COLOMBIA POTENCIA DE LA VIDA

Defensa

SGSI Unidad Gestión General

Agenda

COLOMBIA POTENCIA DE LA VIDA

Defensa

CONTEXTO

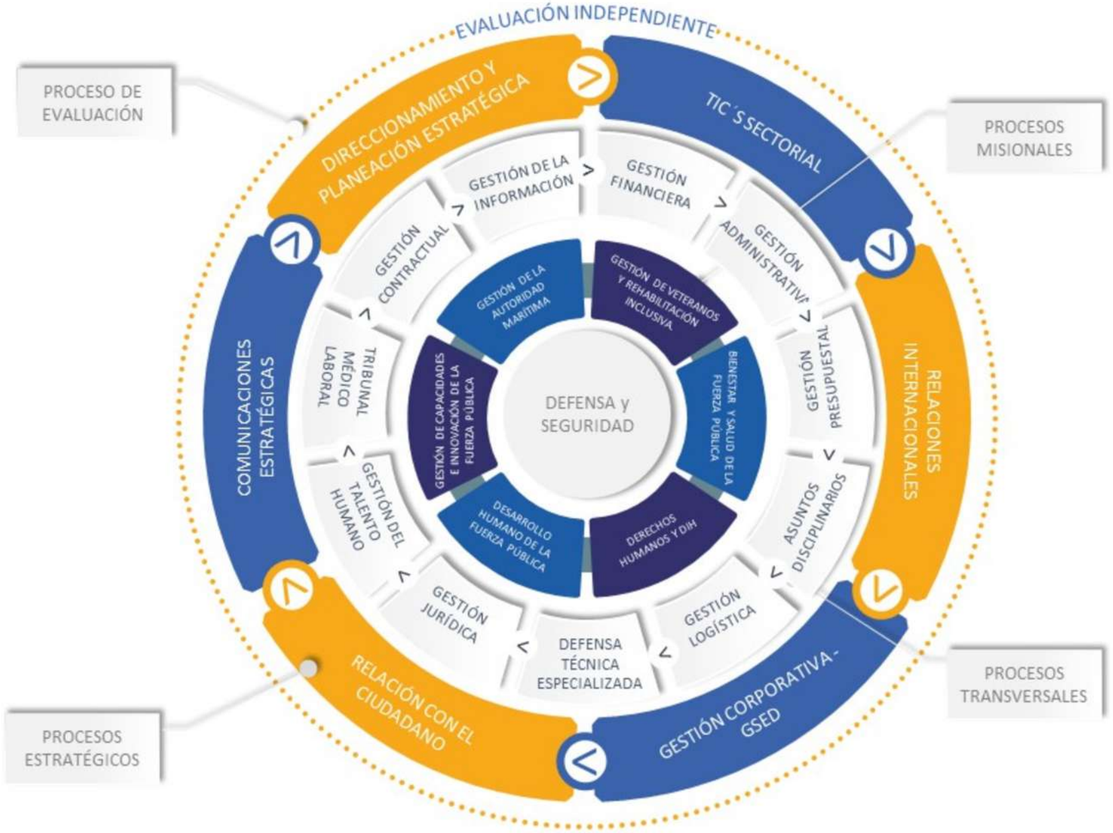
Unidad Gestión General MDN

Misión

La Unidad Gestión General diseña, formula, gestiona y dirige las políticas públicas de seguridad y defensa nacional, se encarga del direccionamiento estratégico de la Fuerza Pública, y provee los medios asociados para el cumplimiento de su misión, bajo el liderazgo del Presidente de la República.

Fuente: MDN

Procesos



COLOMBIA POTENCIA DE LA VIDA

Defensa

Justificación

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001:2022 permitirá a la UGG establecer un marco estructurado para gestionar los riesgos asociados a la seguridad de la información y garantizar el cumplimiento de las regulaciones nacionales e internacionales.

MARCO NORMATIVO

SGSI Unidad Gestión General MDN

Marco Normativo

Para la implementación del SGSI en la UGG, se consideran los siguientes marcos normativos y estándares internacionales:

01 ISO/IEC 27001:2022 - Establece los requisitos para la implementación y mantenimiento de un SGSI.

02 ISO/IEC 27002:2022 - Proporciona directrices para la aplicación de controles de seguridad.

03 ISO/IEC 27005:2022 - Especifica directrices para la gestión de riesgos de seguridad de la información.

04 ISO/IEC 27035:2022 - Define principios y procesos para la gestión de incidentes de seguridad.

05 NIST Cybersecurity Framework - Referencia para la gestión de ciberseguridad en infraestructuras críticas.

06 Ley 1712 del 6 de marzo del 2014 (Artículos 13, 18, 19 y 20) “Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones”.

