REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN: MENCIÓN SEGURIDAD INFORMÁTICA

“ANÁLISIS DE LA SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO/IEC 27002:2022 Y NIST 800-61 PARA EL ÁREA DE OPERACIONES Y SERVICIOS DEL GOBIERNO PROVINCIAL DE IMBABURA”

Trabajo de Titulación previo a la obtención del Título de Magíster en Computación mención Seguridad Informática

AUTOR:

Ing. Jadhira Paola Narváez Guerrón

DIRECTOR:

PHD. Pusdá Chulde Marco Remigio

IBARRA - ECUADOR

2024

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD	0401449095		
APELLIDOS Y NOMBRES	NARVAEZ GUERRON JADHIRA PAOLA		
DIRECCIÓN	PASAJE ELIAS REINA SN Y RIO CHICHIPE		
EMAIL	narvaezjadhira@gmail.com		
TELÉFONO FIJO	2610469	**TELÉFONO MÓVIL:**	0969791194

DATOS DE LA OBRA	
TÍTULO:	ANÁLISIS DE LA SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO/IEC 27002:2022 Y NIST 800-61 PARA EL ÁREA DE OPERACIONES Y SERVICIOS DEL GOBIERNO PROVINCIAL DE IMBABURA
AUTOR (ES):	NARVAEZ GUERRON JADHIRA PAOLA
FECHA: DD/MM/AAAA	24/04/2024
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA DE POSGRADO	
TITULO POR EL QUE OPTA	Magíster en Computación mención Seguridad Informática
ASESOR/TUTOR	MSC. VACA SIERRA TULIA / PHD. PUSDÁ CHULDE MARCO

2. CONSTANCIAS

El autor Narváez Guerrón Jadhira Paola, manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto la obra es original y que es titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 24 días del mes de abril del 2024

EL AUTOR:

Firmado electrónicamente por:
JADHIRA PAOLA
NARVAEZ GUERRON

Firma:
Narváez Guerrón Jadhira Paola
C.I.: 0401449095

APROBACIÓN DEL TUTOR

Yo PhD. Pusdá Chulde Marco, en calidad de tutor del Trabajo de Investigación titulado: "ANÁLISIS DE LA SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO/IEC 27002:2022 Y NIST 800-61 PARA EL ÁREA DE OPERACIONES Y SERVICIOS DEL GOBIERNO PROVINCIAL DE IMBABURA", de autoría de la Ing. Jadhira Paola Narváez Guerrón, para optar por el grado de Magíster en Computación mención Seguridad Informática, doy fe de que dicho trabajo reúne los requisitos y méritos suficientes para ser sometidos a presentación privada y evaluación por parte del jurado examinador que se designe.

En la ciudad de Ibarra, a los 24 días del mes de abril del 2024.

0401200951
MARCO REMIGIO
PUSDA CHULDE

Firmado digitalmente por 0401200951 MARCO REMIGIO PUSDA CHULDE
Fecha: 2024.04.24 07:11:02 -05'00'

PhD. Pusdá Chulde Marco

Tutor

DEDICATORIA

Dedico este proyecto a mis hijos, por ser la fuente de inspiración y motivación para poder superarme todos los días, quienes me brindan su apoyo moral para seguir adelante y mejorar. A mi esposo, por su apoyo constante, comprensión y aliento. Gracias por acompañarme en cada paso de este viaje académico. A mis padres, por su apoyo incondicional en cada etapa de mi vida. Sus consejos y los valores inculcados han sido fundamentales en mi educación, siendo su guía y buen ejemplo la fuerza impulsora que me ha llevado a alcanzar mis metas.

Jadhira Paola Narváez Guerrón

AGRADECIMIENTO

Quiero expresar mi más sincero agradecimiento a la Universidad Técnica del Norte ilustre institución en la que me ha formado como profesional. También quiero reconocer y agradecer a todas las personas que contribuyeron directa e indirectamente al éxito de mi proyecto de titulación.

En primer lugar, quiero agradecer a mi tutor de tesis, MSc. Marco Pusdá, por su orientación experta, paciencia y dedicación a lo largo de todo el proceso. Sus valiosas sugerencias y comentarios han sido fundamentales para dar forma y mejorar mi trabajo.

Asimismo, quiero agradecer a la MSc. Tulia Vaca por su asesoramiento y por compartir su experiencia en el campo. Sus valiosas sugerencias y perspectivas enriquecieron mi enfoque de investigación y contribuyeron significativamente a la calidad del trabajo final.

Además, agradezco a mi familia por su inquebrantable respaldo, comprensión y motivación. Su apoyo ha sido mi fuente de fortaleza y determinación a lo largo de este viaje académico.

Jadhira Paola Narváez Guerrón

INDICE DE CONTENIDOS

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE II
DEDICATORIA V
AGRADECIMIENTO VI
INDICE DE CONTENIDOS VII
INDICE DE FIGURAS IX
INDICE DE TABLAS X
RESUMEN XI
ABSTRACT XII
CAPITULO I 13
EL PROBLEMA 13
1.1 PROBLEMA DE INVESTIGACIÓN 13
1.2 INTERROGANTES DE LA INVESTIGACIÓN 14
1.3 OBJETIVOS DE LA INVESTIGACIÓN 14
1.3.1 OBJETIVO GENERAL 14
1.3.2 OBJETIVOS ESPECÍFICOS 15
1.4 JUSTIFICACIÓN 15
CAPITULO II 16
MARCO REFERENCIAL 16
2.1 ANTECEDENTES 16
2.2 MARCO TEÓRICO 17
2.2.1 SEGURIDAD DE LA INFORMACIÓN 17
2.2.2 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) 17
2.2.3 PRINCIPIOS DE LA SEGURIDAD INFORMÁTICA 17
2.2.4 ANÁLISIS Y VALORACIÓN DE LOS RIESGOS 18
2.2.5 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 19
2.2.6 ESTÁNDARES DE SEGURIDAD 20
Norma ISO/IEC 27002:2022 ..... *20*
NIST 800-61 ..... *21*
2.2.7 ANÁLISIS DE SEGURIDAD INFORMÁTICA 28
2.2.8 COMITÉ DE SEGURIDAD DE LA INFORMACIÓN (CSI) 28
2.2.9 OFICIAL DE SEGURIDAD DE LA INFORMACIÓN (OSI) 29
2.2.10 ÁREA DE OPERACIONES Y SERVICIOS 29
2.2.11 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 30
2.3 MARCO LEGAL 30
2.3.1 CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR 30
2.3.2 LEY ORGÁNICA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA 30
2.3.3 LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS 30
2.3.4 NORMAS DE CONTROL INTERNO 31

2.3.5 LEY ESPECIAL DE TELECOMUNICACIONES....36
2.3.6 CÓDIGO ORGÁNICO INTEGRAL PENAL....36
2.3.7 LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES....37
2.3.8 ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN (EGSI)....37
CAPITULO III....38
MARCO METODOLÓGICO....38
3.1 DESCRIPCIÓN DEL ÁREA DE ESTUDIO....38
3.2 ENFOQUE Y TIPO DE INVESTIGACIÓN....41
3.3 PROCEDIMIENTO DE INVESTIGACIÓN....42
FASE 1: DIAGNÓSTICO SITUACIÓN ACTUAL....42
FASE 2: DISEÑO DE PLAN DE SEGURIDAD INFORMÁTICA....43
FASE 3: EVALUACIÓN DEL NIVEL DE CONFIDENCIALIDAD, DISPONIBILIDAD E INTEGRIDAD DE LA INFORMACIÓN....43
CAPITULO IV....46
RESULTADOS....46
4.1 ANÁLISIS DE LOS RESULTADOS DEL DIAGNÓSTICO....46
ENCUESTA A FUNCIONARIOS....46
4.2 PROPUESTA DEL DISEÑO DE PLAN DE SEGURIDAD INFORMÁTICA DEL GPI....56
4.3 EVALUACIÓN DE CONFIDENCIALIDAD, DISPONIBILIDAD E INTEGRIDAD DE LA INFORMACIÓN....69
APLICABILIDAD CONTROLES ISO 27002:2022....69
CONCLUSIONES Y RECOMENDACIONES....71
CONCLUSIONES....71
RECOMENDACIONES....71
BIBLIOGRAFÍA....73
ANEXOS....75
ANEXO 1: ISO/IEC 27002:2022....75
ANEXO 2: ENCUESTA SOBRE SEGURIDAD INFORMÁTICA EN EL GAD PROVINCIAL DE IMBABURA....87
ANEXO 3: APLICABILIDAD CONTROLES ISO 27002:2022....90

INDICE DE FIGURAS

Figura 1. Principios de la seguridad informática 17
Figura 2. Proceso para la Gestión del Riesgo de la Seguridad de la Información 19
Figura 3. Marco Ciberseguridad del NIST 21
Figura 4. Ciclo de Vida de Respuesta de Incidentes 21
Figura 5. Ubicación del GAD Provincial de Imbabura 38
Figura 6. Orgánico estructural del GPI 38
Figura 7. Fases de la investigación 42
Figura 8. Resultados Pregunta 1 46
Figura 9. Resultados Pregunta 2 46
Figura 10. Resultados Pregunta 3 47
Figura 11. Resultados Pregunta 4 48
Figura 12. Resultados Pregunta 5 48
Figura 13. Resultados Pregunta 6 49
Figura 14. Resultados Pregunta 7 50
Figura 15. Resultados Pregunta 8 50
Figura 16. Resultados Pregunta 9 51
Figura 17. Resultados Pregunta 10 52
Figura 18. Resultados Pregunta 11 52
Figura 19. Resultados Pregunta 12 53
Figura 20. Resultados Pregunta 13 53
Figura 21. Resultados Pregunta 14 54
Figura 22. Resultados Pregunta 15 55
Figura 23. Resultados Pregunta 16 55
Figura 24. Etapas del Plan de Seguridad 57

INDICE DE TABLAS

Tabla 1. Lista de verificación de manejo de incidentes 28
Tabla 2. Resumen de Normas de Control Interno para Tecnología de la Información 31
Tabla 3. Población de la Investigación 42
Tabla 4. Escala de Likert 59
Tabla 5. Valoración de Activos Subdirección de Tecnologías de Información 59
Tabla 6. Controles de la Norma ISO27002:2022 78
Tabla 7. Aplicabilidad Controles ISO 27002:2022 90

RESUMEN

En un mundo cada vez más dependiente de la tecnología, donde la información y los sistemas informáticos son fundamentales para el funcionamiento efectivo de las organizaciones, la seguridad informática se vuelve un pilar esencial para salvaguardar la integridad, confidencialidad y disponibilidad de la información. En este contexto, el análisis de la seguridad informática, especialmente en entidades gubernamentales como el Gobierno Provincial de Imbabura, se torna crucial. Este análisis, basado en las directrices de la Norma ISO/IEC 27002:2022 y el marco de NIST 800-61, se enfoca específicamente en el área de Operaciones y Servicios. Su propósito es evaluar, fortalecer y adecuar los protocolos de seguridad, adaptándolos a estándares internacionales reconocidos, a fin de identificar riesgos, proponer mejoras y establecer un marco de seguridad eficiente y alineado con las mejores prácticas internacionales en el ámbito de la seguridad informática para el Gobierno Provincial de Imbabura.

ABSTRACT

In a world increasingly dependent on technology, where information and computer systems are fundamental for the effective functioning of organizations, computer security becomes an essential pillar to safeguard the integrity, confidentiality and availability of information. In this context, the analysis of computer security, especially in government entities such as the Gobierno Provincial de Imbabura, becomes crucial. This analysis, based on the guidelines of ISO/IEC 27002:2022 and the NIST 800-61 framework, focuses specifically on the area of Operations and Services. Its purpose is to evaluate, strengthen and adapt security protocols, adapting them to recognized international standards, in order to identify risks, propose improvements and establish an efficient security framework aligned with the best international practices in the field of computer security for the Gobierno Provincial de Imbabura.

CAPITULO I

EL PROBLEMA

1.1 Problema de investigación

La seguridad informática es un aspecto crítico en la era digital y especialmente en el área de operaciones y servicios, donde la protección de datos y la privacidad son fundamentales. A pesar de la importancia de la seguridad informática, muchas organizaciones enfrentan desafíos para implementar medidas efectivas y garantizar la protección de sus sistemas y datos.

El funcionamiento efectivo de cualquier entidad ya sea pública o privada, en la actualidad está estrechamente ligado al nivel de tecnología que posea. La integración de la Tecnología de la Información en estas entidades es crucial para la gestión de la información, ya que en el contexto actual, el uso de la informática permite la automatización de procesos, el almacenamiento y la organización eficiente de datos, la realización de análisis y la toma de decisiones fundamentadas en información precisa, así como la facilitación de la comunicación tanto interna como externa mediante herramientas como el correo electrónico y las redes sociales.

Las redes informáticas desempeñan una función fundamental en la gestión, transferencia y recepción de datos. Por tanto, la configuración óptima de la red y la protección de la información se han convertido en aspectos primordiales debido al aumento de eventos provocados por terceros que intentan acceder a datos restringidos mediante diversos métodos de intrusión o violación de los controles de acceso a los recursos tecnológicos, así como al aprovechar los servicios ofrecidos por la red de manera indebida. En Ecuador poco a poco se ha ido poniendo mayor atención a los avances tecnológicos, permitiendo así que las redes sean un pilar fundamental, con el fin de proteger la información mediante metodologías de seguridad para su manejo, transmisión y recepción de manera segura y eficiente, así mismo permita que este recurso sea escalable y administrable. (Garcés, 2015)

La ausencia de directrices de seguridad dificulta el control adecuado de la gestión y los accesos a las plataformas de procesamiento de datos, lo que aumenta el riesgo de que la información sea utilizada de manera perjudicial para la empresa. De continuar bajo la misma línea de gestión con respecto a la seguridad, la empresa puede ser susceptible a

la ocurrencia de cualquier incidente de seguridad que perjudique las operaciones del negocio. (Bermudez, Kelly, Bailon, Edber, 2015)

La falta de capacitación adecuada y conciencia sobre seguridad informática entre el personal de la organización también puede ser un problema. Los errores humanos pueden ser una fuente importante de fallas de seguridad, y las organizaciones deben asegurarse de que todo su personal esté capacitado para manejar la seguridad informática y proteger los sistemas y datos del Gobierno Provincial de Imbabura (GPI).

La limitación de recursos financieros y tecnológicos puede ser un obstáculo para la implementación de medidas de seguridad más robustas. Las organizaciones no pueden tener acceso a las herramientas o tecnologías necesarias para garantizar una seguridad informática completa y efectiva.

1.2 Interrogantes de la investigación

¿Cuáles son los principales riesgos de seguridad informática que enfrenta el área de operaciones y servicios de una organización?

¿Cómo se puede aplicar la norma ISO/IEC 27002:2022 y el estándar NIST 800-61 para mejorar la seguridad informática en el área de operaciones y servicios?

¿Qué medidas se pueden implementar para prevenir y detectar ataques informáticos en el área de operaciones y servicios del GPI?

1.3 Objetivos de la investigación

1. Identificar los riesgos de seguridad informática que surgen en el área de operaciones y servicios del GPI.
2. Analizar cómo se pueden aplicar la norma ISO/IEC 27002:2022 y el estándar NIST 800-61 para mejorar la seguridad informática en el área de operaciones y servicios.
3. Evaluar la efectividad de las medidas de seguridad informática implementadas en el área de operaciones y servicios de la organización.

1.3.1 Objetivo general

Analizar la seguridad informática para mejorar la confidencialidad, integridad y disponibilidad de la información, basado en la Norma ISO/IEC 27002:2022 y NIST 800-61 para al área de operaciones y servicios del GPI.

1.3.2 Objetivos específicos

1. Diagnosticar la situación actual referente a la seguridad de la información del área de operaciones y servicios del GPI, identificando los activos, las vulnerabilidades existentes, las políticas y controles implementados, y la capacidad de respuesta ante incidentes de seguridad.

2. Diseñar un plan de seguridad informática con base a la norma ISO/IEC 27002:2022 y NIST 800-61.

3. Evaluar el nivel de confidencialidad, disponibilidad e integridad de la información en el GAD provincial de Imbabura.

1.4 Justificación

La seguridad informática en una necesidad primordial en las instituciones. Se conoce que la tecnología optimiza los procesos y acelera los servicios, pero también ha originado nuevas formas de delito, generalmente por intrusión indebida para obtener información o desvíos financieros electrónicos.

Los datos representan uno de los activos primordiales de cualquier entidad, y al mismo tiempo, son uno de los recursos más susceptibles a posibles vulnerabilidades, requiriendo así una protección frente a amenazas tanto internas como externas. En la era actual, las entidades y organizaciones demandan que la información que gestionan esté constantemente accesible, sin sufrir modificaciones en su integridad y manteniendo su fiabilidad.

Una infraestructura segura permitirá administrar los recursos de la red, así como preservar la integridad y disponibilidad de la información en la red, facilitando el uso compartido de archivos y dispositivos interconectados de manera controlada.

El GPI depende de su estructura tecnológica (redes, sistemas, hardware) para operar. Estos componentes trabajan en conjunto para garantizar que la institución pueda ofrecer un servicio eficiente y flexible a la comunidad de Imbabura en áreas como el procesamiento de pagos de tasas, la emisión de permisos ambientales y otras funciones similares.

CAPITULO II

MARCO REFERENCIAL

2.1 Antecedentes

A lo largo de los años, las instituciones u organizaciones han mostrado un enfoque predominante en el mejoramiento de sus sistemas informáticos, relegando la seguridad de la información a un segundo plano. Sin embargo, la evolución de los sistemas computacionales, internet y las comunicaciones en general ha generado una creciente conciencia sobre el valor de la información y la facilidad con la que se puede acceder a los datos, lo cual ha generado un mayor interés en la protección de la información. (Bermudez, Kelly, Bailon, Edber, 2015)

En la actualidad, resulta imprescindible que cualquier mejora implementada en los sistemas informáticos y en la gestión de la información física incluya criterios de seguridad de la información. (Bermudez, Kelly, Bailon, Edber, 2015) Es fundamental proteger y restringir el acceso a la información, impidiendo su exposición a personas no autorizadas a utilizarla. De esta manera, se garantiza la confidencialidad y la integridad de los datos, preservando su valor y minimizando los riesgos asociados a su utilización indebida. (Bermudez, Kelly, Bailon, Edber, 2015)

Uno de los expertos más reconocidos que ha promovido la idea de que la información es el activo más importante es Peter Drucker. El objetivo es garantizar que la información alojada en sus sistemas informáticos sea confiable, esté siempre disponible y se mantenga íntegra. (Bermudez, Kelly, Bailon, Edber, 2015) La incorporación de directrices de seguridad en los procesos críticos de la institución permitiría minimizar los posibles riesgos de fuga de información o manejo inadecuado de la misma. (Bermudez, Kelly, Bailon, Edber, 2015)

A continuación, se presentan los conceptos básicos a ser utilizados en el desarrollo de la investigación planteada, con el propósito de establecer un procedimiento coherente y coordinado de conceptos que contribuirán a una interpretación precisa de los resultados de la investigación. (Bermudez, Kelly, Bailon, Edber, 2015)

2.2 Marco teórico

2.2.1 Seguridad de la Información

Conjunto de medidas preventivas y reactivas de las instituciones y de los sistemas tecnológicos que permiten la preservación de la confidencialidad, integridad y disponibilidad de la información.(Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2020)

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

"El Sistema de Gestión de Seguridad de la Información es el elemento más importante de la norma ISO 27001, que unifica los criterios para la evaluación de los riesgos asociados al manejo de la información institucional." (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2020)

2.2.3 Principios de la Seguridad Informática

La seguridad de la información nace como un concepto cuyo objetivo es el de generar controles, medidas y procesos técnicos y humanos para proteger la información cumpliendo los tres principios de seguridad informática, también llamada la triada CID por sus siglas (Confidencialidad, Integridad y Disponibilidad). *(Fandom, 2021)*

Figura 1. Principios de la seguridad informática

Fuente: (Fandom, 2021)

Confidencialidad: Es la garantía de que la información no generada de la institución no está disponible o divulgada a personas, entidades o procesos no autorizados.

Integridad: Es la capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización. La información que disponemos es válida y consistente.

Disponibilidad: Es la garantía de que los servidores públicos y trabajadores autorizados tienen acceso a la información y a los activos asociados cuando lo requieren. (Gobierno Autónomo Descentralizado Provincial de Imbabura, 2023)

2.2.4 Análisis y Valoración de los Riesgos

Riesgo: Es la posibilidad de que una amenaza específica aproveche una vulnerabilidad para ocasionar una pérdida o daño en un activo de información. Se suele entender como una combinación entre la probabilidad de un evento y sus consecuencias.

Amenaza: Se refiere a una causa potencial de un incidente no deseado que pudiera resultar en un perjuicio para un sistema, persona u organización.

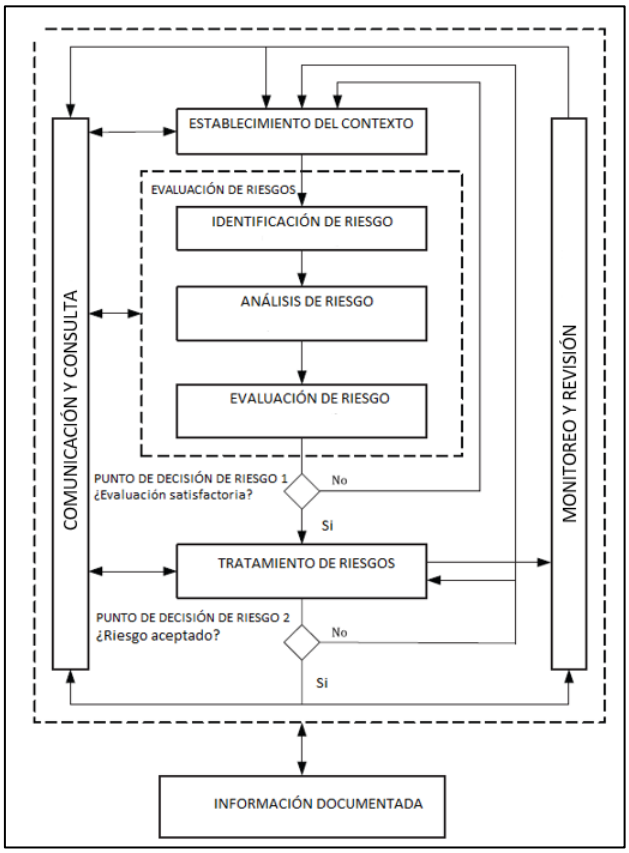
Vulnerabilidad: Se trata de una debilidad en un activo o control que puede ser explotada por una o más amenazas.

Impacto: Es el resultado o efecto que se produce cuando una amenaza se materializa y afecta a un activo. Este impacto puede implicar costos para la institución, ya sea en términos financieros o en aspectos como la reputación o implicaciones legales, entre otros.

Riesgo inherente: Este riesgo existe de manera intrínseca en cada actividad, sin que se hayan implementado controles.

Riesgo residual: Es el riesgo que persiste después de que se han aplicado medidas para mitigarlo.

