PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA SECRETARIA DISTRITAL DE HACIENDA

Líder de Política: SUBSECRETARIA GENERAL
Diana Consuelo Blanco Garzón

Secretaría Distrital de Hacienda
Fecha de corte: 31 de enero de 2021.

BOGOTÁ

Contenido

INTRODUCCIÓN.

La Secretaria Distrital de Hacienda – SDH, dando cumplimiento a lo establecido en el Decreto 612 de 2018, articulo 1, el cual adicionar 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, aprobado mediante acta de la sesión del 27 de enero de 2021de Comité Institucional de Gestión y Desempeño.

1. OBJETIVO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Establecer las actividades que están contempladas en Seguridad y Privacidad de la Información, alineadas con la NTC/IEC ISO 27001:2013, la Política de Seguridad Digital y Continuidad del servicio, de la Secretaria de Hacienda Distrital.

2. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA SECRETARIA DISTRITAL DE HACIENDA.

La Secretaria Distrital de Hacienda, mediante la adopción e implementación del Subsistema de Seguridad y Privacidad de la Información enmarcado en el Sistema de Gestión de Seguridad de la información, protege, preserva y administra la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información que circula en el mapa de procesos, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales previniendo así incidentes y dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información, propendiendo así por el acceso, uso efectivo y apropiación masiva de las TIC, a través de políticas y programas, para mejorar la calidad de vida de cada colombiano y el incremento sostenible del desarrollo del país.

2.1. OBJETIVOS ESPECIFICOS DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA SECRETARIA DISTRITAL DE HACIENDA.

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 Secretaria 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 Secretaria 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.

3. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Aplica a todos los niveles de la Secretaria Distrital de Hacienda, a todos sus funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones y las que la Secretaria Distrital de Hacienda compartan, utilicen, recolecten, procesen, intercambien o consulten su información, así como a los Entes de Control, Entidades relacionadas que accedan, ya sea interna o externamente a cualquier tipo de información, independientemente de su ubicación. Así mismo, esta lo dispuesto en este documento y su implementación aplica a toda la información creada, procesada o utilizada por el de la Secretaria Distrital de Hacienda, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

4. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Las funciones del comité de Seguridad de la Información son tratadas a través del Comité Institucional de Gestión y Desempeño de la entidad creado mediante Resolución No. SHD-000014 del 29 de enero de 2019.

5. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El Plan de implementación para la dimensión de Seguridad y Privacidad de la Información comprende el desarrollo de las siguientes actividades para la vigencia 2021.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA SECRETARIA DE HACIENDA DISTRITAL.					
Gestión	**Actividades**	**Tareas**	**Área responsable**	**Fechas Programación Tareas**	
				Fecha Inicio	**Fecha Final**
Activos de Información	Revisar los lineamientos para el levantamiento de activos de información	Actualización de metodología e instrumento de levantamiento de activos de información	Subdirección de Gestión Documental / Oficina de Análisis y Control del Riesgo / Oficial de Seguridad de la Información	feb-21	abr-21
	Levantamiento Activos de Información	Revisar y fortalecer la guía de activos de Información.	Subdirección de Gestión Documental / Oficina de Análisis y Control del Riesgo / Oficial de Seguridad de la Información	feb-21	jun-21
		Validar activos de información en el instrumento levantado en la vigencia anterior	Subdirección de Gestión Documental / Oficina de Análisis y Control del Riesgo / Oficial de Seguridad de la Información	jun-21	jun-21
		Identificar nuevos activos de información en cada dependencia	Subdirección de Gestión Documental / Oficina de Análisis y Control del Riesgo / Oficial de Seguridad de la Información	jun-21	jun-21
		Revisar los instrumentos de activos de Información y realimentar a las áreas con las modificaciones.	Subdirección de Gestión Documental / Oficina de Análisis y Control del Riesgo / Oficial de Seguridad de la Información	jul-21	jun-21

