO DE ANÁLISIS
magister

TESIS FINAL - VERSION FINAL 02092025

2% Textos sospechosos

2% Similitudes
0% similitudes entre comillas
0% entre las fuentes mencionadas
2% Idiomas no reconocidos (ignorado)
4% Textos potencialmente generados por la IA (ignorado)

Nombre del documento: TESIS FINAL - VERSION FINAL 02092025.docx
ID del documento: a3feea12cc630dedc253b7788e5c409fd745e2a2
Tamaño del documento original: 1,26 MB

Depositante: Edison Jose Toala Quimi
Fecha de depósito: 2/9/2025
Tipo de carga: interface
fecha de fin de análisis: 2/9/2025

Número de palabras: 39.853
Número de caracteres: 263.692

TUTOR (A)

f. _____

Toala Quimí, Edison José

AGRADECIMIENTO

Primero, quiero darle mi más sincero agradecimiento a Dios por darme la vida, salud y esta oportunidad de acabar esta meta personal y profesional.

A mi esposa, gracias por estar siempre a mi lado en las buenas y en las malas, por entender esos momentos en los que no te hacia compañía y por brindarme siempre palabras que me daban ánimos para superar los momentos más difíciles.

A mis padres, gracias por siempre estar dándome todo su apoyo y haberme ayudado en cada etapa de mi vida, no me alcanzaría esta vida para regresarles todo lo que han hecho por mí, también por confiar en mí y por ser mi mayor inspiración.

Extiendo también mi gratitud a mi tutor de trabajo de titulación y profesores de mi carrera, quienes con paciencia y dedicación compartieron sus conocimientos, orientándome a lo largo de este camino académico. Cada granito de arena ha sido un aporte enorme para dar forma a este trabajo de titulación.

DEDICATORIA

A mi esposa, por todo el amor, paciencia y apoyo incondicional, especialmente el apoyo que me brindo, que me dio durante todo este proceso de culminación de mi trabajo de titulación. Gracias a su compañía constante y sus palabras de aliento que me ayudaron a no rendirme y me dieron la fortaleza para terminar este trabajo de titulación.

A mis padres, quienes con su ejemplo de esfuerzo, valores y dedicación me enseñaron a perseverar frente a cada desafío. Todo lo que he alcanzado es fruto de sus enseñanzas y de su confianza en mí. Gracias a mis padres, quienes fueron un ejemplo de esfuerzo, valores y dedicación me enseñaron a perseverar ante cada desafío que se me presente.

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE INGENIERIA

CARRERA DE INGENIERIA EN SISTEMAS COMPUTACIONALES

TRIBUNAL DE SUSTENTACIÓN

f. _____

ING. CESAR ADRIANO SALAZAR TOVAR

DECANO O SU DELEGADO

f. _____

ING. ANA CAMACHO CORONEL, MGS

DIRECTORA DE CARRERA

f. _____

ING. SOSA

COORDINADOR DE ÁREA O SU DELEGADO

ÍNDICE

RESUMEN

El presente proyecto tiene como objetivo presentar una propuesta metodológica para la implementación de SGSI basado en ISO 27001:2022 aplicándolo en el proceso de Gestión de Cobranzas de la empresa Novacobranzas. La investigación aborda la necesidad de mejorar la seguridad de la información dentro de la empresa debido a la creciente exposición a ciberataques y amenazas internas. A través de un análisis de brechas (Análisis GAP), se identificaron deficiencias significativas en la infraestructura de seguridad de la empresa, evidenciando la falta de controles adecuados, políticas de seguridad documentadas y mecanismos de respuesta ante incidentes. El estudio también revela que los empleados tienen bajo conocimiento en seguridad informática, lo que aumenta la vulnerabilidad a ataques externos e internos.

Palabras claves: ISO 27001:2022, Protección de Datos Personales, SGSI, Análisis de brechas, Vulnerabilidad.

ABSTRACT

The purpose of this thesis is to present a methodological proposal for the implementation of an ISMS based on ISO 27001:2022, applying it to the Debt Collection Management process of Novacobranzas. The research addresses the need to improve information security within the company due to the growing exposure to cyberattacks and internal threats.

Through a gap analysis, significant deficiencies in the company's security infrastructure were identified, highlighting a lack of adequate controls, documented security policies, and incident response mechanisms. The study also reveals that employees have limited knowledge of computer security, which increases vulnerability to external and internal attacks.

Key words: ISO 27001:2022, Personal Data Protection, ISMS, GAP Analysis, Risk

INTRODUCCIÓN

En el mundo empresarial, existe una tendencia general de considerar como activos de la empresa solo bienes tangibles: mobiliario, maquinaria, servidores, etc., sin embargo, la información es un bien intangible que constituye uno de los activos más importantes y de mayor preocupación, por lo cual la seguridad de la información es un tema que afecta a todo tipo de organizaciones o personas y cada vez hay más dispositivos tecnológicos que facilitan el acceso, procesamiento y almacenamiento de la información de una manera muy sencilla, por lo cual, no tener establecidas políticas de seguridad de la información, genera riesgos y amenazas que pueden ser explotadas por diferentes tipos de mecanismos tecnológicos o de personal interno de la empresa.

Cuando se habla de seguridad de la información, existen elementos comunes que todas las organizaciones deben considerar al momento de aplicar medidas: las personas, los procesos y la tecnología, donde realizar inversiones para adquirir herramientas tecnológicas que permitan implementar controles de accesos son solo una etapa que debe ser soportada con normas o estándares internacionales sobre las buenas prácticas que las organizaciones deben adoptar para mitigar los riegos y amenazas sobre la información que se genera.

La seguridad de la información siempre ha sido un tema que genera expectativa en congresos y eventos internacionales, con el auge de la tecnología tanto como para resguardar y proteger el acceso a la información, además de contar con mecanismos internos de control de accesos, no asegura un 100% evitar ser objetivos de ataques y robo de información, ya que así también hay organizaciones o personas mal intencionadas que utilizan esas mismas tecnologías para realizar ataques informáticos para robar información.

CAPÍTULO I
EL PROBLEMA

1.1 Ubicación del Problema en un Contexto

La empresa Novacobranzas S.A. ya fue objeto de un ciberataque, el cual fue realizado a través de un dispositivo de comunicación de la empresa (enrutador), que al no tener las seguridades necesarias, el atacante implantó un software malicioso (virus) en una de las computadoras de los empleados, este software ocasionó que ese ordenador envíe de forma masiva correos electrónicos por medio del dominio de la empresa, ocasionando que el dominio de la empresa fuera bloqueado y no pueda enviar correos a través de su dominio, este ataque fue ocasionado por la falta de seguridad, control en los computadores que utilizan los empleados y una serie de factores que posteriormente fueron identificados.

1.2 Causas y Consecuencias del Problema

Las principales causas del problema son la falta de mecanismos de seguridad, la ausencia de normas o estándares que no están definidas en la empresa y la ausencia de políticas de gestión de riesgo, esto puede generar a que la empresa se encuentre más expuesta a que sucedan ataques de forma más continua así como otros eventos que aumenten su nivel de riesgo, generando un mayor perjuicio a la empresa, estos riesgos pueden ser externos (medios tecnológicos) o internos (personal de la empresa), por desconocimiento sobre la seguridad de la información.

1.3 Delimitación del Problema

El problema está enfocado en el análisis, diseño y posterior implementación de políticas de seguridad de la información para la empresa Novacobranzas S.A., para minimizar futuros riesgos y amenazas, sobre la infraestructura tecnológica actual con

la que cuenta la empresa o el incorrecto manejo de la información por parte de los empleados.

1.4 Formulación del Problema

¿Con el análisis e implementación de las políticas de seguridad de la información, la empresa Novacobranzas S.A. dispondrá de una herramienta que le permitirá realizar la gestión de riesgos sobre su activo intangible?

1.5 Evaluación del Problema

Para evaluar el problema de este proyecto de titulación se toma en cuenta la información que proporciona la empresa, la cual debe ser información real ya que con ella se identificará dónde están los procesos más críticos de la empresa y de esos seleccionar el más crítico para la empresa.

Como siguiente punto a considerar está la delimitación del problema, la información proporcionada por la empresa y los antecedentes de ataques que ha sufrido la empresa con anterioridad permitirá realizar el análisis y diseño de políticas de seguridad de la información para su proceso más crítico “Gestión de cobranzas” y posteriormente realizar su implementación.

1.6 Objetivos

1.6.1 Objetivo General

Aplicar la norma ISO 27001:2022 para la implementación de SGSI al proceso “Gestión de Cobranzas” a través de alguna de las metodologías existentes en la actualidad, incluyendo políticas de seguridad de la información para la empresa Novacobranzas S.A.

1.6.2 Objetivos Específicos

- Realizar el levantamiento de la información para definir un diagnóstico y determinar las condiciones actuales del proceso “Gestión de Cobranzas” que viene funcionando en la empresa Novacobranzas S.A.
- Seleccionar y aplicar la metodología de ISO 27001:2022 para la identificación de activos de información del proceso “Gestión de Cobranzas”, realizar el análisis de riesgo y amenazas a las que están expuestos los activos de la empresa Novacobranzas S.A.
- Aplicar las estrategias de gestión de riesgos para mitigar, reducir, transferir o eliminar los riesgos significativos y de alto impacto en los activos de información del proceso “Gestión de Cobranzas”, buscando garantizar la disponibilidad, integridad y confidencialidad de los procesos y/o información de la empresa Novacobranzas S.A.

1.7 Alcances del Problema

Con la finalidad de asegurar la integridad, confidencialidad y disponibilidad de los activos de información de la empresa, este trabajo de titulación está orientado al análisis, diseño e implementación de políticas de seguridad de la información, lo cual permitirá establecer políticas de control sobre la información que se maneja en la empresa.

1.8 Justificación e Importancia

Este componente práctico busca la aplicación de SGSI a través de alguna de las metodologías disponibles en el mercado para que posteriormente la empresa por medio de una auditoría interna opte por la certificación de la ISO 27001:2022, a través del uso herramientas tecnológicas y las buenas prácticas de las normas y estándares que ayuden al control de la información que esta maneja. Con esto se pretende obtener resultados positivos para la empresa por medio del control y almacenamiento de la información por parte de los empleados de esta.

1.9 Hipótesis o Pregunta de Investigación

¿El diseño de una propuesta de implementación de un SGSI basado en ISO 27001:2022 en la empresa Novacobranzas S.A., permitirá gestionar los riesgos y amenazas sobre la información que maneja la empresa?

1.10 Variables de la Investigación

Variable independiente: Diseño e implementación de políticas de seguridad de la información.

Variable dependiente: Gestionar riesgos y amenazas a través de la implementación de la ISO 27001:2022.

CAPITULO II

MARCO TEÓRICO Y CONCEPTUAL

En el siguiente marco teórico se profundizará y se mencionaran algunos conceptos, investigaciones y antecedentes, que aportaran en gran medida al proceso de diseño e implementación del presente trabajo de titulación.

2.1 Novacobranzas S.A.

2.1.1 Visión

Buscar soluciones óptimas y efectivas para la recuperación de cartera de nuestros clientes mediante un conjunto de profesionales capacitados, comprometidos y con el mejor equipo tecnológico.

2.1.2 Misión

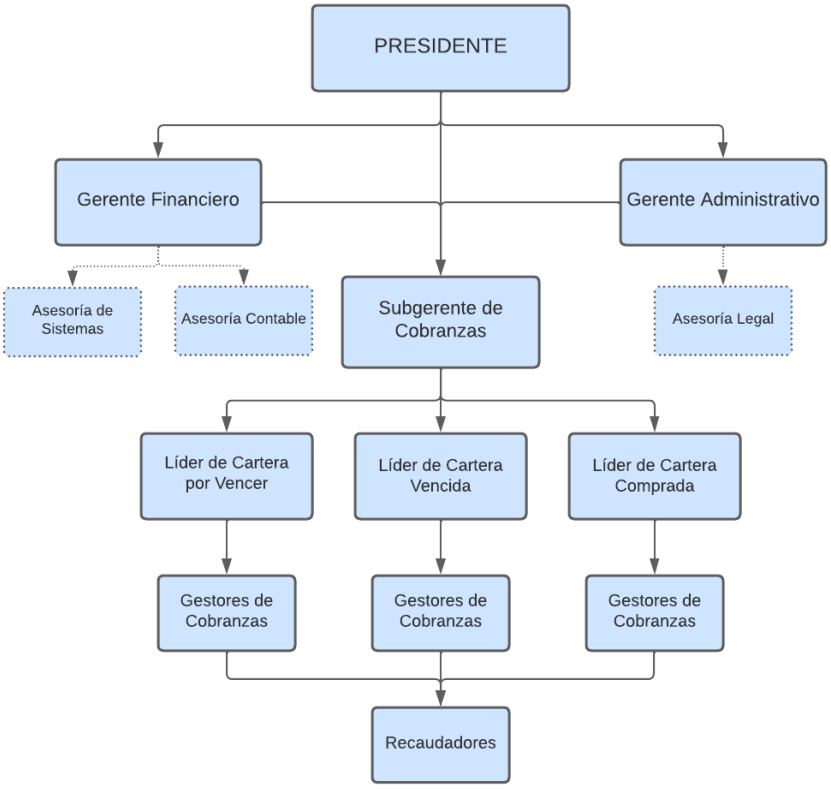
Ser la empresa líder en brindar soluciones óptimas de recuperación de cartera en el sistema financiero ecuatoriano, mediante un mecanismo de transparencia, honestidad, compromiso y cumplimiento.

2.1.3 Producto y/o Servicio

En Novacobranzas S.A. es una empresa dedicada al cobro y compra de carteras de clientes de entidades que deben valores a las mismas. Ellos se encargan de toda la gestión de cobro para las entidades y así mismo recibir una comisión por todos los valores que han logrado que los deudores paguen a dichas empresas.

2.1.4 Organigrama

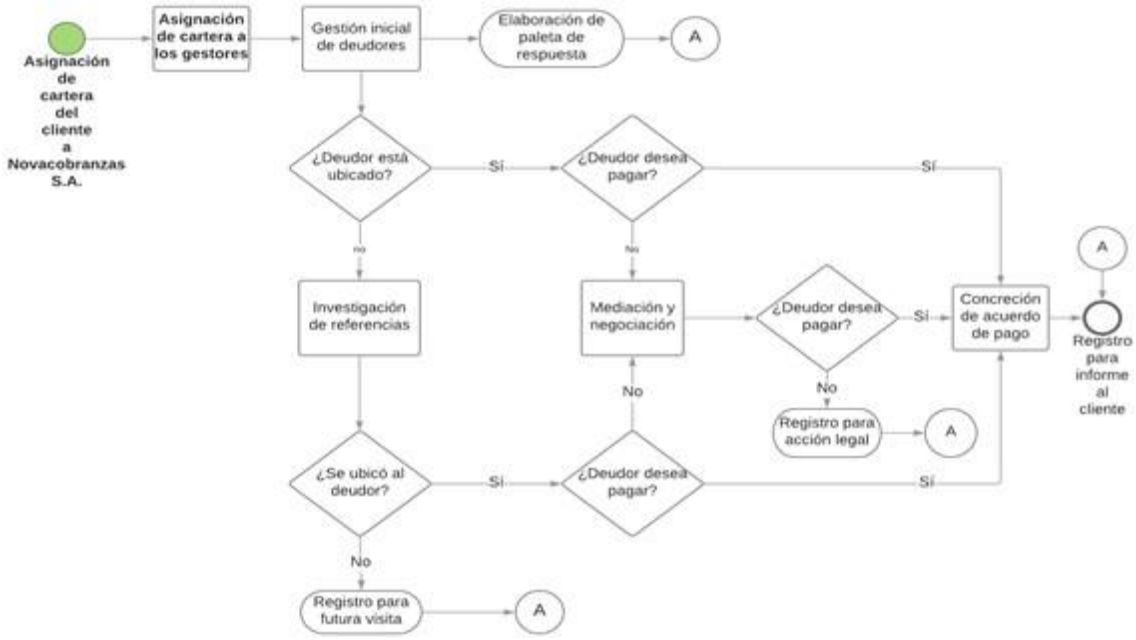
Figura 1. Organigrama de Novacobranzas S.A.



Nota. El organigrama de la empresa

2.1.5 Proceso de Gestión de Cobranzas

Figura 2. Diagrama de flujo del proceso de Gestión de Cobranzas de Novacobranzas S.A.



Nota. Diagrama de flujo del proceso de cobranza que realiza la empresa Novacobranzas S.A.

2.2 Seguridad De La Información

La seguridad de la información se refiere a un conjunto de medidas y técnicas empleadas para controlar y proteger los datos manejados dentro de una organización, como se menciona en un blog de ESGinnova Group (2021). Es esencial para las organizaciones garantizar la protección de sus datos dentro de sus sistemas, ya que estos datos son fundamentales para sus operaciones, independientemente de su tamaño. Incluyen información sensible tanto de clientes como de trabajadores, por lo que se deben implementar medidas de seguridad en protección de datos, en cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPD) vigente, que exige un mejor control de la información de los clientes por parte de las organizaciones. (ESGinnova Group, 2021)

Si tenemos en cuenta que la seguridad de la información varía según las características específicas de cada empresa y el ámbito en el que opera, es posible identificar una serie de objetivos compartidos por todas las empresas que se dedican a salvaguardar sus datos e información. Estos objetivos están descritos en la norma ISO 27001, que proporciona un marco para implementar sistemas de gestión de seguridad de la información. El principal propósito de la norma ISO 27001 es garantizar la protección de los activos de información, que incluyen tanto equipos como usuarios, así como la propia información. (ESGinnova Group, 2021)

La seguridad de la información es la que se encarga de garantizar los siguientes aspectos:

- Confidencialidad
- Integridad
- Disponibilidad

2.2.1 Confidencialidad

Según el blog "¿Qué es la seguridad de la información y cuantos tipos hay?" de ESGinnova Group (2021), la confidencialidad es un principio fundamental en la protección de la información, actuando como un seguro que protege los datos sensibles. Su objetivo es garantizar que solo aquellos con la autorización adecuada, como empleados, clientes o socios, puedan acceder a dicha información. De esta manera, se evita la divulgación no autorizada, el robo o el uso indebido de datos, protegiendo la privacidad e integridad de la información.

Para lograr un adecuado nivel de confidencialidad, es necesario implementar medidas de seguridad robustas en los sistemas de información como por ejemplo controles de acceso, cifrado de datos, gestión de permisos, formación del personal sobre políticas y protocolos de la organización, entre otras. La confidencialidad no solo se aplica a la información digital, sino también a la información física como

documentos escritos, contratos o formularios de clientes donde también es importante protegerla mediante su almacenamiento seguro y el control de su acceso. (ESGinnova Group, 2021)

2.2.2 Integridad

De acuerdo, al libro “Seguridad de la Información. Redes, informática y sistemas de información” de Areitio Bertolin, Javier, esta es responsable de garantizar que la información de la organización no haya sido cambiada o alterada de ninguna forma por personas no autorizadas. También establece dos facetas de integridad:

- Integridad de datos. Establece que los datos no hayan sido alterados sin autorización, mientras se almacenan, procesan o transmiten.
- Integridad del sistema. Es la manera en que un sistema realice la función deseada, libre de manipulación. (JAVIER, 2008a)

2.2.3 Disponibilidad

La disponibilidad de la información se refiere a la certeza de que los usuarios autorizados podrán acceder y utilizar la información que necesitan cuando la necesiten. Esta accesibilidad debe ser permanente, sin restricciones de tiempo, espacio o dispositivo, y debe estar disponible para cualquier persona o entidad con los permisos adecuados. (ESGinnova Group, 2021)

2.3 Activos de información

En el contexto de la norma ISO/IEC 27001, un activo de información se define como "algo que una organización valora y por lo tanto debe proteger". Esta definición abarca una amplia gama de elementos que son esenciales para el funcionamiento y el éxito de una organización. (*¿Qué Es La Gestión de Activos de Información? - NovaSec MS*, n.d.)

Según Vega Velasco, 2008, los activos relacionados con sistemas de información, penden ser clasificados de la siguiente forma (Vega Velasco, 2008):

- Recursos de información:
    - Información: La base del conocimiento:
    - Bases de datos: Almacenes de información crucial para la toma de decisiones estratégicas.
    - Manuales y procedimientos: Guías que estandarizan las operaciones y garantizan la eficiencia.
    - Planes de continuidad: Estrategias para mantener la operatividad ante interrupciones inesperadas.
    - Información archivada: Registro histórico que aporta valor y conocimiento a la organización.
    - Disposiciones de emergencia: Medidas para recuperar información en caso de situaciones imprevistas.
- Software:
    - Software de aplicaciones: Herramientas que permiten realizar tareas específicas con mayor eficiencia.
    - Sistemas operativos: Plataformas que controlan el funcionamiento de los equipos y la ejecución de programas.
    - Herramientas de desarrollo: Programas para crear, modificar y mejorar el software.
    - Utilitarios: Programas que facilitan la gestión de los equipos y la información.
- Equipos:
    - Servidores: Potentes equipos que centralizan el almacenamiento y procesamiento de datos para una mayor accesibilidad y seguridad.

- Computadoras: Dispositivos donde los usuarios interactúan con la información y realizan sus tareas.
- Enrutadores, Switches y Hubs: Elementos que permiten la comunicación y el flujo de información en la red.
- PABX: Sistemas telefónicos que facilitan la comunicación interna y externa de la organización.
- Equipos de energía y aire acondicionado: Elementos que garantizan el funcionamiento continuo y la protección de los equipos.
- Equipos de comunicaciones: Dispositivos que permiten la conexión a internet y otras redes para una mayor comunicación y colaboración.

2.4 Amenazas y Vulnerabilidades de la información

En el mundo actual lo más valioso para una empresa es la información y eso lo saben muchas personas, por eso personas maliciosas encuentran formas de vulnerar la seguridad y obtener dicha información secuestrándola y posteriormente utilizándola para pedir rescates a las empresas o amenazando a la persona natural para estafarla. A continuación, se enlistará algunas de las amenazas que son más frecuentes: (Vega Velasco, 2008)

- Amenazas físicas: Involucran el acceso no autorizado a los recursos físicos, como robos, daños a equipos o sabotajes. También incluye el acceso no autorizado mediante ingeniería social, explotando la confianza del personal.
- Fraude informático: Engaño a los clientes mediante la venta de productos o servicios inexistentes a través de promociones o agencias falsas.
- Intrusiones: Es el acceso no autorizado a los diferentes sistemas de comunicación o los servidores de una empresa, esto como objetivo para dañar la reputación u obtener algún beneficio económico de la empresa.
- Errores humanos: Es toda acción involuntaria que afecta a la seguridad de las empresas como lo son las contraseñas débiles, respaldos mal ejecutados,

afectación en los servidores o configuraciones mal implementadas en los equipos.

- Software ilegal: Al usar software que no esté licenciado puede generar vulnerabilidades en los sistemas, ya que no cuenta con actualizaciones o parches de seguridad oficiales de los creadores del software, esto puede generar agujeros de seguridad que pueden ser aprovechados por terceros.
- Malware: Programas o partes de programas que pueden causar daños en los sistemas informáticos, como virus, troyanos, gusanos o puertas traseras. Estos programas se activan en los equipos finales y su evolución se ha visto impulsada por la creciente conectividad a internet y las técnicas de engaño utilizadas por los atacantes.
- Evaluación de riesgos: Es fundamental estimar los riesgos a los que están expuestos la red, los servidores y los dispositivos de red. Si bien la evaluación precisa de la información es compleja, se puede realizar una aproximación considerando su posible pérdida o alteración.

Figura 3. Estimación de los Riesgos.

Nota: Una metodología de implementar un sistema de seguridad está expuesto en la figura. Adaptado de "POLÍTICAS Y SEGURIDAD DE LA INFORMACIÓN" (p. 67), por W. Vega, 2008, Scielo.

2.5 Normas y estándares

2.5.1 ISO/IEC 27001:2022

La ISO/IEC 27001:2022 se alza como la norma internacional de referencia para los Sistemas de Gestión de la Seguridad de la Información (SGSI). Ofrece un marco sólido y adaptable para proteger la información, sin importar el tamaño o la naturaleza de tu organización. En un mundo donde los riesgos acechan a cada paso, cada vez son más las entidades que optan por implementar un SGSI bajo la norma ISO/IEC 27001:2022. Esta decisión estratégica les permite protegerse contra las amenazas y garantizar la seguridad de sus datos. (*NQA-ISO-27001-Guia-de-Implantacion.Pdf*, n.d.)

A continuación, se enumerará las 10 cláusulas que conforman a la ISO 27001:2022 y se hablara un poco de cada una:

1. Alcance: Define el alcance del SGSI, incluyendo los activos de información a proteger y los procesos relevantes. (*NQA-ISO-27001-Guia-de-Implantacion.Pdf*, n.d.)
2. Referencias normativas: Especifica las normas y documentos que se utilizan como referencia en la norma ISO 27001:2022. (*NQA-ISO-27001-Guia-de-Implantacion.Pdf*, n.d.)
3. Términos y definiciones: Define los términos clave utilizados en la norma. (*NQA-ISO-27001-Guia-de-Implantacion.Pdf*, n.d.)
4. Contexto de la organización: Requiere que la organización comprenda su contexto interno y externo, incluyendo las partes interesadas y los riesgos y

oportunidades relacionados con la seguridad de la información. (*NQA-ISO-27001-Guia-de-Implantacion.Pdf*, n.d.)

5. Liderazgo: Demanda que la alta dirección de la organización se comprometa con el SGSI y asigne los recursos necesarios para su implementación y mantenimiento. (*NQA-ISO-27001-Guia-de-Implantacion.Pdf*, n.d.)
6. Planificación: La organización debe establecer planes para abordar los riesgos y oportunidades relacionados con la seguridad de la información. (*NQA-ISO-27001-Guia-de-Implantacion.Pdf*, n.d.)
7. Soporte: Se refiere a los recursos necesarios para la implementación y mantenimiento del SGSI, incluyendo infraestructura, recursos humanos y financieros. (*NQA-ISO-27001-Guia-de-Implantacion.Pdf*, n.d.)
8. Operación: Describe los controles que la organización debe implementar para proteger sus activos de información, como control de acceso, gestión de incidentes y seguridad de las comunicaciones. (*NQA-ISO-27001-Guia-de-Implantacion.Pdf*, n.d.)
9. Evaluación del desempeño: La organización debe realizar evaluaciones periódicas del SGSI para asegurar su eficacia. (*NQA-ISO-27001-Guia-de-Implantacion.Pdf*, n.d.)
10. Mejora: La organización debe buscar continuamente mejorar el SGSI mediante la acción correctiva, preventiva y la mejora continua. (*NQA-ISO-27001-Guia-de-Implantacion.Pdf*, n.d.)

2.5.2 NIST Cybersecurity Framework

El NIST Cybersecurity Framework (CSF) es un seguro desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos para proteger a las organizaciones de las amenazas cibernéticas. Se trata de un conjunto de normas, guías y mejores prácticas que se adapta a las necesidades de empresas de cualquier tamaño. (Almuhammadi & Alsaleh, 2017)

¿Qué ofrece el NIST Cybersecurity Framework?

- Flexibilidad: No es una norma rígida, sino una guía adaptable para la organización. (Almuhammadi & Alsaleh, 2017)
- Estructura clara: Se basa en cinco funciones clave: identificar, proteger, detectar, responder y recuperar. (Almuhammadi & Alsaleh, 2017)
- Desglose práctico: Cada función se divide en categorías y subcategorías para facilitar su implementación. (Almuhammadi & Alsaleh, 2017)
- Enfoque estratégico: Te ayuda a priorizar las áreas más críticas para tu seguridad.
- Recursos a tu disposición: Ofrece herramientas, plantillas y guías para facilitar su uso. (Almuhammadi & Alsaleh, 2017)

¿Para quién es el NIST Cybersecurity Framework?

- Todas las organizaciones: Empresas privadas, entidades gubernamentales, instituciones sin ánimo de lucro, etc. (Almuhammadi & Alsaleh, 2017)
- Sectores sensibles: Infraestructura crítica, servicios financieros, atención médica, etc. (Almuhammadi & Alsaleh, 2017)
- Organizaciones que buscan mejorar su seguridad: Ideal para quienes aún no tienen un sistema formal de gestión de la seguridad de la información. (Almuhammadi & Alsaleh, 2017)

2.5.3 Ley Orgánica De Protección De Datos Personales

En el año 2019, Ecuador promulgó la Ley Orgánica de Protección de Datos Personales (LOPDP), una armadura legal que vela por el derecho fundamental a la protección de la información personal de todos los ciudadanos ecuatorianos. Esta ley abarca tanto al sector público como al privado, regulando a cualquier persona natural o jurídica que gestione datos personales. (Barrezueta, n.d.)

Lo que regula principalmente la Ley Orgánica de Protección de Datos Personales (LOPDP) es lo siguiente:

- **Principios:** La ley establece una serie de principios que rigen el tratamiento de datos personales, como la licitud, lealtad, transparencia, consentimiento, finalidad, proporcionalidad, exactitud y seguridad. (Barrezueta, n.d.)
- **Derechos del ciudadano:** La LOPDP te empodera con una serie de derechos, incluyendo el acceso, rectificación, cancelación, oposición, portabilidad y limitación del tratamiento de tus datos personales. (Barrezueta, n.d.)
- **Obligaciones para las empresas:** Las empresas que gestionan datos personales tienen la responsabilidad de informar a los ciudadanos sobre el tratamiento de su información, obtener su consentimiento, implementar medidas de seguridad y notificar a la autoridad de control en caso de fugas de datos. (Barrezueta, n.d.)

La Agencia de Protección de Datos Personales (APDP) es la entidad responsable de velar por el cumplimiento de la LOPDP. La APDPD tiene la potestad de sancionar a las empresas que infrinjan la ley. (*Guía-de-Protección-de-Datos-Personales.Pdf*, n.d.)

Las sanciones por incumplir la LOPDP se clasifican en leves, graves y muy graves. Las multas van desde 1000 dólares para las leves, hasta 200.000 dólares para las muy graves. (*Guía-de-Protección-de-Datos-Personales.Pdf*, n.d.)

2.6 Metodologías de identificación y análisis de riesgos

En el complejo mundo de la seguridad de la información, existen diversas estrategias para analizar los riesgos que acechan. Entre las más destacadas encontramos:

2.6.1 Octave (Operationally Critical Threat, As-set, and Vulnerability Evaluation)

De acuerdo con Helena Alemán y Claudia Rodríguez, 2014, destaca como una de las metodologías de análisis de riesgos más populares en el mundo empresarial. Su enfoque práctico se basa en guías específicas para la evaluación y administración de riesgos, lo que la convierte en una herramienta invaluable para proteger la información de tu organización. (Investigación & unad, 2021)

Ofrece una evaluación integral analizando los riesgos de seguridad de la información en la organización y propone un plan para mitigarlos, concientizando más allá de lo técnico a toda la organización sobre la importancia de la seguridad informática. Este mismo funciona con la evaluación de activos en donde el primer paso es identificar y valorar los activos de información de tu organización, como siguiente paso se hace un análisis de la infraestructura de la información para definir los elementos más importantes y finalmente se hacen planes de seguridad que buscan desarrollar estrategias específicas para la organización. (Investigación & unad, 2021)

Esto trae como beneficios la identificación de riesgo, evaluación de riesgos y una estrategia de protección que permite conocer los riesgos que pueden impedir el logro de los objetivos y reducir los riesgos de seguridad de la información prioritaria. (Investigación & unad, 2021)

2.6.2 Magerit

Según Helena Alemán y Claudia Rodríguez, 2014, Magerit es una metodología de análisis y gestión de riesgos de la información desarrollada por el Consejo Superior de Administración Electrónica. Su objetivo principal es estudiar los riesgos que soporta un sistema de información y su entorno, así como recomendar medidas para prevenirlos, controlarlos o mitigarlos. (Investigación & unad, 2021)

Los principales elementos para el análisis de riesgos según Magerit son:

- Activo
- Amenaza
- Vulnerabilidad
- Impacto
- Riesgo
- Salvaguardas

El proceso de análisis de riesgos se desarrolla en las siguientes etapas:

- Planificación
- Análisis de riesgos
- Gestión de riesgos
- Selección de salvaguardas

Magerit describe los pasos para realizar un análisis del estado del riesgo y gestionar su mitigación, así como las tareas básicas para realizar un proyecto de análisis y gestión de riesgos. También aplica la metodología al caso del desarrollo de Sistemas de Información (SI) y muestra una serie de aspectos prácticos derivados de la experiencia acumulada en el tiempo. (Investigación & unad, 2021)

2.6.3 Mehari

En el estudio de Helena Alemán y Claudia Rodríguez, 2014, MEHARI es una metodología de análisis y gestión de riesgos de la información desarrollada por el Club Francés de la Seguridad de la Información (CLUSIF) en 1996. Es de acceso público y gratuita para todo tipo de organizaciones. (Investigación & unad, 2021)

Esta metodología funciona de la siguiente forma, primero se realiza un módulo de análisis de intereses en donde MEHARI analiza los intereses implicados por la seguridad después con el método de análisis de riesgo que ofrece un el análisis de

riesgos con herramientas de apoyo y para finalizar se hace uso de un conjunto de herramientas y elementos que proporciona Mehari necesarios para su implementación. (Investigación & unad, 2021)

2.6.4 NIST SP 800 – 30

El documento "Guía de gestión de riesgo para sistemas de tecnología de la información - Recomendaciones del Instituto Nacional de Estándares y Tecnología" proporciona un conjunto de sugerencias y acciones para una gestión de riesgos efectiva como parte integral de la seguridad de la información. Sin embargo, para lograr el éxito en la gestión de riesgos, es necesario el respaldo y la participación de toda la organización. (Investigación & unad, 2021)

La metodología NIST SP 800-30 consta de nueve pasos fundamentales para llevar a cabo el análisis de riesgos: caracterización del sistema, identificación de amenazas, identificación de vulnerabilidades, análisis de control, determinación del riesgo, análisis de impacto, determinación del riesgo y recomendaciones de control. Esta metodología sirve como base para el desarrollo de un programa efectivo de gestión de riesgos, proporcionando tanto las definiciones como la orientación práctica necesarias para evaluar y mitigar los riesgos identificados dentro de los sistemas de tecnología de la información. Su objetivo principal es facilitar a las organizaciones un proceso de tres pasos: evaluación, mitigación y análisis y evaluación del riesgo, con el fin de gestionar de manera más efectiva los riesgos. (Investigación & unad, 2021)

2.6.5 Coras – Construct a Platform for Risk Analysis of Security Critical Systems.

En el estudio de Helena Alemán y Claudia Rodríguez, 2014, esta técnica es particularmente útil para equipos heterogéneos que buscan identificar vulnerabilidades y amenazas a sus activos de valor. Esta metodología proporciona un modelo, con elementos que son específicos de un análisis de riesgos

principalmente en la realización de dichos modelos, un lenguaje grafico basado en UML (Unified Modelling Language), un editor gráfico que es compatible con Microsoft Visio, una biblioteca de casos reutilizables, una herramienta de gestión de casos para la gestión y reutilización de casos, representación en texto basada en XML (eXtensible Markup Language), y un modelo estandarizado de informes que nos permite contribuir a la mejora de la comunicación entre las partes del proceso de análisis de riesgos. (Investigación & unad, 2021)

2.6.6 Cramm (CCTA Risk Analysis and Management Method)

En el ámbito de la seguridad informática, la gestión de riesgos es un proceso fundamental para proteger los sistemas y datos de una organización. Hay un gran número de metodologías, CRAMM (Checklist for Risk Analysis and Management of Major Information Systems) destaca por ser una opción robusta y flexible. Esta metodología fue desarrollada por Central Communication and Telecommunication Agency (CCTA), el mismo es considerado una herramienta de referencia para el análisis de riesgos para el continente europeo, esta a su vez siendo utilizada por un gran número de empresas, incluyendo organizaciones gubernamentales. (Investigación & unad, 2021)

2.6.7 Ebios - Expresión de las necesidades e identificación de los objetivos de seguridad

En el panorama actual, la seguridad de la información es una responsabilidad crítica para las organizaciones de todo tipo. La gestión eficaz de los riesgos asociados a la seguridad informática es fundamental para proteger los activos y la reputación de una empresa. En este contexto, la metodología EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) se destaca como una herramienta valiosa para la evaluación y el tratamiento de riesgos. (Investigación & unad, 2021)

Desarrollada en Francia, EBIOS se ha convertido en una referencia en el ámbito de la gestión de riesgos de la información. Se caracteriza por su enfoque integral, que abarca desde la identificación de amenazas y vulnerabilidades hasta la implementación de medidas de seguridad y la evaluación de su eficacia. Es una herramienta integral que permite evaluar y abordar los riesgos asociados con la seguridad informática, fomentando una comunicación efectiva dentro de la empresa y con sus colaboradores, cumpliendo con los estándares ISO 27001, 27005 y 31000 para la gestión de riesgos, y proporcionando las justificaciones necesarias para la toma de decisiones, incluyendo descripciones precisas, desafíos estratégicos y riesgos detallados con su impacto en la entidad, así como objetivos y requisitos de seguridad explícitos. (Investigación & unad, 2021)

Tabla 1. Ventajas y Desventajas entre las diferentes Metodologías de Análisis de Riesgo

METODOLOGÍA	ÁMBITO DE APLICACIÓN	VENTAJAS	DESVENTAJAS
OCTAVE	Pymes, organizaciones públicas y privadas.	○ Es auto gestionable, lo que permite que sea desarrollado por empleados de la misma empresa con la ayuda de un equipo multidisciplinario. ○ Elaboración de perfiles de amenazas basados en activos. ○ Creación de planes y estrategias de seguridad. ○ Incluye las fases de análisis y gestión de riesgos. ○ Establece relaciones entre amenazas y vulnerabilidades. ○ Gratuito para uso interno. ○ Ofrece tres métodos: Octave, Octaves y Octave Allegro, los cuales pueden adaptarse a las necesidades de una empresa.	○ No considera el principio de no rechazo de la información. ○ Requiere el uso de numerosos documentos durante el proceso de evaluación de riesgos. ○ Se necesitan conocimientos técnicos extensos para su aplicación. ○ La definición de activos de información no está claramente establecida. ○ Para su aplicación externa, es necesario adquirir una licencia del SEI si se desea implementar la metodología en una entidad externa.
MAGERIT	Gobierno, compañías comerciales y no comerciales, Pymes	○ Brinda una capa completa en lo que es la evaluación y gestión de riesgos. ○ Tiene una documentación bastante completa sobre recursos de información,	○ No añade los procesos, recursos o vulnerabilidades en su modelo. ○ Tiene deficiencias al momento de realizar el inventario de políticas.