Figura 2. Proceso para la Gestión del Riesgo de la Seguridad de la Información



Fuente: (ISO/IEC 27005, 2022)

2.2.5 Gestión de incidentes de seguridad de la información

"La gestión de la seguridad de la información y la identificación y tratamiento de sus respectivos riesgos traen consigo la necesidad de gestionar determinados eventos e incidentes de seguridad identificados. El oportuno tratamiento de incidentes de seguridad de la información permitirá tratar potenciales vulnerabilidades o brechas de seguridad, y al mismo tiempo dotar a la organización de una fuente de aprendizaje y consulta para robustecer todo sistema, programa, o modelo de seguridad de la información y ciberseguridad. Se referencia a las normas NIST SP 800-61 e ISO 27035 como fuentes de consulta para abordar una correcta de gestión de incidentes de seguridad de la información." (Gobierno Autónomo Descentralizado Provincial de Imbabura, 2023)

Mejor Práctica

Una norma de seguridad particular o una metodología que es ampliamente reconocida en la industria por ofrecer el enfoque más eficaz para una implementación específica de seguridad. Las mejores prácticas se establecen para asegurar que las características de seguridad de los sistemas utilizados con frecuencia estén configuradas y administradas

de forma coherente, garantizando un nivel constante de seguridad en toda la entidad. (Gobierno Autónomo Descentralizado Provincial de Imbabura, 2023)

Guía

Un guía es una declaración amplia empleada para recomendar o proponer un método para la implementación de políticas, estándares y buenas prácticas. Las guías o manuales son, en esencia, sugerencias que deben tenerse en cuenta al implementar medidas de seguridad. Aunque no son de cumplimiento obligatorio, se seguirán a menos que existan razones documentadas y aprobadas para no hacerlo. (Gobierno Autónomo Descentralizado Provincial de Imbabura, 2023)

Estándar

Directriz que detalla una acción o respuesta que debe seguirse ante una situación determinada. Las normas son pautas obligatorias destinadas a hacer cumplir las políticas establecidas. Están diseñadas para fomentar la aplicación de las políticas de nivel superior de la entidad antes de considerar la creación de nuevas políticas. (Gobierno Autónomo Descentralizado Provincial de Imbabura, 2023)

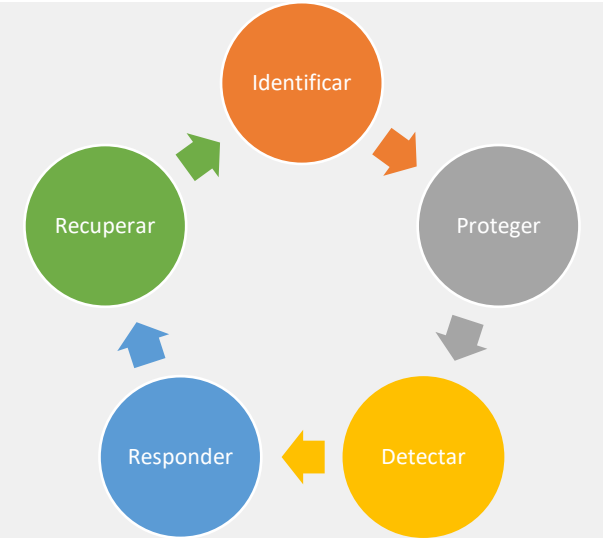
2.2.6 Estándares de seguridad

Norma ISO/IEC 27002:2022

Es una norma internacional que establece un conjunto de referencia de controles genéricos de seguridad de la información, incluida una guía de implementación. (International Organization for Standardization - ISO, 2022) “Este documento está diseñado para ser utilizado por organizaciones: a) dentro del contexto de un sistema de gestión de seguridad de la información (SGSI) basado en ISO/IEC27001; b) para implementar controles de seguridad de la información basados en las mejores prácticas reconocidas internacionalmente; c) para desarrollar directrices de gestión de la seguridad de la información específicas de la organización.” (International Organization for Standardization - ISO, 2022)

NIST 800-61

Figura 3. Marco Ciberseguridad del NIST

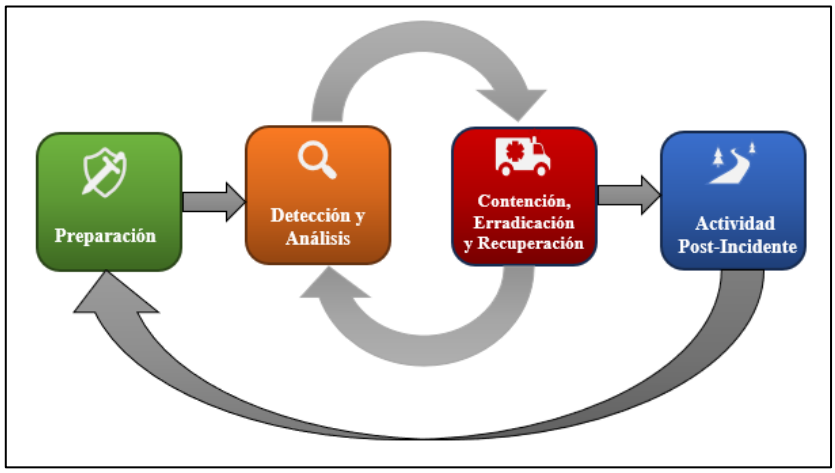


Fuente: Elaboración Propia

Es una guía de manejo de incidentes de seguridad informática la cual proporciona directrices para la manipulación incidente, en particular para el análisis de datos relacionadas con el incidente y determinar la respuesta apropiada a cada incidente. Las directrices se pueden seguir de forma independiente de plataformas específicas de hardware, sistemas operativos, protocolos o aplicaciones. (National Institute of Standards and Technology - NIST 800-61, 2012)

El proceso de respuesta a incidentes tiene varias fases:

Figura 4. Ciclo de Vida de Respuesta de Incidentes



Fuente: (Cichonski et al., 2012)

Tabla 1. Resumen de Proceso de Respuesta a Incidentes

PROCESO DE RESPUESTA A INCIDENTES		
1. Preparación	**1.1 Preparación para manejar incidentes:** Una organización debe tener múltiples mecanismos (separados y diferentes) de comunicación y coordinación en caso de falla de uno de los mecanismos.	**Comunicaciones e instalaciones del manejador de incidentes:** - Información de contacto - Información de guardia. - Mecanismos de notificación de incidentes. - Sistema de seguimiento de problemas. - Teléfonos inteligentes. - Software de cifrado. - Centro de Operaciones. - Instalación de almacenamiento seguro. - Estaciones de trabajo forenses digitales y/o dispositivos de respaldo. - Portátiles. - Estaciones de trabajo, servidores y equipos de red de repuesto, o sus equivalentes virtualizados. - Medios extraíbles en blanco. - Impresora portátil. - Rastreadores de paquetes y analizadores de protocolos. - Software forense digital. - Media removible. - Accesorios para la recogida de pruebas.
		Recursos de análisis de incidentes: - Listas de puertos. - Documentación. - Diagramas de red y listas de activos críticos. - Líneas de base actuales. - Hashes criptográficos. - Acceso a imágenes.
	1.2 Prevención de incidentes: Es vital mantener bajos los incidentes para proteger los procesos comerciales. Si fallan los mecanismos de seguridad, hay riesgo de más incidentes, sobrecargando al equipo. Esto podría causar demoras y respuestas deficientes, generando un impacto comercial negativo mayor, como daños extensos, periodos de servicio prolongados e inaccesibilidad de	**Prácticas recomendadas para proteger redes, sistemas y aplicaciones:** - Evaluaciones de riesgo. - Seguridad del anfitrión. - Seguridad de la red. - Prevención de malware. - Sensibilización y formación del usuario.

	datos.	
2. **Detección y Análisis**	**2.1 Vectores de Ataque:** Los incidentes pueden ser variados, lo que dificulta tener procedimientos detallados para todos. Las organizaciones deben estar preparadas para cualquier tipo de incidente, pero es crucial priorizar enfrentar los más comunes, ya que cada uno requiere una respuesta específica.	La lista de vectores de ataque; tácticas comunes de ataque que pueden servir como punto de partida para establecer procedimientos de manejo más detallados: - Dispositivos Externos / Extraíbles. - Ataques de Atrición. - Ataques Web. - Ataques por Correo Electrónico. - Suplantación de Identidad. - Uso Inadecuado. - Pérdida o Robo de Equipos.
	2.2 Señales de un incidente: La parte más difícil de responder a incidentes para muchas instituciones es identificar y evaluar con precisión posibles eventos adversos, determinando si ha ocurrido algún incidente y, de ser así, comprendiendo su naturaleza, alcance y gravedad.	
	2.3 Fuentes de precursores e indicadores: Se anticipan elementos y señales tempranas mediante diversas fuentes, como reportes de seguridad informática, registros, datos de acceso público y contribuciones individuales.	
	2.4 Análisis de Incidentes: La detección y análisis de incidentes serían simples si cada señal fuera precisa, pero esto no siempre es así. Los indicadores proporcionados por usuarios y sistemas de detección de intrusiones pueden generar falsos positivos, lo que dificulta la evaluación de la legitimidad de cada indicador.	Sugerencias para simplificar y mejorar la eficacia del análisis de incidentes: - Perfil de Redes y Sistemas. - Comprender los comportamientos normales. - Cree una política de retención de registros. - Realizar correlación de eventos. - Mantenga sincronizados todos los relojes del host o anfitrión. - Mantener y utilizar una base de conocimientos de información. - Utilice motores de búsqueda de Internet para realizar investigaciones. - Ejecute rastreadores de paquetes para recopilar datos adicionales. - Filtrar los datos. - Busque ayuda de otros.

	2.5 Documentación de incidentes: Un equipo de respuesta a incidentes debe registrar de inmediato todos los hechos relacionados con el incidente. Se puede utilizar un libro de registro, así como computadoras portátiles, grabadoras de audio y cámaras digitales para este fin.	Documentar eventos del sistema, conversaciones y cambios en archivos puede llevar a un manejo más eficiente, sistemático y menos propenso a errores. Cada paso desde la detección del incidente hasta su resolución debe estar documentado con una marca de tiempo y firmado por el responsable del incidente. Esta información puede utilizarse como prueba en un tribunal si se inicia un proceso legal. Es recomendable que los manejadores trabajen en equipos de al menos dos personas para garantizar una adecuada grabación y realización de tareas técnicas.
	2.6 Priorización de incidentes: La priorización en la gestión de incidentes es crucial, ya que no se deben abordar en el orden en que se presentan debido a limitaciones de recursos.	Se debe priorizar el manejo basándose en los elementos pertinentes, tales como: - Impacto funcional del incidente. - Información Impacto del Incidente. - Recuperabilidad del Incidente.
	2.7 Notificación de incidentes: Al evaluar y priorizar un incidente, el equipo de respuesta debe comunicarse con precisión con las personas relevantes para garantizar su participación oportuna en sus roles respectivos. Las directrices de respuesta a incidentes deben incluir disposiciones sobre la notificación de incidentes, especificando qué información debe comunicarse a quién y cuándo.	Los requisitos de presentación de informes varían entre instituciones, aunque los destinatarios de la notificación abarcan: - CIO (Chief Information Officer) - Director de información. - Jefe de seguridad de la información. - Oficial de seguridad de la información local. - Otros grupos de respuesta a incidentes internos de la institución. - Equipos de respuesta a incidentes externos (si corresponde). - Propietario del sistema. - Departamento de Recursos Humanos (en situaciones que implican a miembros del personal, como acoso por correo electrónico). - Asuntos públicos (para incidentes que puedan generar publicidad). - Departamento legal (para incidentes con posibles ramificaciones legales). - Aplicación de la ley (si corresponde).
3. Contención, Erradicación y Recuperación	**3.1 Elección de una estrategia de contención:** Es esencial controlar la situación antes de que un incidente se vuelva inmanejable o cause más daños.	Los factores que guían la selección de la estrategia adecuada abarcan: - Potencial de daño y riesgo de pérdida de recursos.

	La contención es crucial en la mayoría de los casos y debe ser considerada en cada situación. Proporciona el tiempo necesario para planificar una estrategia de corrección adecuada. La toma de decisiones, como apagar un sistema o desconectarlo de la red, es un aspecto clave de la contención.	- Importancia de preservar pruebas y evidencia. - Disponibilidad de servicios (como conectividad de red y servicios ofrecidos a partes externas). - Tiempo y recursos requeridos para implementar la estrategia. - Eficiencia de la estrategia (por ejemplo, contención parcial o total). - Duración de la solución (por ejemplo, una solución provisional de emergencia que se desactivará en cuatro horas, una solución temporal que se eliminará en dos semanas, una solución permanente).
4. Actividad Post-Incidente	**4.1 Lecciones aprendidas:** El aprendizaje y la mejora continua son aspectos fundamentales, pero a menudo descuidados en la respuesta a incidentes. Cada equipo debe adaptarse a nuevas amenazas, tecnologías mejoradas y lecciones aprendidas. Organizar sesiones de "lecciones aprendidas" después de incidentes significativos, y opcionalmente periódicamente tras incidentes menores, puede fortalecer las medidas de seguridad y optimizar el proceso de gestión de incidentes. Estas reuniones ofrecen la oportunidad de revisar lo sucedido, las intervenciones realizadas y su efectividad, y deben celebrarse dentro de varios días después de finalizado el incidente.	Las preguntas a abordar durante la reunión comprenderán: - ¿Cuál fue la secuencia exacta de eventos y su cronología? - ¿Cómo respondieron tanto el personal como la dirección al manejar el incidente? ¿Se siguieron los procedimientos establecidos y fueron adecuados? - ¿Qué información se hubiera requerido con antelación? - ¿Se tomaron medidas que pudieron obstaculizar la recuperación? - ¿Qué cambios harían el personal y la dirección si se enfrentaran a un incidente similar en el futuro? - ¿De qué manera se puede potenciar la transmisión de información con otras entidades? - ¿Qué acciones correctivas podrían ser adoptadas para prevenir situaciones análogas? - ¿Qué signos o elementos de alerta deben ser vigilados para detectar posibles incidentes futuros? - ¿Qué otros instrumentos o recursos se necesitan para reconocer, examinar y contrarrestar futuros incidentes?
	4.2 Uso de datos de incidentes recopilados: Las actividades de lecciones	**Cantidad de incidentes atendidos:** Es importante recordar que la cantidad de

	aprendidas deben generar datos objetivos y subjetivos sobre cada incidente. Estudiar las características de los incidentes puede revelar debilidades y amenazas de seguridad sistémicas, así como cambios en las tendencias de los incidentes. Además, los datos pueden usarse para medir el éxito del equipo de respuesta a incidentes, siempre que se recolecten y almacenen adecuadamente.	incidentes manejados no siempre refleja un mejor desempeño. Por ejemplo, una disminución en el número de incidentes manejados puede ser resultado de mejoras en los controles de seguridad, no necesariamente de una falta de diligencia por parte del equipo de respuesta a incidentes.
		Duración de cada incidente: El tiempo dedicado a cada incidente puede evaluarse de diversas maneras, como la cantidad total de horas dedicadas al manejo, el tiempo transcurrido desde el inicio hasta la detección, evaluación del impacto inicial y cada fase del proceso, incluyendo contención, recuperación, y el tiempo empleado por el equipo para informar a la dirección y, si es necesario, a terceros externos como US-CERT[1].
		Evaluación objetiva de cada incidente: Después de resolver un incidente, es importante realizar un análisis objetivo de la respuesta para determinar su efectividad. Esto implica revisar registros y documentación de incidentes para verificar el cumplimiento de políticas y procedimientos, identificar precursores e indicadores del incidente, determinar el daño causado antes de su detección, identificar la causa real y el vector de ataque, calcular el daño monetario estimado, medir la diferencia entre la evaluación de impacto inicial y final, e identificar medidas que podrían haber prevenido el incidente.
		Evaluación subjetiva de cada incidente: Los miembros del equipo de respuesta a incidentes pueden evaluar su propio rendimiento y el de sus colegas, así como la efectividad general del equipo. También es crucial considerar la opinión del propietario del recurso afectado para determinar si considera que el incidente se manejó eficientemente y si

1 US-CERT Equipo de preparación para emergencias informáticas de los Estados Unidos

		el resultado fue satisfactorio.
	4.3 Retención de pruebas: Es crucial que las organizaciones establezcan directrices sobre el período de retención de evidencia relacionada con un incidente. La mayoría opta por conservar toda la evidencia durante períodos que pueden extenderse durante meses o incluso años después de la resolución del incidente.	**Procesamiento:** En situaciones en las que sea viable procesar al atacante, es posible que sea necesario preservar las pruebas hasta que todas las acciones legales hayan concluido, lo que podría llevar varios años. Además, la evidencia que inicialmente parece trivial podría volverse crucial en el futuro. Por ejemplo, si un atacante utiliza información obtenida en un primer ataque para realizar un segundo ataque más grave, la evidencia del primer incidente podría ser fundamental para comprender el desarrollo del segundo.
		Retención de datos: La mayoría de las entidades tienen políticas establecidas para la retención de diferentes tipos de información. Por ejemplo, los correos electrónicos pueden ser conservados por un período de 180 días. En el caso de una imagen de disco con miles de correos electrónicos, la entidad podría decidir no retenerla más allá de dicho plazo, a menos que sea absolutamente necesario.
		Costo: Aunque los componentes originales y los medios de almacenamiento para imágenes de disco pueden ser económicos individualmente, el costo de almacenar grandes cantidades de estos componentes durante largos períodos puede ser considerable para una organización. Además, la organización también debe tener computadoras funcionales que puedan utilizar este hardware y medios almacenados.

Fuente: (National Institute of Standards and Technology - NIST 800-61, 2012)

5. Lista de verificación para el manejo de incidentes

La lista de verificación en la Tabla 2 proporciona los pasos principales que se deben realizar en el manejo de un incidente. Tenga en cuenta que los pasos reales realizados pueden variar según el tipo de incidente y la naturaleza de los incidentes individuales.

Tabla 2. Lista de verificación de manejo de incidentes

	ACCIÓN		TERMINADO
Detección y Análisis			
1	Determinar si ha ocurrido un incidente		
	1.1	Analizar los precursores e indicadores.	
	1.2	Busque información correlativa.	
	1.3	Realizar investigaciones (por ejemplo, motores de búsqueda, base de conocimientos)	
	1.4	Tan pronto como el responsable crea que ha ocurrido un incidente, comience a documentar la investigación y a reunir pruebas.	
2	Priorizar el manejo del incidente en función de los factores relevantes (impacto funcional, impacto de la información, esfuerzo de recuperabilidad, etc.)		
3	Informar el incidente al personal interno apropiado y a las organizaciones externas.		
Contención, Erradicación y Recuperación			
4	Adquirir, preservar, proteger y documentar evidencia.		
5	Contener el incidente.		
6	Erradicar el incidente.		
	6.1	Identificar y mitigar todas las vulnerabilidades que fueron explotadas.	
	6.2	Eliminar malware, materiales inapropiados y otros componentes.	
	6.3	Si se descubren más hosts afectados (por ejemplo, nuevas infecciones de malware), repita los pasos de Detección y Análisis (1.1, 1.2) para identificar todos los demás hosts afectados, luego contenga (5) y erradique (6) el incidente.	
7	Recuperarse del incidente.		
	7.1	Devolver los sistemas afectados a un estado operativo listo.	
	7.2	Confirmar que los sistemas afectados están funcionando normalmente.	
	7.3	Si es necesario, implementar un seguimiento adicional para buscar actividades futuras relacionadas.	
Actividad Post-Incidente			
8	Crear un informe de seguimiento.		
9	Celebrar una reunión de lecciones aprendidas (obligatoria en el caso de incidentes importantes, opcional en caso contrario).		

Fuente: (Cichonski et al., 2012)

2.2.7 Análisis de Seguridad Informática

La evaluación exhaustiva de los sistemas, redes y procesos de una organización para identificar vulnerabilidades y amenazas a la seguridad. Esto ayuda a comprender los riesgos y tomar medidas preventivas.

2.2.8 Comité de Seguridad de la Información (CSI)

Es el comité responsable de la confiabilidad, disponibilidad e integridad de la información de los activos de información que tiene el GPI mediante la aprobación de políticas de seguridad y la implementación del esquema de seguridad de la información. (Gobierno Autónomo Descentralizado Provincial de Imbabura, 2023)

- **Compromiso del Comité de Seguridad de la Información (CSI)**

  El Comité de Seguridad de la Información encabezado por la máxima autoridad del GPI, declaran ser responsables con la información, un bien catalogado como el activo más importante dentro de la institución, por lo tanto, manifiestan su total compromiso con el establecimiento, implementación y gestión de un Sistema de Seguridad de la Información que incluye el diseño e implementación de un plan de continuidad y recuperación ante desastres.

  - El CSI demostrará su compromiso a través de:
  - La revisión y aprobación de las políticas contenidas en este documento.
  - La socialización de estas políticas a todos los servidores públicos y trabajadores del GPI.
  - El aseguramiento de los recursos adecuados para implementar y mantener las políticas de Seguridad de la Información. (Gobierno Autónomo Descentralizado Provincial de Imbabura, 2023)

2.2.9 Oficial de Seguridad de la Información (OSI)

El Oficial de Seguridad de Seguridad de la Información, será el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento del Esquema Gubernamental de Seguridad de la Información. Es recomendable que el oficial de Seguridad de la Información sea un miembro independiente de las áreas de tecnología o sistemas, puesto que deberá mantener su independencia para observar las necesidades de seguridad entre la estrategia de la institución y tecnología. (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2020)

2.2.10 Área de Operaciones y Servicios

La sección de una organización responsable de mantener y entregar productos o servicios. Esta área puede ser vulnerable a amenazas cibernéticas debido a su importancia operativa y acceso a información sensible.

2.2.11 Políticas de seguridad de la información

Las políticas de seguridad de la información son un conjunto de directrices establecidas por una organización para proteger y salvaguardar la información sensible y crítica, y para minimizar los riesgos de seguridad.

2.3 Marco legal

2.3.1 Constitución de la República del Ecuador

En la constitución ecuatoriana se estipula los principios por los cuales han sido creadas todas las leyes. Como también establece" El Estado garantizará que los servicios públicos y su provisión respondan a los principios de obligatoriedad, generalidad, uniformidad, eficiencia, responsabilidad, universalidad, accesibilidad, regularidad, continuidad y calidad. (Constitución de la República del Ecuador, 2021)

2.3.2 Ley Orgánica de Transparencia y Acceso a la Información Pública

"La Ley Orgánica de Transparencia y Acceso a la Información Pública en el Registro Oficial Suplemento 337 del 18 de mayo del 2004 se basa en los artículos 18,91 y 92 de nuestra Constitución que garantizan el derecho de los ciudadanos a buscar, recibir, intercambiar, producir o difundir información con responsabilidad sobre sí misma, o sobre sus bienes existente en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas." (Ley Orgánica de Transparencia y Acceso a la Información Pública, 2023)

2.3.3 Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

Respecto de la Confidencialidad y reserva, reglamenta que: "Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta ley y demás normas que rigen la materia. (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, 2002)

2.3.4 Normas de Control Interno

Normas generales y otras específicas relacionadas con la administración financiera gubernamental, talento humano, tecnología de la información y administración de proyectos. (Contraloría General del Estado, 2023)

Tabla 3. Resumen de Normas de Control Interno para Tecnología de la Información

410 TECNOLOGÍA DE LA INFORMACIÓN	
410-01 Organización de la unidad de tecnologías de la información y comunicaciones	El enfoque de seguridad de la información para la unidad de tecnologías de la información y comunicaciones en entidades del sector público se centra en: 1. Establecer un marco de trabajo transparente y controlado. 2. Crear una unidad dedicada para regular y estandarizar temas tecnológicos. 3. Posicionar esta unidad en un nivel que permita asesoría y liderazgo. 4. Garantizar independencia y cobertura de servicios a todas las unidades. 5. Mantener una estructura organizacional flexible y ajustada a necesidades. 6. Contar con áreas mínimas que cubran proyectos, infraestructura, soporte y seguridad. 7. Incorporar un oficial de seguridad de la información independiente para un control adicional.
410-02 Comité de Tecnologías de la Información y Comunicaciones	El Comité de Tecnologías de la Información y Comunicaciones, designado por la máxima autoridad de la entidad, coordina lineamientos y objetivos para proyectos de TIC. Sus integrantes, provenientes de áreas clave, garantizan una perspectiva integral. Este comité promueve la integración interdepartamental, asegura la alineación con la estrategia institucional y fomenta la innovación y mejora continua en el uso de las TIC.
410-03 Segregación de funciones	El enfoque de segregación de funciones en el ámbito de la seguridad de la información reside en: 1. Definir y comunicar claramente las funciones y responsabilidades del personal. 2. Garantizar una adecuada segregación de funciones para evitar conflictos. 3. Supervisar y gestionar roles y funciones, promoviendo rotaciones periódicas. 4. Documentar y aprobar descripciones de puestos de trabajo para evaluar el desempeño y reducir la

	dependencia de personal clave. 5. Asegurar el cumplimiento de funciones del Oficial de Seguridad de la Información según la normativa vigente.
410-04 Plan estratégico y operativo de tecnologías de la información y comunicaciones	El plan estratégico y operativo de tecnologías de la información y comunicaciones se centra en: 1. Alinear los recursos tecnológicos con los objetivos institucionales y gubernamentales. 2. Detallar análisis de situación, propuestas de mejora y participación de unidades. 3. Incluir componentes como estructura, procesos, presupuesto y consideraciones legales. 4. Alinear planes operativos con el estratégico, actualizándolos periódicamente. 5. Aprobar, monitorear y evaluar los planes, tomando medidas correctivas según sea necesario. 6. Realizar adquisiciones de tecnología alineadas con los proyectos del plan estratégico y obtener autorización para excepciones.
410-05 Políticas y procedimientos	Las políticas y procedimientos de seguridad de la información se centran en: 1. Aprobación y organización por la máxima autoridad. 2. Definición, documentación y difusión por parte de la unidad de tecnologías de la información y comunicaciones. 3. Alineamiento con leyes y estándares, abarcando diversas áreas de tecnología de información y comunicaciones. 4. Promoción de convenios para intercambio de información y servicios con otras organizaciones.
410-06 Clasificación y arquitectura de la información	Para la seguridad de la información, se establece un proceso de clasificación de datos y diseño de arquitectura que: 1. Clasifica datos según niveles de seguridad y propiedad. 2. Garantiza disponibilidad, integridad y exactitud de los datos. 3. Documenta la arquitectura en un diccionario de datos actualizado. 4. Facilita la incorporación transparente de aplicaciones y procesos institucionales.
410-07 Administración de proyectos tecnológicos	La administración de proyectos tecnológicos se centra en: 1. Documentar y justificar el proyecto. 2. Establecer un cronograma detallado. 3. Evaluar el Costo Total de Propiedad. 4. Definir claramente responsabilidades. 5. Seguir fases específicas del proyecto.

