Tabla de Contenido

1. INTRODUCCIÓN 2
2. OBJETIVO GENERAL: 2
3. OBJETIVOS ESPECÍFICOS 2
4. ALCANCE 3
5. MARCO NORMATIVO 3
6. METODOLOGÍA DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN: 4
6.1. IDENTIFICACIÓN DE NECESIDADES 4
6.2. CAPACIDAD ORGANIZACIONAL 5
6.3. DEFINICIÓN DE METAS 5
6.4. IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN 5
7. ACTIVIDADES DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN - 2022 5
8. RIESGOS DE INCUMPLIMIENTO DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN Y SUS ACTIVIDADES 9
9. FACTORES DE ÉXITO EN EL CUMPLIMIENTO DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN Y SUS ACTIVIDADES 10
10. REPOSITORIO DE INFORMACIÓN 10
11. TÉRMINOS Y DEFINICIONES 11
12. REGISTRO DE MODIFICACIONES. 14

1. INTRODUCCIÓN

El Modelo de Seguridad y Privacidad de la Información – MSPI, pertenece al habilitador transversal de la Política de Gobierno Digital, el cual se desarrolla a través del – MSPI, está orientado a la gestión e implementación del Sistema de Gestión de Seguridad de la Información – SGSI, cuya finalidad es incorporar el componente de seguridad de la información en todos los procesos, aplicativos, sistemas de información, infraestructura tecnológica, conectividad y lo hace extensivo a todos los demás activos de información de la Secretaría Distrital de la Mujer, cuya finalidad es garantizar la confidencialidad, integridad y disponibilidad de la información.

De otra parte, teniendo en cuenta el Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018, en el artículo 2.2.9.1.1.3. Principios. Define la seguridad de la información como principio de la Política de Gobierno Digital, de igual manera en el artículo 2.2.9.1.2.1 define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales, los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.

La Secretaría Distrital de la Mujer, determina la información y los recursos informáticos como activos vitales para el desarrollo de sus funciones de conformidad con la misión y la visión de la Entidad, de igual forma, la Alta Dirección se encuentra comprometida con la seguridad de la información, este proceso es liderado de manera permanente por la Oficina Asesora de Planeación – Gestión Tecnológica.

Es importante resaltar la necesidad de realizar una adecuada identificación, clasificación y valoración de los riesgos, que pueden afectar la seguridad y privacidad de la información en todos los procesos y dependencias de la Entidad, con el propósito de garantizar la disponibilidad, integridad y confidencialidad de la información, por lo cual se deben establecer controles y medidas de seguridad, cuyo objetivo es asegurar la información de la Entidad en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y activos de información.

La implementación del plan de Seguridad de la Información en la Entidad, obedece a las necesidades objetivas, requisitos y acciones en materia de seguridad, promoviendo así la implementación y apropiación de las mejores prácticas, definidas en el MSPI y en la norma ISO 27001 para la gestión e implementación de Sistemas de Gestión de Seguridad de la Información.

2. OBJETIVO GENERAL:

Definir la hoja de ruta del plan de seguridad de la información de la Secretaría Distrital de la Mujer para la vigencia 2022, en el marco de las directrices del Modelo de Seguridad y Privacidad de la Información - MSPI definido por el Ministerio de Tecnologías de Información – MINTIC.

3. OBJETIVOS ESPECÍFICOS

- Proteger los activos de información de la Secretaría Distrital de la Mujer.
- Identificar los riesgos de seguridad de la información que puedan afectar la confidencialidad, integridad y disponibilidad de la información.
- Sensibilizar las servidoras y servidores públicos, así como a los contratistas de la Entidad, acerca del Modelo de Seguridad y Privacidad de la Información de la Secretaría Distrital de la Mujer, fortaleciendo así el nivel de conciencia de los mismos, frente a la necesidad de proteger los activos de información críticos de la Entidad.
- Monitorear el cumplimiento de los requisitos de seguridad de la información, mediante el uso de la herramienta de diagnóstico del MSPI.

4. ALCANCE

El plan de seguridad de la información aplica a todos los niveles de la entidad en razón del cumplimiento de sus funciones, así como a servidoras, servidores públicos y contratistas en Nivel Central, las CIOM, Casa Refugio, Casa de Todas, en los cuales se genere, acceda, almacene, se comparta y/o se procese información de la entidad, ya sea en medios físicos, electrónicos, haciendo uso de la infraestructura tecnológica, sistemas de información, o cualquier tipo de información que sea provista por la entidad.