POLÍTICA

SGSI Unidad Gestión General MDN

Política

La UGG, entendiendo la importancia sobre la gestión de la información, se compromete con la implementación de un Sistema de Gestión de Seguridad de la Información buscando establecer confianza en el ejercicio de sus funciones y la prestación de trámites y servicios con sus grupos de interés. Lo anterior enmarcado en el cumplimiento de la normatividad vigente y alineado con la misión y visión institucional. Por tal motivo, adopta su Política de Seguridad y Privacidad de la Información con el fin de velar por la protección, confidencialidad, integridad y disponibilidad de los activos de información (procesos, hardware, software, infraestructura, información, funcionarios, contratistas, terceros) que soportan los procesos de la entidad, mediante la implementación de lineamientos, procedimientos y la asignación de responsabilidades, los cuales están orientados a mitigar los riesgos y prevenir incidentes de seguridad dentro de un proceso de mejora continua.

COLOMBIA POTENCIA DE LA VIDA

ALCANCE

SGSI Unidad Gestión General MDN

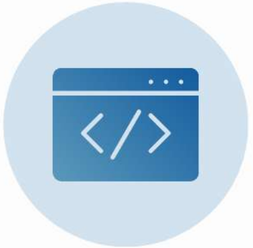
Alcance

Esta política es transversal a todos los procesos y procedimientos institucionales de la Unidad Gestíon General del MDN. Aplica a todos los usuarios internos y externos de la Unidad Gestíon General (servidores públicos, funcionarios vinculados a la planta permanente y provisional, contratistas, consultores, pasantes, proveedores de bienes, entidades del Estado, entes de control) y otros terceros que desempeñen alguna actividad en las instalaciones de la UGG o a nombre de esta.

P.H.V.A.

SGSI Unidad Gestión General MDN

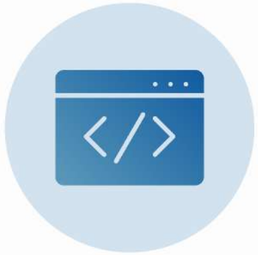
P.H.V.A.



Planear

Definir Alcance SGSI
Definir partes interesadas
Análisis de Riesgos
Definir Política de S.I.

Objetivos



Hacer

Puesta en marcha del SGSI
Implementación Controles
Capacitación y concientización en S.I.
Gestión Incidentes
Gestión Proveedores

Ejecución

Verificar

Auditorias Internas
Monitoreo y revisión Controles
PenTesting y simulacros

Monitoreo

Actuar

Gestión de N.C. y A.C.
Mejora Continua
Actualización Políticas

Mejora

COLOMBIA POTENCIA DE LA VIDA

Defensa

D.A.F.O.

SGSI Unidad Gestión General MDN

D.A.F.O.

D	Debilidades
1	Falta de digitalización integral en procesos de gestión documental y seguridad, dificultando la trazabilidad y cumplimiento normativo
2	Escasez de recursos humanos especializados en ciberseguridad y SGSI, debido a la alta demanda de expertos en el sector.
3	Baja automatización en la detección y respuesta a incidentes de seguridad, lo que incrementa el tiempo de respuesta ante ataques.
4	Desafíos en la gestión de proveedores tecnológicos y seguridad en la cadena de suministro, con necesidad de mejores auditorías y controles.
5	lo que puede afectar la implementación del SGSI y el cumplimiento de normativas como ISO 27001.
6	puede generar costos adicionales y afectar la sostenibilidad del sistema a largo

F	Fortalezas
1	Alta relevancia estratégica de la seguridad de la información dentro de la misión y objetivos de la UGG, lo que facilita la adopción del SGSI.
2	Respaldo normativo y marco legal sólido en seguridad y defensa, alineado con regulaciones nacionales e internacionales.
3	Experiencia en gestión de riesgos de seguridad y defensa, con procedimientos establecidos para la mitigación de amenazas.
4	Infraestructura tecnológica avanzada para el manejo de información clasificada y control de accesos.
5	Relación con organismos internacionales para compartir mejores prácticas y recibir asesoría técnica en la implementación de SGSI.
6	Capacidades en análisis de amenazas y ciberinteligencia, facilitando la detección temprana de riesgos.

