2025

Plan de Seguridad y Privacidad de la Información

Versión: 02

Subdirección de Informática y Sistemas

SECRETARÍA DISTRITAL DE DESARROLLO ECONÓMICO

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA DE DESARROLLO ECONÓMICO
BOGOTÁ

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2025

Versión	Elaboró	Revisó	Aprobó	Fecha
01	**Maria Alejandra Suarez** Contratista Subdirección de Informática y Sistemas	**Adriana Montoya Ríos** Subdirectora de Informática y Sistemas	**Adriana Montoya Ríos** Subdirectora de Informática y Sistemas	29/01/2024
02	**Maria Alejandra Suarez** Contratista Subdirección de Informática y Sistemas	**Adriana Montoya Ríos** Subdirectora de Informática y Sistemas	**Adriana Montoya Ríos** Subdirectora de Informática y Sistemas	

Versión	Control de Cambios del Plan
01	**Versión para la vigencia 2024, aprobado en acta CIGD No.: 001 del 29/01/2024**
02	Complemento del marco normativo con: CONPES 001, 4062, 4070 y la Ley 2195 de 2022 Ajuste del numeral 4 incorporando la casilla "Tipo de Recurso" En el numeral 6 se ajusta la Columna "presupuesto" por "tipo de recurso Se incorpora introducción y diagnóstico. **Versión para la vigencia 2025, aprobado en acta CIGD No.:**

ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA DE DESARROLLO ECONÓMICO

Tabla de Contenido

Introducción

En un contexto marcado por el crecimiento exponencial de la información y la necesidad de garantizar su seguridad, el Plan de Seguridad y Privacidad de la Información 2025 de la Secretaría Distrital de Desarrollo Económico (SDDE) se plantea como una herramienta estratégica para proteger la integridad, confidencialidad y disponibilidad de los activos de información institucional.

Este plan se alinea con las disposiciones del Modelo de Seguridad y Privacidad de la Información (MSPI) y cumple con las normativas nacionales e internacionales vigentes, asegurando el cumplimiento de los estándares en materia de seguridad digital y la mitigación de riesgos asociados. Además, se integra con el Modelo Integrado de Planeación y Gestión (MIPG), fortaleciendo las capacidades institucionales para contribuir al desarrollo económico y la transformación digital del Distrito.

Es relevante destacar que el Plan Distrital de Desarrollo 2024-2027 "Bogotá Camina Segura" incluye entre sus componentes estratégicos la Seguridad Digital para el Distrito y la ciudadanía, con el objetivo de que Bogotá sea un espacio digital seguro tanto para los ciudadanos como para la administración. Este componente contempla la consolidación del equipo distrital de respuesta a incidentes cibernéticos (CSIRT), la promoción de la identificación de vulnerabilidades, la gestión de riesgos, la protección de datos personales y la prevención del cibercrimen.

Mediante una metodología estructurada, el plan define acciones concretas en diagnóstico, planificación, implementación, evaluación y mejora continua, promoviendo una cultura organizacional orientada a la protección de la información. De esta forma, se garantiza una gestión integral de riesgos que apoya la consecución de los objetivos institucionales y refuerza el compromiso de la SDDE con el desarrollo sostenible y seguro en el ámbito digital

1. Marco normativo

El marco normativo descrito influye en el desarrollo del plan de seguridad al proporcionar los lineamientos, estándares y directrices que las entidades deben seguir para garantizar la protección, integridad y disponibilidad de la información, así como para cumplir con las normatividad legal aplicable vigente a la SDDE.

Normatividad	Entidad	Descripción
Circular Externa No. 002 del 21 de agosto de 2024	Superintendencia de Industria y Comercio	Lineamientos sobre el tratamiento de datos personales en sistemas de inteligencia artificial
Acuerdo 002 de 2023	Comisión Distrital de Transformación Digital	Por la cual se adopta el lineamiento para el desarrollo de evaluaciones de impacto a la privacidad.
Ley 2195 de 2022	Congreso de Colombia	Por Medio de la Cual se Adoptan Medidas en Materia de Transparencia, Prevención y Lucha Contra la corrupción Y Se Dictan Otras Disposiciones.

