UNIDAD DE SERVICIOS PENITENCIARIOS Y CARCELARIOS - USPEC

PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C., ENERO 2025

VERSIÓN 01

USPEC

1. OBJETIVO

Fortalecer el Sistema de Gestión de Seguridad de la Información (SGSI) de la Unidad de Servicios Penitenciarios y Carcelarios - USPEC, mediante la actualización e implementación de la estrategia de seguridad digital, con el fin de reducir los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de los activos de información de la Entidad.

1.1 OBJETIVOS ESPECÍFICOS

- ✓ Actualizar, comunicar e implementar la estrategia de seguridad digital de la Entidad.
- ✓ Priorizar los proyectos de seguridad a implementar en la vigencia para fortalecer el SGSI.
- ✓ Realizar seguimiento a la estrategia de seguridad digital con el fin de verificar su implementación.

2. ALCANCE

El Plan Estratégico de Seguridad de la Información de la USPEC busca fortalecer la seguridad de la información en todos los procesos institucionales, a través del mantenimiento del SGSI y la implementación de la estrategia de seguridad digital, enmarcada en la Política de Seguridad y Privacidad de la Información de la Entidad. Este plan se enfoca en la gestión de sus procesos misionales, estratégicos, de apoyo y evaluación y control, con el objetivo de asegurar la confidencialidad, integridad y disponibilidad de la información, y garantizar el cumplimiento de la normativa vigente.

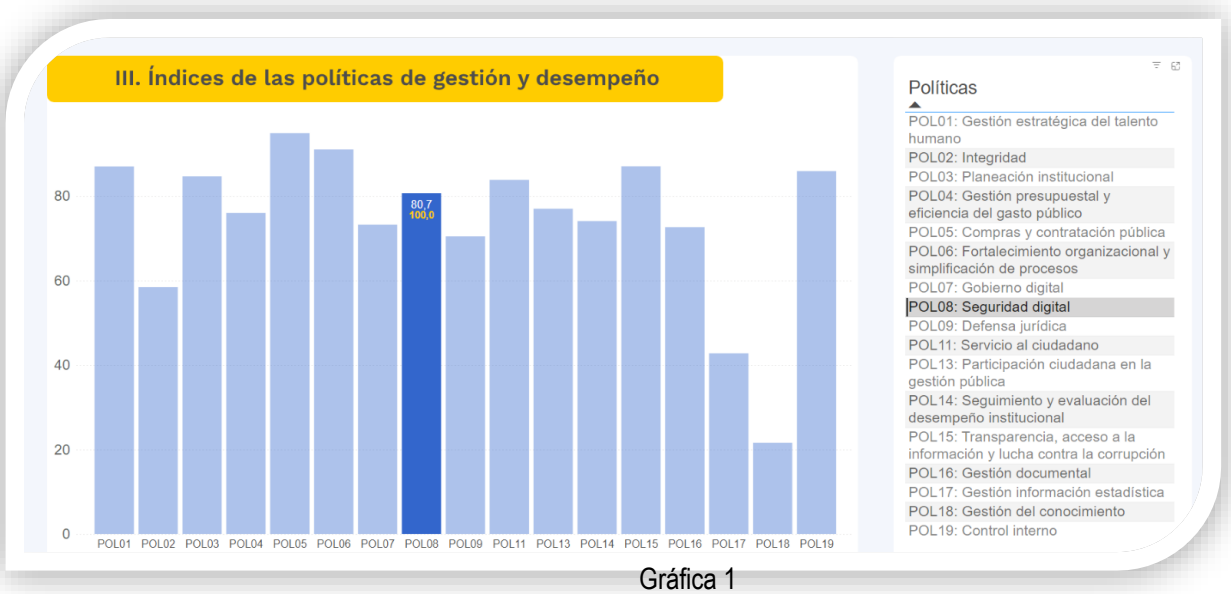
3. DOCUMENTOS DE REFERENCIA

El Plan Estratégico de Seguridad de la Información se basa en los siguientes documentos, normas y lineamientos para su actualización y funcionamiento:

NORMATIVIDAD	
REFERENCIA	**DESCRIPCIÓN**
Decreto 612 de 2018	Fija directrices para la integración de planes al Plan de Acción.
Decreto 767 de 2022	Establece los lineamientos generales de la Política de Gobierno Digital.
Resolución 1519 de 2020	Define estándares para publicar información y requisitos de acceso a la información pública.
Resolución 500 de 2021	Establece lineamientos para la estrategia de seguridad digital.
Norma ISO 27001:2022	Norma internacional para la gestión de seguridad de la información.

