

UNIVERSIDAD CATÓLICA DE CUENCA



Maestría en Ciberseguridad

**Informe de Investigación previo a la obtención del título de
Magíster en Ciberseguridad**

Tema: Programa de Ciberseguridad aplicado en el Ministerio de Defensa
Nacional del Ecuador para enforzar el cumplimiento del
Esquema Gubernamental de Seguridad de la Información v2.0.

Autor: Ing. Santiago Roberto Andrade Burbano

Asesores: Ing. Daniel Andrade Pesántez. Mg

Ing. Juan Carlos Ortega Castro. Mg

Cuenca, 2024

Certificación de Asesores

Se certifica que:

El informe de investigación “Programa de Ciberseguridad aplicado en el Ministerio de Defensa Nacional del Ecuador para enforzar el cumplimiento del Esquema Gubernamental de Seguridad de la Información v2.0”, de autoría del Señor Ingeniero en Electrónica y Telecomunicaciones Santiago Roberto Andrade Burbano, CC: 1002510533, ecuatoriano, previo a la obtención del Título de Cuarto Nivel o Posgrado correspondiente a Magíster en Ciberseguridad, cumple con la caracterización y estructura (parte protocolaria y parte expositiva) y se sujeta a la normativa pertinente exigida por el Consejo de Educación Superior, CES y la Universidad Católica de Cuenca, en consecuencia se autoriza su presentación para los trámites pertinentes.

Santa Ana de los Cuatro Ríos de Cuenca

Septiembre, 2024

Ing. Daniel Jacobo Andrade Pesántez Mg
Asesor Científico

Ing. Juan Carlos Ortega Castro. Mg
Asesor Metodológico

Certificación de Autoría

Certifico que:

“Programa de Ciberseguridad aplicado en el Ministerio de Defensa Nacional del Ecuador para enforzar el cumplimiento del Esquema Gubernamental de Seguridad de la Información v2.0”, es el tema del informe final de investigación de mi AUTORÍA, previo a la obtención del Título de Cuarto Nivel o Posgrado correspondiente a Magíster en Ciberseguridad, por lo que, asumo su originalidad y el uso de fuentes de terceros registrados según las normas APA vigentes.

Santa Ana de los Cuatro Ríos de Cuenca

Septiembre, 2024



Firmado electrónicamente por:
**SANTIAGO ROBERTO
ANDRADE BURBANO**

Ing. Santiago Roberto Andrade Burbano

CC: 1002510533

Agradecimiento

Permitidme expresar este sentido y sincero agradecimiento, primeramente, a Dios por las fuerzas, valentía y abnegación que me ha proporcionado para la realización de este trabajo de investigación, que representa un importante objetivo en mi camino hacia alcanzar este objetivo académico dentro de mi vida profesional como lo es el de magister en Ciberseguridad.

También quiero agradecer a mi esposa y mis hijos por su comprensión y apoyo incondicional a fin de que se me permitiera encontrar un ambiente necesario para realizar mi trabajo de investigación; a mi padres y hermanos agradecerles porque siempre están presentes en cada paso que doy desde muy pequeño; agradecer especialmente a mi tutor Ing. Daniel Andrade, quien con sus instrucciones y conocimientos brindados han permitido culminar este proyecto de titulación.

Por último, quisiera expresar mi gratitud a todas las personas que participaron en mi trabajo de investigación y que incondicionalmente me ayudaron dedicándome su tiempo y conocimientos para ayudar a enriquecer mis hallazgos.

Este logro no habría sido posible sin el apoyo y contribución de cada una de estas personas. A todos ustedes, ¡Dios les pague....!"

Dedicatoria

"A mi esposa y mis hijos, que han sido mi fuente de inspiración y apoyo incondicional durante este arduo camino académico. A mis padres, que me han enseñado e inculcado desde pequeño la importancia de la perseverancia y la dedicación. A mis hermanos y al resto de mi familia, que han comprendido mis ausencias y mi dedicación exclusiva a este objetivo académico.

A mis profesores y tutores, que me han sabido guiar y orientar en este proceso de investigación, compartiendo sus conocimientos y experiencia en el campo de la ciberseguridad.

A mis compañeros de estudio: Danilo y Pablo, que han sido un apoyo y motivación en momentos de frustración e impotencia.

Y especialmente, a mí mismo, por haber tenido la determinación y las ganas de llevar a cabo este proyecto, que espero sea el comienzo de una carrera profesional exitosa en el ámbito de la ciberseguridad."

Resumen

Los gobiernos y los organismos de seguridad reconocen que actualmente se evidencian una mayor cantidad de riesgos de vulneración a la seguridad, incluidos los delitos informáticos, ciberterrorismo, amenazas cibernéticas e inclusive ciberataques a las infraestructuras críticas y servicios esenciales de los estados; los mismos que han causado daños a la sociedad y pérdidas económicas. Por esto, los estados a través de la administración pública y las diversas instituciones estatales y privadas han incrementado sus capacidades en lo referente a ciberseguridad y a ciberdefensa, todo ello fundamentado en la implementación de sistemas tecnológicos, protocolos y sobre todo políticas de seguridad de la información cada vez más robustas y sofisticadas para contrarrestar estos posibles ciberataques en el ciberespacio.

Considerando lo expuesto anteriormente; actualmente uno de los activos más importantes que incluso se podría decir el más importante para las empresas y/o instituciones es la información, así como el aseguramiento de esta como punto primordial, todo ello con el fin de obtener ventajas competitivas y generar valor, manteniendo a buen resguardo la confidencialidad, disponibilidad e integridad (triada CID) del activo denominado información.

En este contexto surge la necesidad en el Ministerio de Defensa Nacional (MIDENA) como institución líder del sector Defensa de enforzar y garantizar el Esquema Gubernamental de Seguridad de la Información (EGSI v2.0) a través de un Programa de Ciberseguridad, el mismo que establecerá directrices y responsabilidades en todos los niveles para avalar el proceso en el cumplimiento de políticas, procesos y estándares de ciberseguridad del EGSI v2.0, el cual se integra y coordina con los elementos funcionales para salvaguardar los activos de la cartera de defensa.

En el presente trabajo de investigación, se ha aplicado la metodología MAGERIT para evaluar y reforzar el cumplimiento del EGSI v2.0 en el MIDENA.

MAGERIT, reconocida por su enfoque sistemático y estructurado en el tratamiento y la gestión de riesgos en sistemas de información, permitió identificar, analizar y evaluar los riesgos inherentes a la infraestructura y procesos tecnológicos del ministerio. A través de este proceso, y mediante la implementación del Programa de Ciberseguridad se busca que se implementen medidas de mitigación y controles o hitos de ciberseguridad adecuados que garanticen la resiliencia y protección de la información crítica digital y sus servicios esenciales. Los resultados obtenidos evidencian una mejora significativa en la postura de ciberseguridad del ministerio, asegurando una mayor conformidad con las normativas establecidas y elevando el nivel de seguridad general de sus operaciones en el ciberespacio.

El Programa de Ciberseguridad deberá ser cumplido con carácter obligatorio para las instituciones del sector de Defensa y a través de la ejecución de este plan se establecerá diagnósticos y métricas para determinar la madurez de la implementación del EGSI v2.0 y el estado actual de cumplimiento en las instituciones del sector defensa. Además, se podrán establecer un conjunto de directrices prioritarias que permitirán la mejora continua en la gestión de la Seguridad de la Información.

Dentro del ámbito de la ciberseguridad; la implementación y puesta en marcha de un plan de auditoría a fin de ejecutar una adecuada evaluación de seguridad del activo llamado información, es fundamental. Los requisitos principales de este sistema son la planificación meticulosa y la independencia de los auditores. Considerando lo expuesto anteriormente, cada funcionario civil o militar, independientemente de su nivel o jerarquía, tiene la responsabilidad de seguir los procesos adecuados para proteger los

activos de información. La supervisión del cumplimiento de estos procedimientos por parte del personal militar y civil recae en los comandantes o funcionarios del nivel jerárquico superior (NJS) de cada nivel investidos en sus atribuciones.

Palabras claves: Programa de ciberseguridad, EGSI v2.0, confidencialidad, integridad, disponibilidad.

Abstract

Governments and security agencies acknowledge the current escalation of security breaches, including cybercrimes, cyberterrorism, cyber threats, and even cyberattacks on critical infrastructure and essential state services. These incidents have caused societal harm and economic losses. Consequently, states, through public administration and various state and private institutions, have enhanced their cybersecurity and cyber defense capabilities. This enhancement is based on implementing increasingly robust and sophisticated technological systems, protocols, and, above all, information security policies to counteract potential cyberattacks in cyberspace.

Given the aforementioned context, one of the most important assets for companies and institutions today, arguably the most important, is information and its security. Ensuring the confidentiality, availability, and integrity (CIA triad) of information is paramount to gain competitive advantages and generate value.

In this context, the need arises for MIDENA to enforce and guarantee the Governmental Information Security Scheme (EGSI v2.0) through a Cybersecurity Program. This program will establish guidelines and responsibilities at all levels to ensure compliance with the cybersecurity policies, processes, and standards of EGSI v2.0, which integrates and coordinates with functional elements to safeguard the defense portfolio assets.

In this research, the MAGERIT methodology has been applied to evaluate and strengthen the compliance of EGSI v2.0 in the Ministry of National Defense of Ecuador. MAGERIT, recognized for its systematic and structured approach to risk management in information systems, enabled the identification, analysis, and evaluation of inherent risks

to the ministry's infrastructure and technological processes. Through this process, and by implementing the Cybersecurity Program, appropriate mitigation measures and information security controls or milestones are sought to enhance the resilience and protection of critical digital information. The results show a significant improvement in the ministry's cybersecurity posture, ensuring greater compliance with established regulations and elevating the overall security level of its cyberspace operations.

The Cybersecurity Program must be mandatorily implemented by defense sector institutions. Through this plan's execution, diagnostics and metrics will be established to determine the maturity of EGSI v2.0 implementation and the current state of compliance within the defense sector institutions. Additionally, a set of priority guidelines will be established to enable continuous improvement in Information Security management.

Within the realm of cybersecurity, the evaluation of information security through an internal audit plan is essential. The main requirements of this system are meticulous planning and auditor independence. Each individual, regardless of their level, is responsible for following the appropriate procedures to protect information assets. The supervision of these procedures' compliance by military and civilian personnel lies with commanders or senior hierarchical officials at each level, vested with their respective authorities.

Keywords: Cybersecurity program, EGSI v2.0, confidentiality, integrity, availability.

Índice de contenidos

1	Capítulo I. Introducción.....	11
1.1	Situación problemática.....	12
1.2	Línea de investigación	13
1.3	Objeto de estudio	14
1.4	Campo de acción	14
1.5	Objetivos	15
1.6	Problema Científico – Preguntas de Investigación	16
1.7	Variables	16
1.8	Justificación – Contribuciones de la Investigación.....	17
1.9	Estado del Arte.....	19
1.10	Fundamentación teórica.....	21
1.10.1	Seguridad de la Información.....	21
1.10.2	Esquema Gubernamental de Seguridad de la Información.....	23
1.10.3	Estándares o normas de seguridad de la información.....	25
1.10.4	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT)	26
2	Capítulo II. Diagnóstico situacional.....	28
2.1	Metodología	28
2.1.1	Proceso para la Gestión del Riesgo:	29

2.2	Análisis situacional	34
2.2.1	Valoración del riesgo	36
2.2.1.1	Identificación de Activos de Información.....	37
2.2.1.2	Identificación de amenazas y vulnerabilidades	38
2.2.1.3	Identificación de controles existentes.....	39
2.2.1.4	Evaluación del riesgo.....	40
2.2.2	Tratamiento Del Riesgo	43
2.2.3	Aceptación del Riesgo	47
2.2.4	Comunicación del Riesgo	47
2.2.5	Monitoreo y revisión del riesgo	47
2.3	Análisis comparativo	48
3	Capítulo III. Propuesta.....	53
3.1	Propuesta del Programa de Ciberseguridad del Ministerio de Defensa Nacional	53
3.2	Plan de Auditoria	93
4	Capítulo IV. Conclusiones.....	104
5	Capítulo V: Recomendaciones	105
	Bibliografía.....	107

Índice de figuras

Figura 1: Metodología en cascada.....	28
Figura 2: Proceso de Gestión del Riesgo.	29
Figura 3: Ciclo PDCA.	33
Figura 4: Metodología de evaluación y tratamiento de riesgos.	35
Figura 5: Desarrollo del Tratamiento de riesgos.....	43
Figura 6: Organigrama CSI.....	55

Índice de tablas

Tabla 1: Proceso de Gestión del Riesgo de seguridad de la información.	29
Tabla 2: Consideraciones establecidas para la identificación de los activos del MIDENA	37
Tabla 3: Criterios de evaluación considerados para medir el nivel de riesgo de los activos del MIDENA.	38
Tabla 4: Ejemplo de valoración de la probabilidad.....	39
Tabla 5: Controles identificados.....	39
Tabla 6: Criterios de evaluación del riesgo en el MIDENA.	40
Tabla 7: Evaluación del riesgo	41
Tabla 8: Tratamiento del riesgo.....	44
Tabla 9: Riesgo residual.	49
Tabla 10: Información del documento.	53
Tabla 11: Controles hace referencia la Política de Seguridad de la Información.	74
Tabla 12: Controles hace referencia la Política de Control de Acceso a los Sistemas de Información.	75
Tabla 13: Controles hace referencia la Política de Concientización.	75
Tabla 14: <i>Controles hace referencia los Procedimientos de organización de la seguridad de la información</i>	76
Tabla 15: Controles hace referencia los Procedimientos de dispositivos móviles y teletrabajo.	78
Tabla 16: Controles hace referencia los Procedimientos de acceso a redes y servicios de red.	79
Tabla 17: Controles hace referencia los Procedimientos de registro, retiro y modificación de usuarios.	80

Tabla 18: Controles hace referencia los Procedimientos para el uso y clasificación de la información.....	80
Tabla 19: Controles hace referencia los Procedimientos para la gestión de acceso de los usuarios.....	81
Tabla 20: Controles hace referencia los Procedimientos de responsabilidad de usuarios y acceso a sistemas y aplicaciones.	82
Tabla 21: Controles hace referencia los Procedimientos de controles criptográficos...	82
Tabla 22: Controles hace referencia los Procedimientos de seguridad física y del entorno.	83
Tabla 23: Controles hace referencia los Procedimientos de escritorio y pantalla limpia de información.....	84
Tabla 24: Controles hace referencia los Procedimientos referentes a responsabilidades operacionales.	84
Tabla 25: Controles hace referencia los Procedimientos a referentes a protección contra códigos maliciosos.....	85
Tabla 26: Controles hace referencia los Procedimientos de seguridad en operaciones.	86
Tabla 27: Controles hace referencia los Procedimientos de gestión de la seguridad de redes.....	87
Tabla 28: Controles hace referencia los Procedimientos de transferencia de información.....	87
Tabla 29: Criterios de evaluación para las auditorías.....	99
Tabla 30: Cronograma primera fase.	101
Tabla 31: Cronograma segunda fase.	101
Tabla 32: Versión e historial.	103

1 Capítulo I. Introducción

El mundo globalizado y sus avances en lo concerniente a las Tecnologías de la Información y Comunicación (TIC) han generado una mayor atención de los estados en lo concerniente a la protección de la triada CID de la información y de esta manera generar confianza en los usuarios y minimizar riesgos relacionados con vulnerabilidades y amenazas informáticas (Ospina & Sanabria, 2020).

El avance tecnológico no ha venido acompañado de un progreso similar en el ámbito de la ciberseguridad, es por ello que en una sociedad que proclama que su recurso más valioso ya no es el petróleo sino los datos, estos se encuentren expuestos cada vez mayores riesgos (Torres et al., 2022).

El Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) a través del acuerdo ministerial N.º 025-2019, emitió el EGSI v2.0, dirigido a las Instituciones de la Administración Pública Central, Institucional y Dependientes de la Función Ejecutiva (APCID). Este esquema se fundamenta en normas técnicas ecuatorianas, específicamente la "INEN ISO/IEC 27000" para la Gestión de la Seguridad de la Información. (MINTEL, Acuerdo Ministerial N.º 025-2019, 2020).

El EGSI v2.0 presenta recomendaciones en algunos aspectos fundamentales para el manejo de la gestión de la Seguridad de la Información, sobre todo promueve poner en práctica la mejora continua en las instituciones de la APCID, sin embargo, es primordial hacer hincapié que las mismas no reemplazan a las normas promulgadas en la INEN ISO/IEC 27000; ya que es necesario la gestión de la seguridad de la información en base a la evolución normativa y tecnológica que el mundo globalizado nos exige.

Los riesgos y amenazas en el ciberespacio actualmente se caracterizan por ser altamente modificables y capaces de actuar en diversos ámbitos; transformándose en nuevas amenazas que revelan vulnerabilidades y provocan incidentes de seguridad;

motivo por el cual el Ministerio de Defensa Nacional (MIDENA) expide el Acuerdo Ministerial 134 del 30 de marzo de 2020 donde se imparten normas con disposiciones orientadas a precautelar la triada CID a través de la implementación del EGSI v2.0 así como la designación de los OSI quienes serán los responsables del seguimiento en todas las instituciones del sector defensa y sus entidades adscritas.

Actualmente, el sector defensa requiere implementar un plan de auditoría (para el seguimiento del cumplimiento del EGSI v2.0), el mismo que se desarrollará para garantizar la aplicación de los catorce dominios (14) y ciento veinte y siete (127) controles; actualmente existen hitos que no se cumplen adecuadamente con lo establecido en el EGSI v2.0.

1.1 Situación problemática

En el MIDENA, hay un problema importante con la falta de observancia de los criterios y regulaciones indicados en el EGSI v2.0. Aunque se reconoce la importancia vital de proteger datos sensibles y estratégicos, las fallas en la implementación y supervisión del EGSI son preocupantes.

Una de las áreas donde se evidencian estas deficiencias es en la gestión de sistemas de información con clasificación. A menudo, se evidencian brechas en seguridad que exponen información confidencial a riesgos de ciberataques o filtraciones, comprometiendo la seguridad nacional. Además, la falta de capacitación adecuada del personal en seguridad informática contribuye a la vulnerabilidad del sistema, ya que los usuarios pueden cometer errores que comprometan la integridad de los datos.

Otro punto crítico es la coordinación insuficiente entre las diferentes instituciones y entidades adscritas al sector defensa y el MIDENA; en lo concerniente a la seguridad de la información digital. La compartimentación excesiva y la falta de protocolos

unificados dificultan la detección y mitigación de amenazas cibernéticas, dejando al sistema vulnerable a ataques coordinados.

En resumen, a pesar de contar con un EGSI aprobado a nivel gubernamental, las deficiencias identificadas en los controles y sobre todo en la aplicación efectiva de los parámetros comprometen la seguridad del MIDENA y, por extensión, la seguridad nacional.

Motivo por el cual es imprescindible el desarrollo e implementación del Programa de Ciberseguridad del MIDENA que se alinee a la norma, donde se lleve un control adecuado de todo el sector defensa en materia de ciberseguridad, y permita implementar estructuras de evaluación y gestión de riesgos en la institución, así como el Plan de Auditoria Interno con sus respectivas evidencias de cumplimiento para mantener un esquema de control eficiente.

A través de este documento que tiene como objetivo reconocer la importancia y el valor de la información en el funcionamiento eficiente y efectivo del MIDENA, se considera que la información no es solo crítica para el éxito de esta cartera de Estado, sino estratégica, y permite garantizar la triada CID.