5. MARCO NORMATIVO

NORMA	DESCRIPCIÓN
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1008 de 2018	Por medio del 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
CONPES 3854 de 2016	Política Nacional de Seguridad Digital
CONPES 3995 de 2020	Política Nacional de Confianza y Seguridad Digital.
Manual para la Implementación de la Política de Gobierno Digital	Implementación de la política de Gobierno Digital. Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2) Versión 7, abril de 2019
Modelo de Seguridad y privacidad de la información - MSPI	Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el

	Estado y TIC para la Sociedad. TIC, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales
NTC/ISO 27001 de 2013	Sistemas de Gestión de Seguridad de la Información. Sistema de Gestión de Seguridad de la Información (SGSI) es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de una organización para alcanzar los objetivos de negocio.

6. METODOLOGÍA DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN:

La metodología de implementación del Plan de Seguridad de la Información de la Secretaría Distrital de la Mujer, está basada en la aplicación del ciclo PHVA (Planear, Hacer, Verificar, y Actuar), de acuerdo con las directrices del Modelo de Seguridad y Privacidad de la Información - MSPI, ISO 27001:2013 y el Decreto 1008 del 14 de junio de 2018.

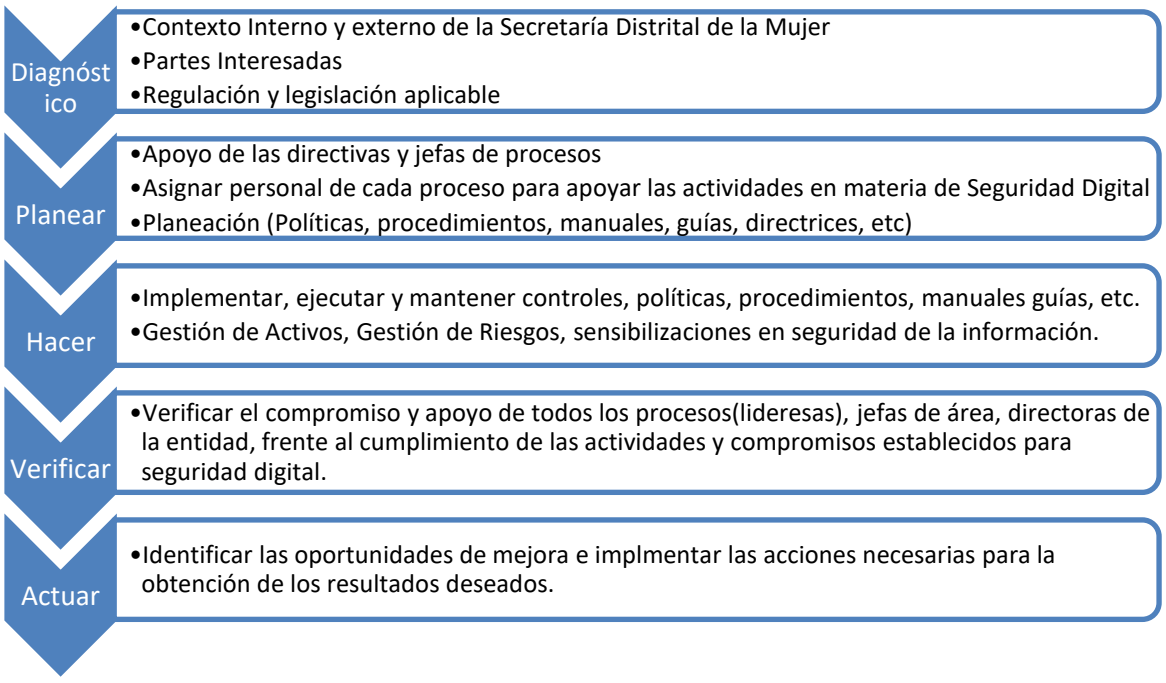

Ilustración 1. PHVA SGSI - SDMUJER
Fuente: Elaboración propia

6.1. IDENTIFICACIÓN DE NECESIDADES

El Plan de Seguridad de la Información requiere de la designación, participación activa y constante de los actores clave (equipo de trabajo) de cada uno de los procesos y dependencias de la entidad,

garantizando la comprensión e identificación del estado actual de la entidad en materia de seguridad de la información, se identifican las necesidades que se requieren gestionar, para logar una adecuada implementación del plan.