METODOLOGÍA	ÁMBITO DE APLICACIÓN	VENTAJAS	DESVENTAJAS
		amenazas y tipos de activos. ○ Esta herramienta es de código abierto y necesita de alguna autorización para utilizarla en un proyecto. ○ Tiene diferentes formas de clasificar a los activos de una empresa para identificar más riesgos y facilitar la implementación de controles preventivos. ○ Tiene 3 objetivos principales: sensibilizar sobre los riesgos y la necesidad de atenderlos a tiempo, proporcionar un método para analizar los riesgos e identificar y planificar las medidas adecuadas para mantener los riesgos controlados. ○ Tiene herramientas para el análisis de riesgo como lo es PILAR.	○ Se tiene la idea de que esta metodología es costosa de implementar para cualquier empresa.
MEHARI	Gobierno, organismos, empresas grandes y medianas, compañías comerciales sin ánimo de lucro (educación, salud, servicios públicos,	○ Es una técnica que puede valorar y reducir los riesgos según las características de la entidad. ○ Se adapta y se ajusta a los requisitos de las normativas ISO 27001,	○ Se centra únicamente en los principios de integridad, confidencialidad y disponibilidad, sin tener en cuenta el principio de no repudio.

METODOLOGÍA	ÁMBITO DE APLICACIÓN	VENTAJAS	DESVENTAJAS
	organizaciones privadas)	27002 y 27005 para establecer los Sistemas de Gestión de la Seguridad de la Información (SGSI) y la gestión de riesgos. ○ A través de este enfoque, se identifican las vulnerabilidades mediante auditorías y se analizan las situaciones de riesgo.	○ La sugerencia de los controles no se integra en el análisis, sino que forma parte de la gestión de los riesgos. ○ La evaluación del impacto de los riesgos se lleva a cabo durante el proceso de gestión y evaluación.
NIST SP 800 30	Utilizada por organizaciones gubernamentales y no gubernamentales.	○ Costo reducido asociado al análisis y resolución del riesgo. ○ Ofrece una síntesis de los aspectos esenciales de las pruebas de seguridad técnica y la evaluación, destacando técnicas específicas, ventajas, limitaciones y sugerencias para su aplicación. ○ La guía proporciona recursos para evaluar y reducir riesgos. ○ Contribuye a mejorar la gestión a través de los resultados del análisis de riesgos.	○ En su modelo no incluye componentes como los procedimientos, los recursos ni las interrelaciones.
CORAS		○ Posee diferentes herramientas de apoyo para el análisis de riesgos, un editor gráfico	○ No lleva a cabo análisis de riesgos de manera cuantitativa.

METODOLOGÍA	ÁMBITO DE APLICACIÓN	VENTAJAS	DESVENTAJAS
		para soportar la elaboración de los modelos basado en Microsoft Visio y utiliza lenguaje grafico basado en UML (Unified Modelling Language). ○ Provee un repositorio de paquetes de experiencias reutilizables. ○ Provee un reporte de las vulnerabilidades encontradas. ○ Útil en el desarrollo y mantenimiento de nuevos sistemas. ○ Basada en modelos de riesgos de sistemas de seguridad críticos.	○ Este modelo, no incluye aspectos como los procesos y las relaciones de dependencia.
CRAMM	Organizaciones públicas y privadas.	○ Puede ser aplicado en diversos tipos de sistemas y redes de información y es útil en todas las fases del ciclo de vida de un sistema de información, desde la planificación y viabilidad hasta el desarrollo e implementación. ○ Es adecuado para su utilización siempre que sea necesario determinar los aspectos de seguridad y/o los requisitos de	○ En su modelo no tiene contemplados elementos como los procesos y los recursos

METODOLOGÍA	ÁMBITO DE APLICACIÓN	VENTAJAS	DESVENTAJAS
		contingencia para un sistema de información o red. ○ Permite la identificación y evaluación de amenazas y vulnerabilidades, la evaluación de niveles de riesgo y la identificación de los controles necesarios. ○ Incluye más de 4.000 contramedidas agrupadas en categorías y subcategorías con aspectos de seguridad similares, abarcando activos de software, hardware y protección ambiental.	
EBIOS	Es utilizada ampliamente en el sector público (en los Ministerios) y en el sector privado (pequeña y grandes empresas)	○ Facilita a las organizaciones obtener un mayor reconocimiento en sus prácticas de seguridad al ser compatible con estándares internacionales como la ISO. ○ Es una herramienta para la mediación y la resolución de algún conflicto y así misma empleada para un gran número de propósitos y	○ Se presenta más como una herramienta de soporte.

METODOLOGÍA	ÁMBITO DE APLICACIÓN	VENTAJAS	DESVENTAJAS
		procesos relacionados con la seguridad. ○ Esta herramienta de código abierto se adapta fácilmente al cumplimiento de normativas como las ISO 27001, 27005 o 31000. ○ Es una herramienta que involucra a todas las partes interesadas de la empresa, a través de diferentes aspectos como entidades, métodos de ataque, vulnerabilidades, objetivos y obligaciones para la seguridad	

Nota. Esta tabla muestra una comparativa de ventajas y desventajas sobre los diferentes métodos de análisis de riesgo. Tomado de "Metodologías Para el análisis de riesgos en los SGSI" (p. 79 -81), por H. Alemán y C. Rodríguez, 2014, UNAD.

En conclusión, cada una de las metodologías presentadas en el cuadro tienen sus ventajas y desventajas, pero la metodología que más está acorde a lo que se quiere realizar en la empresa seria la metodología MAGERIT, ya que es una de las opciones más completas para la gestión de riesgos. Esta metodología abarca desde la identificación de activos hasta la planificación de medidas preventivas, permite tener una visión detallada de los riesgos, algo que no ofrecen otras metodologías. Una de las grandes fortalezas de MAGERIT es la clasificación detallada de activos y la amplia documentación que ofrece. Esta característica permite agrupar los activos en

diferentes categorías (hardware, software, personal, servicios, entre otros), lo que facilita identificar las amenazas y sus respectivas contramedidas.

2.7 Controles de Seguridad

De acuerdo con Javier en el libro “Seguridad de la información. Redes, informática y sistemas de información”, existen dos tipos de controles que son los controles técnicos y los operacionales; los controles técnicos pueden ser preventivos y como su nombre lo indica previenen acceso no autorizados a información sensible o que personas externas puedan tomar la información de la empresa y los controles de detección están para alertar acerca de intrusiones al sistema o registros. También se tiene los controles operacionales que existen los preventivos que se los usa para tener planes de emergencia contingencia o recuperación de un desastre y los de detección que pueden ser revisiones o auditorías internas. (JAVIER, 2008b)

2.7.1 Controles de acceso

Este tipo de seguridad perimetral se centra en la identidad de los usuarios y en el control de acceso a los sistemas y recursos de la empresa. Los elementos clave que conforman a un control de acceso son la autenticación que valida la identidad del usuario, la gestión de acceso que nos muestro quien, como y cuando ingresó a un sistema, también están los perfiles y roles en donde se define los permisos y las restricciones a cada uno de los usuarios según el perfil y el rol que tengan en la empresa y por último la trazabilidad que no es otra cosa que un registro de actividades de los usuarios en la red. Por ejemplo, un sistema de control de acceso basado en roles podría permitir que los empleados del departamento de ventas accedan a la información de clientes, mientras que los empleados del departamento de finanzas solo podrían acceder a la información financiera. (Lavao, 2022)

2.7.2 Encriptación de datos

El cifrado es un proceso que convierte un mensaje en una forma codificada para que solo las personas con la clave correcta puedan leerlo. Es como escribir un mensaje en un idioma secreto que solo los iniciados pueden entender. En esta era digital, donde la información está en constante movimiento a través de redes y dispositivos, el cifrado es crucial para protegerla de accesos no autorizados, robo o manipulación. (Chávez, 2019)

Según Carlos Carvajal, 2019, El cifrado funciona mediante algoritmos matemáticos que transforman el mensaje original (texto plano) en un texto cifrado. Para descifrar el mensaje, se necesita la clave correcta, que actúa como una llave que abre la cerradura. Como ejemplos de cifrado tenemos a las contraseñas, a los pagos en línea o a las comunicaciones que se hacen por correo electrónico. (Chávez, 2019)

2.8 Políticas de Seguridad de la Información

En línea con lo que argumenta Vega Velasco, W. (2008), una política de seguridad consiste en establecer reglas y directrices para acceder a la información y los recursos. Estas políticas deben ser dinámicas y adaptarse constantemente a los cambios en el entorno empresarial. (Vega Velasco, 2008)

El propósito de las políticas de seguridad es preservar la información y los sistemas de la empresa, garantizando la integridad, confidencialidad y disponibilidad de la información. Estas políticas deben incluir procedimientos para hacer cumplir las reglas, así como las responsabilidades de cada nivel dentro de la empresa, respaldadas por el apoyo gerencial. (Vega Velasco, 2008)

2.8.1 Sistema de Gestión de Seguridad de Información (SGSI)

Coincidiendo con Miguel Porras, 2019, un Sistema de Gestión de la Seguridad de la Información (SGSI) comprende un conjunto de políticas, procedimientos, directrices, recursos y actividades coordinadas por una empresa con el fin de

salvaguardar sus activos de información. Se trata de un enfoque metódico orientado a establecer, implementar, operar, monitorear, revisar y mejorar continuamente la seguridad de la información de una entidad para alcanzar sus objetivos comerciales. Este sistema se fundamenta en una evaluación exhaustiva de los riesgos y en los niveles de tolerancia al riesgo establecidos por la organización para gestionar de manera efectiva los riesgos identificados. La identificación de los requisitos para proteger los activos de información y la aplicación de los controles adecuados para asegurar dicha protección contribuyen significativamente a la implementación exitosa de un SGSI. (*M. Porras*, 2019)

Estos principios fundamentales que van a ser enlistados a continuación dan como resultado implementación exitosa de un SGSI:

1. **Cultura de seguridad:**
    - Conciencia: Todos los miembros de la organización deben ser conscientes de la importancia de la seguridad de la información.
    - Responsabilidad: Se deben asignar responsabilidades claras para la gestión de la seguridad de la información.
    - Compromiso: La alta dirección debe comprometerse con la seguridad de la información y considerar las necesidades de las partes interesadas.
    - Valores: Se deben promover valores sociales que respalden la seguridad de la información.
2. **Enfoque basado en riesgos:**
    - Evaluación: Se deben realizar evaluaciones de riesgos para identificar y comprender las amenazas y vulnerabilidades.
    - Controles: Se deben implementar controles adecuados para mitigar los riesgos a un nivel aceptable.
3. **Seguridad integrada:**

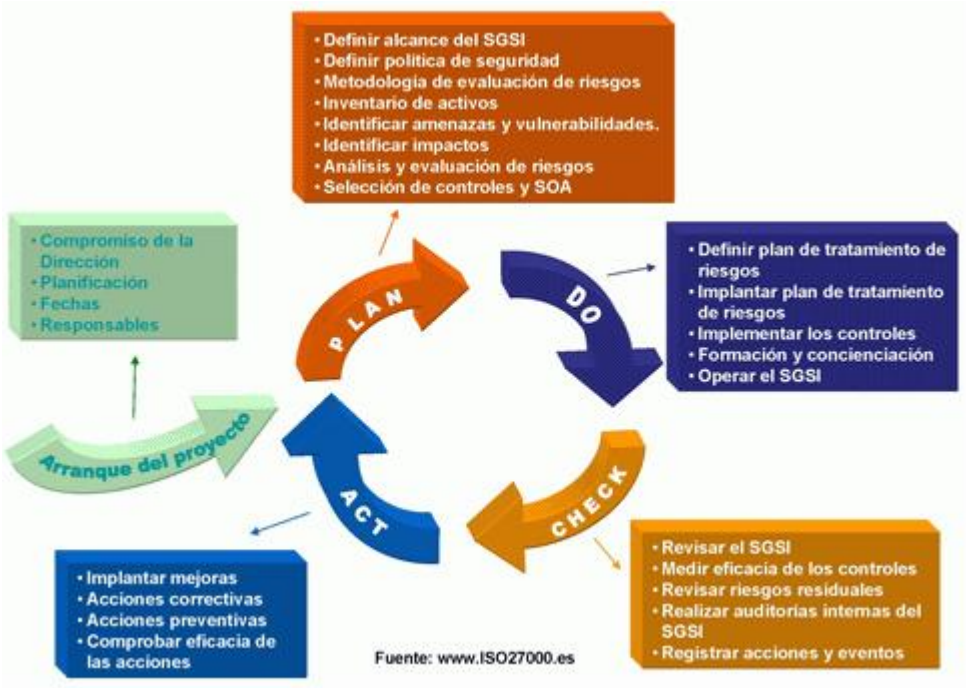
- Diseño: La seguridad debe ser un elemento fundamental en el diseño de redes y sistemas de información.

4. **Prevención y detección:**
    1. Prevención: Se deben tomar medidas para prevenir incidentes de seguridad de la información.
    2. Detección: Se deben implementar mecanismos para detectar y responder a incidentes de seguridad de la información.
5. **Enfoque integral:**
    - Gestión: La seguridad de la información debe gestionarse de forma integral, abarcando todos los aspectos de la organización.
6. **Mejora continua:**
    - Reevaluación: La seguridad de la información debe reevaluarse y mejorarse continuamente. (*M. Porras*, 2019)

2.8.2 Ciclo de mejora continua: Planear, Hacer, Verificar y Actuar

De acuerdo con la norma ISO 27001:2022, a gestión de la seguridad de la información (SGSI) recomienda el uso del ciclo de mejora continua, también conocido como PHVA o Círculo de Deming. Este ciclo permite un mejoramiento constante del SGSI mediante la evaluación y la implementación de mejoras. (A. Hurtado, 2019)

Figura 4. Ciclo Deming (2005) Mejora continua.



Nota. La figura representa los 4 estados del Ciclo Deming. Tomado de iso27000.es por Agustín & Javier, 2015

Planificación (Plan)

Coincidiendo con L. Castillo, se definen los planes y se delinea la visión de los objetivos que persigue la empresa, estableciendo dónde aspira a estar en un período determinado. Una vez que se ha fijado la meta, se procede a realizar un análisis para evaluar la situación actual, identificar las áreas que requieren mejoras y definir los problemas junto con su posible impacto en la empresa. A continuación, se desarrolla una hipótesis de solución para abordar un área específica que necesita mejoras. Se elabora un plan de acción que incluye la implementación y prueba de la solución propuesta. (Pineda, 2019)

Hacer (Do)

Se ejecuta el plan de trabajo elaborado en la etapa de "Planificación", implementando un sistema de supervisión para asegurar que se esté llevando a cabo

conforme a lo establecido. Uno de los métodos de supervisión más destacados es el uso de la gráfica de Gantt, que permite medir el progreso de las tareas y el tiempo dedicado a cada una. (Pineda, 2019)

Verificar (Check)

Durante esta fase de evaluación, se contrastan los resultados previstos con los efectivamente alcanzados, según los indicadores de rendimiento previamente establecidos, dado que lo que no se puede cuantificar no puede ser mejorado de manera sistemática. Un ejemplo ilustrativo podría ser el de un atleta que se prepara para clasificar a los Juegos Olímpicos: se le asigna competir semanalmente contra oponentes de su misma capacidad, lo que le permite verificar si realmente está mejorando su desempeño. (Pineda, 2019)

Actuar (Act)

Finalmente, con esta fase el ciclo de mejora continua termina, ya que, si al revisar los resultados se alcanza lo planificado, se registran y documentan los cambios realizados. Sin embargo, si la revisión revela que no se ha alcanzado lo deseado, es necesario actuar de manera inmediata, corregir lo planeado y establecer un nuevo plan de acción, repitiendo el ciclo de nuevo. (Pineda, 2019)

2.9 Magerit

MAGERIT es una metodología para la gestión de riesgos de las tecnologías de la información (TI) desarrollada por el gobierno español. Se basa en la norma internacional ISO 31000 y proporciona un marco para que las organizaciones tomen decisiones informadas sobre los riesgos de TI. (*Magerit Versión 3.0: Metodología de Análisis y Gestión de Riesgos de Los Sistemas de Información. Libro I: Método*, 2012)

Hay muchas aproximaciones al problema de estar analizando los riesgos que soportan los sistemas TIC como lo son guías informales, aproximaciones metódicas y herramientas de soporte, objetivar este análisis para determinar la seguridad real

de los sistemas. La complejidad del problema radica en la multitud de elementos a considerar por lo tanto un análisis riguroso es fundamental para obtener conclusiones confiables.

MAGERIT propone un enfoque metódico que elimina la improvisación y la arbitrariedad del analista. Persiguiendo los siguientes objetivos:

Directos:

1. Concienciar a los responsables sobre la existencia y la necesidad de gestionar los riesgos.
2. Ofrecer un método sistemático para analizar los riesgos de las TIC.
3. Planificar el tratamiento oportuno para mantener los riesgos bajo control.

Indirectos:

4. Preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación. (*Magerit Versión 3.0: Metodología de Análisis y Gestión de Riesgos de Los Sistemas de Información. Libro I: Método*, n.d.-a)

2.9.1 Introducción al análisis y gestión de riesgos

La seguridad se define como la capacidad de estos sistemas para resistir eventos accidentales o acciones malintencionadas que puedan afectar la disponibilidad, autenticidad, integridad y confidencialidad de la información, así como de los servicios que ofrecen. De esta forma el objetivo a proteger seria la misión de la organización, teniendo en consideración las diferentes dimensiones de seguridad. (*Magerit Versión 3.0: Metodología de Análisis y Gestión de Riesgos de Los Sistemas de Información. Libro I: Método*, n.d.-a)

Por otra parte, tenemos que el riesgo es la probabilidad de que un evento adverso afecte a los activos de una organización, es importante comprender las características de los activos y su vulnerabilidad a las amenazas para determinar el

nivel de riesgo. Un análisis de riesgo es un proceso sistemático para evaluar la magnitud de los riesgos que enfrenta una organización. Este análisis permite identificar las amenazas, estimar su probabilidad e impacto, y determinar las medidas de control necesarias. Existen diferentes estrategias para abordar el riesgo:

- Evitar: Eliminar las condiciones que generan el riesgo.
- Reducir: Disminuir la probabilidad de que el riesgo ocurra.
- Mitigar: Minimizar las consecuencias del riesgo.
- Transferir: Compartir el riesgo con otra organización, como mediante un seguro.
- Asumir: Aceptar el riesgo y tener recursos disponibles para actuar si se materializa. (*Magerit Versión 3.0: Metodología de Análisis y Gestión de Riesgos de Los Sistemas de Información. Libro I: Método*, n.d.-a)

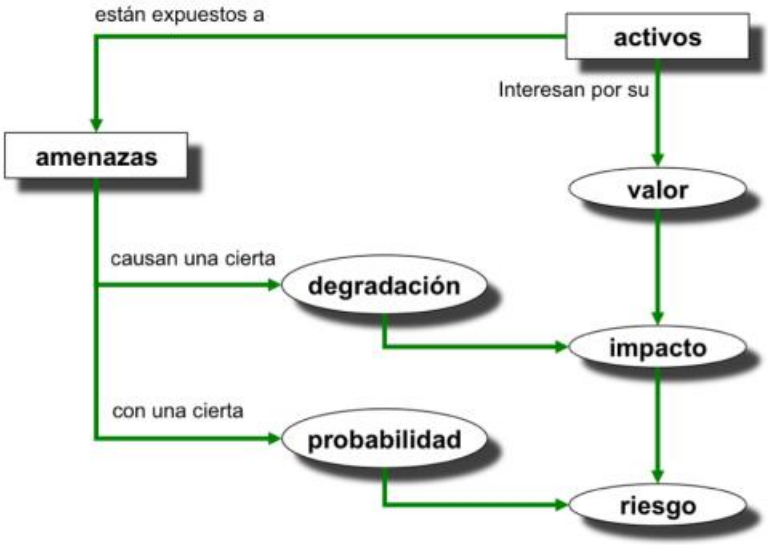
2.9.2 Método de análisis de riesgos

El análisis de riesgos es un proceso sistemático que busca determinar el nivel de riesgo asociado a los activos de una organización. Este proceso se basa en una serie de pasos:

1. Identificación de activos: Se identifican los activos relevantes para la organización, su interrelación y su valor. También se determina el perjuicio que supondría la degradación de cada activo.
2. Identificación de amenazas: Se identifican las amenazas a las que están expuestos los activos.
3. Evaluación de salvaguardas: Se evalúan las salvaguardas existentes y su eficacia para mitigar las amenazas.
4. Estimación del impacto: Se estima el impacto que pueda tener una amenaza sobre cada activo de la empresa.
5. Estimación del riesgo: Se calcula el riesgo real de un activo, esto tomando en consideración la probabilidad de ocurrencia de cada amenaza y el impacto.

6. Impacto y riesgo potenciales: Para tener una organización en la evaluación, los conceptos de impacto y riesgos se calculan como si no existiera algún tipo de control.
7. Impacto y riesgo reales: Después se introducen los controles existentes en la empresa para obtener un estimado real de cuanto fue el impacto y el riesgo. (*Magerit Versión 3.0: Metodología de Análisis y Gestión de Riesgos de Los Sistemas de Información. Libro I: Método*, n.d.-a)

Figura 5. Elementos del Análisis de riesgos potenciales.



Nota. La figura los elementos del Análisis de riesgos potenciales. Tomado de Magerit Versión 3.0: Metodología de Análisis y Gestión de Riesgos de Los Sistemas de Información. Libro I: Método, 2012.

Paso 1: Activos

(*Magerit Versión 3.0: Metodología de Análisis y Gestión de Riesgos de Los Sistemas de Información. Libro I: Método*, n.d.-a) Elemento o característica de un sistema informático que puede ser objetivo de ataques intencionados o accidentales, con implicaciones para la organización. Esto abarca: información, datos, servicios,

programas (software), dispositivos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. (UNE 71504:2008)

En un sistema de información hay 2 cosas esenciales:

- La información que maneja.
- Los servicios que presta.

Bajo esta esencia fundamental, se pueden identificar otros activos relevantes:

- Información que se manifiesta en forma de datos.
- Servicios adicionales necesarios para organizar el sistema.
- Programas informáticos (software) que facilitan la gestión de los datos.
- Dispositivos informáticos (hardware) que albergan datos, programas y servicios.
- Dispositivos de almacenamiento de datos que contienen información.
- Equipos adicionales que complementan el hardware informático.
- Redes de comunicación que posibilitan el intercambio de datos.
- Instalaciones que albergan equipos informáticos y de comunicación.
- Individuos que operan todos los elementos mencionados anteriormente.

No todos los activos son de la misma especie. Dependiendo del tipo de activo, las amenazas y las salvaguardas son diferentes.

Dependencias

Los activos esenciales en un sistema comprenden la información y los servicios ofrecidos, los cuales dependen de activos más básicos como equipos, comunicaciones, instalaciones y personal. Estos activos forman una red de dependencias, donde la seguridad de los activos superiores está vinculada a la de los activos inferiores. El concepto de dependencias entre activos es fundamental, porque esto determina como un activo se ve afectado por un incidente de seguridad.

En la mayoría de los casos, los activos están organizados por capas donde cada capa superior depende de una capa inferior. (*Magerit Versión 3.0: Metodología de Análisis y Gestión de Riesgos de Los Sistemas de Información. Libro I: Método*, n.d.-a)

Valoración

(*Magerit Versión 3.0: Metodología de Análisis y Gestión de Riesgos de Los Sistemas de Información. Libro I: Método*, n.d.-a) ¿Por qué interesa un activo? Su importancia radica en su valor, no en su costo, sino en su utilidad. Si un activo carece de valor, es prescindible. Sin embargo, si no se puede prescindir de él sin consecuencias, es porque tiene valor y, por lo tanto, debe protegerse. La valoración de los activos se realiza dependiendo a la necesidad de protección, ya que cuanto más valiosos sea un activo más alto será el nivel de seguridad. Este puede ser propio o acumulado, y en un esquema de dependencias los activos que están abajo acumulan el valor de los activos que dependen de ellos.

La información y los servicios principales son lo más valioso. En el sistema lo esencial no son los equipos, redes o dispositivos, sino la información que se está manejando y los servicios que se están ofreciendo a través de dicha información. Además, los sistemas de información utilizan datos para ofrecer servicios, tanto internos como externos, lo que implica la existencia de datos necesarios para la prestación de servicios. (*Magerit Versión 3.0: Metodología de Análisis y Gestión de Riesgos de Los Sistemas de Información. Libro I: Método*, n.d.-a)

Dimensiones

(*Magerit Versión 3.0: Metodología de Análisis y Gestión de Riesgos de Los Sistemas de Información. Libro I: Método*, n.d.-a) Se puede evaluar un activo considerando distintas dimensiones:

- Confidencialidad: ¿Cuál sería el impacto si este activo es conocido por terceras personas que no tienen acceso a esta información? Esta evaluación es importante para los datos.
- Integridad: ¿Qué consecuencias tendría si este activo estuviera dañado o corrupto? Esta evaluación es importante para los datos, que podrían estar manipulados, ser falsos total o parcialmente, o incluso estar incompletos.
- Disponibilidad: ¿Qué impacto tendría si este activo no estuviera disponible o no se pudiera utilizar? Esta evaluación es significativa para los servicios.

Paso 2: Amenazas

(*Magerit Versión 3.0: Metodología de Análisis y Gestión de Riesgos de Los Sistemas de Información. Libro I: Método*, n.d.-a) El siguiente paso implica identificar las amenazas que pueden afectar a cada activo. Las amenazas se refieren a eventos que pueden ocurrir y, de entre todas las posibilidades, nos interesa aquello que podría afectar a nuestros activos y provocar daños.

Estas amenazas pueden tener diferentes orígenes:

- Amenazas de origen natural: incluyen eventos como terremotos e inundaciones. Aunque el sistema de información es pasivo ante estos eventos, es importante considerar sus posibles consecuencias.
- Amenazas del entorno industrial: engloban desastres industriales como la contaminación y los fallos eléctricos, a pesar de que son poco comunes, es mejor tomarlos en cuenta y tener prevenciones.
- Defectos en las aplicaciones: son problemas que surgen directamente en el equipamiento debido a su diseño o implementación, con potenciales consecuencias para el sistema, a menudo se conocen como vulnerabilidades técnicas.

- Causas accidentales por parte de las personas: las personas que tienen acceso al sistema pueden ser las responsables de problemas no intencionados, debido a errores u omisiones.
- Causas deliberadas por parte de las personas: las personas con acceso al sistema de información pueden ser responsables de problemas intencionados, como ataques deliberados con el objetivo de beneficiarse indebidamente o causar daños a los legítimos propietarios.

Valoración de amenazas

(*Magerit Versión 3.0: Metodología de Análisis y Gestión de Riesgos de Los Sistemas de Información. Libro I: Método*, n.d.-a) Una vez identificada una amenaza que pueda afectar a un activo, es necesario evaluar su impacto en el valor del activo en dos aspectos: degradación y probabilidad. La degradación se refiere al daño potencial que sufriría un activo en caso de un incidente. Se expresa como una fracción del valor del activo, indicando si ha sido "totalmente degradado" o solo en una fracción. Cuando las amenazas son involuntarias, conocer la fracción afectada puede calcular la pérdida proporcional de valor. Sin embargo, en amenazas intencionales, la proporcionalidad no se aplica ya que el atacante puede causar un daño selectivo.

Por otro lado, la probabilidad de ocurrencia es más compleja de determinar y expresar. A veces se representa cualitativamente utilizando una escala nominal:

Tabla 2. Degradación del valor

Nivel de Impacto	Impacto	Probabilidad	Dificultad
MA	Muy Alta	Casi Seguro	Fácil
A	Alta	Muy Alto	Medio
M	Media	Posible	Difícil
B	Baja	Poco Probable	Muy Difícil
MB	Muy Baja	Muy Raro	Extremadamente Difícil

Nota. La figura nos muestra la degradación del valor. Tomado de Magerit Versión 3.0: Metodología de Análisis y Gestión de Riesgos de Los Sistemas de Información. Libro I: Método, 2012. (Magerit Versión 3.0: Metodología de Análisis y Gestión de Riesgos de Los Sistemas de Información. Libro I: Método, n.d.-b)

En ocasiones, se representa numéricamente como la frecuencia de eventos en un periodo determinado. Es común emplear un año como unidad de tiempo de referencia, utilizando la tasa anual de ocurrencia como indicador de la probabilidad de que un evento ocurra.

Tabla 3. Probabilidad de ocurrencia

Categoría	Valor Numérico	Frecuencia	Periodo
MA	100	Muy Frecuente	A Diario
A	10	Frecuente	Mensualmente
M	1	Normal	Una Vez Al Año
B	1/10	Poco Frecuente	Cada Varios Años
MB	1/100	Muy Poco Frecuente	Siglos

Nota. La tabla nos muestra la Probabilidad de ocurrencia. Tomado de Magerit Versión 3.0: Metodología de Análisis y Gestión de Riesgos de Los Sistemas de Información. Libro I: Método, 2012. (Magerit Versión 3.0: Metodología de Análisis y Gestión de Riesgos de Los Sistemas de Información. Libro I: Método, n.d.-b)

Determinación del impacto potencial

(*Magerit Versión 3.0: Metodología de Análisis y Gestión de Riesgos de Los Sistemas de Información. Libro I: Método*, n.d.-a) El término "impacto" se refiere a la evaluación del daño sufrido por un activo como resultado de la ocurrencia de una amenaza. Conociendo el valor de los activos en diversas dimensiones y la degradación causada

por las amenazas, es posible calcular directamente el impacto que estas tendrían en el sistema.

La única consideración que queda se refiere a las interdependencias entre los activos. Es común que el valor del sistema se centre en la información manejada y los servicios prestados, mientras que las amenazas suelen materializarse en los medios. Para establecer estas conexiones, se recurre a un grafo de dependencias

Impacto repercutido

Se refiere al cálculo del impacto sobre un activo, considerando:

- Su valor total, que incluye tanto su propio valor como el valor acumulado de los activos que dependen de él.
- Las amenazas a las que está expuesto.

El impacto acumulado se determina para cada activo, para cada amenaza y en cada dimensión de valoración, y es una función del valor total acumulado y de la degradación causada por la amenaza.

El impacto es mayor cuando el valor total propio o acumulado de un activo es mayor, así como cuando la degradación del activo atacado es mayor. El cálculo del impacto acumulado sobre los activos que sostienen el sistema de información permite identificar las medidas de seguridad necesarias para proteger los equipos, realizar copias de respaldo, entre otras acciones.

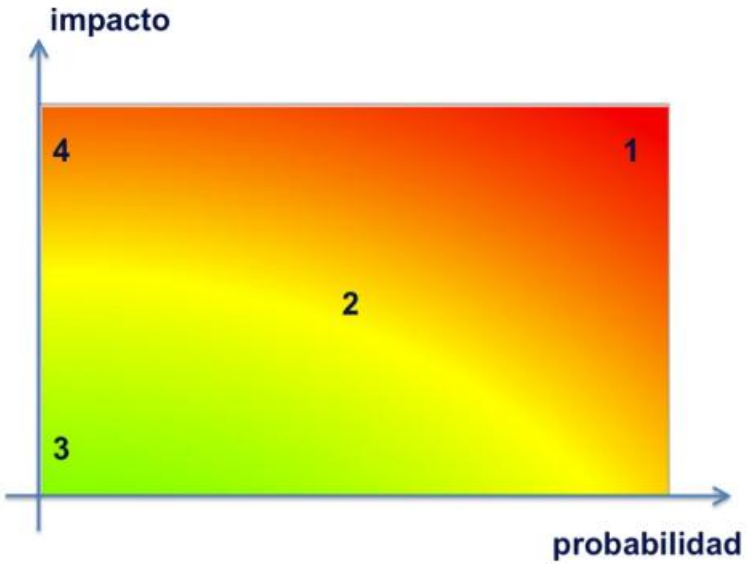
Determinación de riesgo potencial

(*Magerit Versión 3.0: Metodología de Análisis y Gestión de Riesgos de Los Sistemas de Información. Libro I: Método*, n.d.-a) El riesgo se define como la estimación del daño probable que puede ocurrir en un sistema. Al conocer el impacto que las amenazas pueden tener sobre los activos, es posible calcular el riesgo considerando también la probabilidad de que ocurran. El riesgo aumenta proporcionalmente con el

impacto y la probabilidad, lo que permite identificar diferentes niveles de riesgo que deben ser considerados en el tratamiento de este, que serán enlistados a continuación:

- Zona 1 – riesgos muy probables y de muy alto impacto
- Zona 2 – franja amarilla: cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables, pero de impacto bajo o muy bajo
- Zona 3 – riesgos improbables y de bajo impacto
- Zona 4 – riesgos improbables, pero de muy alto impacto

Figura 6. El riesgo en función del impacto y la probabilidad



Nota. La figura nos muestra el riesgo en función del impacto y la probabilidad. Tomado de Magerit Versión 3.0: Metodología de Análisis y Gestión de Riesgos de Los Sistemas de Información. Libro I: Método, 2012.