Normatividad	Entidad	Descripción
CONPES 4062 de 2022	Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación	Política de Propiedad Intelectual
Resolución 460 de 2022	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Por la cual se expide el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la Política de Gobierno digital, y se dictan los lineamientos generales para su implementación.
CONPES 4070 de 2021	Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación	Lineamientos de Política para la Implementación de un Modelo de Estado Abierto
Resolución 500 de 2021	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital.
Decreto 620 de 2020	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Establece los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
Resolución 1519 de 2020.	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos
Resolución 2893 de 2020	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Por la cual se expiden los lineamientos para estandarizar ventanillas únicas, portales específicos de programas transversales, sedes electrónicas, trámites, OPA, y consultas de acceso a información pública, así como en relación con la integración al Portal Único del Estado colombiano, y se dictan otras disposiciones
Directiva 002 de 2020	Presidencia de la Republica	Medidas para atender la contingencia generada por el covid-19, a partir uso de las tecnologías la información y las telecomunicaciones - TIC

Normatividad	Entidad	Descripción
CONPES 3995 de 2020.	Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación	Política Nacional de Confianza y Seguridad Digital.
CONPES D.C. 01 de 2019	Consejo Distrital de Política Económica y Social del Distrito Capital - CONPES D.C	Política Pública Distrital de Transparencia, Integridad y no tolerancia con la corrupción
Decreto 612 de 2018	Presidencia de la Republica	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado
CONPES 3854 de 2016.	Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación	Política de Seguridad Digital del Estado Colombiano
Decreto 1078 de 2015	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Ley 1712 de 2014	Presidencia de la Republica	Ley de Transparencia y el Derecho a la Información Pública Nacional
Ley 1581 de 2012	Congreso de Colombia	Se dictan disposiciones generales para la protección de datos personales
CONPES 3701 de 2011.	Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación	Lineamientos de Política para Ciberseguridad y Ciberdefensa.

2. Definiciones y Siglas

- Activos de información: es: “algo que una organización valora y, por lo tanto, debe proteger”. Se puede considerar como un activo de información a: los datos creados o utilizados por un proceso de la organización en medio digital, en papel o en otros medios. Es importante precisar que el concepto de activos de información definido en la ley 1712 de 2014 es diferente al concepto que maneja el MSPI – ISO 27001.
- Análisis de Vulnerabilidades: Identificación del nivel de exposición existentes en los sistemas, haciendo pruebas de intrusión, que sirven para verificar y evaluar la seguridad física y lógica de los sistemas de información, redes de computadoras, aplicaciones web, bases de datos y servidores
- CSIRT: Equipos de respuesta a incidentes de seguridad.
- Copia de seguridad: copia de datos que se realiza con el propósito de preservar la información en caso de pérdida, daño o destrucción del original
- MSPI: Modelo de Seguridad y Privacidad de la Información

3. Objetivo General

Fortalecer la seguridad de la información en la Secretaría Distrital de Desarrollo Económico, asegurando la integridad, confidencialidad y disponibilidad de sus activos informativos y minimizando los riesgos asociados

3.1. Objetivos Específicos

- **Establecer y ejecutar un conjunto de actividades detalladas para el año 2025** Abordar y resolver las brechas identificadas en el autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) realizado en 2024.

4. Alcance

El presente Plan de Seguridad de la Información se alinea y amplía el alcance establecido en la Política de Seguridad de la Información de la Secretaría Distrital de Desarrollo Económico (SDDE). Este Plan es integral y abarca todos los procesos y procedimientos institucionales de la SDDE, enfatizando su aplicabilidad e importancia estratégica.

El alcance del Plan incluye a todos los usuarios internos y externos asociados con la SDDE. Esto comprende, pero no se limita a, servidores públicos, personal adscrito tanto a la planta permanente como provisional, contratistas, consultores, pasantes, proveedores de bienes y servicios, entidades estatales relacionadas, órganos de control y supervisión, y cualquier

otro tercero que realice actividades en las instalaciones de la SDDE o en representación de esta.

Adicionalmente, el Plan se extiende a todas las formas de interacción con la información de la SDDE, incluyendo el manejo de datos en medios digitales y físicos, las comunicaciones internas y externas, y el uso de redes y sistemas informáticos. Asimismo, contempla la gestión de riesgos asociados a la seguridad de la información en todos los niveles y la promoción de una cultura organizacional que prioriza la protección de datos y la privacidad como pilares fundamentales en todas las operaciones de la Secretaría.

