2024

Plan de Seguridad y Privacidad de la Información

Versión: 01

Subdirección de Informática y Sistemas

SECRETARÍA DISTRITAL DE DESARROLLÓ ECONÓMICO

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

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2024

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

Versión	Control de Cambios del Plan
01	Emisión del documento para la vigencia 2024 **Versión para la vigencia 2024, aprobado en acta CIGD No.: 001 del 29/01/2024**

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

BOGOTÁ

ANEXO 1 Cronograma de Actividades

Tabla de Contenido

1. Objetivo General

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

1.1. Objetivos Específicos

- Establecer y ejecutar un conjunto de actividades detalladas para el año 2024, enfocadas en abordar y resolver las brechas identificadas en el autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) realizado en 2023.
- Desarrollar un plan de acción para establecer los proyectos clave que contribuirán a la implementación del MSPI. Esto incluye la asignación de recursos y la definición de cronogramas, alineada con los objetivos estratégicos de la entidad.

2. 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.

3. 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.
- MSPI: Modelo de Seguridad y Privacidad de la Información

4. Marco normativo

Normatividad	Entidad	Descripción
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.
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.
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

Normatividad	Entidad	Descripción
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
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.
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.

5. 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
Modelo de Seguridad y privacidad de la información	Actualizar autodiagnóstico del MSPI
	Elaborar informe con los resultados de la actualización del autodiagnóstico.

Gestión de activos de información

Identificar los activos de información críticos de la SDDE

LÍNEA DE ACCIÓN	ACTIVIDADES
Actualización activos de información 2024	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
	Elaborar y remitir memorando de solicitud de actualización de activos de información a los lideres de área.

LÍNEA DE ACCIÓN	ACTIVIDADES
	Revisar y retroalimentar los activos de información reportados por las áreas
	Consolidar matriz de activos de información institucional
	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

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
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
	Establecer controles y planes de tratamiento sobre los riesgos
	Aceptar y aprobar los riesgos identificados por cada uno de los lideres de área
Seguimiento planes de tratamiento	Estructura las carpetas para almacenamiento de las evidencias reportadas por las áreas
	Elaborar y remitir memorando de solicitud para realizar seguimiento al plan de tratamiento de los riesgos
	Realizar seguimiento a los planes de manejo de riesgo de seguridad de la información establecidos por cada uno de los lideres de las áreas, con sus respectivas evidencias.

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
Cultura y apropiación	Desarrollar una matriz que documente los aspectos cruciales de la cultura y apropiación relacionados con la seguridad de la información
Ejecución de estrategia	Llevar a cabo las acciones que fomenten la cultura organizacional en materia de 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 realizadas

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
Controles NTC/IEC ISO 27001:2022	Crear la matriz con la declaración de aplicabilidad de los controles de seguridad de la información y su respectiva acción
Política de seguridad de la información	Validar actualización sobre la política de seguridad y privacidad de la información
Gestión de Vulnerabilidades	Documentar procedimiento relacionado con la gestión de vulnerabilidades

LÍNEA DE ACCIÓN	ACTIVIDADES
	Estructurar y ejecutar el plan de análisis de vulnerabilidades
	Elaborar informe con el plan de remediación correspondiente

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
Incidentes de seguridad	Revisar pertinencia sobre la actualización del procedimiento de incidentes de seguridad
Contactos de interés	Elaborar matriz de contacto con autoridades externas (CSIRT Distrito)
	Socializar con el equipo TI los boletines informativos y de gestión para la prevención de incidentes de seguridad
Eventos y monitoreo	Realizar seguimiento a las herramientas de seguridad informática validando comportamientos sospechosos sobre la infraestructura TI

Continuidad de seguridad de la información

LÍNEA DE ACCIÓN	ACTIVIDADES
Respuesta a la contingencia	Implementar solución tecnológica para la ejecución de las copias de seguridad
	Ejecutar y documentar restauración aleatoria sobre copia de seguridad generada
Mantenimiento y revisión	Ejecutar revisiones periódicas sobre la funcionalidad, errores y demás eventos de la solución tecnológica.

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
Indicadores	Reportar el indicador relacionado con la implementación del MSPI
Auditorias e inspecciones de seguridad de la información	Ejecutar revisiones sobre las políticas de seguridad implementadas

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
Mejora	Documentar las acciones para el cierre de brechas derivadas de revisiones internas

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.

ANEXO 1 Cronograma de Actividades

No.	ACTIVIDAD	PRESUPUESTO	RESPONSABLE	ENTREGABLE	FECHA INICIO	FECHA FIN
1	Actualizar autodiagnóstico del MSPI	Recurso humano	Responsable de la seguridad de la información	Documento con autodiagnóstico	01/06/2024	30/06/2024
2	Elaborar informe con los resultados de la actualización del autodiagnóstico.	Recurso humano	Responsable de la seguridad de la información	Documento con informe	1/07/2024	8/07/2024
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	Lista de asistencia	12/08/2024	15/08/2024
4	Elaborar y remitir memorando de solicitud de actualización de activos de información a los lideres de área.	Recurso humano	Responsable de la seguridad de la información y Subdirector de sistemas e informática	Memorando radicado en GesDoc	1/08/2024	10/08/2024
5	Revisar y retroalimentar los activos de información reportados por las áreas	Recurso humano	Responsable de la seguridad de la información	Correo electrónico	16/08/2024	30/08/2024
6	Consolidar matriz de activos de información institucional	Recurso humano	Responsable de la seguridad de la información	gt-p5-f1_ Matriz de activos de información	02/09/2024	9/09/2024
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	gt-p5-f1_ Matriz de activos de información	02/09/2024	9/09/2024
8	Gestionar publicación de los activos de información en la página web institucional	Recurso humano	Responsable de la seguridad de la información	gt-p5-f1_ Matriz de activos de información	10/09/2024	13/09/2024
9	Identificar, analizar y evaluar los riesgos de aquellos activos de información con criticidad alta	Recurso humano	Lideres de área	Formato con riesgos identificados	12/02/2024	22/02/2024

