SECRETARÍA DISTRITAL DE PLANEACIÓN

POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA SDP

Responsables:
Dirección de Tecnologías de la Información y las Comunicaciones
Dirección de Planeación Institucional
Dirección de Información y Estadísticas
Dirección de Servicio a la Ciudadanía
Dirección de Contratación
Dirección Administrativa

TABLA DE CONTENIDO

1. ANTECEDENTES

En cumplimiento del Artículo 20 "DIRECTRICES DE SEGURIDAD DE LOS DATOS Y LA INFORMACIÓN" de la Resolución No. 305 de 2008 emitida por la Comisión Distrital de Sistemas (CDS) "Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre", que indica: ."Los Jefes de las entidades, organismos y órganos de control del Distrito Capital para efectos de facilitar la Gestión de la Seguridad de la Información al interior de cada una de sus entidades y teniendo en cuenta las normas internacionales generalmente aceptadas, deben establecer un Comité de Seguridad de la Información, así como la aplicación de los dominios de control a que se refiere la norma NTC-ISO/IEC 27001 que establece los requisitos del Sistema de Gestión de Seguridad de la Información (SGSI) y las normas NTC-ISO/IEC 17799 con su equivalente NTC-ISO/IEC 27002 y demás normas concordantes", la Secretaría Distrital de Planeación (SDP) lideró durante la vigencia 2010, el proceso para la conformación del Comité de Seguridad de la Información, logrando la adopción de la Resolución 1465 de 2010 por medio de la cual se creó el Comité de Seguridad de la Información (en adelante CSI) y se dictaron otras disposiciones; adicionalmente se construye y aprueba el primer documento de políticas de seguridad de la información de la Entidad que refleja los lineamientos en seguridad de la información dados por la Alta Dirección; a partir del cumplimiento de las funciones que debe desarrollar el CSI y el Grupo Interdisciplinario de Trabajo del CSI (en adelante GIT), se asegura la validación de las políticas de seguridad de la información, así como los procesos, procedimientos, y metodologías específicas para la protección de la información de la Entidad (disponibilidad, integridad y confidencialidad).

Para la vigencia 2013, el GIT, como parte de la validación periódica ejecutada sobre las políticas de seguridad de la información de la Entidad, en cumplimiento del Artículo 23 "Responsables de la promulgación, difusión e implementación de las políticas de seguridad" de la Resolución 305 de 2008 de la CDS, realizó ajustes buscando homologar y complementar las políticas vigentes en la SDP, basándose en las recomendaciones de las normas internacionales: NTC-ISO/IEC 27001 y la norma NTC/ISO IEC 17799 con su equivalente NTC-ISO/IEC 27002. El GIT igualmente se apoyó en las políticas definidas en el Artículo 22 de la citada resolución, donde se define una política de seguridad por cada dominio de control de la norma NTC-ISO/IEC 27001.

En el año 2014, y debido a la actualización de la norma técnica colombiana ISO27001 de su versión 2006 a su versión 2013, se aprobó utilizar como referencia normativa para la implementación del SGSI en la SDP, la norma actualizada. Por lo anterior, el GIT realizó el ajuste sobre el documento de políticas de seguridad de la información bajo los nuevos lineamientos y recomendaciones de dicha norma, y bajo las recomendaciones dadas en el Anexo D "Estructura de las políticas" de la norma GTC-ISO/IEC 27003, documento que es revisado y aprobado por el CSI (comité de seguridad de la información en esa vigencia).

En el año 2016 mediante resolución 1361 del 26 de septiembre 2016 se deroga la resolución 1604 de 2014 con el propósito de garantizar un ejercicio articulado y armónico de cada uno de los subsistemas dando como resultado la fusión del Comité de Seguridad Información en el Comité Coordinador del Sistema Integrado (instancia existente en esa vigencia) con el objetivo de simplificar y racionalizar instancias y facilitar la toma de decisiones.