1.2 Línea de investigación

Para el presente trabajo de investigación se ha determinado la línea de investigación que se orienta en la *energía eléctrica y tecnologías de la información para la innovación y el desarrollo sostenible*; dentro de la subcategoría de ciencia de los ordenadores, análisis de datos y algoritmos computacionales; para ello se utilizará la metodología MAGERIT a ser puesta en práctica para la gestión de riesgos en sistemas de información, donde a través de la cual se identificará, analizará y evaluará los riesgos inherentes a la infraestructura y procesos tecnológicos del ministerio y desarrollar un programa de ciberseguridad que permita enfocar el EGSI v2.0.

1.3 Objeto de estudio

El enfoque principal de la implementación del Programa de Ciberseguridad es proteger la información digital y su infraestructura tecnológica contra las amenazas en el ciberespacio. Los programas de ciberseguridad abordan una variedad de áreas para establecer políticas que nos permitan garantizar la triada CID de la información en entornos digitales como es proteger las redes de computadoras contra accesos no autorizados, ataques de hackers y malware; configuración segura de sistemas, gestión de parches y detección de vulnerabilidades; así como evaluar y gestionar los riesgos basados en regulaciones y estándares; para finalmente planificar y gestionar a incidentes de ciberseguridad, incluyendo la identificación, contención, erradicación y su recuperación.

1.4 Campo de acción

La ciberseguridad debe abordarse con un enfoque interdisciplinario y holístico, aplicándose de manera multilateral para gestionar los riesgos de seguridad en el ciberespacio (Bustillos & Rojas, 2023). Este enfoque debe integrarse plenamente en todos los aspectos de las instituciones del sector de Defensa que dependen del MIDENA. La implementación y el cumplimiento de estos principios por parte de toda la organización garantizan un entorno ciberseguro, que debe ser considerado desde una visión estratégica e incluido en los objetivos de la institución armada.

A través de la ejecución de este plan, se podrán establecer diagnósticos y métricas para evaluar la madurez de la implementación del EGSI v2.0 y el estado actual de cumplimiento en las instituciones del sector defensa. Además, se establecerán directrices prioritarias para permitir la mejora continua.

El proceso de evaluación mediante un plan de auditoría interna es un componente esencial dentro de un SGSI, asegurando la efectiva implementación de los controles y protocolos de seguridad de la información en todos los ámbitos del sector Defensa. Los

requisitos principales de un SGSI son la planificación meticulosa y la independencia de los auditores, lo que asegura una evaluación imparcial y objetiva.

En este contexto, es esencial que cada persona y/o funcionario, en todos los niveles de la organización, sea responsable de adherirse a los procedimientos establecidos para proteger los activos de información. Además, los comandantes de cada nivel tienen la responsabilidad de supervisar y asegurar que tanto el personal militar como el civil acaten estos procedimientos rigurosamente.

La implementación de auditorías internas no solo ayuda a identificar y corregir vulnerabilidades, sino que también promueve una cultura cibersegura y conciencia en todo el sector de la defensa nacional. Este enfoque integral y coordinado refuerza la capacidad de las Fuerzas Armadas para la protección de los activos de información y de esta forma mantener la CID de los datos.

1.5 Objetivos

General:

Implementar un programa de ciberseguridad donde se establezcan políticas para enforzar el EGSI v2.0 en el Ministerio de Defensa Nacional las mismas que serán para cumplimiento de todo el sector Defensa.

Específicos:

- Promover las mejores prácticas de seguridad de la información en la elaboración del programa de ciberseguridad en el cumplimiento a los hitos del EGSI v2.0.
- Operacionalizar el programa de ciberseguridad mediante la emisión de políticas, normas y un plan de auditoría a fin de enforzar el EGSI v2.0 en el sector Defensa.

1.6 Problema Científico – Preguntas de Investigación

Bajo el contexto antes mencionado, nace las siguientes preguntas:

¿Cómo se puede mejorar la ciberseguridad en el MIDENA a través de un programa de ciberseguridad eficaz y robusto para proteger de manera efectiva los activos de información contra amenazas emergentes y ataques cibernéticos?

¿Es necesaria la aplicación de un plan de auditoria para el sector de la Defensa a fin de mejorar el cumplimiento del EGSI v2.0, en lo que respecta a la CID de la información?

Hipótesis:

El implementar un Programa de Ciberseguridad elaborado con un enfoque integral que incluya el uso de herramientas y tecnologías como firewalls, sistemas de detección de intrusiones, antivirus; así como políticas, procedimientos, directrices y procesos establecidos para garantizar la seguridad de la información y un plan de auditoría; permitirá disminuir notablemente los incidentes de ciberseguridad mediante la implementación operativa del programa de ciberseguridad, estableciendo controles conforme al EGSI v2.0 y mitigando los riesgos para asegurar la CID de la información.

1.7 Variables

Independiente:

- Herramientas y tecnologías específicas implementadas, como firewalls, sistemas de detección de intrusiones, antivirus, etc.
- Políticas, procedimientos, directrices y procesos establecidos para garantizar la seguridad de la información.
- Plan de Auditoria para garantizar el seguimiento del cumplimiento de la implementación del EGSI v2.0.

Dependientes:

- Operacionalización del programa de ciberseguridad para el establecimiento de controles establecidos en el EGSI v2.0 y mitigar los riesgos.

1.8 Justificación – Contribuciones de la Investigación

La investigación que se está desarrollando tiene la finalidad de implementar una propuesta de Programa de Ciberseguridad para el MIDENA y sus entidades adscritas, pues al ser una cartera de Estado encargada de la defensa nacional, requiere proteger la información e infraestructura ante cualquier amenaza, ataques informáticos o incidentes de ciberseguridad (Ascencio, 2021).

La evaluación de las amenazas en el ciberespacio es un aspecto a considerar y analizar para fortalecer la seguridad de la información, es primordial poner hincapié en lo que confiere a la prevención, detección, respuesta y recuperación, con cooperación internacional clave para resolver incidentes. Los ataques cibernéticos intentan dañar sistemas y redes, generando pérdidas económicas y robo de información personal. Por lo general los empleados víctimas de los ataques pueden exponer datos críticos de la empresa o personal ubicados no sólo en su propia computadora, sino en toda una red y así robar credenciales de acceso, directorios de correos electrónicos corporativos, números de cuenta, números de Seguro Social, entre otra información (Chambi, 2021).

Finalmente se concluye que la justificación más concreta es que a través del programa de ciberseguridad se trabajará para alcanzar los siguientes aspectos:

- Operacionalizar la ciberseguridad:
 - Proveer dirección estandarizada.
 - Establecer una dirección para definir los indicadores.
 - Establecer procesos repetitivos y estandarizados.

- Abordar las brechas del EGSI v2.0
 - Reportes
 - Auditorias
- Establecer un programa de concientización en ciberseguridad.
- Evaluación de riesgos
 - Las evaluaciones de riesgos son los primeros pasos esenciales para identificar debilidades y desarrollar un hoja de ruta de remediación.
 - Boletines
- Esfuerzos de remediación
 - Las debilidades críticas deben abordarse lo antes posible; lo demás debe integrarse a un plan continuo basado en la disponibilidad de recursos y prioridades.
 - Las debilidades también varían en áreas que van desde los sistemas de TI subyacentes hasta la educación de los usuarios sobre la información aceptable y las prácticas de uso cibernético.
- Validación
 - Concepto de “confiar, pero verificar”, es decir comprobar que todos los esfuerzos u acciones de remediación que anteriormente hayan sido puestos en práctica se hayan constituido en un instrumento efectivo al probar las capacidades existentes y nos permitan cuestionar las suposiciones.
 - Auditorias avisadas y sin avisar.
 - Esfuerzos de validación pueden incluir pruebas de penetración, actividades centradas en irrumpir en los sistemas o ejercicios de juegos cibernéticos, simuladores de mesa de una incidencia.

1.9 Estado del Arte

Actualmente el MIDENA no cuenta con un documento que enfuerce al EGSI v2.0 y de esta manera proteger los sistemas de información, por eso es importante poder identificar la necesidad de desarrollar y poner en práctica un programa de ciberseguridad para su cumplimiento y el mismo que llegue a ser estructurado como una buena práctica dentro de la cartera de la Defensa, con el fin de prevenir o reducir la frecuencia de ataques digitales (Mancilla, 2021).

Es por lo que la ciberseguridad no es solo un aspecto relacionado a las TI, si no su ámbito de aplicación se relaciona en todos los aspectos y no es menos el sector de la Defensa, como bien sostiene Castillo (2018) en materia de Ciberseguridad nada está escrito. Existe todo un compendio de protocolos, normativas, recomendaciones, buenas prácticas, pero nada de esto puede garantizar que su sistema u organización esté segura frente a un ciberataque. Siempre existirá un punto vulnerable que no se tuvo en cuenta y que los atacantes han podido ver.

Por otro lado, según Pinto (2019) la implementación exitosa de proyectos para empresas públicas requiere una comprensión integral de las leyes, regulaciones y directrices relevantes para garantizar una integración perfecta de los aspectos técnicos con las directivas estatales.

Según argumenta Reyna (2023) las empresas contemporáneas necesitan gestionar y organizar datos de manera efectiva y segura. Sin embargo, a medida que la cantidad de información aumenta, aumentan también los riesgos asociados. Estos riesgos pueden resultar perjudiciales si no se controlan de manera adecuada y oportuna.

Es necesario poner a consideración lo expresado por Gómez (2019) indicando: las empresas de cualquier ámbito económico deben implementar medidas de seguridad

adecuadas, tanto políticas, estándares y tecnologías que incrementen las acciones en la protección de la información digital y sus activos tecnológicos, evitando así el robo o caída de su infraestructura especializada.

Por otra parte, un aspecto a ser considerado en la seguridad de la información es el que manifiesta Muyón et al., (2019) las personas encuestadas conocen y aplican medidas preventivas de seguridad más básicas. Cien por ciento de los encuestados bloquean o apagan sus computadoras al final de la jornada laboral, más del 91% de las respuestas reflejan que las personas abren adjuntos de correos electrónicos que únicamente provienen de fuentes de su confianza.

En el ámbito de la ciberseguridad, no hay reglas fijas; hay una amplia gama de protocolos, normativas, recomendaciones y buenas prácticas, pero ninguna de ellas puede asegurar completamente la protección de su sistema u organización contra un ciberataque. Siempre habrá algún punto débil que no se haya tenido en cuenta y que los atacantes puedan explotar. Sin embargo, la documentación existente sí puede ayudar a minimizar los riesgos y a limitar el daño causado por los ataques (Castillo, 2018).

Las principales iniciativas/acciones que una institución debe ejecutar a fin de mejorar su postura de seguridad digital se enfocan en las siguientes áreas de desarrollo, como es considerar un alineamiento con el negocio, la gobernanza de ciberseguridad, la arquitectura de ciberseguridad, la gestión de programas y proyectos, gestión de los riesgos en lo referente a la continuidad y cumplimiento y la gestión de recursos y| continuidad de las operaciones (Guevara, 2022).

En este contexto y en base a los fundamentos expuestos y analizados anteriormente en el estado del arte que se propone, podemos concluir que, actualmente la ciberseguridad alcanza mucha importancia y relevancia en todos los ámbitos de un mundo globalizado, motivo por el cual el desarrollo, implementación y mantenimiento de un

programa de ciberseguridad para el MIDENA no es una tarea minúscula sino más bien de mucho valor institucional; el valor general que el MIDENA logrará a través del desarrollo y la implementación de dicho programa incluirá la reducción de los casos de ataques cibernéticos exitosos; en este contexto el programa de ciberseguridad proporcionará un medio para reducir el impacto de un ataque exitoso en el resultado final debido a su enfoque programático predefinido para identificar y responder a incidentes de ciberseguridad.

1.10 Fundamentación teórica

1.10.1 Seguridad de la Información

La seguridad de la información según Baldeón & Coronel (2015) abarca la salvaguardia de la continuidad operativa y el blindaje contra amenazas, ya sea que residan en una sola computadora o en una red de múltiples dispositivos, la ciberseguridad también abarca el salvaguardar el correcto acceso a los distintos recursos tecnológicos de los sistemas; fundamentado en esos criterios la seguridad de la información se estructura basado en 3 pilares primordiales según indica Pinto (2019), mismos que garantizan que los activos de información permitan un proceso eficiente y efectivo de acceso a la misma, los pilares en mención son los siguientes:

Confidencialidad: esta propiedad concierne a que la información sea revelada sólo a los usuarios autorizados, en la forma y tiempo determinado (Aguilera et al., 2017).

Integridad: este aspecto refiere a la capacidad de garantizar que la información no ha sido modificada de manera no autorizada, para ello es necesario aplicar técnicas como el cifrado de datos, controles de acceso, copias de seguridad, entre otras; en este contexto los ataques a la integridad de los datos consisten en la modificación intencional de los mismos, sin autorización alguna, en algún momento de su ciclo de vida (Gallardo, 2015).

Disponibilidad: se caracteriza en base a que la información esté disponible en el momento en que los funcionarios autorizados requieran acceder, copiar, almacenar, modificar, etc. (Riveros, 2016).

1.10.1.1 Tipos de seguridad

De acuerdo con Balseca & Ledezma (2015) se puede identificar dos clases de seguridad de la información; activa, es aquella que posee un compendio de defensas o medidas cuyo propósito es minimizar y de ser el caso evitar las afectaciones de los riesgos que amenazan a la infraestructura tecnológica. Por otro lado, la seguridad pasiva, engloba las acciones que se ponen en marcha con el fin de reducir el impacto de un incidente de seguridad una vez que ha ocurrido, y para facilitar la recuperación del sistema.

1.10.1.2 Objetivos de la seguridad de la información

Es importante determinar que el objetivo principal es fortalecer las medidas de seguridad de los sistemas de procesamiento de datos y la transferencia de información tanto en instituciones públicas como privadas. Estos servicios deben estar en condiciones primordiales de poder afrontar ciberincidentes mediante el uso de uno o más mecanismos de seguridad, con el fin de proteger la CID de los datos; como señala Ramírez & Rincone (2022) se ha establecido como objetivo el desarrollo e implementación de políticas y controles de ciberseguridad de los datos digitales o de información, lo cual se ha convertido en un procedimiento imprescindible para que las instituciones puedan proteger sus activos tecnológicos y sistemas contra ataques, daños o pérdidas en el ciberespacio.

1.10.1.3 Activos de información

Se define como la información o recurso relacionado con la creación, almacenamiento, manejo o transmisión de dicha información; según Oñate (2021) los recursos de información abarcan una variedad de formas mediante las cuales la información es creada, procesada, almacenada o transmitida. Esta información puede

existir en diferentes medios, como documentos impresos, archivos electrónicos o datos almacenados en dispositivos físicos. Se dividen en diversas categorías, como, por ejemplo: activos lógicos como bases de datos y documentación de sistemas o manuales; activos físicos como ordenadores, servidores, dispositivos de almacenamiento, discos, pendrives y equipamiento de comunicación; y finalmente recursos humanos y servicios de soporte ofrecidos por otros ofertantes.

1.10.1.4 Gestión del riesgo

Según Niño (2019) la gestión del riesgo es un proceso que consiste en analizar, determinar y cuantificar la probabilidad de ocurrencia de una/s amenazas, proponiendo un criterio aceptable de riesgo para la institución, teniendo en cuenta en el análisis el potencial impacto de un incidente que no se desea su ocurrencia y afectación. Este proceso dinámico y coordinado tiene como objetivo identificar los problemas antes de que se materialicen.

1.10.2 Esquema Gubernamental de Seguridad de la Información

El EGSI fue promulgado por la Secretaría Nacional de la Administración Pública mediante el acuerdo ministerial No. 166 de septiembre de 2013, para garantizar que se den cumplimiento las normas básicas de seguridad de la información en el ámbito de cibernético a nivel de Estado. Posteriormente el MINTEL el 10 de enero del 2020, expidió la versión 2.0, en la cual se considera nuevos requisitos normativos.

1.10.2.1 Enfoques para la Protección y Seguridad de la Información

En el proceso de implementación de un procedimiento en este ámbito, es esencial seguir las mejores prácticas, que abarcan la documentación de políticas, asignación clara de responsabilidades, formación adecuada, implementación de procedimientos correctos, registro de incidentes y la búsqueda continua de mejoras. Además, es crucial definir claramente los términos relacionados para garantizar una comprensión y ejecución

efectivas del procedimiento para ello los términos relacionados a abarcar son los siguientes:

- **Política:** Son directrices estratégicas, procedimientos y prácticas que buscan coordinar acciones con una orientación ideológica para la toma de decisiones con el propósito de garantizar la protección de la información sensible y la infraestructura tecnológica de una institución u organización a mediano y largo plazo. Estos documentos, comúnmente utilizados por empresas y entidades gubernamentales en el ámbito de la tecnología de la información, tienen como propósito principal reforzar las defensas contra amenazas como el fraude informático y la intrusión de hackers malintencionados. Es crucial fortalecer estas políticas, ya que su implementación se enfoca en promover comportamientos seguros entre el personal (Esparza, 2023).
- **Norma:** En el ámbito dinámico de la ciberseguridad, las normas sirven como modelos autorizados, meticulosamente elaborados por organizaciones especializadas, para dotar a las organizaciones del conocimiento y la orientación necesarios para poner a buen recaudo sus activos de información y fortalecer sus medidas defensivas contra incidentes cibernéticos. Estos documentos técnicos integrales describen un enfoque estructurado para la gestión de la seguridad de la información, que abarca un compendio de requisitos, directrices y mejores prácticas que, cuando se implementan de manera efectiva, pueden mejorar significativamente la postura de ciberseguridad de una organización.
- **Estándar:** Se define como un conjunto de reglas que describen las acciones a tomar en diferentes situaciones, diseñado específicamente para fomentar el cumplimiento de las políticas establecidas.

- Guía: Se define como el documento generado con la finalidad de recomendar actividades o acciones a cumplir a fin de sustentar la Política.

1.10.2.2 Los objetivos de las políticas de seguridad de la información

Según Balseca & Ledezma (2015) establece que el propósito de la política de seguridad de la información de una entidad tiene dos objetivos principales: en primer lugar, expresar la postura de la organización en cuanto a la seguridad, y, en segundo lugar, proporcionar doctrina fundamentada para el desarrollo y puesta en práctica de procedimientos específicos de ciberseguridad. Estas especificaciones deben detallar de manera inequívoca las prácticas que la institución adoptará. Además, es imperativo que estas políticas sean evaluadas periódicamente y, en caso necesario, actualizadas.

1.10.3 Estándares o normas de seguridad de la información

Un estándar es un documento técnico-legal que define un modelo o norma con requisitos específicos, directrices y prácticas recomendadas para gestionar la seguridad de la información y proteger contra ciberataques en una institución u organización. Estos estándares son desarrollados por organismos especializados y utilizados como guías para implementar medidas de seguridad efectivas, buscando hacer los procesos y actividades organizacionales repetibles, organizados y estructurados (Espinosa & Carmina, 2011).

1.10.3.1 Norma ISO

La norma International Organization for Standardization ISO (por sus siglas en inglés), es un conjunto de normas internacionales desarrolladas y publicadas por la organización mencionada. Es ella la que se encarga de establecer estándares técnicos para diversos sectores alrededor del mundo. Las normas ISO abarcan una amplia gama de áreas, desde sistemas de gestión y calidad hasta normas específicas para productos y servicios.