En esta fase se requiere del apoyo y liderazgo del equipo directivo de la Secretaría Distrital de la Mujer, comprendiendo todos los requerimientos que se realicen, para logar la implementación de un gobierno efectivo de seguridad y privacidad de la información en la entidad; se reitera la necesidad de contar con el personal idóneo y conocedor de cada proceso, facultado para la toma de decisiones, así como también la ejecución eficiente de las actividades planificadas y su debida diligencia en la entrega oportuna de los productos esperados, con lo cual se garantiza la implementación y cumplimiento de los objetivos trazados en el presente plan.

6.2. CAPACIDAD ORGANIZACIONAL

Partiendo de la identificación de las partes interesadas y la designación de los actores clave de cada proceso, es necesario evaluar la capacidad y estructura de los procesos oficiales que se encuentran definidos en el mapa de procesos de la entidad, cuya finalidad es identificar tempranamente debilidades y obstáculos que permitan establecer las acciones a que haya lugar y se propicie el cumplimiento de los objetivos del plan.

6.3. DEFINICIÓN DE METAS

Una vez identificadas las necesidades en materia de seguridad de la información y contando con el apoyo de los actores clave y de las partes interesadas, definidos los objetivos y resultados esperados por la entidad, es necesario estructurar, diseñar, planificar las actividades, tiempos, responsables y producto esperado, lo cual es conducente y coherente para cumplir con los objetivos, alcance y actividades determinados en el presente plan y así alcanzar el cumplimiento de las metas y el estado deseado en materia de seguridad de la información.

6.4. IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN

La etapa de implementación se centra en la ejecución y cumplimiento de las actividades y objetivos acordados y aprobados, de la misma forma se tienen en cuenta los roles y responsabilidades y los tiempos de entrega por parte del equipo de trabajo involucrado en el Plan de Seguridad de la Información (todos los procesos, actores clave, equipo directivo). El resultado esperado de esta fase es la adecuada implementación y cumplimiento de las actividades previstas en el plan de Seguridad la Información - MSPI.

7. ACTIVIDADES DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN - 2022

Para que el modelo de seguridad y privacidad de la información continue su implementación y operación de forma adecuada en la en la Secretaría Distrital de la Mujer, se proponen las siguientes actividades

para la vigencia 2022. En esta fase se definen las actividades y cronograma requeridos para la ejecución del Plan de Seguridad de la Información, entre los meses de Febrero a Diciembre de 2022.

No.	ACTIVIDAD	PRODUCTO	FECHA INICIO	FECHA FIN	RESPONSABLE
1	**AUTODIAGNÓSTICO MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**				
1.1	Realizar actualización del autodiagnóstico de MSPI, con el apoyo de las dependencias involucradas.	Autodiagnóstico MSPI diligenciado y actualizado	01 febrero	30 Noviembre	Oficina Asesora de Planeación – Gestión Tecnológica y dependencias involucradas
1.2	Aprobación del Autodiagnóstico de MSPI por parte del Comité Institucional de Gestión y Desempeño	Autodiagnóstico MSPI aprobado	01 Abril	30 Abril	Oficina Asesora de Planeación – Gestión Tecnológica
1.3	Actualización y aprobación de la declaración de aplicabilidad SOA	Declaración de aplicabilidad - SOA actualizada.	02 Mayo	30 Junio	Oficina Asesora de Planeación – Gestión Tecnológica
2	**MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN**				
2.1	Actualización del Manual de Políticas Específicas de Seguridad de la Información	Manual de Políticas Específicas de Seguridad de la Información	01 Marzo	30 Abril	Oficina Asesora de Planeación – Gestión Tecnológica
2.2	Publicar en la página web y en Lucha el Manual de Políticas Específicas de Seguridad de la Información	Publicar Manual de Políticas Específicas de Seguridad de la Información	02 Mayo	30 Mayo	Oficina Asesora de Planeación – Gestión Tecnológica
2.3	Socialización y divulgación de la Política de Seguridad de la Información en las	Registros de asistencia	Según programación de Talento Humano	Según programación de Talento Humano	Oficina Asesora de Planeación – Gestión Tecnológica

