PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Secretaría Distrital de Hacienda
Oficina de Análisis y Control de Riesgo

Tabla de contenido

CONTEXTO

La Secretaria Distrital de Hacienda – SDH, dando cumplimiento a lo establecido en el Decreto 612 de 2018, articulo 1, el cual adiciona al Capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, el siguiente artículo: "2.2.22.3.14. Integración de los planes institucionales y estratégicos al Plan de Acción. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año.

Por lo anterior la Secretaría Distrital de Hacienda, a través de la Resolución No. SHD-000014 del 29 de enero de 2019, creó el Comité Institucional de Gestión y Desempeño de la entidad y dictó las disposiciones para su funcionamiento.

Que, en cumplimiento de la citada normativa del orden nacional, el Distrito Capital expidió el Decreto Distrital 807 del 24 de diciembre de 2019, “Por medio del cual se reglamenta el Sistema de Gestión en el Distrito Capital”, y se dictan otras disposiciones”, y adoptó el Sistema de Gestión de qué trata el artículo 2.2.22.1.1 del Decreto Nacional 1083 de 2015, modificado por el artículo 1 del Decreto Nacional 1499 de 2017, a través de la implementación del Modelo Integrado de Planeación y Gestión –MIPG.

Que el artículo 4 del Decreto Distrital 807 de 2019, en concordancia con el artículo 2.2.22.1.5 del Decreto 1083 de 2015, señala que “El Sistema de Gestión se complementa y articula, entre otros, con los Sistemas Nacional de Servicio al Ciudadano, de Gestión de la Seguridad y Salud en el Trabajo, de Gestión Ambiental y de Seguridad de la Información. (...)”

Que el artículo 5 del Decreto Distrital 807 de 2019, en concordancia con el artículo 2.2.22.3.2 del Decreto Nacional 1083 de 2015, definió el Modelo Integrado de Planeación y Gestión - MIPG como "(...) el marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio”.

Teniendo en cuenta lo anterior, conforma el presente documento dando cumplimiento a lo establecido en el Decreto 612 de 2018, actualizando el Plan de implementación de Seguridad y Privacidad de la Información al interior de la Secretaria Distrital de Hacienda, de Comité Institucional de Gestión y Desempeño.

OBJETIVO GENERAL

Establecer las actividades que están contempladas para la implementación del sistema de gestión de seguridad de la información incluyendo lo relacionado con el tratamiento de datos personales; basados en el estándar ISO 27001:2022, en el marco del Plan Estratégico de Seguridad de la Información.

OBJETIVOS ESPECÍFICOS

1. Avanzar en la implementación y apropiación del Modelo de Seguridad y Privacidad de la Información MSPI, que permita salvaguardar la información tanto física como digital.
2. Asesorar a las dependencias en la gestión de los riesgos de seguridad de la información y dar cumplimiento normativo.
3. Fortalecer la cultura organizacional a través de la concienciación y apropiación de la seguridad de la información y la seguridad digital.
4. Dar cumplimiento a los requisitos legales y normativos en materia de seguridad de la información, seguridad digital y protección de la información personal.
5. Dar lineamientos que permitan establecer mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información de la Secretaría Distrital de Hacienda.
6. Certificar el sistema de gestión de seguridad de la información de la SDH bajo el estándar ISO 27001:2022.

ALCANCE

La Secretaría Distrital de Hacienda, adopta, establece, implementa, opera, verifica y mejora el Sistema de Gestión de Seguridad de la Información (SGSI), para todos los procesos; estratégicos, misionales, soporte y control, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de la información, así mismo dar cumplimiento a la normatividad aplicable a la entidad.

ACCIONES ESPECIFICAS Y/O PROYECTOS O PROGRAMAS

COMPONENTES	PROYECTO	PRODUCTOS ESPERADOS
Liderazgo de seguridad de la información	**PROYECTO 1:** Desarrollar e implementar el sistema de gestión de seguridad de la información (continuación)	• Actualización del diagnóstico seguridad de la información con la herramienta provista por el ministerio TIC. • Auditoria de precertificación
	PROYECTO 2: Construir matriz de roles y perfiles para los sistemas de información (Bogdata / SiCapital) , alineada con realidad de la operación de los procesos y los perfiles de los cargos	• Estructura para matriz de roles definida • Matriz de Roles y perfiles

