Deja huella en el Servicio Civil

Departamento Administrativo del Servicio Civil Distrital

PLAN GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

E-GES-FM-009
Versión. 8.0
Enero de 2022

ALCALDÍA MAYOR DE BOGOTÁ D.C.

BOGOTÁ

PLAN GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Bogotá, D.C., Versión 9.0, enero de 2024

Recuerde: *Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, se considera "Copia No Controlada". La versión vigente se encuentra publicada en el repositorio de documentos SIG del DASCD.*

Carrera 30 No 25 – 90,
Piso 9 Costado Oriental.
Tel: (57) 60 1 3680038
Código Postal: 111311
www.serviciocivil.gov.co

DEPARTAMENTO ADMINISTRATIVO DEL SERVICIO CIVIL DISTRITAL

CARLOS FERNANDO GALÁN
Alcalde Mayor-Bogotá D.C

LILIANA CABALLERO DURÁN
Secretario(a) General-Alcaldía mayor de Bogotá D.C

NIDIA ROCÍO VARGAS
Director(a) Departamento Administrativo del Servicio Civil Distrital –DASCD

GINA PAOLA SILVA VÁSQUEZ
Subdirector(a) Técnica de Desarrollo Organizacional y Empleo Público

MARÍA TERESA RODRÍGUEZ LEAL
Subdirector(a) Jurídica

MARÍA CONSTANZA ROMERO OÑATE
Subdirector(a) de Gestión Distrital, Bienestar, Desarrollo y Desempeño

SLENDY CONTRERAS AMADO
Subdirector(a) de Planeación y Gestión de Información del Talento Humano Distrital

FREDDY CORTÉS DAZA
Subdirector(a) de Gestión Corporativa

INGRID LORENA MEDINA PATARROYO
Jefe de Oficina de Control Interno

CAROLINA PULIDO CRUZ
Jefe de Oficina de Control Disciplinario Interno

LUIS FERNANDO MONTERO LANCHEROS
Jefe de Oficina de Tecnologías de la Información y las Comunicaciones

Recuerde: *Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, se considera "Copia No Controlada". La versión vigente se encuentra publicada en el repositorio de documentos SIG del DASCD.*

CONTENIDO

1. INTRODUCCIÓN 5
2. JUSTIFICACIÓN 5
3. OBJETIVO 6
3.1. Objetivo General 6
3.2. Objetivos Específicos 6
4. ALCANCE 7
5. CONTEXTO DE LA SEGURIDAD DE LA INFORMACIÓN EN EL DASCD 7
5.1. Autodiagnóstico de la implementación del MSPI 8
5.2. Sistema de Gestión de Seguridad de la Información y Seguridad Digital y La Estrategia de Seguridad Digital 10
6. ESTRATEGIA DE SEGURIDAD DIGITAL 11
7. DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES) 12
7.1. PORTAFOLIO DE PROYECTOS / ACTIVIDADES: 13
7.2. CRONOGRAMA DE TRABAJO 18
8. MARCO NORMATIVO. 22
9. METODOLOGÍA 25
10. CONCEPTOS Y DEFINICIONES 25

Recuerde: *Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, se considera "Copia No Controlada". La versión vigente se encuentra publicada en el repositorio de documentos SIG del DASCD.*

1. INTRODUCCIÓN

La información se ha consolidado como uno de los activos más cruciales y valiosos en la actualidad. Su importancia radica en su papel vital para la toma de decisiones, permitiendo que las organizaciones alcancen mayor competitividad e innovación. Asimismo, facilita la prestación de bienes y servicios de calidad, al tiempo que garantiza el suministro de información fiable, ágil y precisa a clientes y usuarios

Es por la importancia de la información, que hoy por hoy se habla de ***"activos de información"***, los cuales pueden ser atacados, generando incidentes de seguridad de la información los cuales pueden generan una afectación o pérdida de información y efectos negativos a la buena imagen de la entidad, problemas con los usuarios o partes interesadas, pérdidas económicas, y problemas legales. De aquí nace la necesidad de que las organizaciones cuenten con un Sistema de Gestión de la Seguridad de la Información, el cual se enmarca la estrategia de seguridad digital en la que se definen los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos, los cuales se fundamentan en la implementación del Modelo de Seguridad y Privacidad de la Información, compuesto por una estrategia donde se diseñan, documentan, implementan y monitorean controles basados en una gestión de tratamiento de riesgos que minimice el impacto y/o la probabilidad de daño, robo y ataque a los activos de información, que permita además mantener el riesgo en niveles aceptables para el Departamento.

El Modelo de Seguridad y Privacidad de la Información debe ser diseñado para que continuamente sea evaluado y mejorado, teniendo en cuenta los estándares internacionales, normatividad, directrices y lineamientos tanto distritales como nacionales aterrizado al modelo de negocio de cada organización, de acuerdo a su necesidades y requerimientos, razón por la cual a continuación se presenta el Plan de Seguridad y Privacidad de la Información del Departamento Administrativo del Servicio Civil Distrital, el cual es abordado con base en el resultado del autodiagnóstico de implementación del MSPI 2022, donde se plantean actividades de mantenimiento del Modelo, así como recomendaciones y mejoras con el fin de proteger los activos de información que se generan y manejan en cada una de las áreas.

Es importante destacar que los Activos de Información están en cualquier parte de la Entidad, por lo tanto, su seguridad y cuidado es un tema de aplicación transversal, que debe ser de obligatorio cumplimiento para todas aquellas personas que tienen contacto directo o indirectos con la información.

2. JUSTIFICACIÓN

En el marco del proceso de Seguridad de la Información, se ha identificado que los activos de información requieren de controles administrativos, físicos y lógicos, para mitigar tanto el impacto como la probabilidad a la hora de materializarse un riesgo. Como soporte de la anterior premisa, se tienen los resultados de los diagnósticos de implementación del Modelo de Seguridad y

Privacidad de la Información – MSPI, los cuales se han desarrollado en las vigencias 2018, 2020, 2021, 2022 y 2023. En estos resultados se muestran las dimensiones en las cuales se deben enfocar esfuerzos para lograr que los controles propuestos en la ISO 27001:2013, se encuentren en niveles adecuados de cumplimiento, dejando a la entidad en un nivel de madurez en las prácticas de seguridad de la información acorde con la exigencia del cuidado de los activos de información. De acuerdo con los diagnósticos desarrollados, en la vigencia 2018 el DASCD se encontraba en un nivel de madurez de fase inicial, mientras que en la vigencia 2022 se encontró que el avance deja a la entidad en nivel administrado. Paralelamente el DASCD viene diligenciando y reportando el Análisis GAP Protección de Datos – Formulado por la Alta Consejería de las TIC, de tal forma que el DASCD ha venido implementando acciones de mejora frente a los controles propuestos en materia de protección de datos personales

Por lo anterior, es pertinente y necesario continuar la implementación del Modelo de Seguridad y Privacidad de la Información, no solo para dar cumplimiento a las metas establecidas por el ministerio, si no para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información, así como crear una cultura organizacional que permita realizar y mantener un MSPI en el tiempo.