1.10.3.2 ISO 27001: Seguridad de la información

Esta norma guía el proceso de manejo de la seguridad de la información, ofreciendo una estructura para establecer, ejecutar, mantener y mejorar constantemente un SGSI. Define los requisitos para los sistemas de gestión de la seguridad de la información, es reconocida internacionalmente y asegura la CID de los datos y sus sistemas de gestión (Mora, 2021).

1.10.3.3 ISO 27002: Guía de buenas prácticas para la Seguridad de la Información

Esta norma proporciona una guía de buenas prácticas mismas que se fundamentan en criterios de control, así como controles verificados y recomendados en el ámbito de la seguridad de la información. Se enfoca en un amplio espectro de controles y prácticas de seguridad que las organizaciones e instituciones pueden poner en práctica para proteger sus activos de información; estos controles y prácticas abarcan áreas como la gestión de activos, seguridad en el acceso y control, seguridad física, gestión de incidentes, seguridad en las comunicaciones y cumplimiento legal, entre otros (Balseca & Ledezma, 2015).

1.10.4 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT)

La Metodología de Análisis y Gestión de Riesgos de Sistemas de Información (MAGERIT) se centra en evaluar el potencial impacto de los incidentes de seguridad en una institución y/o empresa. Su objetivo es identificar los riesgos y amenazas que podrían causar una afectación y cuáles serían las vulnerabilidades de nuestros sistemas que pueden ser aprovechadas por estos riesgos y amenazas. Esto proporciona una base para determinar las medidas preventivas y correctivas necesarias (Guamán et al., 2023).

MAGERIT consta de seis fases, que son:

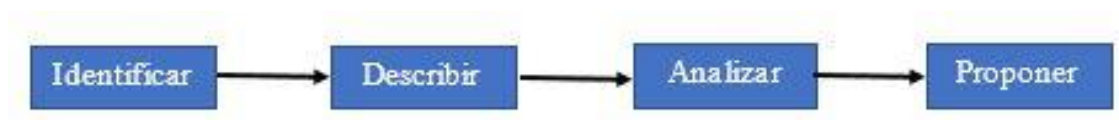
- Delimitar el alcance, es decir, definir las áreas estratégicas que serán objeto de revisión o mejora en términos de seguridad.
- Identificar los activos, para evaluar su valor y comprender la posible pérdida en caso de una amenaza.
- Analizar las vulnerabilidades, riesgos y amenazas a la que los activos de información podrían estar expuestos.
- Identificar salvaguardas, diseñados para contrarrestar las amenazas identificadas.
- Evaluar el riesgo que tendría una amenaza en un activo determinado.
- Tratar el riesgo, asociado con la probabilidad de ocurrencia de estas amenazas (Hurtado, 2018).

2 Capítulo II. Diagnóstico situacional

2.1 Metodología

El enfoque de esta investigación es de carácter cualitativo y descriptivo, en la primera fase de la metodología, se identificará los posibles riesgos y/o vulnerabilidades en los Sistemas de Información del MIDENA. Una vez identificados, se describirán las políticas establecidas para minimizar los riesgos y asignar responsables.

Figura 1: Metodología en cascada



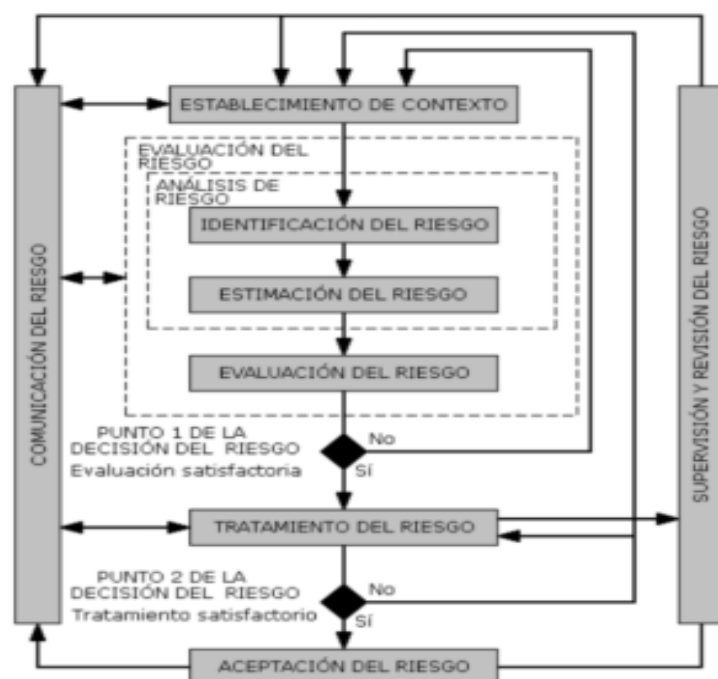
Nota. Fuente: El autor

El estudio actual utiliza un enfoque estratégico, que permite tener en cuenta las tendencias emergentes en ciberseguridad, así como las capacidades y recursos del MIDENA, para ello el MINTEL ha desarrollado la Guía para la Gestión de Riesgos de Seguridad de la Información, fundamentada en la metodología MAGERIT, que se comprende por seis fases, cada una de estas sigue un proceso determinado, ya que se logra gestionar una base sólida para la gestión de la ciberseguridad y puede adaptarse a todo nivel (Guamán et al., 2023).

Esta guía en mención nos servirá como metodología para el manejo de riesgos y en consideración de este aspecto el desarrollo del programa de ciberseguridad; el manejo del riesgo en el ámbito de la seguridad de la información puede seguir un procedimiento iterativo durante el proceso de las fases de evaluación o mitigación. Al adoptar un enfoque iterativo en la evaluación del riesgo, se puede mejorar el alcance y el nivel de detalle en

cada iteración. Este enfoque logra un equilibrio ideal entre reducir el tiempo y esfuerzo requeridos para identificar controles, al mismo tiempo que asegura una evaluación precisa de los riesgos que tienen un impacto significativo; como se evidencia en la **¡Error! No se encuentra el origen de la referencia..**

Figura 2: *Proceso de Gestión del Riesgo.*



Nota. Adaptado de *Guía para la Gestión de Riesgos de Seguridad de la Información* (p. 5), por MINTEL, 2020.

2.1.1 Proceso para la Gestión del Riesgo:

Tabla 1: *Proceso de Gestión del Riesgo de seguridad de la información.*

ACTIVIDADES	PASO
Establecimiento del contexto	- Consideraciones Generales - Levantamiento de información inicial. - Establecer criterios básicos para la Gestión del Riesgo. - Definir alcance y límites del manejo del Riesgo.

	• Establecer una organización para la operación del SGRSI. • Identificar Activos de Información • Identificar las amenazas y las vulnerabilidades • Identificar los controles existentes
Valoración del Riesgo	• Identificar consecuencias • Determinar el valor de las consecuencias • Determinar el valor de los incidentes • Determinar el nivel de estimación del riesgo • Evaluación del riesgo
Tratamiento del Riesgo	Seleccionar controles
Aceptación del Riesgo	Aceptar el riesgo
Comunicación del Riesgo	Comunicar el riesgo
Monitoreo y Revisión del Riesgo	Monitorear y revisar los riesgos

Nota. Adaptado de *Guía para la Gestión de Riesgos de Seguridad de la Información* (p. 5), por MINTEL, 2020.

2.1.1.1 Establecimiento del Contexto

Es crucial definir el entorno tanto externo como interno para la gestión del riesgo en seguridad de la información. Esto incluye establecer los criterios esenciales para dicha gestión, como determinar el alcance y los límites, y organizar eficazmente el proceso de operación del manejo del riesgo en seguridad de la información.

Según el alcance y los objetivos del manejo del riesgo, se pueden emplear diversos criterios, los cuales pueden variar con cada iteración. Es necesario seleccionar o desarrollar un enfoque adecuado de gestión del riesgo que cubra criterios fundamentales, como:

- Criterios de identificación del riesgo.
- Criterio de valoración del riesgo.
- Criterios de impacto.

- Criterios de aceptación de riesgos.

2.1.1.2 Evaluación de Riesgos de Seguridad de la Información

La evaluación de riesgos consiste en medir o explicar de forma descriptiva el riesgo, lo que ayuda a los custodios de los activos a ordenar los riesgos según su nivel de gravedad percibida u otros criterios definidos. Esta etapa suministra todos los datos requeridos para reconocer, evaluar y jerarquizar los riesgos. Las actividades que abarca la evaluación de riesgos son las siguientes:

- Proceso de identificación de riesgos.
- Proceso de análisis de riesgos.
- Proceso de valoración de riesgos.

Identificación del Riesgo: Consiste en reconocer las posibles causas de daño a la organización que puedan obstaculizar el logro de sus metas en seguridad de la información. Al momento se permiten dos métodos para identificar los riesgos, como se detalla a continuación:

- Enfoque centrado en eventos: implica la identificación de situaciones clave o estratégicas considerando las fuentes de riesgo y su impacto en las partes involucradas para alcanzar los objetivos deseados.
- Enfoque basado en activos: se enfoca en identificar escenarios operativos, detallando aspectos relacionados con activos, amenazas y vulnerabilidades.

Identificación de activos: Es fundamental reconocer todos los activos de información e infraestructura crítica en el MIDENA para gestionar adecuadamente los riesgos relacionados con ellos. Identificar quién es el encargado de cada recurso es crucial para designarle la responsabilidad de administrarlo y rendir cuentas al respecto. Aunque este

funcionario en muchos de los casos no posee derechos de propiedad sobre el recurso, sí tiene la responsabilidad de su custodia, mantenimiento, utilización y resguardo. Frecuentemente, el encargado del recurso es la persona más idónea para determinar la importancia que este tiene para la organización.

Identificación de las amenazas: Según el método MAGERIT, una vez que se identifican los activos críticos, se procede a clasificar las amenazas. Esta clasificación se lleva a cabo en función de la probabilidad de que dichas amenazas se conviertan en realidad y del daño que podrían causar. La matriz que sigue muestra el código de cada amenaza, la categoría del activo al que pertenece y las dimensiones evaluadas (triada CID).

Para realizar un análisis y gestión del riesgo basado en la metodología MAGERIT, es necesario evaluar los activos de información e infraestructura crítica del MIDENA. Durante este procedimiento, se reconocen los elementos fundamentales en riesgo junto con las posibles situaciones adversas, teniendo en cuenta tanto la probabilidad de que ocurran como las consecuencias para determinar el nivel de riesgo.

El tratamiento de riesgos por su parte implica tomar decisiones sobre los diferentes riesgos existentes según las normativas implementadas por la institución. Esto también considera que se incluyan controles tanto para disminuir, aceptar, evitar o transferir los riesgos, así como gestionar el riesgo a través de un plan; se establecen 04 fases para el tratamiento: reducción, aceptación, evitación y transferencia.

Es esencial aceptar los riesgos y asumir las responsabilidades correspondientes, registrando esta decisión de forma formal. Esta elección se realiza cuando los costos de implementar medidas de seguridad superan el valor del activo de información a proteger,

o cuando el riesgo es mínimo. En estas situaciones, la organización asume cualquier daño que pueda surgir a raíz de la materialización del riesgo.

En ocasiones, el riesgo residual puede no cumplir con los estándares de aceptación de riesgos, ya que estos estándares no consideran circunstancias particulares. Por ejemplo, es posible justificar la aceptación de riesgos debido a los beneficios significativos que aportan o porque reducir el riesgo resulta demasiado costoso (MINTEL, 2020).

Dentro del marco de gestión de una empresa, se define el SGSI como el método encargado de proteger los datos. Se suele seguir el ciclo PDCA, conocido en sistemas de gestión de calidad:

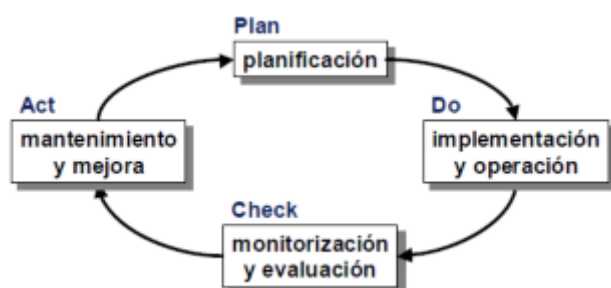
Plan (Planificar): Establecer objetivos y planificar tácticas para lograrlos implica evaluar tanto la situación presente como la futura de la empresa.

Do (Hacer): Se llevan a cabo las estrategias y planes diseñados.

Check (Verificar): Se evalúan los resultados obtenidos para determinar si se han logrado los objetivos planteados.

Act (Actuar): Con el objetivo de mejorar continuamente, se actualizan los planes y su implementación.

Figura 3: *Ciclo PDCA.*



Nota. Adaptado de “Propuesta de un sistema de gestión de seguridad de la información, aplicando la metodología MAGERIT para el gobierno regional Puno caso: Proyecto

especial camélidos sudamericanos – Pecsá, 2017” (p. 64), por W. Yana, 2020. Universidad Privada Telesup.

2.2 Análisis situacional

La evaluación de riesgos se aplicó en base a lo definido en el alcance del EGSI; a todos los activos que forman parte del Ministerio de Defensa Nacional y que se utilizan como parte de su gestión.

En una situación perfecta, el análisis de riesgos nos ayudó a calcular la posibilidad de que ocurran daños a la infraestructura tecnológica y los recursos de información del MIDENA.

Sobre la base de lo expuesto en un trabajo conjunto con la DTIC se realizó en primera instancia el levantamiento de los activos, posteriormente se realizó un pentester sobre los sistemas de información y finalmente se calificó previo análisis los diferentes activos físicos valorándolos y determinado los riesgos y oportunidades que existen sobre ellos con el objeto de disminuir su impacto o probabilidad de ocurrencia. Estas acciones, no necesariamente serán para un solo riesgo u oportunidad, sino que puede suceder que la misma acción aborde un conjunto de riesgos.

Luego de haber definido un plan de trabajo se realizaron las evaluaciones que permitieron definir si las estrategias planteadas han disminuido el riesgo o han aportado al logro de los beneficios derivados de la oportunidad.

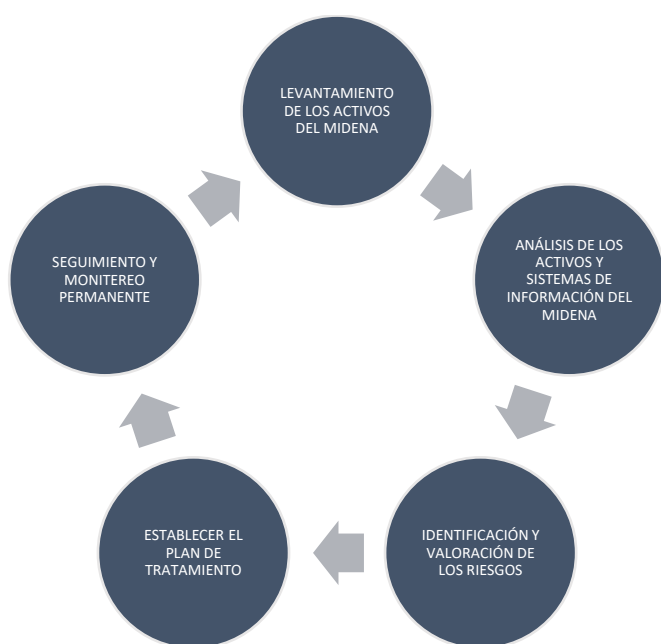
Se llevó a cabo la valoración de riesgos siguiendo las pautas establecidas por la norma "ISO 27005" y el enfoque "MAGERIT", utilizando la tabla de la matriz de evaluación de riesgos. El proceso de evaluación del riesgo fue coordinado con el OSI y en colaboración con la directora de TIC's del MIDENA.

La atención de la gestión del riesgo está planteada en base a las atribuciones de la Dirección de TIC's de esta cartera de Estado, a través del control y monitoreo permanente en virtud del ejercicio de sus funciones como la Dirección responsable de la adecuada operación y funcionamiento de toda la infraestructura tecnológica.

Para este período de análisis se realizó la evaluación y seguimiento con base al monitoreo de los riesgos que se efectuó a través de las Matrices de Riesgos aprobada por la DTIC como parte de la etapa de implementación del EGSI.

Frente a la identificación de los principales riesgos de la entidad, es necesario manifestar que los controles establecidos permitirán reducir significativamente el impacto de seguridad que pudiera tener en caso de presentarse algún riesgo.

Figura 4: Metodología de evaluación y tratamiento de riesgos.



Nota. Fuente: El autor

Como parte del proceso se estableció una metodología para el análisis, seguimiento y revisión del contexto interno y externo, y se orientaron las actividades con base a las siguientes consideraciones:

- Identificar de qué manera la utilización de las tecnologías de la información y la comunicación impulsa el avance de los planes, programas y proyectos del MIDENA, la administración interna de los procedimientos y los datos, la provisión de trámites y servicios a los habitantes y en términos generales, la ejecución de todas las políticas de gestión y rendimiento.
- Analizar tanto el contexto interno y externo del MIDENA a fin de determinar la identificación de los riesgos y sus posibles causas, así como retos, tendencias y oportunidades de mejora e innovación en la gestión.
- Identificar espacios de articulación y cooperación con otras entidades del sector, órganos de control, u organismos internacionales para la implementación de estrategias relacionadas a seguridad y privacidad de la información sensible.

2.2.1 Valoración del riesgo

Se constituye como una herramienta que permite tomar decisiones de cómo: tratar los riesgos, mantener los controles existentes, reevaluar los objetivos, entre otros. Para la toma de decisiones es necesario se considere los requisitos legales, reglamentarios y otros requisitos coordinados.

Durante este procedimiento, es fundamental reconocer los posibles riesgos, detallarlos ya sea de forma cuantitativa o cualitativa, y clasificarlos en función de los criterios de evaluación de riesgos y los objetivos pertinentes para la entidad. A través de esta etapa se recopila toda la información requerida para comprender, evaluar y dar

prioridad a los riesgos. La evaluación de riesgos abarca una serie de tareas que incluyen las siguientes actividades:

En esta situación se han identificado los peligros que puedan perjudicar a la CID de la información, así como las posibles amenazas que podrían obstaculizar la continuidad de las operaciones de este departamento gubernamental dentro del marco de seguridad y protección de la información, establecido por el MINTEL como la autoridad principal en temas de seguridad de la información en el Ecuador. Este proceso permitió identificar a las partes involucradas en los riesgos, los estándares para evaluar las repercusiones de la materialización de los riesgos, y la probabilidad de que ocurran.

2.2.1.1 Identificación de Activos de Información

Tipo de activos de información identificados:

Tabla 2: *Consideraciones establecidas para la identificación de los activos del MIDENA*

Activos de Información Identificados	
Tipo	Descripción
Información digital	Comprende los archivos digitales gestionados a través de los Sistemas de Gestión Documental.
Software	Corresponde a las herramientas de desarrollo, utilitarios y sistemas dispuestas a través de la DTIC.
Servicios	Comprende los servicios tecnológicos que se han dispuesto como parte de los procesos de la institución. (webmail zimbra y telefonía IP).