5. Diagnóstico

Esta fase se enfocó en identificar cómo se están resguardando los activos de información dentro de la SDDE, verificando la aplicación de medidas que cumplen con las normativas de protección de datos personales y contribuyen a la reducción de riesgos en la seguridad de la información.

El diligenciamiento de la herramienta establecida por MinTIC permitió obtener una calificación para cada dominio, promediada a partir de los objetivos de control establecidos en las pestañas “ADMINISTRATIVAS” y “TÉCNICAS” del Instrumento MSPI. Los resultados reflejan la efectividad de los controles según la Normatividad NTC/ISO 27001 del 2013 y el modelo de seguridad y privacidad de la información establecido por el MinTIC para las entidades públicas de orden territorial.

A continuación, se detalla la evaluación de la efectividad de controles:

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	61	100	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	70	100	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	55	100	EFECTIVO
A.9	CONTROL DE ACCESO	64	100	GESTIONADO
A.10	CRIPTOGRAFÍA	50	100	EFECTIVO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	57	100	EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	53	100	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	47	100	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	30	100	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	50	100	EFECTIVO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	20	100	INICIAL
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	27	100	REPETIBLE
A.18	CUMPLIMIENTO	67.5	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		**54**	**100**	EFECTIVO

Fuente: Documento Instrumento_Evaluacion_MSPI_SDDE– Portada.

La imagen muestra una evaluación detallada de diversos dominios de seguridad de la información, calificando su efectividad actual frente a un objetivo de 100. Los dominios incluyen políticas de seguridad, organización, recursos humanos, gestión de activos, control de acceso, criptografía, seguridad física y del entorno, operaciones, comunicaciones,

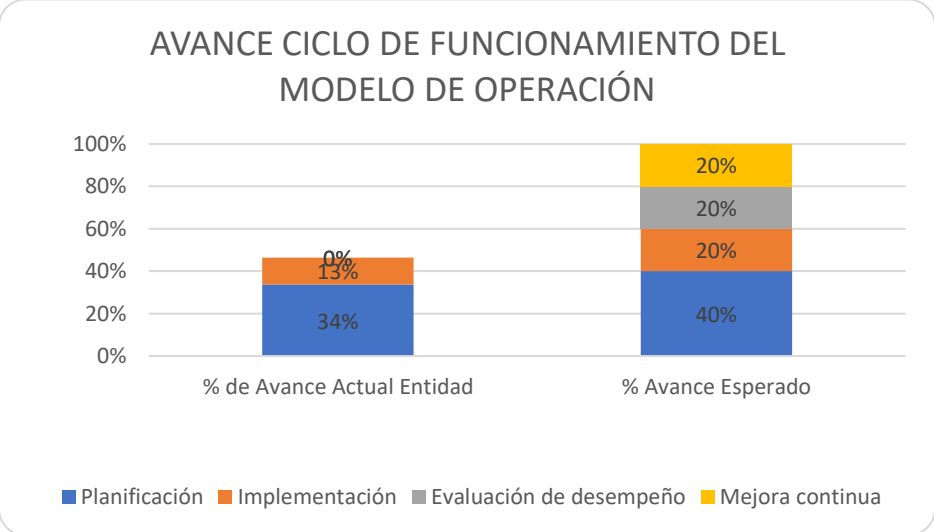
adquisición y mantenimiento de sistemas, relaciones con proveedores, gestión de incidentes, continuidad del negocio y cumplimiento. El promedio de efectividad actual es de 54, destacando áreas como políticas de seguridad y criptografía como optimizadas, mientras que otros dominios como adquisición de sistemas y gestión de incidentes requieren mejoras significativas.

En la evaluación de los dominios, se observa que en varios casos la calificación obtenida supera el nivel repetible (+50%) en la escala de valoración de controles. Por lo tanto, es necesario avanzar en la documentación y comunicación de los procesos y controles. Además, es importante continuar implementando acciones para asegurar el cumplimiento en los dominios donde el funcionamiento no es aún efectivo.

AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

Impacto general en el MSPI
Basándonos en la evaluación y el diagnóstico, se determina que la SDDE se encuentra en un nivel repetible en términos de la implementación de medidas y controles para la seguridad de la información, así como para la protección de los activos que la contienen.