	jornadas de inducción y reinducción				
3	**DATOS PERSONALES**				
3.1	Actualización y aprobación de la Política de Privacidad y Datos Personales	Política de Privacidad y Datos Personales	01 Abril	30 Mayo	Oficina Asesora de Planeación – Gestión Tecnológica
3.2	Publicar la Política de Privacidad y Datos Personales	Publicar la Política de Privacidad y Datos Personales en la página web y en el Sistema Integrado de Gestión	01 Junio	30 Junio	Oficina Asesora de Planeación – Gestión Tecnológica
3.3	Socialización y divulgación de la Política de Privacidad y Datos Personales en las jornadas de inducción y reinducción	Actas de socialización	Según programación de Talento Humano	Según programación de Talento Humano	Oficina Asesora de Planeación – Gestión Tecnológica
4	**GESTIÓN DE ACTIVOS DE INFORMACIÓN**				
4.1	Revisión y Actualización de la metodología de Activos de Información	Metodología de Activos de Información	01 Julio	30 Agosto	Oficina Asesora de Planeación – Gestión Tecnológica y Dirección de Gestión Administrativa y Financiera
4.2	Actualización de Activos de Información	Matriz de Activos	01 Septiembre	30 Noviembre	Dirección de Gestión Administrativa y Financiera y Todos los procesos.
4.3	Actualización y publicación Registro de Activos de Información	Publicación de Activos de Información	01 Diciembre	30 Diciembre	Dirección de Gestión Administrativa y Financiera

4.4	Actualización y publicación del Índice de Información Clasificada y Reservada	Publicación del Índice de Información Clasificada y Reservada	01 Diciembre	30 Diciembre	Dirección de Gestión Administrativa y Financiera
5	**RIESGOS DE SEGURIDAD DE LA INFORMACIÓN**				
5.1	Definir la metodología de riesgos de seguridad de la información	Metodología de riesgos de seguridad de la información	01 Febrero	30 Marzo	Oficina Asesora de Planeación y Gestión Tecnológica
5.2	Identificación y análisis de riesgos de seguridad de la información	Matriz de riesgos de seguridad de la información	01 Marzo	30 Diciembre	Todos los procesos y dependencias de la entidad
5.3	Plan de tratamiento de riesgos de seguridad de la información	Documento plan de tratamiento de riesgos	14 Enero	30 Enero	Oficina Asesora de Planeación – Gestión Tecnológica
6	**PLAN DE SENSIBILIZACIÓN SEGURIDAD DE LA INFORMACIÓN**				
6.1	Actualización del plan de sensibilización en seguridad de la información	Plan de sensibilización en seguridad de la información	01 Abril	30 Mayo	Oficina Asesora de Planeación – Gestión Tecnológica
6.2	Charlas de sensibilización en seguridad de la información para servidoras, servidores públicos y contratistas	Sensibilizaciones - Actas	01 Junio	30 Noviembre	Oficina Asesora de Planeación – Gestión Tecnológica
6.3	Envío de piezas comunicativas de seguridad de la información	Piezas comunicativas de seguridad por correo electrónico y/o boletina	01 Marzo	15 Diciembre	Oficina Asesora de Planeación – Gestión Tecnológica
7	**MESAS DE TRABAJO DE GOBIERNO DIGITAL Y SEGURIDAD DIGITAL - MTGD**				
7.1	Realizar mesas de trabajo para tratar	Reunión Actas	1 Febrero	16 Diciembre	Oficina Asesora de Planeación –

	temas de Gobierno Digital y seguridad Digital en los comités de enlaces MIPG				Gestión Tecnológica y enlaces de GD de todos los procesos/áreas de la entidad
8	**REPORTE FURAG - POLÍTICA DE SEGURIDAD DIGITAL**				
8.1	Reportar las evidencias correspondientes a la política de seguridad digital solicitadas por FURAG	Evidencias correspondientes a la política de seguridad digital	01 Febrero	30 Marzo	Oficina Asesora de Planeación – Gestión Tecnológica
9	**CONTROLES DE SEGURIDAD PERIMETRAL**				
9.1	Fortalecer el diseño, medidas de seguridad y controles a nivel de seguridad perimetral.	Configuración e implementación de reglas en la herramienta de seguridad perimetral.	01 Febrero	30 Abril	Oficina Asesora de Planeación – Gestión Tecnológica
10	**FUNCIONES DE SEGURIDAD EN OFFICE 365 Y ENDPOINT**				
10.1	Fortalecer el diseño, medidas de seguridad y controles a nivel de Office 365 y solución de EndPoint.	Configuración e implementación de controles de seguridad en las herramientas	01 Febrero	30 Abril	Oficina Asesora de Planeación – Gestión Tecnológica

8. RIESGOS DE INCUMPLIMIENTO DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN Y SUS ACTIVIDADES

Los principales riesgos o limitaciones para el adecuado cumplimiento y ejecución del plan son:

- Falta de designación de personal o reemplazo del mismo por parte del equipo Directivo, en caso de licencias, vacaciones, incapacidades, permisos, ausencias u otras actividades prolongadas o intermitentes, que afecten la ejecución de las actividades previstas en el Plan de Seguridad de la Información.
- Falta de Disponibilidad e inasistencia por parte de los miembros del equipo de trabajo designado por cada uno de los procesos, para la realización de las actividades del Plan de Seguridad de la Información.
- Falta de idoneidad y conocimiento por parte de los miembros del equipo de trabajo designado

por cada uno de los procesos, para la realización de las actividades del Plan de Seguridad de la Información.

