UNGRD
Unidad Nacional para la Gestión del Riesgo de Desastres

Plan de Seguridad y Privacidad de la Información 2025

Grupo de Tecnologías de la Información

Enero 2025

Contenido

INTRODUCCIÓN 2
OBJETIVO 2
ALCANCE 2
TÉRMINOS Y DEFINICIONES 2
ESTADO ACTUAL DEL SGSI 3
Política de Seguridad de la Información 3
Objetivos del SGSI 4
Autodiagnóstico 4
ESTRATEGIAS DE SEGURIDAD DIGITAL 6
Plan de Implementación 6
NORMATIVIDAD 8
DOCUMENTOS DE REFERENCIA 9
CONTROL DE CAMBIOS 9

Ilustración 1. Brecha Anexo A ISO 27001:2013 5
Ilustración 2. Estrategias de Seguridad Digital 6

Tabla 1. Evaluación de Efectividad de controles ISO 27001:2013 5
Tabla 2. Plan de Implementación estrategias 8

INTRODUCCIÓN

La Unidad Nacional para la Gestión del Riesgo de Desastres (UNGRD) en cumplimiento de la Política de Gobierno Digital, la Política de Seguridad y Privacidad de la Información y del Modelo de Seguridad y Privacidad de la Información – MSPI elaborado por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, acoge los lineamientos para la implementación de la estrategia de seguridad digital en las entidades públicas, mediante la implementación del Sistema de Gestión de Seguridad de la Información. Teniendo en cuenta lo anterior, la UNGRD establece el presente Plan de Seguridad y Privacidad de la Información, el cual contiene la planeación de actividades del sistema durante la vigencia del 2025.

OBJETIVO

Establecer las actividades para la vigencia 2025, con las cuales se busca desarrollar, verificar y aplicar la mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI en la Unidad Nacional para la Gestión del Riesgo de Desastres – UNGRD, de acuerdo con los requerimientos sugeridos en la norma ISO 27001 y la Política de Seguridad Digital el Modelo de Seguridad y Privacidad de la Información.

ALCANCE

El alcance del Plan de Seguridad y Privacidad de la Información aplica a todos los procesos (Estratégicos, Misionales, de Apoyo y de Evaluación y Seguimiento) de la Unidad Nacional para la Gestión del Riesgo de Desastres.

TÉRMINOS Y DEFINICIONES

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información: Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos, procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de la entidad. (CONPES 3854 de 20116).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000) (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016).
Incidente de Seguridad de la Información: Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (GTC-ISO/IEC27035, 2012).

Partes interesadas: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera. También se puede generar riesgo positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.

Seguridad de la Información: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

Sistema de Gestión de Seguridad de la Información (SGSI): Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

ESTADO ACTUAL DEL SGSI

Política de Seguridad de la Información

En el marco de la Política Integrada del Sistema Integrado de Planeación y Gestión (SIPLAG) de la entidad se establece:

"Propender por el aseguramiento de la confidencialidad, integridad y disponibilidad de la información en la Entidad y sus partes interesadas a través

de la gestión de riesgos de seguridad de la información; así como confirmar el cumplimiento de los objetivos y metas para garantizar la Seguridad de la Información."

Objetivos del SGSI

- Asegurar la preservación de la confidencialidad, integridad y disponibilidad de la información, de acuerdo a las políticas, procedimientos y demás documentación de la UNGRD para la gestión del SGSI.

- Minimizar los riesgos de seguridad de la información a los que pueda estar expuesta la UNGRD y aquella información que sea de interés de sus partes interesadas.

- Generar y divulgar una cultura sobre seguridad de la información a los funcionarios públicos, contratistas, comunidad, proveedores y demás partes interesadas de la UNGRD.

- Desarrollar una cultura de desarrollo, maduración y mejoramiento continuo al interior de la UNGRD de los aspectos relacionados con seguridad de la información, con la participación de los funcionarios y contratistas de la Entidad.