- **Avance total (46%) frente al 100% ideal**:
  - Refleja que las actividades del MSPI no están completamente alineadas con los requerimientos de un ciclo PHVA efectivo.
  - Las áreas críticas como Evaluación de Desempeño y Mejora Continua están desatendidas, lo que dificulta el cumplimiento de las normativas vigentes y los estándares internacionales



Fuente: Documento Instrumento_Evaluacion_MSPI_SDDE– Portada.

6. Desarrollo del Plan de Seguridad y Privacidad de la Información

En el marco de las directrices institucionales y estratégicas de la Secretaría Distrital de Desarrollo Económico, y siguiendo la metodología del Modelo de Seguridad y Privacidad de la Información (MSPI), la Subdirección de Informática y Sistemas establece un conjunto de actividades esenciales para la implementación efectiva de las estrategias de la política de seguridad y privacidad de la información. Estas actividades están alineadas con las disposiciones de la Resolución 500 del 2021, que define los lineamientos y estándares clave para la estrategia de seguridad digital. La adopción del MSPI no solo cumple con estos requisitos, sino que también actúa como un catalizador para habilitar y reforzar la política de Gobierno Digital de la SDDE.

Para lograr esto, se ha diseñado un plan que incluye:

5.1. Planificación

Autodiagnóstico

LÍNEA DE ACCIÓN	ACTIVIDADES	TIPO DE RECURSO
Modelo de Seguridad y privacidad de la información	Actualizar autodiagnóstico del MSPI	Humano Contratista seguridad de la información
	Remitir autodiagnósticos a la Consejería Distrital TICS	

Fuente: Elaboración propia

Gestión de activos de información

Identificar los activos de información críticos de la SDDE

LÍNEA DE ACCIÓN	ACTIVIDADES	TIPO DE RECURSO
Actualización activos de información 2025	Charla de sensibilización de conceptos relacionados con los activos de información, conforme lo establecido en Instructivo de elaboración de la matriz activos de información GT-P5-F1	Humano Contratista seguridad de la información
	Elaborar y remitir memorando de solicitud de actualización de activos de información a los líderes de área	
	Revisar y retroalimentar los activos de información reportados por las áreas	
	Consolidar matriz de activos de información institucional	

LÍNEA DE ACCIÓN	ACTIVIDADES	TIPO DE RECURSO
	Anonimizar y generar matrices con los activos de información y el índice de información clasificada y reservada	
	Gestionar publicación de los activos de información en la página web institucional	

Fuente: Elaboración propia

Gestión de riesgos de seguridad de la información

Evaluar los riesgos asociados a los activos de información críticos de la entidad, asegurando que las medidas de seguridad estén alineadas con las necesidades específicas y el entorno normativo.

LÍNEA DE ACCIÓN	ACTIVIDADES	TIPO DE RECURSO
Identificación, consolidación de riesgos de seguridad de la información y seguridad digital	Identificar, analizar y evaluar los riesgos de aquellos activos de información con criticidad alta en la matriz activos de información GT-P5-F1	Humano Contratista seguridad de la información
	Establecer controles y planes de tratamiento sobre los riesgos	
Seguimiento planes de tratamiento	Estructura las carpetas para almacenamiento de las evidencias reportadas por las áreas	
	Realizar seguimiento a los planes de manejo de riesgo de seguridad de la información establecidos por cada uno de los líderes de área, con sus respectivas evidencias	

Fuente: Elaboración propia

Cultura organizacional y comunicación

Desarrollar programas de capacitación para concienciar a funcionarios y contratistas sobre la importancia de la seguridad y privacidad de la información, fortaleciendo la cultura de seguridad al interior de la entidad.