- Entrega inoportuna o incumplimiento en la entrega de los productos o entregables asignados a los miembros del equipo de trabajo designado por cada uno de los procesos, para la realización de las actividades del Plan de Seguridad de la Información.
- Ausencia de autorización por parte del equipo Directivo, al personal designado para realizar las actividades del Plan de Seguridad de la Información, para la toma de decisiones relacionadas con su proceso en las mesas de trabajo que requieran de las mismas y sea necesario reprocesos nuevas reuniones o mesas de trabajo para dar continuidad a las actividades previstas.
- Ausencia o incumplimiento en la carga de información, evidencias, actas, registros de asistencia y demás relacionados, acorde a las directrices y lineamientos emitidos por parte de la Oficina Asesora de Planeación en las reuniones y mesas de trabajo, frente a las actividades del Plan de Seguridad de la Información a cargo del personal designado por los procesos para tal fin.
- Errores significativos de calidad, fiabilidad o integridad de la información, cometidos por parte de alguno de los miembros del equipo de trabajo designado por los procesos, los cuales afectan la normal ejecución y reproceso de las actividades previstas en el Plan de Seguridad de la Información.
- Pérdida, modificación o eliminación voluntaria o involuntaria de información de los productos, evidencias y demás del repositorio oficial de almacenamiento de información en la nube para las actividades del Plan de Seguridad de la Información, por parte de alguno de los miembros del equipo de trabajo designado.

9. FACTORES DE ÉXITO EN EL CUMPLIMIENTO DEL PLAN DE SEGURIDAD DE LA INFORMACIÓN Y SUS ACTIVIDADES

- Compromiso de la Alta Dirección, equipo directivo, jefas, jefes, directoras(es) frente al cumplimiento de las actividades previstas en el Plan de Seguridad de la Información.
- Adecuada y oportuna designación de personal, por parte del equipo directivo para la ejecución de las actividades del Plan de Seguridad de la Información.
- Cumplimiento en la entrega y ejecución de las actividades, objetivos, entregables y fechas previstas en el Plan de Seguridad de la Información, por parte del equipo de trabajo designado por el equipo directivo.
- Asistencia oportuna y constante de los miembros del equipo de trabajo a las reuniones y actividades programadas en el Plan de Seguridad de la Información.
- Uso de mecanismos eficaces de comunicación entre el equipo de trabajo y las partes interesadas, para garantizar el adecuado cumplimiento de las actividades definidas en el Plan de Seguridad de la Información.

10. REPOSITORIO DE INFORMACIÓN

Se define como repositorio de información relacionada con el Plan de Seguridad de la Información la carpeta “AUTODIAGNÓSTICO DE GOBIERNO DIGITAL\PSI 2022”, creada en las herramientas

colaborativas, para el seguimiento, control, divulgación, almacenamiento, administración y gestión del Plan de Seguridad de la Información.

11. TÉRMINOS Y DEFINICIONES

Activo de Información: Un activo de información es, cualquier elemento que contenga, genere, adquiera, gestione y/o procese información, que tiene valor para uno o más procesos de la organización y debe protegerse (ISO/IEC 27001:2013).

Alta dirección: Persona o grupo de personas que dirige y controla una organización, al nivel más alto (ISO/IEC 27001:2013).

Amenaza: Potencial ocurrencia de un hecho que pueda manifestarse en un lugar específico, con una duración e intensidad determinadas. Cuando el Agente de riesgo selecciona una víctima contra la cual pretende cometer un acto delictivo, automáticamente se convierte en una amenaza para ella. Se puede considerar que es la materialización del riesgo.

Clasificación de la información: Los responsables de los activos de información deben documentar la clasificación de seguridad de los activos de información de los cuales son responsables y designarán un custodio para cada activo, a su vez éste será responsable de la implementación de los controles de seguridad.

La clasificación de la información de la Secretaría Distrital de la Mujer se debe realizar con base en la Ley 1712 de 2014, reglamentada por el Capítulo 2 del Título 1 de la Parte 1 del Decreto 1081 de 2015 y la Ley 594 de 2000 (Ley General de Archivos).