		Realizar correcciones a los instrumentos de activos de Información, Cambios físicos de la ubicación de activos de información	Subdirección de Gestión Documental / Oficina de Análisis y Control del Riesgo / Oficial de Seguridad de la Información	jul-21	jun-21
		Realizar informe de actualización a los activos de información por alguna de las siguientes novedades: Actualizaciones al proceso al que pertenece el activo, Adición de actividades al proceso, Inclusión de un nuevo activo, Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados, Materialización de riesgos que cambien la criticidad del activo.	Subdirección de Gestión Documental / Oficina de Análisis y Control del Riesgo / Oficial de Seguridad de la Información	jul-21	dic-21
	Reporte Datos Personales	Solicitar la información de las bases de datos que contengan datos personales con el fin de realzar el reporte ante la SIC 2021.	Subdirección de Gestión Documental / Oficina de Análisis y Control del Riesgo / Oficial de Seguridad de la Información	ago-21	oct-21
Gestión de Riesgos	Revisión de lineamientos de riesgos	Revisión de la política y metodología de gestión de riesgos	Oficina de Análisis y Control del Riesgo / Oficial de Seguridad de la Información	ago-21	ago-21
	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital	Revisión de la matriz de riesgos elaborada la vigencia anterior con el fin de Identificar, Análizar y Evaluar los Riesgos de Seguridad y Privacidad de la Información y Seguridad Digital	Oficina de Análisis y Control del Riesgo / Oficial de Seguridad de la Información	ago-21	ago-21
		Realimentación, revisión y verificación de los riesgos identificados (Ajustes)	Oficina de Análisis y Control del Riesgo / Oficial de Seguridad de la Información	sept-21	sept-21
	Aceptación de Riesgos Identificados	Aceptación, aprobación Riesgos identificados y planes de tratamiento	Oficina de Análisis y Control del Riesgo / Oficial de Seguridad de la Información	sept-21	sept-21
	Seguimiento Fase de Tratamiento	Seguimiento Estado planes de tratamiento de riesgos identificados y verificación de evidencias	Oficina de Análisis y Control del Riesgo / Oficial de Seguridad de la Información	sept-21	sept-21
	Evaluación de riesgos residuales	Particiopar en la cosntrucción del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	Oficina de Análisis y Control del Riesgo / Oficial de Seguridad de la Información	sept-21	sept-21

	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Oficina de Análisis y Control del Riesgo / Oficial de Seguridad de la Información	nov-21	dic-21
Gestión de Incidentes de Seguridad de la Información	Publicar y Socializar el procedimiento actualizado de incidentes de seguridad de la información	Incluir dentro del plan de carateridación de la DIT, el procedimiento de gestión de incidentes de seguridad de la información.	DIT / Oficial de Seguridad de la Información	mar-21	abr-21
		Socializar el procedimiento a los soportes en sitio y Mesa de Servicios, indicando los cambios en el procedimiento	DIT / Oficial de Seguridad de la Información	abr-21	sept-21
		Socializar el procedimiento a los colabores de la Entidad.	DIT / Oficial de Seguridad de la Información	abr-21	sept-21
	Gestionar los incidentes de Seguridad de la Información identificados	Gestionar los incidentes de seguridad de la información de acuerdo a lo establecido en el procedimiento definido.	DIT / Oficial de Seguridad de la Información	jun-21	nov-21
	CSIRT y/o COLCERT	Socializar los boletines informativos de seguridad, Integrar con CSIRT de Gobierno	Oficial de Seguridad de la Información	mar-21	dic-21
	Eventos/vulnerabilidades	Realizar seguimiento a los informes de eventos y vulnerabilidades asociados a SGSI	DIT / Oficial de Seguridad de la Información	jun-21	dic-21
Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Elaborar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Elaborar el documento del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Subdirección del Talento Humano / Oficial de Seguridad de la Información	jun-21	dic-21
		Publicar y Socializar el Plan de Gestión de Cultura Organizacional en Apropiación del SGSI con los gestores de procesos	Subdirección del Talento Humano / Oficial de Seguridad de la Información	jun-21	dic-21
Matriz de verificación de Requisitos Legales de Seguridad de la Información	Creación de la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Crear la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Dirección Juridica / Oficial de Seguridad de la Información	may-21	dic-21
Plan de Continuidad del Negocio	Ejecutar el proceso contractual que nos permita definir el plan de continuidad del negocio de la Secretaria Distrital de Hacienda	Construir el documentos con los requerimientos tecnicos para la ejecución del contrato.	Oficial de Seguridad de la Información	feb-21	dic-21
		Publicación, adjudicación y seguimiento del proseso contractual	Oficial de Seguridad de la Información	feb-21	dic-21
Politica de Seguridad y Privacidad de la Información	Revisión Manual Políticas de Seguridad de la Información y Resolución de Seguridad de la Información	Actualizar Manual Políticas de Seguridad de la Información y Resolución de Seguridad de la Información.	Oficial de Seguridad de la Información	feb-21	dic-21
		Informe cumplimiento de los controles por dominios asignados (Políticas, Manual, etc.)	Oficial de Seguridad de la Información	feb-21	abr-21