LÍNEA DE ACCIÓN	ACTIVIDADES	TIPO DE RECURSO
Cultura y apropiación	Documentar matriz con las actividades para fomentar la cultura y apropiación relacionados con la seguridad de la información	Humano

LÍNEA DE ACCIÓN	ACTIVIDADES	TIPO DE RECURSO
Ejecución de estrategia	Llevar a cabo las acciones que fomenten la cultura institucional en materia de seguridad de la información	Contratista seguridad de la información
Medición de apropiación en seguridad de la información	Diseñar y ejecutar acción programada que permita medir la apropiación de los conceptos/procedimientos de seguridad en la Entidad, a través de eventos controlados de phishing e ingeniería social	
	Elaborar y presentar informe relacionado con la simulación realizada	

Fuente: Elaboración propia

5.2. Operación

Implementación

Adaptar y aplicar las políticas, procedimientos y controles establecidos en el MSPI, garantizando que estén personalizados para abordar los desafíos y objetivos de la Secretaría.

LÍNEA DE ACCIÓN	ACTIVIDADES	TIPO DE RECURSO
Ciberdefensa	Configurar herramienta de ciberseguridad y realizar las acciones correspondientes con el monitoreo de alertas	Humano Contratista seguridad de la información Profesional en Infraestructura
Derechos de propiedad intelectual	Definir e implementar lineamientos específicos para abordar la protección y gestión de la propiedad intelectual en el proceso de contratación, con el fin de garantizar que los derechos de propiedad intelectual de la SDDE sean considerados y protegidos.	
Eliminación de información	Documentar instructivo relacionado con el borrado seguro de la información	
Arquitectura del sistema seguro y principios de ingeniería	Establecer, documentar y aplicar los principios de ingeniería de seguridad en todas las actividades relacionadas con la ingeniería/desarrollo de sistemas de información. Esto incluye el diseño seguro de	

LÍNEA DE ACCIÓN	ACTIVIDADES	TIPO DE RECURSO
	las capas de arquitectura (negocios, datos, aplicaciones y tecnología)	
Política de seguridad de la información	Validar actualización sobre la política de seguridad y privacidad de la información	
Mantenimiento de equipos	Ejecutar el mantenimiento de la infraestructura tecnológica (que aplique) de acuerdo con las recomendaciones del fabricante	
Gestión de vulnerabilidades	Estructurar y ejecutar el plan de análisis de vulnerabilidades	
	Elaborar informe con el plan de remediación correspondiente	

Fuente: Elaboración propia

Gestión de incidentes de seguridad de la información

Preparar y mantener procedimientos de respuesta ante incidentes de seguridad, asegurando una reacción rápida y efectiva en caso de cualquier brecha o amenaza a la seguridad de la información

LÍNEA DE ACCIÓN	ACTIVIDADES	TIPO DE RECURSO
Contacto autoridades externas	Socializar con el equipo de la Subdirección de informática y sistemas los boletines informativos y de gestión para la prevención de incidentes de seguridad	Humano Contratista seguridad de la información
Documentación	Elaborar documento que permita la orientación y gestión de los incidentes de seguridad institucional	
Eventos y monitoreo	Realizar seguimiento a las herramientas de seguridad informática validando comportamientos sospechosos sobre la infraestructura TI	

Fuente: Elaboración propia

Continuidad de seguridad de la información

LÍNEA DE ACCIÓN	ACTIVIDADES	TIPO DE RECURSO
Copia de seguridad de la información	Ejecutar y documentar restauración aleatoria sobre copia de seguridad generada	Humano
Mantenimiento y revisión	Ejecutar revisiones periódicas sobre los eventos y alertas en la herramienta de ciberseguridad	Contratista seguridad de la información

Fuente: Elaboración propia

5.3. Evaluación de Desempeño

Implementar mecanismos de reporte efectivos para mantener a la alta dirección informada sobre el estado de la seguridad de la información, facilitando la toma de decisiones basada en datos y la gestión proactiva de riesgos

LÍNEA DE ACCIÓN	ACTIVIDADES	TIPO DE RECURSO
Seguimiento	Reportar el seguimiento relacionado con la implementación del MSPI	Humano Contratista seguridad de la información

Fuente: Elaboración propia

5.4. Mejora Continua

Se establecen las actividades para evaluar la efectividad de las medidas de seguridad implementadas y realizar ajustes según sea necesario, manteniendo la seguridad de la información en línea con las tendencias y desarrollos tecnológicos.

LÍNEA DE ACCIÓN	ACTIVIDADES	TIPO DE RECURSO
Mejora	Documentar las acciones para el cierre de brechas derivadas de revisiones internas	Humano Contratista seguridad de la información

Fuente: Elaboración propia

Este enfoque integral garantiza que la SDDE establezca un marco de seguridad y privacidad de la información robusto y adaptativo, esencial para el éxito de nuestras iniciativas de gobierno digital y el desarrollo económico del distrito.