Compromiso de la Dirección: Alineamiento firme de la Dirección de la entidad con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI - Sistema de Gestión de Seguridad de la Información.

Confidencialidad: El acceso a la información es permitido exclusivamente al personal autorizado, sin revelar la misma a terceras partes y/o personas.

Custodio: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado. Tomado de https://www.mintic.gov.co/gestionti/615/articles-482_G5_Gestion_Clasificacion.pdf

Dato Personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables (Ley 1581 de 2012 – Artículo 3).

Disponibilidad: En seguridad informática es un término hace referencia a la característica de poder acceder a la información en el momento que se requiera.

Evento de seguridad de la información: Presencia identificada de una condición de un sistema,

servicio o red, que indica una posible violación de la política de seguridad de la información o falla de salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad (NTC-ISO/IEC 27001 2013).

Gestión de la seguridad en los activos: La Secretaría Distrital de la Mujer a través de los procesos Gestión Tecnológica y Gestión Administrativa deben establecer y divulgar los lineamientos específicos para la identificación, clasificación y buen uso de los activos de información de tipo información, datos, software, hardware y servicios, con el objetivo de garantizar su protección.

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y su tratamiento. (ISO 27000, Glosario de términos y definiciones).

Gobierno de seguridad de la información: Es el conjunto de responsabilidades y prácticas ejercidas por el Grupo Directivo con el propósito de evaluar, dirigir, monitorear y comunicar todas las acciones y/o actividades relacionadas con la protección de la información de la Entidad. (ISO/IEC 27014:2013).

Hardware: Conjunto de equipos de cómputo, servidores, redes, equipos de seguridad, impresoras, scanner, equipos de almacenamiento, entre otros, que utiliza la Secretaría Distrital de la Mujer.

Impacto: Resultado de un incidente de seguridad de la información.

Incidente de seguridad: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información: Es un conjunto de datos ordenados, clasificados y almacenados en cualquier medio (magnético, papel, correo electrónico, conversación telefónica, chat, USB, etc.).

La información documentada: (Inglés: Documented information). Información requerida para ser controlada y mantenida por una organización y el medio en el que está contenida

La información documentada puede estar en cualquier formato y medio y desde cualquier fuente y puede referirse al sistema de gestión (incluidos los procesos relacionados), información creada para que la organización funcione (documentación) y/o evidencias de resultados alcanzados (registros)

Incidente: Según [ISO/lEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información

Inventario de activos: Los responsables de la información deben propender para que se mantenga actualizado el inventario de sus activos de información y hagan entrega de éste al menos una vez al año. La consolidación de dicho inventario está bajo la responsabilidad de la Dirección de Gestión Administrativa.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Propietario de la Información: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso.

Sistema de información: Aplicativo que se encarga de administración de datos e información, organizados y listos para su uso, generados para cubrir una necesidad u objetivo.

SGSI - Sistema de Gestión de Seguridad de la Información: Según [ISO/lEC 27001: 2013]: Sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.

Seguridad de la Información: Preservación de la confidencialidad, integridad, y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas (NTC-ISO/IEC 27001:2013).

Software: Conjunto de programas, sistemas operativos, aplicaciones de ofimática entre otros aplicativos propios y/o tercerizados que utiliza la Secretaría Distrital de la Mujer.

Terceros: Personas que no son empleados de la Secretaría Distrital de la Mujer o empresas diferentes al mismo. Ejemplo: Participantes, beneficiarios, proveedores regulares o potenciales de bienes y servicios, empresas candidatas a prestar servicios a la Secretaría Distrital de la Mujer, entes reguladores, consultores, etc.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

12. REGISTRO DE MODIFICACIONES.

VERSIÓN	FECHA	DESCRIPCIÓN DE LA MODIFICACIÓN
1	19/01/2021	Primer versión del Plan de Seguridad de la Información de la Secretaría Distrital de la Mujer.
2	20/01/2022	Actualización general del documento y de las actividades previstas para el Plan de Seguridad de la Información 2022 de la Secretaría Distrital de la Mujer.
3		

	NOMBRE	CARGO	FIRMA
ELABORÓ	Andrés Giovanny Cadena Herrera	Profesional Especializado - Contratista	
REVISÓ	Sandra Catalina Campos Romero	Jefe Oficina Asesora de Planeación	
APROBÓ	Comité Institucional de Gestión y Desempeño	Comité Institucional de Gestión y Desempeño	