Nota. Fuente: El autor

Para la evaluación del impacto, se consideraron los conceptos fundamentales de la seguridad de la información. Se examinó cómo la afectación a la triada CID afecta

aspectos como las finanzas, las obligaciones legales y contractuales, así como la reputación de la institución. Se establecieron los siguientes criterios con este propósito:

Tabla 3: *Criterios de evaluación considerados para medir el nivel de riesgo de los activos del MIDENA.*

Valoración del impacto	<u>confidencialidad</u> - C	<u>integridad</u> - I	<u>disponibilidad</u> - D
Alto (3)	La difusión no permitida de datos tiene un impacto crucial en el MIDENA. (Ej. Divulgación de información con clasificación: confidencial, reservada o secreta)	La alteración o eliminación no permitida de la información tiene consecuencias graves en la institución.	La falta de acceso a la información o sistemas por parte de usuarios autorizados tiene efectos graves en la institución.
Medio (2)	La difusión no autorizada de datos presenta un impacto limitado para la institución. (Ej. Divulgación de información de interna de la institución)	La modificación o destrucción no autorizada de la información afecta significativamente a la institución.	La imposibilidad de acceder a la información o sistemas por parte de usuarios autorizados tiene un impacto significativo en la institución
Bajo (1)	La difusión de datos no presenta ningún efecto para la institución. (Ej. Divulgación de información sin clasificación o pública.)	La manipulación o destrucción de la información ocasiona un impacto leve en la institución.	La restricción de acceso a la información o sistemas para usuarios autorizados tiene un impacto mínimo en la institución.

Nota. Fuente: El autor

2.2.1.2 Identificación de amenazas y vulnerabilidades

Después de valorar el impacto, se procedió a analizar la posibilidad de que dicho riesgo se haga realidad; es decir, evaluar la oportunidad de que una amenaza saque provecho de la debilidad del bien en cuestión. Se revisó la efectividad de los sistemas de

seguridad actuales y su historial en proporcionar un nivel suficiente de resguardo. Para ello, se establecieron los siguientes criterios:

Tabla 4: *Ejemplo de valoración de la probabilidad.*

Valoración de la probabilidad	Estimación de la amenaza (criterio)	Estimación de la vulnerabilidad (criterio)	Ejemplo de vulnerabilidad (TI)
Alto (3)	La ocurrencia es muy probable (probabilidad > 50%).	No se han establecido medidas de seguridad para evitar que la amenaza ocurra.	No se requiere el uso de contraseñas para acceder a los sistemas.
Medio (2)	La ocurrencia es probable (probabilidad =50%).	Aunque hay medidas de seguridad vigentes, no logran disminuir la posibilidad de que ocurra la amenaza a un nivel aceptable.	A pesar de existir pautas sobre la creación de contraseñas, no se llevan a cabo.
Bajo (1)	La ocurrencia es menos probable (probabilidad >0 y <50%).	La medida de seguridad actual es adecuada	Aunque hay directrices sobre el uso de contraseñas, estas son implementadas de manera efectiva.

Nota. Fuente: El autor

2.2.1.3 Identificación de controles existentes

Tabla 5: *Controles identificados.*

Ítem	Dominio	Controles ECSI V2	Controles que disponía en MDN
1	Políticas de seguridad de la información	2	100%
2	Organización de la seguridad de la información	8	25%
3	Seguridad de los recursos humanos	6	85%
4	Gestión de activos	10	85%
5	Control de acceso	14	85%

6	Criptografía	2	85%
7	Seguridad física y del entorno	15	85%
8	Seguridad de las operaciones	14	0%
9	Seguridad en las comunicaciones	7	80%
10	Adquisición, desarrollo y mantenimiento de los sistemas	13	80%
11	Relaciones con proveedores	5	80%
12	Gestión de incidentes de seguridad de la información	7	80%
13	Aspectos de seguridad de la información para la gestión de la continuidad del negocio	4	90%
14	Cumplimiento	8	100%
TOTAL		115	

Nota. Fuente: El autor

2.2.1.4 Evaluación del riesgo

Para identificar el nivel de riesgo se aplica la formula en la que se determina al multiplicar la posibilidad de que ocurra una amenaza, la probabilidad de que ocurra una vulnerabilidad y el valor del impacto del activo de información:

$$\text{Nivel de riesgo} = \text{Nivel de amenaza} * \text{Nivel de vulnerabilidad} * \text{VA(CID)}$$

Para ello se propuso una semaforización que permitirá visualizar y seleccionar de mejor manera la opción de tratamiento y manejo de los riesgos:

Tabla 6: Criterios de evaluación del riesgo en el MIDENA.

<i>Riesgo es</i>	<i>NIVEL DE RIESGO</i>
<i>definido como:</i>	<i>(nivel de amenaza * nivel de vulnerabilidad * VA)</i>
ALTO	<i>de 9 a 27</i>
MEDIO	<i>de 4 a 8</i>

BAJO*de 1 a 3*

Nota. Fuente: El autor

En el caso de riesgos clasificados en un nivel MEDIO y ALTO, es decir, con un puntaje de 4 a 27, se consideran como riesgos INACEPTABLES y se les dará tratamiento. Por otro lado, los riesgos de nivel BAJO, aquellos con un puntaje de 1 a 3, se consideran como riesgos ACEPTABLES y el MIDENA los asumirá.

Tabla 7: *Evaluación del riesgo*

Análisis de Riesgos				Evaluación de Riesgos					Nivel de Riesgo
				Impacto	Probabilidad		Controles implementados existentes	Cálculo de Evaluación Riesgo	
Nro. activo	Nombre Activo	Amenaza	Vulnerabilidad	CID	Nivel de amenaza	Nivel de vulnerabilidad			
A1	Cisco ISE SNS-3615-K9	medio	medio	2,33	2	2	Control de acceso	9,33	Alto
A2	Wireless LAN Controller Cisco AIR-CT3504-K9	medio	alto	2,33	2	3	Actualización del software del equipo	14,00	
A3	Forti Gate VM64 (UTM)	bajo	medio	2,67	1	2	Actualización de las reglas de seguridad del equipo	5,33	Medio
A4	Cisco Router ISR4321-SEC/K9	bajo	bajo	2,33	1	1	Verificación óptima del equipo	2,33	Bajo
A6	Central IP Alcatel-Lucent Omni-PCX Enterprise	bajo	bajo	2,00	1	1	Control y supervisión de funcionamiento.	2,00	

A7	Servidor IBM 3550 M3 (Correo electrónico Institucional Zimbra)	medio	bajo	2,33	2	1	Políticas de seguridad contra phishing y malware	4,67	Medio
A11	IBM Storage DS3512 (Sistema SECUROS Cámaras Monitoreo PMM)	medio	bajo	2,00	2	1	Análisis de Vulnerabilidades de los sistemas de información provistos en el activo	4,00	Medio
A12	SERVIDOR LENOVO ThinkSystem SR650 SERVIDOR LENOVO ThinkSystem SR650	bajo	medio	2,33	1	2	Verificación permanente del adecuado funcionamiento del equipo	4,67	Medio
A13	Storage_Controller DE2000H	bajo	medio	2,33	1	2	Verificación permanente del adecuado funcionamiento del equipo	4,67	Medio
A14	Servidor Virtual FORTIGATE_MDN Servidor Virtual Antivirus_MDN	bajo	medio	2,33	1	2	Verificación permanente del adecuado funcionamiento del equipo	4,67	Medio
A15	Switch CORE Cisco 9404R	medio	medio	3,00	2	2	Verificación permanente del adecuado funcionamiento del equipo	12,00	Alto

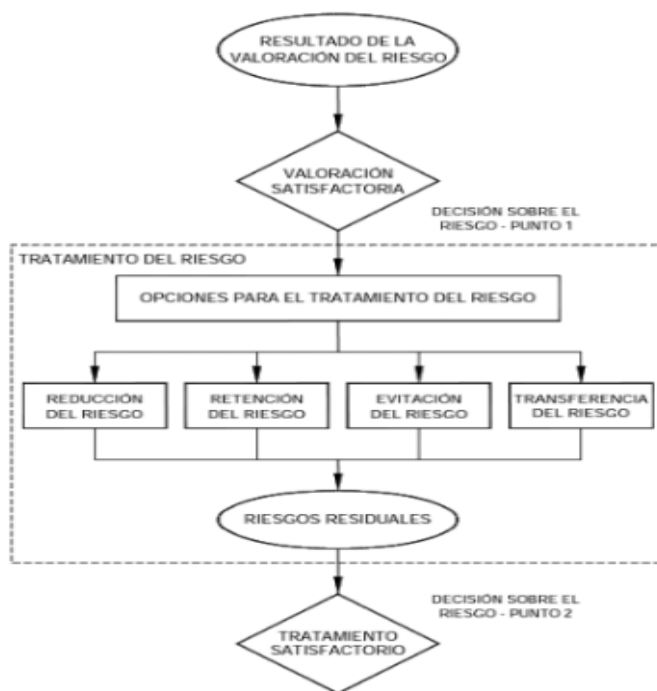
	Antivirus Institucional								
A17	Servicio de Correo Institucional Zimbra	medio	medio	2,67	2	2	Verificar la instalación de un antivirus en todos los equipos	10,67	Alto
	Sistemas y Aplicativos Institucionales								
A18	Data Center	alto	bajo	3,00	3	1	Control de acceso	9,00	Alto

Nota. Fuente: El autor

2.2.2 Tratamiento Del Riesgo

El manejo de los riesgos se efectuará en todos los riesgos catalogados como INACEPTABLES. En este procedimiento, se han establecido cuatro alternativas para tratar los riesgos.:

Figura 5: Desarrollo del Tratamiento de riesgos.



Nota. Adaptado de *Guía para la Gestión de Riesgos de Seguridad de la Información* (p. 5), por MINTEL, 2020.

- **Reducción** la posibilidad de riesgos mediante la implementación de medidas de seguridad.
- **Transferir** la responsabilidad de riesgos a otras entidades, como adquirir un seguro con una empresa de seguros.
- **Evitar** riesgos al interrumpir actividades que representen un alto riesgo, o al modificar la forma en que se realizan.
- **Aceptar** la presencia de riesgos, por ejemplo, si el costo de reducirlos supera el posible daño ocasionado.

Tabla 8: Tratamiento del riesgo

Nombre Activo	Nivel de Riesgo	Método de tratamiento de Riesgos	Tipo de control	Controles a Implementar	Cálculo de Evaluación Riesgo con el control implementado	Nivel de Riesgo con el control Implementado
Cisco ISE SNS-3615-K9	Alto	Mitigar / Evitar / transferir	Control preventivo	Actualización de los parches de seguridad del Equipo.	2,33	BAJO
Wireless Lan Controller Cisco AIR-CT3504-K9	Alto	Mitigar / Evitar / Transferir	Control preventivo	Actualización de los parches de seguridad del Equipo.	2,33	BAJO
Forti Gate VM64 (UTM)	Medio	Mitigar / Evitar / Transferir	Control preventivo	Control de las reglas para el tráfico de datos de la red del MDN	2,33	BAJO
Cisco Router ISR4321-SEC/K9	Bajo	Aceptar	No aplica control	Continuar con la verificación del equipo	2,33	BAJO
Access Point Cisco AIR-AP-	Medio	Mitigar / Evitar / Transferir	Control preventivo	Verificación de los perfiles y accesos de	2,33	BAJO

1852i-A-K9				todos los usuarios del sistema.		
Access Point CiscoAIR-AP-1852i-A-K9 Central IP Alcatel-Lucent Omni-PCX Enterprise	Bajo	Aceptar	No aplica control	No Aplica	2,33	BAJO
Servidor IBM 3550 M3 (Correo electrónico Institucional Zimbra)	Medio	Mitigar / Evitar / Transferir	Control correctivo	Implementación de reglas de seguridad para restringir el tráfico y recepción de correos maliciosos desde correos no autenticados	2,33	BAJO
Servidor IBM 3550 M3 (Correo electrónico Institucional Zimbra)						
Servidor IBM System x 3110	Medio	Mitigar / Evitar / Transferir	Control correctivo	Plan de Acción sobre las vulnerabilidades detectadas	2,33	BAJO
Servidor IBM	Medio	Mitigar / Evitar / Transferir	Control correctivo	Plan de Acción sobre las vulnerabilidades detectadas	2,33	BAJO
Servidor IBM System x 3755 M3	Medio	Mitigar / Evitar / Transferir	Control correctivo	Plan de Acción sobre las vulnerabilidades detectadas	2,33	BAJO
Servidor IBM System x 3755 M3						
IBM Storage DS3512 (Sistema SECUROS Cámaras Monitoreo PMM)	Medio	Mitigar / Evitar / Transferir	Control correctivo	Plan de Acción sobre las vulnerabilidades detectadas	2,33	BAJO
SERVIDOR LENOVO ThinkSystem SR650	Medio	Mitigar / Evitar / Transferir	Control preventivo	Verificar actualizaciones, licenciamientos y operación del equipo	2,33	BAJO
SERVIDOR LENOVO ThinkSystem SR650						
Storage_Controladora DE2000H	Medio	Mitigar / Evitar / Transferir	Control preventivo	Verificar actualizaciones, licenciamientos	2,33	BAJO

Servidor Virtual FORTIGATE_MDN	Medio	Mitigar / Evitar / Transferir		y operación del equipo		BAJO
Servidor Virtual Antivirus_MDN			Control preventivo	Verificar actualizaciones, licenciamientos y operación del equipo	2,33	
Servidor Virtual MUSEOS_INT RANET						
Switch CORE Cisco 9404R	Alto	Mitigar / Evitar / Transferir	Control preventivo	Verificar control de acceso al equipo y garantizar la seguridad del mismo	2,33	BAJO
Switch de Acceso cisco WS-C3560G-24PS	Bajo	ACEPTAR	No aplica control	No Aplica	2,33	BAJO
Switch de Acceso cisco WS-C3560X-48PS	Alto	Mitigar / Evitar / Transferir				BAJO
Antivirus Institucional						
Servicio de Correo Institucional Zimbra			Control preventivo	Verificar el licenciamiento y funcionamiento de los antivirus	2,33	
Sistemas y Aplicativos Institucionales	Alto	Mitigar / Evitar / Transferir				BAJO
Data Center			Control correctivo	Planificación de un plan de seguridad y control de los activos, así como la modernización de los sistemas de control del Data Center	2,33	

Nota. Fuente: El autor

2.2.3 Aceptación del Riesgo

En ciertas ocasiones, es necesario decidir enfrentar los peligros y obligaciones que conlleva una elección, formalizándola de manera adecuada. Esto sucede cuando los gastos relacionados con la implementación de un sistema de seguridad superan el valor del bien de información que se busca resguardar, o cuando el nivel de riesgo se considera muy reducido, situaciones en las cuales la entidad acepta las posibles pérdidas derivadas de la concreción del peligro. En otras circunstancias, el riesgo restante puede no estar en línea con los estándares de aceptación establecidos debido a situaciones particulares que no fueron contempladas por dichos criterios. Por ejemplo, se podría afirmar que es imprescindible tolerar ciertos riesgos por los beneficios sumamente atractivos que conllevan, o porque el costo de modificar dichos riesgos resulta excesivamente elevado. Es esencial que la entidad defina sus propias pautas de aceptación de riesgos para cada caso concreto.

2.2.4 Comunicación del Riesgo

La comunicación eficaz entre los involucrados es primordial, debido a que puede interferir en las decisiones que se tomen en el proceso. La comunicación facilita que los responsables de implementar la gestión de riesgos como aquellos con un interés directo comprendan los fundamentos detrás de las decisiones y la necesidad de acciones específicas. Esta comunicación se caracteriza por ser bidireccional, asegurando un intercambio fluido de información y puntos de vista.

2.2.5 Monitoreo y revisión del riesgo

El MIDENA debe garantizar a través del OSI la idoneidad continua del proceso de manejo del riesgo de seguridad de la información y sus actividades asociadas en las circunstancias actuales, garantizando su efectividad. Cualquier mejora acordada para el

proceso o acciones destinadas a reforzar su cumplimiento deben ser informadas al Comité de Seguridad de la Información (CSI). Esto asegura que no se descuiden ni minimicen riesgos o aspectos relacionados, tomando las medidas pertinentes y adoptando decisiones adecuadas para mantener una comprensión realista del riesgo y la capacidad de respuesta.

2.3 Análisis comparativo

Tabla 9: *Riesgo residual.*

Impacto	Calificación Riesgos Inherente				Controles a Implementar	Calificación Riesgos Residual				Riesgo Residual
	Nivel de amenaza	Nivel de vulnerabilidad	Cálculo de Evaluación Riesgo Inherente	Nivel de Riesgo		Nivel de amenaza	Nivel de vulnerabilidad	Cálculo de Evaluación Riesgo Residual	Nivel de Riesgo con el control Implementado	
2,33	2	2	9,33	Alto	Actualización de los parches de seguridad del Equipo.	1	1	2,33	Bajo	Aceptable
2,33	2	3	14,00	Alto	Actualización de los parches de seguridad del Equipo.	1	1	2,33	Bajo	Aceptable
2,67	1	2	5,33	Medio	Control de las reglas para el tráfico de datos de la red del MIDENA.	1	1	2,33	Bajo	Aceptable
2,33	1	1	2,33	Bajo	Continuar con la verificación del equipo	1	1	2,33	Bajo	Aceptable
2,33	1	2	4,67	Medio	Verificación de los perfiles y accesos de todos los usuarios del sistema.	1	1	2,33	Bajo	Aceptable
2,00	1	1	2,00	Bajo	NO APLICA	1	1	2,33	Bajo	Aceptable
2,33	2	1	4,67	Medio	Implementación de reglas de seguridad para restringir el tráfico y recepción de correos maliciosos desde correos no autenticados	1	1	2,33	Bajo	Aceptable
2,00	2	1	4,00	Medio	Plan de Acción sobre las vulnerabilidades detectas	1	1	2,33	Bajo	Aceptable

2,33	1	2	4,67	Medio	Verificar actualizaciones, licenciamientos y operación del equipo	1	1	2,33	Bajo	Aceptable
2,33	1	2	4,67	Medio	Verificar actualizaciones, licenciamientos y operación del equipo	1	1	2,33	Bajo	Aceptable
2,33	1	2	4,67	Medio	Verificar actualizaciones, licenciamientos y operación del equipo	1	1	2,33	Bajo	Aceptable
3,00	2	2	12,00	Alto	Verificar control de acceso al equipo y garantizar la seguridad del mismo	1	1	2,33	Bajo	Aceptable
2,67	1	1	2,67	Bajo	NO APLICA	1	1	2,33	Bajo	Aceptable
2,67	2	2	10,67	Alto	Verificar el licenciamiento y funcionamiento de los antivirus	1	1	2,33	Bajo	Aceptable
3,00	3	1	9,00	Alto	Planificación de un plan de seguridad y control de los activos, así como la modernización de los sistemas de control del Data Center	1	1	2,33	Bajo	Aceptable

Nota. Fuente: El autor

En la Tabla 9 se puede visualizar que el nivel de riesgo se reduce en su probabilidad al momento de aplicar un control al activo evaluado. Para el tratamiento de riesgo inherente el control aplicado debe estar alineado el EGSI v2.0 a fin de cumplir con la norma establecida. Al estar el EGSI v2.0 basado en un proceso de mejora continua todos los controles implementados podrán ser perfectibles en base al nivel de madurez que se desarrolle producto del tratamiento continuo de los riesgos hasta llegar a su nivel de aceptación.

Se puede observar que el control implementado cumple con los hitos de control que establece el EGSI v2.0 y que son establecidos por medio procedimientos o políticas institucionales que involucran los roles, responsabilidades y obligaciones de cumplimiento a las partes o actores involucrados.