7. Cronograma de Actividades

No.	ACTIVIDAD	TIPO DE RECURSO	RESPONSABLE	ENTREGABLE	FECHA INICIO	FECHA FIN
1	Actualizar autodiagnóstico del MSPI	Recurso humano	Responsable de la seguridad de la información Profesional Universitario de la SIS	Documento con autodiagnóstico	01/06/2025	30/06/2025
2	Remitir autodiagnósticos a la Consejería Distrital TICS	Recurso humano	Responsable de la seguridad de la información Profesional Universitario de la SIS	Correo electrónico remitiendo autodiagnóstico a la consejería Distrital TICS	01/07/2025	30/07/2025
3	Charla de sensibilización de conceptos relacionados con los activos de información, conforme lo establecido en Instructivo de elaboración de la matriz activos de información GT-P5-I1	Recurso humano	Responsable de la seguridad de la información Profesional Universitario de la SIS	Lista de asistencia	01/08/2025	15/08/2025
4	Elaborar y remitir memorando de solicitud de actualización de activos de información a los líderes de área	Recurso humano	Responsable de la seguridad de la información y Subdirector de sistemas e informática	Memorando radicado en GesDoc	01/08/2025	15/08/2025
5	Revisar y retroalimentar los activos de información reportados por las áreas	Recurso humano	Responsable de la seguridad de la información Profesional Universitario de la SIS	Correo electrónico	16/08/2025	30/08/2025

6	Consolidar matriz de activos de información institucional	Recurso humano	Responsable de la seguridad de la información Profesional Universitario de la SIS	gt-p5-f1_ Matriz de activos de información	15/09/2025	30/09/2025
7	Anonimizar y generar matrices con los activos de información y el índice de información clasificada y reservada	Recurso humano	Responsable de la seguridad de la información Profesional Universitario de la SIS	gt-p5-f1_ Matriz de activos de información	15/09/2025	30/09/2025
8	Gestionar publicación de los activos de información en la página web institucional	Recurso humano	Responsable de la seguridad de la información Profesional Universitario de la SIS	gt-p5-f1_ Matriz de activos de información	01/10/2025	30/10/2025
9	Identificar, analizar y evaluar los riesgos de aquellos activos de información con criticidad alta	Recurso humano	Líderes de área	Formato con riesgos identificados	15/02/2025	31/03/2025
10	Establecer controles y planes de tratamiento sobre los riesgos	Recurso humano	Líderes de área	Formato con riesgos identificados, controles y planes de mejora asociados.	15/02/2025	31/03/2025
11	Estructura las carpetas para almacenamiento de las evidencias reportadas por las áreas	Recurso humano	Responsable de la seguridad de la información Profesional Universitario de la SIS	Estructura en Drive	15/02/2025	31/03/2025

12	Realizar Seguimiento a los planes de manejo de riesgo de seguridad de la información establecidos por cada uno de los líderes de las áreas, con sus respectivas evidencias.	Recurso humano	Líderes de área	Memorando radicado en GesDoc	02/05/2025 02/09/2025	10/05/2025 15/09/2025
13	Documentar matriz con las actividades para fomentar la cultura y apropiación relacionados con la seguridad de la información	Recurso humano	Responsable de la seguridad de la información Profesional Universitario de la SIS	Matriz con actividades de cultura y apropiación	26/01/2025	05/02/2025
14	Llevar a cabo las acciones que fomenten la cultura institucional en materia de seguridad de la información	Recurso humano	Responsable de la seguridad de la información Profesional Universitario de la SIS	Listas de asistencia y piezas gráficas enviadas a través de correo electrónico	15/02/2025	15/12/2025
15	Diseñar y ejecutar acción programada que permita medir la apropiación de los conceptos/procedimientos de seguridad en la Entidad, a través de eventos controlados de phishing e ingeniería social	Recurso humano	Responsable de la seguridad de la información Profesional Universitario de la SIS	Correos electrónicos de pruebas	30/05/2025	15/12/2025
16	Elaborar y presentar informe relacionado con la simulación realizada	Recurso humano	Responsable de la seguridad de la información Profesional Universitario de la SIS	Informe	30/05/2025	15/12/2025