Impacto acumulado

(*Magerit Versión 3.0: Metodología de Análisis y Gestión de Riesgos de Los Sistemas de Información. Libro I: Método*, n.d.-a) El impacto acumulado se evalúa para cada activo, ante cada amenaza y en cada dimensión de valoración, siendo una función

de la suma del valor acumulado y la degradación causada. El impacto aumenta en proporción al valor propio o acumulado del activo y a la magnitud de la degradación sufrida por el activo atacado. Al calcularse sobre los activos que sustentan el sistema de información, el impacto acumulado ayuda a identificar las medidas de protección necesarias para los recursos de trabajo, como la seguridad de los equipos y la implementación de copias de respaldo, entre otros.

Impacto repercutido

(*Magerit Versión 3.0: Metodología de Análisis y Gestión de Riesgos de Los Sistemas de Información. Libro I: Método*, 2012) El impacto repercutido se evalúa para cada activo, ante cada amenaza y en cada dimensión de valoración, siendo una función del valor intrínseco y la degradación sufrida. El impacto es mayor conforme aumenta el valor intrínseco del activo y la magnitud de la degradación del activo atacado. Además, el impacto aumenta con la dependencia del activo atacado. Al calcularse sobre los activos que tienen un valor intrínseco, el impacto repercutido permite determinar las consecuencias de los incidentes técnicos en la misión del sistema de información. Se presenta como una herramienta de gestión que facilita la toma de decisiones críticas en un análisis de riesgos, como la aceptación de un cierto nivel de riesgo.

Auditoria

(*Magerit Versión 3.0: Metodología de Análisis y Gestión de Riesgos de Los Sistemas de Información. Libro I: Método*, 2012) Aunque tienen diferencias, las auditorías internas o externas a las que se someten los sistemas de información están muy presentes en este ámbito:

- En algunas ocasiones son exigidas por la ley para operar en determinados sectores (cumplimiento normativo).
- En otras ocasiones son requeridas por la Dirección de la Organización.

- También pueden ser solicitadas por entidades colaboradoras cuyo propio nivel de riesgo está vinculado al nuestro.

Las auditorías pueden utilizar un análisis de riesgos para comprender qué está en juego, a qué se enfrenta el sistema y evaluar la eficacia y eficiencia de las salvaguardas. Casi siempre, los auditores comienzan de un análisis de riesgos, ya sea que el mismo fue realizado por ellos o por terceros. Esto es muy importante ya que es complicado hacer una evaluación sin conocer el contexto de lo que ocurre en la empresa a lo que seguridad se refiere.

El resultado es un informe que destaca principalmente las deficiencias que se encontraron, revelando diferencias entre las necesidades identificadas en el análisis de riesgos y la realidad que se constató al momento de inspeccionar el sistema. Las auditorías deben realizarse periódicamente para mantener actualizado el análisis de riesgos y seguir el desarrollo del plan de seguridad determinado por las actividades de gestión de riesgos.

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

El presente proyecto de investigación emplea una metodología mixta, la cual está conformada por los enfoques cualitativa y la cuantitativa. Esta metodología mixta representa un conjunto de procesos sistemáticos, empíricos y críticos de la investigación, esto forma parte de una serie de pasos previos que se deben realizar para la correcta recolección de los datos como lo es la recolección, modelamiento y análisis de los datos cuantitativos y cualitativos. (*Carbajal*, 2019)

El enfoque cuantitativo utiliza la recolección y el análisis de los datos para contestar una o varias preguntas de investigación y probar que las hipótesis establecidas previamente se cumplen. Está fundamentada en un esquema deductivo y lógico, generaliza los resultados de los estudios mediante unas muestras que son representativas que se asocian con experimentos, encuestas de preguntas cerradas o estudios de medición estandarizados. (Vega, Ávila, Camacho, 2014)

Por otra parte, el enfoque cualitativo por lo general se basa en métodos de recolección de datos sin medición numérica como la descripción y la observación del fenómeno, este enfoque se da comúnmente en fenómenos sociales su énfasis no está en medir las variables involucradas sino en entenderlo por lo tanto no lleva un análisis estadístico. (Vega, Ávila, Camacho, 2014)

Las ventajas de la investigación multi método son la complementariedad, ampliación de la comprensión teórica, aumento gradual de la validez y ampliación de las fronteras del conocimiento, sin embargo, esta también presenta algunos obstáculos para el avance de la investigación como por ejemplo los sesgos, costos, una mayor capacitación por parte del investigador y desafíos analíticos. (Vega, Ávila, Camacho, 2014)

El tipo de investigación que se llevara a cabo para este proyecto es el de campo. Según Tevni Grajales (*Grajales*, 2000), la investigación de campo se distingue de las demás porque esta se lleva a cabo donde se desarrolla la investigación, en si es un proceso, una secuencia de acciones o comportamientos. El trabajo de campo demanda un compromiso por parte del investigador en buscar y encontrar la información necesaria que este dentro del contexto de la investigación si las condiciones son las adecuadas. (Ruano, 2007)

3.1 Población y Muestra

Según la información obtenida mediante el levantamiento de información con el presidente de la organización, hay un total de 26 empleados en total y 17 de esos 26 son asistentes de cobranzas y son quienes realizan la labor de cobro de cartera. A continuación, se detallan los cálculos realizados para la obtención de la muestra representativa de 24 asistentes de cobranzas a evaluar por medio de una encuesta.

La fórmula que se utilizó para definir el tamaño de la muestra es la siguiente:

$$n = \frac{m}{e^2 (m-1) + 1}$$

m = Tamaño de la población

e = error de estimación

n = Tamaño de la muestra

$$n = \frac{26}{(0.05)^2(26-1)+1}$$

$$n = \frac{26}{(0.0025)(25)+1}$$

$$n = \frac{26}{1.0625}$$

$$n = 24.47$$

3.2 Instrumentos de recolección de datos

Se utilizo el tipo de investigación de campo, se debe de averiguar y determinar los requerimientos esperados para la implantación de las normas ISO 27001:2022, también nos permitirá darnos cuenta de las falencias que tiene el proceso de cobranzas y el estado de conocimiento de los gestores de cobranzas sobre la seguridad de la información. Es importante conocer todas las actividades que se realizan durante el proceso de cobranzas y los puntos de vista de los empleados sobre la seguridad de la información, por estas razones se planteó utilizar estas técnicas de recolección de datos que serán detallas a continuación:

3.2.1 Entrevista

Consiste en la comunicación verbal entre las partes, el entrevistador y el entrevistado, para la obtención de los datos. Tiene que ser diseñada con anterioridad con relación al tema de estudio; Según Kerlinger (1997), la entrevista del tipo estructurada sería mejor que los cuestionarios autoadministrados para medir el comportamiento de las personas, las intenciones, emociones, actitudes y los patrones de comportamiento. (*Kerlinger-Investigacion.Pdf*, 1997)

Existen diversos tipos de entrevista, entre las cuales la que más destaca es la entrevista estructurada, en la cual el entrevistador proporciona a cada uno de los encuestados la misma serie de preguntas que fueron previamente elaboradas y el orden de las preguntas debe de mantener coherencia entre ellas. En la entrevista no estructurada hay un tiempo determinado para contestar las preguntas, el entrevistador debe tener en mente un plan para llegar a su objetivo sin tener una ruta definida sino en su lugar realizar las preguntas a medida que se obtengan respuestas de estas. Y por último en la entrevista semiestructurada se utiliza una ruta de entrevista, que consiste en una lista de preguntas y temas, ambas ordenadas para

ser tratados durante la entrevista, donde por lo general en entrevistador sigue una ruta, pero puede desviarse cuando siente que es apropiado dependiendo de las respuestas. (Quispe Parí & Sánchez Mamani, 2011)

En el proyecto se entrevistó a los altos ejecutivos de la organización quienes están a cargo de todo el personal que maneja el proceso de cobranzas. Se requería conocer como es la gestión actual, problemas, conocimientos y lo que se esperaría al momento de la implementación de las políticas de seguridad de la información. Así mismo se entrevistó al encargado del departamento de desarrollo de sistemas para conocer el alcance y a más profundidad el proceso de cobranzas y como se venía aplicando medidas en caso de algún tipo de fuga de información.

3.2.2 Encuesta

De acuerdo con el Diccionario Nueva Espasa Ilustrado (2010), es “un acopio de datos obtenidos mediante consulta, referentes a estados de opinión, costumbres, nivel económico o cualquier otro aspecto de actividad”. La encuesta tiene varios tipos como lo es la encuesta estructurada que consiste en una lista de preguntas que se formulan a todos los interesados, también está la encuesta no estructurada que permite que el encuestador modifique las preguntas en el momento de acuerdo a las respuestas que vayan dando los encuestados. La encuesta verbal es el tipo de encuesta que se utiliza la entrevista para tener una interacción verbal de sus respuestas con preguntas de opciones y por ultima esta la encuesta escrita esta consiste en un documento que con un listado de preguntas se las realiza a una población determinada. (Quispe Parí & Sánchez Mamani, 2011)

Para esta investigación, tomando en cuenta los diferentes tipos de encuestas se tomó la decisión de optar por la encuesta estructurada utilizando la herramienta de Formularios en la nube de Google la cual permitió definir un banco de preguntas cerradas para medir el nivel de conocimiento acerca de si la organización cuenta con

políticas de seguridad de la información, con la finalidad de visualizar los resultados de una forma estadística de las respuestas dadas por los involucrados en la organización.

3.3 Análisis de resultados

En la entrevista realizada al encargado de desarrollo de sistemas dio a conocer que la empresa no cuenta con políticas de seguridad escritas y dadas a conocer a los gestores, también menciono que es importante ahora más que nunca tener las políticas de seguridad de la información para que quede bien definido los procedimientos a seguir en casa de tener una brecha de información.

A continuación, se detallará las respuestas que se obtuvieron en la entrevista:

Pregunta 1: ¿Existen políticas de seguridad para la información?

Respuesta: Sí, pero solo para el control de acceso de usuarios (contraseñas y biométrico) y la seguridad física de los equipos a través de un firewall.

Las políticas son limitadas, enfocándose únicamente en el control de acceso y la seguridad física. No se mencionan políticas de clasificación de información, gestión de incidentes, auditorías internas, o administración de riesgos, esto puede indicar una falta de desarrollo integral en la seguridad de la información.

Pregunta 2: ¿Cómo se lleva a cabo el control de la seguridad de la información?

Respuesta: A través de un firewall para el control de acceso y salida de equipos de los usuarios y un sistema antivirus.

Se utilizan mecanismos básicos de seguridad (firewall y antivirus) y no se hace referencia a controles adicionales más rigurosos, esto sugiere que se haga un enfoque reactivo más que preventivo en la seguridad de la información.

Pregunta 3: ¿Podría describir el control interno informático que se ejecuta en el Departamento de Sistemas?

Respuesta: Respaldos diarios, control de acceso de usuarios al sistema, control de equipos no autorizados, control de acceso seguro y control de cambios al sistema.

Se implementan algunas medidas adecuadas como respaldos y controles de acceso, sin embargo, no se menciona un proceso formal para la realización de una auditoría o de revisiones regulares a los respaldos o a los servidores que contienen la información de toda la empresa.

Pregunta 4: ¿Está familiarizado con un Sistema de Gestión de Seguridad de la Información (SGSI)?

Respuesta: No, solo conocimiento general sobre protección de información.

La falta de familiaridad con un SGSI refleja una ausencia de un marco estructurado para la gestión de la seguridad, esto puede impactar la capacidad de la empresa para manejar riesgos de manera controlada y sistemática.

Pregunta 5: ¿Qué mecanismos, técnicas o herramientas de seguridad se emplean en los sistemas de información y comunicación?

Respuesta: Firewalls, antivirus, correos con certificados SSL y respaldos.

Las herramientas empleadas son básicas y se enfocan en medidas de protección estándar. No se va más allá para la implementación de herramientas avanzadas como sistemas de prevención de intrusos (IPS), análisis de tráfico en tiempo real, o tecnologías de inteligencia de amenazas.

Pregunta 6: ¿Se realizan actividades de control y administración de riesgos relacionados con la seguridad de la información?

Respuesta: No.

La ausencia de gestión de riesgos representa una vulnerabilidad crítica. Esto podría poner en peligro la capacidad de la organización para identificar, evaluar y mitigar amenazas.

Pregunta 7: ¿Se efectúan tareas de monitoreo en los sistemas de información y comunicación?

Respuesta: Solo en la comunicación con los enlaces externos.

El monitoreo limitado que realizan sugiere una visión reducida de las posibles amenazas internas y externas que podría enfrentar la empresa. La falta de monitoreo

integral deja brechas en la detección temprana de incidentes y que no pueda llegar a ser un incidente más grave.

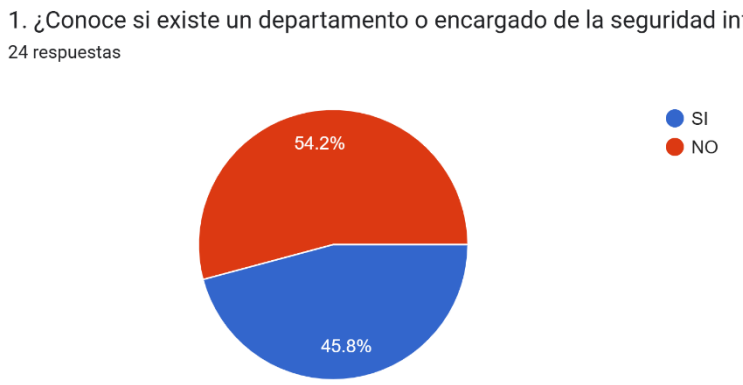
Pregunta 8: ¿Se han llevado a cabo simulacros para enfrentar caídas en los sistemas de información y comunicación?

Respuesta: No, por falta de conocimiento del personal.

La falta de simulacros indica una preparación deficiente o casi nula para el momento en que la empresa deba enfrentar incidentes críticos que afecten directamente a sus clientes. La razón de esta carencia, el "falta de conocimiento", resalta la necesidad urgente de capacitación al personal.

A continuación, se detallará los principales resultados que se obtuvieron en la encuesta, junto a su gráfico. Para una mejor observación de los resultados que se generaron a través de la encuesta.

Figura 7. Pregunta 1 de la encuesta

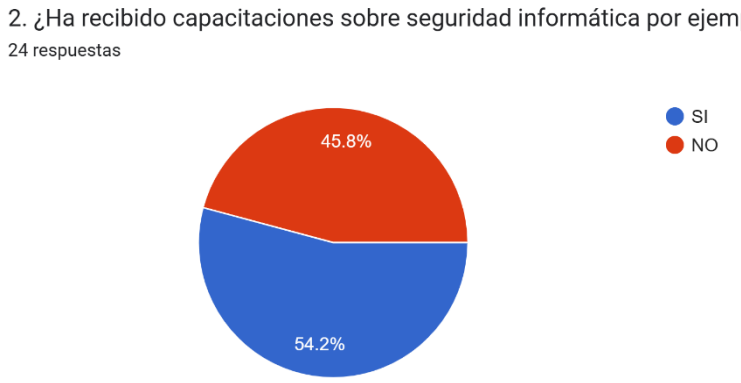


Nota. Resultados sobre el conocimiento de la existencia de un departamento encargado de la seguridad de la información en la empresa.

Existe una brecha considerable en el conocimiento de los empleados acerca de que existe un departamento o persona dedicada a la seguridad de la información. Mas de la mitad de los empleados desconoce si la empresa cuenta con un

departamento que se dedique a esta función, esto podría afectar a la percepción de responsabilidad y acciones que tienen frente a incidentes de seguridad.

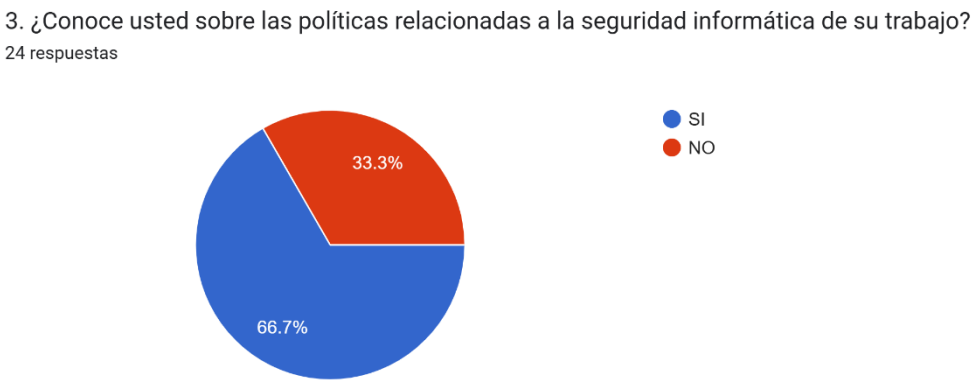
Figura 8. Pregunta 2 de la encuesta



Nota. Resultados sobre si los gestores han recibido alguna capacitación refrenté a la seguridad de la información en la empresa.

El 54.2% de los encuestados ha recibido como una presentación de seguridad de la información porque como tal la empresa no tiene controles acerca de la seguridad de la información, mientras que 45.8% casi la mitad no cuenta con este conocimiento. Esto se puede interpretar que la gran mayoría de quienes operan con información importante para la empresa no sabe cómo reaccionar en caso de algún incidente con respecto a la información.

Figura 9. Pregunta 3 de la encuesta

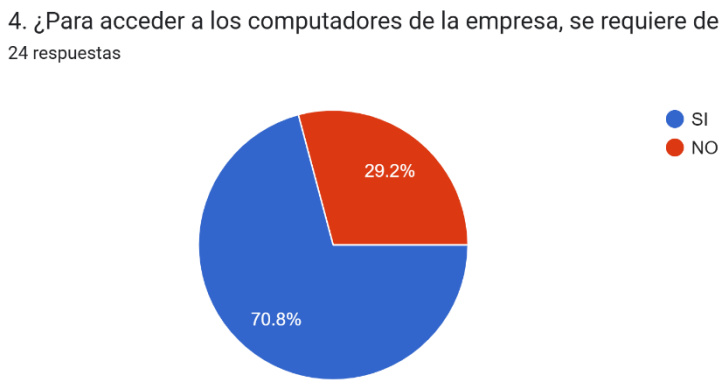


Nota. Resultados sobre si los gestores conocen sobre políticas de seguridad de la información en la empresa.

Un 66.7%, la mayoría de los empleados se familiariza con las políticas de seguridad existentes, el tercio restante no conoce nada sobre las mismas. Esto podría representar un riesgo para la empresa, porque podrían actuar sin tener en cuenta los procedimientos adecuados que ya fueron establecidos, aumentando el riesgo de que aumente los incidentes de seguridad.

Es importante reforzar la capacitación de las políticas de seguridad entre los empleados, asegurando que todos sean conscientes de su importancia y de lo que contiene.

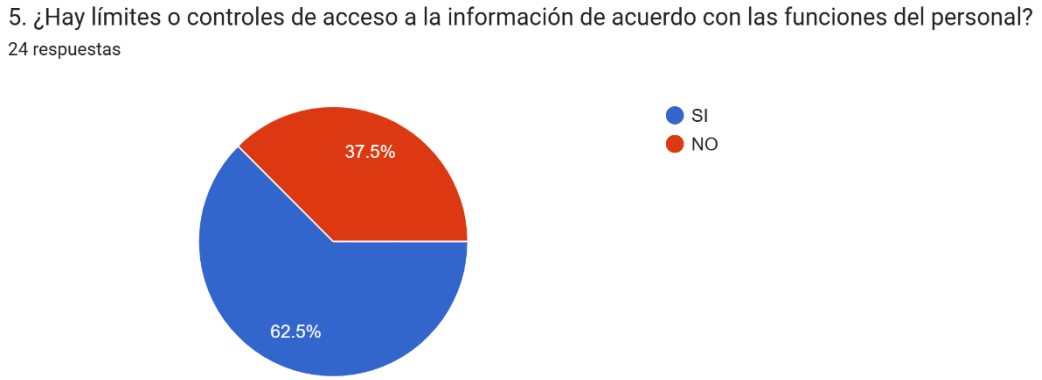
Figura 10. Pregunta 4 de la encuesta



Nota. Resultados sobre si las computadoras cuentan requieren de un usuario y clave para ingresar a las mismas.

El 70.8% indica que los equipos cuentan con autenticación mediante usuario y contraseña, por otra parte, un 29.2% casi un tercio de los encuestados señala la ausencia de este mecanismo o siente que los equipos no cuentan con un usuario y clave personal para cada empleado si no una genérica dependiendo del equipo en el este asignado. Esto podría ser una señal de inconsistencia en la implementación de medidas de seguridad, lo que pone en riesgo la integridad de los datos y sistemas.

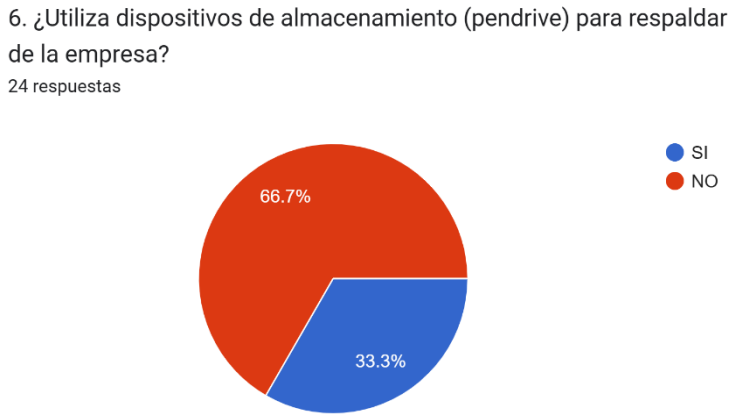
Figura 11. Pregunta 5 de la encuesta



Nota. Resultados sobre si existen controles al momento de tener acceso a cierta información dependiendo de las funciones del personal en la empresa.

Aunque 62.5% de los empleados reconoce la existencia de controles esto debido a que dependiendo del grupo de cobro al que este asignado es la información que podrá visualizar, el hecho del 37.5% de los encuestados considere que no hay restricciones puede reflejar ya que ha habido errores en donde la información se ha mezclado entre carteras, por errores en los programas auditorías y monitoreos realizando revisiones periódicas de los permisos y accesos otorgados, identificando posibles inconsistencias se puede sobrellevar este problema de una mejor manera.

Figura 12. Pregunta 6 de la encuesta

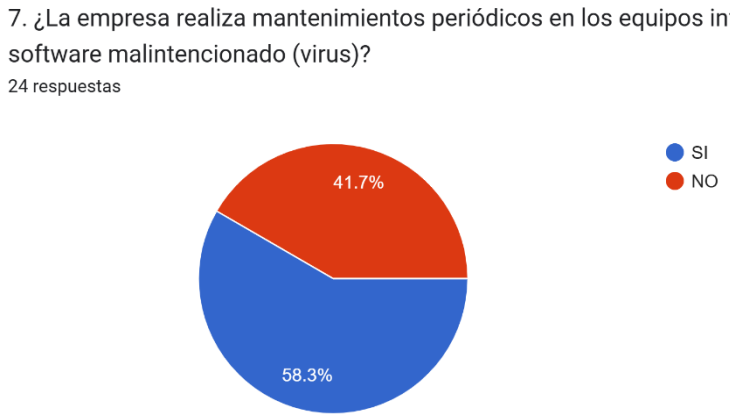


Nota. Resultados sobre si los gestores han utilizado algún tipo de dispositivo de almacenamiento para respaldar la información en la empresa.

El uso de dispositivos de almacenamiento externos como pendrives puede ser una práctica común para respaldos rápidos, pero también presenta riesgos de seguridad importantes, como la pérdida de datos, malware o accesos no autorizados. En este caso la mayoría (66.7%) de los empleados no utiliza dispositivos de almacenamiento externos, lo cual es positivo desde una perspectiva de seguridad, ya que minimiza riesgos relacionados con pérdida de dispositivos o infecciones por

malware, pero en cambio el 33.3% restante que sí utiliza dispositivos y representa un área de atención.

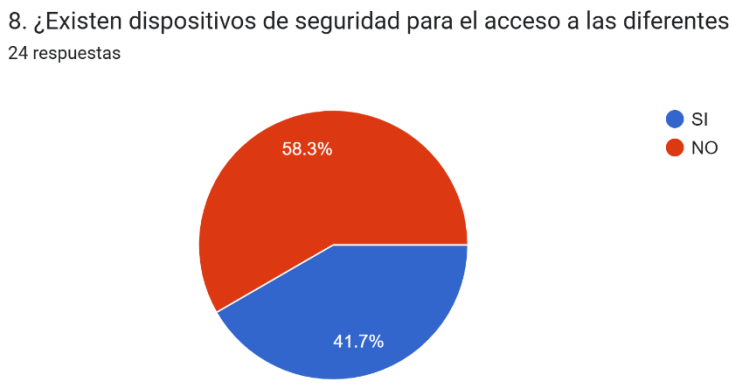
Figura 13. Pregunta 7 de la encuesta



Nota. Resultados sobre si la empresa realiza mantenimientos periódicos en los equipos para la detección de virus en la empresa.

El 58.3% de los empleados conocen que la empresa realiza los mantenimientos periódicos para la detección de algún software malintencionado. Estos mantenimientos permiten identificar y mitigar los riesgos previendo que afecten a los sistemas de la empresa, mejorando su disponibilidad y protección de los sistemas. Un 41.7% de los empleados percibe que no se realizan estos mantenimientos, esto puede deberse por falta de comunicación de los altos mandos sobre las acciones que se realizan en los mantenimientos.

Figura 14. Pregunta 8 de la encuesta



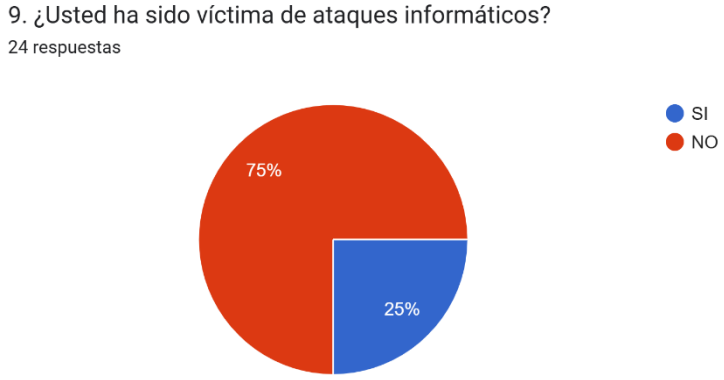
Nota. Resultados sobre si existen dispositivos para el ingreso del personal a las diferentes áreas de la empresa.

Un 41.7% de los encuestados percibe que hay equipos de seguridad en la empresa, esto nos indica que en ciertas áreas críticas de la empresa cuentan con medidas de protección específicas, en cambio en 58.3%, considera que no existen ningún dispositivo de seguridad que restrinja el acceso.

Figura 15

Pregunta 9 de la encuesta

Figura 15. Pregunta 9 de la encuesta



Nota. Resultados sobre si los gestores han víctimas de ataques informáticos en la empresa.

El 75% de los encuestados menciona no haber sido víctima de algún ataque informático, esto indica que, a pesar de no contar con medidas de seguridad robustas en la empresa, esta no ha recibido un ataque significativo como perdida de información o daños a los equipos. Por otro lado, el 25% sí ha sido víctima de ataques informáticos de algún tipo, no necesariamente significa que haya sido un ataque para robar información sino solo de virus a los equipos.

Figura 16. Pregunta 10 de la encuesta

Nota. Resultados sobre si la empresa ha sido víctima de un ataque informático.

El 75% de los encuestados no tiene conocimiento sobre incidentes de seguridad que hayan afectado a la empresa. Esto podría indicar una falta de comunicación interna acerca de los eventos relacionados con la seguridad informática. También sugiere que los ataques podrían haber sido manejados sin informar al personal general, lo cual puede ser una decisión estratégica para evitar alarmas innecesarias o por políticas de confidencialidad.

El 25% de los encuestados tiene conocimiento de ataques, lo que podría implicar que han sido eventos significativos o que afectaron directamente su trabajo, o que ciertos roles tienen mayor acceso a este tipo de información.

CAPÍTULO IV

DESARROLLO DEL PROYECTO

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

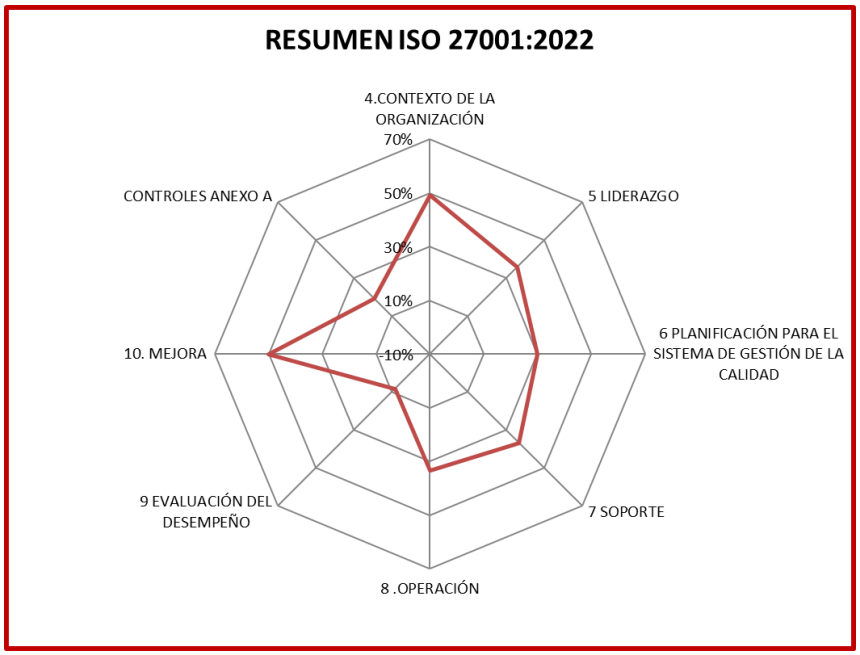
4.1.1 Elaboración de un diagnóstico de la situación actual de la seguridad de la información

Para la realización de esta actividad se llevó a cabo un análisis GAP que permitió identificar el estado actual de la empresa Novacobranzas, determinar cuáles son los controles que están vigentes y cuáles son las que faltan por mejorar en la empresa y enfocarse en las recomendaciones que da la ISO 27001:2022.

El análisis GAP se basa en el uso de una matriz que lista los controles de la norma ISO 27001:2022. En esta matriz evalúo el estado actual de los controles en la organización. El análisis GAP muestra el estado actual de la seguridad de la información antes de la realización de la implementación del SGSI, brindando una visión clara de las áreas que requieren atención y mejora.

A continuación, se presenta las gráficas de resultados del análisis de GAP realizado, como una primera vista de cómo está la empresa en cuanto a controles con respecto a la información que ellos manejan en el proceso de Gestión de Cobranzas.

Figura 17. Gráfico de la situación actual del SGSI en la empresa Novacobranzas S.A.



Nota. Resultados gráficos del análisis de GAP realizado a la empresa Novacobranzas

Como se puede observar en el gráfico, la empresa Novacobranzas S.A. ha alcanzado un avance significativo en el entendimiento del contexto organizacional, demostrando que identifica cuales son los factores internos y externos que afectan la capacidad de cumplir con los objetivos de la seguridad de la información que tiene la empresa hasta el momento. En liderazgo, se puede observar que existe un compromiso parcial de la alta dirección en la seguridad de la información de la empresa. Se han realizado acercamientos para que la alta dirección tome más involucramiento, pero no es suficiente para garantizar decisiones estratégicas.

Por otro lado, la planificación presenta algunas limitaciones, no tiene la debida importancia y no se toman de forma efectiva los riesgos que están relacionados con la seguridad de la información. La empresa debe establecer planes estratégicos más

detallados, con objetivos claros y acciones específicas que permitan mitigar de manera efectiva los riesgos identificados.

También podemos observar que los recursos asignados al SGSI, tanto humanos como tecnológicos y financieros, parecen ser insuficientes. Se puede notar que la empresa no ha capacitado de forma adecuada o socializado las políticas de seguridad de la información a los empleados, teniendo como consecuencia el desconocimiento por parte de sus empleados al momento de saber cómo tratar con un incidente en la seguridad de la información que maneja la empresa. Así mismo en términos operativos, no se pueden evidenciar procedimientos formales de las políticas y planes en acción. Esto representa una gran vulnerabilidad para la empresa, ya que la falta de operatividad puede generar un vacío en la implementación de las medidas de seguridad.

Por parte de la mejora, no se observan acciones concretas orientadas a optimizar los procesos de gestión de la seguridad. Finalmente, aunque se han implementado algunos controles del Anexo A de la norma ISO 27001:2022, su cobertura parece ser limitada. Es importante tomar en cuenta cuales de estos controles no están siendo implementados y cuál sería su impacto para la empresa, dándole prioridad a aquellos que respondan directamente a los riesgos que se tienen identificados, para garantizar una protección adecuada frente a todo tipo de amenazas.

4.1.2 Establecer el SGSI

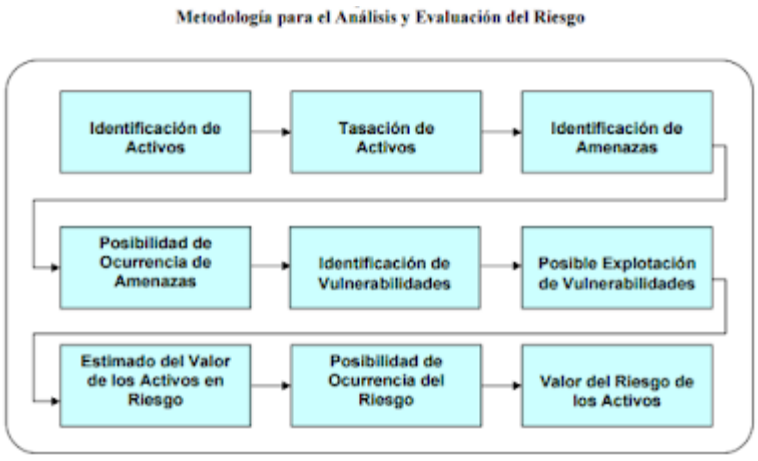
La organización debe tener en cuenta lo siguiente:

- Establecer el alcance y los límites del SGSI considerando las características del negocio, la estructura organizacional, su ubicación, los activos, la tecnología, y justificando cualquier exclusión del alcance. La determinación

de este alcance recae en la dirección de la organización, con el apoyo y asesoramiento del equipo encargado de gestionar el proyecto.