A	Amenazas
1	Creciente sofisticación de ciberataques dirigidos a entidades gubernamentales, con aumento de ransomware, APTs (Advanced Persistent Threats) y campañas
2	Exposición a riesgos de seguridad en la cadena de suministro (proveedores de TI), con posibles vulnerabilidades en software y hardware crítico.
3	Riesgo de espionaje y filtraciones de información clasificada, con intentos de intrusión de actores estatales y no estatales.
4	Cambios políticos que pueden impactar el presupuesto para la implementación del SGSI, afectando la continuidad de programas de ciberseguridad.
5	Vulnerabilidades en infraestructuras críticas utilizadas para la seguridad nacional, lo que podría comprometer la protección de datos estratégicos.
6	Escasez global de talento en ciberseguridad, lo que dificulta la contratación y retención de expertos para el SGSI.

O	Oportunidades
1	Avances tecnológicos en ciberseguridad, como IA y machine learning para mejorar la detección de amenazas y automatización de respuestas.
2	Regulaciones y estándares internacionales (ISO 27001, NIST, CIS Controls) que fomentan la adopción de mejores prácticas y justifican la inversión en seguridad
3	Alianzas estratégicas con instituciones de defensa y organismos de inteligencia, facilitando el intercambio de información sobre amenazas y asistencia técnica.
4	Sensibilización creciente sobre ciberseguridad en el sector público y defensa, lo que genera un entorno favorable para la implementación del SGSI.
5	Oportunidad de fortalecer la resiliencia cibernética en la defensa nacional, aumentando la capacidad de respuesta ante ataques de alto impacto
6	Financiamiento internacional para proyectos de seguridad de la información, lo que puede facilitar la implementación del SGSI.

Estrategias Ofensivas

01 Aprovechar la infraestructura tecnológica y relaciones internacionales para fortalecer el intercambio de inteligencia sobre amenazas cibernéticas.

02 Implementar un programa de formación en ciberseguridad para personal clave, capitalizando los avances tecnológicos en IA y detección de amenazas.

03 Asegurar la alineación del SGSI con regulaciones internacionales (ISO 27001, NIST, CIS Controls) para posicionar a la UGG como un referente en seguridad gubernamental.

D.A.F.O.

D	Debilidades
1	Falta de digitalización integral en procesos de gestión documental y seguridad, dificultando la trazabilidad y cumplimiento normativo
2	Escasez de recursos humanos especializados en ciberseguridad y SGSI, debido a la alta demanda de expertos en el sector.
3	Baja automatización en la detección y respuesta a incidentes de seguridad, lo que incrementa el tiempo de respuesta ante ataques.
4	Desafíos en la gestión de proveedores tecnológicos y seguridad en la cadena de suministro, con necesidad de mejores auditorías y controles.
5	lo que puede afectar la implementación del SGSI y el cumplimiento de normativas como ISO 27001.
6	puede generar costos adicionales y afectar la sostenibilidad del sistema a largo

F	Fortalezas
1	Alta relevancia estratégica de la seguridad de la información dentro de la misión y objetivos de la UGG, lo que facilita la adopción del SGSI.
2	Respaldo normativo y marco legal sólido en seguridad y defensa, alineado con regulaciones nacionales e internacionales.
3	Experiencia en gestión de riesgos de seguridad y defensa, con procedimientos establecidos para la mitigación de amenazas.
4	Infraestructura tecnológica avanzada para el manejo de información clasificada y control de accesos.
5	Relación con organismos internacionales para compartir mejores prácticas y recibir asesoría técnica en la implementación de SGSI.
6	Capacidades en análisis de amenazas y ciberinteligencia, facilitando la detección temprana de riesgos.

A	Amenazas
1	Creciente sofisticación de ciberataques dirigidos a entidades gubernamentales, con aumento de ransomware, APTs (Advanced Persistent Threats) y campañas
2	Exposición a riesgos de seguridad en la cadena de suministro (proveedores de TI), con posibles vulnerabilidades en software y hardware crítico.
3	Riesgo de espionaje y filtraciones de información clasificada, con intentos de intrusión de actores estatales y no estatales.
4	Cambios políticos que pueden impactar el presupuesto para la implementación del SGSI, afectando la continuidad de programas de ciberseguridad.
5	Vulnerabilidades en infraestructuras críticas utilizadas para la seguridad nacional, lo que podría comprometer la protección de datos estratégicos.
6	Escasez global de talento en ciberseguridad, lo que dificulta la contratación y retención de expertos para el SGSI.