3. OBJETIVO

3.1. Objetivo General

Mantener y fortalecer la integridad, confidencialidad y disponibilidad de los activos de información del Departamento Administrativo del Servicio Civil Distrital –DASCD-, para reducir los riesgos a los que está expuesta la organización hasta niveles aceptables, a partir de la implementación de las estrategias de seguridad digital definidas en este documento para la vigencia 2024.

3.2. Objetivos Específicos

- Definir y establecer la estrategia de seguridad digital de la entidad.
- Definir y establecer las necesidades de la entidad para el mantenimiento del Sistema de Gestión de Seguridad de la Información.
- Priorizar las actividades y proyectos a implementar para la correcta implementación del SGSI.
- Planificar la evaluación y seguimiento de los controles y lineamientos implementados en el marco del Sistema de Gestión de Seguridad de la Información.

- Mantener y fortalecer la gestión institucional de seguridad de la información en relación con protección de datos personales.

4. ALCANCE

El Plan Estratégico de Seguridad de la Información al buscar el mantenimiento y fortalecimiento del Sistema de Gestión de Seguridad de la Información y la estrategia de seguridad digital de la entidad, comparte el alcance definido dentro de la Política General de Seguridad de la Información institucional, donde se indica que se tendrán en cuenta todos los procesos de la entidad. Este Plan define las actividades que en el marco del proceso de Seguridad de la Información son desarrolladas para implementar y mantener el Modelo de Seguridad y Privacidad de la Información en el DASCD. Contempla la protección de la información digital, datos personales, medios impresos y físicos digitales y no digitales.

El alcance del presente Plan involucra a toda la entidad, la gestión de todos los procesos e implica el compromiso y participación de todas las dependencias, procesos, funcionarios y contratistas del DASCD.

5. CONTEXTO DE LA SEGURIDAD DE LA INFORMACIÓN EN EL DASCD

El DASCD es una Entidad del orden Distrital de la ciudad de Bogotá, encargada de liderar el servicio civil en el Distrito Capital, responsable de proponer y orientar la implementación de políticas, estrategias y acciones para el fortalecimiento de la gestión integral del talento humano, que optimice la prestación de servicios a los ciudadanos

Tiene por objeto orientar y coordinar los procesos de ajuste organizacional interno de la entidades y organismos distritales, de las plantas de personal, de los manuales de funciones y de requisitos, de nomenclatura y salarios, así como asesorar en el diseño y desarrollo de los programas de bienestar social, mejoramiento del clima laboral, planes de capacitación, sistema de incentivos, en la implementación de los sistemas de evaluación de desempeño y en general en la gestión de las relaciones laborales.

La mayoría de su información generada en las diferentes Subdirecciones requiere de controles efectivos, de procedimientos internos para que permita brindar las condiciones para custodiar sus datos, sistemas de información, planes de tratamientos de riesgos de seguridad y privacidad de la información y acción para el uso y salvaguarda de la información.

Por lo anterior es pertinente y necesario mantener y fortalecer el Modelo de Seguridad y Privacidad de la Información - MSPI en DASCD transversal en sus procesos, apalancado en los procesos de Seguridad de la Información y Gestión de las TIC, por ser estos los procesos principales que tiene en sus funciones y objetivos la seguridad de la información en el DASCD.

5.1. Autodiagnóstico de la implementación del MSPI

La Oficina de Tecnologías de la Información y las Comunicaciones, con los objetivos de inicialmente determinar el estado de implementación del MSPI, desde la vigencia 2018 ha venido aplicando el "Instrumento de Evaluación MSPI", para determinar aspectos y acciones específicas que permitan fortalecer el Sistema de Gestión de Seguridad de la Información. Los resultados obtenidos se presentan en el siguiente gráfico, en el cual se observa el notable avance que se ha obtenido en las distintas dimensiones de la ISO27001:2013, desde el inicio del trabajo en el MSPI en 2018, hasta la pasada vigencia. Si bien se han logrado acortar las brechas evidenciadas en el primer diagnóstico, es necesario dar mantenimiento y sostenimiento al modelo, así como continuar con acciones que permitan al DASCD contar con un MSPI maduro, sostenible y en mejoramiento

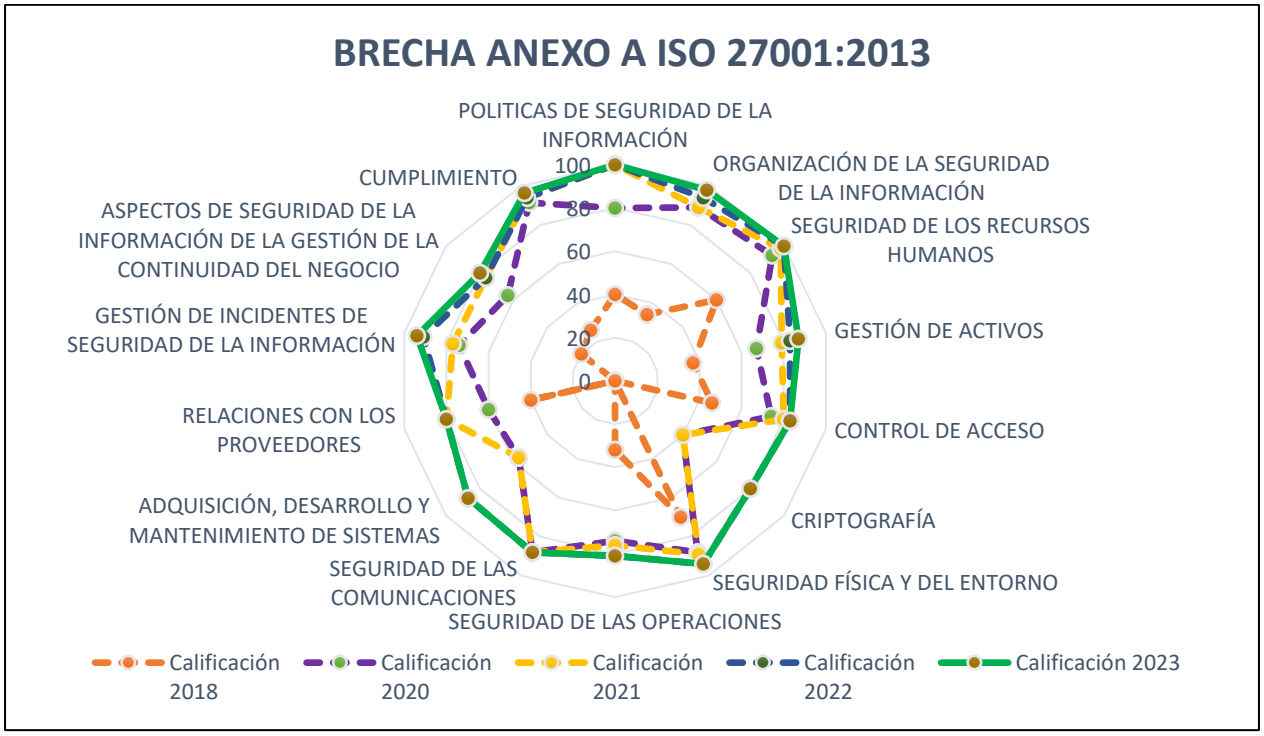


Imagen 1: Evaluación de Efectividad de controles (31/12/2023)