- La organización debe definir la política de seguridad de la información que será el documento que delimite los objetivos generales y el marco principal en materia de seguridad dentro de la organización. Incluirá las disposiciones que estarán en sintonía con la estrategia de gestión de riesgos y se ajustará al contexto organizacional de forma coherente. Asimismo, establecerá los parámetros para evaluar los riesgos y deberá ser aprobada por la alta dirección.
- Se debe definir un enfoque el cual va a tomar la empresa para evaluar los riesgos, se debe establecer que metodología de evaluación de riesgos se ajusta mejor al SGSI y a sus necesidades específicas de la actividad. Es recomendable utilizar un enfoque cualitativo para el cálculo del riesgo, ya que facilita la inclusión de todos los activos. La metodología implica identificar, por cada uno de los activos, sus amenazas potenciales, la probabilidad de que estas se presenten, las vulnerabilidades y su posibilidad de que estas vulnerabilidades sean utilizadas para afectar al sistema.

Figura 18. Metodología para el Análisis y Evaluación de Riesgos



Nota: Muestra la metodología utilizada para el análisis y evaluación del riesgo, detallando los pasos necesarios para identificar activos, amenazas y vulnerabilidades, así como la valoración de los riesgos asociados. Tomado de blog spot, Unknown, 2015 (https://angelwalle.blogspot.com/2015/05/25-analisis-de-riesgo-dentro-del-sgsi.html)

- Identificar los riesgos.
  - Identificación y tasación de los activos de la empresa.

    Los activos se definen como cualquier recurso con valor para la empresa que necesite de protección. EN el caso de los activos de información, como lo son los que almacenan o procesan información, por ejemplo, ficheros, base de datos, contratos, documentación del sistema, aplicaciones, software, equipos informáticos y comunicación, etc.

    El siguiente paso es tasar los activos para determinar cuáles son los activos más significativos. Para hacer esta evaluación se debe hacer la siguiente pregunta ¿Cómo impactaría la pérdida o deterioro de este activo en la disponibilidad, confidencialidad e integridad de los procesos de negocio de la empresa? Para este análisis se utilizará una escala del 1 al 5, donde el 1 representa el impacto mínimo y el 5 representa el impacto máximo. El valor del activo se calculará como el promedio entero de las puntuaciones asignadas a cada uno de estos factores: disponibilidad, confidencialidad e integridad.
  - Identificar amenazas y vulnerabilidades.

    Consiste en reconocer los eventos o agentes potenciales que pueden causar daños a los activos de una organización, así como las debilidades internas que podrían ser aprovechadas por esas amenazas. Una vez realizada la identificación y tasación de los activos, a continuación,

se debe de reconocer cuales son las amenazas y vulnerabilidades de cada uno de esos activos que afectarían a la empresa.

- Identificar impactos.

  Determina las consecuencias negativas que se derivan si una amenaza llegara a utilizar una vulnerabilidad. En este paso se evaluará como se verían afectados los activos de la empresa en términos de confidencialidad, integridad, disponibilidad, reputación o pérdidas económicas, ayudando así a la priorización de riesgos y toma de decisiones para implementar los controles correctos.

- Análisis y evaluación de los riesgos.

  Es crucial analizar el impacto que un fallo de seguridad podría generar en el negocio, evaluando las consecuencias relacionadas con la pérdida de confidencialidad, integridad o disponibilidad de los activos. Además, se debe considerar la probabilidad de que ocurra dicho fallo, basándose en las amenazas y vulnerabilidades existentes, los impactos asociados a los activos y los controles implementados. Posteriormente, se deben calcular los niveles de riesgo y determinar si estos son aceptables o necesitan ser tratados, aplicando los criterios establecidos para la aceptación de riesgos.

- Analizar y evaluar el riesgo

Es esencial analizar las repercusiones que un fallo de seguridad podría causar en la organización, particularmente en casos que impliquen la pérdida de confidencialidad, integridad o disponibilidad de un activo de información. Además, resulta necesario evaluar de forma realista la probabilidad de que dicho fallo ocurra, teniendo en cuenta las amenazas, vulnerabilidades, el impacto en los activos afectados y los controles existentes. Finalmente, este análisis permitirá calcular el nivel de riesgo correspondiente.

- Identificar y evaluar las diferentes opciones para el tratamiento de los riesgos

La identificación y evaluación de las opciones para tratar los riesgos es un paso importante para minimizar su impacto en la empresa. Las estrategias principales incluyen implementar controles efectivos que reduzcan la probabilidad o el impacto del riesgo, aceptar aquellos riesgos que cumplan con las políticas y criterios establecidos. La selección de la estrategia más apropiada debe basarse en el análisis del riesgo, los recursos disponibles y la alineación con los objetivos estratégicos de la organización.

4.1.3 Implementación de la SGSI

Alcance del SGSI

El alcance del Sistema de Gestión de Seguridad de la Información (SGSI) de Novacobranzas se centra en el proceso de cobranzas de la organización, asegurando la protección de la información relacionada con clientes, transacciones financieras, y documentación de gestión de cobros.

Áreas involucradas

- Área de Sistemas y Desarrollo: Se encarga de la administración, asignación y mantenimiento de los recursos tecnológicos de la compañía, también de realizar instalación de artefactos y de realizar la configuración. También diseñar, crear, hacer mantenimiento y dar soporte a los aplicativos de la compañía.
- Área de Cobranzas: Se encarga de gestionar y recuperar deudas pendientes. Sus principales funciones incluyen contactar a deudores, negociar planes de pago, monitorear pagos, tomar acciones legales si es necesario, y mantener registros detallados.
- Área de Financiera: Se encarga de gestionar y supervisar los recursos financieros de la empresa, asegurando la correcta asignación de fondos, el control de gastos, la planificación financiera y la evaluación de la rentabilidad de las operaciones de cobranza.

Procesos involucrados

En este caso el proceso involucrado al que se requiere la implementación de la ISO 27001:2022, el proceso de cobranzas de Novacobranzas S.A. empieza con la asignación de la cartera del cliente a los gestores, quienes inician la gestión verificando si el deudor está ubicado. Si no lo está, se realiza una investigación de referencias; si no se logra ubicar, el caso se registra para una futura visita.

Una vez ubicado, se evalúa si el deudor desea pagar. Si acepta, se concreta un acuerdo de pago. Si no, se intenta una mediación y negociación. Si esta tiene éxito, se acuerda el pago; si no, se registra para acción legal.

Paralelamente, se elabora una paleta de respuesta para apoyar las decisiones del gestor. Todo el proceso culmina con el registro de resultados e informe al cliente. Este modelo permite una gestión estructurada, priorizando la conciliación antes de recurrir a acciones legales.

Aplicativos involucrados

- El aplicativo de cobranzas NOVA: gestiona y automatiza el proceso de recuperación de deudas. Organiza las cuentas de los deudores, envía recordatorios automáticos, registra todas las interacciones, facilita la negociación de pagos, genera reportes de rendimiento y asegura el cumplimiento legal, optimizando así la eficiencia de las cobranzas.
- Zoiper: es un aplicativo de telefonía VoIP que permite realizar y recibir llamadas por medio de internet. Este aplicativo es compatible con diferentes sistemas operativos. Zoiper soporta llamadas de voz, videollamadas, mensajería y gestión de contactos, ofreciendo una solución para comunicaciones empresariales.
- VICIDIAL: es utilizado para automatizar y optimizar procesos, incluye funciones como marcación predictiva, gestión de campañas, grabación de llamadas, monitoreo en tiempo real y reportes detallados, ofreciendo una

solución completa para la gestión de centros de contacto. (*VICIdial.Com » About*, n.d.)

Metodología de riesgos

Para aplicar la metodología MAGERIT en el análisis de los riesgos de seguridad: primero, se identifican los activos de información presentes en la organización y relacionados con el alcance del análisis, y se procede a su valoración. A continuación, se identifican las amenazas que podrían afectar a cada activo y se determina la frecuencia con la que podrían ocurrir.

El uso de esta metodología es eficiente porque se enfoca en los activos más relevantes de la empresa, especialmente aquellos relacionados con la información que se maneja en el proceso de "Gestión de Cobranzas" de la empresa. Para un mejor análisis, se trabajará con agrupaciones de activos según la metodología MAGERIT, la cual está orientada a la gestión de riesgos.

Tabla 4. Tipos de activos según MAGERIT

Activos	Descripción
Instalaciones [L]	Lugar donde se encuentran los sistemas de información y comunicaciones.
Hardware [HW]	Los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización.
Software [SW]	Tareas que han sido automatizadas para su desempeño por un equipo informático.
Datos [D]	La información que permite a la organización prestar sus servicios.
Redes de comunicaciones [COM]	Son los medios de transporte que llevan datos de un sitio a otro.
Equipamiento Auxiliar [AUX]	Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con estos.
Personal [P]	Personas relacionadas con los sistemas de información.
Soportes de información [M]	Dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.

Nota. Esta tabla muestra los tipos de activos y su denominación según MAGERIT. Nota. Tomado de "MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos" (p. 25-51), por M. Ángel Amutio, J. Candau y J. Antonio Mañas, 2012, Ministerio de Hacienda y Administraciones Públicas de España

Identificación de Activos Informáticos

Tabla 5. Identificación de activos

Tipo de Activo	N°	ID	Activo
Instalaciones [L]	1	L1	Instalaciones Gerenciales
	2	L2	Instalaciones Administrativas
Hardware [HW]	3	HW1	Firewall Sophos
	4	HW2	Computadoras de Escritorio
	5	HW3	Computadoras portátiles
	6	HW4	Switch
	7	HW5	Enrutador
	8	HW6	Telefonía IP
	9	HW7	Central Telefónica
	10	HW8	Access Point
Software [SW]	11	SW1	Servidor de aplicaciones
	12	SW2	Servidor de Bases de Datos
	13	SW3	Servidor Telefonía
	14	SW4	Servidor de almacenamiento
	15	SW5	Servidor de Dominio
	16	SW6	Sistema Operativo Windows
	17	SW7	ESET Antivirus
	18	SW8	Play SMS
	19	SW9	ViciDial
	20	SW10	Microsoft Office
	21	SW11	Zoiper
	22	SW12	Anydesk
	23	SW13	Sistemas propios Novacobranzas
Datos [D]	24	D1	Bases de Datos Producción
	25	D2	Bases de Datos Clientes
	26	D3	Bases de Datos Correos empresarial
Redes de Comunicaciones [COM]	27	COM1	Acceso a internet
	28	COM2	Líneas Telefónicas
Servicios [S]	29	S1	Backups de usuarios
	30	S2	Correo electrónico empresarial

Equipamiento Auxiliar [AUX]	31	AUX1	Sistema Eléctrico General
	32	AUX2	Fibra óptica
	33	AUX3	Cableado estructurado
	34	AUX4	UPS Principal
Personal [P]	35	P1	Lideres de Cartera
	36	P2	Asistentes de Cobranzas

Nota. Esta tabla muestra los activos de la empresa Novacobranzas.

Para el correcto análisis de los riesgos asociados con los activos de información, se debe de realizar una evaluación individual teniendo en cuenta los niveles de Confidencialidad, Disponibilidad e Integridad que aseguran la protección de la información. Este proceso, clasifica dichos niveles en un rango que varía de 1 a 5, según se detalla a continuación:

Tabla 6. Clasificación de los niveles de Confidencialidad, Disponibilidad, Integridad

Impacto	Niveles (C, D, I)	Descripción
Muy bajo	**1**	La afectación es insignificante y no tiene consecuencias graves para la organización.
Bajo	**2**	La afectación es menor y afecta ligeramente las operaciones, pero puede resolverse con rapidez.
Medio	**3**	La afectación tiene un impacto moderado en los procesos de la organización y requiere intervención para resolverse.
Alto	**4**	La afectación tiene un impacto significativo en la organización, con posibles daños operativos, económicos o reputacionales importantes.
Muy alto	**5**	La afectación tiene consecuencias críticas, como interrupciones graves, pérdidas económicas mayores, daño irreparable a la reputación o incumplimiento legal.

Nota. Esta tabla muestra la clasificación de los niveles de Confidencialidad, Disponibilidad, Integridad en un rango del 1 al 5 de la empresa Novacobranzas.

Tabla 7. Identificación de riesgos

N°	Activo	Confidencialidad	Disponibilidad	Integridad	Total
1	Instalaciones Gerenciales	4	1	3	3
2	Instalaciones Administrativas	3	3	2	3
3	Firewall Sophos	3	4	4	4
4	Computadoras de Escritorio	4	3	4	4
5	Computadoras portátiles	4	3	4	4
6	Switch	3	4	3	3
7	Enrutador	3	4	3	3
8	Telefonía IP	3	4	4	4
9	Central Telefónica	4	4	4	4
10	Access Point	4	4	3	4
11	Servidor de aplicaciones	4	4	4	4
12	Servidor de Bases de Datos	4	4	4	4
13	Servidor Telefonía	4	4	3	4
14	Servidor de almacenamiento	4	3	4	4
15	Servidor de Dominio	4	4	4	4
16	Sistema Operativo Windows	4	4	3	4
17	ESET Antivirus	3	4	2	3
18	Play SMS	3	4	3	3
19	ViciDial	3	4	3	3
20	Microsoft Office	3	4	3	3
21	Zoiper	2	4	4	3
22	Anydesk	3	4	3	3
23	Sistemas propios Novacobranzas	5	5	5	5
24	Bases de Datos Producción	5	5	5	5
25	Bases de Datos Clientes	5	5	5	5
26	Bases de Datos Correos empresarial	3	3	4	3
27	Acceso a internet	5	5	4	5
28	Líneas Telefónicas	2	1	3	2
29	Backups de usuarios	2	1	2	2
30	Correo electrónico empresarial	4	5	4	4
31	Sistema Eléctrico General	3	4	4	4
32	Fibra óptica	5	5	5	5
33	Cableado estructurado	4	4	4	4
34	UPS Principal	3	5	3	4
35	Lideres de Cartera	3	3	2	3
36	Asistentes de Cobranzas	3	3	3	3

Nota. Esta tabla muestra el nivel de riesgo para cada activo de la empresa Novacobranzas.

Con base en la tabla anterior se seleccionan los activos que tienen un valor mayor o igual a 4 para realizar la evaluación de riesgos.

Tabla 8. Activos con mayor relevancia

N°	Activo	Total
1	Firewall Sophos	4
2	Computadoras de Escritorio	4
3	Computadoras portátiles	4
4	Telefonía IP	4
5	Central Telefónica	4
6	Access Point	4
7	Servidor de aplicaciones	4
8	Servidor de Bases de Datos	4
9	Servidor Telefonía	4
10	Servidor de almacenamiento	4
11	Servidor de Dominio	4
12	Sistema Operativo Windows	4
13	Sistemas propios Novacobranzas	5
14	Bases de Datos Producción	5
15	Bases de Datos Clientes	5
16	Acceso a internet	5
17	Correo electrónico empresarial	4
18	Sistema Eléctrico General	4
19	Fibra óptica	5
20	Cableado estructurado	4
21	UPS Principal	4

Nota. Esta tabla muestra los activos que tienen un valor mayor o igual a 3, por ende, tienen una mayor relevancia para la empresa Novacobranzas.

Tabla 9. Tipo de amenazas según MAGERIT

Tipo de Amenaza Descripción	ID	Amenazas
	N1	Fuego

Tipo de Amenaza Descripción	ID	Amenazas
Desastres Naturales [N]	N2	Daños por agua
	N3	Desastres Naturales
Origen Industrial [I]	I1	Fuego
	I2	Daños por agua
	I3	Desastres Industriales
	I4	Contaminación mecánica
	I5	Contaminación electromagnética
	I6	Avería de origen física o lógica
	I7	Corte eléctrico
	I8	Condiciones inadecuadas de temperatura y/o humedad
	I9	Fallo del servicio de comunicaciones
	I10	Interrupción de otros servicios y suministros esenciales
	I11	Degradación de los soportes de almacenamiento de la información
	I12	Emanaciones electromagnéticas
Errores y fallos no intencionados [E]	E1	Errores de usuarios
	E2	Errores del administrador
	E3	Errores de monitorización (log)
	E4	Errores de configuración
	E5	Deficiencias en la organización
	E6	Difusión de software dañino
	E7	Errores de [re-]encaminamiento
	E8	Errores de secuencia
	E9	Escapes de información
	E10	Alteración accidental de la información
	E11	Destrucción de información
	E12	Fugas de información
	E13	Vulnerabilidad de los programas (software)
	E14	Errores de mantenimiento / actualización de programas (software)
	E15	Errores de mantenimiento / actualización de equipos (hardware)
	E16	Caída del sistema por agotamiento de recursos
	E17	Pérdida de equipos
	E18	Indisponibilidad del personal
Ataques intencionados [A]	A1	Manipulación de los registros de actividad (log)
	A2	Manipulación de la configuración
	A3	Suplantación de la identidad del usuario
	A4	Abuso de privilegios de acceso
	A5	Uso no previsto
	A6	Difusión de software dañino

Tipo de Amenaza Descripción	ID	Amenazas
	A7	[Re-]encaminamiento de mensajes
	A8	Alteración de secuencia
	A9	Acceso no autorizado
	A10	Análisis de tráfico
	A11	Repudio
	A12	Interceptación de información (escucha)
	A13	Modificación deliberada de la información
	A14	Destrucción de información
	A15	Divulgación de información
	A16	Manipulación de programas
	A17	Manipulación de los equipos
	A18	Denegación de servicio
	A19	Robo
	A20	Ataque destructivo
	A21	Ocupación enemiga
	A22	Indisponibilidad del personal
	A23	Extorsión
	A24	Ingeniería social

Nota. Esta tabla muestra los tipos de amenazas y su descripción según MAGERIT. Tomado de "MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos" (p. 25-51), por M. Ángel Amutio, J. Candau y J. Antonio Mañas, 2012, Ministerio de Hacienda y Administraciones Públicas de España

A continuación, para evaluar la vulnerabilidad tenemos que estimar la frecuencia de ocurrencia de las amenazas en una escala de tiempo.

Tabla 10. Categorías de frecuencias de amenazas.

Vulnerabilidad	ID	Valor Frecuencia	Descripción
Extrema Frecuencia	MA	5	1 vez al día
Alta Frecuencia	A	4	1 vez cada 2 semanas

Frecuencia Media	M	3	1 vez cada 2 meses
Baja Frecuencia	B	2	1 vez cada 6 meses
Muy Baja Frecuencia	MB	1	1 vez al año o nunca

Nota. Esta tabla muestra las categorías de frecuencias de amenazas según MAGERIT que sean utilizadas para evaluar. Tomado de "MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos" (p. 25-51), por M. Ángel Amutio, J. Candau y J. Antonio Mañas, 2012, Ministerio de Hacienda y Administraciones Públicas de España

Para poder evaluar el impacto relacionado con la frecuencia de una amenaza, se utilizará la siguiente tabla como referencia para asignar un valor a quien corresponda:

Tabla 11. Valoración de impacto de una amenaza.

Impacto	ID	Valor	Probabilidad
Muy Alto	MA	5	100%
Alto	A	4	75%
Medio	M	3	50%
Bajo	B	2	20%
Muy Bajo	MB	1	5%

Nota. Esta tabla muestra la Valoración de impacto de una amenaza. Que se utilizara para evaluar el impacto en los activos de la empresa Novacobranzas. Tomado de "MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos" (p. 25-51), por M.

Ángel Amutio, J. Candau y J. Antonio Mañas, 2012, Ministerio de Hacienda y Administraciones Públicas de España

Valoración del Riesgo

El riesgo se puede interpretar como la combinación entre la probabilidad de ocurrencia de una amenaza y el impacto que esta genera. El cálculo del riesgo se calcula de la siguiente manera:

RIESGO = IMPACTO X PROBABILIDAD

Se establecen cuatro categorías de riesgo:

- **Crítico:** Se presenta con una alta frecuencia y provoca consecuencias significativas en los activos. Es fundamental realizar una evaluación y aplicar controles adecuados para mitigarlo.
- **Alto:** Ocurre con cierta frecuencia, las afectaciones son moderadas, o bien, su frecuencia es baja, pero el impacto es considerable.
- **Medio:** Se presenta de forma ocasional y produce un impacto moderado, se debe de realizar una evaluación para decidir qué medidas se debe tomar.
- **Bajo:** Se da con poca frecuencia y las afectaciones a los activos son mínimas. Es recomendable documentarlo en una bitácora para su monitoreo.

Tabla 12. Nivel de riesgo

Impacto	Valor	Color
Crítico	10	
Alto	7-9	
Medio	4-6	
Bajo	1-3	

Nota. Esta tabla muestra el nivel de riesgo que se tomara para el análisis y la evaluación.

La siguiente tabla muestra el análisis y evaluación de los riesgos realizado para la empresa Novacobranzas. En ella se detalla, para cada amenaza que afecta un activo, un análisis de la frecuencia con la que podría presentarse, junto con su impacto en las distintas dimensiones de seguridad del activo.

Tabla 13. Análisis y Evaluación del riesgo

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
Firewall Sophos (HW1)	Desastres Naturales (N3)		4		1	1	1	Bajo
	Fuego (I1)		4		2	1	3	Bajo
	Daños por agua (I2)		4		1	1	1	Bajo
	Desastres Industriales (I3)		4		1	1	1	Bajo
	Contaminación mecánica (I4)		4		3	1	4	Medio
	Avería de origen física o lógica (I6)		4		2	1	3	Bajo
	Corte eléctrico (I7)		4		2	1	3	Bajo
	Condiciones inadecuadas de temperatura y/o humedad (I8)		4		2	1	3	Bajo
	Errores del administrador (E2)	3	4	4	2	4	7	Alto
	Errores de mantenimiento / actualización de equipos (hardware) (E14)		4		1	1	1	Bajo
	Caída del sistema por agotamiento de recursos (E15)		4		1	1	1	Bajo

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
	Pérdida de equipos (E16)	3	4		1	2	2	Bajo
	Abuso de privilegios de acceso (A4)	3	4	4	1	4	4	Medio
	Uso no previsto (A5)	3	4	4	1	4	4	Medio
	Acceso no autorizado (A9)	3		4	1	2	2	Bajo
	Manipulación de los equipos (A17)	3	4		2	2	5	Medio
	Denegación de servicio (A18)		4		3	1	4	Medio
	Robo (A19)	3	4		1	2	2	Bajo
Computadoras de Escritorio (HW2)	Desastres Naturales (N3)		3		1	1	1	Bajo
	Fuego (I1)		3		2	1	2	Bajo
	Daños por agua (I2)		3		2	1	2	Bajo
	Desastres Industriales (I3)		3		1	1	1	Bajo
	Contaminación mecánica (I4)		3		3	1	3	Bajo
	Avería de origen física o lógica (I6)		3		2	1	2	Bajo
	Corte eléctrico (I7)		3		2	1	2	Bajo

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
	Condiciones inadecuadas de temperatura y/o humedad (I8)		3		2	1	2	Bajo
	Errores del administrador (E2)	3	3	2	2	3	5	Medio
	Errores de mantenimiento / actualización de equipos (hardware) (E14)		3		4	1	4	Medio
	Caída del sistema por agotamiento de recursos (E15)		3		3	1	3	Bajo
	Pérdida de equipos (E16)	3	3		1	2	2	Bajo
	Abuso de privilegios de acceso (A4)	3	3	2	3	3	8	Alto
	Uso no previsto (A5)	3	3	2	4	3	10	Critico
	Acceso no autorizado (A9)	3		2	3	2	5	Medio
	Manipulación de los equipos (A17)	3	3		2	2	4	Medio
	Denegación de servicio (A18)		3		3	1	3	Bajo
	Robo (A19)	3	3		1	2	2	Bajo
	Desastres Naturales (N3)		3		1	1	1	Bajo

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
Computadoras portátiles (HW3)	Fuego (I1)		3		2	1	2	Bajo
	Daños por agua (I2)		3		2	1	2	Bajo
	Desastres Industriales (I3)		3		1	1	1	Bajo
	Contaminación mecánica (I4)		3		3	1	3	Bajo
	Avería de origen física o lógica (I6)		3		2	1	2	Bajo
	Corte eléctrico (I7)		3		2	1	2	Bajo
	Condiciones inadecuadas de temperatura y/o humedad (I8)		3		2	1	2	Bajo
	Errores del administrador (E2)	3	3	2	2	3	5	Medio
	Errores de mantenimiento / actualización de equipos (hardware) (E14)		3		4	1	4	Medio
	Caída del sistema por agotamiento de recursos (E15)		3		3	1	3	Bajo
	Pérdida de equipos (E16)	3	3		1	2	2	Bajo
	Abuso de privilegios de acceso (A4)	3	3	2	3	3	8	Alto

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
	Uso no previsto (A5)	3	3	2	4	3	10	Critico
	Acceso no autorizado (A9)	3		2	3	2	5	Medio
	Manipulación de los equipos (A17)	3	3		2	2	4	Medio
	Denegación de servicio (A18)		3		3	1	3	Bajo
	Robo (A19)	3	3		1	2	2	Bajo
Telefonía IP (HW12)	Desastres Naturales (N3)		4		1	1	1	Bajo
	Fuego (I1)		4		2	1	3	Bajo
	Daños por agua (I2)		4		1	1	1	Bajo
	Desastres Industriales (I3)		4		1	1	1	Bajo
	Contaminación mecánica (I4)		4		3	1	4	Medio
	Avería de origen física o lógica (I6)		4		3	1	4	Medio
	Corte eléctrico (I7)		4		2	1	3	Bajo
	Condiciones inadecuadas de temperatura y/o humedad (I8)		4		2	1	3	Bajo
	Errores del administrador (E2)	3	4	4	3	4	10	Critico

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
	Errores de mantenimiento / actualización de equipos (hardware) (E14)		4		2	1	3	Bajo
	Caída del sistema por agotamiento de recursos (E15)		4		3	1	4	Medio
	Pérdida de equipos (E16)	3	4		1	2	2	Bajo
	Abuso de privilegios de acceso (A4)	3	4	4	1	4	4	Medio
	Uso no previsto (A5)	3	4	4	2	4	7	Alto
	Acceso no autorizado (A9)	3		4	2	2	5	Medio
	Manipulación de los equipos (A17)	3	4		2	2	5	Medio
	Denegación de servicio (A18)		4		3	1	4	Medio
	Robo (A19)	3	4		1	2	2	Bajo
Central Telefónica (HW13)	Desastres Naturales (N3)		4		1	1	1	Bajo
	Fuego (I1)		4		2	1	3	Bajo
	Daños por agua (I2)		4		1	1	1	Bajo

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
	Desastres Industriales (I3)		4		1	1	1	Bajo
	Contaminación mecánica (I4)		4		3	1	4	Medio
	Avería de origen física o lógica (I6)		4		3	1	4	Medio
	Corte eléctrico (I7)		4		2	1	3	Bajo
	Condiciones inadecuadas de temperatura y/o humedad (I8)		4		2	1	3	Bajo
	Errores del administrador (E2)	4	4	4	3	4	10	Critico
	Errores de mantenimiento / actualización de equipos (hardware) (E14)		4		1	1	1	Bajo
	Caída del sistema por agotamiento de recursos (E15)		4		1	1	1	Bajo
	Pérdida de equipos (E16)	4	4		1	3	3	Bajo
	Abuso de privilegios de acceso (A4)	4	4	4	1	4	4	Medio
	Uso no previsto (A5)	4	4	4	2	4	8	Alto
	Acceso no autorizado (A9)	4		4	1	3	3	Bajo

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
	Manipulación de los equipos (A17)	4	4		2	3	5	Medio
	Denegación de servicio (A18)		4		3	1	4	Medio
	Robo (A19)	4	4		1	3	3	Bajo
Access Point (HW14)	Desastres Naturales (N3)		4		1	1	1	Bajo
	Fuego (I1)		4		2	1	3	Bajo
	Daños por agua (I2)		4		1	1	1	Bajo
	Desastres Industriales (I3)		4		1	1	1	Bajo
	Contaminación mecánica (I4)		4		3	1	4	Medio
	Avería de origen física o lógica (I6)		4		2	1	3	Bajo
	Corte eléctrico (I7)		4		2	1	3	Bajo
	Condiciones inadecuadas de temperatura y/o humedad (I8)		4		2	1	3	Bajo
	Errores del administrador (E2)	4	4	3	2	4	7	Alto

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
	Errores de mantenimiento / actualización de equipos (hardware) (E14)		4		2	1	3	Bajo
	Caída del sistema por agotamiento de recursos (E15)		4		1	1	1	Bajo
	Pérdida de equipos (E16)	4	4		1	3	3	Bajo
	Abuso de privilegios de acceso (A4)	4	4	3	1	4	4	Medio
	Uso no previsto (A5)	4	4	3	1	4	4	Medio
	Acceso no autorizado (A9)	4		3	3	2	7	Alto
	Manipulación de los equipos (A17)	4	4		2	3	5	Medio
	Denegación de servicio (A18)		4		3	1	4	Medio
	Robo (A19)	4	4		1	3	3	Bajo
Servidor de aplicaciones (SW1)	Avería de origen física o lógica (I6)		4		1	1	1	Bajo
	Errores de usuarios (E1)	4	4	4	2	4	8	Alto
	Errores del administrador (E2)	4	4	4	1	4	4	Medio

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
	Difusión de software dañino (E6)	4	4	4	1	4	4	Medio
	Errores de [re-]encaminamiento (E7)	4			1	1	1	Bajo
	Errores de secuencia (E8)			4	1	1	1	Bajo
	Alteración accidental de la información (E9)			4	1	1	1	Bajo
	Destrucción de información (E10)		4		1	1	1	Bajo
	Fugas de información (E11)	4			1	1	1	Bajo
	Vulnerabilidad de los programas (software) (E12)	4	4	4	1	4	4	Medio
	Errores de mantenimiento / actualización de programas (software) (E13)		4	4	1	3	3	Bajo
	Suplantación de la identidad del usuario (A3)	4		4	1	3	3	Bajo
	Abuso de privilegios de acceso (A4)	4	4	4	2	4	8	Alto
	Uso no previsto (A5)	4	4	4	1	4	4	Medio

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
	Difusión de software dañino (A6)	4	4	4	1	4	4	Medio
	[Re-]encaminamiento de mensajes (A7)	4			1	1	1	Bajo
	Alteración de secuencia (A8)			4	1	1	1	Bajo
	Acceso no autorizado (A9)	4		4	2	3	5	Medio
	Modificación deliberada de la información (A13)			4	1	1	1	Bajo
	Destrucción de información (A14)		4		1	1	1	Bajo
	Divulgación de información (A15)	4			1	1	1	Bajo
	Manipulación de programas (A16)	4	4	4	1	4	4	Medio
Servidor de Bases de Datos (SW2)	Avería de origen física o lógica (I6)		4		2	1	3	Bajo
	Errores de usuarios (E1)	4	4	4	3	4	10	Critico
	Errores del administrador (E2)	4	4	4	2	4	8	Alto
	Difusión de software dañino (E6)	4	4	4	1	4	4	Medio

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
	Errores de [re-]encaminamiento (E7)	4			3	1	4	Medio
	Errores de secuencia (E8)			4	1	1	1	Bajo
	Alteración accidental de la información (E9)			4	3	1	4	Medio
	Destrucción de información (E10)		4		2	1	3	Bajo
	Fugas de información (E11)	4			1	1	1	Bajo
	Vulnerabilidad de los programas (software) (E12)	4	4	4	1	4	4	Medio
	Errores de mantenimiento / actualización de programas (software) (E13)		4	4	1	3	3	Bajo
	Suplantación de la identidad del usuario (A3)	4		4	1	3	3	Bajo
	Abuso de privilegios de acceso (A4)	4	4	4	2	4	8	Alto
	Uso no previsto (A5)	4	4	4	2	4	8	Alto
	Difusión de software dañino (A6)	4	4	4	1	4	4	Medio

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
	[Re-]encaminamiento de mensajes (A7)	4			2	1	3	Bajo
	Alteración de secuencia (A8)			4	1	1	1	Bajo
	Acceso no autorizado (A9)	4		4	2	3	5	Medio
	Modificación deliberada de la información (A13)			4	1	1	1	Bajo
	Destrucción de información (A14)		4		1	1	1	Bajo
	Divulgación de información (A15)	4			1	1	1	Bajo
	Manipulación de programas (A16)	4	4	4	1	4	4	Medio
Servidor Telefonía (SW3)	Avería de origen física o lógica (I6)		4		3	1	4	Medio
	Errores de usuarios (E1)	4	4	3	3	4	10	Critico
	Errores del administrador (E2)	4	4	3	2	4	7	Alto
	Difusión de software dañino (E6)	4	4	3	1	4	4	Medio

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
	Errores de [re-]encaminamiento (E7)	4			3	1	4	Medio
	Errores de secuencia (E8)			3	2	1	2	Bajo
	Alteración accidental de la información (E9)			3	1	1	1	Bajo
	Destrucción de información (E10)		4		1	1	1	Bajo
	Fugas de información (E11)	4			1	1	1	Bajo
	Vulnerabilidad de los programas (software) (E12)	4	4	3	1	4	4	Medio
	Errores de mantenimiento / actualización de programas (software) (E13)		4	3	1	2	2	Bajo
	Suplantación de la identidad del usuario (A3)	4		3	1	2	2	Bajo
	Abuso de privilegios de acceso (A4)	4	4	3	2	4	7	Alto
	Uso no previsto (A5)	4	4	3	2	4	7	Alto
	Difusión de software dañino (A6)	4	4	3	1	4	4	Medio

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
	[Re-]encaminamiento de mensajes (A7)	4			1	1	1	Bajo
	Alteración de secuencia (A8)			3	1	1	1	Bajo
	Acceso no autorizado (A9)	4		3	2	2	5	Medio
	Modificación deliberada de la información (A13)			3	1	1	1	Bajo
	Destrucción de información (A14)		4		1	1	1	Bajo
	Divulgación de información (A15)	4			1	1	1	Bajo
	Manipulación de programas (A16)	4	4	3	1	4	4	Medio
Servidor de almacenamiento (SW4)	Avería de origen física o lógica (I6)		3		2	1	2	Bajo
	Errores de usuarios (E1)	4	3	4	2	4	7	Alto
	Errores del administrador (E2)	4	3	4	2	4	7	Alto
	Difusión de software dañino (E6)	4	3	4	1	4	4	Medio

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
	Errores de [re-]encaminamiento (E7)	4			1	1	1	Bajo
	Errores de secuencia (E8)			4	1	1	1	Bajo
	Alteración accidental de la información (E9)			4	2	1	3	Bajo
	Destrucción de información (E10)		3		1	1	1	Bajo
	Fugas de información (E11)	4			1	1	1	Bajo
	Vulnerabilidad de los programas (software) (E12)	4	3	4	1	4	4	Medio
	Errores de mantenimiento / actualización de programas (software) (E13)		3	4	1	2	2	Bajo
	Suplantación de la identidad del usuario (A3)	4		4	1	3	3	Bajo
	Abuso de privilegios de acceso (A4)	4	3	4	2	4	7	Alto
	Uso no previsto (A5)	4	3	4	3	4	10	Critico
	Difusión de software dañino (A6)	4	3	4	1	4	4	Medio