Como, por ejemplo: la Política de Seguridad de la Información que establece las normas y obligaciones generales de todas las áreas del ministerio. Los Procedimientos de Seguridad en Operaciones que establece a la DTIC la separación de los entornos de desarrollo, pruebas y producción; los Procedimiento de Seguridad de la Información para la Gestión de la Continuidad que establece la planificación de la continuidad de la seguridad de la información, implementación de la continuidad, verificar, revisar y evaluar la continuidad de la seguridad de la información.

La seguridad de la información se debe manejar con responsabilidad y buen gobierno ya que cualquier afectación en su disponibilidad, integridad, confidencialidad y accesibilidad afectará directamente a la imagen y reputación del MIDENA

Es fundamental en esta situación tomar una postura proactiva y planificada en cuanto a la protección de la información. Llevar a cabo el Enfoque Global de Seguridad de la Información de forma sólida, constante y en concordancia con los estándares más

destacados posibilitará resguardar los bienes de información de esta cartera de Estado, cumplir con las normativas actuales y asegurar la confianza de los usuarios tanto personal militar como civil.

Es por ello que la implementación de un Programa de Ciberseguridad es crucial en el contexto actual debido a la creciente amenaza de ataques cibernéticos a instituciones y organizaciones. Este programa no solo asegura la protección de los activos digitales y la información sensible, sino que también garantiza el cumplimiento de estándares y normativas establecidos, como los delineados en el EGSi v2.0.

Este documento permitirá el enforzar los hitos de control que deben ser rigurosamente seguidos a través de procedimientos y políticas institucionales claras. Estas políticas definen los roles, responsabilidades y obligaciones de cumplimiento para todas las partes involucradas, asegurando así una implementación efectiva y coordinada del programa de ciberseguridad. Este enfoque integral no solo fortalece la resistencia de la organización frente a posibles amenazas cibernéticas, sino que también promueve una cultura de seguridad proactiva y continua en toda la entidad.

3 **Capítulo III. Propuesta**

**3.1 Propuesta del Programa de Ciberseguridad del Ministerio de Defensa
Nacional**

Información del Documento

Tabla 10: *Información del documento.*

HISTORIA DEL DOCUMENTO				
Nombre del Documento	PROGRAMA DE CIBERSEGURIDAD DEL MINISTERIO DE DEFENSA NACIONAL			
Elaborado por:	MAYO COM SANTIAGO ANDRADE BURBANO			
Unidad responsable	Subsecretaria de Defensa Nacional	Fecha de Elaboración:	ENERO - AGOSTO 2024	

Nota. Fuente: El autor

I. Capítulo 1 del Programa de Ciberseguridad

1. Objetivos

a. Objetivo General:

Direccionar las políticas y procedimientos de seguridad de la información como parte de la implementación de un SGSI, que norme las actividades de los funcionarios del MIDENA con el fin de preservar la CID de la información, así como evitar, reducir y contrarrestar cualquier incidente de ciberseguridad.

b. Base Legal:

- Política Nacional de Ciberseguridad.

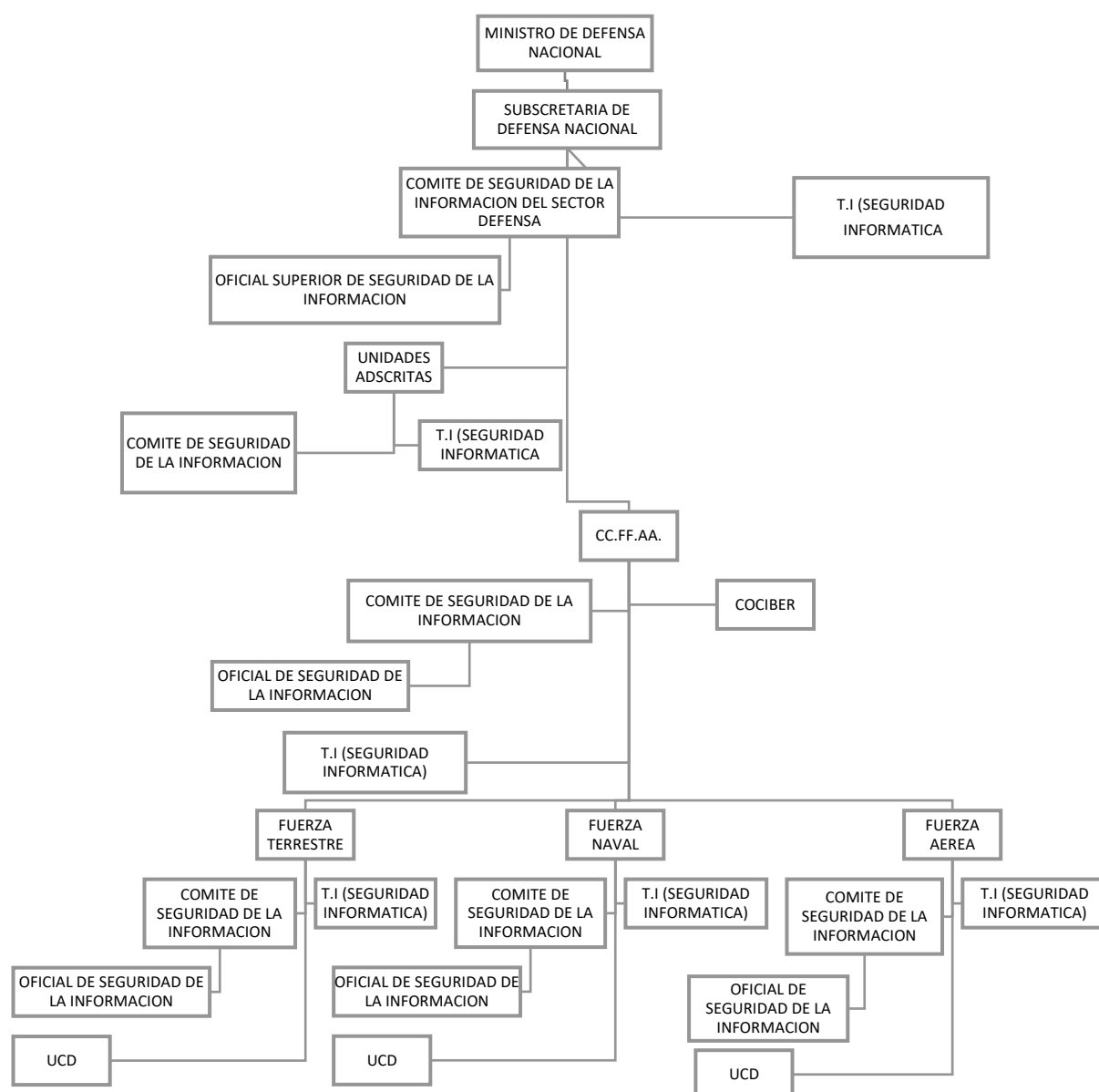
- Estrategia Nacional de Ciberseguridad.
- Estrategia de Ciberdefensa del sector Defensa.
- Esquema Gubernamental de Seguridad de la Información (EGSI v2.0)

c. Alcance

Este documento establece políticas y procedimientos aplicables al sector Defensa, mediante el desarrollo del Programa de Ciberseguridad del MIDENA para enforzar y garantizar el cumplimiento de las políticas, procesos y estándares de ciberseguridad del EGSI v2.0. Se integra y coordina con los elementos funcionales del EGSI para salvaguardar los activos de información del MIDENA. El Programa de Ciberseguridad establece las condiciones necesarias para la operación de tecnologías de la información (TI), apoye la preparación y la resiliencia de las misiones y garantice la CID de la información.

d. Roles y responsabilidades

- Ministerio de Defensa Nacional
- Subsecretaria de Defensa Nacional
- Comando Conjunto de las Fuerzas Armadas
- Fuerza Terrestre
- Fuerza Naval
- Fuerza Aérea
- Entidades Adscritas
- Oficial Superior de Seguridad de la Información del MIDENA

Figura 6: Organigrama CSI

Nota: Fuente el autor

e. Definiciones

EGSI: Es de cumplimiento obligatorio de todos los funcionarios del MIDENA con el fin de preservar la CID de la información.

Integridad: se refiere a garantizar que la información se conserve de manera precisa, sin sufrir cambios no autorizados por personas o sistemas.

Disponibilidad: Se refiere a la cualidad que tiene la información de estar siempre accesible y utilizada por aquellas personas, entidades o procesos autorizados que la necesiten.

Confidencialidad: Se relaciona con la característica que busca asegurar que la información solamente sea vista por individuos o sistemas con la autorización correspondiente.

Información: Conjunto organizado de datos procesados, se refiere a cualquier dato digital o electrónico que tenga valor para una organización o individuo.

Copias de respaldo: Una copia de seguridad es una duplicación de los datos originales, elaborada con la finalidad de generar un recurso para recuperarlos en caso de una afectación que conlleve a su pérdida. Las copias de seguridad generalmente son almacenadas en un sitio seguro, constituido por un dispositivo de almacenamiento diferente al que contiene los datos originales y que siempre están separados, a fin de reconstruir la información si el original se daña o pierde.

Servidor: Sistema de infraestructura que proporciona servicios, recursos o funciones a otros dispositivos o usuarios a través de una red, los mismos pueden incluir servidores web, de correo electrónico, de bases de datos, entre otros. Su función principal es gestionar y almacenar datos críticos o sensibles, asegurando que el acceso a estos recursos esté controlado y protegido contra amenazas cibernéticas como ataques de malware, intrusiones o intentos de acceso no autorizado.

Activo de Información: En el MIDENA, se clasifican como activos de información aquellos elementos que se consideran de gran importancia o validez para la institución. Estos datos contienen información crucial, ya sea generada o empleada por los procesos de la institución, ya sea en formato digital, físico u otros medios.

Áreas seguras: Sitio donde se maneja información sensible o valiosos equipos informáticos.

Riesgo: es la posibilidad de que una amenaza o evento adverso ocurra, específicamente logre aprovechar una debilidad para causar daños o pérdidas en un activo de información. Por lo general, se interpreta como la combinación entre la probabilidad de que ocurra un evento y las consecuencias que este pueda tener.

Vulnerabilidad: Se trata de una vulnerabilidad en un dispositivo informático o sistema de información que podría ser explotada por amenazas para causar daño. Estas debilidades pueden afectar diferentes partes de un equipo, ya sea su hardware, sistema operativo o software.

Amenaza: Se define como una situación con el potencial de generar daños o pérdidas. En otras palabras, las amenazas pueden concretarse en forma de ataques a un equipo, como por ejemplo la propagación de un virus.

Seguridad digital: Corresponde al campo de la informática que se dedica a resguardar la infraestructura computacional y todo lo asociado a ella, especialmente la información que se almacena o se transmite. Incluye aspectos como la seguridad de la información (mediante políticas, procedimientos y otros controles) y la seguridad informática (a través de herramientas específicas).

Correo electrónico institucional: Es el servicio de correo que le asigna el MIDENA a cada colaborador para que lo utilice en el desarrollo de sus funciones.

Teletrabajo: El trabajo fuera de la oficina abarca diversas formas de generar producción económica, como es el trabajo a distancia, el lugar de trabajo flexible, el trabajo remoto y los entornos de trabajo virtual. Estas modalidades permiten a los trabajadores desempeñar sus funciones en entornos no convencionales.

T.I: Tecnologías de la información que incluyen las gestiones de redes, comunicaciones, dispositivos, infraestructura, hardware, software, aplicaciones y operación de servicios relacionados.

Dispositivos móviles: Como laptops, tablets y teléfonos celulares, son herramientas que nos posibilitan trabajar fuera de las dependencias gubernamentales, como el MIDENA.

f. Sinopsis

La implementación del Programa de Ciberseguridad en el MIDENA es de suma importancia ya que a través de este se busca proteger los activos digitales, este programa incluye la adopción de medidas avanzadas de protección de redes, sistemas y datos, asegurando así la CID de la información crítica. Se establecen políticas rigurosas de acceso y control, así como protocolos de respuesta ante incidentes cibernéticos para mitigar riesgos y fortalecer la resiliencia frente a posibles amenazas. Con un enfoque proactivo y basado en estándares internacionales, el MIDENA busca garantizar un ambiente cibernético seguro y robusto, fundamental para sus operaciones y estrategias.

II. Capítulo 2 del Programa de Ciberseguridad

1. Responsabilidades

Las máximas autoridades en todos los niveles de las instituciones relacionadas al sector defensa, propietarios de sistemas de información y comunicaciones, aplicaciones, servicios digitales y custodios de los activos de información en todos los campos, son responsables de la implementación y el cumplimiento de este programa y a su vez garantizarán la rendición de cuentas individual de actividades bajo su propósito.

a. Máximas autoridades del MIDENA y CC.FF.AA, comandantes de la Fuerza Terrestre, Naval y Aérea y directores de las entidades adscritas del sector Defensa.

Serán los responsables de Implementar el Programa de Ciberseguridad que permita asegurar la correcta interrelación del personal, procesos y tecnologías de información; mismos quienes tienen responsabilidad de desarrollo, adquisición, integración, modificación, operación y mantenimiento de todos los activos de información y estructuras tecnológicas. Esto incluye, pero no se limita a:

Desarrollar, mantener y modificar las tecnologías según sea necesario para avalar la aplicación correcta de políticas, procedimientos y estándares de ciberseguridad, de acuerdo con lo que establece el SGSI y demás regulaciones vigentes relacionadas a la actividad.

Desarrollar e implementar la planificación relacionada al SGSI asignado, como se describe en los procedimientos para el manejo de incidentes de seguridad de la información.

Proporcionar avisos referentes a los derechos de privacidad y explicar las políticas de supervisión a todos los usuarios, las cuales permiten identificar cualquier tipo de anomalía en el tráfico de la red.

Implementar procedimientos de autenticación de usuario a todos los sistemas de información y redes de las instituciones de acuerdo con la Política de Control de Acceso.

Asegurar que exista un proceso eficaz de gestión de vulnerabilidades, el mismo que deberá incluir:

- a) Asegurarse que las configuraciones de línea base disponen los parches necesarios y siguen los procedimientos establecidos y aplicables, los mismos que deben ser actualizados tras la publicación de alertas de vulnerabilidad nuevas o revisadas.
- b) Planificar periódicamente análisis de vulnerabilidad sobre todos los activos tecnológicos.
- c) Determinar procedimientos que garanticen la mitigación de vulnerabilidades y respuesta a incidentes con el fin de:
 - Cumplir de manera oportuna y eficiente con las directivas, directrices y alertas de ciberseguridad emitidas por el MIDENA a través del EcuCert y el COCIBER, orientadas a implementar mitigaciones y medidas correctivas de los sistemas de información de cada institución.
 - Limitar los daños y garantizar la restauración de los servicios después de un incidente.

- Recopilar y conservar datos de auditoría para apoyar el análisis técnico de cualquier incidente, así como proporcionar estos a otras agencias de investigación relacionadas de ser el caso.
- d) Asegurar que los parches de seguridad estén disponibles, según las directrices operativas.
- e) Implementar un proceso de parcheo automatizado, cuando sea práctico, con el fin de minimizar la inactividad del sistema.

Establecer procedimientos de Control de versiones y Control de modificaciones siguiendo las pautas de Gestión de servicios de TI.

Implementar procedimientos de monitoreo de amenazas internas, definidas como parte de un programa integral de ciberseguridad dirigido por el MIDENA a través del OSI.

Asignar roles y responsabilidades en todos los niveles dentro de cada Institución según sea necesario, para implementar, administrar y hacer cumplir las regulaciones que se desprenden de este programa.

Determinar los procedimientos de designación de usuarios privilegiados según las funciones designadas, asegurando para el efecto, que cumplan con los requisitos preestablecidos en las Políticas de Seguridad de la Información de cada una de las instituciones del sector Defensa.

Asegurar que todo el personal relacionado con la implementación, supervisión, control, monitoreo y demás roles que se desprendan del presente programa de ciberseguridad estén designados por escrito. Así mismo cada Institución será la responsable de gestionar su entrenamiento y certificación.

Disponer que todos los funcionarios que laboran en la institución:

- a) Estén debidamente autorizados, capacitados, calificados y autorizados de acuerdo con las emisiones aplicables de seguridad de la información, antes de acceder a los servicios e infraestructura tecnológica de cada institución.
- b) Legalizar un acuerdo de confidencialidad previo a la creación y activación de credenciales de acceso a cualquier sistema de información dentro de la institución, el mismo que deberá incluir:
 - La aceptación y acatamiento de normas y procedimientos que garanticen la seguridad de la información, así como las responsabilidades y comportamientos esperados durante el manejo y acceso de todos los activos de información disponibles en el MIDENA.
 - La aceptación y acatamiento de los derechos de privacidad.

El no acatar las reglas y pasos establecidos por este programa puede considerarse como motivo de responsabilidad administrativa, según la gravedad y tipo de la falta, y será castigado por las autoridades correspondientes. La falta de conocimiento no libera de la aplicación de sanciones y/o penalidades por el incumplimiento.

Desarrollar capacidades para apoyar los objetivos de ciberseguridad y garantizar que estos estén alineados a las políticas establecidas por el MIDENA.

Identificar los recursos necesarios para implementar el presente programa para su inclusión en el proceso de planificación y programación anual.

Identificar y evaluar a través una adecuada gestión de riesgos, la implementación del presente programa en cada institución.

Disponer un programa de concientización y difusión continua, que permita mantener actualizado los conocimientos de amenazas y vulnerabilidades de ciberseguridad para apoyar las decisiones de gestión de riesgos.

Asegurar que la seguridad informática y de la información esté presente desde el inicio y durante todo el proceso de desarrollo de los sistemas de información.

Incluir dentro de la cultura organizacional, campañas de ciberseguridad dentro de cada institución, orientadas a la protección de la triada de la información.

Dar cumplimiento a los procedimientos que implementan el canal de comunicación directo para reportar incidentes sospechosos o confirmados de acuerdo con las regulaciones establecidas a través del MIDENA y puestas en conocimiento a través del COCIBER con los procesos establecidos.

Cumplir con las políticas específicas del Programa de Ciberseguridad de manera oportuna y eficiente, así como las recomendaciones de ciberseguridad emitidas por el MIDENA para mitigar y tomar medidas preventivas o correctivas de acuerdo al caso.

b. Comando Conjunto de las Fuerzas Armadas, Fuerza Terrestre, Naval y Aérea y entidades adscritas y dependientes relacionadas al sector Defensa

Además de las responsabilidades emitidas en el apartado anterior deberá incluir las siguientes actividades:

Incorporar la verificación de temas relacionados a la ciberseguridad en los programas de inspección organizacional y las visitas de comando.

Incluir evaluaciones que permitan definir el nivel de reacción ante posibles incidentes o afectaciones a los sistemas de información e infraestructura tecnológica de cada institución para definir el nivel de preparación.

c. Comando de Ciberdefensa (COCIBER)

- 1) Articular la gestión de incidentes de ciberseguridad en el sector defensa.
- 2) Establecer y mantener un canal para el reporte de incidentes del ciberespacio de todas las instituciones relacionadas al sector defensa.
- 3) Desarrollar guías, listas de verificación y procedimientos de respuesta a incidentes en el ciberespacio en apoyo a todas las instituciones relacionadas al sector defensa.
- 4) Ejecutar y establecer auditorías, con la finalidad de verificar el nivel de cumplimiento y madurez de las Instituciones relacionadas al sector defensa en el ámbito de la Ciberseguridad.
- 5) Evaluar los informes de incidentes para identificar problemas sistémicos o críticos relacionados con la ciberseguridad y notificarlos al MIDENA a través del CC.FF.AA.
- 6) Desarrollar políticas, estándares, procesos y procedimientos operativos de ciberseguridad en coordinación con los programas de ciberseguridad del MIDENA.
- 7) Operar y mantener una base de datos de vulneraciones, mitigaciones e incidentes del ciberespacio de las instituciones del sector defensa, los mismos que deberán ser remitidos a través de boletines mensuales al MIDENA.
- 8) Administrar la mitigación de vulnerabilidades de las instituciones en el sector defensa y presentar informes de incidentes con el fin de:
 - a) Restaurar los daños y servicios de manera efectiva después de un incidente en coordinación con las Unidades de Ciberdefensa de las fuerzas.