AVANCE PHVA		
COMPONENTE	**% de Avance Actual**	**% Avance Esperado**
Planificación	40%	40%
Implementación	19%	20%
Evaluación de desempeño	20%	20%
Mejora continua	20%	20%
TOTAL	**99%**	**100%**

Imagen 2: Avance ciclo de funcionamiento del modelo de operación (PHVA) (31/12/2023)

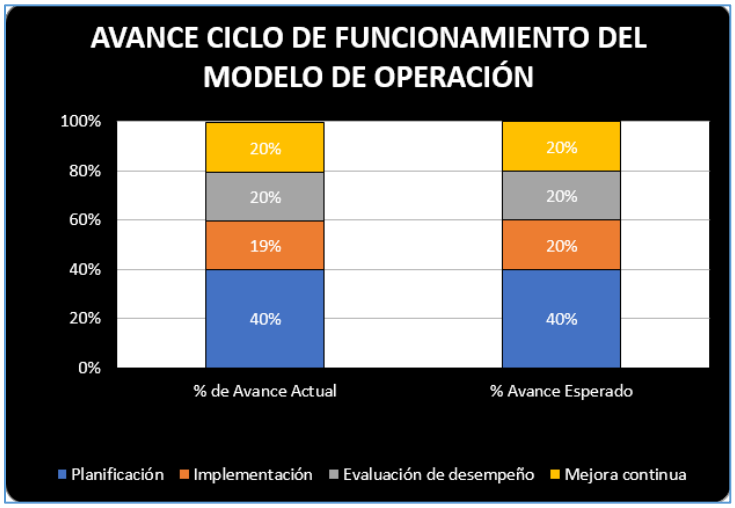


Imagen 3: Imagen 4: Avance ciclo de funcionamiento del modelo de operación (PHVA) (31/12/2023)

Adicional a lo anterior, el DASCD también lleva el registro de reporte **GAP DE PROTECCIÓN DE DATOS PERSONALES** formulado por la Alta Consejería de las TIC –Alcaldía Mayor-, para determinar aspectos y acciones específicas que permitan fortalecer el Sistema de Gestión de Seguridad de la Información en relación a protección de Datos Personales. Los resultados obtenidos se presentan en el siguiente gráfico:

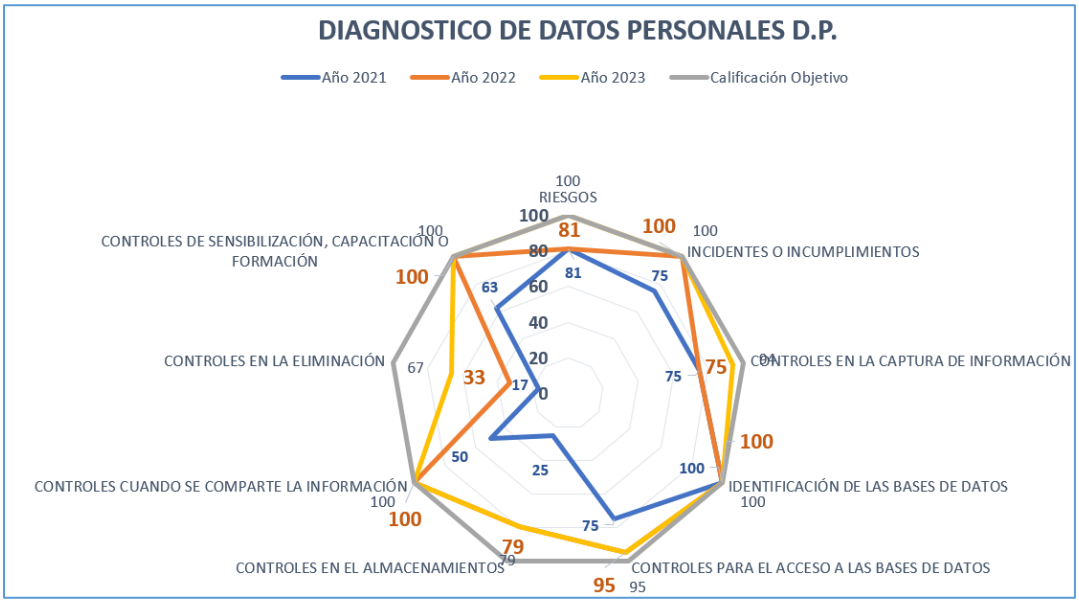


Imagen 5 – Autodiagnóstico Protección de Datos Personales (31/12/2023)

5.2. Sistema de Gestión de Seguridad de la Información y Seguridad Digital y La Estrategia de Seguridad Digital

Según la resolución 0500 de 2021, el DASCD *"como sujeto obligado debe aplicar los modelos, guías, y demás documentos técnicos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones a través del habilitador de seguridad y privacidad de la información en el marco de la Política de Gobierno Digital y propenderán por la incorporación de estándares internacionales y sus respectivas actualizaciones o modificaciones, al igual que otros marcos de trabajo que defina mejores prácticas en la materia."* En este orden se adopta la estrategia de seguridad de la información y de seguridad digital, mediante la aplicación y puesta en funcionamiento del proceso, procedimientos, los instrumentos, documentos y demás herramientas que se definan desde el proceso de seguridad de la información

La Estrategia de seguridad digital consiste principalmente en la implementación, mantenimiento y mejora continua del Modelo de Seguridad y Privacidad de la Información – MSPI, la gestión de riesgos de seguridad de la información y la gestión de los incidentes de seguridad digital. Todos estos aspectos son gestionados mediante los procedimientos definidos en el Proceso de Seguridad de la Información y desarrollados mediante las actividades planteadas en este Plan de Seguridad y Privacidad de la Información.

Recuerde: *Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, se considera "Copia No Controlada". La versión vigente se encuentra publicada en el repositorio de documentos SIG del DASCD.*

El DASCD cuenta con el **PROCESO SEGURIDAD DE LA INFORMACIÓN, CÓDIGO: E-SIN-CP-001**, establecido en el MACROPROCESO ESTRATÉGICO DIRECCIONAMIENTO INSTITUCIONAL dentro del MAPA DE PROCESOS INSTITUCIONAL, donde se articula la política, el manual, los procedimientos, instructivos, indicadores y otros elementos del Sistema de Gestión de Seguridad de la información de la entidad.