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
	[Re-]encaminamiento de mensajes (A7)	4			1	1	1	Bajo
	Alteración de secuencia (A8)			4	1	1	1	Bajo
	Acceso no autorizado (A9)	4		4	2	3	5	Medio
	Modificación deliberada de la información (A13)			4	1	1	1	Bajo
	Destrucción de información (A14)		3		1	1	1	Bajo
	Divulgación de información (A15)	4			1	1	1	Bajo
	Manipulación de programas (A16)	4	3	4	1	4	4	Medio
Servidor de Dominio (SW5)	Avería de origen física o lógica (I6)		4		3	1	4	Medio
	Errores de usuarios (E1)	4	4	4	3	4	10	Critico
	Errores del administrador (E2)	4	4	4	2	4	8	Alto
	Difusión de software dañino (E6)	4	4	4	1	4	4	Medio

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
	Errores de [re-]encaminamiento (E7)	4			1	1	1	Bajo
	Errores de secuencia (E8)			4	1	1	1	Bajo
	Alteración accidental de la información (E9)			4	2	1	3	Bajo
	Destrucción de información (E10)		4		1	1	1	Bajo
	Fugas de información (E11)	4			1	1	1	Bajo
	Vulnerabilidad de los programas (software) (E12)	4	4	4	1	4	4	Medio
	Errores de mantenimiento / actualización de programas (software) (E13)		4	4	1	3	3	Bajo
	Suplantación de la identidad del usuario (A3)	4		4	1	3	3	Bajo
	Abuso de privilegios de acceso (A4)	4	4	4	2	4	8	Alto
	Uso no previsto (A5)	4	4	4	1	4	4	Medio
	Difusión de software dañino (A6)	4	4	4	1	4	4	Medio

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
	[Re-]encaminamiento de mensajes (A7)	4			2	1	3	Bajo
	Alteración de secuencia (A8)			4	1	1	1	Bajo
	Acceso no autorizado (A9)	4		4	2	3	5	Medio
	Modificación deliberada de la información (A13)			4	1	1	1	Bajo
	Destrucción de información (A14)		4		1	1	1	Bajo
	Divulgación de información (A15)	4			1	1	1	Bajo
	Manipulación de programas (A16)	4	4	4	1	4	4	Medio
Sistema Operativo Windows (SW7)	Avería de origen física o lógica (I6)		4		2	1	3	Bajo
	Errores de usuarios (E1)	4	4	3	2	4	7	Alto
	Errores del administrador (E2)	4	4	3	1	4	4	Medio
	Difusión de software dañino (E6)	4	4	3	3	4	10	Critico

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
	Errores de [re-]encaminamiento (E7)	4			1	1	1	Bajo
	Errores de secuencia (E8)			3	1	1	1	Bajo
	Alteración accidental de la información (E9)			3	2	1	2	Bajo
	Destrucción de información (E10)		4		1	1	1	Bajo
	Fugas de información (E11)	4			3	1	4	Medio
	Vulnerabilidad de los programas (software) (E12)	4	4	3	1	4	4	Medio
	Errores de mantenimiento / actualización de programas (software) (E13)		4	3	2	2	5	Medio
	Suplantación de la identidad del usuario (A3)	4		3	3	2	7	Alto
	Abuso de privilegios de acceso (A4)	4	4	3	3	4	10	Critico
	Uso no previsto (A5)	4	4	3	4	4	10	Critico
	Difusión de software dañino (A6)	4	4	3	1	4	4	Medio

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
	[Re-]encaminamiento de mensajes (A7)	4			3	1	4	Medio
	Alteración de secuencia (A8)			3	1	1	1	Bajo
	Acceso no autorizado (A9)	4		3	4	2	9	Alto
	Modificación deliberada de la información (A13)			3	1	1	1	Bajo
	Destrucción de información (A14)		4		1	1	1	Bajo
	Divulgación de información (A15)	4			1	1	1	Bajo
	Manipulación de programas (A16)	4	4	3	1	4	4	Medio
Sistemas propios Novacobranzas (SW16)	Avería de origen física o lógica (I6)		5		3	2	5	Medio
	Errores de usuarios (E1)	5	5	5	4	5	10	Critico
	Errores del administrador (E2)	5	5	5	4	5	10	Critico
	Difusión de software dañino (E6)	5	5	5	1	5	5	Medio

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
	Errores de [re-]encaminamiento (E7)	5			3	2	5	Medio
	Errores de secuencia (E8)			5	1	2	2	Bajo
	Alteración accidental de la información (E9)			5	4	2	7	Alto
	Destrucción de información (E10)		5		3	2	5	Medio
	Fugas de información (E11)	5			1	2	2	Bajo
	Vulnerabilidad de los programas (software) (E12)	5	5	5	4	5	10	Critico
	Errores de mantenimiento / actualización de programas (software) (E13)		5	5	4	3	10	Critico
	Suplantación de la identidad del usuario (A3)	5		5	1	3	3	Bajo
	Abuso de privilegios de acceso (A4)	5	5	5	3	5	10	Critico
	Uso no previsto (A5)	5	5	5	1	5	5	Medio
	Difusión de software dañino (A6)	5	5	5	1	5	5	Medio

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
	[Re-]encaminamiento de mensajes (A7)	5			4	2	7	Alto
	Alteración de secuencia (A8)			5	1	2	2	Bajo
	Acceso no autorizado (A9)	5		5	3	3	10	Critico
	Modificación deliberada de la información (A13)			5	1	2	2	Bajo
	Destrucción de información (A14)		5		1	2	2	Bajo
	Divulgación de información (A15)	5			1	2	2	Bajo
	Manipulación de programas (A16)	5	5	5	1	5	5	Medio
Bases de Datos Producción (D2)	Errores de usuarios (E1)	5	5	5	4	5	10	Critico
	Errores del administrador (E2)	5	5	5	4	5	10	Critico
	Errores de monitorización (log) (E3)			5	4	2	7	Alto
	Errores de configuración (E4)			5	4	2	7	Alto

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
	Alteración accidental de la información (E9)			5	3	2	5	Medio
	Destrucción de información (E10)		5		3	2	5	Medio
	Fugas de información (E11)	5			1	2	2	Bajo
	Manipulación de los registros de actividad (log) (A1)			5	1	2	2	Bajo
	Manipulación de la configuración (A2)	5	5	5	2	5	10	Critico
	Suplantación de la identidad del usuario (A3)	5		5	1	3	3	Bajo
	Abuso de privilegios de acceso (A4)	5	5	5	2	5	10	Critico
	Acceso no autorizado (A9)	5		5	1	3	3	Bajo
	Modificación deliberada de la información (A13)			5	1	2	2	Bajo
	Destrucción de información (A14)		5		1	2	2	Bajo

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
	Divulgación de información (A15)	5			2	2	3	Bajo
Bases de Datos Clientes (D3)	Errores de usuarios (E1)	5	5	5	4	5	10	Critico
	Errores del administrador (E2)	5	5	5	4	5	10	Critico
	Errores de monitorización (log) (E3)			5	4	2	7	Alto
	Errores de configuración (E4)			5	4	2	7	Alto
	Alteración accidental de la información (E9)			5	3	2	5	Medio
	Destrucción de información (E10)		5		3	2	5	Medio
	Fugas de información (E11)	5			1	2	2	Bajo
	Manipulación de los registros de actividad (log) (A1)			5	1	2	2	Bajo
	Manipulación de la configuración (A2)	5	5	5	2	5	10	Critico
	Suplantación de la identidad del usuario (A3)	5		5	1	3	3	Bajo

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
	Abuso de privilegios de acceso (A4)	5	5	5	2	5	10	Critico
	Acceso no autorizado (A9)	5		5	1	3	3	Bajo
	Modificación deliberada de la información (A13)			5	1	2	2	Bajo
	Destrucción de información (A14)		5		1	2	2	Bajo
	Divulgación de información (A15)	5			2	2	3	Bajo
Acceso a internet (COM1)	Fallo del servicio de comunicaciones (I9)		5		3	2	5	Medio
	Errores del administrador (E2)	5	5	4	1	5	5	Medio
	Errores de [re-]encaminamiento (E7)	5			4	2	7	Alto
	Errores de secuencia (E8)			4	1	1	1	Bajo
	Alteración accidental de la información (E9)			4	1	1	1	Bajo
	Destrucción de información (E10)		5		1	2	2	Bajo

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
	Fugas de información (E11)	5			1	2	2	Bajo
	Caída del sistema por agotamiento de recursos (E15)		5		2	2	3	Bajo
	Suplantación de la identidad del usuario (A3)	5		4	1	3	3	Bajo
	Abuso de privilegios de acceso (A4)	5	5	4	4	5	10	Critico
	Uso no previsto (A5)	5	5	4	4	5	10	Critico
	[Re-]encaminamiento de mensajes (A7)	5			2	2	3	Bajo
	Alteración de secuencia (A8)			4	1	1	1	Bajo
	Acceso no autorizado (A9)	5		4	1	3	3	Bajo
	Análisis de tráfico (A10)	5			1	2	2	Bajo
	Modificación deliberada de la información (A13)			4	1	1	1	Bajo
	Divulgación de información (A15)	5			1	2	2	Bajo
	Denegación de servicio (A18)		5		3	2	5	Medio

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
Correo electrónico empresarial (S3)	Errores de usuarios (E1)	4	5	4	1	4	4	Medio
	Errores del administrador (E2)	4	5	4	2	4	9	Alto
	Errores de [re-]encaminamiento (E7)	4			5	1	7	Alto
	Errores de secuencia (E8)			4	4	1	5	Medio
	Destrucción de información (E10)		5		1	2	2	Bajo
	Fugas de información (E11)	4			1	1	1	Bajo
	Caída del sistema por agotamiento de recursos (E15)		5		4	2	7	Alto
	Suplantación de la identidad del usuario (A3)	4		4	1	3	3	Bajo
	Abuso de privilegios de acceso (A4)	4	5	4	2	4	9	Alto
	Uso no previsto (A5)	4	5	4	3	4	10	Critico
	[Re-]encaminamiento de mensajes (A7)	4			1	1	1	Bajo
	Alteración de secuencia (A8)			4	1	1	1	Bajo

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
	Acceso no autorizado (A9)	4		4	1	3	3	Bajo
	Modificación deliberada de la información (A13)			4	1	1	1	Bajo
	Destrucción de información (A14)		5		1	2	2	Bajo
	Divulgación de información (A15)	4			1	1	1	Bajo
	Denegación de servicio (A18)		5		3	2	5	Medio
Sistema Eléctrico General (AUX1)	Desastres Naturales (N3)		4		1	1	1	Bajo
	Fuego (I1)		4		2	1	3	Bajo
	Daños por agua (I2)		4		2	1	3	Bajo
	Desastres Industriales (I3)		4		1	1	1	Bajo
	Contaminación mecánica (I4)		4		4	1	5	Medio
	Avería de origen física o lógica (I6)		4		1	1	1	Bajo
	Corte eléctrico (I7)		4		2	1	3	Bajo

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
	Condiciones inadecuadas de temperatura y/o humedad (I8)		4		2	1	3	Bajo
	Interrupción de otros servicios y suministros esenciales (I10)		4		1	1	1	Bajo
	Errores de mantenimiento / actualización de equipos (hardware) (E14)		4		1	1	1	Bajo
	Pérdida de equipos (E16)	3	4		1	2	2	Bajo
	Uso no previsto (A5)	3	4	4	1	4	4	Medio
	Manipulación de los equipos (A17)	3	4		2	2	5	Medio
Fibra óptica (AUX4)	Desastres Naturales (N3)		5		1	2	2	Bajo
	Fuego (I1)		5		2	2	3	Bajo
	Daños por agua (I2)		5		2	2	3	Bajo
	Desastres Industriales (I3)		5		1	2	2	Bajo
	Contaminación mecánica (I4)		5		3	2	5	Medio
	Avería de origen física o lógica (I6)		5		2	2	3	Bajo

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
	Corte eléctrico (I7)		5		2	2	3	Bajo
	Condiciones inadecuadas de temperatura y/o humedad (I8)		5		2	2	3	Bajo
	Interrupción de otros servicios y suministros esenciales (I10)		5		1	2	2	Bajo
	Errores de mantenimiento / actualización de equipos (hardware) (E14)		5		1	2	2	Bajo
	Pérdida de equipos (E16)	5	5		1	3	3	Bajo
	Uso no previsto (A5)	5	5	5	1	5	5	Medio
	Manipulación de los equipos (A17)	5	5		2	3	7	Alto
Cableado estructurado (AUX5)	Desastres Naturales (N3)		4		1	1	1	Bajo
	Fuego (I1)		4		2	1	3	Bajo
	Daños por agua (I2)		4		2	1	3	Bajo
	Desastres Industriales (I3)		4		1	1	1	Bajo
	Contaminación mecánica (I4)		4		3	1	4	Medio

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
	Avería de origen física o lógica (I6)		4		2	1	3	Bajo
	Corte eléctrico (I7)		4		2	1	3	Bajo
	Condiciones inadecuadas de temperatura y/o humedad (I8)		4		2	1	3	Bajo
	Interrupción de otros servicios y suministros esenciales (I10)		4		1	1	1	Bajo
	Errores de mantenimiento / actualización de equipos (hardware) (E14)		4		1	1	1	Bajo
	Pérdida de equipos (E16)	4	4		1	3	3	Bajo
	Uso no previsto (A5)	4	4	4	1	4	4	Medio
	Manipulación de los equipos (A17)	4	4		2	3	5	Medio
UPS Principal (AUX6)	Desastres Naturales (N3)		5		1	2	2	Bajo
	Fuego (I1)		5		2	2	3	Bajo
	Daños por agua (I2)		5		1	2	2	Bajo
	Desastres Industriales (I3)		5		1	2	2	Bajo

Activo	Amenaza	[C]	[D]	[I]	Frecuencia	Impacto	Riesgo	Nivel de Riesgo
	Contaminación mecánica (I4)		5		4	2	7	Alto
	Avería de origen física o lógica (I6)		5		1	2	2	Bajo
	Corte eléctrico (I7)		5		2	2	3	Bajo
	Condiciones inadecuadas de temperatura y/o humedad (I8)		5		2	2	3	Bajo
	Interrupción de otros servicios y suministros esenciales (I10)		5		1	2	2	Bajo
	Errores de mantenimiento / actualización de equipos (hardware) (E14)		5		1	2	2	Bajo
	Pérdida de equipos (E16)	3	5		1	3	3	Bajo
	Uso no previsto (A5)	3	5	3	1	4	4	Medio
	Manipulación de los equipos (A17)	3	5		2	3	5	Medio

Nota. Esta tabla muestra el análisis y la evaluación del riesgo en los activos de la empresa Novacobranzas.

Una vez realizado el análisis y la evaluación de riesgos de los activos más importantes de la empresa, y de identificar las amenazas junto a su probabilidad de ocurrencia, es posible identificar los activos que tienen una mayor probabilidad de ser afectados, ya sea por daños, ataques, vulnerabilidades u otras causas.

Selección de objetivos de control

El próximo procedimiento para avanzar en el desarrollo del SGSI consiste en vincular los controles establecidos por la norma ISO 27001:2022 con los activos que presentan una mayor valoración en términos de riesgo, tal como se muestra en las tablas previamente. A continuación, se presentan los 4 dominios o anexos que integran el estándar ISO 27001:2002 (Organización Internacional de Normalización, 2022):

- **Anexo 5:** Controles Organizativos.
- **Anexo 6:** Control de Personas.
- **Anexo 7:** Controles Físicos.
- **Anexo 8:** Controles Tecnológicos.

Tabla 14. Selección de objetivos de control

Activo	Amenaza	Frecuencia	Objetivos de Control	Controles de la norma ISO 27001
Firewall Sophos (HW1)	Errores del administrador (E2)	MB	5. Controles organizacionales 6. Controles de personas 7. Controles físicos 8. Controles tecnológicos	5.4 Responsabilidades de la dirección 5.8 Seguridad de la información en la gestión de proyectos 5.36 Cumplimiento de políticas, normas y estándares 6.3 Concienciación, educación y formación en seguridad 7.13 Mantenimiento de equipos 8.32 Gestión de cambios
Computadoras de Escritorio (HW2)	Abuso de privilegios de acceso (A4)	M	5. Controles organizacionales 8. Controles tecnológicos	5.2 Roles y responsabilidades de seguridad de la información 5.15 Control de acceso 5.16 Gestión de identidades 5.18 Derechos de acceso 8.2 Derechos de acceso privilegiado 8.18 Uso de programas utilitarios privilegiados
	Uso no previsto (A5)	A	5. Controles organizacionales 6. Controles de personas 8. Controles tecnológicos	5.10 Uso aceptable de la información y otros activos asociados 5.36 Cumplimiento de políticas, normas y estándares 6.3 Concienciación, educación y formación en seguridad 8.3 Restricción de acceso a la información
Computadoras portátiles (HW3)	Abuso de privilegios de acceso (A4)	M	5. Controles organizacionales 8. Controles tecnológicos	5.2 Roles y responsabilidades de seguridad de la información 5.15 Control de acceso 5.16 Gestión de identidades 5.18 Derechos de acceso 8.2 Derechos de acceso privilegiado 8.18 Uso de programas utilitarios privilegiados
	Uso no previsto (A5)	A	5. Controles organizacionales 6. Controles de personas 8. Controles tecnológicos	5.10 Uso aceptable de la información y otros activos asociados 5.36 Cumplimiento de políticas, normas y estándares 6.3 Concienciación, educación y formación en seguridad 8.3 Restricción de acceso a la información

Activo	Amenaza	Frecuencia	Objetivos de Control	Controles de la norma ISO 27001
Telefonía IP (HW12)	Errores del administrador (E2)	M	5. Controles organizacionales 6. Controles de personas 7. Controles físicos 8. Controles tecnológicos	5.4 Responsabilidades de la dirección 5.8 Seguridad de la información en la gestión de proyectos 5.36 Cumplimiento de políticas, normas y estándares 6.3 Concienciación, educación y formación en seguridad 7.13 Mantenimiento de equipos 8.32 Gestión de cambios
	Uso no previsto (A5)	B	5. Controles organizacionales 6. Controles de personas 8. Controles tecnológicos	5.10 Uso aceptable de la información y otros activos asociados 5.36 Cumplimiento de políticas, normas y estándares 6.3 Concienciación, educación y formación en seguridad 8.3 Restricción de acceso a la información
Central Telefónica (HW13)	Errores del administrador (E2)	M	5. Controles organizacionales 6. Controles de personas 7. Controles físicos 8. Controles tecnológicos	5.4 Responsabilidades de la dirección 5.8 Seguridad de la información en la gestión de proyectos 5.36 Cumplimiento de políticas, normas y estándares 6.3 Concienciación, educación y formación en seguridad 7.13 Mantenimiento de equipos 8.32 Gestión de cambios
	Uso no previsto (A5)	B	5. Controles organizacionales 6. Controles de personas 8. Controles tecnológicos	5.10 Uso aceptable de la información y otros activos asociados 5.36 Cumplimiento de políticas, normas y estándares 6.3 Concienciación, educación y formación en seguridad 8.3 Restricción de acceso a la información
Access Point (HW14)	Errores del administrador (E2)	B	5. Controles organizacionales 6. Controles de personas 7. Controles físicos 8. Controles tecnológicos	5.4 Responsabilidades de la dirección 5.8 Seguridad de la información en la gestión de proyectos 5.36 Cumplimiento de políticas, normas y estándares 6.3 Concienciación, educación y formación en seguridad 7.3 Seguridad en oficinas, salas e instalaciones 8.32 Gestión de cambios
	Acceso no autorizado (A9)	M	5. Controles organizacionales 8. Controles tecnológicos	5.15 Control de acceso 5.18 Derechos de acceso 8.2 Derechos de acceso privilegiado 8.3 Restricción de acceso a la información 8.22 Segregación de redes

Activo	Amenaza	Frecuencia	Objetivos de Control	Controles de la norma ISO 27001
Servidor de aplicaciones (SW1)	Errores de usuarios (E1)	B	5. Controles organizacionales 6. Controles de personas 8. Controles tecnológicos	5.36 Cumplimiento de políticas, normas y estándares 6.3 Concienciación, educación y formación en seguridad 8.3 Restricción de acceso a la información 8.5 Autenticación segura
	Abuso de privilegios de acceso (A4)	B	5. Controles organizacionales 8. Controles tecnológicos	5.2 Roles y responsabilidades de seguridad de la información 5.15 Control de acceso 5.16 Gestión de identidades 5.18 Derechos de acceso 8.2 Derechos de acceso privilegiado 8.18 Uso de programas utilitarios privilegiados
Servidor de Bases de Datos (SW2)	Errores de usuarios (E1)	M	5. Controles organizacionales 6. Controles de personas 8. Controles tecnológicos	5.36 Cumplimiento de políticas, normas y estándares 6.3 Concienciación, educación y formación en seguridad 8.3 Restricción de acceso a la información 8.5 Autenticación segura
	Errores del administrador (E2)	B	5. Controles organizacionales 6. Controles de personas 7. Controles físicos 8. Controles tecnológicos	5.4 Responsabilidades de la dirección 5.8 Seguridad de la información en la gestión de proyectos 5.36 Cumplimiento de políticas, normas y estándares 6.3 Concienciación, educación y formación en seguridad 7.13 Mantenimiento de equipos 8.32 Gestión de cambios
	Abuso de privilegios de acceso (A4)	B	5. Controles organizacionales 8. Controles tecnológicos	5.2 Roles y responsabilidades de seguridad de la información 5.15 Control de acceso 5.16 Gestión de identidades 5.18 Derechos de acceso 8.2 Derechos de acceso privilegiado 8.18 Uso de programas utilitarios privilegiados
	Uso no previsto (A5)	B	5. Controles organizacionales 6. Controles de personas 8. Controles tecnológicos	5.10 Uso aceptable de la información y otros activos asociados 5.36 Cumplimiento de políticas, normas y estándares 6.3 Concienciación, educación y formación en seguridad 8.3 Restricción de acceso a la información

Activo	Amenaza	Frecuencia	Objetivos de Control	Controles de la norma ISO 27001
Servidor Telefonía (SW3)	Errores de usuarios (E1)	M	5. Controles organizacionales 6. Controles de personas 8. Controles tecnológicos	5.36 Cumplimiento de políticas, normas y estándares 6.3 Concienciación, educación y formación en seguridad 8.3 Restricción de acceso a la información 8.5 Autenticación segura
	Errores del administrador (E2)	B	5. Controles organizacionales 6. Controles de personas 7. Controles físicos 8. Controles tecnológicos	5.4 Responsabilidades de la dirección 5.8 Seguridad de la información en la gestión de proyectos 5.36 Cumplimiento de políticas, normas y estándares 6.3 Concienciación, educación y formación en seguridad 7.13 Mantenimiento de equipos 8.32 Gestión de cambios
	Abuso de privilegios de acceso (A4)	B	5. Controles organizacionales 8. Controles tecnológicos	5.2 Roles y responsabilidades de seguridad de la información 5.15 Control de acceso 5.16 Gestión de identidades 5.18 Derechos de acceso 8.2 Derechos de acceso privilegiado 8.18 Uso de programas utilitarios privilegiados
	Uso no previsto (A5)	B	5. Controles organizacionales 6. Controles de personas 8. Controles tecnológicos	5.10 Uso aceptable de la información y otros activos asociados 5.36 Cumplimiento de políticas, normas y estándares 6.3 Concienciación, educación y formación en seguridad 8.3 Restricción de acceso a la información
Servidor de almacenamiento (SW4)	Errores de usuarios (E1)	B	5. Controles organizacionales 6. Controles de personas 8. Controles tecnológicos	5.36 Cumplimiento de políticas, normas y estándares 6.3 Concienciación, educación y formación en seguridad 8.3 Restricción de acceso a la información 8.5 Autenticación segura
	Errores del administrador (E2)	B	5. Controles organizacionales 6. Controles de personas 7. Controles físicos 8. Controles tecnológicos	5.4 Responsabilidades de la dirección 5.8 Seguridad de la información en la gestión de proyectos 5.36 Cumplimiento de políticas, normas y estándares 6.3 Concienciación, educación y formación en seguridad 7.13 Mantenimiento de equipos 8.32 Gestión de cambios

Activo	Amenaza	Frecuencia	Objetivos de Control	Controles de la norma ISO 27001
	Abuso de privilegios de acceso (A4)	B	5. Controles organizacionales 8. Controles tecnológicos	5.2 Roles y responsabilidades de seguridad de la información 5.15 Control de acceso 5.16 Gestión de identidades 5.18 Derechos de acceso 8.2 Derechos de acceso privilegiado 8.18 Uso de programas utilitarios privilegiados
	Uso no previsto (A5)	M	5. Controles organizacionales 6. Controles de personas 8. Controles tecnológicos	5.10 Uso aceptable de la información y otros activos asociados 5.36 Cumplimiento de políticas, normas y estándares 6.3 Concienciación, educación y formación en seguridad 8.3 Restricción de acceso a la información
Servidor de Dominio (SW5)	Errores de usuarios (E1)	M	5. Controles organizacionales 6. Controles de personas 8. Controles tecnológicos	5.36 Cumplimiento de políticas, normas y estándares 6.3 Concienciación, educación y formación en seguridad 8.3 Restricción de acceso a la información 8.5 Autenticación segura
	Errores del administrador (E2)	B	5. Controles organizacionales 6. Controles de personas 7. Controles físicos 8. Controles tecnológicos	5.4 Responsabilidades de la dirección 5.8 Seguridad de la información en la gestión de proyectos 5.36 Cumplimiento de políticas, normas y estándares 6.3 Concienciación, educación y formación en seguridad 7.13 Mantenimiento de equipos 8.32 Gestión de cambios
	Abuso de privilegios de acceso (A4)	B	5. Controles organizacionales 8. Controles tecnológicos	5.2 Roles y responsabilidades de seguridad de la información 5.15 Control de acceso 5.16 Gestión de identidades 5.18 Derechos de acceso 8.2 Derechos de acceso privilegiado 8.18 Uso de programas utilitarios privilegiados
Sistema Operativo Windows (SW7)	Errores de usuarios (E1)	B	5. Controles organizacionales 6. Controles de personas 8. Controles tecnológicos	5.36 Cumplimiento de políticas, normas y estándares 6.3 Concienciación, educación y formación en seguridad 8.3 Restricción de acceso a la información 8.5 Autenticación segura

Activo	Amenaza	Frecuencia	Objetivos de Control	Controles de la norma ISO 27001
	Difusión de software dañino (E6)	M	8. Controles tecnológicos	8.7 Protección contra software malicioso 8.15 Registro de eventos 8.16 Monitorización de actividades
	Suplantación de la identidad del usuario (A3)	M	5. Controles organizacionales 8. Controles tecnológicos	5.16 Gestión de identidades 5.17 Información de autenticación 8.5 Autenticación segura
	Abuso de privilegios de acceso (A4)	M	5. Controles organizacionales 8. Controles tecnológicos	5.2 Roles y responsabilidades de seguridad de la información 5.15 Control de acceso 5.16 Gestión de identidades 5.18 Derechos de acceso 8.2 Derechos de acceso privilegiado 8.18 Uso de programas utilitarios privilegiados
	Uso no previsto (A5)	A	5. Controles organizacionales 6. Controles de personas 8. Controles tecnológicos	5.10 Uso aceptable de la información y otros activos asociados 5.36 Cumplimiento de políticas, normas y estándares 6.3 Concienciación, educación y formación en seguridad 8.3 Restricción de acceso a la información
	Acceso no autorizado (A9)	A	5. Controles organizacionales 8. Controles tecnológicos	5.15 Control de acceso 5.18 Derechos de acceso 8.2 Derechos de acceso privilegiado 8.3 Restricción de acceso a la información 8.22 Segregación de redes
Sistemas propios Novacobranzas (SW16)	Errores de usuarios (E1)	A	5. Controles organizacionales 6. Controles de personas 8. Controles tecnológicos	5.36 Cumplimiento de políticas, normas y estándares 6.3 Concienciación, educación y formación en seguridad 8.3 Restricción de acceso a la información 8.5 Autenticación segura
	Errores del administrador (E2)	A	5. Controles organizacionales 6. Controles de personas 7. Controles físicos 8. Controles tecnológicos	5.4 Responsabilidades de la dirección 5.8 Seguridad de la información en la gestión de proyectos 5.36 Cumplimiento de políticas, normas y estándares 6.3 Concienciación, educación y formación en seguridad 7.13 Mantenimiento de equipos 8.32 Gestión de cambios

Activo	Amenaza	Frecuencia	Objetivos de Control	Controles de la norma ISO 27001
	Alteración accidental de la información (E9)	A	5. Controles organizacionales 8. Controles tecnológicos	5.33 Protección de registros 8.13 Copia de seguridad de la información 8.32 Gestión de cambios
	Vulnerabilidad de los programas (software) (E12)	A	8. Controles tecnológicos	8.8 Gestión de vulnerabilidades técnicas 8.25 Ciclo de vida de desarrollo seguro 8.27 Principios de arquitectura e ingeniería segura
	Errores de mantenimiento / actualización de programas (software) (E13)	A	8. Controles tecnológicos	8.25 Ciclo de vida de desarrollo seguro 8.26 Requisitos de seguridad para aplicaciones 8.32 Gestión de cambios
	Abuso de privilegios de acceso (A4)	M	5. Controles organizacionales 8. Controles tecnológicos	5.2 Roles y responsabilidades de seguridad de la información 5.15 Control de acceso 5.16 Gestión de identidades 5.18 Derechos de acceso 8.2 Derechos de acceso privilegiado 8.18 Uso de programas utilitarios privilegiados
	[Re-]encaminamiento de mensajes (A7)	A	8. Controles tecnológicos	8.20 Seguridad de la red 8.21 Seguridad de los servicios de red 8.22 Segregación de redes
	Acceso no autorizado (A9)	M	5. Controles organizacionales 8. Controles tecnológicos	5.15 Control de acceso 5.18 Derechos de acceso 8.2 Derechos de acceso privilegiado 8.3 Restricción de acceso a la información 8.22 Segregación de redes
Bases de Datos Producción (D2)	Errores de usuarios (E1)	A	5. Controles organizacionales 6. Controles de personas 8. Controles tecnológicos	5.36 Cumplimiento de políticas, normas y estándares 6.3 Concienciación, educación y formación en seguridad 8.3 Restricción de acceso a la información 8.5 Autenticación segura

Activo	Amenaza	Frecuencia	Objetivos de Control	Controles de la norma ISO 27001
	Errores del administrador (E2)	A	5. Controles organizacionales 6. Controles de personas 7. Controles físicos 8. Controles tecnológicos	5.4 Responsabilidades de la dirección 5.8 Seguridad de la información en la gestión de proyectos 5.36 Cumplimiento de políticas, normas y estándares 6.3 Concienciación, educación y formación en seguridad 7.13 Mantenimiento de equipos 8.32 Gestión de cambios
	Errores de monitorización (log) (E3)	A	8. Controles tecnológicos	8.15 Registro de eventos 8.16 Monitorización de actividades
	Errores de configuración (E4)	A	5. Controles organizacionales 8. Controles tecnológicos	5.8 Seguridad de la información en la gestión de proyectos 8.9 Gestión de configuración 8.32 Gestión de cambios
	Manipulación de la configuración (A2)	B	8. Controles tecnológicos	8.9 Gestión de configuración 8.32 Gestión de cambios 8.33 Información de prueba
	Abuso de privilegios de acceso (A4)	B	5. Controles organizacionales 8. Controles tecnológicos	5.2 Roles y responsabilidades de seguridad de la información 5.15 Control de acceso 5.16 Gestión de identidades 5.18 Derechos de acceso 8.2 Derechos de acceso privilegiado 8.18 Uso de programas utilitarios privilegiados
Bases de Datos Clientes (D3)	Errores de usuarios (E1)	A	5. Controles organizacionales 6. Controles de personas 8. Controles tecnológicos	5.36 Cumplimiento de políticas, normas y estándares 6.3 Concienciación, educación y formación en seguridad 8.3 Restricción de acceso a la información 8.5 Autenticación segura
	Errores del administrador (E2)	A	5. Controles organizacionales 6. Controles de personas 7. Controles físicos 8. Controles tecnológicos	5.4 Responsabilidades de la dirección 5.8 Seguridad de la información en la gestión de proyectos 5.36 Cumplimiento de políticas, normas y estándares 6.3 Concienciación, educación y formación en seguridad 7.13 Mantenimiento de equipos 8.32 Gestión de cambios

Activo	Amenaza	Frecuencia	Objetivos de Control	Controles de la norma ISO 27001
	Errores de monitorización (log) (E3)	A	8. Controles tecnológicos	8.15 Registro de eventos 8.16 Monitorización de actividades
	Errores de configuración (E4)	A	5. Controles organizacionales 8. Controles tecnológicos	5.8 Seguridad de la información en la gestión de proyectos 8.9 Gestión de configuración 8.32 Gestión de cambios
	Manipulación de la configuración (A2)	B	8. Controles tecnológicos	8.9 Gestión de configuración 8.32 Gestión de cambios 8.33 Información de prueba
	Abuso de privilegios de acceso (A4)	B	5. Controles organizacionales 8. Controles tecnológicos	5.2 Roles y responsabilidades de seguridad de la información 5.15 Control de acceso 5.16 Gestión de identidades 5.18 Derechos de acceso 8.2 Derechos de acceso privilegiado 8.18 Uso de programas utilitarios privilegiados
Acceso a internet (COM1)	Errores de [re-]encaminamiento (E7)	A	8. Controles tecnológicos	8.1 Dispositivos de usuario final 8.20 Seguridad de la red 8.21 Seguridad de los servicios de red
	Abuso de privilegios de acceso (A4)	A	5. Controles organizacionales 8. Controles tecnológicos	5.2 Roles y responsabilidades de seguridad de la información 5.15 Control de acceso 5.16 Gestión de identidades 5.18 Derechos de acceso 8.2 Derechos de acceso privilegiado 8.18 Uso de programas utilitarios privilegiados
	Uso no previsto (A5)	A	5. Controles organizacionales 6. Controles de personas 8. Controles tecnológicos	5.10 Uso aceptable de la información y otros activos asociados 5.36 Cumplimiento de políticas, normas y estándares 6.3 Concienciación, educación y formación en seguridad 8.3 Restricción de acceso a la información

Activo	Amenaza	Frecuencia	Objetivos de Control	Controles de la norma ISO 27001
Correo electrónico empresarial (S3)	Errores del administrador (E2)	B	5. Controles organizacionales 6. Controles de personas 7. Controles físicos 8. Controles tecnológicos	5.4 Responsabilidades de la dirección 5.8 Seguridad de la información en la gestión de proyectos 5.36 Cumplimiento de políticas, normas y estándares 6.3 Concienciación, educación y formación en seguridad 7.13 Mantenimiento de equipos 8.32 Gestión de cambios
	Errores de [re-]encaminamiento (E7)	MA	8. Controles tecnológicos	8.1 Dispositivos de usuario final 8.20 Seguridad de la red 8.21 Seguridad de los servicios de red
	Caída del sistema por agotamiento de recursos (E15)	A	5. Controles organizacionales 8. Controles tecnológicos	5.30 Preparación TIC para la continuidad del negocio 8.6 Gestión de la capacidad 8.14 Redundancia de instalaciones de procesamiento de información
	Abuso de privilegios de acceso (A4)	B	5. Controles organizacionales 8. Controles tecnológicos	5.2 Roles y responsabilidades de seguridad de la información 5.15 Control de acceso 5.16 Gestión de identidades 5.18 Derechos de acceso 8.2 Derechos de acceso privilegiado 8.18 Uso de programas utilitarios privilegiados
	Uso no previsto (A5)	M	5. Controles organizacionales 6. Controles de personas 8. Controles tecnológicos	5.10 Uso aceptable de la información y otros activos asociados 5.36 Cumplimiento de políticas, normas y estándares 6.3 Concienciación, educación y formación en seguridad 8.3 Restricción de acceso a la información
Fibra óptica (AUX4)	Manipulación de los equipos (A17)	B	7. Controles físicos	7.8 Ubicación y protección de equipos 7.14 Eliminación o reutilización segura de equipos
UPS Principal (AUX6)	Contaminación mecánica (I4)	A	7. Controles físicos	7.5 Protección contra amenazas físicas y ambientales 7.13 Mantenimiento de equipos

Nota. Esta tabla muestra toda la selección de los objetivos de control para cada tipo de activo de acuerdo con su amenaza.