En la misma resolución, Artículo 13 - Objeto y responsabilidades del Grupo Operativo del Sistema Integrado de Gestión, se establecían las responsabilidades de dicho grupo las cuales incluyen los subsistemas entre los cuales se encuentra el de Seguridad y Privacidad de la Información por lo cual el Grupo Interdisciplinario de Trabajo no existe y sus responsabilidades se delegan al Grupo Operativo del Sistema Integrado de Gestión, según el mencionado artículo.

En el 2017 la Comisión Distrital emite la modificación a la Resolución 305 de 2008 mediante resolución 004 de 2017 en la cual en su ARTÍCULO 6°-: Modificar el artículo 16 de la Resolución CDS 305 de 2008, el cual en lo sucesivo tendrá el siguiente tenor: Artículo 16 - POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. "Las entidades, organismos y órganos de control del Distrito Capital deben adoptar políticas de seguridad y custodia de los datos y la información, y establecer los procedimientos para el adecuado uso y administración de los recursos informáticos de los cuales se valgan para cumplir con sus funciones administrativas, operativas y misionales. Las entidades, organismos y órganos de control del Distrito Capital deberán atender la normatividad y lineamientos que formulen las entidades nacionales sobre el particular, incluyendo los que han sido formulados y los que llegue a formular el MinTIC, así como los que emitan otras autoridades competentes del orden nacional (por ejemplo, el Ministerio de Defensa, la Dirección Nacional de Inteligencia y el DNP, que son citados por el CONPES 3854 de Seguridad Digital como autoridades en la materia) y que sean aplicables a la respectiva entidad".

En el mismo año, se actualiza la resolución interna por la cual se modifica y compila la reglamentación del Sistema Integrado de Gestión de la Secretaría Distrital de Planeación y se dictan otras disposiciones, siendo expedida el 8 de septiembre de 2017 con

número 1508.

En el año 2019 se genera una nueva resolución interna número 0137 de 2019 "por la cual se ajusta el Sistema Integrado de Gestión de la Secretaria Distrital de Planeación e implementa como su marco de referencia el Modelo Integrado de Planeación y Gestión y se crea el Comité Institucional de Gestión y Desempeño de la Secretaria Distrital de Planeación y se dictan otras disposiciones", resolución que reglamenta el desarrollo el Sistema Integrado de Gestión - SIG a través de 7 dimensiones MIPG y estas a su vez integradas por diferentes Políticas de Gestión y Desempeño Institucional. Teniendo en cuenta que el Sistema de Seguridad y Privacidad de la Información es un habilitador Transversal, éste será gestionado a través de la Dimensión - Gestión en Valores para Resultados, Polítticas de Gobierno y Seguridad Digital lideradas por la Dirección de Sistemas.

Para la vigencia 2021 se emitió la resolución 0601 de mayo 04 DE 2021, la cual derogó resolución interna número 0137 de 2019.

De igual manera, se emitió en el mes de julio la Resolución interna No. 0998 DE 2021 "Por la cual se Ajusta el Sistema Integrado de Gestión -SIG de la Secretaría Distrital de Planeación, el cual de ahora en adelante se entenderá como Sistema de Gestión SG bajo el Modelo Integrado de Planeación y Gestión -MIPG y se dictan otras disposiciones".

Posteriormente de conformidad con lo establecido en el Decreto Distrital 432 del 04 de octubre de 2022, por medio del cual "se modifica La estructura organizacional de la Secretaría Distrital de Planeación y se dictan otras disposiciones". Se hace necesario modificar las dependencias responsables y líderes de la implementación de las siete (7) dimensiones, diecinueve (19) políticas de gestión y desempeño institucional y un componente ambiental que hacen parte del Sistema de Gestión -SG en el marco de las directrices del Modelo Integrado de Planeación y Gestión. Así como se hace necesario ajustar los integrantes del Comité Institucional de Gestión y Desempeño, teniendo en cuenta la nueva estructura organizacional de la entidad. En este sentido se expidió la Resolución No. 1923 del 01 de noviembre de 2022, "Por la cual se dictan otras disposiciones relacionadas con el Sistema de Gestión SG-MIPG de la Secretaría Distrital de Planeación y se deroga la Resolución 0998 de 2021".