	6. Identificar y gestionar riesgos. 7. Monitorear avances y realizar informes. 8. Controlar cambios y asegurar calidad. 9. Formalizar el cierre con pruebas y aceptación.
410-08 Desarrollo, mantenimiento y adquisición de software de aplicación	Las ideas clave para el desarrollo, mantenimiento y adquisición de software son: 1. Regular los procesos de desarrollo, mantenimiento y adquisición. 2. Adoptar políticas y estándares internacionales. 3. Identificar y priorizar requerimientos institucionales. 4. Especificar criterios de aceptación y análisis de riesgos. 5. Considerar estándares de desarrollo, calidad y seguridad. 6. Establecer contratos detallados para garantizar cumplimiento. 7. Autorizar y revisar servicios externos de desarrollo. 8. Garantizar derechos de autor y entrega de código fuente. 9. Registrar derechos de autor y obtener licencias. 10. Implementación personalizada y realizar pruebas exhaustivas. 11. Formalizar aceptación por parte de usuarios. 12. Estabilizar y revisar conformidades. 13. Controlar versiones y elaborar manuales. 14. Difundir, publicar y actualizar manuales permanentemente.
410-09 Adquisiciones de infraestructura tecnológica	Las adquisiciones de infraestructura tecnológica incluyen: 1. Alineación con estándares y objetivos de la organización. 2. Justificación, análisis de costos y evaluación de riesgos. 3. Detalles completos en contratos, incluyendo garantías. 4. Especificaciones formales sobre seguridad en contratos de servicios. 5. Previsión de disponibilidad de programas fuente. 6. Análisis de riesgos y clasificación de información para contratación en la "nube". 7. Respaldo seguro de información antes de bajas de equipamiento o finalización de contratos.
410-10 Mantenimiento, actualización y control de la infraestructura tecnológica	El mantenimiento, actualización y control de la infraestructura tecnológica incluye: 1. Definición de procedimientos de mantenimiento y actualización de software. 2. Registro y autorización previa de cambios en procedimientos y sistemas. 3. Control de versiones del software en producción. 4. Actualización continua de manuales técnicos y de usuario.

	5. Establecimiento de ambientes de desarrollo y producción independientes. 6. Elaboración de un plan de mantenimiento preventivo y correctivo. 7. Control de activos informáticos mediante un inventario actualizado. 8. Mantenimiento de bienes en garantía por parte del proveedor.
410-11 Seguridad de tecnología de información	La seguridad de la tecnología de la información incluye: ° Cumplimiento de normativas de protección de datos y propiedad intelectual. ° Uso de estándares y plataformas del sector público. ° Alineación con objetivos organizacionales y calidad de servicio. ° Inclusión en planes institucionales y excepciones aplicables. ° Implementación de política de seguridad basada en normativas vigentes.
410-12 Plan de contingencias	La unidad de tecnologías de la información y comunicaciones debe desarrollar un plan de contingencias que aborde: 1. Respuesta a riesgos con asignación de roles críticos. 2. Procedimientos de control de cambios para mantener actualizado el plan. 3. Continuidad de operaciones con centro de cómputo alterno y recuperación de datos. 4. Recuperación de desastres con actividades previas, durante y después del evento. 5. Designación de un comité y responsables de ejecución. 6. El plan es confidencial y describe procedimientos en caso de emergencia. 7. Se difunde entre el personal y se somete a pruebas y evaluaciones periódicas.
410-13 Administración de soporte de tecnología de información	La unidad de tecnologías de la información y comunicaciones debe establecer procedimientos para la gestión del soporte tecnológico, abordando: 1. Revisiones periódicas de capacidad y desempeño. 2. Seguridad mediante identificación única de usuarios. 3. Estandarización de identificación, autenticación y autorización. 4. Revisiones regulares de cuentas y privilegios de usuarios. 5. Medidas contra software malicioso y virus. 6. Definición y manejo de niveles de servicio.

	7. Alineación de servicios con requerimientos de la organización. 8. Administración de incidentes y solicitudes de servicio. 9. Implementación de mecanismos para seguimiento de trámites administrativos. 10. Mantenimiento de repositorio actualizado de configuraciones de hardware y software. 11. Gestión adecuada de información, librerías de software y respaldos. 12. Incorporación de mecanismos de seguridad para protección de información sensible.
410-14 Monitoreo y evaluación de los procesos y servicios	El Monitoreo y evaluación de los procesos y servicios incluye: 1. Establecer un marco de trabajo de monitoreo para evaluar el impacto de la tecnología de información en la entidad. 2. Definir indicadores de desempeño y métricas para monitorear la gestión. 3. Ejecutar procedimientos para medir la satisfacción de los clientes internos y externos. 4. Presentar informes periódicos de gestión a la alta dirección para identificar acciones correctivas y de mejora.
410-15 Portal web, servicios telemáticos e intranet	El Portal web, servicios telemáticos e intranet incluye: 1. Elaborar normas, procedimientos e instructivos para servicios telemáticos, intranet, correo electrónico y portal web. 2. Cumplir con disposiciones legales y considerar los requerimientos de usuarios externos e internos. 3. Desarrollar aplicaciones web y/o móviles para automatizar procesos y trámites.
410-16 Capacitación relacionada a las tecnologías de la información y comunicaciones	La capacitación relacionada a las tecnologías de la información y comunicaciones se centra en: 1. Identificar y documentar necesidades de capacitación del personal en tecnologías de la información. 2. Establecer temas obligatorios y continuos en el Plan de Capacitación. 3. Involucrar a la unidad de tecnologías de la información y comunicaciones y de talento humano en esta tarea. 4. Dirigir la capacitación tanto al personal técnico como a los usuarios de las áreas administrativas y operativas.
410-17 Firmas electrónicas	Las principales consideraciones para la seguridad de la información en relación con las firmas electrónicas son: 1. Verificación de autenticidad: Se requieren certificados de entidades acreditadas para garantizar la autenticidad de

	las firmas electrónicas. 2. Conservación de archivos: Los archivos firmados deben conservarse en su estado original usando medios que garanticen su autenticidad, integridad y disponibilidad a largo plazo. 3. Actualización de datos de certificados: Los usuarios deben informar cualquier cambio en los datos relacionados con los certificados. 4. Seguridad de certificados y dispositivos: Los titulares deben proteger adecuadamente sus certificados y dispositivos, y solicitar la revocación en caso de compromiso. 5. Renovación de certificados: Los usuarios deben renovar sus certificados a tiempo para garantizar su vigencia y validez. 6. Capacitación en seguridad: Las entidades públicas deben capacitar a sus servidores sobre las medidas de seguridad y responsabilidades en el uso de firmas electrónicas, según la normativa vigente.

Fuente: (Contraloría General del Estado, 2023)

2.3.5 Ley Especial de Telecomunicaciones

El artículo 76 de la Ley Orgánica de Telecomunicaciones en referencia a las medidas técnicas de seguridad e invulnerabilidad dispone que "Las y los prestadores de servicios ya sea que usen red propia o la de un tercero, deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios y la invulnerabilidad de la red y garantizar el secreto de las comunicaciones y de la información transmitida por sus redes. Dichas medidas garantizarán un nivel de seguridad adecuado al riesgo existente. (Ley Especial de Telecomunicaciones, 2015)

2.3.6 Código Orgánico Integral Penal

"La Sección Tercera del Código Orgánico Integral Penal, COIP, respecto de los Delitos contra la seguridad de los activos de los sistemas de información y comunicación, establece sanciones con pena privativa de libertad para delitos como la revelación ilegal de base de datos, interceptación ilegal de datos, transferencia electrónica de activo patrimonial, ataque a la integridad de sistemas informáticos, delitos contra la información pública reservada legalmente, y el acceso no consentido a

un sistema informático, telemático o de telecomunicaciones;" (Código Orgánico Integral Penal, 2014).

2.3.7 Ley Orgánica de Protección de Datos Personales

"El artículo 38 de la Ley Orgánica de Protección de Datos Personales respecto de las medidas de seguridad en el ámbito del sector público, dispone que el mecanismo gubernamental de seguridad de la información deberá incluir las medidas que deben implementarse en el caso de tratamiento de datos personales para hacer frente a cualquier riesgo, amenaza, vulnerabilidad, accesos no autorizados, pérdidas, alteraciones, destrucción o comunicación accidental o ilícita en el tratamiento de los datos conforme al principio de seguridad de datos personales;" (Asamblea Nacional del Ecuador, 2021). (Ley Orgánica de Protección de Datos Personales, 2021).

2.3.8 Esquema Gubernamental de Seguridad de la Información (EGSI)

"Art. 5.- La máxima autoridad designara al interior de su institución, un Comité de Seguridad de la Información (CSI), que estará integrado por los responsables de las siguientes áreas o quienes hagan sus veces: Talento Humano, Administrativa, Planificación y Gestión estratégica, Comunicación Social, Tecnologías de Información, Unidades Agregadoras de Valor y el Área Jurídica participara como asesor. (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2019)

CAPITULO III

MARCO METODOLÓGICO

3.1 Descripción del área de estudio

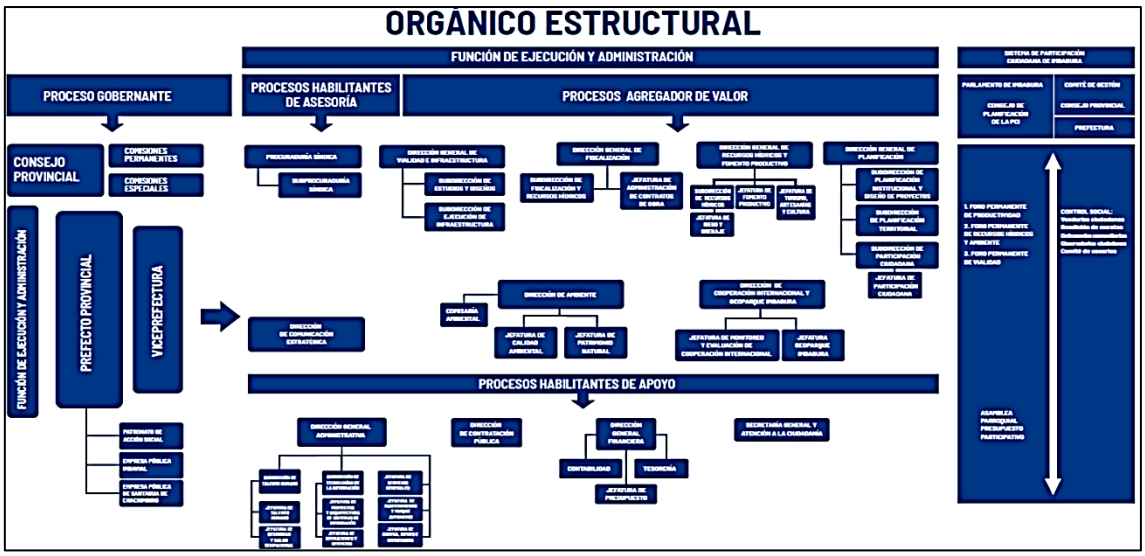
La presente investigación se llevó a cabo en el Gobierno Provincial de Imbabura (GPI), las instalaciones del edificio principal se encuentran ubicadas en la calle Bolívar y Oviedo esquina del cantón Ibarra de la provincia de Imbabura.

Figura 5. Ubicación del GAD Provincial de Imbabura

Fuente: Tomado de Google Maps (2023)

Orgánico Estructural

Figura 6. Orgánico estructural del GPI



Fuente: Talento Humano del GPI 2023

Misión institucional

El GAD Provincial de Imbabura es la institución encargada de coordinar, planificar, ejecutar y evaluar el Plan de Desarrollo Provincial Participativo; fortaleciendo la productividad, la vialidad, el manejo adecuado de sus recursos naturales y promoviendo la participación ciudadana; a fin de mejorar la calidad de vida de sus habitantes. (Gobierno Autónomo Descentralizado Provincial de Imbabura)

Visión institucional

El GAD Provincial de Imbabura, se consolida como una institución de derecho público autónoma, descentralizada, transparente, eficiente, equitativa, incluyente y solidaria, líder del desarrollo económico, social y ambiental provincial.

Como grupo de estudio se ha determinado el área de Operaciones y Servicios de la Subdirección de Tecnologías de Información. (Gobierno Autónomo Descentralizado Provincial de Imbabura)

Estructura y Procesos Gestión de TI

Según el estatuto orgánico por procesos vigente se establece:

Misión

Proveer y garantizar los servicios de tecnologías de la información de calidad, confiables y con alta disponibilidad en apoyo al cumplimiento de los objetivos estratégicos de la entidad. (Gobierno Autónomo Descentralizado Provincial de Imbabura, 2016)

Atribuciones y Responsabilidades de la Subdirección de Tecnologías de la Información.

- Asesorar a las autoridades, directivos y servidores de la institución en temas de computación, informática y comunicaciones.
- Dirigir y evaluar la gestión de la Subdirección de Tecnologías de la Información.
- Coordinar la implementación de sistemas de información y tecnológicos y organizacionales de la entidad.
- Proponer políticas para la gestión de los recursos tecnológicos.

- Poner a consideración y aprobación de la máxima autoridad los planes tecnológicos y de contingencia institucional.
- Dirigir, elaborar, coordinar y evaluar el Plan Operativo Anual y el Plan Anual de Compras de la dirección,
- Evaluar la calidad de productos y servicios tecnológicos para la generación de un Plan de Mejoramiento Continuo de la institución.
- Coordinar la ejecución de los planes tecnológicos de contingencia institución,
- Asesorar a los niveles Directivos en los procesos de adquisición, mantenimiento y reemplazo de equipos de computación y comunicación,
- Para todos los bienes tecnológicos Identificar y registrar los bienes tecnológicos y de comunicación para la prestación de servicios incluidos los de software de base o de aplicación y versiones de actualización.
- Las demás funciones delegadas por el Prefecto o Prefecta Provincial. (Gobierno Autónomo Descentralizado Provincial de Imbabura, 2016)

Productos y Servicios de la Subdirección de Tecnologías de la Información

- Plan Informático Estratégico de Tecnología.
- Políticas y procedimientos de organización de tecnología.
- Plan de Contingencias.
- Procedimientos de Operación.
- Plan de Capacitación Tecnológico Anual.
- Políticas y reglamentación para el cumplimiento de Normas de Control Interno.

Servicios de infraestructura, redes y comunicaciones. (Gobierno Autónomo Descentralizado Provincial de Imbabura, 2016)

Jefatura de Operaciones y Servicios

Atribuciones y Responsabilidades Jefatura de Operaciones y Servicios

- Apoyar en la elaboración de presupuestos para proyectos que impliquen adquisición o arrendamiento de equipos tecnológicos.
- Garantizar que la prestación de servicios de Tecnologías de la Información cumpla con los niveles de servicio acordados.
- Solucionar y documentar los problemas en sistemas y servicios.
- Diseñar e implementar mecanismos de protección de información, seguridad y control de los sistemas informáticos.

- Controlar y mantener en correcto funcionamiento la red de datos y comunicaciones.
- Las demás funciones delegadas por el Director (a) General de Tecnologías de la Información. (Gobierno Autónomo Descentralizado Provincial de Imbabura, 2016)

Productos y Servicios:

- Normas, procedimientos e instructivos de instalación, configuración y utilización de varios sistemas.
- Cableados, equipos, hardware y software instalados y en funcionamiento.
- Servicios de soporte técnico a los usuarios y mantenimiento de los equipos.
- Inventario de hardware de la institución.
- Inventario de contratos de licencias de software, servicios de internet y telefonía. (Gobierno Autónomo Descentralizado Provincial de Imbabura, 2016)

3.2 Enfoque y tipo de investigación

La investigación se iniciaría con un enfoque exploratorio, ya que se busca recopilar toda la información necesaria que servirá como base para las etapas subsiguientes. Posteriormente, se adoptará un enfoque cualitativo para analizar la situación actual referente a la seguridad de la información del área de operaciones y servicios del Gobierno Provincial de Imbabura. Para cumplir con los objetivos planteados es necesario identificar los requisitos para el diseño del esquema del plan de seguridad informática en base a los controles de la norma ISO/IEC 27002:2022 y NIST 800-61 y la evaluación de confidencialidad, disponibilidad e integridad de la información en el GAD Provincial de Imbabura.

Población y Muestra

Población considerada para este caso de estudio son 10 profesionales de la Subdirección de Tecnologías de Información la cual tiene como misión proveer y garantizar los servicios de tecnologías de la información de calidad, confiables y con alta disponibilidad en apoyo al cumplimiento de los objetivos estratégicos (Gobierno Autónomo Descentralizado Provincial de Imbabura, 2016) del GAD Provincial de Imbabura. Dado que poseen la experiencia y conocimientos necesarios para llevar a

cabo cada uno de los procesos en su área, se considera que son los más idóneos para esta evaluación.

Tabla 4. Población de la Investigación

POBLACIÓN	CANTIDAD
Subdirectora de Tecnologías de Información	1
Oficial de Seguridad Informática	1
Funcionarios área Operaciones y Servicios	4
Funcionarios área de Software y Web	4
TOTAL	**10**

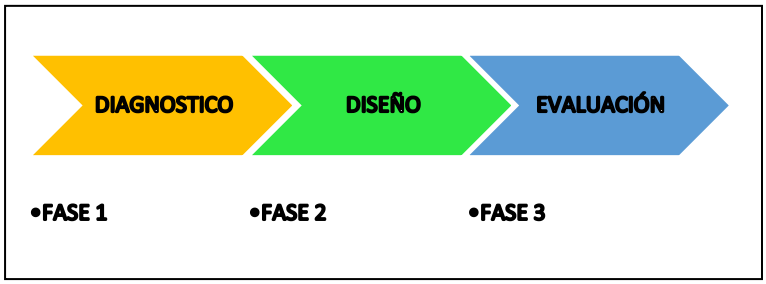
Fuente: Elaboración Propia

No fue preciso tomar una muestra dada la pequeña dimensión de la población. Se tomó en cuenta la idea expresada por Hernández et al. (2014): "es el conjunto de todos los casos que concuerdan con una serie de especificaciones" (p. 174). En el mismo sentido, Sánchez et al. (2020) definen una muestra como "un grupo de elementos seleccionados con la intención de averiguar algo sobre una población determinada" (p. 23), añadiendo que los hallazgos del estudio deberían ser aplicables a la población en general.

3.3 Procedimiento de investigación

Este proceso de investigación tiene como propósito identificar los riesgos y vulnerabilidades existentes, evaluar los controles de seguridad implementados y proponer recomendaciones para fortalecer la seguridad informática en el área de operaciones y servicios.

Figura 7. Fases de la investigación



Fuente: Elaboración Propia

Fase 1: Diagnóstico Situación Actual

El diagnóstico de la situación actual de la seguridad informática en el GPI se basó en comprender claramente los requerimientos y necesidades actuales. Por lo que este capítulo se enfocó en recopilar toda la información relevante del área de operaciones y servicios del Gobierno Provincial de Imbabura. En aspectos como estructura

organizativa, infraestructura tecnológica, documentación legal, sistema de seguridad actual, análisis de amenazas y vulnerabilidades. (Cachipuendo, 2023)

Situación Actual

Componentes del instrumento: Considerando los lineamientos de la norma ISO 27002:2022 en el Anexo 1 y NIST 800-61, se diseña el guión de preguntas.

Aplicación del instrumento: Con el propósito de evaluar el estado actual de la institución en cuanto a la gestión de incidentes de ciberseguridad, se aplicó un instrumento (encuesta) a profesionales de la Subdirección de Tecnologías de Información, encargados del mantenimiento y funcionamiento de las tecnologías y sistemas de información de la institución.

Para obtener el diagnóstico de la situación actual se ejecutó una encuesta la cual consto de 16 preguntas y se muestra en el Anexo 2, por medio de la herramienta de formulario de Google y su distribución se manejó a través de correo electrónico al personal escogido de muestra en la institución. La visita de campo permitió identificar que la información más relevante se encuentra en las áreas financiero, administrativo y áreas agregadoras de valor.

Fase 2: Diseño de Plan de Seguridad Informática

Basándonos en el diagnóstico previamente realizado a través de una encuesta y siguiendo los lineamientos del Esquema Gubernamental de Seguridad de la Información (EGSI) respaldado por las normas ISO 27002:2017 y 2022, específicamente detallada en el Anexo 1, así como el NIST 800-61, se establecen los cimientos para un modelo sólido que se enfoca en la formulación del plan de seguridad informática.

Fase 3: Evaluación del nivel de confidencialidad, disponibilidad e integridad de la información

Para proteger toda la información de la institución, se hace necesario aplicar una evaluación del nivel de confidencialidad, integridad, disponibilidad de la información en el GAD provincial de Imbabura. De tal forma que se pueda asegurar la protección ante cualquier tipo de ciberataque.

Para aplicar los controles de seguridad de ISO 27002:2022 y NIST 800-61 implica seguir un proceso minucioso. A continuación, se presenta una descripción detallada:

ISO 27002:2022

Comprensión de la Norma: Familiarizarse con los principios, objetivos y directrices de la norma ISO 27002:2022. Examinar detenidamente los controles de seguridad y su alcance.

Identificación de Requisitos: Evaluar los requisitos específicos de seguridad de la información según el contexto organizativo. Esto implica identificar los activos críticos, las amenazas, vulnerabilidades y los riesgos asociados.

Selección de Controles Relevantes: Basándose en la evaluación de riesgos, elegir los controles de seguridad de la ISO 27002:2022 que mejor se adapten a las necesidades de la organización.

Implementación de Controles: Desarrollar un plan detallado para implementar los controles seleccionados. Esto incluye asignar responsabilidades, establecer procesos y procedimientos, y proporcionar recursos necesarios.

Monitoreo y Evaluación: Realizar un seguimiento continuo para asegurar que los controles se apliquen adecuadamente. Llevar a cabo evaluaciones periódicas para identificar áreas de mejora.

NIST 800-61

Comprensión del Marco NIST: Estudiar el NIST 800-61 y comprender sus directrices, procedimientos y recomendaciones para la detección y respuesta a incidentes de seguridad.

Preparación ante incidentes: Establecer un plan de respuesta a incidentes basado en las pautas proporcionadas por el NIST. Definir roles, responsabilidades y procedimientos de manejo de incidentes.