Declaración de Aplicabilidad (SoA)

Según Miguel Ángel Mendoza en su artículo sobre la Declaración de Aplicabilidad (SoA por las siglas en inglés de Statement of Applicability), este documento es un requisito que exige el estándar ISO/IEC 27001 enfocado en mantener un registro y control de las medidas de seguridad que serán aplicadas a la empresa. Este documento lista los controles de seguridad especificados en el Anexo A del estándar ISO/IEC 27001, que incluye un total de 93 controles organizados en 4 objetivos de control según la versión de 2022 de la norma de seguridad. (Mendoza, 2015)

El Anexo A es utilizado como referencia principal para la implementación de medidas de protección de la información, permitiendo detallar y verificar los controles relevantes según la situación específica de la empresa. El documento nos permite identificar los controles de seguridad que pueden aplicarse en la empresa, y así como justificar aquellos que sí y aquellos que no resultan viables.

Tabla 15. Pertinencia de controles.

ISO/IEC 27001:2022			
	Aplicable	**No Aplicable**	**Justificación**
5. CONTROLES ORGANIZACIONALES			
5.1 Políticas para la seguridad de la información	X		Es fundamental para la empresa que exista una serie de políticas que aseguren la información, debe ser socializado a todo el personal de la empresa.
5.2 Roles y responsabilidades de seguridad de la información	X		Se deben establecer, comunicar y revisar regularmente los roles y responsabilidades para asegurar una adecuada gestión de la seguridad de la información.
5.3 Separación de funciones	X		Es necesario este control ya que con la separación de funciones se evita conflictos de interés entre quienes

			registran las gestiones y quienes supervisan.
5.4 Responsabilidades de la dirección	X		La dirección de la empresa debe tener una mayor participación al momento de aplicar los controles y asignar las responsabilidades para cada área.
5.5 Contacto con autoridades	X		Si aplica ya que el área de cobranzas en algunos casos puede requerir de tener contacto con autoridades legales por incumplimiento o fraudes.
5.6 Contacto con grupos de interés especiales		X	El área de cobranzas no tiene relaciones con asociaciones externas ya que eso no le compete al área.
5.7 Inteligencia de amenazas	X		Es indispensable identificar y contrarrestar los riesgos de la información y los controles de seguridad en cada parte de los proyectos de la empresa.
5.8 Seguridad de la información en la gestión de proyectos	X		Se debe integrar la seguridad de la información en todas las fases de los proyectos para prevenir riesgos desde su concepción.
5.9 Inventario de información y otros activos asociados	X		Se debe mantener un inventario actualizado de la información y de los activos que la soportan, para asegurar que estén debidamente identificados, clasificados y protegidos según su importancia para el proceso de cobranzas.
5.10 Uso aceptable de la información y otros activos asociados	X		Se deben definir normas de uso aceptable de la información y activos para reducir riesgos de mal uso o pérdida.
5.11 Devolución de activos	X		Es importante que los colaboradores que terminen su relación laboral con la empresa, deben devolver los equipos y accesos.
5.12 Clasificación de la información	X		Es importante que la información que se tiene o se les proporciona a los colaboradores debe ser clasificado como confidencial ya que estos contienen datos sensibles de los clientes.
5.13 Etiquetado de la información	X		Es importante que el área de cobranzas cuente con una correcta etiquetación de sus documentos para seleccionar el tipo de información que va a ver cada colaborador.

5.14 Transferencia de la información	X		Se deben establecer controles de seguridad como el cifrado, el uso de canales seguros, políticas de acceso autorizado y procedimientos de protección de documentos, para garantizar la confidencialidad e integridad de la información durante su transferencia.
5.15 Control de acceso	X		El acceso a la información debe estar controlado bajo el principio de mínimo privilegio y necesidad de conocer.
5.16 Gestión de identidades	X		Es necesario establecer procedimientos para la gestión de identidades digitales, asegurando que cada colaborador tenga únicamente los accesos que le corresponden, y que se eliminen o modifiquen cuando cambie o termine la relación laboral.
5.17 Información de autenticación	X		Si aplica porque es necesario tener una autenticación segura para las aplicaciones de cobranzas.
5.18 Derechos de acceso	X		Debe de existir normativas para el control del uso correcto de los activos y por consiguiente un uso correcto de la información.
5.19 Seguridad en relaciones con proveedores	X		El área de cobranzas depende de proveedores externos al momento de proporcionar la información, es necesario establecer requisitos de seguridad al momento de recibir las carteras por parte de los proveedores.
5.20 Seguridad dentro de acuerdos con proveedores	X		Es necesario que los acuerdos con dichos proveedores incluyan cláusulas de seguridad de la información, confidencialidad y cumplimiento normativo, garantizando que los datos sensibles de los clientes estén protegidos en todo momento.
5.21 Gestión de seguridad en la cadena de suministro TIC	X		Es necesario gestionar la seguridad en toda la cadena de suministro TIC para prevenir riesgos asociados a proveedores que manejan o almacenan información sensible, asegurando la continuidad de los servicios y el cumplimiento de las políticas de seguridad de la organización.
5.22 Supervisión, revisión y gestión de cambios en servicios de proveedores	X		Es indispensable establecer procesos de supervisión, revisión y aprobación de dichos cambios, con el fin de garantizar que no afecten la confidencialidad,

			integridad ni disponibilidad de la información sensible del proceso de cobranzas.
5.23 Seguridad para el uso de servicios en la nube	X		La empresa implementa accesos remotos a sistemas de cobranzas por medio de VPN, es necesario que se establezcan controles de seguridad para garantizar que la información que se utiliza al momento del teletrabajo está protegida.
5.24 Planificación y preparación para la gestión de incidentes	X		Es necesario que el área de cobranzas tenga un plan en caso de algún incidente que tengan relación a los datos de los clientes.
5.25 Evaluación y decisión sobre eventos de seguridad	X		Si aplica porque el área de cobranzas maneja mucha información sensible de los clientes y estos deben estar correctamente asignados a los colaboradores correspondientes.
5.26 Respuesta a incidentes de seguridad	X		Es importante que el área de cobranzas cuente con un plan de respuesta para los incidentes de seguridad ya que ellos tienen información muy sensible de la empresa.
5.27 Aprendizaje a partir de incidentes de seguridad	X		Este control es importante ya que permite mejorar el proceso de cobranzas tras algún incidente de seguridad que pueda ocurrir.
5.28 Recolección de evidencia	X		En caso de que se presente alguna eventualidad legal por parte de los deudores al momento de realizar la recuperación de cobranzas, contar con la evidencia para llevar el caso a instancias legales.
5.29 Seguridad de la información durante interrupciones	X		Se requiere que el área de cobranzas cuente con un plan para garantizar continuidad de la información ante cualquier fallo técnico que ocurra.
5.30 Preparación TIC para la continuidad del negocio	X		Es importante que el área de TIC asegure la continuidad del negocio por medio de contingencias en casa de algún error.
5.31 Cumplimiento de requisitos legales, regulatorios y contractuales	X		Es necesario que el proceso de cobranzas cumpla con normativa legal de protección de datos ya que esta maneja información muy sensible.

5.32 Derechos de propiedad intelectual	X		Este control es importante ya que se debe respetar todos los derechos de propiedad intelectual del software que se utilizan en el proceso.
5.33 Protección de registros	X		Es necesario que el proceso cuente con registros de las gestiones de cobranzas que se hayan realizado día a día, protegiéndose de perdidas o alteraciones.
5.34 Privacidad y protección de PII	X		Si aplica este control porque se deben proteger los datos personales, que son sensibles, de los clientes de cobranzas.
5.35 Revisión independiente de la seguridad de la información	X		Es importante que se realicen auditorias para validar que la seguridad en el proceso de cobranzas es la adecuado y no tengo algún fallo.
5.36 Cumplimiento de políticas, normas y estándares	X		Es necesario que la empresa haga que sus colaboradores cumplan con las políticas internas de seguridad.
5.37 Procedimientos operativos documentados	X		Este control es importante porque el área debe contar con toda la documentación de sus procesos y aplicar procedimientos seguros.
6. CONTROLES DE PERSONAS			
6.1 Verificación	X		Es importante que la empresa verifique los antecedentes al momento del proceso de selección para que no ocurran filtraciones por parte de los colaboradores.
6.2 Términos y condiciones del empleo	X		Los términos de empleo deben incluir compromisos sobre seguridad de la información.
6.3 Concienciación, educación y formación en seguridad	X		Es necesario capacitar a los empleados sobre seguridad de la información de forma periódica.
6.4 Proceso disciplinario	X		La organización debe establecer procesos disciplinarios para gestionar incumplimientos de seguridad.
6.5 Responsabilidades después del cambio o terminación del empleo	X		Se deben retirar accesos y responsabilidades al finalizar o cambiar la relación laboral.
6.6 Acuerdos de confidencialidad o no divulgación	X		Los acuerdos de confidencialidad garantizan la protección de la información sensible de la organización.
6.7 Trabajo remoto	X		El trabajo remoto debe gestionarse con controles adecuados para proteger la información fuera de la empresa.

6.8 Reporte de eventos de seguridad	X		El personal debe reportar cualquier incidente, fallo o anomalías que se presenten en el sistema de cobranzas.
7. CONTROLES FÍSICOS			
7.1 Perímetros de seguridad física	X		Se deben establecer perímetros de seguridad física para proteger instalaciones críticas.
7.2 Controles de entrada física	X		Es necesario que existan controles físicos de entrada y de salida para cada área, para así tener un control de las personas que salen y entran a las diferentes áreas de la empresa.
7.3 Seguridad en oficinas, salas e instalaciones	X		La empresa debe implementar controles de seguridad al momento de ingresar y salir de las diferentes áreas.
7.4 Monitoreo de seguridad física	X		Es importante que existan cámaras o circuitos cerrados para llevar un control de seguridad por cualquier eventualidad que se presente.
7.5 Protección contra amenazas físicas y ambientales		X	El área de cobranzas no cuenta con equipos críticos que necesiten algún control para amenazas ambientales o físicas.
7.6 Trabajo en áreas seguras		X	El área de cobranzas no cuenta con áreas críticas o sensibles que sean restringidas para el personal.
7.7 Política de escritorio limpio y pantalla limpia	X		Deben de existir procedimientos para el uso de los equipos de la empresa fuera de sus instalaciones, como lo es una aprobación previa al momento de sacar algún activo de la empresa.
7.8 Ubicación y protección de equipos	X		Los equipos del área de cobranzas deben estar ubicados en lugares apropiados que reduzcan riesgos de daños físicos o ambientales, como exposición al calor, humedad o accesos no autorizados, garantizando así la continuidad de la operación.
7.9 Seguridad de activos fuera de las instalaciones	X		Para prevenir la fuga de información al momento de reasignar o eliminar un equipo, se debe de realizar un respaldo o eliminación correcta de los datos que se encuentran almacenados.
7.10 Medios de almacenamiento	X		Los medios de almacenamiento deben protegerse contra accesos no autorizados y eliminación insegura.

7.11 Servicios auxiliares	X		Es necesario asegurar la disponibilidad de estos servicios mediante mecanismos de respaldo, mantenimientos preventivos y acuerdos con proveedores, evitando interrupciones que puedan afectar la continuidad del proceso de cobranzas.
7.12 Seguridad del cableado	X		Es importante tener el cableado con canaletas cerradas y procedimientos de inspección para asegurar la integridad del cableado para que no ocurren incidentes de disponibilidad.
7.13 Mantenimiento de equipos	X		Todos los equipos que se utilizan en el área de cobranzas tienen que contar con mantenimiento que garanticen un correcto funcionamiento, reduciendo el riego de fallos que se puedan presentar. Esto asegura la continuidad de la operación, la protección de la información sensible y su disponibilidad en los sistemas de cobranzas.
7.14 Eliminación o reutilización segura de equipos	X		La eliminación y reutilización de equipos debe realizarse asegurando la destrucción segura de datos.
8. CONTROLES TECNOLÓGICOS			
8.1 Dispositivos de usuario final	X		Se deben establecer políticas y controles de seguridad para los dispositivos de usuario final (computadores, laptops, tabletas y teléfonos móviles) utilizados para acceder, procesar o almacenar información de la empresa.
8.2 Derechos de acceso privilegiado	X		El uso de accesos privilegiados debe estar restringido y monitoreado, solo utilizado por las personas que cuentan con los permisos y accesos correctos.
8.3 Restricción de acceso a la información	X		La información tiene que estar protegida en contra de accesos indebidos y estar clasificado acorde a la información que contiene.
8.4 Acceso al código fuente		X	Este control no aplica porque el área de cobranzas no desarrolla ningún tipo de software.
8.5 Autenticación segura	X		Los sistemas deben implementar una autenticación fuerte para garantizar un acceso seguro a los empleados.
8.6 Gestión de la capacidad	X		Es necesario que el proceso de cobranzas garantice una capacidad adecuada para el correcto cumplimiento de su operación.

8.7 Protección contra software malicioso	X		Se deben implementar políticas y controles como el uso de antivirus, actualizaciones de seguridad y monitoreo continuo, para proteger los equipos del área de cobranzas contra software malicioso que pueda comprometer la confidencialidad e integridad de la información.
8.8 Gestión de vulnerabilidades técnicas	X		Es necesario contar con políticas para la instalación de software que haya sido debidamente probado en un entorno de pruebas, aprobado su instalación por TIC y que deba ser mantenido en producción con el soporte adecuado para los equipos de la empresa.
8.9 Gestión de configuración	X		Con la información obtenida sobre ataques o vulnerabilidades de la empresa, el área de TIC puede tomar medidas correctivas.
8.10 Eliminación de información	X		Debe de existir controles para la correcta eliminación de la información sensible de los clientes al finalizar el uso de la misma.
8.11 Enmascaramiento de datos		X	El sistema de cobranzas no expone los datos en entornos de prueba de forma masiva.
8.12 Prevención de fuga de datos	X		Se deben implementar controles para evitar la fuga de datos intencional o accidental.
8.13 Copia de seguridad de la información	X		Si aplica porque el área de cobranzas al utilizar información sensible de los clientes al momento de hacer la gestión, es necesario un control para respaldar esa información.
8.14 Redundancia de instalaciones de procesamiento de información		X	En el área de cobranzas no existen las instalaciones redundantes.
8.15 Registro de eventos	X		Se deben establecer políticas y procedimientos para el registro y conservación de eventos relevantes, con el fin de detectar actividades no autorizadas y disponer de evidencias en caso de incidentes de seguridad.
8.16 Monitorización de actividades	X		El área de TIC debe estar en constante monitoreo para detectar actividades sospechosas realizadas por los colaboradores en el proceso de cobranzas.

8.17 Sincronización del reloj		X	Este control no aplica porque esto aplica a nivel de infraestructura de TI, no es responsabilidad del área de cobranzas.
8.18 Uso de programas utilitarios privilegiados		X	Este control no aplica ya que no utilizan programas utilitarios avanzados.
8.19 Instalación de software en sistemas operativos		X	La instalación de cualquier programas o software es netamente competencia del área de TI y no de cobranzas.
8.20 Seguridad de la red	X		Las redes deben estar protegidas con medidas de seguridad que garanticen su disponibilidad y confidencialidad.
8.21 Seguridad de los servicios de red	X		Los servicios de red deben garantizar la seguridad en el proceso de cobranzas ya que tiene información sensible de los clientes.
8.22 Segregación de redes		X	La segregación de las redes es responsabilidad del área de TI.
8.23 Filtrado web	X		Se deben implementar controles de filtrado web que restrinjan el acceso a sitios no autorizados o maliciosos desde los equipos del área de cobranzas, reduciendo el riesgo de exposición a software malicioso y fuga de información.
8.24 Uso de criptografía	X		La información sensible del proceso de cobranzas debe protegerse mediante el uso de técnicas criptográficas, asegurando la confidencialidad e integridad de los datos.
8.25 Ciclo de vida de desarrollo seguro		X	Este control no aplica porque el área de cobranzas no desarrolla ningún tipo de software.
8.26 Requisitos de seguridad para aplicaciones		X	Este control no aplica porque el área de cobranzas no adquiere directamente cualquier aplicación.
8.27 Principios de arquitectura e ingeniería segura		X	El área de TI es la responsable de diseñar arquitecturas tecnológicas.
8.28 Codificación segura		X	Este control no aplica porque el área de cobranzas no adquiere directamente cualquier aplicación.
8.29 Pruebas de seguridad en desarrollo y aceptación	X		Se debe implementar entornos de pruebas para los desarrollos de software de la empresa, esto asegura que cada componente y el sistema completo funcionen correctamente permitiendo detectar y corregir errores en etapas

			tempranas, minimizando riesgos y costos asociados con fallos posteriores.
8.30 Desarrollo externalizado	X		El área de TIC contrata desarrollos externos para los sistemas de cobranzas.
8.31 Separación de entornos de desarrollo, prueba y producción	X		Se deberá implementar medidas de protección de los datos utilizados en las pruebas asegurando que la información sensible y confidencial empleada durante los procesos de prueba esté resguardada contra accesos no autorizados, alteraciones o filtraciones.
8.32 Gestión de cambios	X		Se debe fijar políticas, procesos y registros relacionados con la administración de los proveedores que entregan un servicio que está involucrado en los servicios de TIC de la empresa.
8.33 Información de prueba	X		El control es aplicable para asegurar que los datos sensibles de los clientes no sean expuestos en los entornos de prueba, estos deben ser enmascarados para evitar accesos no autorizados o fuga de información.
8.34 Protección de sistemas de información durante auditorías		X	Este control no aplica porque las auditorias son a nivel organizacional.

Nota. Esta tabla muestra la aplicabilidad de los controles para la empresa Novacobranzas.

Cumplimiento de los controles de la norma ISO 27001:2022

Una vez realizada la declaración de aplicabilidad para la empresa Novacobranzas S.A., se determina el nivel de cumplimiento de los 4 Anexos con los respectivos dominios y objetivos de control.

5. Controles Organizacionales.

5.1 Políticas para la seguridad de la información

En la empresa Novacobranzas S.A. ya cuenta con algunas políticas de seguridad de la información definidas y documentadas. Las políticas de seguridad incluyen el proceso de cobranzas y aseguran que la información sea gestionada de manera adecuado y con su protección respectiva. Toda política cuenta con su objetivo, alcance e implementación, lo que garantiza claridad en el cumplimiento. Las políticas son revisadas y actualizadas en caso de requerir una nueva actualización y han sido comunicadas al personal mediante capacitaciones.

5.2 Roles y responsabilidades de seguridad de la información

La asignación de responsabilidades para la seguridad de la información en la empresa está en un estado óptimo, reflejando la totalidad de su cumplimiento. Esto indica que los roles y responsabilidades relacionados con la gestión de la seguridad de la información han sido claramente definidos y asignados. Además, las responsabilidades están alineadas con los objetivos estratégicos de la empresa, lo que garantiza que cada individuo conozca sus funciones y tareas dentro del sistema de gestión de seguridad de la información (SGSI).

5.3 Separación de funciones

En la empresa se ha comenzado a implementar la separación de funciones en el proceso de cobranzas. Actualmente existen ciertos roles diferenciados en actividades críticas, lo que contribuye a reducir riesgos operativos. Sin embargo, aún hay áreas donde las funciones de autorización, ejecución y revisión recaen en las mismas personas, lo que limita la efectividad de los controles internos. Para alcanzar un nivel de cumplimiento total, es necesario fortalecer la distribución de responsabilidades y asegurar que ninguna función crítica sea ejecutada de principio a fin por un solo colaborador.

5.4 Responsabilidades de la dirección

La alta dirección de la empresa ha mostrado tener un compromiso inicial con la seguridad de la información, estableciendo lineamientos básicos y asignando ciertos recursos para apoyar el SGSI. Sin embargo, aún no se ha alcanzado un nivel de participación plena: la revisión periódica de resultados, la aprobación formal de políticas y el seguimiento activo de los objetivos de seguridad se realizan de manera parcial. Esto refleja que, si bien existe una base de apoyo, todavía es necesario fortalecer el liderazgo de la dirección.

5.5 Contacto con autoridades

La empresa tiene un avance parcial en el establecimiento de contacto con las autoridades competentes en materia de seguridad de la información, alcanzando un 50% de cumplimiento. Esto nos dice que existen algunos canales de comunicación establecidos, pero estos no están completamente consolidados o formalizados. Se debe formalizar procedimientos claros para comunicarse con las autoridades en caso de incidentes de seguridad, y es recomendable fortalecer las relaciones con estas entidades regulatorias.

5.6 Contacto con grupos de interés especial

Este control no aplica para el proceso de cobranzas de empresa, ya que la naturaleza de las operaciones no requiere interacción con grupos de interés especial relacionados con amenazas, tecnologías o buenas prácticas en seguridad de la información. La gestión de la seguridad en este proceso se desarrolla de manera interna, sin necesidad de establecer vínculos con asociaciones externas o foros especializados.

5.7 Inteligencia de amenazas

En Novacobranzas S.A. no se cuenta con un proceso formal para la inteligencia de amenazas. Actualmente no se recopila ni analiza información sobre amenazas de seguridad de

la información provenientes de fuentes externas o internas, lo que impide anticiparse a incidentes potenciales. La ausencia de un sistema de monitoreo refleja un nivel de cumplimiento nulo. Esto limita la capacidad de la organización para identificar tendencias, prevenir ataques o fortalecer sus controles antes de que se materialicen riesgos.

5.8 Seguridad de la información en la gestión de proyectos

En la empresa no existe un proceso para la seguridad de la información dentro de la gestión de proyectos. La seguridad no se considera en ninguna de las fases de los proyectos, desde la planificación hasta la ejecución o cierre, lo que refleja un nivel de incumplimiento de este control. No se realizan evaluaciones de riesgos de seguridad en los proyectos, ni se han definido lineamientos o capacitaciones específicas para asegurar que los equipos de trabajo incorporen prácticas seguras.

5.9 Inventario de información y otros activos asociados

La empresa tiene implementado un inventario completo de los activos, lo que proporciona visibilidad y control sobre todos los recursos que deben ser protegidos. Esto refleja una buena gestión para este aspecto. Sin embargo, es importante realizar revisiones periódicas y la incorporación de herramientas automatizadas que faciliten la actualización en tiempo real, y tener una visión de que es lo que tiene la empresa como posibles riesgos. Es recomendable que se vincule el inventario a responsables para garantizar una gestión más eficiente y transparente.

5.10 Uso aceptable de la información y otros activos asociados

Las políticas para el uso aceptable de los activos tienen un avance parcial, ya que estas no están completamente implementadas ni comunicadas en toda la empresa. Se pudo reconocer que algunos bienes de la empresa no están siendo manejados adecuadamente por los empleados, algunos casos como dejar visible información en el escritorio que puede ser manipulada al momento que se deje el puesto de trabajo, así como el uso de internet ya sea

alámbrica o inalámbricamente se utilizan para acceder a todo tipo de páginas o redes sociales. Esto conlleva a un uso indebido o negligente de los recursos. Para abordar esta situación, se deben ampliar las políticas existentes para cubrir todos los tipos de activos, tanto físicos como digitales, y socializarlas con los empleados a través de capacitaciones y materiales de referencia.

5.11 Devolución de activos

La devolución de activos cuenta con un procedimiento formal y documentado, el cual se aplica de manera efectiva en el proceso. Cada vez que un empleado deja la organización o cambia de puesto, se asegura la devolución de todos los activos asignados, incluyendo dispositivos, credenciales y documentos. El procedimiento establece responsables claros, registros de control y verificaciones que garantizan la protección de la información y la continuidad de las operaciones.

5.12 Clasificación de la información

Toda la información utilizada en el proceso debe ser clasificada de acuerdo con las políticas internas que establecen categorías claras como pública, interna, confidencial y sensible. Esta clasificación está debidamente documentada y comunicada a los empleados, lo que permite aplicar medidas de seguridad acordes al nivel de sensibilidad de cada tipo de información. Además, el personal ha sido capacitado en la correcta identificación, manejo y protección de la información según su clasificación.

5.13 Etiquetado de la información

El etiquetado de la información presenta un bajo nivel de cumplimiento, esto quiere decir que la empresa apenas ha comenzado a etiquetar toda la información que tiene, por la falta de procedimientos claros para identificar y manejar información clasificada. Si deben definen procedimientos para el etiquetado y así controlar el riesgo de accesos indebidos o de uso

incorrecto de datos sensibles, capacitando al personal sobre el manejo adecuado de la información clasificada e implementar controles técnicos que respalden estos procesos.

5.14 Transferencia de la información

El cumplimiento total en este punto asegura que la organización cuenta con políticas y procedimientos bien definidos para el intercambio de información. Esto garantiza que las prácticas de intercambio se realicen de forma segura y controlada. Para mantener este nivel de cumplimiento, es esencial realizar revisiones periódicas de las políticas y procedimientos para garantizar su actualización frente a nuevas tecnologías o cambios normativos. Asimismo, se recomienda capacitar regularmente al personal para asegurar que comprendan y sigan estas políticas.

5.15 Control de acceso

El cumplimiento parcial refleja que no se están gestionando de manera adecuada los accesos con privilegios especiales, lo que representa un riesgo significativo para la seguridad. Se debe establecer controles más estrictos sobre los accesos con privilegios, como la implementación de procesos de aprobación, registros detallados de las actividades que realizan los usuarios.

En la empresa se encuentran implementados controles necesarios para la gestión de accesos en el proceso de cobranzas. El acceso a la información y a los sistemas están definidos por perfiles que tengan los permisos adecuados dependiendo del cargo. Además, se realizan monitoreos continuos y se mantienen registros detallados de las actividades de los usuarios, garantizando la trazabilidad y minimizando los riesgos de uso indebido.

5.16 Gestión de identidades

El cumplimiento parcial refleja que no se están gestionando de manera adecuada los accesos con privilegios especiales, lo que representa un riesgo significativo para la seguridad. Es crucial establecer controles más estrictos sobre los accesos privilegiados, como la implementación de procesos de aprobación, monitoreo continuo y registros detallados de las actividades realizadas por usuarios con privilegios especiales.

5.17 Información de autenticación

El cumplimiento total en este control demuestra que se han implementado medidas robustas para proteger la información confidencial utilizada en la autenticación de usuarios. Para mantener este nivel, es importante continuar utilizando técnicas de cifrado avanzadas y realizar evaluaciones periódicas de las prácticas de manejo de información confidencial para garantizar que cumplan con las mejores prácticas y normativas vigentes.

5.18 Derechos de acceso

El progreso limitado en la revisión de los derechos de acceso indica que este proceso no se realiza de manera regular ni exhaustiva. Esto puede llevar a que usuarios mantengan accesos innecesarios o que representen un riesgo. Es fundamental establecer un calendario formal para realizar revisiones periódicas de los derechos de acceso, automatizar estas revisiones para minimizar errores y garantizar que se retiren de inmediato los accesos que ya no sean necesarios o que puedan representar una amenaza.

5.19 Seguridad en relaciones con proveedores

El nulo cumplimiento refleja la ausencia de una política formal que defina cómo los proveedores deben gestionar la información de la organización. Esta falta de lineamientos claros aumenta el riesgo de mal manejo de datos sensibles y posibles incumplimientos. Es imprescindible desarrollar una política específica que establezca los requisitos y estándares de seguridad que los proveedores deben cumplir. Esta política debe ser comunicada formalmente a

todos los proveedores e incorporada en los contratos como un requisito obligatorio. Además, se recomienda revisar y actualizar periódicamente la política para adaptarla a nuevas amenazas y normativas aplicables.

5.20 Seguridad dentro de acuerdos con proveedores

No existen actualmente políticas, procedimientos ni cláusulas contractuales que incluyan requisitos de seguridad de la información en los acuerdos con proveedores del proceso de cobranzas. No se realizan evaluaciones de riesgos específicas antes de la firma de contratos, ni se establecen lineamientos claros sobre medidas de mitigación que los proveedores deban implementar. Tampoco se cuenta con mecanismos de seguimiento que garanticen la correcta gestión de la seguridad durante la relación contractual.

5.21 Gestión de seguridad en la cadena de suministro TIC

El cumplimiento limitado en la gestión de la cadena de suministro indica que no se están evaluando ni controlando los riesgos a lo largo de todos los eslabones que intervienen en la provisión de tecnologías de la información y comunicaciones. Esto podría comprometer la seguridad del sistema y sus servicios. Se recomienda evaluar los componentes y los riesgos asociados a cada proveedor para establecer controles que mitiguen dichos riesgos.

5.22 Supervisión, revisión y gestión de cambios en servicios de proveedores

El bajo nivel de cumplimiento en la gestión de cambios evidencia que no existen procedimientos claros para controlar las actualizaciones realizadas por terceros. Esto puede generar riesgos, como interrupciones o incumplimientos de seguridad. Se recomienda establecer un procedimiento para la gestión de cambios, asegurando que todos los cambios sean evaluados, aprobados y documentados antes de su implementación. También se deben incluir cláusulas contractuales que definan cómo deben gestionarse estos cambios y quién tiene la

autoridad para aprobarlos. Un monitoreo activo de las modificaciones realizadas garantizará que no afecten negativamente la seguridad o el desempeño de los servicios.

5.23 Seguridad para el uso de servicios en la nube

En Novacobranzas S.A. el uso de servicios en la nube presenta un cumplimiento parcial en cuanto a seguridad de la información. Actualmente existen prácticas iniciales como la definición de controles de acceso y el uso de credenciales seguras. Para alcanzar un nivel óptimo es necesario establecer lineamientos claros de seguridad para proveedores de nube, incluir cláusulas específicas, aplicar cifrado y auditorías periódicas, y capacitar al personal en las responsabilidades compartidas que implica este modelo de servicio.

5.24 Planificación y preparación para la gestión de incidentes

La baja definición de responsabilidades y procedimientos para la gestión de incidentes refleja un área crítica de mejora. La falta de roles claramente asignados y procedimientos detallados puede ocasionar demoras y confusión en la respuesta a incidentes. Para mejorar, es necesario documentar procedimientos claros que aborden cada etapa del ciclo de vida de un incidente y asignar responsabilidades específicas a los equipos involucrados. Además, es importante socializar estos procedimientos mediante capacitaciones periódicas, asegurando que todos los empleados sepan cómo actuar en caso de un evento de seguridad.

5.25 Evaluación y decisión sobre eventos de seguridad

Actualmente, los eventos no se clasifican ni se priorizan según su impacto o probabilidad, lo que impide una respuesta efectiva y oportuna. Tampoco se dispone de herramientas o mecanismos automatizados que apoyen este proceso. Esta ausencia refleja un nivel de cumplimiento nulo y aumenta significativamente el riesgo de respuestas inadecuadas frente a incidentes de seguridad.

5.26 Respuesta a incidentes de seguridad

El nivel de cumplimiento en la respuesta a incidentes demuestra avances, pero los procedimientos actuales no son suficientemente robustos ni específicos para todos los tipos de incidentes. Para fortalecer esta área, es necesario ampliar los procedimientos existentes, detallando las acciones específicas que deben tomarse según el tipo de incidente. Garantizar que estas acciones estén alineadas con las políticas y normativas de seguridad de la organización es clave. Además, realizar pruebas periódicas mediante simulacros permitirá evaluar y mejorar la preparación de los equipos frente a incidentes reales.

5.27 Aprendizaje a partir de incidentes de seguridad

El bajo nivel de cumplimiento en el aprendizaje a partir de los incidentes de seguridad indica que no se están aprovechando las oportunidades para prevenir eventos similares en el futuro. Para mejorar, es fundamental establecer un proceso formal para documentar y analizar cada incidente, identificando las lecciones aprendidas. Estas lecciones deben integrarse en las políticas y procedimientos de seguridad para fortalecer el sistema general de gestión de incidentes. Además, compartir los aprendizajes con los equipos involucrados contribuirá a reducir la recurrencia de incidentes similares.

5.28 Recolección de evidencia

Con un cumplimiento parcial en la recopilación de evidencias refleja que, aunque se han implementado medidas iniciales, estas no garantizan la validez o la integridad de que las evidencias fueron correctamente recolectadas. Para mejorar, es recomendable desarrollar procedimientos para la recopilación, almacenamiento y preservación de evidencias, asegurando que se mantenga la cadena de custodia. Se debe capacitar al personal sobre cómo manejar las evidencias para su gestión garantizando que estas puedan ser utilizadas de manera efectiva en procedimientos legales.

5.29 Seguridad de la información durante interrupciones

El cumplimiento total en la planificación de la continuidad de la seguridad de la información indica que la organización ha establecido un plan detallado y bien estructurado para abordar riesgos y definir estrategias claras. Este enfoque proactivo garantiza que se cuente con un marco sólido para gestionar la continuidad en caso de incidentes. Para mantener este nivel, es esencial revisar periódicamente el plan para adaptarlo a posibles cambios tecnológicos, regulatorios o internos. Asimismo, realizar capacitaciones regulares asegurará que todos los empleados estén familiarizados con sus roles en el plan. Documentar las lecciones aprendidas a partir de simulacros o incidentes reales contribuirá a una mejora continua de las estrategias.

5.30 Preparación TIC para la continuidad del negocio

En Novacobranzas S.A. la preparación de las TIC para la continuidad del negocio presenta un cumplimiento parcial. La organización ha definido planes de continuidad, pero su implantación no se ha realizado de manera uniforme en todas las áreas críticas del proceso de cobranzas. En cuanto a las instalaciones de procesamiento de información, existen medidas iniciales como fuentes de respaldo, pero estas aún no son suficientes para asegurar la disponibilidad en situaciones críticas.

5.31 Cumplimiento de requisitos legales, regulatorios y contractuales

El bajo nivel de cumplimiento en la identificación de la legislación aplicable refleja una falta de alineación con las normativas legales y regulatorias específicas de la organización. Genera un riesgo de incumplimientos que derivan en sanciones legales. Es importante establecer un proceso donde se identifique, documente y actualice. Este proceso debe ser dirigido por un equipo responsable que conozca los temas legales, garantizado una respuesta rápida frente a nuevas regulaciones.

5.32 Derechos de propiedad intelectual

La protección de los derechos de propiedad intelectual presenta un nivel de cumplimiento parcial, lo que indica que existen medidas iniciales, pero no son suficientes para garantizar la adecuada gestión de licencias, derechos de autor y uso de software o tecnologías. Para abordar esta deficiencia, es fundamental reforzar las políticas internas relacionadas con el respeto a los derechos de propiedad intelectual y la gestión de licencias. Además, se deben realizar auditorías periódicas para asegurar que se cumplan todas las normativas aplicables y capacitar al personal sobre la importancia de respetar estos derechos.