Gobierno Digital	Gobierno Digital	Actualizar el documento de autodiagnóstico de la entidad en la implementación de Seguridad y Privacidad de la Información.	DIT / Oficial de Seguridad de la Información	mar-21	dic-21
		Revisar y alinear la documentación del SGSI de la Entidad al MSPI, de acuerdo con la Normatividad vigente.	DIT / Oficial de Seguridad de la Información	feb-21	mar-21
		Revisar el avance de implementación de Seguridad Digital en la Entidad	Oficial de Seguridad de la Información	feb-21	mar-21
		Reuniones de Socialización de los avances de la implementación de Seguridad Digital y la Estrategia del Modelo de Seguridad y Privacidad de la información	Oficial de Seguridad de la Información	mar-21	mar-21
Polítia Nacional de Confianza y Seguridad Digital	CCOC	Cumplimiento requerimientos infraestructuras críticas del gobierno	Oficial de Seguridad de la Información	mar-21	dic-21
Auditorías Internas y Externas	Participación en las auditorías internas y externas de la norma ISO 27001:2013	Participar en las auditorías internas y externas de la norma ISO 27001:2013 programadas	Oficina de Control Interno / Oficial de Seguridad de la Información	feb-21	dic-21
Indicadores SGSI	Provisión de información a los indicadores de medición del SGSI	Formular, Implementar y actualizar los indicadores del SGSI	Oficial de Seguridad de la Información	feb-21	dic-21
		Reportar indicadores	Oficial de Seguridad de la Información	feb-21	dic-21
Vulnerabilidades	Definir lineamientos para ejecutas las pruebas de vulnerabilidades y pentest	Definir los lineamientos y el alcance para la realización de pruebas de vulnerabilidades para el proceso contractaul a ejecutar en esta vigencia.	Oficial de Seguridad de la Información	feb-21	jun-21
	Contratar Análisis de Vulnerabilidades y Pentest	Definir estudios previos y procesos de contratación para realizar el pentest y análisis de vulnerabilidades teniendo en cuenta el alcance y metodología	DIT / Oficial de Seguridad de la Información	jul-21	dic-21
	Ejecutar las pruebas de vulnerabilidades y pentest	Ejecución de las pruebas de vulnerabilidades y pentest de acuerdo al alcance determinado en el proceso contractual	DIT / Oficial de Seguridad de la Información	abr-21	abr-21
	Ejecutar plan de remediación	Ejecutar el plan de remediación sobre los sistemas y plataforma de acuerdo a los resultados del análisis de vulnerabilidades y pentest	DIT / Oficial de Seguridad de la Información	may-21	jul-21

Protección de datos personales	Recolectar bases de datos	Elaborar y emitir un memorando para la recolección de bases de datos personales de acuerdo a los estándares emitidos por la SIC	DIT / Oficial de Seguridad de la Información	ago-21	ago-21
	Revisión de bases de datos	Revisar y realimentar la información recolectada por las áreas para el registro de las bases de datos	DIT / Oficial de Seguridad de la Información	nov-21	dic-21
	Registro y actualización de las bases de datos	Registrar o actualizar las bases de datos teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de información	DIT / Oficial de Seguridad de la Información	nov-21	dic-21

6. DOCUMENTOS DE REFERENCIA

- **Constitución Política de Colombia.** Artículo 15.
- **Ley 44 de 1993.** Por la cual se modifica y adiciona la Ley 23 de 2082 y se modifica la Ley 29 de 2044 y Decisión Andina 351 de 2015 (Derechos de autor).
- **Ley 527 de 1999.** Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- **Ley 594 de 2000.** Por medio de la cual se expide la Ley General de Archivos.
- **Ley 850 de 2003.** Por medio de la cual se reglamentan las veedurías ciudadanas
- **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 1221 del 2008.** Por la cual se establecen normas para promover y regular el Teletrabajo 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.
- **Ley 1341 de 2009.** Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones - TIC- Se crea la agencia Nacional de espectro y se dictan otras disposiciones.
- **Ley 1437 de 2011.** Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.
- **Ley 1474 de 2011.** Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- **Ley 1581 de 2012.** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **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.
- **Ley 1915 de 2018.** Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- **Ley 1952 de 2019.** Por medio de la cual se expide el código general disciplinario

- **Ley 1955 de 2019.** por el cual se expide el Plan Nacional de Desarrollo 2018-2022. "Pacto por Colombia, Pacto por la Equidad".
- **Ley 1978 de 2019. P**or la cual se moderniza el sector de las Tecnologías de la Información y las Comunicaciones TIC), se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones.
- **Decreto 2609 de 2012.** Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
- **Decreto 0884 del 2012.** Por el cual se reglamenta parcialmente la Ley 1221 del 2008.
- **Decreto 1377 de 2013.** Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- **Decreto 886 de 2014.** Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- **Decreto 103 de 2015.** Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- **Decreto 1074 de 2015.** Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- **Decreto 1080 de 2015.** Por medio del cual se expide el Decreto Reglamentario del Sector Cultura.
- **Decreto 1081 de 2015.** Por medio del cual se expide el Decreto Reglamentario del Sector Presidencia.
- **Decreto 728 de 2017.** Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico
- **Decreto 1499 de 2017.** Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- **Decreto 1008 del 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 2106 de 2019.** Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
- **Decreto 620 de 2020.** por el cual se subroga el título 17 de la parte 2 del libro 2 del Decreto 1078 de 2015, para reglamentarse parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011, los literales e), j) y literal a) del parágrafo 2 del artículo 45 de la Ley 1753 de 2015, el numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9° del Decreto 2106 de 2019, estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- **CONPES 3701 de 2011.** Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- **CONPES 3854 de 2016.** Política Nacional de Seguridad digital.
- **CONPES 3905 de 2020.** Política Nacional de Confianza y Seguridad Digital.