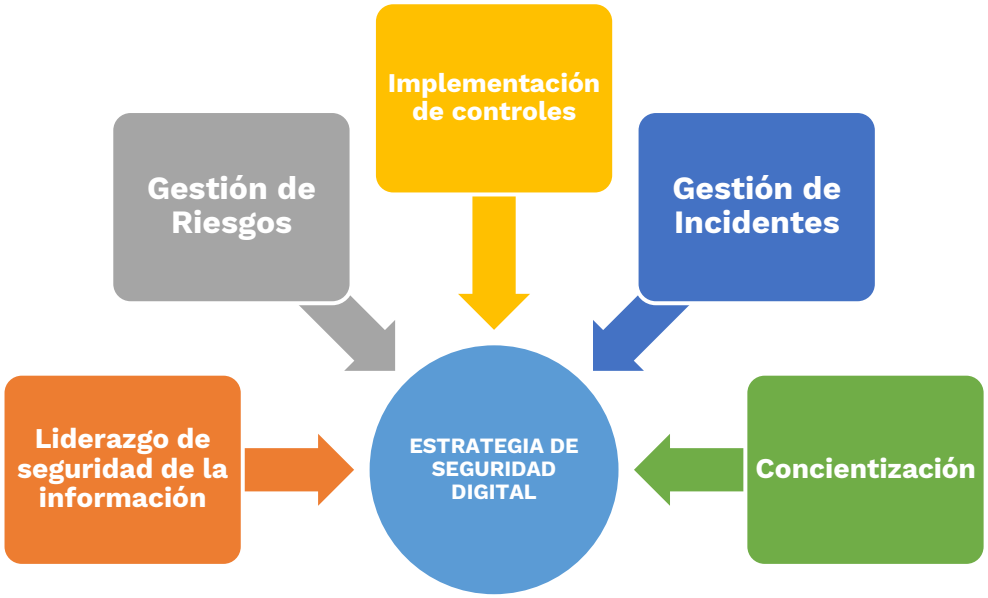
Así mismo, dentro del PROCESO DE GERENCIA ESTRATÉGICA E-GES-CP-001 establecido en el MACROPROCESO ESTRATÉGICO DIRECCIONAMIENTO INSTITUCIONAL, se establece y articula la **E-GES-MA-002 POLÍTICA DE GESTIÓN DE RIESGOS** y el **E-GES-PR-006 PROCEDIMIENTO PARA LA GESTIÓN DE RIESGOS,** cuyo alcance contempla la administración y gestión de riesgos de seguridad de la información institucional sobre todos los procesos de la entidad.

Con el objetivo de establecer los lineamientos para el tratamiento de datos personales en el Departamento Administrativo del Servicio Civil Distrital – DASCD, en concordancia con la Ley 1581 de 2012, y el Decreto Nacional 1377 de 2013 y las demás normas complementarias y relacionadas con el fin de dar un tratamiento y protección de los datos personales que en el ejercicio de sus funciones son tratados por los empleados y contratistas de esta entidad, el DASCD cuenta con la **E-SIN-DE-002 - POLÍTICA PARA EL TRATAMIENTO DE DATOS PERSONALES EN EL DASCD**. Así mismo, cuenta con el **E-SIN-PR-006 PROCEDIMIENTO TRATAMIENTO DE DATOS PERSONALES V1.0**, en el cual se abordan cada uno de los temas relacionados con la gestión de los datos personales

6. ESTRATEGIA DE SEGURIDAD DIGITAL

El DASCD establece una estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira entorno a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes que debe establecerse (Ver Resolución 500 de 2021).

Por tal motivo, El DASCD define las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:



7. DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES)

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MPSI y la resolución 500 de 2021:

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad de la información	Mantener y propiciar la mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la política general, lineamientos y plan de acción definidos y aprobados, buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información.

Gestión de riesgos	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.
Concientización	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.
Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, se pueden subdividir en controles tecnológicos y/o administrativos.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.

7.1. PORTAFOLIO DE PROYECTOS / ACTIVIDADES:

Para cada estrategia específica, El DASCD define los siguientes proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI):

ESTRATEGIA / EJE /FASE	ACTIVIDADES	PRODUCTOS ESPERADOS
A. Liderazgo de seguridad de la información	1. Actualizar los planes de Seguridad y Privacidad de la Información en cumplimiento al Decreto 612 de 2018 2. Mantener actualizado el Autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI), las políticas de Seguridad de la Información, los indicadores y riesgos de gestión de Seguridad y Privacidad de la información de la entidad mediante la aplicación de la mejora continua	• PLAN GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN actualizado a la vigencia 2024 • PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN actualizado a la vigencia 2024 • Autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) actualizado, y/o aprobado por parte del Comité de Gestión y Desempeño Institucional • Políticas de Seguridad de la Información revisadas, ajustadas y actualizadas -Según aplique su necesidad- • Definir, aprobar, implementar, actualizar y/o realizar seguimiento a los indicadores de Seguridad de la Información mediante un proceso de mejora continua • Reportes realizados en el aplicativo Gestiona 360 o repositorio correspondiente, sobre el cumplimiento de la ejecución de controles, acciones de mejora, planes de acción o actividades resultantes de los riesgos de gestión, auditorias u otros en materia de Seguridad de la Información. • Envió de los reportes que durante el semestre fueron requeridos por entes externos e internos en materia de Seguridad de la información
B. Gestión de riesgos	3. Implementar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información Institucional, conforme a la metodología y lineamientos del DASCD	• Informe de resultados gestión de riesgos de Seguridad de la Información vigencia 2023 • Matriz de riesgos de seguridad de la información identificada, valorada, actualizada y aprobada mediante mejora continua –por cada proceso priorizado- • Reporte cuatrimestral en Formato Excel correspondiente al cumplimiento de los controles establecidos en la Matriz de Riesgos de seguridad de la información por cada Proceso del DASCD • Informe, actas de reunión y/o registros de acompañamiento a los procesos del DASCD en la identificación, valoración, actualización y aprobación de las Matrices de Riesgo de Seguridad de la información

Recuerde: *Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, se considera "Copia No Controlada". La versión vigente se encuentra publicada en el repositorio de documentos SIG del DASCD.*