Detección y respuesta: Implementar tecnologías y procesos para la detección temprana de incidentes de seguridad. Establecer protocolos claros para la notificación, investigación y mitigación de los incidentes.

Análisis Post-Incidente: Después de un incidente, realizar un análisis exhaustivo para comprender la causa raíz y mejorar los controles de seguridad para evitar futuros problemas similares.

Mejora continua: Utilizar los datos obtenidos de los incidentes para mejorar los procedimientos, controles y capacidades de detección y respuesta.

En ambos casos, la aplicación exitosa de los controles de seguridad implica un enfoque holístico, desde la comprensión de los estándares hasta la adaptación de los controles a las necesidades específicas de seguridad de la organización, seguido de una implementación cuidadosa y una mejora continua basada en la retroalimentación y la evolución de las amenazas y riesgos.

CAPITULO IV

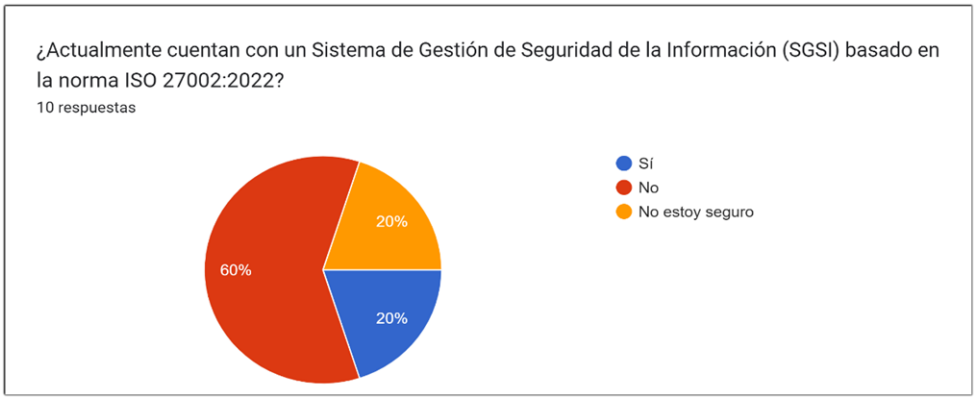
RESULTADOS

4.1 Análisis de los resultados del diagnóstico

Encuesta a funcionarios

La información obtenida a través de las encuestas aplicadas al personal administrativo y directivo de la subdirección de Tecnologías e Información del GPI arroja los siguientes resultados:

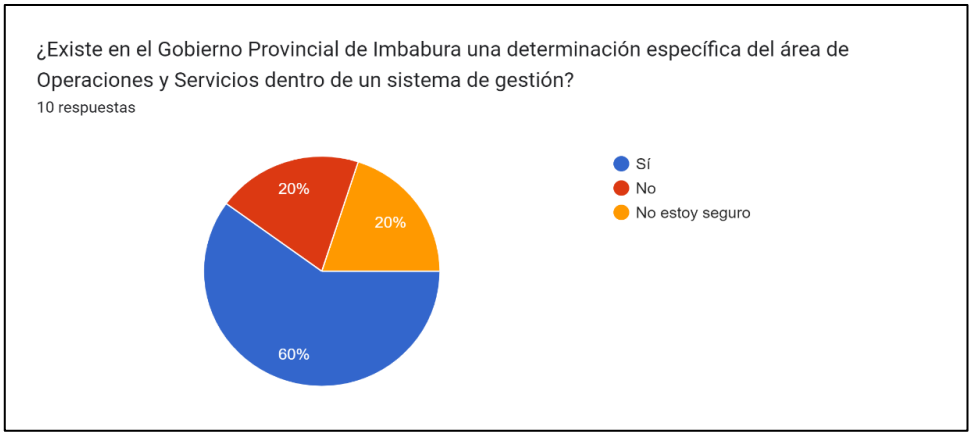
Figura 8. Resultados Pregunta 1



Fuente: Elaboración Propia

La mayoría de los encuestados indicaron la ausencia de un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con la norma ISO 27002:2022, lo que sugiere una vulnerabilidad frente a posibles amenazas cibernéticas. Algunos participantes revelaron estar en proceso de desarrollo de un SGSI, lo que refleja un avance positivo. Sin embargo, una parte significativa de los encuestados no está al tanto de la existencia de este sistema, señalando la necesidad de mejorar la comunicación interna y la concienciación sobre las prácticas de seguridad de la información.

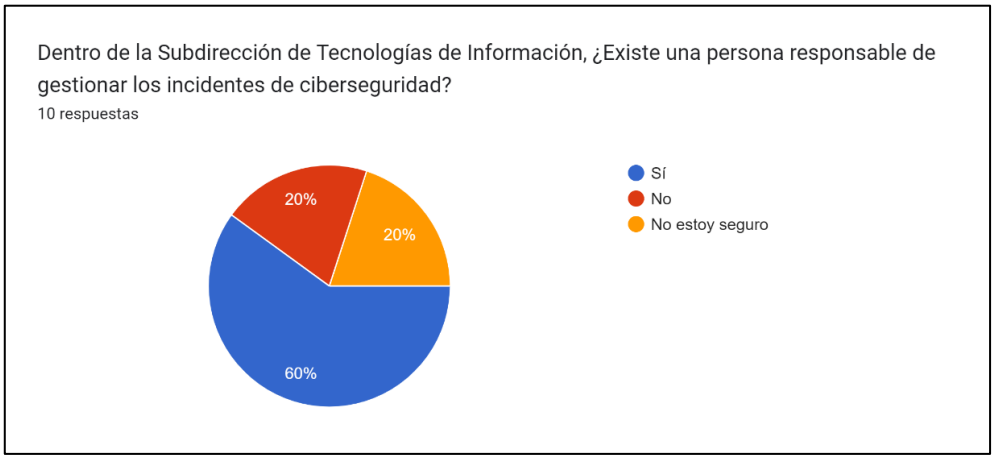
Figura 9. Resultados Pregunta 2



Fuente: Elaboración Propia

De acuerdo con la Figura 3.4, una parte considerable del personal del área de operaciones y servicios muestra un buen conocimiento de las políticas y procedimientos de seguridad, lo cual es alentador. Sin embargo, se observa un grupo que parece no estar debidamente informado, lo que indica una preocupación sobre la falta de concienciación en seguridad en esta área. Además, otra parte del personal muestra cierta incertidumbre, lo que resalta la necesidad de mejorar la comunicación interna y la capacitación en seguridad dentro del GPI. Resulta fundamental garantizar que todos los empleados estén completamente informados y sensibilizados sobre las políticas de seguridad, lo que contribuirá a fortalecer la postura de seguridad de la organización.

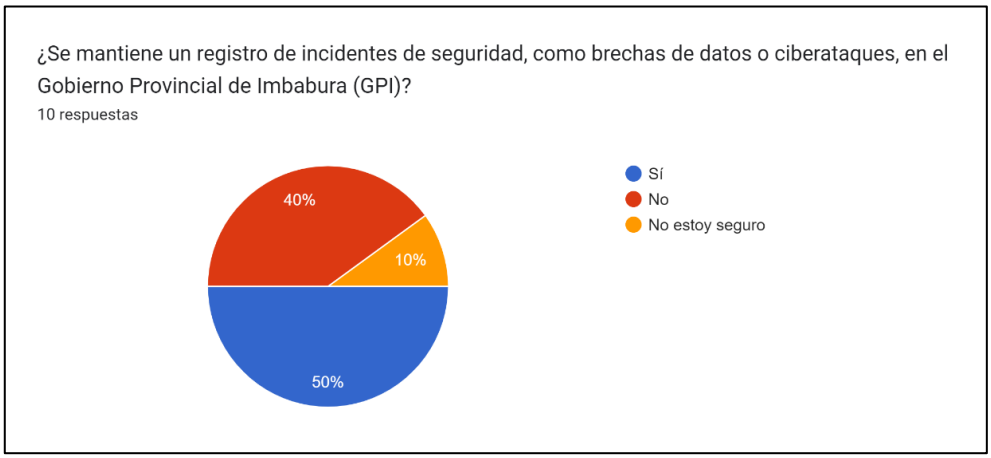
Figura 10. Resultados Pregunta 3



Fuente: Elaboración Propia

Se observa que una parte significativa de los encuestados reconoció la existencia de un responsable de gestión de incidentes de ciberseguridad en la Subdirección de Tecnologías de Información, lo cual es un indicio positivo. Sin embargo, otro grupo indicó la ausencia de una figura responsable, lo que podría generar inquietudes en cuanto a la seguridad. Además, una parte adicional expresó desconocimiento sobre este tema, lo que subraya la importancia de mejorar la comunicación y la concienciación en esta área para asegurar una gestión efectiva de incidentes de ciberseguridad.

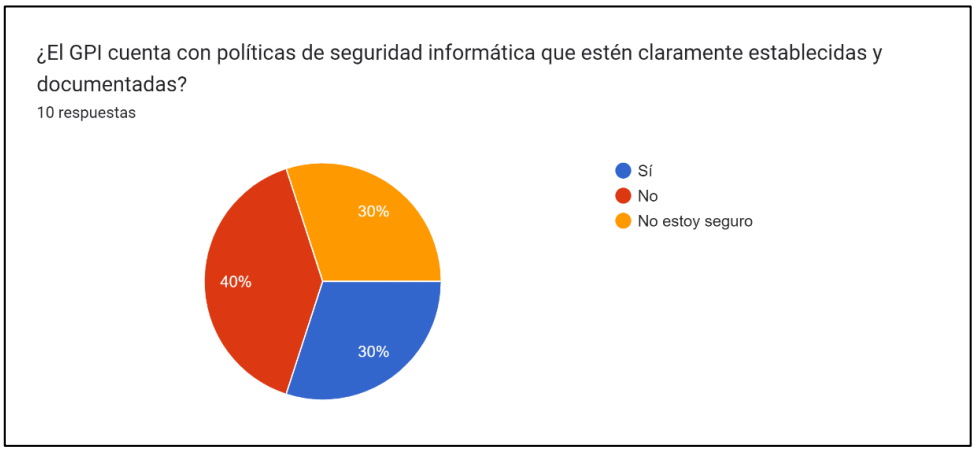
Figura 11. Resultados Pregunta 4



Fuente: Elaboración Propia

Se observa que una parte de los profesionales encuestados lleva un registro de los incidentes de ciberseguridad, lo que sugiere una práctica positiva dentro de la institución. Sin embargo, otro grupo no mantiene este registro, lo que plantea la necesidad de mejorar la concienciación y la documentación de procedimientos en esta área. Esta información indica que existe una iniciativa para realizar seguimiento y registro de los incidentes de ciberseguridad, aunque se requiere una mayor uniformidad y compromiso en toda la institución para mejorar esta práctica.

Figura 12. Resultados Pregunta 5

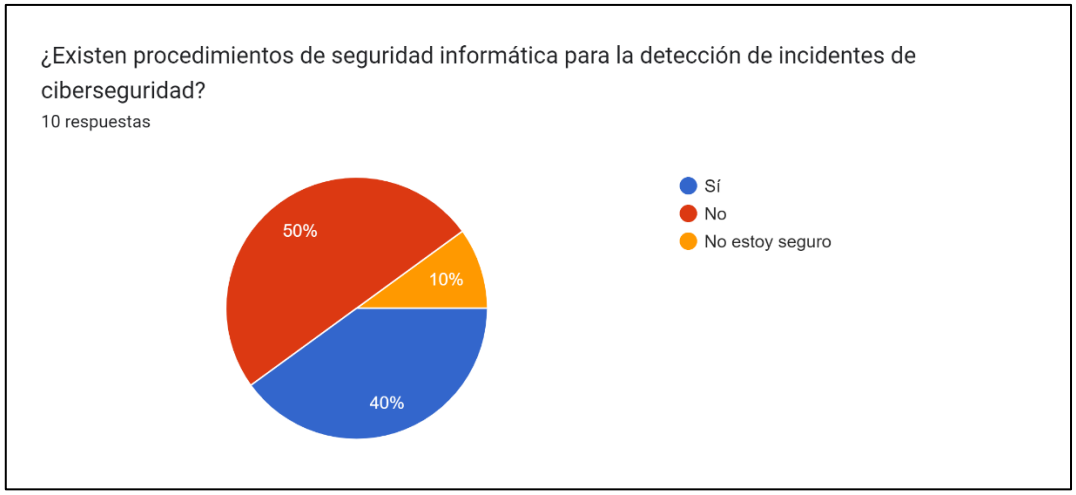


Fuente: Elaboración Propia

Una proporción de los encuestados indicó que no disponen de las políticas mencionadas, mientras que otro grupo afirmó tenerlas. Sin embargo, resulta interesante destacar que una parte expresó incertidumbre o falta de conocimiento sobre la existencia de estas políticas.

Esta falta de certeza podría sugerir una posible carencia de comunicación interna en la institución con respecto a las políticas de seguridad informática. Por ende, sería crucial implementar estrategias de comunicación y concienciación para garantizar que todos los miembros del GPI estén debidamente informados y alineados con las políticas de seguridad informática vigentes.

Figura 13. Resultados Pregunta 6

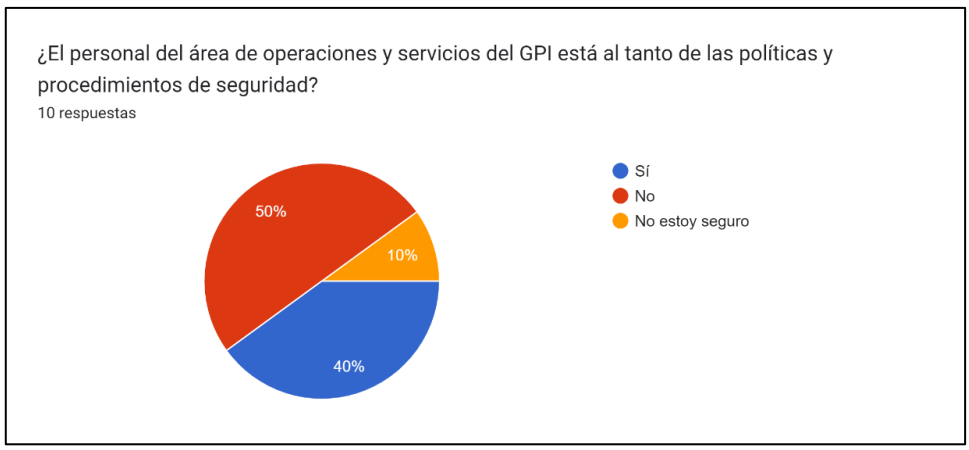


Fuente: Elaboración Propia

Una parte significativa de los encuestados afirmó la ausencia de procedimientos específicos para la seguridad informática en la detección de incidentes de ciberseguridad. Esta carencia podría indicar una falta de preparación para responder a amenazas cibernéticas y una potencial exposición a riesgos de seguridad. Otro grupo mencionó la existencia de tales procedimientos, lo que sugiere un cierto nivel de preparación. Sin embargo, una parte adicional expresó incertidumbre o falta de conocimiento sobre estos procedimientos.

Estos resultados resaltan la necesidad crítica de la institución de establecer procedimientos claros para la detección de incidentes de ciberseguridad en caso de que aún no existan. Además, es fundamental garantizar que todos los miembros estén debidamente informados acerca de estos procedimientos para asegurar una respuesta efectiva frente a posibles amenazas de ciberseguridad.

Figura 14. Resultados Pregunta 7

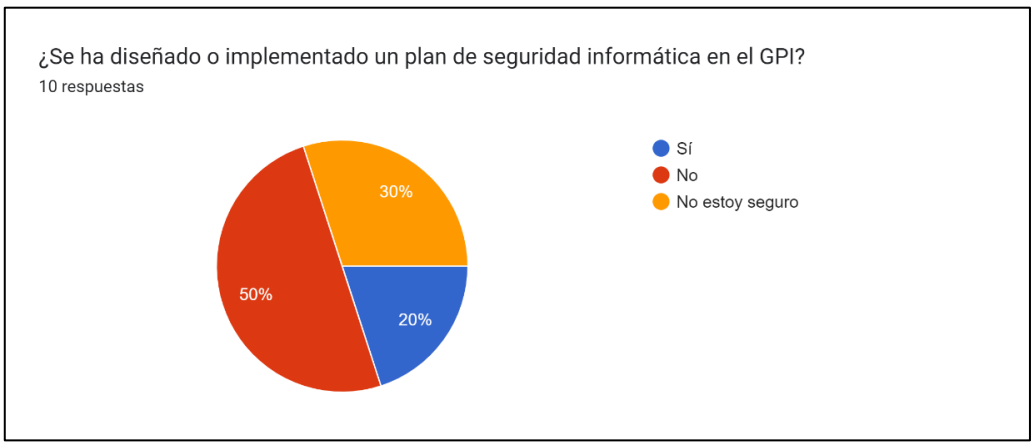


Fuente: Elaboración Propia

Se observa que una parte de los encuestados percibe que el personal del área no está completamente informado sobre las políticas y procedimientos de seguridad, lo que podría indicar una brecha en la comunicación interna. Sin embargo, una proporción considerable mencionó que el personal está al tanto de estas políticas y procedimientos, lo cual es una señal positiva para la organización. No obstante, una minoría expresó incertidumbre o falta de conocimiento sobre la conciencia del personal respecto a estas políticas.

Estos hallazgos resaltan la importancia crucial de mejorar la comunicación interna y la concienciación en toda la organización, específicamente entre el personal del área de tecnologías de información, para garantizar que todos estén debidamente informados y alineados con las políticas y procedimientos de seguridad establecidos.

Figura 15. Resultados Pregunta 8

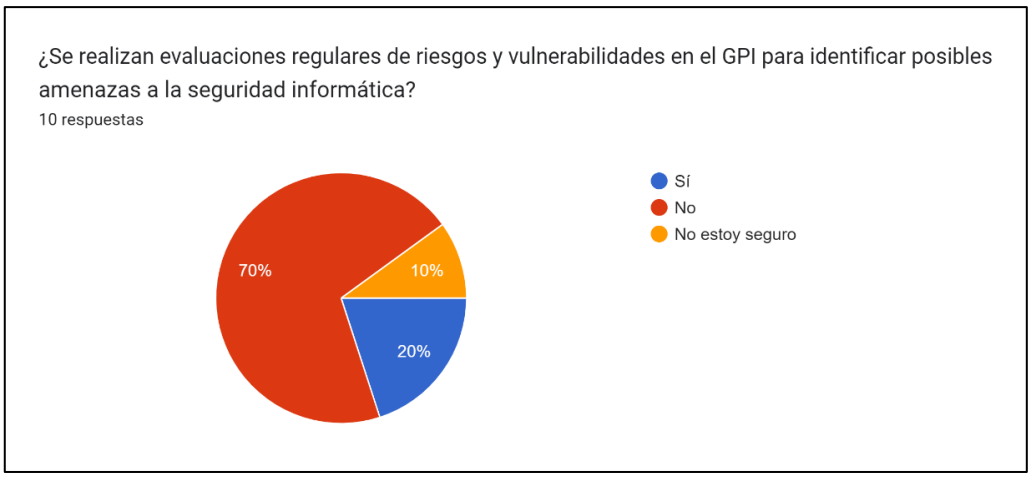


Fuente: Elaboración Propia

Se observa que una parte de los encuestados indicó la ausencia de un plan de seguridad informática en la organización, lo que sugiere una importante falta en la preparación y protección de los activos de información. Además, una proporción expresó incertidumbre o falta de conocimiento sobre la existencia de dicho plan, lo que podría señalar una carencia en la comunicación interna o la concienciación respecto a las medidas de seguridad informática en el GPI.

Por otro lado, una minoría mencionó la existencia de un plan de seguridad informática, lo cual se percibe como una señal positiva. Sin embargo, dado que esta proporción es relativamente baja, se destaca una clara necesidad de mejorar la implementación y comunicación de las políticas como también las prácticas de seguridad informática dentro de la organización para fortalecer su postura en materia de seguridad.

Figura 16. Resultados Pregunta 9



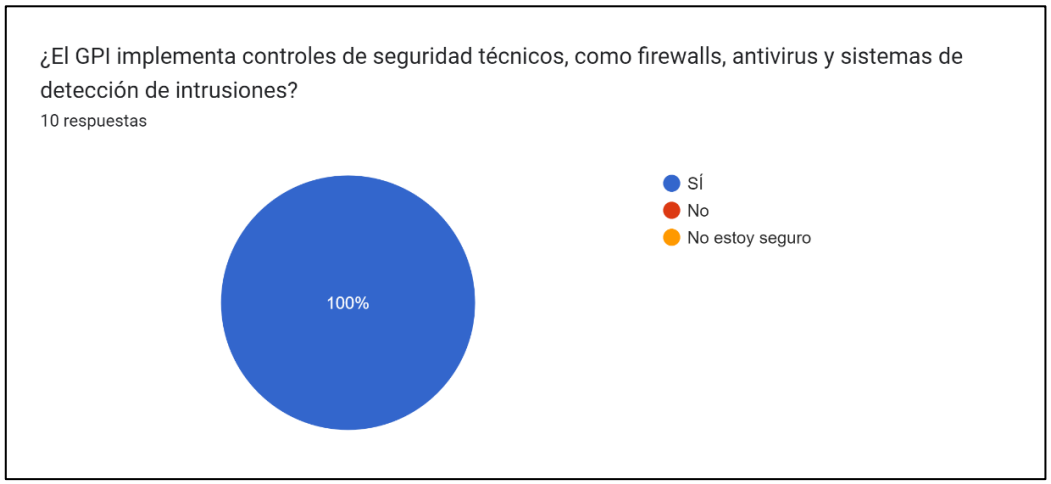
Fuente: Elaboración Propia

La mayoría de los encuestados mencionaron la ausencia de evaluaciones regulares de riesgos y vulnerabilidades en la organización, lo que sugiere una falta general de prácticas establecidas para identificar y abordar riesgos de seguridad informática. Sin embargo, una proporción señaló la realización de tales evaluaciones, lo cual es una señal positiva de que al menos una parte de la organización está adoptando medidas proactivas para este fin.

Por otro lado, una minoría expresó incertidumbre o falta de conocimiento sobre la realización de estas evaluaciones, lo que subraya la necesidad urgente de implementar prácticas regulares de evaluación de riesgos y vulnerabilidades en el GPI. Esto permitirá identificar posibles amenazas a la seguridad informática y tomar medidas adecuadas para su mitigación. Además, es crucial mejorar la comunicación interna y la

concienciación dentro de la organización respecto a la importancia y la implementación de estas prácticas de seguridad.

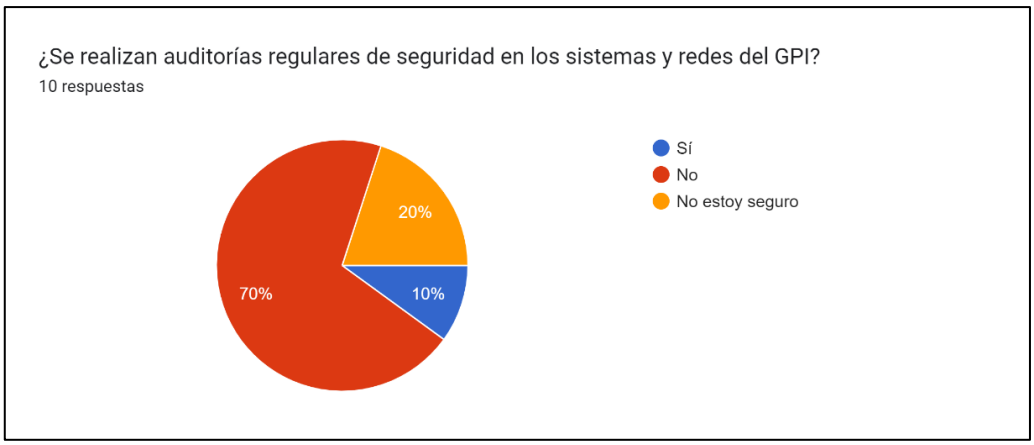
Figura 17. Resultados Pregunta 10



Fuente: Elaboración Propia

Este resultado es altamente alentador, ya que demuestra que la organización está adoptando medidas efectivas para resguardar sus activos de información mediante la aplicación de controles técnicos bien establecidos, tales como firewalls, sistemas antivirus y sistemas de detección de intrusiones. No obstante, es esencial mantener una vigilancia continua y realizar mejoras en estos controles técnicos con el fin de mantener un nivel de seguridad óptimo a lo largo del tiempo.