Concientización	**PROYECTO 1:** Desarrollar e implementar una estrategia transversal de sensibilización en gestión de seguridad de la información.	• Plan de Sensibilización • Jornadas de sensibilización a todo el personal. • Cursos especializados - Formación de auditores en ISO 27001 • Resultado de evaluaciones de conocimiento.
Implementación de controles	**PROYECTO 1:** Diseño e implementación de los controles requeridos por parte de las dependencias responsables para cada una de las categorías: **CONTROLES TECNOLÓGICOS** (DIT) **CONTROLES ORGANIZACIONALES** (SGD, OACR, DGC, DIT, DJ, OCI) **CONTROLES PERSONAS** (STH, SAC, OCDI, OCI) **CONTROLES FÍSICOS** (SAF, SGD, STH, DIT) **PROYECTO 2:** Implementar una estrategia de recuperación de servicios de Bogdata y SICapital, que responda a las necesidades de las áreas de negocio en el marco del Plan de Continuidad de Negocio de la entidad	• Inventario detallado de controles a implementar • Controles implementados en los procesos de acuerdo con el anexo A de la ISO27001 • Seguimiento en la implementación • Estrategia implementada
Gestión de incidentes	**PROYECTO 1:** Implementación de un esquema de monitoreo en línea a través de un SOC que permita identificar alertas en tiempo real de situaciones de ataque o explotación de vulnerabilidades en los sistemas de información y reaccionar de manera oportuna a las mismas **PROYECTO 2:** Analisis de vulnerabilidades.	• Implementación del SOC • Informe de resultados de gestión del SOC. • Casos de uso a ser implementados por el SOC. • Resultado del análisis de vulnerabilidades

CALENDARIO O CRONOGRAMA DE ACTIVIDADES (FECHA, RESPONSABLE, METAS, RECURSO)

COMPONENTE	PROYECTO	PRODUCTOS ESPERADOS	AÑO 2025 / TRIMESTRE			
			1	2	3	4
Liderazgo de seguridad de la información	Desarrollar e implementar una política de seguridad	Actualización del diagnóstico seguridad de la información con la herramienta provista por el ministerio TIC				
		Preauditoria de certificación				
	Construir matriz de roles y perfiles para los sistemas de información (Bogdata / SiCapital), alineada con realidad de la operación de los procesos y los perfiles de los cargos.	Estructura para matriz de roles definida				
		Desarrollo de matrices roles y perfiles				
Concientización	Desarrollar e implementar una estrategia transversal de sensibilización en gestión de seguridad de la información.	Plan de Sensibilización				
		Jornadas de sensibilización a todo el personal				
		Cursos especializados en Auditor interno y Auditor líder en ISO 27001, a través del PIC de la entidad, liderado por la subdirección de talento humano, con el cual se extienda la capacitación del grupo de auditores internos actuales liderados por la OAP, para que cuenten con entrenamiento certificado en ISO 27001:2022.				
		Resultado de evaluaciones de conocimiento				
Implementación de controles	Diseño e implementación de los controles con las áreas estén involucradas con los siguientes grupos: CONTROLES TECNOLÓGICOS (DIT) CONTROLES ORGANIZACIONALES (SGD, OACR, DGC, DIT, DJ, OCI) CONTROLES PERSONAS (STH, SAC,OCDI, OCI) CONTROLES FÍSICOS (SAF, SGD, STH, DIT)	Inventario detallado de controles a implementar				
		Controles implementados en los procesos de acuerdo con el anexo A de la ISO27001				
		Seguimiento en la implementación				
		Actualizar la matriz de riesgos de acuerdo con el resultado de la implementación.				
	Implementación de la estrategia de recuperación de servicios de Bogdata y SICapital, por parte de la DI. , a través de un estudio de mercado, con el fin de determinar el costo de la implementación y reorganizar el recurso aprobado en la DIT para la vigencia y dar cumplimiento con la implementación del Plan de Continuidad de Negocio de la entidad	Estudio de mercado – estrategia de continuidad tecnológica				
		Implementación de estrategias de continuidad tecnológica de definición interna, que cumplan con necesidades de negocio establecidas en el BIA				
		Implementación de la estrategia definida con contratación externa				
Gestión de incidentes		Proceso contractual SOC				