Autodiagnóstico

Según el autodiagnóstico realizado con base en el Modelo de Seguridad y Privacidad de la Información de la Política Nacional de Gobierno Digital, el porcentaje de efectividad en la implementación de los controles establecidos en la Norma NTC/ISO 27001:2013 es de:

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	**OPTIMIZADO**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	100	100	**OPTIMIZADO**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	80	100	**GESTIONADO**
A.8	GESTIÓN DE ACTIVOS	100	100	**OPTIMIZADO**
A.9	CONTROL DE ACCESO	98	100	**OPTIMIZADO**
A.10	CRIPTOGRAFÍA	100	100	**OPTIMIZADO**

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	100	100	**OPTIMIZADO**
A.12	SEGURIDAD DE LAS OPERACIONES	98	100	**OPTIMIZADO**
A.13	SEGURIDAD DE LAS COMUNICACIONES	98	100	**OPTIMIZADO**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	100	100	**OPTIMIZADO**
A.15	RELACIONES CON LOS PROVEEDORES	100	100	**OPTIMIZADO**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	100	100	**OPTIMIZADO**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	67	100	**GESTIONADO**
A.18	CUMPLIMIENTO	92,5	100	**OPTIMIZADO**
PROMEDIO EVALUACIÓN DE CONTROLES		**95**	**100**	**OPTIMIZADO**

Tabla 1. Evaluación de Efectividad de controles ISO 27001:2013

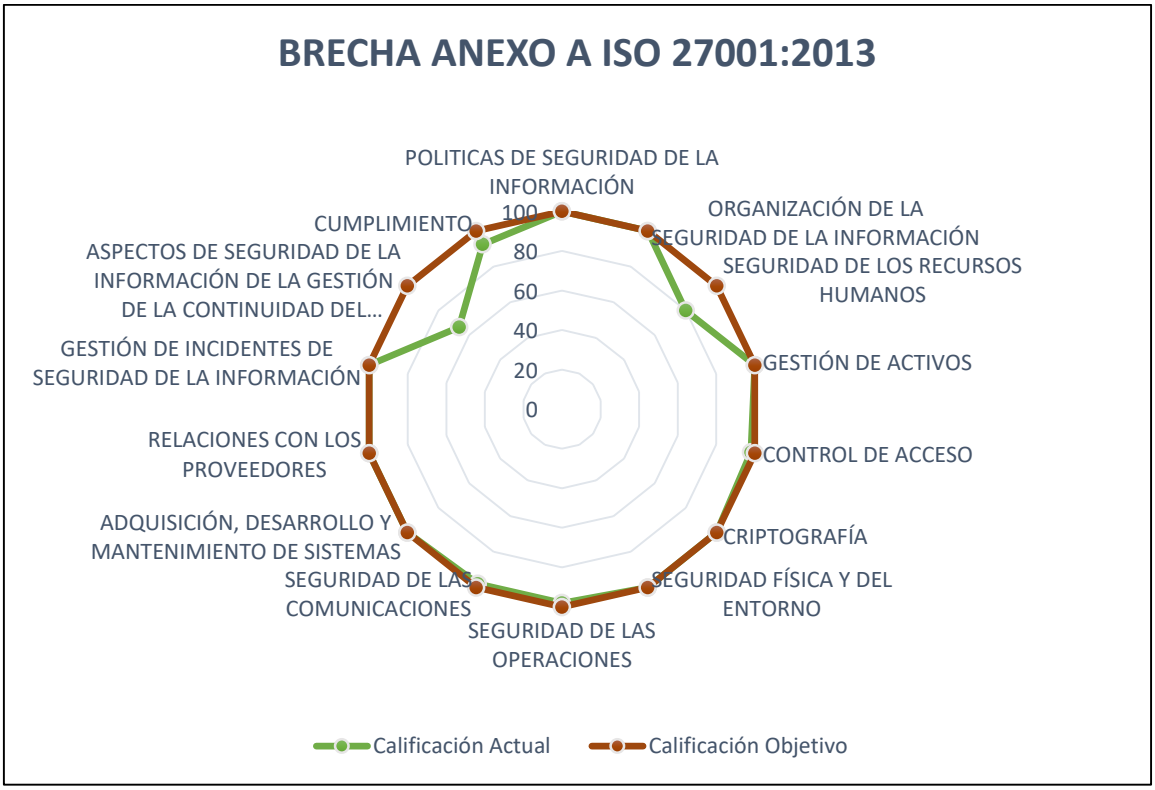

Ilustración 1. Brecha Anexo A ISO 27001:2013

De las gráficas anteriores, se observa un sistema en estado optimizado y se identifican aspectos por mejorar en la continuidad del negocio y seguridad de los recursos humanos.