10	Establecer controles y planes de tratamiento sobre los riesgos	Recurso humano	Lideres de área	Formato con riesgos identificados, controles y planes de mejora asociados.	12/02/2024	22/02/2024
11	Aceptar y aprobar los riesgos identificados por cada uno de los lideres de área	Recurso humano	Lideres de área	Memorando de entrega con la respectiva matriz de riesgos	23/02/2024	29/02/2024
12	Estructura las carpetas para almacenamiento de las evidencias reportadas por las áreas	Recurso humano	Responsable de la seguridad de la información	Estructura en Drive	2/02/2024	6/02/2024
13	Elaborar y remitir memorando de solicitud para realizar seguimiento al plan de tratamiento de los riesgos	Recurso humano	Responsable de la seguridad de la información y Subdirector de sistemas e informática	Memorando radicado en GesDoc	7/02/2024	9/02/2024
14	Realizar Seguimiento a los planes de manejo de riesgo de seguridad de la información establecidos por cada uno de los lideres de las áreas, con sus respectivas evidencias.	Recurso humano	Lideres de área	Memorando radicado en GesDoc	2/05/2024 2/09/2024	10/05/2024 10/05/2024
15	Desarrollar una matriz que documente los aspectos cruciales de la cultura y apropiación relacionados con la seguridad de la información	Recurso humano	Responsable de la seguridad de la información	Matriz con actividades de cultura y apropiación	26/01/2024	31/01/2024
16	Llevar a cabo las acciones que fomenten la cultura organizacional en materia de seguridad de la información	Recurso humano	Responsable de la seguridad de la información	Listas de asistencia y piezas gráficas	1/02/2024	15/02/2024
17	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	Correos de pruebas	1/08/2024	16/08/2024

18	Elaborar y presentar informe relacionado con la simulación realizadas	Recurso humano	Responsable de la seguridad de la información	Informe	20/08/2024	26/08/2024
19	Crear la matriz con la declaración de aplicabilidad de los controles de seguridad de la información y su respectiva acción	Recurso humano	Responsable de la seguridad de la información	Matriz de aplicabilidad documentada	1/04/2024	31/05/2024
20	Identificar actualización sobre la política de seguridad y privacidad de la información	Recurso humano	Responsable de la seguridad de la información	Política actualizada o con su respectiva justificación en caso de no requerir actualización	15/03/2024	08/04/2024
21	Documentar procedimiento relacionado con la gestión de vulnerabilidades	Recurso humano	Responsable de la seguridad de la información	Procedimiento documentado	8/04/2024	30/04/2024
22	Estructurar y ejecutar el plan de análisis de vulnerabilidades	Recurso humano	Responsable de la seguridad de la información	Plan de análisis de vulnerabilidades	1/10/2024	8/10/2024
23	Elaborar informe con el plan de remediación correspondiente	Recurso humano	Responsable de la seguridad de la información	Informe con análisis y recomendaciones	11/10/2024	21/10/2024
24	Revisar pertinencia sobre la actualización del procedimiento de incidentes de seguridad	Recurso humano	Responsable de la seguridad de la información	Procedimiento actualizado	4/06/2024	28/06/2024
25	Elaborar matriz de contacto con autoridades externas (CSIRT Distrito)	Recurso humano	Responsable de la seguridad de la información	Matriz de contacto	26/02/2024	29/02/2024
26	Socializar con el equipo TI los boletines informativos y de gestión para la prevención de incidentes de seguridad	Recurso humano	Responsable de la seguridad de la información	Correo electrónico	1/02/2024	15/12/2024

27	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	1/02/2024	15/12/2024
28	Implementar solución tecnológica para la ejecución de las copias de seguridad	Recurso humano	Responsable de la seguridad de la información Equipo de infraestructura	Herramienta configurada	9/01/2024	9/02/2024
29	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	1/11/2024	15/12/2024
30	Ejecutar revisiones periódicas sobre la funcionalidad, errores y demás eventos de la solución tecnológica.	Recurso humano	Responsable de la seguridad de la información Equipo de infraestructura	Reportes de las herramientas	9/02/2024	15/12/2024
31	Reportar el indicador relacionado con la implementación del MSPI	Recurso humano	Responsable de la seguridad de la información	Correo electrónico	1/02/2024	15/12/2024
32	Ejecutar revisiones sobre las políticas de seguridad implementadas	Recurso humano	Responsable de la seguridad de la información	Correo electrónico Informes	1/02/2024	15/12/2024
33	Documentar las acciones para el cierre de brechas derivadas de revisiones internas	Recurso humano	Responsable de la seguridad de la información	Reportes relacionados con las acciones para cierre de brechas	2/01/2024	15/12/2024


BOGOTA