- b) Recopilar y mantener los datos para apoyar el análisis técnico relacionado con el uso indebido, penetración u otros incidentes.

d. Oficial de seguridad de la información del MIDENA (OSI)

El OSI del MIDENA, será un oficial superior en el grado de Mayor o Teniente Coronel, de cualquiera de las tres ramas de las Fuerzas Armadas y será el responsable de dirigir y coordinar el Programa de Ciberseguridad del MIDENA; esto incluye, pero no se limita a:

- Supervisar el desarrollo y la difusión de la política general de ciberseguridad para el MIDENA.
- Cumplir con las funciones de OSI del MIDENA y a su vez ser miembro con derecho a voto del CSI de esta cartera de Estado.
- Desarrollar políticas para garantizar que el proceso de evaluación de la ciberseguridad en Fuerzas Armadas siendo consistente con la política y la orientación del CSI y la Subsecretaría de Defensa Nacional.
- Servir como punto de coordinación de ciberseguridad para los programas conjuntos.
- Coordinar con las autoridades pertinentes para integrar los conceptos de ciberseguridad en el proceso de adquisición dentro del MIDENA.
- Recomendar actualizaciones y adiciones para los controles de seguridad del SGSI.
- Será el responsable de supervisar que se mantenga la postura de seguridad operativa adecuada y trabajará con los OSI de las instituciones

y entidades adscritas del sector Defensa para garantizar el cumplimiento del mismo.

e. Comité de Seguridad de la Información

El CSI será presidido por la máxima autoridad o su delegado e integrado por los funcionarios responsables o sus delegados de las siguientes dependencias: Coordinación Administrativa Financiera, Recursos Humanos, Operaciones, Inteligencia, Logística, CCSS, Gestión Estratégica, Gestión por Procesos, OSI de la institución y DTIC's como miembros permanentes, considerando que se podrá citar a otros miembros Ad-hoc y /transversales.

Dentro de sus funciones se enlista para su cumplimiento:

- Proponer la designación del OSI dentro de cada Institución, quienes deberán poseer los suficientes conocimientos en Seguridad de la Información, deberá pertenecer al nivel jerárquico superior y obligatoriamente no deberá estar subordinado a las dependencias de TI de las instituciones, con la finalidad de dar cumplimiento a la independencia de funciones.
- Examinar y, si es necesario, ayudar en la puesta en marcha de los proyectos de seguridad informática en todas las organizaciones.
- Entender la administración de riesgos que puedan impactar los activos de información frente a las amenazas más significativas.
- Analizar las propuestas e iniciativas presentadas por el OSI y gestionar su aprobación por parte de la máxima autoridad.

- El Comité remitirá a través de la máxima autoridad a la Subsecretaria de Defensa Nacional el reporte de cumplimiento.

f. OSI perteneciente a las instituciones y/o unidades adscritas

Será designado por la máxima autoridad de cada Institución y responsable de garantizar que se mantenga la postura de seguridad operacional adecuada para el sistema de información de cada Institución, así como cumplir con todas las políticas y procedimientos de ciberseguridad propuestos por el OSI del MIDENA. Del mismo modo garantizará que todos los usuarios de las Instituciones sean conscientes de sus responsabilidades en materia de ciberseguridad, esto incluye actividades relacionadas con el mantenimiento de la conciencia situacional y la puesta en marcha de acciones para mejorar o restaurar una postura sólida de ciberseguridad:

- Desarrollar propuestas para crear la documentación esencial del SGSI en cada entidad.
- Crear un Plan de sensibilización en seguridad de la información basado en el SGSI.
- Establecer un plan para supervisar y controlar la ejecución de mejoras o acciones correctivas.
- Coordinar y gestionar la elaboración del Plan de Contingencia de Seguridad de la Información con todos los Departamentos o Direcciones relevantes de cada entidad.
- Brindar orientación y establecer un proceso adecuado para manejar incidentes de seguridad de la información internos.

- Organizar y legalizar debidamente la documentación de implementación del SGSI, avalada por la máxima autoridad de cada entidad.
- Reportar al CSI el progreso de la implementación del EGSi v2.0 y alertar sobre posibles obstáculos en cada entidad.

g. Unidades responsables de TIC

Serán los funcionarios responsables de la implementación de los diversos controles técnicos que viabilizan la imposición de las disposiciones establecidas en políticas y procedimientos, así como los estándares de seguridad en los marcos de referencia.

Efectuar actividades de ingeniería de seguridad de sistemas de información, incluida la arquitectura del sistema, el diseño, el desarrollo y la configuración, que definen técnicamente la postura de seguridad general de un sistema.

h. Unidades de Ciberdefensa

En cumplimiento a la Estrategia de Ciberdefensa la inclusión de unidades de ciberdefensa en las Fuerzas Terrestre, Naval y Aérea representa un avance fundamental para adaptarse a los desafíos actuales en materia de seguridad nacional. Estas unidades, especializadas en resguardar las redes y sistemas informáticos militares, juegan un rol esencial en la defensa proactiva contra las amenazas cibernéticas en evolución. Su presencia refuerza la capacidad de las Fuerzas para proteger la información confidencial y mantener la continuidad operativa en un entorno cada vez más digitalizado. Además, están preparadas para colaborar estrechamente entre las ramas de las Fuerzas Armadas y organismos especializados en ciberseguridad, garantizando una respuesta conjunta y eficiente frente a posibles ataques en línea y cuyas responsabilidades son:

- 1) Gestión de vulnerabilidades propias de cada una de las fuerzas
procedimientos de búsqueda, análisis y seguimiento de las mismas, en
coordinación con el OSI, TIC de la Fuerza y COCIBER.
- 2) Gestión de incidentes propios de cada una de las fuerzas en coordinación con
el OSI, TIC de la Fuerza y COCIBER.
- 3) Gestión de conocimiento para el entrenamiento de personal técnico
especializado y aporte a la concienciación.
- 4) Gestión de monitoreo en coordinación con el OSI, TIC de la Fuerza y
COCIBER
- 5) Gestión de evaluación interna de ciberseguridad en coordinación con el OSI.

i. Usuarios (personal militar, servidores y trabajadores públicos y personas que presten servicios ocasionales, temporales)

Los usuarios serán responsables sobre el o los activos de información a su cargo, cumpliendo lo estipulado en el acuerdo de buen uso de activos de la información, generando un compromiso que implique la apropiada custodia, administración y encargo sobre el activo, el uso adecuado del hardware, software, información y recursos que puedan ser entregados para el cumplimiento de sus funciones, velando que éstos sean utilizados para beneficio institucional durante las funciones asignadas y en los lugares físicos y lógicos destinados para el desarrollo de procesos, tareas y actividades atribuidas a las funciones designadas.

III. Capítulo 3 del Programa de Ciberseguridad

1. Consideraciones del Programa de Ciberseguridad del Ministerio de Defensa Nacional

a. Funciones del Programa de Ciberseguridad

El Programa de Ciberseguridad del MIDENA sincroniza y estandariza los requisitos de ciberseguridad para salvaguardar los activos de información de las Instituciones, así como las TI, para apoyar la ejecución de misiones y funciones.

El Ministerio de Defensa Nacional debe:

- Incorporar las mejores prácticas y principios de gestión de riesgos en el ciberespacio en las consideraciones de planificación estratégica de todas las instituciones del sector Defensa, las misiones principales y los procesos de negocio, y apoyar la TI de la organización.
- Establecer límites prácticos y significativos para los sistemas de información organizacionales con el fin de identificar lo que la organización es responsable de proteger.
- Identificar la necesidad de proteger bajo control y administración directa todos los activos de información que por su naturaleza sean exclusivos y calificados.
- Planificar el manejo de riesgos cibernéticos para minimizar el impacto, para lo cual se deberá considerar la resiliencia operativa (continuidad operativa); se deberá asegurar que los activos de información sean confiables y cumplan con los requisitos de acuerdo a las políticas de ciberseguridad y finalmente asegurar que se cuente con planes de

contingencia que garanticen la prevalencia de los activos de información y TI, frente a eventos adversos.

- Gestionar los resultados de la Ciberseguridad y Seguridad de la Información en función de metas y objetivos estratégicos.
- Implementar políticas y procedimientos para minimizar el riesgo en entornos operativos.
- Trabajar para ejecutar y hacer cumplir las responsabilidades de todo el MIDENA alineando los objetivos y estándares de la misión, de acuerdo con las pautas de ciberseguridad.
- Compartir información relacionada a la ciberseguridad y seguridad de la información entre las instituciones del sector defensa, que permitan apoyar la toma de decisiones basada en riesgos vigentes para la evaluación y aceptación de la gestión de riesgos en cada institución.

b. Actividades de gobernanza de la ciberseguridad

La gobernanza proporcionará la orientación estratégica, que garantice la consecución de los objetivos de ciberseguridad, así como una adecuada evaluación del riesgo y su gestión. Las actividades de gobernanza garantizarán:

- Alineación de los objetivos de ciberseguridad con la misión y las estrategias del MIDENA y el Acuerdo Ministerial 199 donde se expide la Política de Ciberdefensa para cumplimiento de todo el sector de la defensa nacional.
- Comprensión de los requisitos regulatorios, legales y de riesgo, que constituyen la gestión de los riesgos cibernéticos, el desarrollo de políticas y la asignación de recursos.

- Integración de consideraciones y requisitos de ciberseguridad en procesos que involucran el desarrollo de estrategias, arquitectura empresarial, planificación de capital y gestión de carteras de TI, supervisión presupuestaria, planificación de la fuerza laboral, capacitación y educación, acuerdos de nivel de servicio, gestión de riesgos de la cadena de suministro, relaciones con socios de misión, programas tradicionales de seguridad y gestión de riesgos, e inspecciones, auditorías e investigaciones.

IV. Capítulo 4 del Programa de Ciberseguridad

1. Implementación del Programa de Ciberseguridad del Ministerio de Defensa Nacional.

En el mundo actual, donde todos estamos conectados y dependemos tanto de la tecnología, es muy importante que las organizaciones de todas las industrias tengan un programa de ciberseguridad. Teniendo esto en cuenta, tener un plan de ciberseguridad sólido es muy importante para mantener seguros sus datos digitales, reducir los riesgos y fortalecer su organización. Este programa tiene como objetivo mantener sus sistemas y redes a salvo de los malos. También le enseña a su personal cómo estar seguro y cómo solucionar cualquier problema rápidamente. Es por ello que para su implementación se deben establecer políticas de seguridad las mismas que son:

a. Política de Seguridad de la Información

Documento que permite planear, organizar, dirigir y controlar las medidas esenciales de seguridad que se deben adoptar, para protegerse apropiadamente

contra amenazas que podrían afectar en alguna medida la CID, ocasionando pérdidas o mal uso de los activos de información.

Cada institución elaborará su política de seguridad de la información en base a sus necesidades y considerando que la misma cumpla con las directrices del EGSI V2.0.

Esta política hace referencia a los siguientes controles:

Tabla 11: *Controles hace referencia la Política de Seguridad de la Información.*

Ítem	Sección	Descripción	Observaciones
92	11.1.1	Política de seguridad de la información en las relaciones con los proveedores	Política de compras públicas

Nota. Adaptado de *Esquema Gubernamental de Seguridad de la Información (EGSI) Versión 2.0* (p. 39), por MINTEL, 2020.

b. Política de Control de Acceso a los Sistemas de Información

Documento elaborado por cada institución con el objeto de reconocer la importancia y el valor de la información y la arquitectura de TI, con respecto al funcionamiento eficiente y efectivo de cada una de las Instituciones, considerando como premisa que la información no es sólo crítica para el éxito y consecución de las Instituciones, sino estratégica, y que permite garantizar la CID de la información a través de una estructura digital que garantice flexibilidad y seguridad.

Esta política hace referencia a los siguientes controles:

Tabla 12: *Controles hace referencia la Política de Control de Acceso a los Sistemas de Información.*

Ítem	Sección	Descripción	Observaciones
	5	Control de acceso	
	5.1	Requisitos institucionales para el control de acceso	
27	5.1.1	Política de control de acceso	Política de control de acceso
	5.4	Control de acceso a sistemas y aplicaciones	
40	5.5	Control de acceso al código fuente del programa	Política de control de acceso

Nota. Adaptado de *Esquema Gubernamental de Seguridad de la Información (EGSI) Versión 2.0* (p. 55), por MINTEL, 2020.

c. Programa de Concientización en ciberseguridad para los usuarios

Documento dirigido por el MIDENA que establezca las pautas para desarrollar y mantener el plan de comunicación y concienciación sobre la seguridad de la información, con el propósito de garantizar una cobertura completa a todos los empleados de las Instituciones. Esto permitirá definir tácticas para concienciar, comunicar y capacitar a todos los usuarios.

Esta política hace referencia a los siguientes controles:

Tabla 13: *Controles hace referencia la Política de Concientización.*

Ítem	Sección	Descripción	Observaciones
14	3.2.2	Concienciación, educación y formación en seguridad de la información	Política de concienciación

Nota. Adaptado de Esquema Gubernamental de Seguridad de la Información (EGSI) Versión 2.0 (p. 46), por MINTEL, 2020.

d. Políticas de Seguridad Digital

1) Procedimientos de organización de la seguridad de la información

Procedimiento que establece el esquema directivo de gestión de seguridad de la información la cual establecerá separación de funciones y de áreas para emisión de gobernanza y controlar la implementación operativa de la seguridad de la información, a fin de garantizar la independencia en la seguridad de la información, se hace referencia a los siguientes controles:

Tabla 14: *Controles hace referencia los Procedimientos de organización de la seguridad de la información*

Ítem	Sección	Descripción	Observaciones
1	1	Políticas de Seguridad de la Información	
	1.1	Dirección de gestión de seguridad de la información	
1	1.1.1	Políticas de Seguridad de la Información	Política de control de acceso
2	1.1.2	Control de acceso a sistemas y Revisión de las políticas para la seguridad de la información	
2	2	Organización de la Seguridad de la Información	Política de control de acceso
3	2.1.1	Compromiso de la máxima autoridad de la institución con la seguridad de la información	
7	2.1.5	Seguridad de la Información en la gestión de proyectos	Política de compras públicas
14	3.2.2	Concienciación, educación y formación en seguridad de la información	Política de concientización
63	8.3.1	Copias de seguridad de la información	Política de respaldos
92	11.1.1	Política de seguridad de la información en las relaciones con los proveedores	Política de compras públicas
12	12	Gestión de incidentes de seguridad de la información	
98	12.1	Reporte de los eventos de seguridad de la información	Política de Gestión de Incidentes de Seguridad de la información
99	12.1.2	Reporte de debilidades de seguridad de la información	Política de Gestión de Incidentes de Seguridad de la información
100	12.1.3	Apreciación y decisión sobre los eventos de seguridad de la información	Política de Gestión de Incidentes de Seguridad de la información
101	12.1.4	Respuesta a incidentes de seguridad de la información	Política de Gestión de Incidentes de Seguridad de la información
102	12.1.5	Aprendizaje de los incidentes de seguridad de la información	Política de Gestión de Incidentes de Seguridad de la información

98	12.1.6	Reporte de los eventos de seguridad de la información	Política de Gestión de Incidentes de Seguridad de la información
104	13.1.1	Planificación de la continuidad de seguridad de la información	Política de continuidad de servicios
105	13.1.2	Planificación de la continuidad de seguridad de la información	Política de continuidad de servicios
106	13.1.3	Planificación de la continuidad de seguridad de la información	Política de continuidad de servicios

Nota. Adaptado de *Esquema Gubernamental de Seguridad de la Información (EGSI)* Versión 2.0, por MINTEL, 2020.

2) Procedimientos de dispositivos móviles y teletrabajo

Posibilita establecer las pautas, los encargados y los elementos que respaldan la política de seguridad cibernética, focalizándose en los DISPOSITIVOS MÓVILES Y EL TELETRABAJO. Esto se realiza con el propósito de proteger la CID de los datos de todas las instituciones y sus estructuras de Tecnologías de la Información.

Se hace referencia a los siguientes controles:

Tabla 15: Controles hace referencia los Procedimientos de dispositivos móviles y teletrabajo.

Ítem	Sección	Descripción	Observaciones
	2.2	Dispositivos móviles y teletrabajo	
10	2.2.2	Teletrabajo	Política de Teletrabajo

Nota. Adaptado de *Esquema Gubernamental de Seguridad de la Información (EGSI) Versión 2.0* (p. 42), por MINTEL, 2020.

3) *Procedimientos de acceso a redes y servicios de red*

Permite establecer las normas que regulen el uso aceptable de los servicios informáticos institucionales de las instituciones, considerando como una herramienta de apoyo en la gestión y desempeño de las funciones y actividades laborales, permitirán normar y proteger la Información, los activos de información, sistemas de almacenamiento, así como toda la infraestructura tecnológica, evitando de esta manera amenazas latentes por el uso del servicio de Internet como herramienta de trabajo.

Se hace referencia a los siguientes controles:

Tabla 16: *Controles hace referencia los Procedimientos de acceso a redes y servicios de red.*

Ítem	Sección	Descripción	Observaciones
28	5.1.2	Acceso a redes y servicios de red	Política de control de la red

Nota. Adaptado de *Esquema Gubernamental de Seguridad de la Información (EGSI) Versión 2.0* (p. 56), por MINTEL, 2020.

4) *Procedimiento de registro, retiro y modificación de usuarios*

Normas para establecer los procesos oficiales que regulan el ingreso, salida y cambios en los usuarios, con la finalidad de autorizar la asignación de permisos de entrada a las diversas fuentes de información y sistemas tecnológicos de todas las Instituciones del sector Defensa.

Se hace referencia a los siguientes controles:

Tabla 17: *Controles hace referencia los Procedimientos de registro, retiro y modificación de usuarios.*

Ítem	Sección	Descripción	Observaciones
29	5.2.1	Registro y retiro de usuarios	Política de control de la red

Nota. Adaptado de *Esquema Gubernamental de Seguridad de la Información (EGSI) Versión 2.0* (p. 57), por MINTEL, 2020.

5) *Procedimiento para el uso y clasificación de la información*

Procedimiento que operacionalice el cumplimiento del Reglamento Interno para la Elaboración, Manejo, Custodia, Difusión y Seguridad de la Información Militar clasificada del MIDENA.

Se hace referencia a los siguientes controles:

Tabla 18: Controles *hace referencia los Procedimientos para el uso y clasificación de la información.*

Ítem	Sección	Descripción	Observaciones
	4.2	Clasificación de la información	
21	4.2.1	Directrices de Clasificación de la información	Política de criptografía

Nota. Adaptado de *Esquema Gubernamental de Seguridad de la Información (EGSI) Versión 2.0* (p. 52), por MINTEL, 2020.