NORMATIVIDAD	
REFERENCIA	**DESCRIPCIÓN**
Manual de Gobierno Digital	Establece lineamientos para los componentes de la política y habilitadores transversales.
Modelo de Seguridad y Privacidad de la Información	Define el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
Guía para la administración de riesgos y el diseño de controles de las entidades públicas	Guía del DAFP para la administración de riesgos y diseño de controles.
Política de Seguridad y Privacidad de Información de la USPEC	Política de seguridad y privacidad de la información específica de la USPEC.
NIST Cybersecurity Framework (CSF) 2.0	Conjunto de pautas que ayudan a las organizaciones a gestionar y reducir sus riesgos de ciberseguridad.

4. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN



Gráfica 1

Fuente. Resultados medición del desempeño institucional 2022 – DAFP
https://www.funcionpublica.gov.co/web/mipg/resultados-medicion

Según los resultados de la medición del desempeño institucional 2023, publicado por el Departamento Administrativo de la Función Pública, la política de **Seguridad Digital** tuvo un porcentaje de avance del 80.7% en comparación con los resultados de la vigencia 2022, en el cual se obtuvo un porcentaje de 69.7%.

Es de aclarar que los resultados de la vigencia 2022 no son comparables con los resultados obtenidos en otras vigencias, dado los cambios realizados por los líderes de la política sobre las preguntas que fueron actualizados con respectos nuevas temáticas y directrices.

Teniendo en cuenta los aspectos evaluados en la política de seguridad digital, se determinaron los porcentajes de 3 aspectos específicos:

POLÍTICA 8 Seguridad Digital	i22.Asiganción de Recursos	i23.Implementación Lineamientos de Política	i24.Despliegue de Controles
80,7	70,0	81,3	100,0

Índice de la Política de Seguridad Digital
Fuente. Resultados del índice del desempeño institucional 2022 – DAF

Y de acuerdo a los lineamientos evaluados desde la Política de Gobierno Digital, el porcentaje de avance de seguridad y privacidad de información es de 68.5%

POLÍTICA 7 Gobierno Digital	i14.Seguridad y Privacidad de la información
73,2	68,5

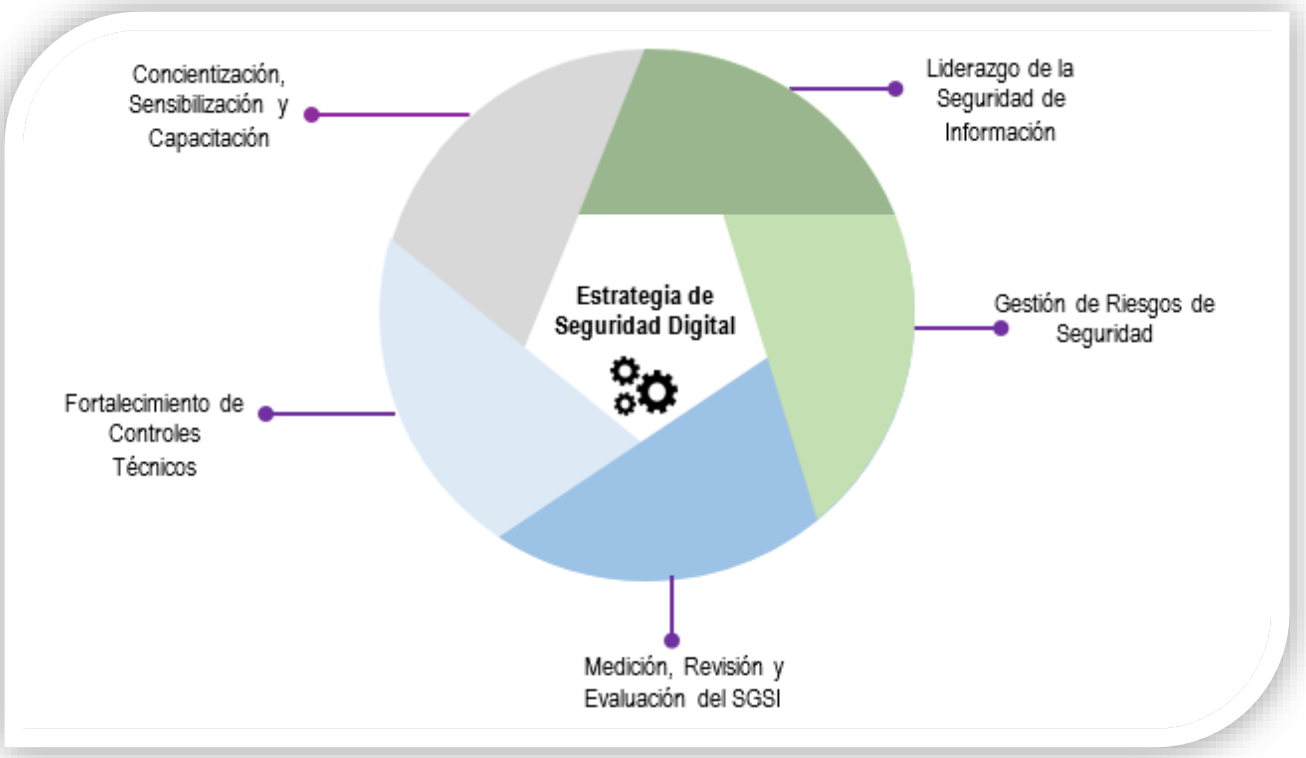
Índice de la Política de Gobierno Digital
Fuente. Resultados del índice del desempeño institucional 2022 – DAF

