UNGRD

Unidad Nacional para la Gestión del Riesgo de Desastres

Plan de Seguridad y Privacidad de la Información 2026

Grupo de Tecnologías de la Información

Enero 2026

Contenido

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) del Ministerio TIC, desarrolla acciones para fortalecer la seguridad digital mediante la implementación y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

Para la vigencia 2026, este Plan establece las actividades prioritarias del SGSI, con énfasis en la transición y alineación del sistema hacia ISO/IEC 27001:2022, fortaleciendo la gestión del riesgo, la continuidad del negocio, la gestión de incidentes y la cultura institucional de seguridad y privacidad.

OBJETIVO

Establecer las actividades para la vigencia 2026, orientadas a desarrollar, verificar y aplicar la mejora continua del SGSI en la UNGRD, garantizando su alineación y transición hacia ISO/IEC 27001:2022, en articulación con la Política de Seguridad Digital, el MSPI y la normatividad aplicable.

ALCANCE

El alcance del Plan aplica a todos los procesos (Estratégicos, Misionales, de Apoyo y de Evaluación y Seguimiento) de la UNGRD, e involucra a funcionarios, contratistas, proveedores y demás partes interesadas que interactúan con información institucional.

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 del SIPLAG, la UNGRD orienta su gestión a asegurar la confidencialidad, integridad y disponibilidad de la información mediante un enfoque de gestión del riesgo y verificación del cumplimiento de objetivos y metas del SGSI.

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

Para la vigencia 2026, la UNGRD realizará el autodiagnóstico del SGSI bajo el marco ISO/IEC 27001:2022, con el fin de establecer una línea base institucional actualizada, identificar brechas y orientar el plan de trabajo para la actualización del SGSI y su mejora continua.

Teniendo en cuenta que en vigencias anteriores la medición y seguimiento del SGSI se estructuró con base en la organización de controles del Anexo A de ISO/IEC 27001:2013, dichos resultados se conservarán como referente histórico de avance; sin embargo, no se tomarán como línea base directa para 2026, debido a que ISO/IEC 27001:2022 reorganiza el Anexo A, incorpora controles nuevos y ajusta el enfoque de varios controles existentes, lo cual requiere una evaluación específica y consistente con el marco 2022.

En ese sentido, el autodiagnóstico 2026 se orientará a:

- Determinar el nivel de implementación y efectividad de los controles aplicables del Anexo A ISO/IEC 27001:2022, garantizando trazabilidad con el contexto y alcance del SGSI.

- Identificar y priorizar brechas de seguridad y privacidad de la información, considerando criticidad de procesos, activos y riesgos.

- Actualizar y formalizar la Declaración de Aplicabilidad (SoA) bajo ISO/IEC 27001:2022, definiendo para cada control su aplicabilidad, justificación, responsable y evidencia.

- Consolidar un plan de tratamiento (acciones, responsables y seguimiento) que permita el cierre progresivo de brechas, articulado con el MSPI y los instrumentos de gestión institucional.

La evaluación de efectividad se soportará en evidencias documentales (políticas, procedimientos, lineamientos, matrices, SoA) y evidencias de operación (registros, bitácoras, reportes, tickets, resultados de pruebas, actividades de monitoreo), con un enfoque orientado a verificar que los controles no solo existan, sino que funcionen y generen resultados.

Finalmente, los resultados del autodiagnóstico serán presentados a las instancias de dirección y seguimiento definidas por la Entidad, con el propósito de priorizar decisiones, recursos y acciones requeridas para la transición y fortalecimiento del SGSI bajo ISO/IEC 27001:2022.

ESTRATEGIAS DE SEGURIDAD DIGITAL

Se mantienen las **mismas 6 estrategias** de los planes 2024–2025, incorporando dentro de ellas las actividades específicas de transición a ISO/IEC 27001:2022 (brecha, actualización documental, implementación, verificación y mejora).