Producto del ajuste institucional, la Secretaría Distrital de Planeación expidió la Resolución 2153 de 2023, "Por la cual se actualiza el Sistema de Gestión -SG bajo el Modelo Integrado de Planeación y Gestión -MIPG de la Secretaría Distrital de Planeación.", en el sentido de ajustar el Sistema Integrado de Gestión -SIG de la Secretaría Distrital de Planeación, denominado de ahora en adelante como Sistema de Gestión - SG bajo el Modelo Integrado de Planeación y Gestión - MIPG, para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión institucional, con el fin de generar resultados que resuelvan las necesidades y problemas de los ciudadanos con integridad y calidad en el servicio. En este mismo documento en la parte resolutiva que el Sistema de Gestión - SG, en el marco de las directrices del MIPG se integra los Sistemas de Desarrollo Administrativo y de Gestión de la Calidad y se desarrolla a través de siete (7) dimensiones, diecinueve (19) políticas de gestión y desempeño institucional y un componente ambiental, definiendo además las dependencias que lideran cada política.

De otra pare, como antecedente documental, es importante tener en cuenta que el documento POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN en sus 6 versiones anteriores se publicó en el módulo de gestión documental del Sistema de Procesos automáticos SIPA como E-LE-028 y por correcciones de nomenclatura se cambió a A-LE-429. Posteriormente, por migración del sistema de gestión SIPA al sistema de gestión GESTIONATE se modificó nuevamente quedando con el código GTI-PO-011.

Como parte de las iniciativas de mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) en 2024, la Dirección de TIC y la Oficina de Control Interno han identificado la necesidad de unificar las políticas de seguridad de la información en un solo documento. Esta acción se enmarca en el cumplimiento de las directrices del Ministerio de TIC.

2. GENERALIDADES

La seguridad de la información es la práctica de proteger información y sistemas de información de accesos no autorizados, uso, divulgación, interrupción, modificación o destrucción. En otras palabras, es el conjunto de medidas técnicas y organizativas destinadas a garantizar la confidencialidad, integridad y disponibilidad de la información.

- **Confidencialidad:** Asegurar que la información sea accesible solo a aquellos autorizados a verla.
- **Integridad:** Garantizar que la información sea completa y precisa, y que no se altere sin autorización.
- **Disponibilidad:** Asegurar que la información y los recursos asociados estén accesibles y operativos cuando sean necesarios.

La Importancia de la Seguridad de la Información para la SDP radica en la gran cantidad de información sensible que maneja la entidad, como datos personales, planes de desarrollo, estudios de impacto y otra información estratégica que en cumpliendo con las leyes de protección de datos la Entidad está obligada a proteger y garantizando la preservación de la integridad institucional, la continuidad de las operaciones, el cumplimiento normativo y la protección de los activos de información para el desarrollo de Bogotá.

Las amenazas a la seguridad de la información en la SDP pueden ser de diversa índole, como:

- **Ataques cibernéticos:** Hackers, malware, phishing, ransomware, etc.
- **Errores humanos:** Acciones involuntarias de los empleados, como la pérdida de dispositivos o la divulgación de información confidencial.
- **Desastres naturales:** Incendios, inundaciones, terremotos, etc.
- **Sabotaje:** Acciones intencionales de personas internas o externas para dañar los sistemas o la información.

Con el objetivo de proteger la información, la SDP ha adoptado un enfoque integral basado en estándares internacionales y ha desarrollado un Modelo de Seguridad y Privacidad de la Información e implementado un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con la norma ISO 27001. Este sistema incluye una serie de controles de seguridad diseñados para garantizar la confidencialidad, integridad y disponibilidad de la información.