5. ESTRATEGIA DE SEGURIDAD DIGITAL

La USPEC actualiza su estrategia de seguridad digital en la que se integren las políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira alrededor del fortalecimiento de los elementos del Modelo de Seguridad y Privacidad de la Información (MSPI), evaluados a través de las herramientas de medición citadas en el numeral anterior.
Adicionalmente, se tienen como referencia los lineamientos contenidos en los siguientes documentos de la Entidad:

- ✓ Política de seguridad y privacidad de la información (Resolución 0008 de 2025)
- ✓ Política de administración de riesgos de la entidad – GEPO001
- ✓ Manual de políticas de seguridad de información – TIMA005
- ✓ Procedimiento de gestión de eventos e incidentes de seguridad de información – TIPR004

Por lo anterior, la USPEC define las siguientes seis (6) estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:



5.1 DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MPSI

ESTRATEGIA	DESCRIPCIÓN
Liderazgo de seguridad de la información	Aplicar las buenas prácticas del Modelo de Seguridad y Privacidad de la Información (MSPI) mediante la actualización de los lineamientos asociados, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información institucional. Esto se logrará a través del compromiso visible de la alta dirección y el liderazgo activo de los responsables de procesos.
Gestión de riesgos de seguridad de información	Fortalecer la gestión de riesgos de seguridad de la información mediante la evaluación de los resultados obtenidos en el año 2024, incluyendo el análisis de los riesgos identificados, la efectividad de los controles implementados y las recomendaciones de la auditoría de seguridad realizada. Con base en este análisis, se actualizará el plan de tratamiento de riesgos según la metodología establecida por la Entidad, priorizando la implementación de controles de seguridad que prevengan o reduzcan los impactos de amenazas a la seguridad física y digital.

ESTRATEGIA	DESCRIPCIÓN
Concientización, sensibilización y capacitación	Fortalecer la cultura de seguridad de la información en la entidad mediante la implementación de un sistema de gestión de seguridad de la información (SGSI) que promueva la conciencia del todo el personal que hace parte de la Entidad sobre la importancia de proteger la información institucional.
Medición, revisión y evaluación del SGSI	Establecer un proceso de monitoreo, revisión y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) que permita evaluar periódicamente su eficacia y eficiencia, asegurar el cumplimiento de las actividades, metas y objetivos establecidos, e identificar oportunidades de mejora. Basado en las versiones de la normatividad vigente y estándares internacionales.
Fortalecimiento de controles técnicos	Fortalecer la ciberseguridad de la plataforma tecnológica de la entidad. Para ello, se realizará la validación de los controles de seguridad existentes y se implementarán acciones para mitigar las amenazas y vulnerabilidades identificadas, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información institucional.

5.2 PORTAFOLIO DE PROYECTOS / ACTIVIDADES

La USPEC define los siguientes proyectos y productos esperados, que tienen por objetivo lograr el fortalecimiento y el mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI), permitiendo un seguimiento preciso del progreso y facilitando la evaluación del cumplimiento de los objetivos.

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
Liderazgo de seguridad de la información	**PROYECTO 1:** Fortalecimiento del grupo de seguridad y actualización de lineamientos del SGSI.	1. Autodiagnóstico de seguridad y privacidad de información. 2. Acta de aprobación 3. Planes y documentos actualizados y aprobados 4. Acta de aprobación 5. Actas de reunión del grupo de seguridad