6) *Procedimientos para la gestión de acceso de los usuarios*

Procedimientos que permiten normar y regularizar la gestión de acceso a los usuarios a los diferentes activos de información, sistemas, aplicaciones y arquitecturas de TI, para prevenir accesos no autorizados.

Se hace referencia a los siguientes controles:

Tabla 19: *Controles hace referencia los Procedimientos para la gestión de acceso de los usuarios.*

Ítem	Sección	Descripción	Observaciones
	5.2	Gestión de acceso de los usuarios	
30	5.2.2	Provisión de accesos a usuarios	Política de control de acceso
31	5.2.3	Gestión de los derechos de acceso con privilegios especiales	Política de control de acceso
33	5.2.5	Revisión de los derechos de acceso de usuario	Política de control de acceso
34	5.2.6	Retiro o adaptación de los derechos de acceso	Política de control de acceso

Nota. Adaptado de *Esquema Gubernamental de Seguridad de la Información (EGSI) Versión 2.0* (p. 57), por MINTEL, 2020.

7) *Procedimientos de responsabilidad de usuarios y acceso a sistemas y aplicaciones*

Procedimientos para normar responsabilidades sobre el uso de credenciales de acceso a la información y a la arquitectura TI de cada institución, dentro del desarrollo y cumplimiento de actividades administrativas.

Se hace referencia a los siguientes controles:

Tabla 20: *Controles hace referencia los Procedimientos de responsabilidad de usuarios y acceso a sistemas y aplicaciones.*

Ítem	Sección	Descripción	Observaciones
	5.3	Responsabilidades del usuario	
	5.4	Control de acceso a sistemas y aplicaciones	

Nota. Adaptado de *Esquema Gubernamental de Seguridad de la Información (EGSI) Versión 2.0* (p. 60), por MINTEL, 2020.

8) *Procedimientos de controles criptográficos*

El MIDENA definirá estándares de cifrado. Mientras tanto, las instituciones implementarán temporalmente directrices y procedimientos para regular y controlar el cifrado en el almacenamiento y transmisión de toda la información sensible y clasificada. Esto asegura políticas efectivas de seguridad de la información para garantizar el uso adecuado y eficiente de la criptografía, protegiendo así la confidencialidad, integridad y disponibilidad de la información en los activos de información de diversas arquitecturas TI.

Se hace referencia a los siguientes controles:

Tabla 21: *Controles hace referencia los Procedimientos de controles criptográficos.*

Ítem	Sección	Descripción	Observaciones
	6	Criptografía	
	6.1	Controles criptográficos	
41	6.1.1	Política de uso de los controles criptográficos	Política de criptografía
112	14.1.5	Reglamentos de controles criptográficos	Política de criptografía

Nota. Adaptado de *Esquema Gubernamental de Seguridad de la Información (EGSI) Versión 2.0* (p. 64), por MINTEL, 2020.

9) *Procedimientos de seguridad física y del entorno*

Basado en la estructura tecnológica de cada institución, es fundamental implementar procedimientos que aseguren la seguridad de la infraestructura mediante una homogeneidad efectiva. Esto implica establecer medidas generales de seguridad, tanto técnicas como organizativas, diseñadas para cumplir con garantías esenciales como autenticidad, integridad, confidencialidad, disponibilidad, conservación de la información y trazabilidad. Estas medidas se centran en la seguridad física y del entorno de los activos de información.

Se hace referencia a los siguientes controles:

Tabla 22: *Controles hace referencia los Procedimientos de seguridad física y del entorno.*

Ítem	Sección	Descripción	Observaciones
	7	Seguridad física y del entorno	
43	7.1.1	Perímetro de seguridad física	Política de seguridad física

Nota. Adaptado de *Esquema Gubernamental de Seguridad de la Información (EGSI) Versión 2.0* (p. 66), por MINTEL, 2020.

10) *Procedimientos de escritorio y pantalla limpia de información*

Normativas que regulan las acciones destinadas a evitar accesos no autorizados, así como la pérdida o daño de la información alojada en estaciones

de trabajo, computadoras, dispositivos de almacenamiento extraíbles, impresoras y escáneres, tanto durante como fuera del horario laboral.

Se hace referencia a los siguientes controles:

Tabla 23: *Controles hace referencia los Procedimientos de escritorio y pantalla limpia de información.*

Ítem	Sección	Descripción	Observaciones
	7	Seguridad física y del entorno	
56	7.2.8	Equipo informático de usuario desatendido	Política de escritorio limpio
57	7.2.9	Política de puesto de trabajo despejado y pantalla limpia	Política de escritorio limpio

Nota. Adaptado de *Esquema Gubernamental de Seguridad de la Información (EGSI) Versión 2.0* (p. 73), por MINTEL, 2020.

11) *Procedimientos referentes a responsabilidades operacionales*

Procedimiento que permite garantizar la continuidad y protección de las instalaciones que albergan dispositivos y sistemas tecnológicos empleados en el tratamiento y guarda de datos en las distintas entidades, incluyendo actividades como activación y desactivación, respaldo de información, mantenimiento de dispositivos, manejo de soportes, salas de computación, así como la gestión y protección del correo institucional.

Se hace referencia a los siguientes controles:

Tabla 24: *Controles hace referencia los Procedimientos referentes a responsabilidades operacionales.*

Ítem	Sección	Descripción	Observaciones
	8.1	Procedimientos y responsabilidades operacionales	

58 8.1.1 Documentación de procedimientos de operación

Nota. Adaptado de *Esquema Gubernamental de Seguridad de la Información (EGSI) Versión 2.0* (p. 74), por MINTEL, 2020.

12) Procedimientos referentes a protección contra códigos maliciosos

Enfoques dirigidos a garantizar el correcto funcionamiento y la seguridad de las instalaciones de procesamiento de datos, la defensa contra programas maliciosos considerando los controles empleados tanto en el hardware como en el software, la instalación y actualización de las plataformas de detección, la creación de procedimientos o guías específicas sobre el funcionamiento de la plataforma, la identificación y recuperación de ataques de software malicioso, y la aplicación de métodos para recopilar información de forma periódica, como la suscripción a boletines informativos de cada una de las instituciones.

Se hace referencia a los siguientes controles:

Tabla 25: *Controles hace referencia los Procedimientos a referentes a protección contra códigos maliciosos.*

Ítem	Sección	Descripción	Observaciones
	8	Seguridad de las operaciones	
	8.2	Protección contra un malware	
62	8.2.1	Controles contra malware	Política de gestión de parches

Nota. Adaptado de *Esquema Gubernamental de Seguridad de la Información (EGSI) Versión 2.0* (p. 77), por MINTEL, 2020.

13) Procedimientos de seguridad en operaciones

Procedimientos tendientes a garantizar las operaciones correctas y seguras de las instalaciones de procesamiento de información, así como la correcta operación, administración y funcionamiento de los mismos en cada una de las instituciones.

Se hace referencia a los siguientes controles:

Tabla 26: Controles hace referencia los Procedimientos de seguridad en operaciones.

Ítem	Sección	Descripción	Observaciones
	8	Seguridad de las operaciones	
	8.1	Procedimientos y responsabilidades operacionales	
58	8.1.1	Documentación de procedimientos de operación	
59	8.1.2	Gestión de cambios	Política de control de cambios
60	8.1.3	Gestión de capacidades	Política de monitoreo de redes
61	8.1.4	Separación de ambientes de desarrollo, pruebas y producción	Política de arquitectura de software

Nota. Adaptado de *Esquema Gubernamental de Seguridad de la Información (EGSI)*

Versión 2.0 (p. 74), por MINTEL, 2020.

14) Procedimientos de gestión de la seguridad de redes

Estos procedimientos son fundamentales para garantizar la seguridad de los datos transmitidos a través de redes informáticas y salvaguardar la infraestructura que los respalda. Su implementación refuerza la protección de la información en entornos de red, siendo aplicables de manera universal a todas las redes, servicios de red y mecanismos de control empleados para resguardar la integridad de la información durante su transferencia en cada institución.

Se hace referencia a los siguientes controles:

Tabla 27: *Controles hace referencia los Procedimientos de gestión de la seguridad de redes.*

Ítem	Sección	Descripción	Observaciones
	9.1	Gestión de la seguridad de redes	
74	9.1.3	Separación en las redes	Política de monitoreo de redes

Nota. Adaptado de *Esquema Gubernamental de Seguridad de la Información (EGSI) Versión 2.0* (p. 85), por MINTEL, 2020.

15) *Procedimientos de transferencia de información*

Procedimientos necesarios para establecer los mecanismos de transferencia de información dentro de cada Institución y hacia cualquier entidad externa mediante el uso de todo tipo de instalaciones de comunicación, como correo electrónico, Red privada virtual (VPN), Secure File Transfer Protocol (SFTP), etc.

Se hace referencia a los siguientes controles:

Tabla 28: *Controles hace referencia los Procedimientos de transferencia de información.*

Ítem	Sección	Descripción	Observaciones
	9.2	Transferencia de información	
75	9.2.1	Separación en las redes	Política de gestión y transferencia de la información
76	9.2.2	Acuerdos de transferencia de información	Política de gestión y transferencia de la información

Nota. Adaptado de Esquema Gubernamental de Seguridad de la Información (EGSI) Versión 2.0 (p. 87), por MINTEL, 2020.

16) Procedimientos para la seguridad de los sistemas de información

Procedimientos orientados a normar la seguridad digital como parte integral de los sistemas de información de cada una de las instituciones durante el ciclo de vida del activo de información o vigencia tecnológica de la arquitectura TI.

17) Procedimientos para la seguridad en el desarrollo y en los procesos de soporte

Procedimientos que permiten orientar a los funcionarios responsables de las TI de cada institución a asegurar, que la seguridad digital esté diseñada y sea implementada en el ciclo de vida de planeación y desarrollo de los sistemas de información.

18) Procedimiento para el uso y manejo de datos personales

Se establecerán los procedimientos necesarios que operacionalicen el cumplimiento de la Ley Orgánica de Protección de Datos Personales, publicada en el Registro Oficial – quinto suplemento Nro. 459 de 26 de mayo de 2021.

19) Procedimientos de seguridad en la relación con los proveedores

Estas normativas establecen los requisitos indispensables para brindar servicios, además de las obligaciones y medidas de seguridad diseñadas para salvaguardar tanto los datos como la estructura tecnológica de cada entidad. Su finalidad es resguardar contra potenciales riesgos como interceptaciones, reproducciones no autorizadas, alteraciones, revelaciones inapropiadas y daños que puedan comprometer los principios esenciales de integridad,

disponibilidad y confidencialidad de la información, así como la continuidad de la infraestructura tecnológica.

20) Procedimientos para la gestión de incidentes de seguridad de la información

Procedimiento que permitan garantizar una recuperación adecuada de los servicios tecnológicos de cada institución, de la posibilidad de un incidente que interrumpa la operación normal de la infraestructura digital por un corto período o por eventos catastróficos o ataques informáticos que impidan la continuidad de los servicios digitales.

Permite normar los componentes generales de la gestión de incidentes, sus principales acciones, aplicabilidad, acciones sobre tipo o activos de información sobre el cual se presente y/o exista un indicio de incidente de seguridad.

21) Procedimientos de seguridad de la información para la gestión de la continuidad

Procedimientos orientados a asegurar que todos los aspectos relacionados con la seguridad de la información y la arquitectura de la infraestructura TI se incluyan en los planes de continuidad.

22) Procedimientos de cumplimiento de los requisitos legales y contractuales

Con el propósito de garantizar y cumplir con las responsabilidades legales, estatutarias, normativas, o contractuales relacionadas con la protección de la información y la infraestructura tecnológica, así como con cualquier requisito de seguridad establecido por cada entidad, es fundamental llevar a cabo revisiones y actualizaciones de manera regular. Estas acciones deben

realizarse al menos una vez al año, e incluir la implementación de procedimientos específicos.

e. Plan de continuidad de TI.

Definir un plan que permita recuperar los servicios tecnológicos de cada una de las Instituciones ante la posibilidad de un incidente que interrumpa la operación normal de la infraestructura digital por un corto período o por eventos catastróficos o ataques informáticos que impidan la continuidad de los servicios digitales.

V. Capítulo 5 del Programa de Ciberseguridad

1. Cumplimiento

a. Supervisión e inspecciones

El MIDENA a través de un enfoque estratégico buscará implementar y lograr una alineación e integración de los requisitos de inspección y supervisión de los componentes y el comando de los programas tradicionales de seguridad (información, personal, físico e industrial) y ciberseguridad con el fin de identificar las tendencias de cumplimiento que presentan un riesgo de ciberseguridad inaceptable o resultan en un uso ineficiente de los recursos. Esto se logrará mediante la aplicación de las siguientes acciones claves:

- Recopilación de datos a través de procesos automatizados, siempre que sea posible, con el fin de limitar la interrupción de las actividades de la organización de la que se requiere la información y apoyar los objetivos de monitoreo continuo.
- Realizar evaluaciones de vulnerabilidad, evaluaciones de intrusión, pruebas de penetración y otras actividades aplicables (utilizando capacidades internas o externas) para proporcionar una visión sistémica de la postura actual de riesgo de TI.
- Aprovechar los datos recopilados por las inspecciones, auditorías, investigaciones y evaluaciones de programas existentes siempre que sea práctico, para informar el cumplimiento y las evaluaciones de riesgos.
- Las actividades del MIDENA compartirán los resultados de la evaluación aplicable con el COCIBER, para tomar las medidas apropiadas para resolver problemas sistémicos y mitigar riesgos. El propósito de compartir

estos resultados no es apoyar medidas punitivas u otras medidas negativas, sino identificar y resolver problemas sistémicos y mitigar los riesgos.

b. Requisitos de reporte de cumplimiento de normas

Todas las Instituciones informarán sobre el estado de las métricas de ciberseguridad, para garantizar que el liderazgo tenga información útil y actualizada sobre el nivel de rendimiento y las brechas existentes en la postura de ciberseguridad.

1) Evaluaciones de impacto sobre la privacidad.

Se llevará a cabo una evaluación del impacto en la privacidad de los instrumentos de recopilación de datos que recopilan, mantienen, usan y/o difunden en forma electrónica sobre miembros del público, con el fin de evaluar si la información se recopila, almacena o difunde de una manera que proteja la privacidad de las personas y su información.

a) Preparación para la ciberseguridad.

Las autoridades enfatizarán la importancia de la disciplina de ciberseguridad dentro de sus organizaciones, y asegurarán que en su programa institucional se evalúe la preparación y el cumplimiento de la ciberseguridad frente a la política y orientación de gestión de riesgos. Las evaluaciones de preparación para la ciberseguridad se incluirán en los informes de estado de las instituciones en todos los niveles.

b) Problemas sistémicos o críticos de ciberseguridad.

Los problemas sistémicos o críticos relacionados con la ciberseguridad se informarán y atenderán a través del COCIBER.

c) Eventos cibernéticos.

Informe de incidentes sospechosos o confirmados de acuerdo con las regulaciones del MIDENA.

3.2 Plan de Auditoria

A. Antecedentes

La seguridad de la información se evalúa a través de la auditoría interna, la cual representa un elemento fundamental en un SGSI. Este sistema requiere principalmente una planificación adecuada y que los auditores sean independientes.

El proceso de verificación debe manejar el requisito de independencia. Por ello, tal proceso lo realizará el OSI de cada una de las instituciones del sector defensa, de acuerdo a su nivel.

B. Descripción General del Plan

1. Alcance

El presente plan se ha desarrollado para dar seguimiento a la implementación de los catorce dominios (14) y los ciento veinte y siete (127) controles (dentro de lo aplicable en cada nivel) del ESQUEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL MIDENA (EGSI v2.0) que se remite mediante Acuerdo Ministerial N.º 134 del 30 de marzo de 2020.

2. Importancia

Mediante la ejecución de este plan se podrán establecer diagnósticos y métricas para determinar la madurez de la implementación del EGSI v2.0 y el estado actual de cumplimiento en las instituciones del sector defensa. Además, se podrán establecer un conjunto de directrices prioritarias que permitirán la mejora continua en la Gestión de la Seguridad de la Información.

C. Objetivos

1. Objetivo general

Realizar una evaluación interna de cumplimiento para valorar sistemáticamente la implementación de los controles del EGSI (v2.0), acorde a la normativa emitida por el MINTEL y expedido a través del Acuerdo ministerial No. 025-2019.

2. Objetivos específicos

- a. Evaluar el nivel de implementación del EGSI v2.0 en las entidades pertenecientes al sector Defensa.
- b. Determinar el estado de cumplimiento de la normativa vigente por parte de los usuarios finales con respecto a la seguridad de la información y así diagnosticar la postura de los usuarios frente a la cultura de ciberseguridad.
- c. Orientar la mejora continua en la implementación del EGSI v2.0 dentro de cada una de las instituciones del sector defensa.

D. Situación Actual

El MIDENA expidió la directiva para la implementación del EGSI v2.0, el mismo que se constituye en la norma vigente para la implementación de mencionado cuerpo normativo en vigencia.

En todas las instituciones del sector defensa ha sido dispuesto la implementación del EGSI v2.0 y han sido nombrados los OSI, quienes son los responsables del seguimiento de la implementación.

Si bien en las unidades existen limitaciones en recursos para la implementación de controles técnicos, el alcance de la implementación se ha dado por los controles organizacionales y el cumplimiento de la normativa, las mejores prácticas y las recomendaciones que apuntan a mantener la CID de la información que es generada, editada, transportada, almacenada, procesada y empleada por los procesos de las entidades del sector defensa.

E. Metodología

El MIDENA, para el cumplimiento de la implementación del EGSI v2.0 dentro de las entidades del sector de la defensa utiliza la metodología de la “Mejora Continua” o ciclo de Deming, conocido como el círculo PDCA, por sus siglas en inglés (Plan-Do-Check-Act).

Para obtener los resultados de la evaluación interna de cumplimiento del EGSI v2.0, se seguirán una serie de pasos que permitirán observar con claridad y orden cada uno de los controles implementados y analizar la forma en la cual han sido efectuados.

La evaluación se dividirá en dos fases. En la primera fase se evaluará al Comando Conjunto de las Fuerzas Armadas y a las Fuerza Terrestre, Naval y Aérea. Esta evaluación estará a cargo de un equipo conformado por el Comando de Ciberdefensa (COCIBER) y el OSI del MIDENA. La segunda fase constituirá la evaluación a las entidades adscritas por parte de los OSI de las mismas entidades y personal del COCIBER.

Se procederá de la manera y orden que se especifica a continuación:

1. Los pasos a seguir en la primera fase serán los siguientes:
 - a. Planificación del COCIBER, elaboración de cronogramas.
 - b. Difusión de tablas, listas de chequeo y material para la evaluación.
 - c. Inicio de visitas a las entidades a ser evaluadas de acuerdo a cronograma.
 - d. Arribo del equipo del COCIBER y del OSI del MIDENA.
 - e. Entrevista con el OSI de las instituciones.
 - f. Análisis de la información emitida por el OSI de las instituciones.
 - g. Verificación de documentos recibidos relacionados con seguridad de la información.
 - h. Revisión y análisis de Información generada: políticas, normativas, procedimientos, mejores prácticas y otros.
 - i. Verificación de la apropiada difusión de documentos normativos y sobre recomendaciones de seguridad de la información.