Ilustración 1. Estrategias de Seguridad Digital

Plan de Implementación

#	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 1: "Cambios clave ISO 27001:2022 + Responsabilidades SGSI"	Grupo de tecnologías de la información	Primer semestre 2026
		Charla 2: "Protección de la información y privacidad (buenas prácticas)"	Grupo de tecnologías de la información	Segundo semestre 2026
		Dos pruebas de ingeniería social	Grupo de tecnologías de la información	Vigencia 2026
		Envío de piezas gráficas y recomendaciones	Grupo de tecnologías de la información	Bimensual vigencia 2026
2	**Medición y seguimiento**	Actualizar instrumento de línea base / autodiagnóstico (MSPI + ISO 27001:2022) Soa actualizado	Grupo de tecnologías de la información	Primer Bimestre 2026
		Realizar análisis de brecha entre SGSI actual vs ISO/IEC 27001:2022 (cláusulas + controles) Soa actualizado	Grupo de tecnologías de la información	Segundo bimestre 2026
		Actualizar indicadores del SGSI y realizar seguimiento	Grupo de tecnologías de la información	Trimestral 2026
		Atender auditorías internas/evaluaciones/seguimientos y presentar informes	Grupo de tecnologías de la información Oficina de control Interno	Vigencia 2026
		Revisión por la Dirección / Comité (resultados, riesgos, acciones y recursos)	Grupo de tecnologías de la información Comité de Gestión y Desempeño	Segundo semestre 2026
3	**Gestión de Activos de información**	Mesas de trabajo con los delegados de cada proceso para revisión, clasificación, propietarios y valoración de activos	Todos los procesos de la entidad	septiembre 2026 octubre 2026
		Consolidar información y asegurar trazabilidad (inventario, dueños, criticidad, ubicación)	Grupo de tecnologías de la información	octubre 2026
		Publicar/actualizar instrumento de activos en NEOGESTION	Grupo de tecnologías de la información	octubre 2026

#	ESTRATEGIA	ACTIVIDADES	RESPONSABLE	FECHA
4	**Gestión de Riesgos de Seguridad**	Mesas de trabajo para identificar/valorar riesgos (incluye riesgos tecnológicos/ciber)	Todos los procesos de la entidad	mayo–junio 2026
		Actualizar plan de tratamiento de riesgos (controles ISO 27001:2022) y responsables	Grupo de tecnologías de la información	julio 2026
		Publicar el instrumento de Riesgos de información de la UNGRD en NEOGESTION	Grupo de tecnologías de la información	diciembre 2026
		Monitoreo y revisión de riesgos	Grupo de tecnologías de la información con apoyo de todos los procesos de la entidad	Cuatrimestral 2026
5	**Gestión de incidentes de Seguridad**	Actualizar procedimiento de gestión de incidentes (roles, escalamiento, evidencias, lecciones aprendidas)	Grupo de tecnologías de la información	Mensual
		Seguimiento a incidentes reportados (mesa de ayuda, correo, telefónico)	Grupo de tecnologías de la información	Mensual
		Socializar boletines de seguridad integrando CSIRT Gobierno / COLCERT	Grupo de tecnologías de la información	Cuando aplique
		Dos pruebas de ETHICAL HACKING	Grupo de tecnologías de la información	Vigencia 2026
		Gestión de actualizaciones de seguridad (firmware firewall / firmas AV / parches críticos)	Grupo de tecnologías de la información	Recurrente 2026
		Pruebas de vulnerabilidades (escaneo) y gestión de remediación	Grupo de tecnologías de la información	Vigencia 2026
6	**Continuidad del Negocio**	Actualizar PCN/DRP y su alineación con ISO 27001:2022 (servicios críticos, RTO/RPO, dependencias)	Grupo de tecnologías de la información	Vigencia 2026
		Pruebas de continuidad/recuperación en infraestructura tecnológica (incluye restauración de backups)	Grupo de tecnologías de la información	Vigencia 2026

Tabla 1. 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.

- 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 5.0 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 y 2025 – UNGRD.

CONTROL DE CAMBIOS

Fecha	Versión	Descripción del cambio
19/01/2026	1	Emisión inicial

Elaboró: Carlos Andrés Granados Guevara / Oficial de Seguridad de la Información / Contratista
Aprobó: Comité Institucional de Gestión y Desempeño (xx/xx/xxxx)