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
Gestión de riesgos de seguridad de información	**PROYECTO 2:** Actualización y optimización de la Gestión de riesgos de seguridad de información.	1. Matriz de riesgos de seguridad de información actualizada 2. Acta de aprobación 3. Planes de tratamiento de riesgos de seguridad de información actualizados 4. Actas de aprobación 5. Reporte trimestral de seguimiento a la implementación del PTR 6. Informe de evaluación al plan de tratamiento de riesgos de seguridad
Concientización, sensibilización y capacitación	**PROYECTO 3:** Fortalecimiento de la Cultura de Seguridad de la Información a través de la Sensibilización, Comunicación y Capacitación	1. Plan de Sensibilización actualizado 2. Registro de materiales de capacitación: Como videos, simulaciones y juegos para hacer la capacitación más atractiva. 3. Informe de seguimiento al plan de sensibilización, comunicación y capacitación 4. Resultado de las encuestas de medición 5. Test de temas promovidos en las sensibilizaciones y capacitaciones.
Medición, revisión y evaluación del SGSI	**PROYECTO 4:**	1. Indicadores actualizados 2. Reporte de Seguimiento a indicadores

ESTRATEGIA / EJE	PROYECTO	PRODUCTOS ESPERADOS
	Mejoramiento continuo y evaluación del desempeño del SGSI	3. Informe de revisión por la dirección 4. Compromisos de la alta dirección frente a las necesidades del SGSI 5. Seguimiento al plan de mejoramiento 6. Informe de Auditoria al SGSI 7. Plan de mejoramiento actualizado 8. Reporte de seguimiento al plan de mejoramiento 9. Dashboard implementado
Fortalecimiento de controles técnicos	**PROYECTO 5** Mejorar la capacidad de la entidad para prevenir, detectar y responder a incidentes de seguridad	1. Registro de activación de controles técnicos

5.3 PLAN OPERACIONAL DE SEGURIDAD DE INFIORMACIÓN

El Plan Operacional de Seguridad (POS) es un componente crucial del Plan de Seguridad y Privacidad de la Información de la USPEC. Este documento detalla los proyectos, las actividades, los responsables y las fechas de implementación de cada una de las estrategias plasmadas en el presente plan.

Por motivos de seguridad y para garantizar la confidencialidad de la información, el POS no se publica en este documento. Su acceso está restringido al personal autorizado y se maneja con la debida discreción. Esta medida preventiva busca evitar que la información sensible caiga en manos equivocadas y sea utilizada para fines maliciosos.

6. ANÁLISIS PRESUPUESTAL 2025

A continuación, se presenta el presupuesto referente al Sistema de Gestión de Seguridad de Información, establecido y aprobado a través del plan anual de adquisiciones:

PROYECTO	INVERSIÓN
Proyecto 1: Fortalecimiento del grupo de seguridad y actualización de lineamientos del SGSI.	$0
Proyecto 2: Actualización y optimización de la Gestión de riesgos de seguridad de información	$0
Proyecto 3: Fortalecimiento de la Cultura de Seguridad de la Información a través de la Sensibilización, Comunicación y Capacitación	$0
Proyecto 4: Mejoramiento continuo y evaluación del desempeño del SGSI	$40.000.000
Proyecto 5: Mejorar la capacidad de la entidad para prevenir, detectar y responder a incidentes de seguridad	$676.400.000
TOTAL:	**$ 716.400.000**

7. INDICADORES

INDICADORES			
Proyecto	**Formula del indicador**	**Periodicidad**	**Tipo de indicador**
Proyecto 2: Actualización y optimización de la Gestión de riesgos de seguridad de información	(Σ del porcentaje de avance en la implementación del PTR por cada riesgo/ Número de riesgos)	Trimestral	Eficacia

RESUMEN DE CAMBIOS

Versión	Fecha	Numerales	Descripción de la modificación
1.0	17/01/2022	Todos	Se crea el plan estratégico de seguridad de información.
2.0	23/01/2023	Todos	Se actualiza el plan estratégico de seguridad de información
3.0	15/01/2024	Todos	Se actualiza el plan estratégico de seguridad de información
4.0	27/01/2025	Todos	Se actualiza el plan estratégico de seguridad de información para la vigencia 2025 y se aprueba a través del Comité Institucional de

			Gestión y Desempeño, según acta N° 13 del 30 de enero 2025

RESPONSABILIDAD Y AUTORIDAD		
Elaboró / Actualizó:	**Revisó:**	**Aprobó:**
Firma:	Firma:	Firma:
Nombre: Daniel Ricardo Muñoz Mayra Alexandra Agudelo	Nombre: Imelda Muñoz Mancipe	Nombre: Imelda Muñoz Mancipe
Cargo: Oficial de Seguridad de Información Profesional Especializado	Cargo: Jefe Oficina de Tecnología	Cargo: Jefe Oficina de Tecnología
Dependencia: Dirección General Oficina de Tecnología	Dependencia: Oficina de Tecnología	Dependencia: Oficina de Tecnología