17	Configurar la herramienta de ciberseguridad y llevar a cabo las acciones necesarias para el monitoreo continuo de alertas que indiquen anomalías en la red, con el fin de identificar, analizar y mitigar posibles amenazas de manera oportuna	Recurso humano	Responsable de la seguridad de la información	Herramienta con políticas definidas y funcionales	15/01/2025	28/03/2025
18	Definir e implementar lineamientos específicos para abordar la protección y gestión de la propiedad intelectual en el proceso de contratación, con el fin de garantizar que los derechos de propiedad intelectual de la SDDE sean considerados y protegidos.	Recurso humano	Responsable de la seguridad de la información Profesional Universitario de la SIS	Memorando Oficina Jurídica.	15/01/2025	28/03/2025
19	Documentar instructivo relacionado con el borrado seguro de la información	Recurso humano	Responsable de la seguridad de la información Profesional Universitario de la SIS	Documento publicado en intranet	02/06/2025	29/08/2025
20	Establecer, documentar y aplicar los principios de ingeniería de seguridad en todas las actividades relacionadas con la ingeniería/desarrollo de sistemas de información. Esto incluye el diseño seguro de las capas de arquitectura (negocios, datos, aplicaciones y tecnología)	Recurso humano	Ingenieros de desarrollo	Arquitectura documentada en los nuevos desarrollos	02/06/2025	15/12/2025
21	Validar actualización sobre la política de seguridad y privacidad de la información	Recurso humano	Responsable de la seguridad de la información Profesional Universitario de la SIS	Política actualizada o con su respectiva justificación en caso de no requerir actualización	15/03/2025	08/04/2025

22	Ejecutar el mantenimiento de la infraestructura tecnológica (que aplique) de acuerdo con las recomendaciones del fabricante	Recurso humano	Responsable de la seguridad de la información Profesional Universitario de la SIS	Parches de seguridad aplicados, actualización del recurso tecnológico o mantenimiento físico soportado con formato	15/03/2025	15/12/2025
23	Estructurar y ejecutar el plan de análisis de vulnerabilidades	Recurso humano	Responsable de la seguridad de la información Profesional Universitario de la SIS	Plan de análisis de vulnerabilidades	01/04/2025	15/12/2025
24	Elaborar informe con el plan de remediación correspondiente	Recurso humano	Responsable de la seguridad de la información Profesional Universitario de la SIS	Informe con análisis y recomendaciones	01/05/2025	30/11/2025
25	Socializar con el equipo de la Subdirección de informática y sistemas los boletines informativos y de gestión para la prevención de incidentes de seguridad	Recurso humano	Responsable de la seguridad de la información Profesional Universitario de la SIS	Matriz de contacto	01/02/2025	15/12/2025
26	Realizar seguimiento a las herramientas de seguridad informática validando comportamientos sospechosos sobre la infraestructura TI	Recurso humano	Responsable de la seguridad de la información Equipo de infraestructura	Reportes de las herramientas	01/04/2025	15/12/2025

27	Ejecutar y documentar restauración aleatoria sobre copia de seguridad generada	Recurso humano	Responsable de la seguridad de la información Equipo de infraestructura	Informe de restauración	01/11/2025	15/12/2025
28	Ejecutar revisiones periódicas sobre los eventos y alertas en la herramienta de ciberseguridad	Recurso humano	Responsable de la seguridad de la información Equipo de infraestructura	Reportes de las herramientas	20/03/2025	15/12/2025
29	Reportar el seguimiento relacionado con la implementación del plan de seguridad y privacidad de la información	Recurso humano	Responsable de la seguridad de la información Profesional Universitario de la SIS	Correo electrónico	30/04/2025	15/12/2025
30	Documentar las acciones para el cierre de brechas derivadas de revisiones internas	Recurso humano	Responsable de la seguridad de la información Profesional Universitario de la SIS	Correo electrónico Informes	01/03/2025	15/12/2025
31	Elaborar documento que permita la orientación y gestión de los incidentes de seguridad institucional	Recurso humano	Responsable de la seguridad de la información Profesional Universitario de la SIS	Documento publicado en intranet	01/08/2025	10/11/2025