O	Oportunidades
1	Avances tecnológicos en ciberseguridad, como IA y machine learning para mejorar la detección de amenazas y automatización de respuestas.
2	Regulaciones y estándares internacionales (ISO 27001, NIST, CIS Controls) que fomentan la adopción de mejores prácticas y justifican la inversión en seguridad
3	Alianzas estratégicas con instituciones de defensa y organismos de inteligencia, facilitando el intercambio de información sobre amenazas y asistencia técnica.
4	Sensibilización creciente sobre ciberseguridad en el sector público y defensa, lo que genera un entorno favorable para la implementación del SGSI.
5	Oportunidad de fortalecer la resiliencia cibernética en la defensa nacional, aumentando la capacidad de respuesta ante ataques de alto impacto
6	Financiamiento internacional para proyectos de seguridad de la información, lo que puede facilitar la implementación del SGSI.

Estrategias Defensivas

01 Implementar mecanismos de detección temprana de amenazas, mediante la integración de inteligencia de amenazas y monitoreo continuo en la infraestructura tecnológica.

02 Diseñar un plan de respuesta ante incidentes robusto, alineado con marcos como ISO/IEC 27035 (gestión de incidentes de seguridad de la información).

03 Garantizar la seguridad de la información clasificada mediante el control estricto de accesos y auditorías periódicas, asegurando conformidad con ISO 27001.

R.A.C.I.

SGSI Unidad Gestión General MDN

En el marco de la implementación del SGSI para la Unidad de Gestión General (UGG) del Ministerio de Defensa (MDN) hemos definido:

1.Contexto de la organización.
Implementar un SGSI para proteger la información del sector defensa.

2.Liderazgo
Determinar el liderazgo del SGSI y de los niveles subsiguientes bajo la matriz RACI.

3.Planeación.
Definir los requerimientos, pasos y acciones para llevar a cabo cada fase para la implementación del SGSI

4.Evaluación de desempeño
Hacer seguimiento de las acciones implementadas en procura de la mejora continua.

R.A.C.I.

Actividad /Control	Alta Dirección (ministro)	Talento Humano	Jefe de Seguridad de la Información	Dirección Jurídica	Oficina de Control Interno Sectorial	Dirección de las Tecnologías y de las comunicaciones	Dirección de Planeación y Presupuesto
PLANEAR							
1. Definir el alcance del SGSI	A	C	C	C	I	I	R
2. Realizar el análisis de riesgos de seguridad de la información	I	I	A	C	I	C	R
3. Implementar controles de seguridad	I	I	A	I	C	R	C
HACER							
Definir y comunicar la Política de Seguridad de la Información	A	C	R	C	I	C	C
5. Capacitación y sensibilización en Seguridad de la Información	I	R	A	C	I	C	I
6. Establecer procedimientos de respuesta ante incidentes	I	I	A	I	I	R	C
VERIFICAR							
Realizar auditorías internas del SGSI (Cláusula 9.2 - ISO 27001)	A	I	I	I	R	I	C
Evaluar y mejorar continuamente el SGSI (Cláusula 10 - ISO 27001)	I	I	A	C	R	C	C
R: Responsable *Ejecuta la tarea*	A: Aprobador Tiene la autoridad Final		C: Consultado Brinda información y asesoría		I: Informado Recibe Actualizaciones		

COLOMBIA POTENCIA DE LA VIDA

Defensa

SOA

SGSI Unidad Gestión General MDN

S.o.A.

La Declaración de Aplicabilidad (SoA) es un documento vital para el SGSI que asegura que la organización seleccione y justifique adecuadamente los controles necesarios para mitigar los riesgos de seguridad de la información. Siguiendo estos pasos, se podrás realizar una SoA efectiva, alineada con los requisitos de la ISO/IEC 27001:2022 y la ISO/IEC 27002:2022, para proteger la información y los activos críticos de la organización.

Declaración de Aplicabilidad

01 **Controles organizacionales**: Políticas de seguridad, roles y responsabilidades, control de acceso.

02 **Controles tecnológicos**: Protección contra malware, gestión de vulnerabilidades, gestión de identidades.

03 **Controles físicos**: Seguridad de las instalaciones, control de acceso físico, protección contra desastres.

COLOMBIA POTENCIA DE LA VIDA

Defensa

GRACIAS

Lisa Barrios
Ana Catalina Cano
Jeison Melo
Ramiro Morales

Defensa