PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Secretaría Distrital de Hacienda
Oficina de Análisis y Control de Riesgo

Tabla de contenido

CONTEXTO

La Secretaría 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 Secretaría Distrital de Hacienda, de Comité Institucional de Gestión y Desempeño.

OBJETIVO GENERAL.

Establecer las actividades de Seguridad y Privacidad de la Información, que están contempladas en el plan de trabajo de la Oficina de Análisis y Control de Riesgo - OACR, alineadas con la NTC/IEC ISO 27001, resolución SDH - 000172 de 2022, Política de seguridad de la información y seguridad digital de la Secretaría Distrital de Hacienda.

OBJETIVOS ESPECÍFICOS

1. Definir, reformular y formalizar los elementos normativos sobre los temas de protección de la información.
2. Gestionar los riesgos de seguridad y privacidad de la información, Seguridad Digital y continuidad de la operación de manera integral.
3. Mitigar los incidentes de Seguridad y Privacidad de la Información, Seguridad Digital de forma efectiva, eficaz y eficiente.
4. Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, legalidad, confiabilidad, continuidad y no repudio de la información del de la Secretaría Distrital de Hacienda.
5. Definir los lineamientos necesarios para el manejo de la información tanto física como digital en el marco de una gestión documental basada en Seguridad y Privacidad de la Información.
6. Generar conciencia para el cambio organizacional requerido para la apropiación de la Seguridad y Privacidad de la Información como eje transversal de la Secretaría Distrital de Hacienda.
7. Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la información, seguridad digital y protección de la información personal.

ALCANCE

El presente documento aplica a todo el modelo de operación de la Secretaría Distrital de Hacienda, dando cumplimiento a lo establecido en el Decreto 612 de 2018, a la Política de Gobierno Digital y su Modelo de Seguridad y Privacidad de la Información alineado con la NTC/IEC ISO 27001, así como la estrategia de Seguridad Digital del Estado Colombiano.

ACCIONES ESPECÍFICAS Y/O PROYECTOS O PROGRAMAS

Actividad	Actividades Secundarias
Actualización de la política de seguridad de la información por cambio del estándar ISO 27001	a. Adquisición de normas técnicas b. Documento borrador de política c. Socialización de política en la entidad d. Solicitud de cambio de resolución e. Actualización de documento en MIGEMA
Actualización de la declaración de aplicabilidad	a Actualización de la declaración de aplicabilidad b Presentación y aprobación de la declaración en el comité de gestión institucional c Actualización de documento en MIGEMA
Actualización de la política de tratamiento de datos personales de la SDH.	a. Revisión normativa b. Documento actualizado de la política de seguridad de la información c. Documento borrador de política de tratamiento de datos personales d. Socialización de política en la entidad

	e. Realizar ajustes de ser necesario. f. Solicitud de cambio de resolución g. Actualización de documento en MIGEMA
Actualización del formato de inventario de activos de información	a. Actualizar el formato de inventario b. Elaborar guia para el diligenciamiento del inventario.
Actualización del inventario de activos de información	a. Actualizar el inventario de activos de información de 30 áreas de la entidad durante el segundo, tercero y cuarto trimestre de la vigencia. b. Actualizar el índice de información clasificada y reservada. c. Publicar el inventario de activos de información y el índice de información clasificada y reservada en la sede electrónica de la SDH y en el portal de datos abiertos.
Actualización general de la matriz de riesgos de seguridad de la información	a. Actualización de controles con los relacionados en la norma NTC/ISO 27001:2022. b. Ajustar los riesgos amenazas y vulnerabilidades de la matriz. c. Actualizar los riesgos identificados en análisis de vulnerabilidades realizado en la vigencia 2023.
Autodiagnóstico de seguridad de la información	a. Realizar la actualización de la herramienta de análisis GAP, ajustándola a los controles establecidos en la NTC/ISO 27001:2022. a. Incluir controles de ciberseguridad del estándar ISO 27032, para identificación de riesgos cibernéticos. b. Incluir controles relacionados con el framework de ciberseguridad ISO 27110, “Tecnología de información, la ciberseguridad y la protección de la privacidad” c. Revisar mapeo de las mejores prácticas del framework de la NIST. b. Realizar el análisis de brechas de la SDH con la nueva herramienta ajustada.
Definir lineamientos de seguridad de la información para la Anonimización de datos personales	a. Incluir los lineamientos de seguridad de la información para la Anonimización de datos personales en el manual de seguridad de la información. b. Socialización del manual de seguridad de la información en la entidad c. Realizar ajustes de ser necesario. d. Solicitud actualización de documento en MIGEMA
Monitoreo de controles	a. Identificar los riesgos críticos y altos b. Identificar los controles asociados a dichos riesgos que serán sujeto de revisión, de acuerdo con la fórmula establecida para muestreo c. Solicitar evidencias a los responsables de controles sujetos de evaluación. d. Revisar las evidencias aportadas por las áreas e. Elaborar los informes finales. f. Actualizar la matriz de riesgos de acuerdo con el resultado del análisis de efectividad de los controles. (De ser necesario).
Capacitacion y sensibilización	a. Diseño del plan de sensibilización de la gestión integral de riesgo - OACR - 2024 b. Evaluación de conocimiento de la gestión integral de riesgo - OACR - 2024

