Formato de Alcance del SGSI

1. Información General

Nombre de la organización:
Unidad de Gestión General (UGG)
Fecha de creación del SGSI:

Versión del documento:
1.0

2. Objetivo del SGSI

El objetivo del Sistema de Gestión de Seguridad de la Información (SGSI) es proteger la confidencialidad, integridad y disponibilidad de la información crítica de la **UGG** en el marco de las políticas públicas de seguridad y defensa. El SGSI garantizará la protección de la información a través de la implementación de controles efectivos para la gestión de los riesgos asociados a la seguridad de la información.

3. Definición del Alcance

3.1 Ámbito Geográfico
El alcance del SGSI abarca todas las instalaciones y oficinas físicas de la **UGG** involucradas en la seguridad y defensa nacional, incluyendo aquellas dependencias clave para el procesamiento y almacenamiento de información clasificada.

3.2 Departamentos y Unidades
El SGSI se implementará en las siguientes áreas clave dentro de la **UGG**:

- **Dirección General de Seguridad Informática**
- **Área de Análisis de Riesgos y Ciberdefensa**
- **Infraestructura Tecnológica y Comunicaciones Estratégicas**
- **Gestión de Proyectos Tecnológicos**
- **Centro de Operaciones de Seguridad (SOC)**

3.3 Activos Protegidos
El SGSI protegerá los siguientes activos de información:

- **Datos clasificados** (información sensible relacionada con la seguridad nacional).
- **Sistemas de comunicación estratégica** utilizados para la defensa y coordinación de las Fuerzas Armadas.
- **Bases de datos** relacionadas con la administración de personal de la Fuerza Pública y la infraestructura de defensa.
- **Equipos de tecnología de la información**, incluyendo servidores, dispositivos de red, estaciones de trabajo y otros equipos esenciales.
- **Documentación confidencial** asociada a políticas y operaciones de seguridad.

3.4 Exclusiones del Alcance El SGSI no aplicará a los siguientes elementos dentro de la organización:

- **Servicios externos de consultoría** que no están involucrados en el procesamiento de información clasificada.
- **Información no crítica** relacionada con operaciones administrativas generales que no comprometen la seguridad nacional o la defensa.

4. Definición de Riesgos y Amenazas

Se ha realizado un análisis de riesgos para identificar las amenazas y vulnerabilidades en las áreas cubiertas por el SGSI. Las amenazas identificadas incluyen:

- **Accesos no autorizados** a sistemas de información críticos.
- **Ataques cibernéticos** como malware y ransomware dirigidos a la infraestructura de TI.
- **Fugas de información confidencial** debido a errores humanos o fallos en los controles de acceso.

Los controles definidos en el SGSI mitigarán estos riesgos a través de la implementación de políticas, procedimientos y herramientas de seguridad como el control de acceso, autenticación multifactor y la encriptación de datos.

5. Descripción de los Controles del SGSI

A continuación, se especifican algunos de los controles clave que serán implementados para proteger la información dentro del alcance del SGSI:

- **Control de acceso**: Establecimiento de roles y permisos de acceso según la necesidad de conocimiento y el puesto.
- **Cifrado de datos**: Implementación de tecnologías de cifrado para proteger la información durante su almacenamiento y transmisión.
- **Planificación de respuesta ante incidentes**: Procedimientos establecidos para identificar, responder y recuperar ante incidentes de seguridad de la información.

6. Propósito y Objetivos de Seguridad

El propósito principal de este SGSI es garantizar que todos los activos protegidos en el alcance estén sujetos a los controles adecuados de seguridad. Los objetivos de seguridad son los siguientes:

1. **Confidencialidad**: Asegurar que la información solo sea accesible por personas autorizadas.
2. **Integridad**: Garantizar que la información se mantenga precisa y completa.
3. **Disponibilidad**: Asegurar que la información esté disponible para su uso cuando sea necesario.

7. Responsabilidades y Roles

- **Alta Dirección**: Responsabilidad final por la implementación, gestión y mejora continua del SGSI.
- **CISO (Chief Information Security Officer)**: Responsable de la ejecución diaria del SGSI y la gestión de la seguridad de la información.
- **Equipos de TI**: Responsables de la implementación de los controles tecnológicos y la protección de los activos informáticos.
- **Empleados**: Deben seguir las políticas de seguridad y participar en la capacitación sobre buenas prácticas de seguridad.

8. Revisión y Actualización del Alcance

Este documento de alcance será revisado al menos una vez al año o en caso de que se produzcan cambios significativos en los activos, riesgos, tecnología o estructura organizacional de la **UGG**.

Aprobación

Firma del Director General de la UGG:
Nombre y Firma

Fecha de Aprobación:
Fecha

Firma del CISO:
Nombre y Firma

Fecha de Aprobación:
Fecha