5.33 Protección de registros

El nivel parcial de cumplimiento en la protección de los registros de la organización evidencia que no se están aplicando controles uniformes para garantizar la integridad y disponibilidad de esta información. Esto puede aumentar el riesgo de pérdida, acceso no autorizado o uso indebido de datos críticos. Para mitigar estos riesgos, se deben establecer políticas claras para la gestión y protección de los registros, implementar controles de acceso basados en roles y realizar auditorías regulares que permitan verificar la efectividad de las medidas adoptadas.

5.34 Privacidad y protección de PII

El cumplimiento parcial en la protección de datos personales refleja que, aunque existen medidas básicas, estas no son suficientes para garantizar el cumplimiento con normativas internacionales y locales de privacidad. Para mejorar, es necesario desarrollar políticas específicas que regulen el tratamiento de datos personales, asegurando que se implementen controles efectivos para su protección. También es crucial realizar evaluaciones de impacto en la privacidad y capacitar al personal sobre las mejores prácticas para el manejo seguro de información sensible.

5.35 Revisión independiente de la seguridad de la información

El cumplimiento parcial en las revisiones independientes indica que estas no se realizan de manera regular ni abarcan todas las áreas críticas. Limita la capacidad de la empresa para evaluar objetivamente las prácticas de seguridad. Es necesario contratar auditores externos que puedan proporcionar una evaluación objetiva de la seguridad de la información. Todo esto debe complementarse con auditorías internas para tener una visión más amplia de que se puede mejorar.

Al tener un nulo cumplimiento en las revisiones independientes de la seguridad, la organización no cuenta con evaluaciones externas ni mecanismos que permitan obtener una visión objetiva de la eficacia de sus controles y prácticas de seguridad. Esta ausencia limita la capacidad de detectar debilidades de forma imparcial y aumenta el riesgo de mantener vulnerabilidades sin identificar.

5.36 Cumplimiento de políticas, normas y estándares

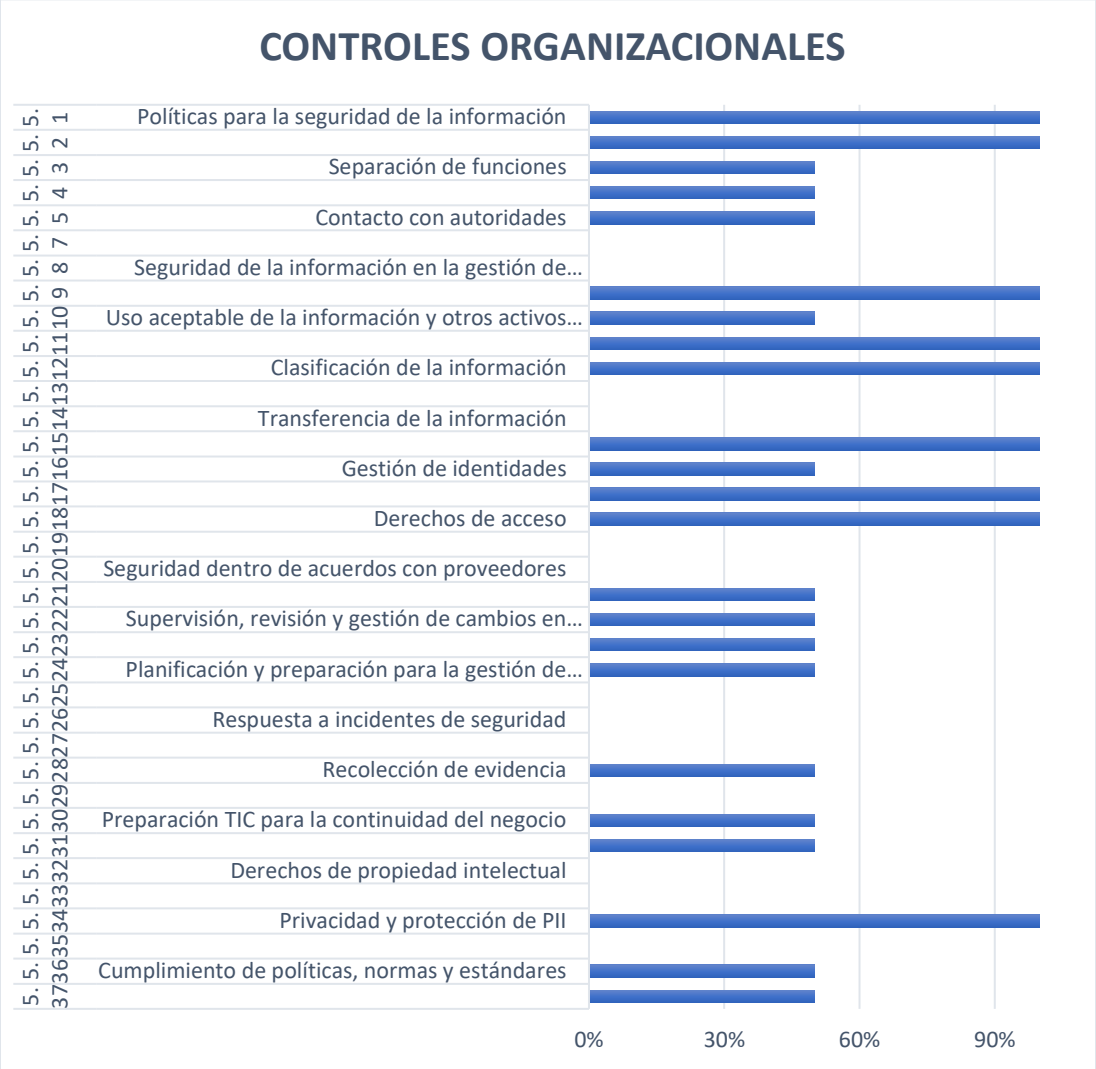
El cumplimiento de políticas, normas y estándares presenta un nivel parcial. La organización cuenta con lineamientos de seguridad establecidos, pero su aplicación no es uniforme en todas las áreas del proceso de cobranzas. Esto genera un riesgo de incumplimiento en ciertas operaciones críticas. Además, no se realizan revisiones regulares para asegurar la actualización de las políticas frente a nuevos riesgos, y la capacitación al personal aún es limitada.

5.37 Procedimientos operativos documentados

El bajo nivel de cumplimiento refleja que los procedimientos de operación no están completamente documentados o que la documentación existente no está actualizada. Esto genera inconsistencias en las operaciones y aumenta el riesgo de errores en el proceso. Es importante desarrollar y mantener una documentación detallada para el procedimiento,

asegurándose que sea fácilmente accesible para todos los empleados que la requieran, realizando revisiones garantiza que la documentación este alineada a los cambios.

Figura 19. Cumplimiento del control 5. CONTROLES ORGANIZACIONALES



Nota: Muestra el porcentaje de cumplimiento en que se encuentra el control en la empresa Novacobranzas S.A.

6. Controles de personas

6.1 Verificación

Las responsabilidades de gestión en lo que se refiere a seguridad de la información están completamente definidas y asignadas, lo que garantiza que los líderes conocen sus roles y están alineados con los objetivos estratégicos de la empresa. Se debe continuar supervisando el desempeño de los responsables a través de indicadores o KPI´s para mantener un control de las responsabilidades asignadas a los empleados. Además, estas responsabilidades deben ser revisadas y actualizadas periódicamente para adaptarse a los cambios en el entorno de riesgos y las prioridades de la organización.

6.2 Términos y condiciones del empleo

En Novacobranzas S.A. se cumple de manera total con el control de términos y condiciones del empleo. La organización cuenta con procedimientos formalmente documentados y aplicados que regulan el ciclo de vida laboral, desde la contratación hasta el cese o cambio de funciones. Estos procedimientos garantizan que, al finalizar una relación laboral o producirse un cambio de puesto, se revoquen de forma inmediata todos los accesos y se recuperen oportunamente los activos asignados.

6.3 Concienciación, educación y formación en seguridad

El progreso en la capacitación de la seguridad, no es suficiente para garantizar que los empleados conozcan que procedimientos deben tomar en caso de un ataque. Esto implicaría un bajo nivel de preparación para afrontar una amenaza, es importante que se diseñe capacitaciones, que incluyan evaluaciones regulares para medir el nivel de los empleados en lo que respecta a amenazas emergentes y como poder mitigarlas.

6.4 Proceso disciplinario

El proceso disciplinario muestra que existe un marco claro con un proceso disciplinario formal y documentado que regula los incumplimientos relacionados con la seguridad de la información en el proceso de cobranzas. Este proceso establece sanciones claras y

proporcionales según la gravedad de la falta, asegurando un tratamiento justo y transparente. Además, ha sido comunicado a todos los empleados para garantizar que comprendan las expectativas y las consecuencias de sus acciones.

6.5 Responsabilidades después del cambio o terminación del empleo

El cumplimiento total en la gestión se íntegra con las responsabilidades posteriores al cambio o terminación del empleo. La organización cuenta con procedimientos formales que aseguran la revocación inmediata de accesos y la recuperación de todos los activos asignados en cuanto un empleado finaliza su relación laboral o cambia de puesto. Estos procesos se aplican de manera sistemática y están respaldados por registros que garantizan su cumplimiento.

6.6 Acuerdos de confidencialidad o no divulgación

Los términos y condiciones de contratación cumplen completamente con los requisitos, lo que demuestra que los contratos laborales incluyen cláusulas claras relacionadas con la seguridad de la información. Esto establece desde el inicio del empleo expectativas concretas para los empleados. Se recomienda mantener la práctica de revisar periódicamente estos contratos para adaptarlos a cambios regulatorios o necesidades organizacionales. Asimismo, se debe asegurar que los empleados comprendan estas condiciones antes de iniciar sus labores, reforzando el compromiso con la seguridad.

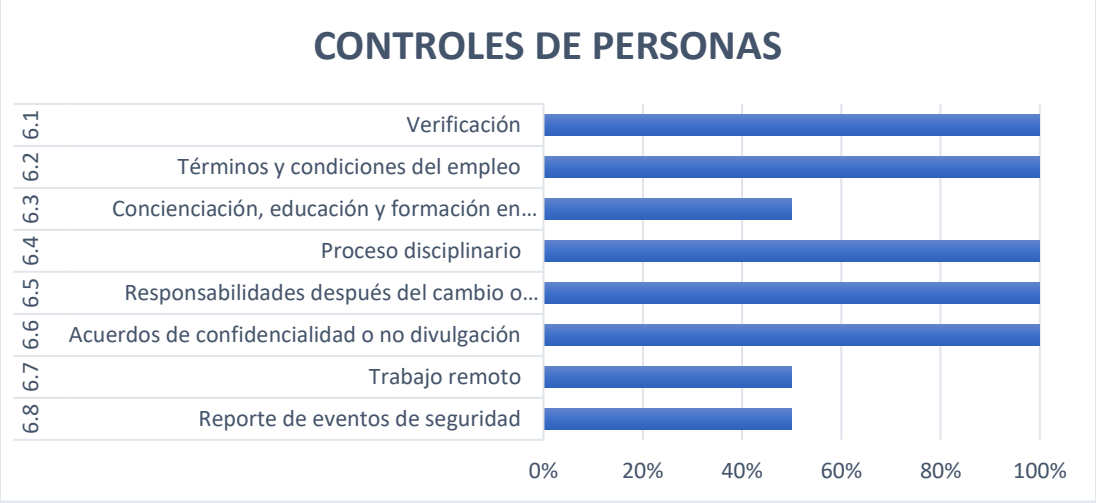
6.7 Trabajo remoto

El manejo del control de la empresa en la gestión del trabajo remoto presenta un cumplimiento parcial. Aunque existen controles técnicos implementados para facilitar actividades de teletrabajo de forma segura, la organización no cuenta aún con políticas que regulen esta modalidad. Esta falta de lineamientos claros puede generar riesgos de accesos indebidos o uso inadecuado de los recursos corporativos.

6.8 Reporte de eventos de seguridad

El bajo cumplimiento en la notificación de vulnerabilidades evidencia que no existe un proceso claro para identificar y reportar puntos débiles en los sistemas de seguridad. Esto limita la capacidad de la organización para actuar de manera proactiva frente a posibles riesgos. Para mejorar, es fundamental implementar un canal de comunicación seguro y accesible para que empleados y socios puedan reportar vulnerabilidades. También se deben establecer políticas que incentiven la notificación temprana de puntos débiles, complementadas con análisis regulares de vulnerabilidades en los sistemas para identificar y abordar riesgos potenciales.

Figura 20. Cumplimiento del control 6. CONTROLES DE PERSONAS



Nota: Muestra el porcentaje de cumplimiento en que se encuentra el control en la empresa Novacobranzas S.A.

7. CONTROLES FISICOS

7.1 Perímetros de seguridad física

El cumplimiento parcial en el control del perímetro de seguridad física indica que, aunque existen medidas iniciales para proteger los accesos a las instalaciones, estas no son suficientes

para garantizar un control total. Esto puede exponer a la organización a intrusiones no autorizadas o riesgos asociados a la falta de barreras adecuadas. Es necesario reforzar los mecanismos de control perimetral, como implementar cercas, cámaras de vigilancia y sistemas de alarma, asegurándose de que estos controles se supervisen regularmente. Adicionalmente, establecer procedimientos claros para la vigilancia del perímetro y realizar auditorías periódicas contribuirá a mejorar este control.

7.2 Controles de entrada física

El cumplimiento en su totalidad de los controles de entrada física refleja que la empresa ha implementado mecanismos efectivos para restringir el acceso a las áreas restringidas, protegiendo así la seguridad de las instalaciones y los activos críticos, únicamente al personal autorizado. Estos controles son esenciales para proteger la seguridad de las instalaciones y los activos.

7.3 Seguridad en oficinas, salas e instalaciones

El cumplimiento total en este control demuestra que se han implementado medidas robustas para garantizar la seguridad de las oficinas, despachos y recursos dentro de las instalaciones. Para mantener este nivel de protección, es fundamental realizar revisiones periódicas que verifiquen la efectividad de las medidas implementadas y actualizar las políticas de seguridad según las necesidades cambiantes. Además, capacitar continuamente al personal sobre las prácticas de seguridad contribuirá a mantener un entorno protegido.

7.4 Monitoreo de seguridad física

En Novacobranzas S.A. se cumple en su totalidad con el monitoreo de la seguridad física en el proceso de cobranzas. La organización cuenta con sistemas de vigilancia continua, incluyendo cámaras de seguridad, alarmas y controles automatizados, que permiten supervisar de manera efectiva las áreas críticas y restringidas. Estos sistemas están respaldados por

registros y rondas de seguridad periódicas, garantizando la detección temprana de accesos no autorizados o incidentes físicos.

7.5 Protección contra amenazas físicas y ambientales

Este control no aplica al proceso de cobranzas en Novacobranzas S.A., ya que la gestión de la protección contra amenazas físicas y ambientales, como incendios, desastres naturales o fallas en la infraestructura, es responsabilidad del área de administración de la organización. Dichas medidas se gestionan de manera centralizada para todas las instalaciones de la empresa y no dependen directamente del proceso de cobranzas. Por esta razón, este control no es relevante dentro del alcance definido para este proceso.

7.6 Trabajo en áreas seguras

Este control no aplica al proceso de cobranzas en Novacobranzas S.A., ya que este proceso no se desarrolla en áreas clasificadas como seguras ni requiere condiciones especiales de acceso físico para su operación. La naturaleza de las actividades de cobranzas no implica el manejo de equipos críticos ni el trabajo en instalaciones restringidas de alta seguridad. Por este motivo, el control no es relevante dentro del alcance definido para este proceso.

7.7 Política de escritorio y pantalla limpios

La implementación total de esta política asegura que las estaciones de trabajo y pantallas estén protegidas contra accesos no autorizados, reduciendo el riesgo de exposición accidental de información sensible. Igualmente se deben realizar capacitaciones periódicas para reforzar el conocimiento de la política entre los empleados. También se recomienda realizar inspecciones aleatorias que verifiquen su correcta aplicación y actualizar los lineamientos de la política conforme se identifiquen nuevos riesgos o necesidades operativas.

7.8 Ubicación y protección de equipos

Este control presenta un cumplimiento parcial, lo que indica que las medidas aplicadas no son completamente efectivas. Esto expone a los equipos a riesgos de daño físico o accesos no autorizados. Se recomienda garantizar que todos los equipos críticos estén ubicados en áreas seguras y protegidos frente a factores ambientales y humanos. También es necesario implementar sistemas de monitoreo que detecten intentos de acceso no autorizado o daños, y realizar inspecciones regulares para evaluar la efectividad de estas medidas.

Se cumple en su totalidad con el control de ubicación y protección de equipos en el proceso de cobranzas. Todos los equipos críticos se encuentran ubicados en áreas seguras y cuentan con medidas de protección física que garantizan su integridad. La organización dispone de sistemas de monitoreo para detectar accesos no autorizados o intentos de manipulación, así como de inspecciones regulares que verifican la efectividad de los controles implementados.

7.9 Seguridad de activos fuera de las instalaciones

El cumplimiento parcial refleja que no se han implementado medidas suficientes para garantizar la seguridad de los equipos y activos cuando están fuera de las instalaciones. Esto aumenta el riesgo de pérdida, daño o acceso no autorizado. Para mejorar, es necesario establecer políticas claras que regulen el transporte, almacenamiento y uso de estos activos en ubicaciones externas. También se recomienda utilizar herramientas de monitoreo y cifrado para proteger los datos almacenados en los dispositivos.

7.10 Medios de almacenamiento

Se cumple en su totalidad con el control de medios de almacenamiento dentro del proceso de cobranzas. Usar dispositivos extraíbles está totalmente restringido y solo está permitido bajo autorización de la alta dirección. Se cuenta con herramientas que monitorean la utilización de estos dispositivos. Los empleados reciben capacitaciones sobre el manejo de estos dispositivos.

7.11 Servicios auxiliares

Tiene un cumplimiento total en la seguridad de las instalaciones garantizando la disponibilidad de los servicios, protegiendo los sistemas críticos energías, comunicaciones y otros servicios esenciales. Para mantener un buen cumplimiento, es importante realizar inspecciones regulares, verificando que las medidas de seguridad sean las adecuadas para mantener la operatividad de las mismas.

7.12 Seguridad del cableado

El cumplimiento de este control asegura que se han tomado medidas adecuadas para proteger los cables contra daños físicos y accesos no autorizados. Estas prácticas son cruciales para mantener la integridad de la red y evitar interrupciones en los servicios. Se deben realizar inspecciones periódicas que permitan identificar posibles vulnerabilidades. Además, es importante documentar las medidas aplicadas y capacitar al personal técnico en las mejores prácticas.

En cuanto a la seguridad del cableado, este presenta un cumplimento parcial. Esto quiere decir que se han tomado medidas básicas para proteger los cables en cuanto a daños físicos, estas medidas no son suficientes que garanticen una protección a la infraestructura. La falta de inspecciones y de documentación de qué medidas se aplicaron aumenta el riesgo a interrupciones en los servicios.

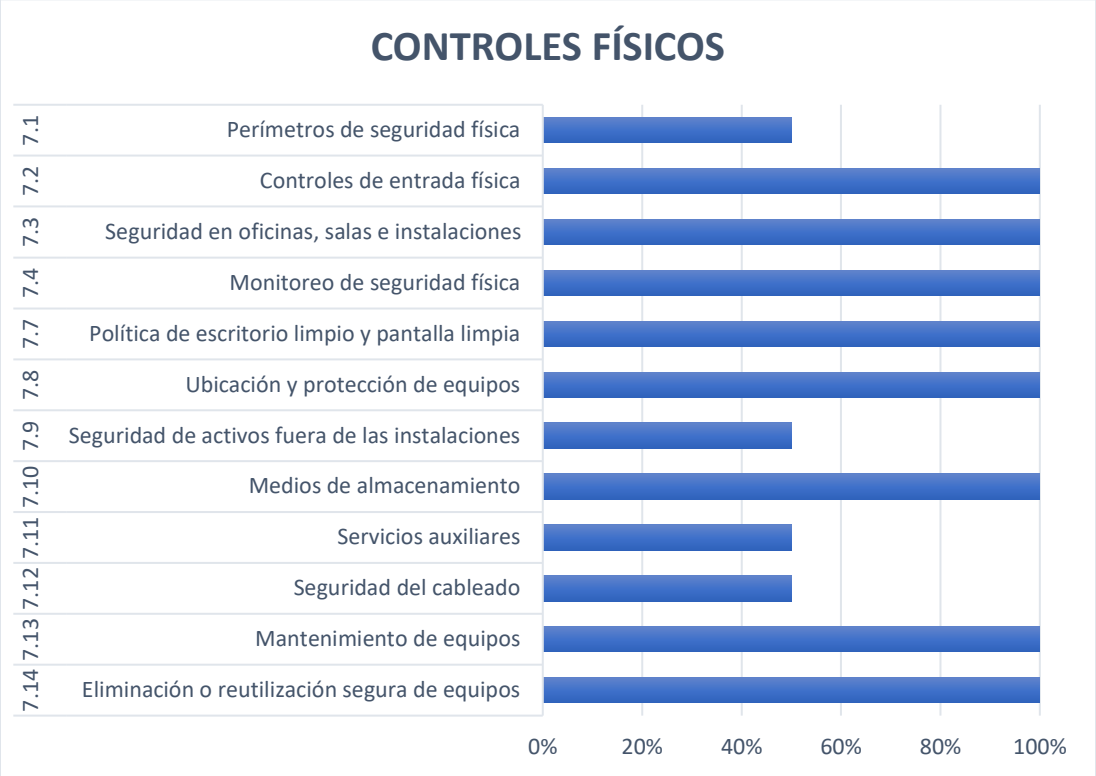
7.13 Mantenimiento de equipos

El cumplimiento total en el mantenimiento de los equipos indica que la organización realiza revisiones regulares para garantizar que los sistemas y equipos funcionen correctamente. Este nivel de cumplimiento debe mantenerse implementando un programa formal de mantenimiento preventivo y correctivo, que incluya un registro detallado de todas las actividades realizadas. Capacitar al personal técnico sobre las mejores prácticas de mantenimiento ayudará a evitar fallos imprevistos y prolongará la vida útil de los equipos.

7.14 Eliminación o reutilización segura de equipos

Tiene un cumplimiento total en la eliminación o reutilización segura de equipos dentro del proceso de cobranzas. La organización cuenta con procedimientos que garantizan la eliminación completa de los datos antes de reutilizar o retirar cualquier equipo. Este proceso incluye el uso de herramientas de borrado seguro y, cuando corresponde, la destrucción física de los dispositivos.

Figura 21. Cumplimiento del control 7. CONTROLES FÍSICOS



Nota: Muestra el porcentaje de cumplimiento en que se encuentra el control en la empresa Novacobranzas S.A.

8. CONTROLES TECNOLOGICOS

8.1 Dispositivos de usuario final

El control sobre dispositivos de usuario final tiene un cumplimiento parcial. Aunque los empleados tienen conocimientos básicos sobre el uso de soportes extraíbles y existen controles para impedir el uso de dispositivos de almacenamiento extraíbles, no existen políticas formales ni herramientas de monitoreo que permitan un control adecuado. Esto representa un riesgo de pérdida de información o accesos no autorizados.

8.2 Derechos de acceso privilegiado

En Novacobranzas S.A. se cumple en su totalidad con la gestión de los derechos de acceso privilegiado dentro del proceso de cobranzas. Todos los accesos con privilegios especiales están claramente definidos, asignados según el principio de mínimo privilegio y sujetos a autorización. Los registros de actividad de cuentas privilegiadas son monitoreados y revisados de manera regular, garantizando un control total sobre este tipo de accesos.

8.3 Restricción de acceso a la información

Este control cumple en su totalidad las restricciones de acceso a la información en el proceso. Los controles están implementados y se aplican para los usuarios con privilegios y autorizados a ver la información sensible, asegurando que cada empleado solo acceda a la información necesaria para el desempeño de sus funciones.

8.4 Acceso al código fuente

Este control no aplica al proceso de cobranzas en Novacobranzas S.A., ya que el área de cobranzas no realiza actividades de desarrollo de software ni gestiona directamente código fuente en este proceso. Las aplicaciones propias utilizadas son desarrolladas por terceros y su mantenimiento es responsabilidad de dichos proveedores y del área de tecnología.

8.5 Autenticación segura

El cumplimiento parcial en los procedimientos seguros de inicio de sesión indica que, aunque se han implementado medidas básicas, como contraseñas, estas no son suficientes para garantizar la seguridad de los accesos. Se recomienda introducir la autenticación multifactorial en todos los sistemas críticos, establecer políticas estrictas de contraseñas y aplicar mecanismos de bloqueo tras intentos fallidos. Paralelamente, se deben ofrecer capacitaciones a los usuarios para reforzar la importancia de seguir procedimientos seguros.

8.6 Gestión de la capacidad

No existen procesos formales para la gestión de la capacidad en el proceso de cobranzas. Actualmente no se llevan a cabo evaluaciones ni revisiones que permitan anticipar necesidades de recursos tecnológicos o de infraestructura, lo que limita en cierta parte la capacidad de la organización para garantizar la disponibilidad y el rendimiento de los sistemas. Esta ausencia de prácticas incrementa el riesgo de fallos por sobrecarga, interrupciones en el servicio o falta de escalabilidad ante el crecimiento de la demanda.

8.7 Protección contra software malicioso

Este control esta completo totalmente, la organización ha implementado herramientas de detección y prevención de malware en todos los sistemas críticos, garantizando un nivel robusto de seguridad. Asimismo, se aplican políticas de actualización y parches de forma regular para mantener las defensas tecnológicas al día.

8.8 Gestión de vulnerabilidades técnicas

El cumplimiento parcial en la gestión de vulnerabilidades técnicas demuestra que la organización tiene procedimientos documentados para identificar y mitigar riesgos, pero no se están llevando a cabo este control. Es importante mantener y fortalecer los procesos actuales mediante escaneos de vulnerabilidades más frecuentes y priorizando la mitigación de aquellas consideradas críticas para reducir al máximo los riesgos.

8.9 Gestión de configuración

La gestión de configuración presenta un nivel de cumplimiento parcial. Aunque existen controles implementados, como restricciones en la instalación de software no autorizado, aún no se cuenta con procedimientos formales y completos para gestionar los cambios en sistemas o aplicaciones. Esta situación incrementa el riesgo de errores operativos, interrupciones o vulnerabilidades en los entornos de producción.

8.10 Eliminación de información

En Novacobranzas S.A. se cumple en su totalidad con el control de eliminación de información dentro del proceso de cobranzas. La organización cuenta con procedimientos formales y documentados que aseguran la eliminación segura de datos sensibles cuando los soportes o equipos llegan al final de su vida útil o requieren ser reutilizados. Estos procedimientos incluyen técnicas de borrado seguro y, en los casos necesarios, la destrucción física de los dispositivos.

8.11 Enmascaramiento de datos

El cumplimiento parcial sugiere que, aunque se han tomado medidas para proteger los datos utilizados en pruebas, estas no son suficientes para garantizar su confidencialidad e integridad. Es necesario implementar técnicas como la anonimización o el cifrado de los datos utilizados en entornos de prueba, asegurando que estos no puedan ser accedidos ni utilizados de manera indebida.

Este control no aplica al proceso de cobranzas, ya que en el área de cobranzas no se realiza actividades de desarrollo ni pruebas de software que requieran el uso de datos. El enmascaramiento de datos se gestiona únicamente en áreas de tecnología de la información cuando corresponde, y no está relacionado con las operaciones del proceso de cobranzas.

8.12 Prevención de fuga de datos

En Novacobranzas S.A. la prevención de fuga de datos presenta un nivel de cumplimiento parcial. Aunque existen políticas básicas de intercambio de información y medidas de seguridad aplicadas, estas no cubren todos los canales y situaciones en las que podría producirse una filtración de datos. Persisten riesgos asociados al manejo inadecuado de información sensible y al uso de dispositivos o medios no controlados.

8.13 Copia de seguridad de la información

El cumplimiento total de este control nos garantiza la protección de los datos críticos frente a posibles pérdidas o incidentes. Este nivel de implementación es clave para mantener la continuidad del negocio en caso de fallos en los sistemas. Se deben realizar pruebas periódicas de restauración que aseguren la funcionalidad de las copias de seguridad. Además, es importante actualizar las políticas de respaldo según las necesidades de la organización y garantizar que las copias se almacenen en ubicaciones seguras, tanto físicas como digitales.

8.14 Redundancia de instalaciones de procesamiento de información

Este control no aplica al proceso de cobranzas en la empresa, ya que el área de cobranzas no gestiona directamente instalaciones críticas de procesamiento de información ni depende de infraestructura propia para garantizar la continuidad de los servicios. La redundancia de instalaciones es responsabilidad del área de tecnología de la información de manera centralizada, que administra los centros de datos y sistemas de respaldo de la organización. Por este motivo, este control se considera fuera del alcance del proceso de cobranzas.

8.15 Registro de eventos

El bajo cumplimiento en el registro y gestión de eventos de actividad refleja la falta de un monitoreo adecuado, lo que limita la capacidad de la organización para identificar incidentes o

actividades sospechosas. Se necesita implementar herramientas de registro y monitoreo que operen en tiempo real. También se deben definir procedimientos claros para analizar y gestionar los registros de actividad, y capacitar al personal en la interpretación de estos eventos para detectar posibles problemas de seguridad.

8.16 Monitorización de actividades

La monitorización de actividades presenta un nivel de cumplimiento parcial. Actualmente, los registros de actividad y la supervisión no se gestionan de manera centralizada ni con herramientas de monitoreo en tiempo real. Esta situación limita la capacidad de la organización para detectar incidentes o acciones sospechosas, además de dificultar la trazabilidad de las actividades críticas. Se recomienda implementar soluciones de monitoreo, establecer procedimientos formales de gestión y análisis de registros.

8.17 Sincronización del reloj

Este control no aplica al proceso de cobranzas en Novacobranzas S.A., ya que la sincronización de relojes en sistemas y dispositivos es una responsabilidad centralizada del área de tecnología. El proceso de cobranzas no administra ni depende directamente de configuraciones técnicas de sincronización horaria, por lo que este control se está fuera del proceso.

8.18 Uso de programas utilitarios privilegiados

Este control no aplica al proceso, ya que el uso de programas utilitarios privilegiados está relacionado con la gestión de sistemas y entornos de producción, actividades que son responsabilidad exclusiva del área de tecnología de la información. El proceso de cobranzas no necesita este tipo de programas ni tiene control sobre la administración técnica de los sistemas, por lo que este control se considera fuera del alcance definido para este proceso.

8.19 Instalación de software en sistemas operativos

Este control no aplica al proceso de cobranzas en la empresa, ya que la instalación de software en sistemas operativos es una responsabilidad exclusiva del área de tecnología de la información. El proceso de cobranzas utiliza aplicaciones ya instaladas y gestionadas por el área de TI, sin involucrarse técnicamente en la instalación o configuración de los sistemas.

8.20 Seguridad de la red

El cumplimiento parcial en los controles de red indica que no todas las medidas necesarias están completamente implementadas. Esto podría exponer a la organización a accesos no autorizados o ciberataques debido a configuraciones insuficientes o supervisión limitada. Para mitigar estos riesgos, es crucial implementar autenticación robusta y segmentación de red, garantizando que solo usuarios autorizados puedan acceder a los recursos críticos. También es necesario configurar firewalls y sistemas de prevención de intrusiones (IPS) en puntos estratégicos, complementados con auditorías regulares que identifiquen y solucionen vulnerabilidades en las redes.

8.21 Seguridad de los servicios de red

Aunque se han implementado mecanismos iniciales de seguridad para proteger los servicios de red, estos no son consistentes en toda la organización, lo que puede aumentar los riesgos de ataques o mal uso de los servicios. Para abordar esta deficiencia, es importante desarrollar políticas claras que definan los estándares de seguridad requeridos para cada servicio de red. Además, se debe garantizar el uso de cifrado en la transmisión de datos sensibles y realizar evaluaciones de seguridad periódicas que permitan identificar y resolver brechas en los mecanismos implementados.

8.22 Segregación de redes

Este control no aplica al proceso de cobranzas en la empresa, ya que la gestión y configuración de las redes corporativas es responsabilidad exclusiva del área de tecnología de la información. El proceso de cobranzas no interviene en la administración o la segregación de redes.

8.23 Filtrado web

En la empresa el filtrado web presenta un nivel de cumplimiento parcial. Actualmente existen medidas iniciales para restringir el acceso a ciertos sitios, pero estas no abarcan todas las categorías de riesgo ni están implementadas de forma uniforme en toda la organización. Esta situación deja expuestos a los usuarios a contenidos maliciosos o páginas no autorizadas que pueden comprometer la seguridad de la información.

8.24 Uso de criptografía

El cumplimiento parcial en la gestión de claves indica que existen procedimientos iniciales para su creación, almacenamiento y rotación, pero estos no son lo suficientemente robustos. Es importante que se establezca un sistema centralizado y seguro para la generación, almacenamiento y administración de claves. Asimismo, deben implementarse políticas claras que incluyan la rotación periódica de claves, minimizando el impacto de posibles compromisos.

8.25 Ciclo de vida de desarrollo seguro

El nivel bajo de cumplimiento indica que la política de desarrollo seguro de software no está completamente implementada o comunicada a los equipos de desarrollo. Esto aumenta el riesgo de introducir vulnerabilidades en las aplicaciones desarrolladas. Se recomienda diseñar una política clara que incluya prácticas seguras de codificación, revisiones regulares de código y herramientas para la detección de vulnerabilidades durante el desarrollo.

Este control no aplica al proceso de cobranzas, ya que la empresa no realiza actividades de desarrollo de software dentro de este proceso. Las aplicaciones utilizadas en cobranzas son adquiridas a terceros o administradas de forma centralizada por el área de tecnología de la información, que se encarga de su mantenimiento y seguridad.

8.26 Requisitos de seguridad para aplicaciones

Este control no aplica al proceso de cobranzas en Novacobranzas S.A., ya que la empresa no desarrolla ni adquiere aplicaciones específicas dentro de este proceso. Las aplicaciones utilizadas en cobranzas son proporcionadas y administradas de forma centralizada por el área de tecnología de la información o por proveedores externos, quienes se encargan de incorporar y garantizar los requisitos de seguridad correspondientes.

8.27 Principios de arquitectura e ingeniería segura

Este control no aplica al proceso, ya el proceso no involucra actividades de diseño, arquitectura o implementación de sistemas. Las prácticas de ingeniería segura y de arquitectura son responsabilidad del área de TIC, que gestiona de los sistemas y su seguridad.

8.28 Codificación segura

Este control no aplica al proceso de cobranzas en Novacobranzas S.A., ya que este proceso no contempla actividades de desarrollo de software. Las aplicaciones utilizadas son provistas por terceros para el área de tecnología de la información, que se encarga de aplicar prácticas de codificación segura.

8.29 Pruebas de seguridad en desarrollo y aceptación

En la empresa las pruebas de seguridad en el desarrollo y aceptación presentan un nivel de cumplimiento parcial. Actualmente se realizan pruebas básicas de funcionalidad, pero no

abarcan de forma exhaustiva los aspectos de seguridad, lo que aumenta el riesgo de que vulnerabilidades no sean detectadas antes del despliegue de aplicaciones o sistemas.