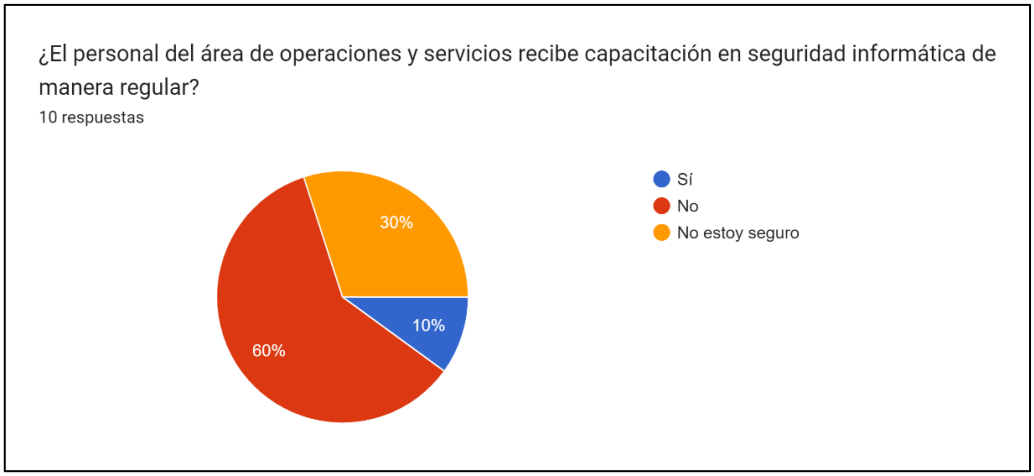
Figura 18. Resultados Pregunta 11



Fuente: Elaboración Propia

El resultado indica que la mayoría de los encuestados no creen que se realicen auditorías regulares de seguridad en los sistemas y redes del GPI. Un pequeño porcentaje piensa que sí se llevan a cabo, mientras que otro grupo no está seguro. Esto señala la necesidad potencial de revisar y mejorar las prácticas de seguridad en la organización.

Figura 19. Resultados Pregunta 12

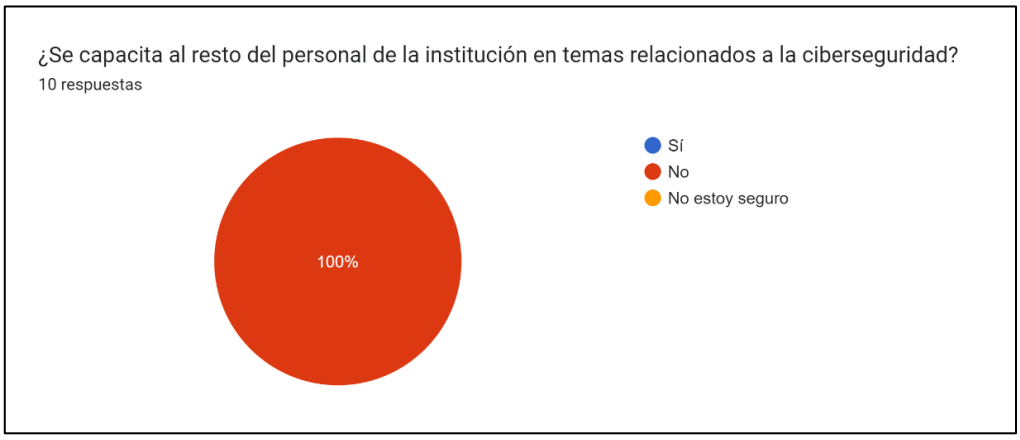


Fuente: Elaboración Propia

Una parte significativa del personal del área de operaciones y servicios mencionó que no recibe capacitación regular en seguridad informática, lo cual podría representar un riesgo en la preparación frente a posibles amenazas cibernéticas. En contraste, una minoría recibe capacitación regular, lo que se considera como un aspecto positivo. Sin embargo, una proporción expresó incertidumbre sobre la capacitación, lo que resalta la necesidad de mejorar la comunicación y la transparencia en este ámbito.

Establecer un programa de capacitación regular en seguridad informática en el área de operaciones y servicios resulta crucial para fortalecer la concienciación y la preparación del personal ante posibles amenazas cibernéticas. Esto permitirá mejorar la preparación general del equipo frente a riesgos y potenciales ataques.

Figura 20. Resultados Pregunta 13

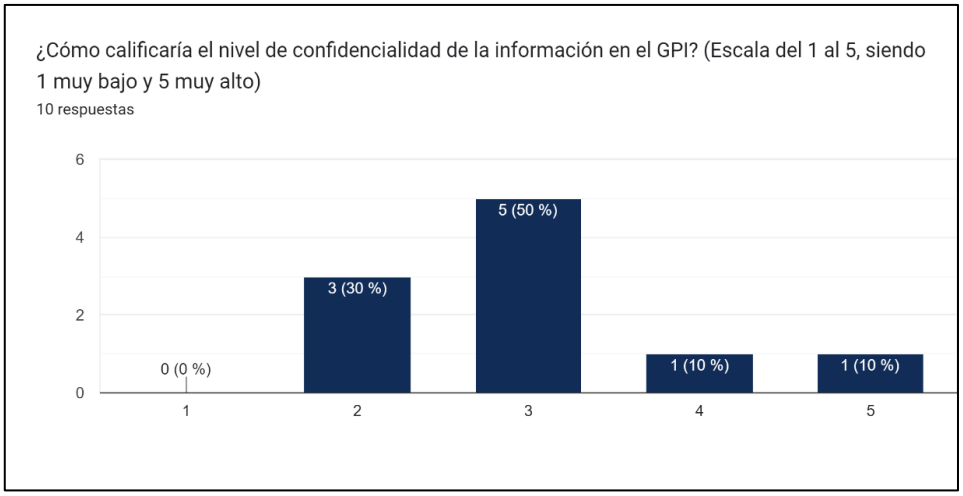


Fuente: Elaboración Propia

La ausencia de capacitación en temas relacionados con la ciberseguridad para todo el personal indica una brecha considerable en la preparación de la institución frente a

posibles amenazas cibernéticas. Este hallazgo resalta una necesidad urgente de implementar programas de capacitación efectivos para elevar el nivel de conciencia y preparación del personal ante riesgos y posibles ataques cibernéticos. Mejorar la formación en ciberseguridad se convierte en una prioridad clave para fortalecer la postura de seguridad de la organización.

Figura 21. Resultados Pregunta 14

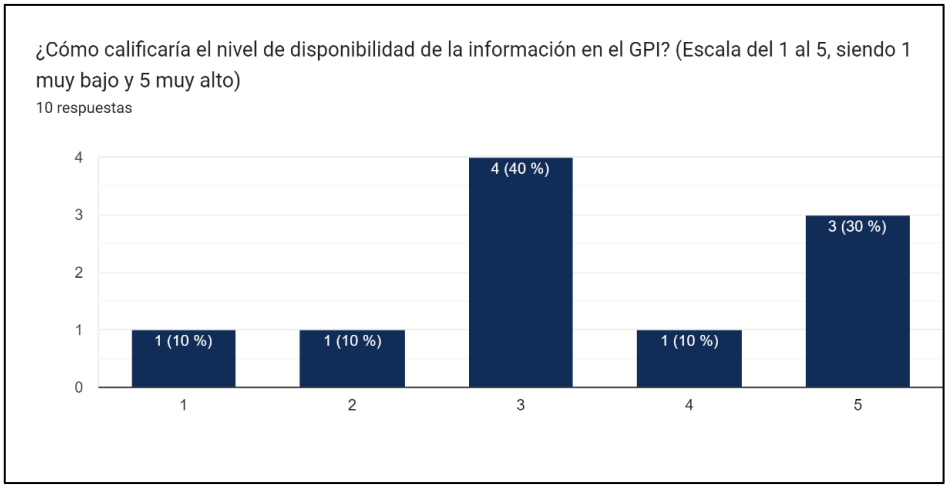


Fuente: Elaboración Propia

Los resultados de la pregunta sobre el nivel de confidencialidad de la información en el GPI muestran una diversidad en las percepciones de los encuestados. Se observa una gama amplia de calificaciones: algunas personas la consideran baja, otras la perciben como moderada, mientras que una minoría la califica como alta o muy alta. Esta variación en las percepciones podría indicar la necesidad de una evaluación exhaustiva de las políticas y prácticas de confidencialidad en la organización.

Además, estos resultados podrían ser una oportunidad para generar conciencia sobre la importancia de la confidencialidad de la información y promover medidas destinadas a fortalecerla dentro del GPI. Sería crucial trabajar en estrategias que unifiquen y eleven el nivel de confidencialidad percibido, mejorando así la protección de la información sensible en la organización.

Figura 22. Resultados Pregunta 15

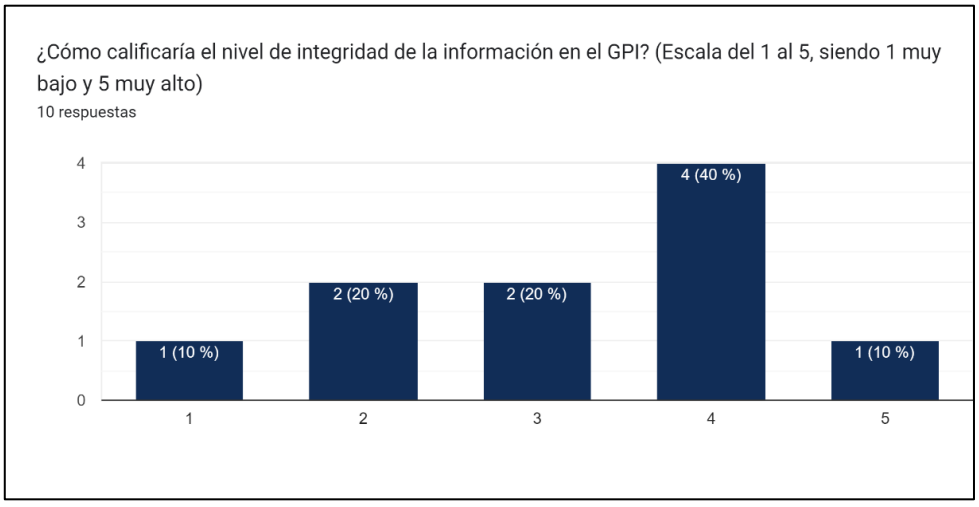


Fuente: Elaboración Propia

Los resultados de la pregunta sobre el nivel de disponibilidad de la información en el GPI muestran una diversidad de percepciones entre los encuestados. Las calificaciones abarcan un amplio rango, desde considerarla muy baja hasta muy alta. Estas variaciones podrían originarse en diferentes interpretaciones del concepto de disponibilidad y en las experiencias individuales de los encuestados.

Para mejorar la disponibilidad de la información en la organización, es esencial considerar y abordar estas percepciones variadas. Esto implica tomar en cuenta las preocupaciones planteadas por los encuestados, especialmente aquellas relacionadas con calificaciones más bajas. Al comprender estas perspectivas diversas, se puede trabajar en estrategias para mejorar y garantizar una disponibilidad óptima de la información en el GPI.

Figura 23. Resultados Pregunta 16



Fuente: Elaboración Propia

El análisis de los resultados sobre el nivel de integridad de la información en el GPI refleja una variedad de percepciones entre los encuestados. Se observa una gama amplia de calificaciones, desde considerarla muy baja hasta muy alta. Esta diversidad de opiniones resalta la variación en la percepción sobre la integridad de la información en la organización.

Aunque la mayoría percibe un nivel alto de integridad, la presencia de calificaciones más bajas sugiere inquietudes en ciertos sectores de la organización. Es crucial mantener y mejorar los mecanismos de control de la integridad de la información para abordar cualquier preocupación relacionada con la integridad de los datos. Esto permitirá fortalecer la confianza y la fiabilidad de la información en el GPI.

Los resultados de la encuesta aplicada a los profesionales de tecnologías de información del Gobierno Provincial de Imbabura indican que actualmente, esta área carece de un modelo establecido para la gestión de incidentes de ciberseguridad. A pesar de que la organización se encuentra en proceso de desarrollar e implementar un sistema de gestión de seguridad de la información, como se menciona en la pregunta número tres de la encuesta, el análisis de las respuestas del personal del área revela una notoria falta de implementación en lo que respecta a incidentes de ciberseguridad.

4.2 Propuesta del Diseño de Plan de Seguridad Informática del GPI

Esta sección representa el resultado del análisis de la situación actual en el ámbito de seguridad informática del GPI para identificar los parámetros fundamentales que deben considerarse en la creación del Plan de Seguridad Informática.

Al diseñar el esquema de seguridad, se busca fortalecer las medidas de protección y prevención, garantizando la confidencialidad, integridad y disponibilidad de la información. La aplicación de los controles definidos en estas normas permite establecer un marco sólido para gestionar los riesgos de seguridad y proteger los activos de la organización de manera efectiva.

La estructura de la propuesta se conforma de la siguiente manera:

Esquema General del Plan de Seguridad

El presente esquema está basado en las mejores prácticas respaldadas por estándares de seguridad internacionalmente reconocidos, como ISO 27002:2022 y NIST 800-61, con el propósito de fortalecer y promover una sólida cultura de seguridad en la institución.

Figura 24. Etapas del Plan de Seguridad

Fuente: Elaboración Propia

A continuación, se detalla cada aspecto de la seguridad de la información y etapa que contendría el documento del plan de seguridad informática en el Gobierno Provincial de Imbabura, proporcionando un marco sólido y estructurado para proteger los activos de información y minimizar los riesgos de seguridad:

1. Definición del Alcance del Plan

El Gobierno Provincial de Imbabura ha iniciado la implementación de la seguridad de informática en institución al establecer un equipo de trabajo denominado como Comité de Seguridad de la Información. Una vez se definan responsabilidades y autorizaciones correspondientes, se establecerá el alcance del Plan de Seguridad de la Información.

2. Identificación de Activos de Información

Identificar y clasificar los activos de información críticos para la organización. Esto incluye datos, sistemas, aplicaciones y cualquier otro elemento relevante.

Activos Primarios

Son los activos esenciales para el desarrollo de las funciones del Gobierno Provincial de Imbabura, en esta categoría se catalogan: La información, los procesos y procedimientos.

Activos de Soporte

En esta categoría se clasifican los activos que permiten dar tratamiento a la información atendiendo a las recomendaciones que formulan las normas técnicas de gestión de la seguridad de la información, se destacan:

- El Hardware. En esta sección encontramos todo dispositivo físico como computadores portátiles tabletas, teléfonos inteligentes, estaciones de trabajo y demás equipos de procesamiento de información, impresoras, scanner, cámaras fotográficas, lectoras de datos, discos extraíbles, entre otros.
- El Software. Sistemas para el procesamiento de información como: utilitarios para el usuario final, correo electrónico, antivirus, herramientas de desarrollo de software, software para control de inventarios, sistemas financieros, sistemas para gestión de talento humano, software para gestión de bases de datos, sitios web, etc.
- La Infraestructura de servidores y seguridades. Toda la infraestructura del centro de datos como UPS, aire acondicionado, control de acceso, sensores de humedad, temperatura, servidores, sistemas de almacenamiento, etc.
- La Infraestructura de redes. En esta categoría están los medios de transmisión que soportan a las redes y los equipos activos que permiten la transmisión de datos sobre las redes.
- El Personal. Funcionarios y trabajadores del GAD Provincial de Imbabura.
- La Infraestructura física. Edificios, maquinaria, equipamiento y menaje de la institución.
- Y finalmente la Estructura Organizacional del GPI. (Gobierno Autónomo Descentralizado Provincial de Imbabura, 2023)

En el análisis de este caso de estudio, se han tomado en cuenta los diversos tipos de activos involucrados en el proceso, entre los cuales se incluyen hardware, software y personal.

En cada uno de estos activos, se llevó a cabo una evaluación del impacto que generan en la confidencialidad, disponibilidad e integridad de la información. Esta evaluación se realizó empleando la escala Likert, siendo:

Tabla 5. Escala de Likert

1	2	3	4	5
Muy bajo	Bajo	Medio	Alto	Muy Alto

Fuente: Elaboración Propia

A continuación, se muestra en la tabla 4. la valoración de los activos de la subdirección de tecnologías de la información.

Tabla 6. Valoración de Activos Subdirección de Tecnologías de Información

(Escala del 1 al 5, siendo 1 muy bajo y 5 muy alto)						
CÓDIGO	**ACTIVOS DE SOPORTE**	**AREA RESPONSABLE DEL BIEN**	**CONFIDENCIALIDAD**	**DISPONIBILIDAD**	**INTEGRIDAD**	**RESULTADO**
HW1	ACCES POINT	REDES Y TELECOMUNICACIONES	5	5	5	5
HW2	CABLEADO ESTRUCTURADO	REDES Y TELECOMUNICACIONES	5	5	5	5
HW3	CHASIS DE SERVIDORES	REDES Y TELECOMUNICACIONES	5	5	5	5
HW4	COMPUTADOR DE ESCRITORIO	MANTENIMIENTO Y SOPORTE	5	4	5	5
HW5	COMPUTADORA PORTATIL	MANTENIMIENTO Y SOPORTE	5	4	5	5
HW6	DISCO DURO EXTERNO	MANTENIMIENTO Y SOPORTE	5	4	4	4
HW7	DISCO DURO SERVIDORES	REDES Y TELECOMUNICACIONES	5	5	5	5
HW8	EQUIPO SEGURIDAD PERIMETRAL UTM	REDES Y TELECOMUNICACIONES	5	5	5	5
HW9	ESCANERS	MANTENIMIENTO Y SOPORTE	2	3	3	3
HW10	IMPRESORAS	MANTENIMIENTO Y SOPORTE	2	3	3	3
HW11	INSTALACIÓN ELECTRICA	MANTENIMIENTO Y SOPORTE	2	5	3	3
HW12	RACK	REDES Y TELECOMUNICACIONES	5	5	5	5
HW13	ROUTER	REDES Y TELECOMUNICACIONES	5	5	5	5
HW14	SERVIDOR	REDES Y TELECOMUNICACIONES	5	5	5	5
HW15	SISTEMA AIRE ACONDICIONADO	MANTENIMIENTO Y SOPORTE	3	5	3	4
HW16	SISTEMA DE DETECCION Y EXTINCION INCENDIOS PARA DATA CENTER	MANTENIMIENTO Y SOPORTE	3	5	3	4
HW17	SWITCH	REDES Y TELECOMUNICACIONES	5	5	5	5
HW18	TELEFONOS IP	REDES Y TELECOMUNICACIONES	3	4	5	4
HW19	UPS	MANTENIMIENTO Y SOPORTE	3	5	3	4
SW1	ANTIVIRUS	MANTENIMIENTO Y SOPORTE	3	4	5	4

SW2	CORREO ELECTRONICO	DESARROLLO	5	5	5	5
SW3	ERP ODOO	DESARROLLO	5	5	5	5
SW4	HELPDESK	DESARROLLO	5	5	5	5
SW5	MOODLE	DESARROLLO	5	5	5	5
SW6	YUPAK INVENTARIOS Y ACTIVOS FIJOS	DESARROLLO	5	5	5	5
SW7	QUIPUX	DESARROLLO	5	5	5	5
SW8	SISTEMA OPERATIVO LINUX CENTOS	MANTENIMIENTO Y SOPORTE	5	5	5	5
SW9	SISTEMA OPERATIVO WINDOWS SERVER	MANTENIMIENTO Y SOPORTE	5	5	5	5
SW10	WEB SITE	DESARROLLO	5	5	5	5
P1	ADMINISTRADOR DE RED	REDES Y TELECOMUNICACIONES	5	5	5	5
P2	DESARROLLADOR	DESARROLLO	5	5	5	5
P3	TECNICO DE SOPORTE	MANTENIMIENTO Y SOPORTE	4	4	5	4

Fuente: Elaboración Propia

3. Evaluación de Riesgos

La evaluación de riesgos es un proceso fundamental en la seguridad informática que permite identificar, analizar y priorizar los riesgos a los que la institución está expuesta. Aquí tienes algunas recomendaciones para llevar a cabo una evaluación de riesgos efectiva:

Establecer un alcance claro: Definir claramente los activos de información que serán evaluados, así como los sistemas, redes y procesos que están relacionados con estos activos. También se debe definir el alcance temporal y geográfico de la evaluación.

Identificar activos críticos: Identificar los activos de información más importantes para la institución, incluyendo datos confidenciales, sistemas críticos, infraestructura de red y otros recursos fundamentales para las operaciones.

Identificar amenazas: Enumerar y analizar las posibles amenazas que podrían afectar a los activos, como ataques cibernéticos, desastres naturales, errores humanos, entre otros. Considera tanto las amenazas internas como externas.

Evaluar vulnerabilidades: Identificar las vulnerabilidades en los sistemas, procesos y controles de seguridad que podrían ser explotadas por las amenazas identificadas. Esto puede incluir fallos de software, configuraciones inseguras, falta de parches, entre otros.

Estimar la probabilidad de ocurrencia: Evaluar la probabilidad de que una amenaza específica explote una vulnerabilidad particular. Puedes utilizar información histórica, análisis de tendencias, evaluaciones técnicas y la experiencia de expertos para estimar esta probabilidad.

Evaluar el impacto: Determinar el impacto que tendría la materialización de cada riesgo en términos de pérdida financiera, daño a la reputación e interrupción de operaciones, entre otros factores. Esto ayudará a priorizar los riesgos según su gravedad.

Calcular el riesgo residual: Calcular el riesgo residual de cada amenaza después de tener en cuenta los controles de seguridad existentes. Esto permitirá identificar qué riesgos son aceptables y cuáles requieren medidas adicionales de mitigación.

Priorizar los riesgos: Clasificar los riesgos identificados según su nivel de riesgo, combinando la probabilidad de ocurrencia y el impacto potencial. Esto ayudará a centrar los recursos en los riesgos más críticos y urgentes.

Desarrollar un plan de acción: Desarrollar un plan detallado para abordar los riesgos prioritarios, identificando medidas de mitigación específicas, asignando responsabilidades y estableciendo plazos para su implementación.

Monitorear y revisar continuamente: Implementar un proceso de monitoreo continuo para detectar cambios en el entorno de riesgo y revisar regularmente tu evaluación de riesgos para asegurarte de que sigue siendo relevante y actualizada.

Siguiendo estas sugerencias, se llevaría a cabo una evaluación completa y eficaz de los riesgos, lo cual facilitará la toma de decisiones destinadas a proteger los activos de información y reducir los riesgos de seguridad.

Basándose en estos aspectos, se puede realizar una evaluación de riesgos más detallada, asignando probabilidades e impactos a los riesgos identificados, y priorizando acciones para mitigarlos y gestionarlos de manera efectiva. Esto permitirá al GAD provincial de Imbabura y al área de operaciones y servicios del GPI tomar medidas proactivas para fortalecer la seguridad de la información y proteger sus activos contra posibles amenazas y vulnerabilidades.

4. Normativas y estándares

Asegurarse de estar al tanto de las regulaciones y estándares aplicables a la institución. Las normas recomendadas en el ámbito de la seguridad de la información pueden variar según la industria, la ubicación geográfica y otros factores específicos de cada organización. Sin embargo, hay varias normas ampliamente reconocidas y utilizadas que pueden servir como referencia para establecer y mejorar la seguridad de la información. La aplicación de estándares como ISO/IEC 27002:2022 y guías como

NIST SP 800-61 pueden ser relevantes tanto para el control interno y gestión de seguridad de la información.

5. Políticas y procedimientos existentes

Revisar las políticas y procedimientos de seguridad informática actuales de la organización, si los hubiera, para determinar si están actualizados y cumplen con las necesidades.