ESTRATEGIAS DE SEGURIDAD DIGITAL

El Grupo de Tecnologías de la Información (GTI) define las estrategias para implementar el Modelo de Seguridad y Privacidad de la Información (MSPI) en el contexto del Sistema de Gestión de Seguridad de la Información (SGSI). Estas estrategias se desarrollan considerando los aspectos identificados como áreas de mejora en el autodiagnóstico, las políticas internas de la entidad y la normatividad vigente.

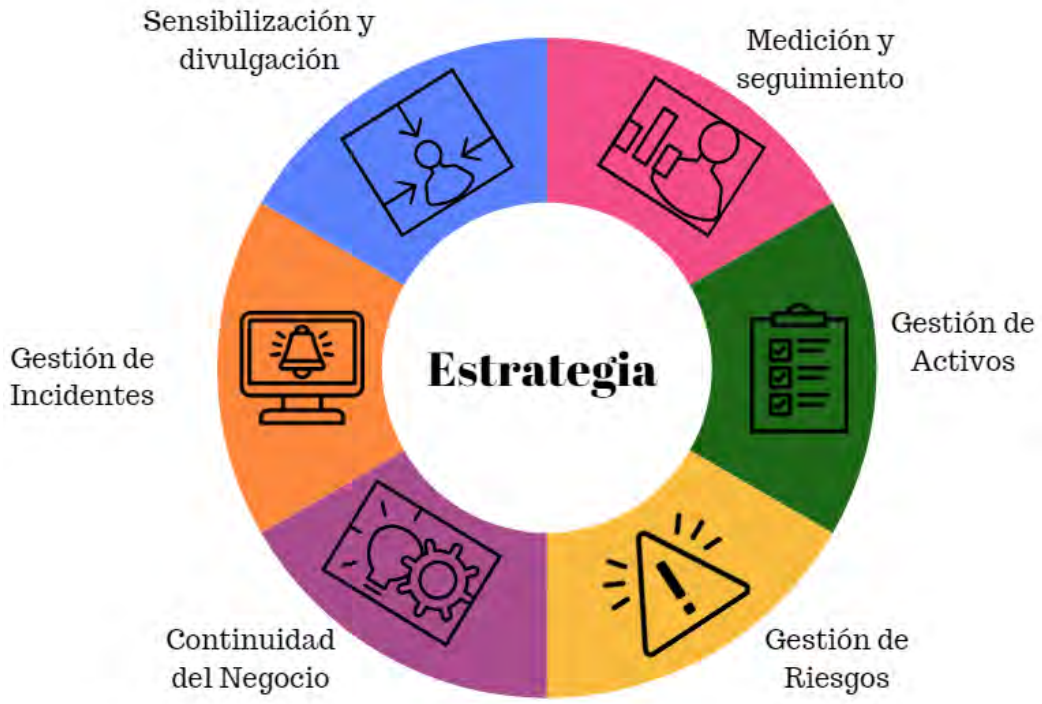

Ilustración 2. Estrategias de Seguridad Digital

Plan de Implementación

El Plan de implementación de Seguridad y Privacidad de la Información se ejecuta de acuerdo con el siguiente cronograma, al cual se le hace seguimiento mes a mes:

#	ESTRATEGIA	ACTIVIDADES	RESPONSABLE	FECHA
1	**Sensibilización y divulgación**	Presentar el SGSI en las jornadas de inducción y reinducción que adelante la entidad.	Grupo de tecnologías de la información	Según calendario del Grupo de Talento Humano
		Charla de seguridad de la información	Grupo de tecnologías de la información	Primer semestre 2025
		Dos pruebas de ingeniería social	Grupo de tecnologías de la información	Vigencia 2025
		Envío de piezas gráficas con recomendaciones e información general sobre la seguridad	Grupo de tecnologías de la información	Mensual vigencia 2025
		Dos pruebas de ETHICAL HACKING	Grupo de tecnologías de la información	Vigencia 2025
		Charla de seguridad de la información.	Grupo de tecnologías de la información	Segundo semestre 2025
2	**Medición y seguimiento**	Actualizar el Instrumento de identificación de la línea base de seguridad (MINTIC)	Grupo de tecnologías de la información	Primer Cuatrimestre 2025
		Realizar medición y seguimiento a los indicadores del SGSI	Grupo de tecnologías de la información	Trimestral vigencia 2025
		Atender las auditorías internas, evaluaciones y seguimientos al Sistema de Gestión de Seguridad de la Información y presentar los informes respectivos.	Grupo de tecnologías de la información Oficina de Control Interno	Vigencia 2025
		Realizar encuesta de impacto a los funcionarios y contratistas	Grupo de tecnologías de la información Oficina de Control Interno	Diciembre 2025
3	**Gestión de Activos de información**	Mesas de trabajo con los delegados de cada proceso para revisión de los activos y su valoración	Todos los procesos de la entidad	Marzo 2025 Septiembre 2025
		Consolidar la información de los procesos	Grupo de tecnologías de la información	Marzo 2025 Octubre 2025
		Publicar el instrumento de activos de información de la UNGRD en NEOGESTION	Grupo de tecnologías de la información	Marzo 2025 Octubre 2025

#	ESTRATEGIA	ACTIVIDADES	RESPONSABLE	FECHA
4	**Gestión de Riesgos de Seguridad**	Mesas de trabajo con los delegados de cada proceso para identificar y valorar los riesgos de seguridad de la información, según la política de tratamiento de riesgos de la entidad.	Todos los procesos de la entidad	Noviembre-Diciembre 2025
		Consolidar la información de los procesos	Grupo de tecnologías de la información	Diciembre 2025
		Publicar el instrumento de Riesgos de información de la UNGRD en NEOGESTION	Grupo de tecnologías de la información	Diciembre 2025
		Monitoreo y revisión de riesgos de seguridad de la información	Grupo de tecnologías de la información con apoyo de todos los procesos de la entidad	Cuatrimestral vigencia 2025
5	**Gestión de incidentes de Seguridad**	Seguimiento a los incidentes de seguridad de la información reportados en los canales de comunicación establecidos por GTI (Mesa de ayuda, correo, vía telefónica)	Grupo de tecnologías de la información	Mensual
		Socializar los boletines informativos de seguridad, integrando con CSIRT de Gobierno y COLCERT	Grupo de tecnologías de la información	Cuando aplique
		Prueba de Vulnerabilidades	Grupo de tecnologías de la información	Vigencia 2025
6	**Continuidad del Negocio**	Actualizar el plan de continuidad de Negocio.	Grupo de tecnologías de la información	Vigencia 2025
		Pruebas de continuidad en la infraestructura tecnológica.	Grupo de tecnologías de la información	Vigencia 2025

Tabla 2. Plan de Implementación estrategias

NORMATIVIDAD

- Decreto 612 de 4 de abril de 2018, Por el cual se fijan directrices para la integración de los planes.

- Decreto 1008 de 14 de junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.

- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.

- Ley 1712 de 2014. 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.

- Resolución 500 de 2021. Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital.

- Resolución 0448 de 2022, Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones, se definen lineamientos frente al uso y manejo de la información y se deroga la resolución 2256 de 2020.

DOCUMENTOS DE REFERENCIA

- Documento Maestro del Modelo de Seguridad y Privacidad de la Información Versión 4.0 Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC).

- M-1101-GTI-03 Manual del Sistema de Gestión de Seguridad de la Información – UNGRD.

- Plan de Seguridad y privacidad de la Información 2024 – UNGRD.

CONTROL DE CAMBIOS

Fecha	Versión	Descripción del cambio
17/01/2025	1	Emisión inicial

Elaboró: Sylvia Ribero Corzo / Oficial de Seguridad de la Información / Contratista GTI
Revisó: Álvaro Wilington Ortiz Suaza / Líder Grupo de Tecnologías de la Información / Contratista GTI
Aprobó: Comité Institucional de Gestión y Desempeño (28/01/2025)