ESTRATEGIA / EJE /FASE	ACTIVIDADES	PRODUCTOS ESPERADOS
		• Historia de usuario y/o acompañamiento funcional para desarrollar una herramienta de TI que consolide y sistematice la Matriz de Riesgos de Seguridad de la Información • Reporte de monitoreo y/o seguimiento a la Gestión del Plan de Tratamiento de Riesgos de Seguridad de la información institucional de la entidad
C. Concientización	4. Establecer el Plan de Comunicación y Sensibilización de Seguridad de la Información Institucional de la vigencia 2024 y desarrollar actividades encaminadas a la Toma de Conciencia, Educación y Formación en la Seguridad y Privacidad de la Información	• Plan de Comunicación y Sensibilización de Seguridad de la Información vigencia 2024 actualizado • Evidencias de las actividades de sensibilización al personal del DASCD, que fueron realizadas durante el trimestre conforme lo definido en el Plan de Comunicación y Sensibilización de S.I. 2024 • Evidencias de las sesiones, charlas o reuniones brindadas en el cuatrimestre por la Alta Consejería de las TIC, el MINTIC o entes externos en materia a seguridad de la información y en las cuales participo el DASCD • Elaboración de un curso E-Learning de seguridad de la información, cuyo público objetivo sea funcionarios y contratistas del DASCD
D. Implementación de controles	5. Realizar la actualización por procesos de la Matriz de Caracterización de Activos de Información -MCAI- 6. Realizar los reportes de Bases de Datos Personales sobre el aplicativo de la SIC - Registro Nacional de Bases de Datos -RNBD- 7. Implementar, mantener y fortalecer la aplicación de controles de Seguridad de la Información correspondientes al Modelo de Seguridad y Privacidad de la Información -MSPI- Institucional	• Matriz de Caracterización de Activos de Información -MCAI- actualizada –por cada proceso del DASCD- • Matriz de Caracterización de Activos de Información institucional revisada, consolidada y actualizada • Registro de Activos de Información, Índice de Información Clasificada y Reservada, y Esquema de Publicación de Información actualizados y publicados en el portal web • Historia de usuario y/o acompañamiento funcional para desarrollar una herramienta de TI que consolide y sistematice la Matriz de Caracterización de Activos de Información -MCAI- • Resultados de realizar una revisión, análisis y determinar si es posible realizar una depuración y/o actualización de las Bases de datos Personales del DASCD relacionadas en el aplicativo RNBD de la SIC.

Recuerde: *Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, se considera "Copia No Controlada". La versión vigente se encuentra publicada en el repositorio de documentos SIG del DASCD.*

ESTRATEGIA / EJE /FASE	ACTIVIDADES	PRODUCTOS ESPERADOS
		• Reporte ante el aplicativo RNBD de la SIC en donde se informen las reclamaciones realizadas por los titulares ante los operadores y/o responsables del tratamiento. • Resultado de revisión y análisis del procedimiento de tratamiento de datos personales y actualización del documento -si aplica la necesidad- • Reporte ante el aplicativo RNBD de la SIC en donde se informen las novedades relacionadas con actualizaciones, eliminación o creación de nuevas bases de datos. • Documentación del proceso de Seguridad de la Información definidos, revisados, actualizados, implementados y/o aprobados durante la vigencia 2024 mediante un proceso de mejora continua • Actualización de las políticas o lineamientos documentados sobre las copias de respaldo de la información • Reporte de resultado de verificación sobre los usuarios habilitados en el Directorio Activo, donde se realice comparación contra el reporte de SIDEAP de funcionarios y contratistas activos. De tal manera que se realice depuración de las cuentas que no han sido reportadas y que deben ser deshabilitadas, actualizadas o creadas por medio del proceso de solicitud de acceso a usuarios • Informe de revisión, análisis y/o diagnóstico de los requisitos de seguridad de la información para la planificación de la continuidad de negocio y/o la recuperación en caso de desastres. • Revisión, análisis, depuración, configuración de las políticas/reglas del Firewall • Solución y/o respuesta a requerimientos en materia de TI y Seguridad de la Información que hayan sido requeridas por el proceso de Gestión Documental en cuanto a la preservación digital a largo plazo. • Requerimiento al CSIRT Gobierno, ColCert o CSIRT sectorial para que realice

Recuerde: *Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, se considera "Copia No Controlada". La versión vigente se encuentra publicada en el repositorio de documentos SIG del DASCD.*

ESTRATEGIA / EJE /FASE	ACTIVIDADES	PRODUCTOS ESPERADOS
		análisis de vulnerabilidades de seguridad a los activos de información del DASCD • Normograma revisado y/o actualizado del proceso de Seguridad de la Información
E. **Gestión de incidentes**	8. Mantener y fortalecer la gestión de incidentes de seguridad y privacidad de la información institucional	• Resultados de la gestión cuatrimestral en relación a eventos o incidentes de seguridad de la información (En caso de requerirse) y/o resultados de la gestión sobre la identificación de brechas de seguridad de la información y/o propuestas de oportunidades de mejora • Evidencias de actividades de sensibilización al personal del DASCD, en materia a Gestión de Incidentes de Seguridad de la Información que se hayan realizado durante el semestre

Recuerde: *Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, se considera "Copia No Controlada". La versión vigente se encuentra publicada en el repositorio de documentos SIG del DASCD.*

7.2. CRONOGRAMA DE TRABAJO

Estas actividades han sido planteadas para desarrollarse de la siguiente forma:

PRODUCTO	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
A. LIDERAZGO DE SEGURIDAD DE LA INFORMACIÓN												
PLAN GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN actualizado a la vigencia 2024												
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN actualizado a la vigencia 2024												
Autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) actualizado, y/o aprobado por parte del Comité de Gestión y Desempeño Institucional												
Políticas de Seguridad de la Información revisadas, ajustadas y actualizadas -Según aplique su necesidad												
Definir, aprobar, implementar, actualizar y/o realizar seguimiento a los indicadores de Seguridad de la Información mediante un proceso de mejora continua												
Reportes realizados en el aplicativo Gestiona 360 o repositorio correspondiente, sobre el cumplimiento de la ejecución de controles, acciones de mejora, planes de acción o actividades resultantes de los riesgos de gestion, auditorias u otros en materia de Seguridad de la Información.												
Envio de los reportes que durante el semestre fueron requeridos por entes externos e internos en materia de Seguridad de la información												

Recuerde: *Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, se considera "Copia No Controlada". La versión vigente se encuentra publicada en el repositorio de documentos SIG del DASCD.*

B. GESTIÓN DE RIESGOS DE S.I.												
Informe de resultados gestión de riesgos de Seguridad de la Información vigencia 2023												
Matriz de riesgos de seguridad de la información identificada, valorada, actualizada y aprobada mediante mejora continua –por cada proceso priorizado-												
Reporte cuatrimestral en Formato Excel correspondiente al cumplimiento de los controles establecidos en la Matriz de Riesgos de seguridad de la información por cada Proceso del DASCD												
Informe, actas de reunión y/o registros de acompañamiento a los procesos del DASCD en la identificación, valoración, actualización y aprobación de las Matrices de Riesgo de Seguridad de la información												
Historia de usuario y/o acompañamiento funcional para desarrollar una herramienta de TI que consolide y sistematice la Matriz de Riesgos de Seguridad de la Información												
Reporte de monitoreo y/o seguimiento a la Gestión del Plan de Tratamiento de Riesgos de Seguridad de la información institucional de la entidad												
C. CONCIENTIZACIÓN												
Plan de Comunicación y Sensibilización de Seguridad de la Información vigencia 2024 actualizado												
Evidencias de las actividades de sensibilización al personal del DASCD, que fueron realizadas durante el trimestre conforme lo definido en el Plan de Comunicación y Sensibilización de S.I. 2024												
Evidencias de las sesiones, charlas o reuniones brindadas en el cuatrimestre por la Alta Consejería de las TIC, el MINTIC o entes externos en materia a seguridad de la información y en las cuales participo el DASCD												
Elaboración de un curso E-Learning de seguridad de la información, cuyo público objetivo sea funcionarios y contratistas del DASCD												