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

Actividad	Meta	Responsable	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
Actualización de la declaración de aplicabilidad	Un documento	Juan Gabriel Prieto Otavo												
Actualización de la política de seguridad de la información por cambio del estándar ISO 27001	Un documento	Juan Gabriel Prieto Otavo												
Actualización de la política de tratamiento de datos personales de la SDH.	Un documento	Juan Gabriel Prieto Otavo												
Actualización del formato de inventario de activos de información	Un documento	Danilo Santamaria												
Actualización del inventario de activos de información	30 inventarios actualizados durante el segundo, tercer y cuarto trimestres del 2024	Danilo Santamaria												
Actualización general de la matriz de riesgos de seguridad de la información.	Una matriz	Danilo Santamaria												
Autodiagnóstico de seguridad de la información	Resultado del análisis GAP de la SDH	Juan Gabriel Prieto Otavo												
Definir lineamientos de seguridad de la información para la Anonimización de datos personales	Un documento	Juan Gabriel Prieto Otavo												
Monitoreo de controles	Tres documentos de monitoreo de controles	Danilo Santamaria												
Capacitacion y sensibilización	Evaluación de conocimiento	Juan Gabriel Prieto Otavo												

INDICADORES DE EVALUACIÓN / SEGUIMIENTO

Actividad	Indicador
Actualización de la declaración de aplicabilidad	No. de declaraciones de aplicabilidad actualizadas
Actualización de la política de seguridad de la información por cambio del estándar ISO 27001	No. De documentos a actualizados
Actualización de la política de tratamiento de datos personales de la SDH.	No. De documentos a actualizados
Actualización del formato de inventario de activos de información	No. De inventarios actualizados
Actualización del inventario de activos de información	No. de inventarios realizados / No. De áreas a actualizar el inventario de activos durante la vigencia
Actualización general de la matriz de riesgos de seguridad de la información.	No. De actualizaciones / 4
Autodiagnóstico de seguridad de la información	No. De Actualizaciones del autodiagnóstico / 1
Definir lineamientos de seguridad de la información para la Anonimización de datos personales	No. De documentos a actualizar
Monitoreo de controles	No. controles / No. Controles Críticos
Capacitacion y sensibilización	No. De evaluaciones de conocimiento

PRESUPUESTO / PROVISIÓN DE RECURSOS

La norma técnica ISO/NTC 27001 Fue actualizada a finales del año 2022, y fue liberada por el ICONTEC a principios del 2023, y se constituye esta norma y otras adicionales de la familia ISO 27000 como insumo para hacer la actualización de la política y manual de seguridad de la información.

Dirección	Tipo PPTO	Estado	Grupo de Compras (Dirección)	Material (Código UNSPSC)	Posición presupuestaria
Oficina de Análisis y Control de Riesgo	PAA	Aprobado	5	81112202	O21202020090292913

Nombre Pospre	Vr. 2024 Final	Vr. Inicial	Modalidad de contratación	Objeto	Dependencia Destino
Servicios de educación para la formación y el trabajo	$ 3.000.000	$3.000.000	Contratación Directa	Adquisición de Estándares 27000 adquisición de los estándares NTC – Norma Técnica Colombiana del ICONTEC para la actualización de la política y manual de seguridad de la información de la Secretaría Distrital de Hacienda	50001005

SEGUIMIENTO AL PLAN

ACTIVIDADES	FECHA O PERIODO DE CORTE O SEGUIMIENTO	PORCENTAJE DE AVANCE	DESCRIPCIÓN DEL AVANCE	ESTADO DE LA ACCIÓN	OBSERVACIONES
Actualización de la declaración de aplicabilidad	Anual				
Actualización de la política de seguridad de la información por cambio del estándar ISO 27001	Anual				
Actualización de la política de tratamiento de datos personales de la SDH.	Anual				
Actualización del formato de inventario de activos de información	Anual				
Actualización del inventario de activos de información	Anual				
Actualización general de la matriz de riesgos de seguridad de la información.	Trimestral				
Autodiagnóstico de seguridad de la información	Anual				
Definir lineamientos de seguridad de la información para la Anonimización de datos personales					
Monitoreo de controles	Trimestral				
Capacitacion y sensibilización	Semestral				