Políticas de seguridad de la información

Las Políticas de Seguridad se establecen como un pilar esencial para proteger la información, asegurando la continuidad operativa de los sistemas informáticos en línea con los objetivos del GPI y reduciendo al máximo el riesgo de daños. Estas políticas representan una declaración de principios que gobiernan la conducta, la ética y las responsabilidades asumidas por la extensión, y son aceptadas por sus colaboradores. Su misión fundamental es establecer y mantener un entorno seguro para la gestión de la información, abarcando tanto la información propia como la de estudiantes y terceras partes.

El propósito principal de las Políticas de Seguridad de la Información es proporcionar a los empleados y/o funcionarios públicos la orientación necesaria sobre las reglas y herramientas que deben seguir y emplear para salvaguardar tanto los activos de información principales como los secundarios.

Estructura documento de políticas de seguridad de información actual aprobado y publicado en el sitio web del GAD Provincial de Imbabura conforme indica RESOLUCIÓN ADMINISTRATIVA Nro. GPI-NA-P-02-2023.

Las políticas están diseñadas para salvaguardar los activos de información, que pueden clasificarse como principales o secundarios:

1. Políticas Generales
    1.1 Los recursos informáticos sólo pueden ser utilizados por los colaboradores del GPI: servidores públicos o trabajadores, practicantes, pasantes y contratistas que cuentan con la debida autorización de la Máxima Autoridad, o de la Dirección General a la cual pertenecen o están vinculados.
    1.2 Las políticas de seguridad de la Información serán aprobadas por el Comité de Seguridad de la información Comité de Seguridad de la Información.

1.3 La socialización de la Políticas de Seguridad de la información será viabilizada por el Oficial de Seguridad de la Información, a través de los medios digitales existentes en la institución o mediante procesos de capacitación continua y de inducción cuando exista incorporación de nuevos servidores públicos y/o trabajadores; de igual forma se notificará a todo el personal cuando existan cambios o mejoras en las políticas.

1.4 El desarrollo de nuevos proyectos que involucren el uso de recursos tecnológicos será realizado y liderado por la Dirección General de TI.

1.5 La adquisición de bienes y/o servicios, donde se incluyan equipos informáticos como parte integrante o complementaria de otros procesos, será realizada y validada por la Dirección General de TI.

1.6 La Dirección General de TI autorizará la conexión de cualquier elemento electrónico en la red de datos interna del GPI en base a autorización del Director General de TI y de la Dirección a la cual pertenece el solicitante de este requerimiento presentando su respectiva justificación.

1.7 La Dirección General de TI verificará que los equipos tecnológicos tengan: disponibilidad de energía eléctrica, cableado estructurado y mantengan las condiciones físicas aceptables y adecuadas de temperatura, entre otros para su normal funcionamiento de acuerdo con las especificaciones técnicas del fabricante, siempre que se cumplan los ítems 1.4 al 1.6.

1.8 La Dirección General de TI debe velar por la debida privacidad y confidencialidad de los datos personales registrados de los servidores públicos, trabajadores o usuarios ciudadanos en los sistemas de información del GPI y solo se permitirá el acceso a ésta, previo consentimiento de la parte involucrada o por pedido de una autoridad competente, dentro de un proceso legal, si fuera el caso, solicitado de manera formal y avalado por la Dirección Requirente y la Dirección propietaria de la información, presentando el respectivo informe de justificación y las firmas de autorización para éste acceso.

1.9 Todo servidor público y trabajador que genere o consuma información del GPI, tiene la responsabilidad de respaldarla, siguiendo los lineamientos entregados por la Dirección General de TI para este efecto.

1.10 El acceso a los servicios ofrecidos por la Dirección General de TI, para el consumo de información, navegación, etc., se solicitará de manera formal a

través del sistema de gestión documental con la respectiva justificación y responsabilidad a la Dirección General requirente, requisito principal es la firma del acuerdo de confidencialidad aprobado y publicado para este fin.

1.11 La Dirección General de TI dentro de sus responsabilidades está la de proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como de bancos de datos de información digitalizados, el mismo que se lo realizará de forma automatizada en general.

2. Responsabilidades de Servidores Públicos y Trabajadores
3. Licenciamiento de Software
4. Derechos de Autor
5. Soporte
6. Equipo de Cómputo
7. Desarrollos de Sistemas de Información
8. Seguridad
9. Continuidad De Los Servicios TI
10. Uso De Internet
11. Correo Electrónico
12. Renovación De Equipos
13. Administración De Sistemas Informáticos
14. Teletrabajo
15. Dispositivos Móviles (Gobierno Autónomo Descentralizado Provincial de Imbabura, 2023)

6. Definición Objetivos de Seguridad

Los objetivos de seguridad informática son metas específicas que una organización establece para salvaguardar sus activos de información, infraestructura y sistemas contra amenazas y riesgos. Estos objetivos deben estar diseñados para garantizar la confidencialidad, integridad y disponibilidad de los datos, así como para proteger los recursos informáticos de posibles ataques y vulnerabilidades.

Objetivos Basados en ISO/IEC 27002:2022

- **Gestión Integral de la Seguridad de la Información**
  Establecer y mantener un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a ISO/IEC 27002, asegurando la integración de políticas y prácticas de seguridad en todos los niveles de la organización.
- **Clasificación y Control de Activos de Información**
  Implementar procesos de clasificación y manejo de activos de información para proteger la confidencialidad, integridad y disponibilidad de los datos.
- **Gestión de Riesgos y Evaluación Continua**
  Realizar evaluaciones periódicas de riesgos de seguridad de la información, estableciendo medidas de mitigación y revisión continua según ISO/IEC 27002.
- **Seguridad Física y del Entorno**
  Asegurar la protección física de las instalaciones y los datos, implementando controles de acceso y medidas contra amenazas físicas y ambientales.
- **Seguridad en Recursos Humanos**
  Fomentar una cultura de seguridad entre los empleados mediante formación continua, concienciación y gestión de la seguridad en todo el ciclo de vida laboral del empleado.
- **Gestión de Comunicaciones y Operaciones**
  Establecer controles operativos y de comunicaciones para proteger la información en redes y durante su procesamiento, incluyendo la gestión de dispositivos móviles y teletrabajo.
- **Control de Acceso y Autenticación**
  Implementar un sistema robusto de control de acceso basado en roles y políticas de autenticación y autorización fuertes.

7. Aplicabilidad Controles de Seguridad

Los controles de seguridad son medidas técnicas, administrativas y físicas que una organización debe implementar para proteger sus activos de información y sistemas contra amenazas y riesgos. La aplicabilidad de estos controles puede cambiar dependiendo de varios factores, tales como el tamaño de la entidad, el sector en el que opera, el marco regulatorio vigente y los riesgos particulares a los que se encuentre expuesta la organización.

Recomendaciones a considerar:

- **Análisis de riesgos y necesidades**

  Realizar una evaluación exhaustiva de los riesgos que confronta la entidad y las demandas particulares de seguridad. Esto incluye identificar activos críticos, evaluar amenazas y vulnerabilidades, y determinar los impactos potenciales de los riesgos.
- **Mapeo de controles de seguridad**

  Utilizar la ISO/IEC 27002:2022 para identificar los controles de seguridad relevantes que aplican a la organización.

  Mapear los controles de seguridad de la ISO/IEC 27002:2022 con las pautas y controles de seguridad del NIST SP 800-61 para garantizar una cobertura integral.
- **Priorización de controles**

  Priorizar los controles de seguridad en función de la criticidad de los activos de información y los riesgos identificados. Identificar los controles que deben implementarse de manera inmediata y aquellos que pueden abordarse en etapas posteriores.
- **Evaluación y monitoreo continuo**

  Realizar evaluaciones periódicas para medir la efectividad de los controles de seguridad implementados.
- **Auditorías y revisión**

  Realizar auditorías periódicas de seguridad para verificar el acatamiento de las medidas de seguridad y las políticas establecidas.

  Revisar y actualizar regularmente los controles de seguridad en función de los cambios en el entorno operativo y las nuevas amenazas de seguridad.

8. Concientización del personal

La concientización del personal es fundamental para promover una cultura de seguridad informática dentro de una organización, ya que el factor humano suele ser un punto débil en la seguridad esto contribuiría en reducir el riesgo de incidentes de seguridad causados por errores humanos o comportamientos no seguros.

Recomendaciones a considerar:

- **Identificación de temas clave**

  Identificar los temas clave de seguridad de la información que son relevantes para la organización y que se alineen con los controles y prácticas recomendadas

por ISO/IEC 27002:2022 y NIST SP 800-61. Estos pueden incluir la gestión de contraseñas, el manejo de correos electrónicos, la detección de phishing, entre otros.

- **Involucramiento de la alta dirección**

  Obtener el apoyo de la alta dirección es esencial para las actividades de concientización en seguridad. Su participación promueve la importancia de la seguridad de la información y ayuda a establecer una cultura de seguridad en toda la organización. Esto refuerza el compromiso del personal con las políticas de seguridad y fortalece la postura de seguridad de la institución.

- **Campañas de concientización continuas**

  Llevar a cabo campañas continuas de concientización en seguridad de la información, utilizando diversos medios de comunicación, como correos electrónicos, carteles, boletines informativos y redes sociales.

9. Gestión de incidentes

La Gestión de Incidentes es un componente crítico de la seguridad de información que implica la detección, respuesta, mitigación y recuperación de eventos de seguridad. El NIST (National Institute of Standards and Technology) proporciona pautas detalladas para la Gestión de Incidentes en su documento NIST SP 800-61, titulado "Computer Security Incident Handling Guide". Una breve descripción de los principales pasos recomendados por el NIST 800-61 para la gestión de incidentes se muestran en el capítulo 2 sección 2.2.6 sobre estándares de seguridad.

Recomendaciones a considerar:

- **Establecer un equipo de respuesta a incidentes**

  Designar un equipo dedicado para gestionar y responder a incidentes de seguridad de la información. Definir roles y responsabilidades dentro del equipo, incluyendo líderes de equipo, investigadores de incidentes, comunicadores y coordinadores de respuesta.

- **Desarrollar un plan de gestión de incidentes**

  Crear un plan detallado que describa los procedimientos para la detección, evaluación, notificación, respuesta y recuperación de incidentes de seguridad. Asegurarse de que el plan esté alineado con las pautas y procesos definidos en NIST SP 800-61.

- **Capacitar al personal en detección y respuesta**

  Proporcionar formación y concientización en detección y respuesta a incidentes de seguridad. Entrenar al personal en la identificación de indicadores de compromiso (IOC) y comportamientos anómalos que puedan indicar un incidente de seguridad.

10. Continuidad del Negocio

La continuidad del negocio es crucial para garantizar que una organización pueda mantener sus operaciones en funcionamiento incluso en situaciones adversas, como desastres naturales, ciberataques o interrupciones.

Recomendaciones a considerar:

- **Desarrollo de plan de continuidad del negocio**

  Desarrollar un plan detallado que describa los pasos que se deben seguir para mantener las operaciones en caso de interrupción. Esto puede incluir procedimientos de respuesta a emergencias, asignación de responsabilidades, contactos de emergencia y ubicaciones alternativas de trabajo.
- **Revisión y actualización periódica**

  Revisar y actualizar regularmente plan de continuidad del negocio en función de los cambios en el entorno operativo, las lecciones aprendidas de ejercicios y pruebas anteriores, y las nuevas amenazas y vulnerabilidades identificadas.

11. Pruebas y Evaluación

Planificar auditorías, pruebas de penetración y ejercicios de respuesta a incidentes para garantizar que el plan sea efectivo y se mantenga actualizado.

Recomendaciones a considerar:

- **Planificación de pruebas y evaluaciones**

  Desarrollar un plan detallado que identifique los objetivos, alcance, recursos y cronograma de las pruebas y evaluaciones de seguridad.
- **Seguimiento y revisión continua**

  Realizar un seguimiento de la implementación de las recomendaciones y acciones correctivas derivadas de las pruebas y evaluaciones.

  Revisar periódicamente el plan de pruebas y evaluaciones para garantizar que siga siendo relevante y efectivo en función de los cambios en el entorno operativo y las nuevas amenazas de seguridad.

12. Recursos y Presupuesto

Asegurarse de contar con los recursos necesarios, incluido el presupuesto, para implementar y mantener el Plan de Seguridad Informática y Plan de Continuidad del Negocio.

Recomendaciones a considerar:

- **Establecimiento de criterios de priorización**

  Establecer criterios claros para priorizar la asignación de recursos y presupuesto en función de la criticidad de los activos de información y los riesgos identificados.

  Considerar factores como la probabilidad e impacto de las amenazas, así como los requisitos regulatorios y de cumplimiento.

13. Revisión y Actualización del Plan

Establecer un programa de revisión y actualización periódica de los planes para mantenerlos alineados con las amenazas y necesidades cambiantes.

4.3 Evaluación de confidencialidad, disponibilidad e integridad de la información Aplicabilidad Controles ISO 27002:2022

Para la evaluación del nivel de confidencialidad, disponibilidad e integridad de la información se ha utilizado la aplicabilidad de controles de seguridad de la ISO 27002:2022, para lo que fue necesario realizar un análisis detallado de cada uno de los controles mencionados en relación con los sistemas y procesos del Gobierno Provincial de Imbabura. La matriz de aplicabilidad de controles de seguridad en base a la ISO 27002:2022 y el EGSI se muestra en el Anexo 3.

Confidencialidad

Los controles de acceso y cifrado de datos implementados son efectivos para proteger la confidencialidad de la información.

Sin embargo, es necesario mejorar los controles de acceso, como la autenticación fuerte y la gestión de contraseñas. Además, se deberían implementar medidas de cifrado adicionales para proteger los datos confidenciales. La revisión periódica de permisos garantizara el acceso autorizado y seguro a la información confidencial.

Disponibilidad

Aun no se han establecido planes de continuidad del negocio y procedimientos de respaldo y recuperación de datos, lo que podría afectar la disponibilidad de los sistemas y datos.

Se debe elaborar planes de seguridad informática y de continuidad del negocio, así como realizar pruebas periódicas de los procedimientos de respaldo y recuperación bien definidos para garantizar su efectividad en situaciones de emergencia.

Integridad

Los controles de cambio y los registros de auditoría garantizan la integridad de los datos y la trazabilidad de las actividades del sistema.

Se debe fortalecer la gestión de cambios, asegurando que se documenten adecuadamente y se implementen de manera controlada. Además, es importante mejorar la supervisión y revisión de los registros de auditoría para detectar posibles anomalías o actividades sospechosas.

La evaluación utilizando los controles de seguridad de la ISO 27002:2022 muestra que el GAD provincial de Imbabura tiene una base sólida en términos de seguridad de la información. Sin embargo, existen áreas específicas que requieren atención y mejora continua para fortalecer aún más la protección de los activos de información críticos del GAD. Estos resultados proporcionan una visión clara sobre los aspectos en los que el GAD puede centrarse para mejorar su postura de seguridad de la información y mitigar los riesgos asociados con la confidencialidad, disponibilidad e integridad de la información.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Se ha realizado un diagnóstico de la situación actual en cuanto a la seguridad de la información del área de operaciones y servicios del GPI. Este diagnóstico incluyó la identificación de vulnerabilidades existentes, políticas y controles implementados, así como la capacidad de respuesta ante incidentes de seguridad. Esto proporciona una base sólida para comprender el estado actual de la seguridad informática en la organización.

2. Se ha diseñado un plan de seguridad informática basado en las normas ISO/IEC 27002:2022 y NIST 800-61. Este plan proporciona un marco sólido para mejorar la seguridad de la información en el GPI, abordando aspectos como la gestión de riesgos, políticas de seguridad, controles y procedimientos. El diseño de este plan es un paso crucial hacia la protección de la confidencialidad, integridad y disponibilidad de la información.

3. Se ha evaluado el nivel de confidencialidad, disponibilidad e integridad de la información en el Gobierno Provincial de Imbabura. Estos resultados proporcionan información valiosa sobre cómo se percibe la seguridad de la información en la organización y destacan áreas que requieren mayor atención y mejora.

RECOMENDACIONES

1. Llevar a cabo el esquema plan de seguridad de información basado en ISO/IEC 27002:2022 y NIST 800-61, asignando recursos y estableciendo responsabilidades para cumplir los objetivos de seguridad.

2. Para mejorar concienciación en seguridad se recomienda el desarrollo de programas de formación para que todo el personal comprenda la importancia de la seguridad de la información y las mejores prácticas.

3. Es necesario establecer un proceso claro para la gestión de incidentes esto se lograría definiendo responsables para minimizar impactos de igual manera se debe mantener un registro detallado de incidentes el cual proporcionara datos cruciales para la mejora continua.

4. Es recomendable realizar auditorías y pruebas de seguridad periódicas para identificar debilidades, evaluar la efectividad de los controles y tomar medidas correctivas.

BIBLIOGRAFÍA

Bermudez, Kelly, Bailon, Edber. (2015). Análisis en seguridad informática y seguridad de la información basado en la norma ISO/IEC 27001- Sistemas de Gestión de Seguridad de la Información dirigido a una empresa de servicios financieros. Universidad Politécnica Salesiana Sede Guayaquil.

Código Orgánico Integral Penal. (10 de febrero de 2014). *Registro Oficial Suplemento, 180.* Obtenido de https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Constitución de la República del Ecuador. (25 de enero de 2021). Registro Oficial, 449. págs. https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf.

Contraloría General del Estado. (2023). *Normas técnicas de control interno.* Obtenido de https://www.contraloria.gob.ec/WFDescarga.aspx?id=1487&tipo=mul

Fandom. (2021). *Principios de la seguridad informática: Confidencialidad, Integridad y Disponibilidad de la información.* Obtenido de Fandom.

Garcés, S. (2015). SEGURIDAD INFORMÁTICA PARA LA RED DE DATOS EN LA COOPERATIVA DE AHORRO Y CRÉDITO UNIÓN POPULAR LTDA. Universidad Técnica de Anbato.

Gobierno Autónomo Descentralizado Provincial de Imbabura. (2016). *imbabura.gob.ec.* Obtenido de Estatuto Orgánico por Procesos 2016: https://www.imbabura.gob.ec/index.php/biblioteca/category/63-estatuto-organico-por-procesos

Gobierno Autónomo Descentralizado Provincial de Imbabura. (2023). *imbabura.gob.ec.* Obtenido de Políticas de Seguridad de la Información: https://www.imbabura.gob.ec/phocadownloadpap/S-Actos-legislativos/ResolucionesAdministrativas/resoluciones-administrativas-2023/resolucion_adm_nro_gpi-p-na-02-2023.pdf

Gobierno Autónomo Descentralizado Provincial de Imbabura. (s.f.). *imbabura.gob.ec.* Obtenido de Prefectura Imbabura: https://www.imbabura.gob.ec/index.php/institucion/mision-vision

International Organization for Standardization - ISO. (2022). *ISO/IEC 27002:2022.* Obtenido de https://www.iso.org/standard/75652.html

ISO/IEC 27005. (2022). *Orientación sobre la gestión de riesgos de seguridad de la información.* Obtenido de ISO - International Organization for Standardization: https://es.scribd.com/document/634149413/ISO-IEC-27005-2022-en

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. (17 de abril de 2002). *Registro Oficial Suplemento, 557.* Obtenido de https://www.telecomunicaciones.gob.ec/wp-

content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf

Ley de Propiedad Intelectual. (28 de diciembre de 2006). *Registro Oficial Suplemento, 426.* Obtenido de https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2018/10/Ley-de-Propiedad-Intelectual.pdf

Ley Especial de Telecomunicaciones. (18 de febrero de 2015). (2015), Registro Oficial, 439. págs. https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2016/05/Ley-Org%C3%A1nica-de-Telecomunicaciones.pdf.

Ley Orgánica de Protección de Datos Personales. (21 de mayo de 2021). Obtenido de https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf

Ley Orgánica de Transparencia y Acceso a la Información Pública. (07 de febrero de 2023). Registro Oficial Suplemento 245. págs. https://www.gob.ec/sites/default/files/regulations/2023-08/LOTAIP-2023.pdf.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2019). *Acuerdo-No.-025-2019 Esquema Gubernamental de Seguridad de la Información EGSI.* Obtenido de https://www7.quito.gob.ec/mdmq_ordenanzas/Administraci%C3%B3n%202019-2023/Proyectos%20ordenanzas/214.%20Ordenanza%20Sustitutiva%20Gobierno%20Electr%C3%B3nico/Expediente%20primer%20debate/Aportes/GADDMQ-SDPC-2022-0108/completossinconcordanci.pdf

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2020). *Guía para la Gestión de Riesgos de Seguridad de la Información*. Obtenido de Guía para la Gestión de Riesgos de Seguridad de la Información: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/04/GU%C3%8DA-PARA-LA-GESTI%C3%93N-DE-RIESGOS-DE-SEGURIDAD-DE-LA-INFORMACI%C3%93N-ABRIL-2020.pdf

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2020). *Guía para la implementación del Esquema Gubernamental de Seguridad de la Información.* Obtenido de https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/04/GUÍA-PARA-LA-IMPLEMENTACIÓN-DEL-EGSI-ABRIL2020.pdf

National Institute of Standards and Technology - NIST 800-61. (2012). NIST 800-61 - Guía de Manejo de Incidentes de Seguridad Informática. Subsecretaria de Comercio para los Estándares y Tecnología.

Ruiz, G. (2021). Sistema de Gestión de Seguridad de la Información de servicios en la nube para la empresa “masiva” de la ciudad de Quito, con base en la norma ISO/IEC 27017. Universidad Técnica del Norte, Ibarra, Ecuador.

ANEXOS

ANEXO 1: ISO/IEC 27002:2022

1. **Referencias normativas:** no hay referencias normativas.
2. **Términos, definiciones y términos abreviados:** hace referencia a los siguientes términos y definiciones.
3. **Términos y definiciones**

   3.1 Control de acceso: medios para garantizar que el acceso físico y lógico a los activos esté autorizado y restringido en función de los requisitos de seguridad de la información y del negocio.

   3.2 Activo: cualquier cosa que tenga valor para la organización.

   3.3 Ataque: intento no autorizado exitoso o fallido de destruir, alterar, deshabilitar, obtener acceso a un activo cualquier intento de exponer, robar o hacer uso no autorizado de un activo.

   3.4 Autenticación: provisión de seguridad de que una característica declarada de una entidad es correcta.

   3.5 Autenticidad: propiedad de que una entidad es lo que dice ser.

   3.6 Cadena de custodia: posesión, movimiento, manipulación y ubicación demostrables del material de un momento a otro.

   3.7 Información confidencial: información que no está destinada a estar disponible o divulgada a personas, entidades o procesos no autorizados.

   3.8 Control: medida que mantiene y/o modifica el riesgo.

   3.9 Interrupción: incidente, ya sea anticipado o no, que causa una desviación negativa no planificada de la entrega esperada de productos y servicios de acuerdo con los objetivos de una organización.

   3.10 Dispositivo de punto final: dispositivo de hardware de tecnología de la información y la comunicación (TIC) conectado a la red.

   3.11 Entidad: elemento relevante para el propósito de operación de un dominio que tiene una existencia reconocible y distinta.

   3.12 Instalación de procesamiento de información: cualquier sistema, servicio o infraestructura de procesamiento de información, o la ubicación física que lo alberga.

   3.13 Violación de seguridad de la información: compromiso de la seguridad de la información que conduce a la destrucción, pérdida, alteración, divulgación o acceso

no deseado a información protegida transmitida, almacenada o procesada de otra manera.

3.14 Evento de seguridad de la información: ocurrencia que indica una posible violación de la seguridad de la información o falla de los controles.

3.15 Incidente de seguridad de la información: uno o múltiples eventos de seguridad de la información relacionados e identificados que pueden dañar los activos de una organización o comprometer sus operaciones.

3.16 Gestión de incidentes de seguridad de la información: ejercicio de un enfoque consistente y eficaz para el manejo de incidentes de seguridad de la información.

3.17 Sistema de información: conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes de manejo de información.

3.18 Parte interesada: Interesado. – Persona u organización que puede afectar, verse afectada o percibirse a sí misma como afectada por una decisión o actividad.