Recuerde: *Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, se considera "Copia No Controlada". La versión vigente se encuentra publicada en el repositorio de documentos SIG del DASCD.*

D. IMPLEMENTACIÓN DE CONTROLES												
Matriz de Caracterización de Activos de Información -MCAI- actualizada –por cada proceso del DASCD-												
Matriz de Caracterización de Activos de Información institucional revisada, consolidada y actualizada												
Registro de Activos de Información, Índice de Información Clasificada y Reservada, y Esquema de Publicación de Información actualizados y publicados en el portal web												
Historia de usuario y/o acompañamiento funcional para desarrollar una herramienta de TI que consolide y sistematice la Matriz de Caracterización de Activos de Información -MCAI-												
Resultados de realizar una revisión, análisis y determinar si es posible realizar una depuración y/o actualización de las Bases de datos Personales del DASCD relacionadas en el aplicativo RNBD de la SIC.												
Reporte ante el aplicativo RNBD de la SIC en donde se informen las reclamaciones realizadas por los titulares ante los operadores y/o responsables del tratamiento.												
Resultado de revisión y análisis del procedimiento de tratamiento de datos personales y actualización del documento -si aplica la necesidad-												
Reporte ante el aplicativo RNBD de la SIC en donde se informen las novedades relacionadas con actualizaciones, eliminación o creación de nuevas bases de datos.												
Documentación del proceso de Seguridad de la Información definidos, revisados, actualizados, implementados y/o aprobados durante la vigencia 2024 mediante un proceso de mejora continua												
Actualización de las políticas o lineamientos documentados sobre las copias de respaldo de la información												

Recuerde: *Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, se considera "Copia No Controlada". La versión vigente se encuentra publicada en el repositorio de documentos SIG del DASCD.*

Reporte de resultado de verificación sobre los usuarios habilitados en el Directorio Activo, donde se realice comparación contra el reporte de SIDEAP de funcionarios y contratistas activos. De tal manera que se realice depuración de las cuentas que no han sido reportadas y que deben ser deshabilitadas, actualizadas o creadas por medio del proceso de solicitud de acceso a usuarios												
Informe de revisión, análisis y/o diagnóstico de los requisitos de seguridad de la información para la planificación de la continuidad de negocio y/o la recuperación en caso de desastres.												
Revisión, análisis, depuración, configuración de las políticas/reglas del Firewall												
Solución y/o respuesta a requerimientos en materia de TI y Seguridad de la Información que hayan sido requeridas por el proceso de Gestión Documental en cuanto a la preservación digital a largo plazo.												
Requerimiento al CSIRT Gobierno, ColCert o CSIRT sectorial para que realice análisis de vulnerabilidades de seguridad a los activos de información del DASCD												
Normograma revisado y/o actualizado del proceso de Seguridad de la Información												
E. GESTIÓN DE INCIDENTES												
Resultados de la gestión cuatrimestral en relación a eventos o incidentes de seguridad de la información (En caso de requerirse) y/o resultados de la gestión sobre la identificación de brechas de seguridad de la información y/o propuestas de oportunidades de mejora												
Evidencias de actividades de sensibilización al personal del DASCD, en materia a Gestión de Incidentes de Seguridad de la Información que se hayan realizado durante el semestre												

Recuerde: *Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, se considera "Copia No Controlada". La versión vigente se encuentra publicada en el repositorio de documentos SIG del DASCD.*

8. MARCO NORMATIVO.

Las normas, regulaciones, leyes y/o lineamientos a considerar en lo referente a la Secretaría Distrital del Hábitat, la Comisión Distrital de Sistemas y el Ministerio de Tecnologías de la Información y las comunicaciones – MINTIC, son las siguientes:

Norma	Descripción
Decreto 680 de Agosto 31 2001	Por el Cual se modifica la Comisión Distrital de Sistemas.
Directiva Presidencial 02 de 2002	Respeto al derecho de autor y los derechos conexos, en lo referente a utilización de programas de ordenador (software).
Decreto 053 de 15 de febrero de 2002	Por el cual se crea el Comité para la implementación del Número Único de Emergencias y Seguridad del Distrito Capital, del cual forma parte el Secretario Técnico de la CDS.
Directiva Distrital 002 de Marzo 8 de 2002	Reglamenta la formulación de proyectos informáticos y de comunicaciones. El Alcalde Mayor asignó a la Comisión Distrital de Sistemas la función de evaluar la viabilidad técnica y la pertinencia de la ejecución de los proyectos informáticos y de comunicaciones de impacto interinstitucional o de costo igual o mayor a 500 SMLV, previa a la inscripción de los mismos ante el Departamento Administrativo de Planeación Distrital.
Acuerdo 057 de Abril 17 de 2002	Por el cual se dictan disposiciones generales para la implementación del sistema Distrital de Información - SDI -, se organiza la Comisión Distrital de Sistemas, y se dictan otras disposiciones.
Decreto 397 de 17 de septiembre de 2002	Delegar en el Secretario General de la Alcaldía Mayor de Bogotá las atribuciones conferidas al Alcalde Mayor en el Acuerdo 57 de 2002 como presidente de la Comisión Distrital de Sistemas, y las demás funciones que se requieran en el ejercicio de esta atribución.
Resolución 001 de Noviembre 7 de 2003	Por la cual se establece el reglamento interno de la Comisión Distrital de Sistemas. Derogado mediante Resolución 256 de 2008.
Acuerdo 308 del 9 de Junio de 2008	Por el cual se adopta el Plan de Desarrollo Económico, Social, Ambiental y de Obras Públicas para Bogotá, D. C., 2008 - 2012 "BOGOTÁ POSITIVA: PARA VIVIR MEJOR.
Acuerdo 130 de 7 de diciembre de 2004	Por medio del cual se establece la infraestructura integrada de datos espaciales para el Distrito Capital y se dictan otras disposiciones.