8.30 Desarrollo externalizado

En Novacobranzas S.A. el control de desarrollo externalizado presenta un nivel de cumplimiento parcial. Actualmente la empresa delega el desarrollo de software del aplicativo de Novacobranzas a terceros, también utiliza herramientas o componentes de terceros dentro de sus procesos. Sin embargo, no existen políticas o acuerdos formales que aseguren que, en caso de recurrir a proveedores externos para desarrollo o mantenimiento, estos cumplan con los requisitos de seguridad de la información.

8.31 Separación de entornos de desarrollo, prueba y producción

En Novacobranzas S.A. se cumple en su totalidad con la separación de entornos de desarrollo, prueba y producción. Cada entorno está claramente definido, lo que evita conflictos entre ellos y garantiza que las aplicaciones sean probadas de manera segura antes de pasar a producción. Esto asegura que los cambios se validen en un entorno controlado, reduciendo riesgos de errores, vulnerabilidades o interrupciones en los servicios del proceso de cobranzas. Además, se cuenta con políticas y procedimientos formales que regulan el acceso y uso de cada entorno, asegurando un control adecuado y alineado con las mejores prácticas de seguridad.

8.32 Gestión de cambios

El control de gestión de cambios presenta un nivel de cumplimiento parcial. Existen procedimientos definidos para controlar las modificaciones en sistemas y aplicaciones, su implementación no es uniforme, lo que puede generar inconsistencias, interrupciones o vulnerabilidades en el proceso. Es necesario formalizar y estandarizar los procedimientos existentes, asegurando que se apliquen a todos los sistemas relevantes.

8.33 Información de prueba

El cumplimiento parcial sugiere que, aunque se han tomado medidas para proteger los datos utilizados en pruebas, estas no son suficientes para garantizar su confidencialidad e integridad. Es necesario implementar técnicas como la anonimización o el cifrado de los datos utilizados en entornos de prueba, asegurando que estos no puedan ser accedidos ni utilizados de manera indebida.

8.34 Protección de sistemas de información durante auditorías

Este control no aplica, ya que el área no gestiona directamente auditorías técnicas sobre sistemas de información. La protección de los sistemas durante auditorías es responsabilidad del área de tecnología de la información y de auditoría interna, quienes se encargan de asegurar que las revisiones no afecten la disponibilidad, confidencialidad ni integridad de los sistemas.

Figura 22. Cumplimiento del control 8. CONTROLES TECNOLOGICOS

Nota: Muestra el porcentaje de cumplimiento en que se encuentra el control en la empresa Novacobranzas S.A.

Planteamiento de políticas de Seguridad de la información

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA NOVACOBRANZAS S.A.

Objetivo

Las presentes políticas de seguridad de la información tienen como objetivo establecer los lineamientos para proteger la información confidencial, sensible y crítica de Novacobranzas S.A., así como garantizar la disponibilidad, integridad y confidencialidad de la misma.

Alcance

Estas políticas aplican a todos los empleados y cualquier otra persona que tenga acceso a la información de Novacobranzas S.A., independientemente del lugar donde se encuentren o del dispositivo que utilicen.

Clasificación de la Información

La información de Novacobranzas S.A. se clasificará en tres niveles de confidencialidad:

- Confidencial: Información que solo debe ser conocida por personal autorizado para su uso específico.
- Sensible: Información que podría ser utilizada para causar daño a la empresa o a sus clientes si se divulga de manera no autorizada.
- Crítica: Información vital para la operación del negocio que no debe ser interrumpida, modificada o eliminada.

Controles de Acceso

Los usuarios solo podrán acceder a la información que esté dentro de su nivel de autorización.

Las contraseñas de acceso a la información de Novacobranzas S.A. deben ser seguras y confidenciales.

Protección de la Información

La información confidencial, sensible y crítica de Novacobranzas S.A. debe ser protegida contra el acceso no autorizado, la divulgación, la modificación, la destrucción o el robo.

Se implementarán medidas de seguridad físicas, técnicas y administrativas para proteger la información de Novacobranzas S.A.

Se realizarán auditorías de seguridad periódicas para verificar la eficacia de las medidas de seguridad implementadas.

Manejo de Incidentes de Seguridad

Se implementará un procedimiento para la gestión de incidentes de seguridad que incluya la identificación, el análisis, la contención y la recuperación de los incidentes.

Se notificará a las autoridades correspondientes en caso de que se produzca un incidente de seguridad que pueda tener un impacto significativo en Novacobranzas S.A.

Capacitación y Concienciación

Se brindará capacitación a todos los empleados sobre las políticas de seguridad de la información de Novacobranzas S.A.

Revisión y Actualización

Las presentes políticas de seguridad de la información serán revisadas y actualizadas periódicamente para garantizar su eficacia y adaptabilidad a los cambios en el entorno.

MATRIZ DE CLASIFICACION DE LA INFORMACIÓN PARA NOVACOBRANZAS S.A.

Objetivo

Clasificar la información de Novacobranzas S.A. en tres niveles de confidencialidad: Confidencial, Sensible y Crítica.

Nivel de Confidencialidad

- Confidencial: Información que solo debe ser conocida por personal autorizado para su uso específico.
- Sensible: Información que podría ser utilizada para causar daño a la empresa o a sus clientes si se divulga de manera no autorizada.
- Crítica: Información vital para la operación del negocio que no debe ser interrumpida, modificada o eliminada.

Nivel de Confidencialidad	**Tipo de Información**	**Ejemplos**
Confidencial	Información financiera	Estados financieros, información bancaria, datos de tarjetas de crédito
	Información de clientes	Nombres, direcciones, números de teléfono, información de crédito
	Información de empleados	Salarios, expedientes de personal, información de contacto
Sensible	Estrategias de negocio	Planes de marketing, estrategias de cobranza, información de precios
	Informes de auditoría	Informes de auditoría interna y externa
	Contratos y acuerdos	Contratos con clientes, proveedores y empleados
Crítica	Sistemas y aplicaciones	Código fuente, datos de configuración, información de acceso
	Datos de producción	Base de datos de clientes, información de cobranzas, registros de llamadas

	Infraestructura de TI	Diseño de la red, información de servidores, dispositivos de seguridad

Procedimiento para la Clasificación de la Información

La información se clasificará en función de su impacto potencial en Novacobranzas S.A. si se divulga, modifica o destruye de manera no autorizada.

Se utilizará la matriz de clasificación de la información como guía para clasificar la información.

En caso de duda sobre la clasificación de la información, se consultará con el responsable de seguridad de la información.

Revisión y Actualización

La matriz de clasificación de la información será revisada y actualizada periódicamente para garantizar su eficacia y adaptabilidad a los cambios en el entorno.

POLÍTICAS DE CONTRASEÑAS PARA NOVACOBRANZAS S.A.

Objetivo

Establecer medidas de creación y uso de contraseñas en Novacobranzas S.A., con el fin de tener contraseñas más robustas y proteger la información confidencial, sensible o critica de personas externas a la empresa.

Alcance

Esta política aplica a todos los empleados y a personas que cuenten con accesos a la información confidencial, sensible o critica de Novacobranzas S.A., independientemente del lugar donde se encuentren o del dispositivo que utilicen.

Requisitos de las Contraseñas

- Las contraseñas deben tener al menos 12 caracteres de longitud.

- Las contraseñas deben contener una combinación de letras mayúsculas y minúsculas, números y ciertos símbolos especiales (@, #, _, ^, *, %, /,.).
- Las contraseñas no deben contener nombres propios o información personal.
- Las contraseñas no deben ser reutilizadas en diferentes sistemas o aplicaciones.
- No se podrá reutilizar ninguna de las últimas 5 contraseñas utilizadas en un mismo sistema.

Gestión de Contraseñas

- Las contraseñas deben ser cambiadas cada 90 días.
- Las contraseñas deben ser cambiadas de inmediato si se sospecha que han sido comprometidas.
- Las contraseñas no deben ser compartidas con nadie.

PROCEDIMIENTO PARA LA GESTION DE INCIDENTES DE SEGURIDAD PARA NOVACOBRANZAS S.A.

Objetivo

Establecer un procedimiento para la gestión de incidentes de seguridad en Novacobranzas S.A., con el fin de minimizar el impacto negativo en la empresa.

Alcance

Este procedimiento aplica a todos los incidentes de seguridad que afecten a la información confidencial, sensible y crítica de Novacobranzas S.A., independientemente del lugar donde se produzca o del dispositivo que esté involucrado.

Etapas del Procedimiento

1. Detección:

- Los incidentes de seguridad pueden ser detectados por diferentes medios, como:
    - Monitoreo de los sistemas y aplicaciones.
    - Reportes de los usuarios.
    - Auditorías de seguridad.

2. Reporte:

- Todos los incidentes de seguridad deben ser reportados al responsable de seguridad de la información de Novacobranzas S.A.
- El reporte debe incluir la siguiente información:
    - Fecha y hora del incidente.
    - Descripción del incidente.
    - Sistemas y aplicaciones afectadas.
    - Impacto potencial del incidente.

3. Análisis:

- El responsable de seguridad de la información analizará el incidente para determinar su gravedad y su impacto potencial en la empresa.
- Se clasificará el incidente de acuerdo a su severidad:
    - Severidad baja: Impacto mínimo en la empresa, sin interrupción del servicio.
    - Severidad media: Impacto moderado en la empresa, con interrupción del servicio por un tiempo corto.
    - Severidad alta: Impacto significativo en la empresa, con interrupción del servicio por un tiempo prolongado.

4. Contención:

- Se tomarán las medidas necesarias para contener el incidente y evitar su propagación.
- Las medidas de contención pueden incluir:

- Deshabilitar cuentas de usuario.
- Aislar sistemas y aplicaciones.
- Bloquear acceso a la información.

5. Erradicación:

- Se tomarán las medidas necesarias para eliminar la causa del incidente y restaurar los sistemas y aplicaciones a su estado normal.
- La erradicación puede incluir:
  - Eliminar malware.
  - Reparar vulnerabilidades.
  - Restaurar datos de respaldo.

6. Recuperación:

- Se tomarán las medidas necesarias para recuperar los sistemas y aplicaciones a su estado normal y minimizar el impacto en la empresa y sus clientes.
- La recuperación puede incluir:
  - Restablecer el acceso a la información.
  - Notificar a los clientes afectados.
  - Implementar medidas para evitar que el incidente vuelva a ocurrir.

POLITICA DE ESCRITORIOS Y PANTALLAS LIMPIAS

Objetivo

Establecer los controles para reducir la exposición de información confidencial, sensible y crítica en los espacios de trabajo, manteniéndolo ordenado y libre de cualquier filtración no intencionada que pueda ocurrir en la empresa.

Alcance

Esta política aplica a todos los empleados y a personas que cuenten con accesos a la información confidencial, sensible o critica de Novacobranzas S.A., independientemente del lugar donde se encuentren o del dispositivo que utilicen.

Requisitos

- Los escritorios deben estar limpios y ordenados al final de cada jornada laboral.
- La información confidencial, sensible y crítica no debe ser dejada en el escritorio sin supervisión.
- Los documentos confidenciales deben ser triturados o eliminados de forma segura cuando ya no sean necesarios.
- Los dispositivos de almacenamiento extraíble (como memorias USB) no deben ser utilizados para almacenar información confidencial, sensible o crítica sin autorización.
- Las pantallas de los computadores deben ser bloqueadas cuando el usuario se ausente del escritorio.
- Bloqueo de sesión del ordenador cuando esté en inactividad.
- Configurar el protector de pantallas en base a un tiempo predeterminado.
- No tener accesos directos hacia los archivos de información en los escritorios de los ordenadores.

POLÍTICAS DE SEGURIDAD PARA LA GESTIÓN DE ACTIVOS

Objetivo

Establecer lineamientos y controles para la gestión segura de los activos de Novacobranzas con el fin de prevenir pérdidas, garantizar su correcto uso y mantener la integridad de la información asociada.

Alcance

Estas políticas aplican a todos los activos físicos y digitales de Novacobranzas, incluyendo equipos informáticos, software, información confidencial y demás bienes de la empresa.

Clasificación de activos

Se establecen las siguientes categorías:

- Activos físicos: Equipos de cómputo, dispositivos móviles, servidores, entre otros.
- Activos digitales: Software, bases de datos, información confidencial y sistemas internos.
- Activos de información: Documentos físicos y electrónicos que contengan datos sensibles de la empresa y sus clientes.

Medidas de seguridad

Seguridad Física

- Se debe restringir el acceso a áreas donde se almacenan activos críticos.
- Los activos de alto valor deben contar con mecanismos de protección contra robo o daño.
- El ingreso de terceros a áreas restringidas deberá estar autorizado y registrado.

Seguridad Digital

- Se implementarán controles de acceso mediante autenticación robusta.
- Los dispositivos electrónicos deben contar con cifrado y protección antivirus.
- Se realizarán copias de seguridad periódicas para evitar pérdida de información.
- El acceso a software y bases de datos será limitado según el rol del usuario.

Gestión de Inventario

- Todo activo debe estar debidamente registrado.
- Se realizarán auditorías periódicas para verificar la existencia y estado de los activos.
- Cualquier baja o reasignación de activos debe ser documentada y aprobada.

Control de uso y mantenimiento

- Los empleados son responsables del uso adecuado de los activos asignados.
- Se debe notificar cualquier daño, pérdida o mal funcionamiento de un activo.
- Los equipos tecnológicos deben recibir mantenimiento preventivo de manera regular.

Disposición de activos

- Los activos obsoletos o en desuso deben ser dados de baja siguiendo el procedimiento aprobado.
- Los dispositivos que contengan información confidencial deben ser eliminados de manera segura antes de su disposición final.

POLÍTICA DE CAPACITACIÓN Y CONCIENCIACIÓN EN SEGURIDAD DE LA INFORMACIÓN

NOVACOBRANZAS S.A.

Objetivo

Establecer directrices que aseguren que todos los colaboradores de la empresa Novacobranzas S.A. cuenten con las capacitaciones adecuadas en temas de seguridad de la información, promoviendo una cultura organizacional orientada a la protección de los activos de información y al cumplimiento del SGSI, conforme a la norma ISO/IEC 27001:2022.

Alcance

Esta política aplica a todos los empleados y a personas que cuenten con accesos a la información confidencial, sensible o critica de Novacobranzas S.A., independientemente del lugar donde se encuentren o del dispositivo que utilicen.

Lineamientos Generales

Capacitación Inicial

Todo nuevo colaborador deberá recibir una inducción en seguridad de la información como parte del proceso de ingreso a la empresa.

Esta capacitación incluirá:

- Principios básicos de seguridad de la información.
- Políticas y procedimientos clave (contraseñas, uso aceptable, gestión de incidentes, etc.).
- Responsabilidades del usuario.

Capacitación Continua

Se impartirán sesiones periódicas (al menos anuales) sobre nuevas amenazas, mejores prácticas, cambios normativos y actualizaciones del SGSI.

Los temas incluirán: phishing, ingeniería social, manejo seguro de información, dispositivos móviles, protección de contraseñas, uso de redes, gestión de incidentes, etc.

Evaluación y Seguimiento

- Los participantes deberán aprobar evaluaciones breves tras las capacitaciones clave.
- Se llevará un registro de asistencia y cumplimiento como evidencia para auditorías internas y externas.

Cumplimiento

El incumplimiento de esta política podrá ser considerado una falta disciplinaria, conforme al reglamento interno de trabajo, y sujeto a acciones correctivas según la gravedad.

POLÍTICAS DE SEGURIDAD PARA CONTROL DE ACCESOS

Objetivo

Establecer medidas de seguridad para el control de acceso en la empresa Novacobranzas S.A., garantizando que se proteja las instalaciones, sistemas o información confidencial, sensible o critica de la empresa.

Alcance

Esta política aplica a todos los empleados y a personas que cuenten con accesos a la información confidencial, sensible o critica de Novacobranzas S.A., independientemente del lugar donde se encuentren o del dispositivo que utilicen.

Control de acceso físico

- Se limitará el acceso a las instalaciones solo a personal autorizado.
- Los empleados deberán utilizar en todo momento los sistemas de identificación (credenciales, biometría, etc.).
- Visitantes y proveedores deberán registrarse y contar con supervisión durante su estancia.
- Se establecerán zonas restringidas a las que solo accederán personas con autorización específica.

Control de acceso digital

- Todo usuario debe contar con credenciales únicas y personalizadas.
- Se utilizarán autenticaciones seguras, como doble factor de autenticación (2FA).
- Los accesos serán otorgados según el principio de mínimo privilegio.
- Se realizarán auditorías periódicas de accesos a sistemas críticos.

Monitoreo y registro de accesos

- Todos los accesos físicos y digitales serán registrados en sistemas de monitoreo.
- Se revisarán logs de accesos de manera periódica para detectar anomalías.

- Cualquier intento de acceso no autorizado será reportado y gestionado de inmediato.

Gestión de credenciales

- Las contraseñas deben cumplir con estándares de complejidad y periodicidad de cambio.
- Las credenciales serán revocadas inmediatamente cuando un empleado deje la empresa o cambie de función.
- No se permitirá compartir credenciales de acceso en ninguna circunstancia.

POLÍTICAS PARA LA PROTECCIÓN CONTRA CÓDIGO MALICIOSO

Objetivo

Establecer las medidas de prevención, detección y respuesta ante las amenazas de ataques por código malicioso que puedan comprometer en la seguridad de los sistemas o información sensible de la empresa Novacobranzas S.A.

Alcance

Esta política aplica a todos los empleados y a personas que cuenten con accesos a la información confidencial, sensible o critica de Novacobranzas S.A., independientemente del lugar donde se encuentren o del dispositivo que utilicen.

Medidas de prevención

- Se implementarán soluciones antivirus y antimalware en todos los dispositivos corporativos.
- Se mantendrá actualizado el software de seguridad y los parches de los sistemas operativos.
- Se restringirá la instalación de software no autorizado.

- Se bloquearán sitios web y descargas de fuentes no confiables.
- Se capacitará a los empleados sobre amenazas como phishing y ransomware.

Detección y Respuesta

- Se realizarán escaneos regulares para identificar posibles amenazas.
- Cualquier intento de ejecución de código malicioso será reportado y gestionado de inmediato.
- Se establecerá un protocolo de respuesta para la contención y eliminación de programa maligno.

POLÍTICAS DE SEGURIDAD PARA LA CONTINUIDAD DEL NEGOCIO

Objetivo

Establecer controles que garanticen la continuidad de las operaciones de los sistemas de la empresa Novacobranzas S.A. en caso de que ocurran incidentes que puedan afectar su normal funcionamiento normal, minimizando los impactos y asegurando la pronta recuperación.

Alcance

Esta política aplica a todos los empleados y a personas que cuenten con accesos a la información confidencial, sensible o critica de Novacobranzas S.A., independientemente del lugar donde se encuentren o del dispositivo que utilicen.

Identificación de riesgos y análisis de impacto

- Se realizará un análisis periódico de riesgos que puedan afectar la continuidad del negocio.
- Se identificarán procesos críticos y se definirán planes de recuperación adecuados.

- Se establecerán niveles de prioridad para la reactivación de servicios clave.

Estrategias de continuidad

- Se implementarán planes de respaldo y recuperación para sistemas de información y bases de datos.
- Se definirán protocolos para la reubicación temporal de personal y operaciones en caso de incidentes mayores.
- Se garantizará la redundancia de infraestructuras críticas para minimizar tiempos de inactividad.

Pruebas y mejoras continuas

- Se realizarán pruebas periódicas del plan de continuidad para identificar oportunidades de mejora.
- Se actualizará la estrategia de continuidad según la evolución del negocio y cambios en el entorno.
- Se capacitará al personal para asegurar una respuesta efectiva ante incidentes.

POLÍTICAS DE USO DE RECURSOS TECNOLÓGICOS

Objetivo

Establecer controles para el correcto uso de los recursos tecnológicos de la empresa Novacobranzas S.A., garantizando la seguridad de la información, la eficiencia de la operación y el cumplimento de las normas internas.

Alcance

Esta política aplica a todos los empleados y a personas que utilicen recursos tecnológicos de la empresa Novacobranzas S.A., incluyendo equipos, redes, software, dispositivos móviles y sistemas internos.

Uso adecuado de los recursos tecnológicos

- Los recursos tecnológicos deben ser utilizados exclusivamente para actividades relacionadas con las funciones laborales.
- Queda prohibido el uso de equipos y redes de la empresa para acceder a contenido ilegal o inapropiado.
- El uso de software debe estar autorizado y contar con licencias oficiales.
- No se permite la instalación de programas sin la aprobación del departamento de TI.

Uso de correo electrónico y comunicaciones

- El correo electrónico corporativo debe utilizarse solo para fines laborales.
- Se prohíbe el envío de información confidencial a cuentas personales o externas sin autorización.
- No se deben abrir archivos adjuntos o enlaces sospechosos que puedan comprometer la seguridad del sistema.

POLÍTICA DE SEGURIDAD DE DATOS PERSONALES

Objetivo

Garantizar la protección de los datos personales gestionados por Novacobranzas S.A., en cumplimiento con la Ley Orgánica de Protección de Datos Personales del Ecuador (LOPDP), asegurando su confidencialidad, integridad y disponibilidad.

Alcance

Esta política aplica a todos los empleados, proveedores y terceros que tengan acceso a los datos personales gestionados por la empresa, incluyendo información de clientes, colaboradores y aliados estratégicos.

Principios de protección de datos

De acuerdo con la LOPDP, Novacobranzas S.A. se compromete a respetar los siguientes principios:

- Licitud y transparencia: el tratamiento de datos se realizará con el consentimiento del titular o en cumplimiento de una obligación legal.
- Finalidad y minimización: los datos serán recolectados con propósitos legítimos y en la mínima cantidad necesaria.
- Exactitud: se garantizará la actualización y corrección de los datos personales.
- Limitación del plazo de conservación: los datos serán almacenados únicamente por el tiempo requerido para cumplir con su finalidad.
- Seguridad y confidencialidad: se implementarán medidas técnicas y organizativas para evitar accesos no autorizados, pérdidas o alteraciones de los datos.

Derechos de los titulares de datos

Los titulares de datos personales tienen los siguientes derechos:

- Acceso: conocer qué datos personales son tratados por la empresa.
- Rectificación: solicitar la actualización o corrección de información inexacta.
- Eliminación: exigir la supresión de datos cuando no sean necesarios.
- Oposición: negarse al tratamiento de datos bajo ciertas condiciones.
- Portabilidad: obtener sus datos en un formato estructurado y reutilizable.

Medidas de seguridad

Para proteger los datos personales, Novacobranzas S.A. implementará:

- Control de acceso: limitación de acceso a datos según funciones y responsabilidades.
- Cifrado de datos: protección de información confidencial mediante mecanismos de encriptación.
- Auditorías periódicas: evaluaciones regulares para verificar el cumplimiento de la normativa.
- Respaldo y recuperación: copias de seguridad para garantizar la disponibilidad de la información.
- Capacitación del personal: formación continua en protección de datos y seguridad de la información.

Tratamiento de incidentes y violaciones de datos

En caso de una violación de datos personales:

- Se notificará a la autoridad competente y a los titulares afectados dentro del plazo legal.
- Se activarán protocolos de respuesta para contener el incidente.
- Se implementarán medidas correctivas para evitar recurrencias.

Relación con proveedores y terceros

Todo proveedor o tercero con acceso a datos personales deberá suscribir un acuerdo de confidencialidad y tratamiento de datos, asegurando el cumplimiento de la LOPDP y los estándares de seguridad definidos por Novacobranzas S.A.

POLÍTICA DE REVISIÓN Y ACTUALIZACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Objetivo

Establecer los lineamientos para la revisión, validación, actualización y aprobación de todas las políticas que conforman el marco normativo del Sistema de Gestión de Seguridad de la Información (SGSI) de Novacobranzas S.A., garantizando su vigencia, pertinencia y alineación con los objetivos de seguridad, requisitos legales y normativos vigentes.

Alcance

Esta política aplica a todas las políticas de seguridad de la información emitidas en el marco del SGSI, sin importar el área que las haya propuesto, redactado o implementado. Incluye políticas generales, específicas, técnicas y operativas relacionadas con la protección de la información.

Lineamientos Generales

Periodicidad de Revisión

Las políticas de seguridad de la información deben ser revisadas al menos una vez al año.

Además, deberán revisarse cuando ocurran cualquiera de los siguientes eventos:

- Cambios significativos en el riesgo de seguridad, amenazas o vulnerabilidades.
- Cambios organizacionales, regulatorios, contractuales o tecnológicos.
- Resultados de auditorías internas, externas o revisiones por la dirección.
- Cambios en los requisitos de partes interesadas o normativas internacionales (ej. actualizaciones de ISO/IEC 27001).

Responsables

El responsable de la revisión y actualización de cada política será el propietario del documento, en conjunto con el Oficial de Seguridad de la Información (CISO).

Toda política deberá contar con:

- Un propietario designado.
- Un historial de versiones con fecha y descripción del cambio.
- Evidencia de su aprobación formal por la Alta Dirección o Comité de Seguridad.

Aprobación y Publicación

Las nuevas versiones de las políticas deben ser aprobadas formalmente antes de su publicación.

Solo la última versión vigente será publicada en los medios oficiales de la organización (intranet, portal SGSI, etc.).

Las versiones anteriores quedarán archivadas por razones de auditoría, con control de acceso restringido.

Cumplimiento

El cumplimiento de esta política es obligatorio. El incumplimiento de los procesos de revisión y actualización podrá generar no conformidades en auditorías y será gestionado conforme al procedimiento de acciones correctivas del SGSI.

Vigencia y Revisión

Esta política será revisada anualmente por el Oficial de Seguridad de la Información y actualizada según sea necesario, en línea con la mejora continua del SGSI.

Conclusiones

En conclusión, la evaluación que se realizó a la empresa Novacobranzas S.A. permitió identificar importantes debilidades en lo que es la gestión de seguridad de la información. Se pudo evidenciar la ausencia de políticas formalizadas, falta de procedimientos de atención en caso de un incidente y un bajo nivel de capacitación a los empleados en seguridad de la información. Todo esto mostro que la necesidad de implementar un Sistema de Gestión de Seguridad de la Información (SGSI) que ofrezca lineamientos estructurados y acorde a las prácticas internacionales.

En este sentido, la implementación de la norma ISO 27001:2022 es la más adecuada para garantizar la protección de los activos de información de acuerdo a los principios de confidencialidad, integridad y disponibilidad. Esto facilito que los controles de seguridad se alineen con los objetivos de la empresa Novacobranzas S.A., permitiendo establecer un enfoque claro, ordenado y medible en la gestión de los riesgos. A través de la metodología Magerit, se logró identificar y darle un valor a las amenazas internas y externas, priorizando todas las que estén acorde al proceso de cobranzas.

Como resultado, se diseñó las políticas de seguridad de la información basándose en el Anexo A de la norma ISO 27001:2022, teniendo en cuenta aspectos críticos como la seguridad de las comunicaciones, acceso a información crítica

Recomendaciones

Se recomienda que la empresa Novacobranzas S.A. fortalezca la cultura de seguridad de la información por medio de capacitaciones a sus empleados. Esto permitiría reducir significativamente los riesgos asociados al error humano y que los empleados tomen una actitud más preventiva en caso de que exista un posible ataque al sistema de cobranzas. El Sistema de Gestión de Seguridad de la Información (SGSI) debe ser revisado periódicamente para garantizar que sea eficaz, es recomendable que las evaluaciones se realicen al menos una vez al año y que el sistema por lo menos sea actualizado cada vez que vaya a ocurrir un cambio que este alineado con los objetivos de la empresa.

Es importante que la empresa invierta en la adquisición de herramientas que le ayuden a monitorear y detectar las diferentes violaciones en las políticas de seguridad para mitigar de forma oportuna las amenazas más críticas que fueron detectadas en el análisis de riesgos, garantizando la disponibilidad del sistema.

Y, por último, una vez implementadas las políticas y controles de seguridad, se debe avanzar para tener un proceso de auditoría externa con el propósito de obtener la certificación ISO/IEC 27001:2022. Este certificado internacional permitirá reforzar la idea de que la empresa tiene medidas de seguridad de la información robustas y posicionarla de manera competitiva en el mercado, generando un mayor grado de confianza entre clientes, proveedores y aliados estratégicos.

Bibliografía

Almuhammadi, S., & Alsaleh, M. (2017). Information Security Maturity Model for Nist Cyber Security Framework. *Computer Science & Information Technology (CS & IT)*, 51–62. https://doi.org/10.5121/csit.2017.70305

Barrezueta, H. D. P. (n.d.). *DIRECTOR DEL REGISTRO OFICIAL*.

Chávez, C. A. C. (2019). La encriptación de datos empresariales: Ventajas y desventajas. *RECIMUNDO*, *3*(2), Article 2. https://doi.org/10.26820/recimundo/3.(2).abril.2019.980-997

Guía-de-protección-de-datos-personales.pdf. (n.d.). Retrieved January 29, 2024, from https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2019/11/Gu%C3%ADa-de-protecci%C3%B3n-de-datos-personales.pdf

Investigación, R. P. e, & unad, hemeroteca. (2021). *Metodologías para el análisis de riesgos en los sgsi | Publicaciones e Investigación*. https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/index

ISO/IEC 27001:2022/Amd 1:2024. (n.d.). ISO. Retrieved August 27, 2025, from https://www.iso.org/standard/88435.html

JAVIER, A. B. (2008a). *Seguridad de la información. Redes, informática y sistemas de información*. Ediciones Paraninfo, S.A.

JAVIER, A. B. (2008b). *Seguridad de la información. Redes, informática y sistemas de información*. Ediciones Paraninfo, S.A.

Kerlinger-investigacion.pdf. (n.d.). Retrieved August 21, 2024, from https://padron.entretemas.com.ve/INICC2018-2/lecturas/u2/kerlinger-investigacion.pdf

Lavao, M. S. E. (2022). *SEGURIDAD PERIMETRAL PARA LA GESTIÓN Y CONTROL DE ACCESO E IDENTIDAD EN EL SECTOR EMPRESARIAL*.

Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método. (n.d.-a).

Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método. (n.d.-b).

Mendoza, M. A. (2015, April 1). *¿Qué es una Declaración de Aplicabilidad (SoA) y para qué sirve?* https://www.welivesecurity.com/la-es/2015/04/01/que-es-declaracion-de-aplicabilidad-soa/

NQA-ISO-27001-Guia-de-implantacion.pdf. (n.d.). Retrieved January 28, 2024, from https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Object, object. (n.d.). *PARADIGMAS EN LA INVESTIGACIÓN. ENFOQUE CUANTITATIVO Y CUALITATIVO*. Retrieved August 20, 2024, from https://core.ac.uk/reader/236413540

Pineda, L. C. (n.d.). *El modelo Deming (PHVA) como estrategia competitiva para realzar el potencial administrativo.*

Qué es la gestión de activos de información - NovaSec MS. (n.d.). Retrieved January 28, 2024, from https://www.novasec.co/blog/67-gestion-de-activos-de-informacion

Quispe Parí, D. J., & Sánchez Mamani, G. (/). Encuestas y entrevistas en investigación científica. *Revista de Actualización Clínica Investiga*, 490.

Secme-22923_1.pdf. (n.d.). Retrieved August 20, 2024, from http://ri.uaemex.mx/bitstream/handle/20.500.11799/108419/secme-22923_1.pdf?sequence=1

TIPOS DE INVESTIGACION. (n.d.). *T037_45702501_T.pdf*. (n.d.). Retrieved January 29, 2024, from https://repositorio.upla.edu.pe/bitstream/handle/20.500.12848/2604/T037_45702501_T.pdf?sequence=1&isAllowed=y

Toro, R. (2021, March 11). ¿Qué es la seguridad de la información y cuantos tipos hay? *PMG SSI - ISO 27001*. https://www.pmg-ssi.com/2021/03/que-es-la-seguridad-de-la-informacion-y-cuantos-tipos-hay/

Vega Velasco, W. (2008). POLITICAS Y SEGURIDAD DE LA INFORMACION. *Fides et Ratio - Revista de Difusión cultural y científica de la Universidad La Salle en Bolivia*, *2*(2), 63–69.

VICIdial.com » About. (n.d.). Retrieved September 2, 2024, from https://www.vicidial.com/?page_id=11

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Mora Henríquez**, **Álvaro Fernando,** con C.C: # 0922483805 autor/a del componente práctico del examen complexivo: **"Propuesta metodológica para la implementación de SGSI basado en ISO 27001:2022 aplicada al proceso "Gestión de Cobranzas" de la empresa Novacobranzas S.A."** previo a la obtención del título de **Ingeniero en Sistemas Computacionales** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 04 de septiembre de 2025

_____

Nombre: **Mora Henríquez, Álvaro Fernando**

C.C: **0922483805**

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TEMA Y SUBTEMA:	**Propuesta metodológica para la implementación de SGSI basado en ISO 27001:2022 aplicada al proceso "Gestión de Cobranzas" de la empresa Novacobranzas S.A.**		
AUTOR(ES)	**Mora Henríquez, Álvaro Fernando**		
REVISOR(ES)/TUTOR(ES)	**Toala Quimí, Edison José**		
INSTITUCIÓN:	**Universidad Católica de Santiago de Guayaquil**		
FACULTAD:	**Ingeniería**		
CARRERA:	**Ingeniería en Sistemas Computacionales**		
TITULO OBTENIDO:	**Ingeniero en Sistemas Computacionales**		
FECHA DE PUBLICACIÓN:	04 de septiembre de 2025	**No. DE PÁGINAS:**	**190 páginas**
ÁREAS TEMÁTICAS:	**Seguridad de la información, ISO 27001, Control de información, Protección de datos, Educación de usuarios.**		
PALABRAS CLAVES/ KEYWORDS:	**ISO 27001:2022, Protección de Datos Personales, SGSI, Análisis de brechas, Vulnerabilidad.**		
RESUMEN/ABSTRACT: El presente proyecto tiene como objetivo presentar una propuesta metodológica para la implementación de SGSI basado en ISO 27001:2022 aplicándolo en el proceso de Gestión de Cobranzas de la empresa Novacobranzas. La investigación aborda la necesidad de mejorar la seguridad de la información dentro de la empresa debido a la creciente exposición a ciberataques y amenazas internas. A través de un análisis de brechas (Análisis GAP), se identificaron deficiencias significativas en la infraestructura de seguridad de la empresa, evidenciando la falta de controles adecuados, políticas de seguridad documentadas y mecanismos de respuesta ante incidentes. El estudio también revela que los empleados tienen bajo conocimiento en seguridad informática, lo que aumenta la vulnerabilidad a ataques externos e internos.			
ADJUNTO PDF:	☒ SI	☐ NO	
CONTACTO CON AUTOR/ES:	**Teléfono:**+593-968-480462	E-mail: **alvaro.mora96@hotmail.com**	
CONTACTO CON LA INSTITUCIÓN (C00RDINADOR DEL PROCESO UTE)::	**Toala Quimí, Edison José**		
	Teléfono: +593-990-976776		
	E-mail: edison.toala@cu.ucsg.edu.ec		
SECCIÓN PARA USO DE BIBLIOTECA			
Nº. DE REGISTRO (en base a datos):			
Nº. DE CLASIFICACIÓN:			
DIRECCIÓN URL (tesis en la web):			