- j. Verificación de la implementación y cumplimiento de controles organizacionales.
 - k. Verificación de la implementación y cumplimiento de controles técnicos.
 - l. Verificación de limitaciones para la implementación de controles.
 - m. Verificación de indicadores y métricas de seguridad de la información.
 - n. Inspección de Instalaciones (redes, data center, seguridad física y otros relacionados).
 - o. Orientación para auditoría a las instituciones del sector defensa.
 - p. Aplicación de encuesta para determinar cultura de ciberseguridad en el personal de usuarios.
 - q. Charla magistral de concienciación (por parte del jefe del equipo de auditoría del COCIBER).
 - r. Obtención de resultados.
 - s. Elaboración de Informe final.
2. Los pasos a seguir en la segunda fase serán los siguientes:
- a. Planificación con base en el presente plan para la evaluación a las entidades adscritas al MIDENA en la que se incluya al OSI de las Fuerzas Terrestre, Naval y Aérea para la evaluación a estas entidades adscritas.
 - b. Envío de la planificación a la Subsecretaría de Defensa para registro y control de cumplimiento.

- c. Se visitará las entidades adscritas en las cuales se llevará a cabo los pasos similares realizados en los niveles Comando Conjunto y Fuerzas.
- d. Entrevista con el OSI de las entidades adscritas.
- e. Análisis de la información emitida por el OSI de cada entidad.
- f. Verificación de documentos recibidos relacionados con seguridad de la información.
- g. Revisión y análisis de Información generada: políticas, normativas, procedimientos, mejores prácticas y otros.
- h. Verificación de la apropiada difusión de documentos normativos y sobre recomendaciones de seguridad de la información.
- i. Verificación de la implementación y cumplimiento de controles organizacionales.
- j. Verificación de la implementación y cumplimiento de controles técnicos.
- k. Verificación de limitaciones para la implementación de controles.
- l. Verificación de indicadores y métricas de seguridad de la información.
- m. Inspección de instalaciones.
- n. Aplicación de encuesta para determinar cultura de ciberseguridad en el personal de usuarios.
- o. Obtención de resultados.

- p. Elaboración de Informe final.
- q. Envío del informe final a la Subsecretaría de Defensa Nacional.

F. Criterios de la Evaluación

Cada organización (entidad o dependencia) evaluada será valorizada según su efectividad en cada uno de los controles, de acuerdo con lo implementado según los parámetros de la tabla a continuación:

Tabla 29: *Criterios de evaluación para las auditorías.*

Efectividad	Descripción del hallazgo	Valoración
0%	No cumple, no se hace: carencia completa de un proceso/control reconocible, no se ha identificado ni reconocido que existe un problema a resolver.	No Conformidad Mayor
10%	Se reconoce la importancia de esta práctica por lo que se desarrollan y documentan algunas actividades y/o proceso alrededor de la misma. No existen plantillas definidas a nivel corporativo.	
50%	Se desarrollan actividades y/o procesos, sin embargo, no han sido documentadas, ni hay entrenamiento, ni comunicación formal de la misma. Se deja la responsabilidad a cada funcionario	No Conformidad Menor
90%	Esta práctica se ha estandarizado, documentado y ha sido difundida mediante entrenamiento: Toda la institución participa en el proceso.	Oportunidad de Mejora

	Esta práctica se monitorea y mide su cumplimiento. Se	
95%	toman medidas cuando los procesos y/o actividades no están logrando su objetivo, requiere mejoras.	
100%	Los procesos están bajo constante mejora (se han redefinido al nivel de mejor practica). Existen evidencia de la mejora continua.	Conforme

Nota. Fuente: El autor

G. Cronograma Tentativo para Evaluación en los Diferentes Niveles:

El plan de auditoria consta de dos fases de desarrollo, para la verificación y cumplimiento de las instituciones del sector Defensa.

La primera fase será ejecutada y aplicada a las siguientes instituciones:

- Comando Conjunto de las Fuerzas Armadas
- Fuerza Terrestre
- Fuerza Naval
- Fuerza Aérea

La segunda fase será ejecutada y aplicada a las entidades adscritas al sector defensa, de acuerdo al siguiente detalle:

- Instituto Geográfico Militar
- Instituto Oceanográfico y Antártico de la Armada del Ecuador
- Instituto de Seguridad Social de Fuerzas Armadas

1. Cronograma para la primera fase

Tabla 30: *Cronograma primera fase.*

ORD.	UNIDAD	RESPONSABLE	FECHA INICIO	FECHA TERMINA
01	Comando Conjunto	Comando de Ciberdefensa	01-10-2024	03-10-2024
02	Fuerza Terrestre	Comando de Ciberdefensa	21-10-2024	25-10-2024
03	Fuerza Naval	Comando de Ciberdefensa	04-11-2024	08-11-2024
04	Fuerza Aérea	Comando de Ciberdefensa	11-11-2024	15-11-2024

Nota. Fuente: El autor

2. Cronograma base dentro del que se enmarcará la segunda fase de acuerdo a la planificación de cada unidad.

Tabla 31: *Cronograma segunda fase.*

ORD.	UNIDAD	RESPONSABLE	INICIA	TERMINA
01	Instituto Geográfico Militar	Comando de Ciberdefensa	18-11-2024	22-11-2024
02	Instituto Oceanográfico y Antártico de la Armada del Ecuador	Comando de Ciberdefensa	02-12-2024	06-12-2024
03	Instituto de Seguridad Social de FF.AA.	Comando de Ciberdefensa	16-12-2024	20-12-2024

Nota. Fuente: El autor

H. Equipo para la Evaluación

El COCIBER, a través del Grupo de Defensa, conformará un equipo para la evaluación de seguridad de la información. El equipo estará conformado por 03

técnicos con conocimiento de la norma ISO 27000, seguridad informática, estandarización en TI y procedimientos del OSI.

Con la orientación que se emita en la primera fase de la evaluación al CC.FF.AA y a las Fuerzas, los OSI conformarán sus equipos para las visitas a las unidades adscritas bajo los mismos criterios de selección.

I. Normas, Estándares o Políticas Relacionadas

1. Esquema Gubernamental de Seguridad de la Información v2.0.
2. Norma ISO 27001.

J. Derogatoria

Este plan deroga a anteriores emitidos con relación al cumplimiento de implementación.

K. Vigencia

El presente plan entra en vigencia a partir de la fecha de su legalización y de su ejecución y cumplimiento deberán encargarse a las entidades involucradas y sus correspondientes autoridades.

L. Versión e Historial

1. Versión actual

El Plan de Auditoria se encuentra en su versión 1.0, expedida en la fecha constante en el presente documento.

2. Versiones anteriores

Tabla 32: *Versión e historial.*

Versión	Fecha Expedición	Fecha de Derogación	Reemplazada por Versión	Responsable
N/A	N/A	N/A	v 1.0	OSI

Nota. Fuente: El autor

4 Capítulo IV. Conclusiones

En conclusión, el presente trabajo de investigación ha logrado implementar un programa de ciberseguridad efectivo en el Ministerio de Defensa Nacional del Ecuador, que establece políticas y normas para enfocar el cumplimiento del EGSI v2.0 en todo el sector Defensa.

El programa de ciberseguridad diseñado y propuesto en este trabajo permitirá promover las mejores prácticas de seguridad de la información en la elaboración del programa, cumpliendo con los hitos establecidos en el EGSI v2.0. Esto se ha sustentado mediante la identificación de los riesgos y vulnerabilidades en la gestión de la información en el MIDENA, y la implementación de medidas de seguridad efectivas para mitigarlos.

La emisión de políticas, normas y la creación de un plan de auditoría constituyen pasos fundamentales para la operacionalización del programa de ciberseguridad. Estas acciones no solo establecen un marco regulatorio claro y preciso, sino que también brindan los instrumentos necesarios para supervisar y evaluar de manera continua la eficacia del programa, detectar oportunidades de mejora y asegurar el cumplimiento sostenido del EGSI v2.0 en el ámbito de la Defensa.

5 Capítulo V: Recomendaciones

Implementar un programa de capacitación continua en ciberseguridad para todos los empleados del MIDENA. Esto incluiría sesiones de concientización sobre buenas prácticas de seguridad, entrenamiento técnico para personal de TI y formación especializada para equipos responsables de la gestión de la seguridad de la información.

Establecer un proceso de revisión y actualización periódica del programa de ciberseguridad para garantizar que esté alineado con los cambios en las amenazas cibernéticas, las tecnologías emergentes y las regulaciones gubernamentales. Esto podría incluir la realización de evaluaciones de riesgos regulares y la incorporación de nuevas medidas de seguridad según sea necesario.

Definir métricas claras y medibles para evaluar el desempeño del programa de ciberseguridad y su impacto en la protección de los activos de información del Ministerio de Defensa Nacional. Estas métricas podrían incluir indicadores de cumplimiento, tasas de detección y respuesta a incidentes, tiempo de recuperación ante ataques, entre otros.

Promover la colaboración y el intercambio de información en materia de ciberseguridad con otras instituciones gubernamentales, organismos de seguridad y entidades del sector privado. Esto permitirá una mejor comprensión de las amenazas cibernéticas a nivel nacional y facilitará la adopción de enfoques coordinados para abordar los desafíos de seguridad compartidos.

Continuar invirtiendo en tecnologías y herramientas de seguridad de última generación que fortalezcan la postura de seguridad del Ministerio de Defensa Nacional. Esto podría incluir soluciones de detección y prevención de intrusiones, sistemas de gestión de eventos de seguridad, herramientas de análisis forense digital, entre otras.

Elaborar un plan de respuesta a incidentes detallado que establezca los procedimientos a seguir en caso de que ocurra un incidente de seguridad cibernética. Este

plan debería incluir roles y responsabilidades claras, protocolos de comunicación, acciones de mitigación y procesos de aprendizaje posterior al incidente para mejorar la resiliencia de la organización.

Realizar auditorías externas e independientes periódicas para evaluar la efectividad del programa de ciberseguridad y garantizar el cumplimiento de los estándares y regulaciones pertinentes. Estas auditorías pueden proporcionar una perspectiva objetiva y ayudar a identificar áreas de mejora para fortalecer aún más la seguridad de la información del MIDENA.

Bibliografía

- Aguilera, O., Pérez, E., & Rivero, R. (2017). La protección de la información. Una visión desde las entidades educativas cubanas. *Ciencias de la Información*., 48(3), 41-47. <https://cinfo.idict.cu/index.php/cinfo/article/view/129>
- Ascencio, D. (2021). Políticas de Seguridad para la protección de la información e infraestructura en la unidad informática de la UNESUM. *Repositorio digital UNESUM*. <http://repositorio.unesum.edu.ec/handle/53000/2812>
- Baldeón, M., & Coronel, C. (2015). Plan Maestro de seguridad informática para la UTIC de la ESPE con lineamientos de la norma ISO/IEC 27002. *Repositorio espe.edu.ec*. <https://repositorio.espe.edu.ec/bitstream/21000/6026/1/AC-GS-ESPE-034491.pdf>
- Balseca, J., & Ledezma, D. (2015). Desarrollo de políticas de seguridad de la información basadas en las normas ISO 27002 para una coordinación zonal del INEC. *Tesis (Magister en Gerencia Informática) - Pontificia Universidad Católica del Ecuador, Departamento de Investigación y Posgrados*. <http://repositorio.pucesa.edu.ec/handle/123456789/1555>
- Barranco, J. (2001). *Metodología del análisis estructurado de sistemas*. Madrid.
- Bustillos, O., & Rojas, J. (julio de 2023). Cómo promueven los Estados la Ciberseguridad de las Pymes. *Revista de la Carrera de Ingeniería de Sistemas*, 21-37. <https://doi.org/> <https://doi.org/10.26439/interfases2023.n017.6246>
- Castillo, C. (02 de junio de 2018). Ciberseguridad: Por dónde Empezar. *Revista de Tecnología*, 18(01), 1-12. <https://revistas.unbosque.edu.co/index.php/RevTec/issue/view/404>

Chambi, L. (2021). Estrategias para evitar ataques de Phishing en Empresas. *Revista PGI: Investigación, Ciencia y Tecnología en Informática.*, 65-68.

https://ojs.umsa.bo/ojs/index.php/inf_fcpn_pgi/article/view/110

Esparza, R. (04 de diciembre de 2023). Marco de Trabajo de Buenas Prácticas de Ciberseguridad en el teletrabajo para las empresas de desarrollo de software basado en los controles establecidos en la norma ISO 27002:2022 y la NIST SP 800-46. *Repositorio Digital Universidad Técnica del Norte.*

<http://repositorio.utn.edu.ec/handle/123456789/15305>

Espinosa , M., & Carmina, C. (30 de julio de 2011). Geoetiquetación: Los riesgos de hacer pública tu ubicación. *Repositorio Universitario de la DGTIC.*

<http://revista.seguridad.unam.mx/numero-11/geoetiquetación-los-riesgos-de-hacer-pública-tu-ubicación>

Gallardo, I. (2015). Ataques Informáticos Basados en la Integridad de la Información. *Salud y Administración*, 2(05), 43-50.

<https://revista.unsis.edu.mx/index.php/saludyadmon/article/view/66/63>

Gómez, Á. (28 de junio de 2019). Diseño de un Programa de Ciberseguridad de una empresa basado en el marco de trabajo NIST.

<http://creativecommons.org/licenses/by-nc-nd/3.0/es/>

Guamán, M., Carrillo, J., Flores, C., Flores, C., & Ron, M. (septiembre de 2023).

Análisis de riesgos y amenazas de ciberseguridad en el estado ecuatoriano, utilizando la metodología Magerit. *ProSciences*, 7(49).

<https://doi.org/https://doi.org/10.29018/issn.2588-1000vol7iss49.2023pp139-165>

- Guevara, D. (2022). Gestión estratégica del programa de ciberseguridad y su impacto en la postura de seguridad digital de Centria, en el año 2020. *Repositorio Universidad Tecnológica del Perú*. <https://hdl.handle.net/20.500.12867/5974>
- Huapaya, D. (2022). Aportes para la política exterior peruana en materia de amenazas híbridas en el ciberespacio. *Academia Diplomática del Perú Javier Pérez de Cuéllar*. <http://repositorio.adp.edu.peADP/209>
- Hurtado, M. (15 de 05 de 2018). Gestión de riesgo, metodologías Octave y Magerit. *Universidad Piloto de Colombia*. <http://repository.unipiloto.edu.co/handle/20.500.12277/2965>
- Mancilla, D. (26 de febrero de 2021). Implementación de Programas de cumplimiento en Ciberseguridad como una práctica de buen Gobierno Corporativo en las entidades que forman parte del sistema financiero peruano. *Repositorio de Tesis PUCP*. <http://hdl.handle.net/20.500.12404/18475>
- Mantari Pacheco, V. A. (2022). Implementación de un Programa de Ciberseguridad para la prevención de ciberataques en el área de centro de operaciones de seguridad en la empresa VMWARESIS S.A.C. Lima, Perú.
- Marin, A., & Santa María, E. (2022). El ciberdelito de redes delictivas a escala global a entidades gubernamentales y la responsabilidad del organo de control interno en un municipalidad de la región de Ucayali, año 2020. *Repositorio de la Universidad Nacional de Ucayali*. <http://repositorio.unu.edu.pe/handle/UNU/5184>

MIDENA. (2018). *Política de la Defensa Nacional del Ecuador "Libro Blanco"*. Quito.

<https://www.defensa.gob.ec/wp-content/uploads/2019/01/Política-de-Defensa-Nacional-Libro-Blanco-2018-web.pdf>

MINTEL. (10 de enero de 2020). Acuerdo Ministerial N.º 025-2019. Quito.

<https://n9.cl/tjp9m1>

MINTEL. (2020). *Guía para la Gestión de Riesgos de Seguridad de la Información*.

[chromhttps://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](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)

Mora, J. (2021). Propuesta metodológica para la gestión de la seguridad de la

información alineada a la norma ISO 27001 y ciberseguridad.

<https://repositorio.puce.edu.ec/handle/123456789/27410>

Muyón, C., Guarda, T., Vargas, G., & Ninahualpa, G. (febrero de 2019). Esquema

Gubernamental de Seguridad de la Información EGSI y su aplicación en las entidades públicas del Ecuador. *Revista Ibérica de Sistemas e Tecnologías de Informação*, 310-317.

<https://www.proquest.com/openview/f4b193b46ccb16a251428b15a52d084a/1?pq-origsite=gscholar&cbl=1006393>

Niño, M. (27 de noviembre de 2019). Modelo de un sistema de gestión de seguridad de

Información - SGSI, para fortalecer la Confidencialidad, Integridad,

Disponibilidad y Monitorear los activos de información para el Instituto

Nacional de Estadística e Informática - INEI Filial Lambayeque. *Repositorio Institucional UNPRG*. <https://hdl.handle.net/20.500.12893/5935>

Oñate, A. (03 de agosto de 2021). Propuesta de Políticas de Seguridad de la Información para proteger los activos de información en las organizaciones. *[Monografía]. Repositorio Institucional UNAD*. .
<https://repository.unad.edu.co/handle/10596/41984>

Ospina, M., & Sanabria, P. (2020). Desafíos Nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Revista Criminalidad*, 62(2).
<https://doi.org/https://doi.org/10.47741/17943108.168>

Otálora, N. (2023). Recomendaciones basadas en las mejores prácticas para la gestión de riesgos de ciberseguridad a nivel de gobernanza en las organizaciones empresariales. *Repositorio Institucional Universidad Militar Nueva Granada*.
<http://hdl.handle.net/10654/45839>

Pinto, A. (01 de abril de 2019). Análisis y Planteamiento de Políticas de acuerdo al Esquema Gubernamental de Seguridad de la Información (EGSI) para la Empresa Pública Yachay. *Tesis de pregrado, Universidad Técnica del Norte*.
<http://repositorio.utn.edu.ec/handle/123456789/9001>

Ramírez, E., & Rincone, M. (07 de abril de 2022). La importancia de la seguridad de la información en el sector público en Colombia. *Revista Ibérica de Sistemas e Tecnologías de Informação*. <https://doi.org/10.17013/risti.46.87-99>

Reyna, A. (2023). Sistema de gestión de seguridad de la información para mejorar la gestión del riesgo informático de clínica San Pedro Chimbote. *Repositorio Institucional - UNITRU*. <https://hdl.handle.net/20.500.14414/19799>

- Ricart, R. (enero de 2023). El nexo entre la ciberseguridad y el primer ciclo de monitoreo del programa para la década digital de la Unión Europea. *Empresa Seguridad y Sociedad Digital*. <https://n9.cl/3ritx>
- Riveros, E. (02 de febrero de 2016). ¿El concepto de seguridad de la información aplica para las PYMES?. *Repositorio Universidad Piloto de Colombia*. <http://repository.unipiloto.edu.co/handle/20.500.12277/2757>
- Rodriguez, J. J. (20 de 04 de 2023). Propuesta de un modelo de mejora continua para la gestión de riesgos de la seguridad de la información a una institución educativa privada mediante el ciclo CAP-DO. *Repositorio Universidad Estatal Península de Santa Elena*. <https://repositorio.upse.edu.ec/handle/46000/9273>
- Salinas, A. (2022). Modelo de Ciberseguridad para cajas municipales en tiempos de Transformación Digital - un nuevo enfoque. *Repositorio de la Universidad Privada del Norte*. <https://hdl.handle.net/11537/29733>
- Torres, L., Martínez, A., Jaén, A., & Hermosilla, J. (2022). La percepción del profesorado de la Universidad Pablo de Olavide sobre su Competencia Digital Docente. *Pixel - Bit Revista de Medios y Educación*.(63). <https://doi.org/https://doi.org/10.12795/pixelbit.91943>