GRUPO 1

Bogotá 01 de Febrero 2025

Ana Catalina Cano
Jeison Stiven Melo
Lisa Barrios
Ramiro Morales

Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en la Unidad de Gestión General (UGG) basado en ISO/IEC 27001:2022

1. Introducción

1.1 Contexto de la UGG

La Unidad de Gestión General (UGG) tiene como misión diseñar, formular y gestionar políticas públicas en materia de seguridad y defensa, liderando el direccionamiento estratégico de la Fuerza Pública. En este contexto, la información que maneja es de alto valor estratégico y requiere una gestión segura y eficiente para garantizar su confidencialidad, integridad y disponibilidad.

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.

1.2 Objetivo del Documento

Este documento tiene como propósito describir la implementación del SGSI en la UGG conforme a ISO/IEC 27001:2022, incorporando ejemplos prácticos y alineándolo con los dominios clave de **ISO/IEC 27002:2022** para la gestión de controles de seguridad.

1.3 Marco Normativo

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

- **ISO/IEC 27001:2022** - Establece los requisitos para la implementación y mantenimiento de un SGSI.
- **ISO/IEC 27002:2022** - Proporciona directrices para la aplicación de controles de seguridad.
- **ISO/IEC 27005:2022** - Especifica directrices para la gestión de riesgos de seguridad de la información.
- **ISO/IEC 27035:2022** - Define principios y procesos para la gestión de incidentes de seguridad.
- **Reglamentos de Protección de Datos Personales** - Aplicables a la gestión de información clasificada y de carácter personal.
- **NIST Cybersecurity Framework** - Referencia para la gestión de ciberseguridad en infraestructuras críticas.
- 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”.
- Directiva permanente N°DIR2014-18 que trata sobre las “Políticas de seguridad de la información para el Sector Defensa”.

2. Pasos Estratégicos para la Implementación del SGSI en la UGG

2.1 Planificación del SGSI

2.1.1 Definir el Alcance del SGSI (Cláusula 4.3 de ISO 27001)

- Identificar las unidades organizacionales, procesos y sistemas de información críticos.
- La UGG decide incluir dentro del alcance del SGSI la gestión documental de información clasificada y los sistemas de comunicación de alto nivel.
- Se define que el SGSI cubra la seguridad de las redes internas utilizadas por las unidades estratégicas de la UGG, asegurando un perímetro protegido contra amenazas externas.
-

2.1.2 Identificación de Partes Interesadas (Cláusula 4.2)

- Identificar stakeholders como Fuerzas Armadas, Ministerio de Defensa, organismos de auditoría y proveedores de tecnología.
- Se establece un comité de gestión de la seguridad con representantes de cada unidad clave.
- Se identifican proveedores estratégicos que manejan información clasificada y se establecen requisitos de seguridad para su contratación y evaluación continua.

2.1.3 Evaluación de Riesgos y Oportunidades (Cláusula 6.1)

- Aplicar metodologías de análisis de riesgos como ISO/IEC 27005.
- Identificar amenazas, vulnerabilidades y evaluar el impacto.
- Se detecta un riesgo alto asociado a accesos no autorizados a bases de datos críticas.
- Se identifican vulnerabilidades en el acceso remoto de funcionarios autorizados y se propone la implementación de un sistema de VPN con autenticación multifactor.

2.1.4 Definir la Política de Seguridad de la Información (Cláusula 5.2)

- Desarrollar una política alineada con la misión de la UGG y los requisitos normativos.
- La política establece directrices estrictas de acceso y control de datos clasificados.

2.2 Implementación del SGSI (Do)

2.2.1 Implementación de Controles de Seguridad (Anexo A - ISO 27001 / ISO 27002)

- Aplicar controles organizacionales, físicos, tecnológicos y de personas.
- Se implementa autenticación multifactor para acceso a sistemas críticos.
- Se instalan sistemas de detección de intrusos (IDS/IPS) en la red interna para mitigar ataques dirigidos.

2.2.2 Capacitación y Concienciación en Seguridad (Cláusula 7.3)

- Programas de formación sobre amenazas, phishing, manejo seguro de información.
- Se realiza un taller de simulación de ataques de ingeniería social para empleados.
- Se desarrolla una campaña de concienciación sobre el uso seguro de dispositivos móviles en entornos gubernamentales.

2.2.3 Gestión de Incidentes de Seguridad (ISO/IEC 27035)

- Establecer procedimientos para identificar, responder y mitigar incidentes de seguridad.
- Se implementa un SOC (Security Operations Center) para monitorear eventos de seguridad en tiempo real.

2.3 Verificación y Evaluación

2.3.1 Auditorías Internas del SGSI (Cláusula 9.2)

- Definir un programa de auditorías internas periódicas.
- Se realizan auditorías cada seis meses para evaluar el cumplimiento de los controles.
- Se ejecutan auditorías sorpresa a los procedimientos de gestión de accesos en sistemas de información clasificada.

2.3.2 Monitoreo de la Seguridad (Cláusula 9.1)

- Implementar herramientas SIEM para correlación de eventos de seguridad.
- Se detectan intentos de acceso no autorizado mediante análisis de registros.

2.4 Mejora Continua del SGSI

2.4.1 Gestión de No Conformidades y Acciones Correctivas (Cláusula 10)

- Identificar desviaciones y tomar medidas correctivas y preventivas.
- Tras un incidente de seguridad, se refuerza la autenticación en redes internas.
- Se establece un programa de simulacros de incidentes de seguridad para evaluar la efectividad de la respuesta ante amenazas reales.

2.4.2 Actualización de Políticas y Procedimientos

- Revisar y actualizar la documentación del SGSI en función de nuevas amenazas y regulaciones.
- Se incorpora una nueva política de teletrabajo seguro tras la adopción de esquemas híbridos de trabajo.

3. Controles Clave de Seguridad Basados en ISO/IEC 27002:2022

3.1 Controles Organizacionales

- Políticas de seguridad y roles y responsabilidades.
- Se establece un comité de ciberseguridad con reuniones mensuales.

3.2 Controles de Personas

- Capacitación, gestión de accesos y conciencia en seguridad.
- Programa de formación en seguridad dirigido a empleados y terceros.

3.3 Controles Físicos

- Protección de infraestructuras, acceso a instalaciones y monitoreo.
- Implementación de controles biométricos para ingreso a áreas restringidas.

3.4 Controles Tecnológicos

- Seguridad en redes, cifrado, autenticación y protección contra malware.
- Implementación de firewalls de nueva generación con detección de anomalías basada en IA.

4. Conclusión

La implementación de un **SGSI en la UGG** basado en **ISO/IEC 27001:2022** es un paso clave para fortalecer la seguridad de la información en un entorno estratégico. Siguiendo el modelo **PHVA** y aplicando los controles de **ISO/IEC 27002:2022**, se garantiza una gestión estructurada de la seguridad, alineada con las mejores prácticas internacionales.

Este documento establece una **guía integral** para la implementación del SGSI en la UGG, asegurando la protección de la información crítica en el marco de la seguridad y defensa nacional.

5. Próximos Pasos

- Implementación de un plan de concienciación anual.
- Desarrollo de ejercicios de simulación de incidentes de seguridad.
- Revisión anual del SGSI para adaptarlo a nuevas amenazas y regulaciones.

Con estas acciones, la UGG fortalecerá su postura de seguridad y garantizará la protección de su información estratégica en el largo plazo.