Recuerde: *Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, se considera "Copia No Controlada". La versión vigente se encuentra publicada en el repositorio de documentos SIG del DASCD.*

Norma	Descripción
Directiva 005 del 12 de Junio de 2005	Por medio de la cual se adoptan las Políticas Generales de Tecnología de Información y Comunicaciones aplicables al Distrito Capital.
Acuerdo 279 del 29 de Marzo de 2007	Dicta los lineamientos para la Política de Promoción y Uso del Software libre en el Sector Central, el Sector Descentralizado y el Sector de las Localidades del Distrito Capital.
Resolución 185 del 6 de Junio de 2007	Políticas de Conectividad para las Entidades del Distrito Capital.
Resolución 355 del 17 de Diciembre de 2007	Política específica de la Infraestructura de Datos Espaciales IDEC@.
Decreto 619 del 28 de Diciembre de 2007	Se establece la Estrategia de Gobierno Electrónico de los organismos y de las entidades de Bogotá, Distrito Capital y se dictan otras disposiciones.
Decreto Nacional 1151 del 14 de abril de 2008 y Manual para la implementación de la Estrategia de Gobierno en Línea de la República de Colombia	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones.
Decreto 185 del 17 de junio de 2008	Por el cual se prorroga el plazo para formular la Estrategia Distrital de Gobierno Electrónico de los organismos y de las entidades de Bogotá, Distrito Capital.
Decreto 296 de 2008	Por el cual se le asignan las funciones relacionadas con el Comité de Gobierno en Línea a la Comisión Distrital de Sistemas y se dictan otras disposiciones en la materia
Resolución 256 de 2008	Por la cual se establece el reglamento interno de la Comisión Distrital de Sistemas - C.D.S. deroga la resolución 001 de 2003
Decreto 316 DE 2008	Por medio del cual se modifica parcialmente el artículo 3°del Decreto Distrital 619 de 2007 que adoptó las acciones para el desarrollo de la Estrategia Distrital de Gobierno Electrónico.
Resolución 305 de 2008	Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materias de Tecnologías de la Información y Comunicaciones respecto al planeación, seguridad, democratización, calidad, racionalización de gasto, conectividad, infraestructura de Datos Espaciales y Software Libre
Resolución 378 de 2008	Por la cual se adopta la Guía para el diseño y desarrollo de sitios Web de las entidades y organismos del Distrito Capital.

Recuerde: *Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, se considera "Copia No Controlada". La versión vigente se encuentra publicada en el repositorio de documentos SIG del DASCD.*

Norma	Descripción
Ley 1266 de 2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Decreto 319 de 2011	Por el cual se designa el/la delegado/a del/a Alcalde/sa Mayor en la Comisión Distrital de Sistemas y se dictan otras disposiciones.
Decreto 203 de 2011	Por el cual se adopta el Mapa de Referencia como instrumento oficial de consulta para Bogotá, Distrito Capital.
Ley 1581 de 2012	Protección de datos personales, habeas data
La 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
Decreto 2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea, se reglamenta parcialmente la ley 1341 de 2009 y se dictan otras disposiciones+
Ley 1753 de 2015	Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 “Todos por un nuevo país
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones
Decreto 612 de 2018	“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”, donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.
Resolución 0500 de 2021	“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
	Manual de Gobierno Digital – MINTIC
	Modelo de Seguridad y Privacidad de la Información – MINTIC

Recuerde: *Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, se considera “Copia No Controlada”. La versión vigente se encuentra publicada en el repositorio de documentos SIG del DASCD.*

9. METODOLOGÍA

Por ser el DASCD una entidad del orden distrital debe cumplir con lineamientos ya establecidos por el MINTIC, el DAFP y la Alcaldía Mayor de Bogotá, como los son la Resolución 0500 de 2021, la Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública – DAFP, guías técnicas del MINTIC para el MSPI, controles ISO 27001:2013, también estándares ya implementados en los sistemas de Gestión como la ISO 31000. La metodología de tratamiento de riesgos DAFP y una serie de leyes que tienen que ver con el manejo de la información como son: datos abiertos, ley 1581 de octubre de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales", reglamentada por el Decreto Nacional 1377 de 2013; la ley 1712 de marzo de 2014 "Por medio de la cual se decreta la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.

Herramientas y metodología utilizadas:

- Resolución 0500 de 2021
- Anexo 1 – Modelo de Seguridad y Privacidad de la Información
- Instrumento de evaluación MSPI de MINTIC (Autodiagnóstico)
- Anexo A de la Norma ISO 27001:2013
- Modelo de operación (PHVA)
- Nivel de madurez MSPI
- Mejores prácticas de la industria.
- Lineamientos de MINTIC y la Alcaldía Mayor de Bogotá
- Solicitud de información
- Entrevistas
- Pruebas administrativas
- Selección de procesos misionales y críticos
- Guía para la administración del riesgo y el diseño de controles en entidades públicas

10. CONCEPTOS Y DEFINICIONES

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

- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- **Análisis de riesgos :** Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo (ISO/IEC 27000).

- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o Entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 1712 de 2014 - Art. 6)

- **Ciberdefensa:** Capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales. Implica el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética. (Decreto 338 de 2022 (marzo 8); MinTIC).

- **Confidencialidad:** Propiedad de la información de que no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados (Gestión inventario clasificación de activos e infraestructura critica Ver 04 - MinTIC).

- **Control:** Medida que permite reducir o mitigar un riesgo. (Guía para la administración del riesgo y el diseño de controles en entidades públicas Ver 5 - DAFP).

- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

  - **Dato público:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no están sometidas a reserva. (Decreto 1377 de 2013. Art. 3).

  - **Dato semiprivado:** Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios a que se refiere el Título IV de la presente ley. (Ley 1266 de 2008. Art. 3).

  - **Dato privado:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1266 de 2008. Art. 3).

- **Datos sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013. Art. 3).

- **Disponibilidad:** Propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona entidad o proceso autorizada cuando así lo requiera está, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso. (Gestión inventario clasificación de activos e infraestructura critica Ver 04 - MinTIC).

- **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3)

- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- **Gestión de Riesgo:** Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino logrando que la evaluación de los riesgos se convierta en una parte natural del proceso de planeación. (Guía MinTIC).

- **Incidente de seguridad de la información:** Un incidente de seguridad de la información es un evento no planificado o no deseado que afecta negativamente la seguridad de los sistemas de información de la entidad. Esto puede incluir ataques cibernéticos, robo de información, malware, phishing, ingeniería social, violaciones de datos y otras amenazas cibernéticas. La seguridad de la información se refiere a la protección de los datos y sistemas de una organización contra el acceso no autorizado, la divulgación, la modificación o la destrucción no autorizada de información, o una violación a una Política de Seguridad de la Información de la entidad. (ISO (International Organization for Standardization). (2013). ISO/IEC 27035-1:2016 Information technology – Security techniques – Information security incident management – Part 1: Principles of incident management. Recuperado de: https://www.iso.org/standard/44706.html).

- **Incidente de seguridad digital:** Ocurrencia de una situación que pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información o la información que el sistema procesa, almacena o transmite; o que constituye una violación a las

políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable. (Decreto 338 de 2022 (marzo 8); MinTIC).

- **Impacto:** Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo..

- **Información:** Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen; (Ley 1712 de 2014 - Art. 6).

- **Información pública:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal (Ley 1712 de 2014 - Art. 6).

- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

- **Infraestructura Cibernética (Ic):** Son las infraestructuras soportadas por Tecnologías de Información y Comunicaciones (TIC) o Tecnologías de Operación (TO). (Guía para la Identificación de Infraestructura Crítica Cibernética (ICC) de Colombia Primera Edición).