	Implementación de un esquema de monitoreo en línea a través de un SOC que permita identificar alertas en tiempo real de situaciones de ataque o explotación de vulnerabilidades en los sistemas de información y reaccionar de manera oportuna a las mismas	Implementación del SOC				
		Informe de resultados de gestión del SOC.				
		Casos de uso a ser implementados por el SOC.				
	Analisis de vulnerabilidades.	Proceso contractual				
		Ejecución análisis de vulnerabilidades				

INDICADORES DE EVALUACIÓN / SEGUIMIENTO

Actividad	Indicador
Medición del estado de implementación de la política de Seguridad de la Información	Una actualización del autodiagnóstico en el año
Construcción de matriz de roles y perfiles para los sistemas de información (Bogdata / SiCapital), alineada con realidad de la operación de los procesos y los perfiles de los cargos.	Número de matrices de roles definidas en el año / Número de matrices planeadas para el año
Desarrollar e implementar una estrategia transversal de sensibilización en gestión de seguridad de la información.	No. Funcionarios evaluados con resultados por encima de 70% / funcionarios evaluados
Diseño e implementación de controles	1 inventario de controles (hoja de ruta) No de controles implementados / No controles planeados para implementar en el año
Implementación de un esquema de monitoreo en línea a través de un SOC que permita identificar alertas en tiempo real de situaciones de ataque o explotación de vulnerabilidades en los sistemas de información y reaccionar de manera oportuna a las mismas	Un centro de operaciones de seguridad SOC implementado
Analisis de vulnerabilidades.	Un documento resultado del analisis de vulnerabilidades

PRESUPUESTO / PROVISIÓN DE RECURSOS

Con base a los proyectos definidos en el cronograma de actividades, se debe generar el presupuesto aproximado por cada vigencia para la Oficina de Analisis y Control de Riesgo, según los proyectos establecidos y presentarlo a la Alta Dirección para las consideraciones y viabilidad pertinentes:

Dirección	Tipo PPTO	Estado	Grupo de Compras (Dirección)	Material (Código UNSPSC)	Posición presupuestaria
Oficina de Análisis y Control de Riesgo	PAA	Aún no	5	81111808	O21202020090292913

Nombre Pospre	Vr. 2025 Final	Vr. Inicial	Modalidad de contratación	Objeto	Dependencia Destino
1000004933	$ 160.000.000	$ 160.000.000	Mínima cuantía	Prestar los servicios para la realización de pruebas de análisis de vulnerabilidades, pruebas de intrusión digital y física (Ethical Hacking), pruebas de ingeniería social, análisis de Código estático y dinámico y servicio de Red Team.	50001005
Por definir	$ 40.000.000	$ 40.000.000	Mínima cuantía	Prestar servicios para una preauditoria del sistema de gestión de seguridad de la información para a SDH	50001005

SEGUIMIENTO AL PLAN *(Esta sección aplicará para futuros seguimientos, de acuerdo con el cronograma y lineamientos establecidos para la vigencia)*

Utilice este título para relacionar los seguimientos considerados en cuanto al avance la implementación y ejecución del plan. Se sugiere la siguiente estructura.

ACTIVIDADES	FECHA O PERIODO DE CORTE O SEGUIMIENTO	PORCENTAJE DE AVANCE	DESCRIPCIÓN DEL AVANCE	ESTADO DE LA ACCIÓN	OBSERVACIONES
Medición del estado de implementación de la política de Seguridad de la Información	Anual				
Construcción de matriz de roles y perfiles para los sistemas de información (Bogdata / SiCapital), alineada con realidad de la operación de los procesos y los perfiles de los cargos.	Trimestral				
Desarrollar e implementar una estrategia transversal de sensibilización en gestión de seguridad de la información.	Semestral				
Diseño e implementación de controles	Trimestral				
Implementar una estrategia de recuperación de servicios de Bogdata y SICapital, que responda a las necesidades de las áreas de negocio en el marco del Plan de Continuidad de Negocio de la entidad	Anual				
Implementación de un esquema de monitoreo en línea a través de un SOC que permita identificar alertas en tiempo real de situaciones de ataque o explotación de vulnerabilidades en los sistemas de información y reaccionar de manera oportuna a las mismas	Anual				
Analisis de vulnerabilidades.	Anual				

En caso de usar un formato aparte para realizar el seguimiento, relacionar el enlace para la consulta de dicho avance o generar el anexo correspondiente. (Borre esta descripción cuando utilice el formato)