3.19 No repudio: capacidad de probar la ocurrencia de un evento o acción reivindicada y sus entidades originarias.

3.20 Personal: personas que trabajan bajo la dirección de la organización.

3.21 Información de identificación personal PII: cualquier información que (a) pueda utilizarse para establecer un vínculo entre la información y la persona física a la que se refiere dicha información, o (b) esté o pueda estar directa o indirectamente vinculada a una persona física.

3.22 Director de PII: Persona física a quien se refiere la información de identificación personal (PII).

3.23 Procesador de PPI: parte interesada en la privacidad que procesa información de identificación personal (PII) en nombre y de acuerdo con las instrucciones de un controlador de PII.

3.24 Política: intenciones y dirección de una organización, expresadas formalmente por su alta dirección.

3.25 Evaluación del impacto en la privacidad PIA: Proceso general de identificación, análisis, evaluación, consulta, comunicación y planificación del tratamiento de posibles impactos en la privacidad con respecto al procesamiento de información de identificación personal (PII), enmarcado dentro de la gestión de riesgos más amplios de una organización. Estructura.

3.26 Procedimiento: forma especificada de llevar a cabo una actividad o un proceso.

3.27 Proceso: Conjunto de actividades interrelacionadas o que interactúan y que utilizan o transforman insumos para producir un resultado.

3.28 Registro: información creada, recibida y mantenida como evidencia y como un activo por una organización o persona, en cumplimiento de obligaciones legales o en la transacción de negocios.

3.29 Objetivo del punto de recuperación RPO: momento en el que se deben recuperar los datos después de que se haya producido una interrupción.

3.30 Objetivo de tiempo de recuperación RTO: Período de tiempo dentro del cual los niveles mínimos de servicios y/o productos y los sistemas, aplicaciones o funciones de soporte deben recuperarse después de que se haya producido una interrupción.

3.31 Fiabilidad: Propiedad del comportamiento y resultados previstos consistentes.

3.32 Regla: principio o instrucción aceptado que establece las expectativas de la organización sobre lo que se debe hacer, lo que está permitido o no.

3.33 Información sensible: información que debe protegerse contra la indisponibilidad, el acceso no autorizado, la modificación o la divulgación pública debido a posibles efectos adversos en un individuo, organización, seguridad nacional o seguridad pública.

3.34 Amenaza: causa potencial de un incidente no deseado, que puede resultar en daño a un sistema u organización.

3.35 Política de tema específico: intenciones y dirección sobre un tema o tema específico, tal como lo expresa formalmente el nivel apropiado de gestión. **EJEMPLO:** Política temática específica sobre control de acceso, política temática específica sobre escritorio y pantalla despejados.

3.36 Usuario: parte interesada con acceso a los sistemas de información de la organización. **EJEMPLO:** Personal, clientes, proveedores.

3.37 Dispositivo de punto final del usuario: dispositivo de punto final utilizado por los usuarios para acceder a los servicios de procesamiento de información.

3.38 Vulnerabilidad: debilidad de un activo o control que puede ser explotado por una o más amenazas.

4. Controles:

Los controles se clasifican en:

a) Controles organizativos, b) Controles de personas, c) Controles físicos, d) Controles tecnológicos.

Tabla 7. Controles de la Norma ISO27002:2022

ID	CONTROL	CATEGORÍA DE CONTROL	TIPO DE CONTROL	PROPIEDAD SEGURIDAD DE LA INFORMACIÓN	CONCEPTO DE CIBERSEGURIDAD (NIST)	CAPACIDAD OPERACIONAL	DOMINIOS DE SEGURIDAD
5.1	Políticas de seguridad de la información	Organizacional	Preventivo	Confidencialidad - Integridad – Disponibilidad	Identificar	Gobernanza	Gobernanza_y_Ecosistema – Resilencia
5.2	Roles y responsabilidades de seguridad de la información	Organizacional	Preventivo	Confidencialidad - Integridad – Disponibilidad	Identificar	Gobernanza	Gobernanza_y_Ecosistema – Protección -Resilencia
5.3	Segregación de funciones	Organizacional	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Gobernanza - Identificar_y_Gestión_de_Acceso	Gobernanza_y_Ecosistema
5.4	Responsabilidades de la dirección	Organizacional	Preventivo	Confidencialidad - Integridad – Disponibilidad	Identificar	Gobernanza	Gobernanza_y_Ecosistema
5.5	Contacto con las autoridades	Organizacional	Preventivo - Correctivo	Confidencialidad - Integridad – Disponibilidad	Identificar -Proteger – Responder - Recuperar	Gobernanza	Defensa -Resilencia
5.6	Contacto con grupos de interés especial	Organizacional	Preventivo - Correctivo	Confidencialidad - Integridad – Disponibilidad	Proteger -Responder – Recuperar	Gobernanza	Defensa
5.7	Inteligencia de amenazas	Organizacional	Preventivo - Detectivo - Correctivo	Confidencialidad - Integridad – Disponibilidad	Identificar -Detectar – Responder	Gestión_de_Amenazas_y_Vulnerabilidades	Defensa -Resilencia
5.8	Seguridad de la información en la gestión de proyectos	Organizacional	Preventivo	Confidencialidad - Integridad – Disponibilidad	Identificar -Proteger	Gobernanza	Gobernanza_y_Ecosistema – Protección
5.9	Inventario de información y otros activos asociados	Organizacional	Preventivo	Confidencialidad - Integridad – Disponibilidad	Identificar	Gestión_de_Activos	Gobernanza_y_Ecosistema – Protección
5.1	Uso aceptable de la información y	Organizacional	Preventivo	Confidencialidad - Integridad –	Proteger	Gestión_de_Activos - Protección_de_Información	Gobernanza_y_Ecosistema – Protección

	otros activos asociados			Disponibilidad			
5.11	Devolución de activos	Organizacional	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Gestión_de_Activos	Protección
5.12	Clasificación de la información	Organizacional	Preventivo	Confidencialidad - Integridad – Disponibilidad	Identificar	Protección_de_Información	Protección -Defensa
5.13	Etiquetado de la información	Organizacional	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Protección_de_Información	Defensa -Protección
5.14	Transferencia de información	Organizacional	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Gestión_de_Activos – Protección_de_Información	Protección
5.15	Control de acceso	Organizacional	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Identificación_y_Gestión_de_Acceso	Protección
5.16	Gestión de identidad	Organizacional	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Identificación_y_Gestión_de_Acceso	Protección
5.17	Información de autenticación	Organizacional	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Identificación_y_Gestión_de_Acceso	Protección
5.18	Derechos de acceso	Organizacional	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Identificación_y_Gestión_de_Acceso	Protección
5.19	Seguridad de la información en las relaciones con los proveedores	Organizacional	Preventivo	Confidencialidad - Integridad – Disponibilidad	Identificar	Seguridad_en_Relaciones_con_Proveedores	Gobernanza_y_Ecosistema – Protección
5.2	Abordar la seguridad de la información en los acuerdos con proveedores	Organizacional	Preventivo	Confidencialidad - Integridad – Disponibilidad	Identificar	Seguridad_en_Relaciones_con_Proveedores	Gobernanza_y_Ecosistema – Protección
5.21	Gestión de la seguridad de la información en la	Organizacional	Preventivo	Confidencialidad - Integridad – Disponibilidad	Identificar	Seguridad_en_Relaciones_con_Proveedores	Gobernanza_y_Ecosistema – Protección

	cadena de suministro de las TIC						
5.22	Monitoreo, revisión y gestión de cambios de servicios de proveedores	Organizacional	Preventivo	Confidencialidad - Integridad – Disponibilidad	Identificar	Seguridad_en_Relaciones_con_Proveedores	Gobernanza_y_Ecosistema – Protección -Defensa – Garantía_Seguridad_de_la_Información
5.23	Seguridad de la información para el uso de servicios en la nube	Organizacional	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Seguridad_en_Relaciones_con_Proveedores	Gobernanza_y_Ecosistema – Protección
5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	Organizacional	Correctivo	Confidencialidad - Integridad – Disponibilidad	Responder - Recuperar	Gobernanza - Seguridad_de_la_información_Gestión_de_Eventos	Defensa
5.25	Evaluación y decisión sobre eventos de seguridad de la información	Organizacional	Detectivo	Confidencialidad - Integridad – Disponibilidad	Detectar -Responder	Seguridad_de_la_información_Gestión_de_Eventos	Defensa
5.26	Respuesta a incidentes de seguridad de la información	Organizacional	Correctivo	Confidencialidad - Integridad – Disponibilidad	Responder - Recuperar	Seguridad_de_la_información_Gestión_de_Eventos	Defensa
5.27	Aprendizaje de los incidentes de seguridad de la información	Organizacional	Preventivo	Confidencialidad - Integridad – Disponibilidad	Identificar -Proteger	Seguridad_de_la_información_Gestión_de_Eventos	Defensa
5.28	Recopilación de evidencias	Organizacional	Correctivo	Confidencialidad - Integridad – Disponibilidad	Detectar -Responder	Seguridad_de_la_información_Gestión_de_Eventos	Defensa
5.29	Seguridad de la información durante la interrupción	Organizacional	Preventivo - Correctivo	Confidencialidad - Integridad – Disponibilidad	Proteger -Responder	Continuidad	Protección -Resiliencia

5.3	Preparación de las TIC para la continuidad del negocio	Organizacional	Correctivo	Disponibilidad	Responder	Continuidad	Resiliencia
5.31	Requisitos legales, estatutarios, reglamentarios y contractuales	Organizacional	Preventivo	Confidencialidad - Integridad – Disponibilidad	Identificar	Legalidad_y_Cumplimiento	Gobernanza_y_Ecosistema – Protección
5.32	Derechos de propiedad intelectual	Organizacional	Preventivo	Confidencialidad - Integridad – Disponibilidad	Identificar	Legalidad_y_Cumplimiento	Gobernanza_y_Ecosistema
5.33	Protección de registros	Organizacional	Preventivo	Confidencialidad - Integridad – Disponibilidad	Identificar -Proteger	Legalidad_y_Cumplimiento – Gestión_de_Activos - Protección_de_Información	Defensa
5.34	Privacidad y protección de PII	Organizacional	Preventivo	Confidencialidad - Integridad – Disponibilidad	Identificar -Proteger	Protección_de_Información - Legalidad_y_Cumplimiento	Protección
5.35	Revisión independiente de la seguridad de la información	Organizacional	Preventivo - Correctivo	Confidencialidad - Integridad – Disponibilidad	Identificar -Proteger	Garantía_Seguridad_de_la_Información	Gobernanza_y_Ecosistema
5.36	Cumplimiento de políticas, normas y estándares de seguridad de la información	Organizacional	Preventivo	Confidencialidad - Integridad – Disponibilidad	Identificar -Proteger	Legalidad_y_Cumplimiento - Garantía_Seguridad_de_la_Información	Gobernanza_y_Ecosistema
5.37	Procedimientos operativos documentados	Organizacional	Preventivo - Correctivo	Confidencialidad - Integridad – Disponibilidad	Proteger -Recuperar	Gestión_de_Activos – Seguridad_Física - Seguridad_en_Sistemas_y_Redes – Seguridad_en_Aplicativos - Configuración_Segura - Identificación_y_Gestión_de_Acceso - Gestión_de_Amenazas_y_Vulnerabilidades – Continuidad - Seguridad_de_la_información_Gestión_de_Eventos	Gobernanza_y_Ecosistema – Protección -Defensa
6.1	Reclutamiento (Screening)	Personas	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Seguridad_Recursos_Humanos	Gobernanza_y_Ecosistema

6.2	Términos y condiciones del empleo.	Personas	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Seguridad_Recursos_Humanos	Gobernanza_y_Ecosistema
6.3	Concientización, educación y capacitación en seguridad de la información	Personas	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Seguridad_Recursos_Humanos	Gobernanza_y_Ecosistema
6.4	Proceso disciplinario	Personas	Preventivo - Correctivo	Confidencialidad - Integridad – Disponibilidad	Proteger -Responder	Seguridad_Recursos_Humanos	Gobernanza_y_Ecosistema
6.5	Responsabilidades después de la terminación o cambio de empleo	Personas	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Seguridad_Recursos_Humanos – Gestión_de_Activos	Gobernanza_y_Ecosistema
6.6	Acuerdos de confidencialidad o de no divulgación	Personas	Preventivo	Confidencialidad	Proteger	Seguridad_Recursos_Humanos - Protección_de_Información - Relaciones_con_Proveedores	Gobernanza_y_Ecosistema
6.7	Teletrabajo (Trabajo a distancia)	Personas	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Gestión_de_Activos – Protección_de_Información - Seguridad_Física – Seguridad_en_Sistemas_y_Redes	Protección
6.8	Reporte de eventos de seguridad de la información	Personas	Detectivo	Confidencialidad - Integridad – Disponibilidad	Detectar	Seguridad_de_la_información_Gestión _de_Eventos	Defensa
7.1	Perímetros de seguridad física	Físico	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Seguridad_Física	Protección
7.2	Entrada física	Físico	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Seguridad_Física – Identificación_y_Gestión_de_Acceso	Protección
7.3	Asegurar oficinas, salas e instalaciones	Físico	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Seguridad_Física – Gestión_de_Activos	Protección

7.4	Monitoreo de la seguridad física	Físico	Preventivo - Detectivo	Confidencialidad - Integridad – Disponibilidad	Proteger -Detectar	Seguridad_Física	Protección -Defensa
7.5	Protección contra amenazas físicas y ambientales.	Físico	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Seguridad_Física	Protección
7.6	Trabajo en áreas seguras	Físico	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Seguridad_Física	Protección
7.7	Escritorio y pantalla limpios	Físico	Preventivo	Confidencialidad	Proteger	Seguridad_Física	Protección
7.8	Emplazamiento y protección de equipos	Físico	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Seguridad_Física – Gestión_de_Activos	Protección
7.9	Seguridad de los activos fuera de las instalaciones	Físico	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Seguridad_Física – Gestión_de_Activos	Protección
7.1	Medios de almacenamiento	Físico	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Seguridad_Física – Gestión_de_Activos	Protección
7.11	Instalaciones de suministro	Físico	Preventivo - Detectivo	Integridad - Disponibilidad	Proteger -Detectar	Seguridad_Física	Protección
7.12	Seguridad del cableado	Físico	Preventivo	Confidencialidad – Disponibilidad	Proteger	Seguridad_Física	Protección
7.13	Mantenimiento de los equipos	Físico	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Seguridad_Física – Gestión_de_Activos	Protección -Resiliencia
7.14	Eliminación o reutilización segura de equipos	Físico	Preventivo	Confidencialidad	Proteger	Seguridad_Física – Gestión_de_Activos	Protección
8.1	Dispositivos de punto final de usuario	Tecnológico	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Gestión_de_Activos – Protección_de_Información	Protección
8.2	Gestión de privilegios de acceso	Tecnológico	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Identificación_y_Gestión_de_Acceso	Protección

8.3	Restricción del acceso a la información	Tecnológico	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Identificación_y_Gestión_de_Acceso	Protección
8.4	Acceso al código fuente	Tecnológico	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Identificación_y_Gestión_de_Acceso - Seguridad_en_Aplicativos – Configuración_Segura	Protección
8.5	Autenticación segura	Tecnológico	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Identificación_y_Gestión_de_Acceso	Protección
8.6	Gestión de capacidad	Tecnológico	Preventivo - Detectivo	Integridad - Disponibilidad	Identificar -Proteger – Detectar	Continuidad	Gobernanza_y_Ecosistema – Protección
8.7	Protección contra malware	Tecnológico	Preventivo - Detectivo - Correctivo	Confidencialidad - Integridad – Disponibilidad	Proteger -Detectar	Seguridad_en_Sistemas_y_Redes - Protección_de_Información	Protección -Defensa
8.8	Gestión de vulnerabilidades técnicas	Tecnológico	Preventivo	Confidencialidad - Integridad – Disponibilidad	Identificar -Proteger	Gestión_de_Amenazas_y_Vulnerabilidades	Gobernanza_y_Ecosistema – Protección -Defensa
8.9	Gestión de la configuración	Tecnológico	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Configuración_Segura	Protección
8.1	Eliminación de información	Tecnológico	Preventivo	Confidencialidad	Proteger	Protección_de_Información - Legalidad_y_Cumplimiento	Protección
8.11	Enmascaramiento de datos	Tecnológico	Preventivo	Confidencialidad	Proteger	Protección_de_Información	Protección
8.12	Prevención de fuga de datos	Tecnológico	Preventivo - Detectivo	Confidencialidad	Proteger -Detectar	Protección_de_Información	Protección -Defensa
8.13	Copias de seguridad de la información	Tecnológico	Correctivo	Integridad - Disponibilidad	Recuperar	Continuidad	Protección
8.14	Redundancia de las instalaciones de procesamiento de información	Tecnológico	Preventivo	Disponibilidad	Proteger	Continuidad – Gestión_de_Activos	Protección -Resiliencia
8.15	Inicio sesión	Tecnológico	Detectivo	Confidencialidad - Integridad – Disponibilidad	Detectar	Seguridad_de_la_información_Gestión_de_Eventos	Protección -Defensa

8.16	Monitoreo de actividades	Tecnológico	Detectivo - Correctivo	Confidencialidad - Integridad – Disponibilidad	Detectar -Responder	Seguridad_de_la_información_Gestión _de_Eventos	Defensa
8.17	Sincronización de reloj	Tecnológico	Detectivo	Integridad	Proteger -Detectar	Seguridad_de_la_información_Gestión _de_Eventos	Protección -Defensa
8.18	Uso de utilidades con privilegios del sistema	Tecnológico	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Seguridad_en_Sistemas_y_Redes – Configuración_Segura – Seguridad_en_Aplicativos	Protección
8.19	Instalación de software en sistemas operativos	Tecnológico	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Configuración_Segura – Seguridad_en_Aplicativos	Protección
8.2	Seguridad en redes	Tecnológico	Preventivo - Detectivo	Confidencialidad - Integridad – Disponibilidad	Proteger -Detectar	Seguridad_en_Sistemas_y_Redes	Protección
8.21	Seguridad de los servicios de red.	Tecnológico	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Seguridad_en_Sistemas_y_Redes	Protección
8.22	Segregación de redes	Tecnológico	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Seguridad_en_Sistemas_y_Redes	Protección
8.23	Filtrado web	Tecnológico	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Seguridad_en_Sistemas_y_Redes	Protección
8.24	Uso de criptografía	Tecnológico	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Configuración_Segura	Protección
8.25	Política de desarrollo seguro	Tecnológico	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Seguridad_en_Aplicativos - Seguridad_en_Sistemas_y_Redes	Protección
8.26	Requerimientos de seguridad en aplicaciones	Tecnológico	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Seguridad_en_Aplicativos - Seguridad_en_Sistemas_y_Redes	Protección -Defensa
8.27	Principios de arquitectura e ingeniería de	Tecnológico	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Seguridad_en_Aplicativos - Seguridad_en_Sistemas_y_Redes	Protección

	sistemas seguros						
8.28	Codificación segura	Tecnológico	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Seguridad_en_Aplicativos - Seguridad_en_Sistemas_y_Redes	Protección
8.29	Pruebas de seguridad en el desarrollo y la aceptación	Tecnológico	Preventivo	Confidencialidad - Integridad – Disponibilidad	Identificar	Seguridad_en_Aplicativos - Garantía_Seguridad_de_la_Información - Seguridad_en_Sistemas_y_Redes	Protección
8.3	Externalización del desarrollo de software	Tecnológico	Preventivo - Detectivo	Confidencialidad - Integridad – Disponibilidad	Identificar -Proteger – Detectar	Seguridad_en_Sistemas_y_Redes – Seguridad_en_Aplicativos – Seguridad_en_Relaciones_con_Proveedores	Gobernanza_y_Ecosistema – Protección
8.31	Separación de los entornos de desarrollo, prueba y producción	Tecnológico	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Seguridad_en_Aplicativos - Seguridad_en_Sistemas_y_Redes	Protección
8.32	Gestión del cambio	Tecnológico	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Seguridad_en_Aplicativos - Seguridad_en_Sistemas_y_Redes	Protección
8.33	Información de prueba	Tecnológico	Preventivo	Confidencialidad - Integridad	Proteger	86rotección_de_Información	Protección
8.34	Protección de los sistemas de información durante las pruebas de auditoría	Tecnológico	Preventivo	Confidencialidad - Integridad – Disponibilidad	Proteger	Seguridad_en_Sistemas_y_Redes - Protección_de_Información	Gobernanza_y_Ecosistema – Protección

Fuente: (ISO/IEC 27002, 2022)

ANEXO 2: Encuesta sobre seguridad informática en el GAD Provincial de Imbabura

1. ¿Actualmente cuentan con un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27002:2022?
   Sí
   No
   No estoy seguro

2. ¿Existe en el Gobierno Provincial de Imbabura una determinación específica del área de Operaciones y Servicios dentro de un sistema de gestión?
   Sí
   No
   No estoy seguro

3. Dentro de la Subdirección de Tecnologías de Información, ¿Existe una persona responsable de gestionar los incidentes de ciberseguridad?
   Sí
   No
   No estoy seguro

4. ¿Se mantiene un registro de incidentes de seguridad, como brechas de datos ciberataques, en el Gobierno Provincial de Imbabura (GPI)?
   Sí
   No
   No estoy seguro

5. ¿El GPI cuenta con políticas de seguridad informática que estén claramente establecidas y documentadas?
   Sí
   No
   No estoy seguro

6. ¿Existen procedimientos de seguridad informática para la detección de incidentes de ciberseguridad?

Sí

No

No estoy seguro

7. ¿El personal del área de operaciones y servicios del GPI está al tanto de las políticas y procedimientos de seguridad?

Sí

No

No estoy seguro

8. ¿Se ha diseñado o implementado un plan de seguridad informática en el GPI?

Sí

No

No estoy seguro

9. ¿Se realizan evaluaciones regulares de riesgos y vulnerabilidades en el GPI para identificar posibles amenazas a la seguridad informática?

Sí

No

No estoy seguro

10. ¿El GPI implementa controles de seguridad técnicos, como firewalls, antivirus y sistemas de detección de intrusiones?

SÍ

No

No estoy seguro

11. ¿Se realizan auditorías regulares de seguridad en los sistemas y redes del GPI?

Sí

No

No estoy seguro

12. ¿El personal del área de operaciones y servicios recibe capacitación en seguridad informática de manera regular?

Sí

No

No estoy seguro

13. ¿Se capacita al resto del personal de la institución en temas relacionados a la ciberseguridad?

Sí

No

No estoy seguro

14. ¿Cómo calificaría el nivel de confidencialidad de la información en el GPI?

Escala del 1 al 5, siendo 1 muy bajo y 5 muy alto)

1 2 3 4 5

15. ¿Cómo calificaría el nivel de disponibilidad de la información en el GPI?

(Escala del 1 al 5, siendo 1 muy bajo y 5 muy alto)

1 2 3 4 5

16. ¿Cómo calificaría el nivel de integridad de la información en el GPI?