- **Infraestructura Crítica (IC) :** Son las infraestructuras estratégicas cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales. (Adaptación Ley 8/2011-Gobierno de España.).

- **Infraestructura Crítica Cibernética (ICC):** Son las infraestructuras estratégicas soportadas por Tecnologías de Información y Comunicaciones (TIC) o Tecnologías de Operación (TO), cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales. (Fuente Ministerio de Defensa.).

- **Infraestructura Estratégica (IE):** Son las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que se soporta el funcionamiento de los servicios esenciales. (Adaptación Ley 8/2011-Gobierno de España.).

- **Infraestructura Estratégica Cibernética (IEC):** Son las infraestructuras soportadas por Tecnologías de Información y Comunicaciones (TIC) y Tecnologías de Operación (TO), sobre las que se soporta el funcionamiento de los servicios esenciales. (Fuente Ministerio de Defensa.).

- **Integridad:** La integridad se refiere a la exactitud y completitud de la información (ISO 27000) esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción. (Gestión inventario clasificación de activos e infraestructura critica Ver 04 - MinTIC).

- **Mapa de Riesgos:** Documento con la información resultante de la gestión del riesgo. ().

- **Nivel de riesgo:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. (Guía para la administración del riesgo y el diseño de controles en entidades públicas Ver 5 - DAFP).

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

- **Plan de Continuidad de Negocio (PCN) :** Establece la continuidad de una organización desde múltiples perspectivas: infraestructura TIC, recursos humanos, mobiliario, sistemas de comunicación, logística, sistemas industriales, infraestructuras físicas, etc. Cada uno de estos ámbitos tendrá a su vez un plan de continuidad más específico, ya que no es lo mismo la inundación de un almacén de logística que el corte del suministro eléctrico en una sala de servidores.

- **Plan de Continuidad de Tecnología de la Información (PCTIC):** Según el NIST Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos, es un proceso integral de administración de riesgos que incluye la identificación de amenazas potenciales a las operaciones de TI, la evaluación de la importancia de las funciones de TI y la implementación de una estrategia de recuperación para garantizar la continuidad de las operaciones en caso de una interrupción." Esta definición destaca que un Plan de Continuidad de TI se centra en garantizar la continuidad de las operaciones de tecnología de la información en situaciones de interrupción o desastres. (Fuente: "NIST Special Publication 800-34, Contingency Planning Guide for Federal Information Systems," Instituto Nacional de Estándares y Tecnología (NIST), Estados Unidos.) ().

- **Plan de Recuperación de Desastres:** (DRP, por sus siglas en inglés, Disaster Recovery Plan) es un conjunto de procedimientos y estrategias diseñados para ayudar a una organización a recuperarse de manera rápida y eficiente después de un desastre o incidente grave que afecta sus sistemas de tecnología de la información y comunicaciones

(TIC). (Fuente: NIST (National Institute of Standards and Technology). (2012). NIST Special Publication 800-34 Revision 1: Contingency Planning Guide for Federal Information Systems. Recuperado de: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf) ().

- **Plan de Contingencia de TI :** Según el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos: "Un Plan de Contingencia de TI (IT Contingency Plan) es un conjunto de procedimientos que describen cómo una organización restaurará las operaciones de TI después de un evento disruptivo. Estos procedimientos también describen cómo la organización recuperará los datos necesarios para respaldar las operaciones críticas y cómo protegerá la integridad y la confidencialidad de esos datos." Un Plan de Contingencia de TI es esencial para ayudar a las organizaciones a prepararse para eventos inesperados que podrían afectar la disponibilidad de sus sistemas y datos. Estos planes incluyen medidas para la recuperación de sistemas, la gestión de datos, la continuidad de las operaciones y la mitigación de riesgos en el entorno de tecnología de la información. La fuente citada, el NIST, es una autoridad en estándares y buenas prácticas de seguridad de la información y tecnología, y su definición es ampliamente reconocida y utilizada en el campo de la gestión de la continuidad de negocio y la seguridad informática. ().

- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

- **Política de Administración del Riesgo:** Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo (NTC ISO31000 Numeral 2.4). La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos (NTC ISO31000).

- **Probabilidad:** se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

- **Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

- **Responsable del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art. 3).

- **Riesgo de Seguridad de la Información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de

información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **Riesgo de Seguridad digital:** Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de los objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos. (Guía para la administración del riesgo y el diseño de controles en entidades públicas Ver 5 - DAFP).

- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio impreso o digital. (ISO/IEC 27000).

- **Seguridad digital** Es la situación de normalidad y de tranquilidad en el entorno digital, a través de la apropiación de políticas, buenas prácticas, y mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades; que demanda la voluntad social y política de las múltiples partes interesadas. (Decreto 338 de 2022 (marzo 8); MinTIC).

- **Tratamiento de Datos Personales:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

Recuerde: *Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, se considera "Copia No Controlada". La versión vigente se encuentra publicada en el repositorio de documentos SIG del DASCD.*

CONTROL DE CAMBIOS:

VERSIÓN No.	FECHA	DESCRIPCIÓN DE LA MODIFICACIÓN
1.0	Julio 2018	Elaboración Plan de Seguridad y Privacidad de la Información DASCD
2.0	Diciembre 2018	Actualización e inclusión de cronograma, actualización de entregables y actualización de resultados.
3.0	Enero 2019	Actualización del cronograma de acuerdo con el plan de acción 2019
4.0	Diciembre 2019	Actualización del cronograma de acuerdo con el plan de acción 2019
5.0	Enero 2021	Actualización del documento de acuerdo con el autodiagnóstico realizado en 2020 y al plan de acción 2021
6.0	Enero 2022	Actualización del Plan de Seguridad y Privacidad de la Información, según las directrices de la resolución 0500 de 2021 y el plan de acción 2022
7.0	Marzo 2022	Adición del Seguimiento de las vulnerabilidades técnicas de seguridad digital (sección 7.1)
8.0	Enero 2023	Actualización del todo el documento en cumplimiento al Decreto 612-2018, el plan de acción 2023, y en relación con el producto tipo: PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN" emitido por el MinTIC
9.0	Enero 2024	Actualización general de todo el Documento en cumplimiento al Decreto 612-2018 y el plan de acción 2024

ELABORACIÓN, REVISIÓN Y APROBACIÓN:

ETAPA	NOMBRE Y CARGO
Elaboró / Actualizó	Cristhian Andrés Ríos Alayón – Profesional Especializado Oficina de Tecnologías de la Información y las Comunicaciones
Revisó	Luis Fernando Montero Lancheros– Jefe Oficina de Tecnologías de la Información y las Comunicaciones
Aprobó	Comité Institucional de Gestión y Desempeño
Declaramos que hemos revisado el presente documento y lo encontramos ajustado a las normas y disposiciones legales.	