(Escala del 1 al 5, siendo 1 muy bajo y 5 muy alto)

1 2 3 4 5

ANEXO 3: Aplicabilidad Controles ISO 27002:2022

Tabla 8. Aplicabilidad Controles ISO 27002:2022

CONTROLES ISO 27002:2022							
Nro.	**Título del Control**		**Control**	**Aplicabilidad**		**Justificación**	**Recomendación**
				SI	**NO**		
	5. Controles Organizacionales						
1	**5.1**	Políticas de seguridad de la información	La política de seguridad de la información y las políticas específicas de cada tema deben ser definidas, aprobadas por la dirección, publicada, comunicada y reconocida por el personal relevante y las partes interesadas relevantes, y revisadas a intervalos planificados y si se producen cambios significativos.	X			Realizar una difusión mensual mediante correo electrónico.
2	**5.2**	Roles y responsabilidades de seguridad de la información	Las funciones y responsabilidades de seguridad de la información deben definirse y asignarse de acuerdo con las necesidades de la organización.	X			
3	**5.3**	Segregación de funciones	Deben separarse los deberes y áreas de responsabilidad conflictivos.	X		Segmentación de redes a nivel de firewall, las políticas de navegación están gestionadas por el ActiveDirectory Área de TI, con reglas claras, pero procesos no normalizados.	
4	**5.4**	Responsabilidades de la dirección	La gerencia debe exigir que todo el personal aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y los procedimientos específicos de cada tema de la organización.	X		Es necesario promover la difusión y comprensión de la política de seguridad de la información.	Administrar el seguimiento del cumplimiento de la política de seguridad de la información.
5	**5.5**	Contacto con las autoridades	La organización debe establecer y mantener contacto con las autoridades pertinentes.	X			Actualizar regularmente la información de contacto de los proveedores de bienes o

							servicios de telecomunicaciones o acceso a internet, con el fin de facilitar la gestión efectiva de posibles incidentes.
6	**5.6**	Contacto con grupos de interés especial	La organización debe establecer y mantener contacto con grupos de intereses especiales u otros foros especializados en seguridad y asociaciones profesionales.	X			
7	**5.7**	Inteligencia de amenazas	La información relacionada con las amenazas a la seguridad de la información debe recopilarse y analizarse para producir inteligencia sobre amenazas.	X		NGFW (Next Generation Firewall), Escáner de vulnerabilidades, monitoreo de salud de la infraestructura, SOC (Security Operation Center) de Telconet, Gateway de seguridad de correo	
8	**5.8**	Seguridad de la información en la gestión de proyectos	La seguridad de la información debe integrarse en la gestión de proyectos.	X		Procesos de compras públicas se encuentran implementados, falta normalizar procesos en las otras áreas.	
9	**5.9**	Inventario de información y otros activos asociados	Se debe desarrollar y mantener un inventario de información y otros activos asociados, incluidos los propietarios.	X		La evaluación solamente fue realizada en área de TI	
10	**5.10**	Uso aceptable de la información y otros activos asociados	Se deben identificar, documentar e implementar reglas para el uso aceptable y procedimientos para el manejo de la información y otros activos asociados.	X		La evaluación solamente fue realizada en área de TI	
11	**5.11**	Devolución de activos	El personal y otras partes interesadas, según corresponda, deben devolver todos los activos de la organización que estén en su poder en caso de cambio o terminación de su empleo, contrato o acuerdo.	X		Existe un proceso, pero no está normalizado	Optimizar el procedimiento de terminación de la relación laboral mediante la formalización de un proceso que comprenda la entrega de software, documentos corporativos y equipos asignados.

12	**5.12**	Clasificación de la información	La información debe clasificarse de acuerdo con las necesidades de seguridad de la información de la organización en función de la confidencialidad, integridad, disponibilidad y los requisitos relevantes de las partes interesadas.	X		La resolución se encuentra en estado pendiente.	Los responsables de los activos de información asuman la responsabilidad de clasificarlos, con la asesoría del departamento legal de la institución, garantizando así una adecuada gestión y protección de la información.
13	**5.13**	Etiquetado de la información	Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de información de acuerdo con el esquema de clasificación de información adoptado por la organización.	X		Existe un proceso, pero no está normalizado	Formalizar el procedimiento de control y etiquetado de activos de información, para cumplimiento de las áreas pertinentes.
14	**5.14**	Transferencia de información	Deben existir reglas, procedimientos o acuerdos de transferencia de información para todo tipo de instalaciones de transferencia dentro de la organización y entre la organización y otras partes.	X			Establecer reglas, procedimientos y acuerdos específicos para la transferencia de información. Protocolos que deben ser comunicados a todos los involucrados, garantizando así una gestión segura y eficiente de la información en todas transacciones de la organización.
15	**5.15**	Control de acceso	Se deben establecer e implementar reglas para controlar el acceso físico y lógico a la información y otros activos asociados en función de los requisitos de seguridad de la información y del negocio.	X		Se ha tomado en cuenta en las políticas y se han establecido controles correspondientes.	
16	**5.16**	Gestión de identidad	Se debe gestionar el ciclo de vida completo de las identidades.	X		La identificación única de personas y sistemas que acceden a la información de organización está gestionado mediante el Active Directory.	
17	**5.17**	Información de autenticación	La asignación y gestión de la información de autenticación debe controlarse mediante un proceso de gestión, incluido el asesoramiento al personal sobre el manejo adecuado de la información de autenticación.	X		La política está presente, pero aún falta llevar a cabo la socialización correspondiente.	

18	**5.18**	Derechos de acceso	Los derechos de acceso a la información y otros activos asociados deben proporcionarse, revisarse, modificarse y eliminarse de acuerdo con la política temática específica de la organización y las reglas para el control de acceso.	X		Las credenciales de acceso y privilegios están gestionadas mediante Active Directory.	
19	**5.19**	Seguridad de la información en las relaciones con los proveedores	Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor.	X			Establecer procesos para gestionar riesgos de seguridad en productos o servicios de proveedores, incluyendo vulnerabilidades, acceso no autorizado, y pérdida de datos.
20	**5.20**	Abordar la seguridad de la información en los acuerdos con proveedores	Los requisitos de seguridad de la información relevantes deben establecerse y acordarse con cada proveedor en función del tipo de relación con el proveedor.	X			Definir acuerdos de recuperación y contingencia para asegurar la disponibilidad de la información.
21	**5.21**	Gestión de la seguridad de la información en la cadena de suministro de las TIC	Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de TIC.	X			Implementar un proceso de monitoreo para validar que los productos de TIC entregados cumplan con las normas de seguridad.
22	**5.22**	Monitoreo, revisión y gestión de cambios de servicios de proveedores	La organización debe monitorear, revisar, evaluar y gestionar periódicamente los cambios en las prácticas de seguridad de la información de los proveedores y en la prestación de servicios.	X			Realizar un monitoreo constante del rendimiento para verificar el cumplimiento de los niveles de servicio esperados por la institución, de acuerdo con los términos establecidos en el contrato.
23	**5.23**	Seguridad de la información para el uso de servicios en la nube	Los procesos de adquisición, uso, gestión y salida de los servicios en la nube deben establecerse de acuerdo con los requisitos de seguridad de la información de la organización.	X			Establecer los procesos de adquisición, utilización, administración y desvinculación de los servicios en la nube en estricta conformidad con los requisitos de seguridad de la información de la organización.
24	**5.24**	Planificación y preparación de la gestión de incidentes de seguridad de la información	La organización debe planificar y prepararse para gestionar incidentes de seguridad de la información definiendo, estableciendo y comunicando procesos, roles y responsabilidades de gestión de incidentes de seguridad de la información.	X			Planificar y preparar la gestión de incidentes de seguridad de la información mediante la definición de procesos, roles y responsabilidades.

25	**5.25**	Evaluación y decisión sobre eventos de seguridad de la información	La organización debe evaluar los eventos de seguridad de la información y decidir si deben clasificarse como incidentes de seguridad de la información.	X		La evaluación y la clasificación de incidentes se la realiza en la mesa de ayuda (Help desk).	
26	**5.26**	Respuesta a incidentes de seguridad de la información	Los incidentes de seguridad de la información deben responderse de acuerdo con los procedimientos documentados.	X		Existen procedimientos documentados para la respuesta a incidentes dependiendo de la prioridad y complejidad de los incidentes.	
27	**5.27**	Aprendizaje de los incidentes de seguridad de la información	El conocimiento adquirido a partir de incidentes de seguridad de la información debe utilizarse para fortalecer y mejorar los controles de seguridad de la información.	X		En el sistema de mesa de ayuda (Help desk) se lleva el registro de la resolución de incidentes generándose una base de conocimiento.	
28	**5.28**	Recopilación de evidencias	La organización debe establecer e implementar procedimientos para la identificación, recopilación, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información.	X			Establecer y seguir procedimientos internos para la recolección y presentación de evidencia en eventos de seguridad informática.
29	**5.29**	Seguridad de la información durante la interrupción	La organización debe planificar cómo mantener la seguridad de la información en un nivel apropiado durante la interrupción.	X			Establecer niveles apropiados de seguridad de la información que deben mantenerse durante la interrupción, considerando la criticidad de los datos y sistemas.
30	**5.30**	Preparación de las TIC para la continuidad del negocio	La preparación de las TIC debe planificarse, implementarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.	X			El responsable del área de tecnologías de información s94era la persona encargada de coordinar la continuidad de los servicios informáticos.
31	**5.31**	Requisitos legales, estatutarios, reglamentarios y contractuales	Los requisitos legales, estatutarios, regulatorios y contractuales relevantes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos deben identificarse, documentarse y mantenerse actualizados.	X			Inventariar todas la normas legales, estatutarias, reglamentarias y contractuales pertinentes para cada programa de software, servicio informático y en general todo activo de información que utiliza la institución.
32	**5.32**	Derechos de propiedad intelectual	La organización debe implementar procedimientos apropiados para proteger los derechos de propiedad intelectual.	X			Elaborar, implementar y socializar una política para el cumplimiento de los derechos de propiedad intelectual, definiendo el uso legal de aplicativos y del software intelectual.

33	**5.33**	Protección de registros	Los registros deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada.	X			Clasificar los registros electrónicos y físicos por tipos, especificando los periodos de retención y los medios de almacenamiento, como discos.
34	**5.34**	Privacidad y protección de PII (Información de Identificación Personal)	La organización debe identificar y cumplir los requisitos relacionados con la preservación de la privacidad y la protección de la PII de acuerdo con las leyes, regulaciones y requisitos contractuales aplicables.	X			Implementar medidas técnicas y organizacionales apropiada para gestionar de manera responsable la información personal de acuerdo con la legislación correspondientes.
35	**5.35**	Revisión independiente de la seguridad de la información	El enfoque de la organización para gestionar la seguridad de la información y su implementación, incluidas las personas, los procesos y las tecnologías, debe revisarse de forma independiente a intervalos planificados o cuando se produzcan cambios significativos.	X			Revisar en intervalos regulares reportes e informes de seguridad de sistemas de información.
36	**5.36**	Cumplimiento de políticas, normas y estándares de seguridad de la información	Se debe revisar periódicamente el cumplimiento de la política de seguridad de la información de la organización, las políticas, reglas y estándares específicos de cada tema.	X			Evaluar acciones necesarias para el cumplimiento de las políticas y normas de seguridad.
37	**5.37**	Procedimientos operativos documentados	Los procedimientos operativos para las instalaciones de procesamiento de información deben documentarse y ponerse a disposición del personal que los necesite.	X			Documentar los procesos de servicios de procesamiento de datos, incluyendo la interrelación con otros sistemas.
6 CONTROL DE PERSONAS							
38	**6.1**	Reclutamiento (Screening)	Se deben realizar verificaciones de antecedentes de todos los candidatos a formar parte del personal antes de unirse a la organización y de manera continua, teniendo en cuenta las leyes, regulaciones y ética aplicables, y ser proporcionales a los requisitos del negocio, la clasificación de la información a la que se accederá y los riesgos percibidos.	X			
39	**6.2**	Términos y condiciones del empleo.	Los acuerdos contractuales de empleo deben establecer las responsabilidades del personal y de la organización en materia de seguridad de	X			Socializar los derechos y responsabilidades legales de los empleados, contratistas y cualquier otro usuario sobre la protección de

			la información.				datos y derechos de propiedad intelectual.
40	**6.3**	Concientización, educación y capacitación en seguridad de la información	El personal de la organización y las partes interesadas relevantes deben recibir concientización, educación y capacitación adecuadas sobre seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, políticas y procedimientos específicos de temas, según sea relevante para su función laboral.	X			Capacitar de forma periódica al menos una vez al año sobre las normas y procedimientos para la seguridad de información.
41	**6.4**	Proceso disciplinario	Se debe formalizar y comunicar un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación de la política de seguridad de la información.	X			Establecer y comunicar un procedimiento disciplinario claro para abordar violaciones a la política de seguridad de la información.
42	**6.5**	Responsabilidades después de la terminación o cambio de empleo	Las responsabilidades y deberes de seguridad de la información que siguen siendo válidos después de la terminación o el cambio de empleo deben definirse, hacerse cumplir y comunicarse al personal relevante y otras partes interesadas.	X			Socializar los derechos y responsabilidades legales de los empleados, contratistas y cualquier otro usuario sobre la protección de datos y derechos de propiedad intelectual.
43	**6.6**	Acuerdos de confidencialidad o de no divulgación	Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deben ser identificados, documentados, revisados periódicamente y firmados por el personal y otras partes interesadas relevantes.				Establecer acuerdos de confidencialidad o no divulgación, antes de que los empleados, contratistas y usuarios de terceras partes, tengan acceso a la información.

44	**6.7**	Teletrabajo (Trabajo a distancia)	Se deben implementar medidas de seguridad cuando el personal trabaja de forma remota para proteger la información a la que se accede, procesa o almacena fuera de las instalaciones de la organización.	X			Provisión de equipos para actividades de teletrabajo, donde no se permita el uso de equipos privados que no estén bajo el control de la institución.
45	**6.8**	Reporte de eventos de seguridad de la información	La organización debe proporcionar un mecanismo para que el personal informe eventos de seguridad de la información observados o sospechados a través de canales apropiados de manera oportuna.	X			Establecer un procedimiento formal para el reporte de los eventos de seguridad de la información.
7 CONTROLES FÍSICOS							
46	**7.1**	Perímetros de seguridad física	Se deben definir y utilizar perímetros de seguridad para proteger áreas que contienen información y otros activos asociados.	X		Se dispone de sistema de vigilancia.	
47	**7.2**	Entrada física	Las áreas seguras deben estar protegidas por controles de entrada y puntos de acceso adecuados.	X		Existen perímetros de seguridad como puertas de acceso controladas con tarjetas y reconocimiento facial.	
48	**7.3**	Asegurar oficinas, salas e instalaciones	Se debe diseñar e implementar la seguridad física para oficinas, salas e instalaciones.	X			Proteger las instalaciones de tal manera que se evite el acceso libre al público, establecer sitios adecuados para recepción y procesamiento de trámites.
49	**7.4**	Monitoreo de la seguridad física	Las instalaciones deben ser monitoreadas continuamente para detectar accesos físicos no autorizados.	X		Se dispone de sistema de vigilancia.	
50	**7.5**	Protección contra amenazas físicas y ambientales.	Se debe diseñar e implementar protección contra amenazas físicas y ambientales, como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura.	X			Realizar una evaluación exhaustiva de los riesgos y vulnerabilidades específicos a los que está expuesta la infraestructura. Para identificar posibles amenazas naturales (terremotos, inundaciones, incendios forestales, etc.) y amenazas humanas (vandalismo, terrorismo,

							robos, etc.).
51	**7.6**	Trabajo en áreas seguras	Se deben diseñar e implementar medidas de seguridad para trabajar en áreas seguras.	X			Realizar una evaluación exhaustiva de los riesgos presentes en las áreas de trabajo. Para identificar posibles peligros físicos, químicos, biológicos o ergonómicos, así como riesgos de seguridad informática en entornos digitales.
52	**7.7**	Escritorio despejado y pantalla limpia	Se deben definir y hacer cumplir adecuadamente reglas claras de escritorio para documentos y medios de almacenamiento extraíbles y reglas claras de pantalla para las instalaciones de procesamiento de información.	X		Active directory activa pantalla de bloqueo a los equipos en un tiempo determinado sin uso.	
53	**7.8**	Ubicación y protección de equipos	El equipo debe estar ubicado de forma segura y protegida.	X			Proteger equipos que procesan información sensible para minimizar el riesgo de fugas de información.
54	**7.9**	Seguridad de los activos fuera de las instalaciones	Se deben proteger los activos externos.	X			Los equipos y dispositivos retirados de las instalaciones no deben quedar sin supervisión en espacios públicos.
55	**7.10**	Medios de almacenamiento	Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.	X			Crear un esquema de clasificación y un plan integral para gestionar de manera segura la información almacenada en los medios, considerando su importancia y sensibilidad.
56	**7.11**	Instalaciones de suministro	Las instalaciones de procesamiento de información deben protegerse de cortes de energía y otras interrupciones causadas por fallas en los servicios públicos de soporte.	X			Inspeccionar regularmente todos los sistemas de suministro mediante pruebas apropiadas.
57	**7.12**	Seguridad del cableado	Los cables que transportan energía, datos o servicios de información de soporte deben protegerse contra interceptaciones, interferencias o daños.	X			Proteger el cableado de la red contra la interceptación o daño.

58	**7.13**	Mantenimiento de los equipos	El equipo debe mantenerse correctamente para garantizar la disponibilidad, integridad y confidencialidad de la información.	X		Se realiza mantenimientos periódicos a los equipos y dispositivos, de acuerdo con las especificaciones y recomendaciones del proveedor.	
59	**7.14**	Eliminación o reutilización segura de equipos	Los elementos del equipo que contienen medios de almacenamiento deben verificarse para garantizar que todos los datos confidenciales y el software con licencia se hayan eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.	X			Evaluar dispositivos dañados con información sensible y software licenciado antes de repararlos, decidiendo entre borrar datos, eliminar físicamente o reutilizar según sea necesario.
8 CONTROLES TECNOLÓGICOS							
60	**8.1**	Dispositivos de punto final de usuario	La información almacenada, procesada o accesible a través de dispositivos terminales de usuario debe estar protegida.	X			Proteger la información en dispositivos terminales de usuario mediante autenticación fuerte, cifrado de datos, actualizaciones regulares, políticas de uso seguro, gestión de dispositivos móviles, restricciones de acceso, capacitación continua, auditorías de seguridad, respuesta a incidentes, copias de seguridad y gestión de licencias de software.
61	**8.2**	Gestión de privilegios de acceso	La asignación y el uso de derechos de acceso privilegiados deben restringirse y gestionarse.	X		La identificación de los usuarios y sus privilegios se gestión a través del Active Directory	
62	**8.3**	Restricción del acceso a la información	El acceso a la información y otros activos asociados debe restringirse de acuerdo con la política temática establecida sobre control de acceso.	X			Monitorear cuales son los datos a los que acceda un usuario determinado, de acuerdo con el perfil definido.
63	**8.4**	Acceso al código fuente	El acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las bibliotecas de software debe gestionarse adecuadamente.	X			Asignar a un administrador del código fuente de programas y software.
64	**8.5**	Autenticación segura	Se deben implementar tecnologías y procedimientos de autenticación segura basados en las restricciones de acceso a la información y la política temática específica sobre control de acceso.		X		

65	**8.6**	Gestión de capacidad	El uso de los recursos debe monitorearse y ajustarse de acuerdo con los requisitos de capacidad actuales y esperados.		X		
66	**8.7**	Protección contra malware	La protección contra el malware debe implementarse y respaldarse mediante una adecuada concienciación de los usuarios.	X			Elaborar, implementar y socializar una política formal para prohibir el uso de software no autorizado.
67	**8.8**	Gestión de vulnerabilidades técnicas	Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a dichas vulnerabilidades y se deben tomar las medidas apropiadas.		X		
68	**8.9**	Gestión de la configuración	Se deben establecer, documentar, implementar, monitorear y revisar las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes.		X		
69	**8.10**	Eliminación de información	La información almacenada en sistemas, dispositivos o cualquier otro medio de almacenamiento de información deberá eliminarse cuando ya no sea necesaria.		X		
70	**8.11**	Enmascaramiento de datos	El enmascaramiento de datos debe usarse de acuerdo con la política temática específica de la organización sobre control de acceso y otras políticas específicas relacionadas y requisitos comerciales, teniendo en cuenta la legislación aplicable.		X		
71	**8.12**	Prevención de fuga de datos	Se deben aplicar medidas de prevención de fuga de datos a sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información confidencial.		X		
72	**8.13**	Copias de seguridad de la información	Las copias de seguridad de la información, el software y los sistemas deben mantenerse y probarse periódicamente de acuerdo con la política temática específica acordada sobre copias de seguridad.	X			Elaborar, implementar y socializar política de respaldos de información.

73	**8.14**	Redundancia de las instalaciones de procesamiento de información	Las instalaciones de procesamiento de información deben implementarse con redundancia suficiente para cumplir con los requisitos de disponibilidad.		X		
74	**8.15**	Inicio sesión	Se deben producir, almacenar, proteger y analizar registros que registren actividades, excepciones, fallas y otros eventos relevantes.	X			Establecer e implementar un procedimiento seguro de inicio de sesión con autentificación robusta.
75	**8.16**	Monitoreo de actividades	Se deben monitorear las redes, sistemas y aplicaciones para detectar comportamientos anómalos y se deben tomar las acciones adecuadas para evaluar posibles incidentes de seguridad de la información.	X		Existe segmentación de red.	Realizar capacitación al personal y realizar simulacros de respuesta a incidentes para mejorar continuamente la seguridad.
76	**8.17**	Sincronización de reloj	Los relojes de los sistemas de procesamiento de información utilizados por la organización deben estar sincronizados con las fuentes horarias aprobadas.	X			Verificar y corregir cualquier variación de relojes en sistema de procesamiento donde el tiempo es factor clave.
77	**8.18**	Uso de utilidades con privilegios del sistema	El uso de programas de utilidad que puedan anular los controles del sistema y de las aplicaciones debe restringirse y controlarse estrictamente.	X			
78	**8.19**	Instalación de software en sistemas operativos	Se deben implementar procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas operativos.	X			Establecer procedimientos para controlar la instalación adecuada de software.
79	**8.20**	Seguridad en redes	Las redes y los dispositivos de red deben protegerse, administrarse y controlarse para proteger la información en los sistemas y aplicaciones.	X			Establecer responsabilidades y los procedimientos para la administración de los equipos en la infraestructura de red.
80	**8.21**	Seguridad de los servicios de red.	Se deben identificar, implementar y monitorear los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red.	X			Definir e implementar parámetros técnicos para conexiones seguras, de acuerdo con la necesidad institucional.
81	**8.22**	Segregación de redes	Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en las redes de la organización.	X			

82	**8.23**	Filtrado web	El acceso a sitios web externos debe gestionarse para reducir la exposición a contenido malicioso.	X			
83	**8.24**	Uso de criptografía	Deben definirse e implementarse reglas para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas.	X		Fue adquirido, se proporcionaron directrices, implementación pendiente.	
84	**8.25**	Política de desarrollo seguro	Se deben establecer y aplicar reglas para el desarrollo seguro de software y sistemas.	X			Definir política y socializar al área de desarrollo de software.
85	**8.26**	Requerimientos de seguridad en aplicaciones	Los requisitos de seguridad de la información deben identificarse, especificarse y aprobarse al desarrollar o adquirir aplicaciones.	X			Definir requerimientos de seguridad. Ejemplo: criptografía, control de sesiones.
86	**8.27**	Principios de arquitectura e ingeniería de sistemas seguros	Se deben establecer, documentar, mantener y aplicar principios para diseñar sistemas seguros a cualquier actividad de desarrollo de sistemas de información.	X			Determinar permisos mínimos al inicio, para ir escalando privilegios de acuerdo con los perfiles establecidos en el diseño.
87	**8.28**	Codificación segura	Los principios de codificación segura deben aplicarse al desarrollo de software.		X	No existe un escáner de vulnerabilidades de código.	
88	**8.29**	Pruebas de seguridad en el desarrollo y la aceptación	Los procesos de prueba de seguridad deben definirse e implementarse en el ciclo de vida del desarrollo.	X			
89	**8.30**	Externalización del desarrollo de software	La organización debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo del sistema subcontratado.		X		
90	**8.31**	Separación de los entornos de desarrollo, prueba y producción	Los entornos de desarrollo, prueba y producción deben estar separados y asegurados.	X		Se encuentra definido y documentado entornos de desarrollo, pruebas y producción.	
91	**8.32**	Gestión del cambio	Los cambios en las instalaciones de procesamiento de información y los sistemas de información deben estar sujetos a procedimientos de gestión de cambios.	X			Identificar y registrar los cambios significativos.
92	**8.33**	Información de prueba	La información de las pruebas debe seleccionarse, protegerse y gestionarse adecuadamente.		X		

93	**8.34**	Protección de los sistemas de información durante las pruebas de auditoría	Las pruebas de auditoría y otras actividades de aseguramiento que implican la evaluación de sistemas operativos deben planificarse y acordarse entre el evaluador y la dirección correspondiente.			No hay auditorías	

Fuente: Elaboración Propia