2.1.CONTROLES DE SEGURIDAD DE LA INFORMACION

En cumplimiento con el marco normativo de la ISO 27001:2022, y en el contexto de la implementación del MSPI y el SGSI en la SDP, se hace necesario aplicar los controles de seguridad específicos que permitan a la entidad proteger su información. Estos controles son esenciales para asegurar el cumplimiento de los requisitos legales y regulatorios en materia de seguridad de la información. En este sentido, la Secretaría Distrital de Planeación en el instrumento GTI-MA-005 - DECLARACIÓN DE APLICABILIDAD DEL SGSI EN LA SDP, definió los controles de seguridad de la información[1] aplicables en la Entidad relacionados continuación:

CATEGORÍA	CONTROLES
	37 controles 5.1 Políticas de seguridad de la información 5.2 Roles y responsabilidades de seguridad de la información 5.3 Segregación de deberes 5.4 Responsabilidades de gestión 5.5 Contacto con autoridades 5.6 Contacto con grupos de interés especial 5.7 Inteligencia de amenazas 5.8 Seguridad de la información en la gestión de proyectos. 5.9 Inventario de información y otros activos asociados 5.10 Uso aceptable de la información y otros activos asociados 5.11 Devolución de activos 5.12 Clasificación de la información 5.13 Etiquetado de información 5.14 Transferencia de información 5.15 Control de acceso 5.16 Gestión de identidad 5.17 Información de autenticación 5.18 Derechos de acceso

5. Controles organizacionales	5.19 Seguridad de la información en las relaciones con los proveedores 5.20 Abordar la seguridad de la información en los acuerdos con los proveedores 5.21 Gestión de la seguridad de la información en la cadena de suministro de tecnologías de la información y la comunicación (TIC) 5.22 Seguimiento, revisión y gestión de cambios de servicios de proveedores 5.23 Seguridad de la información para el uso de servicios en la nube 5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información 5.25 Evaluación y decisión sobre eventos de seguridad de la información 5.26 Respuesta a incidentes de seguridad de la información 5.27 Aprender de los incidentes de seguridad de la información 5.28 Recolección de evidencia 5.29 Seguridad de la información durante la interrupción 5.30 Preparación de las TIC para la continuidad del negocio 5.31 Requisitos legales, estatutarios, reglamentarios y contractuales 5.32 Derechos de propiedad intelectual 5.33 Protección de registros 5.34 Privacidad y protección de la información de identificación personal (PII) 5.35 Revisión independiente de la seguridad de la información. 5.36 Cumplimiento de políticas, normas y estándares de seguridad de la información 5.37 Procedimientos operativos documentados
6. Controles orientados a las personas	**8 controles** 6.1 Poner en pantalla 6.2 Términos y condiciones de empleo 6.3 Concientización, educación y capacitación en seguridad de la información 6.4 Proceso Disciplinario 6.5 Responsabilidades después de la terminación o cambio de empleo 6.6 Acuerdos de confidencialidad o no divulgación 6.7 Trabajo remoto 6.8 Informes de eventos de seguridad de la información
7. Controles físicos	**14 controles** 7.1 Perímetros físicos de seguridad 7.2 Entrada física 7.3 Asegurar oficinas, salas e instalaciones 7.4 Monitoreo de seguridad física 7.5 Protección contra amenazas físicas y ambientales. 7.6 Trabajar en áreas seguras 7.7 Escritorio despejado y pantalla despejada 7.8 Emplazamiento y protección de equipos 7.9 Seguridad de los activos fuera de las instalaciones 7.10 Medios de almacenamiento 7.11 Utilidades de apoyo 7.12 seguridad del cableado

	7.13 Mantenimiento de equipo 7.14 Eliminación segura o reutilización de equipos
8. Controles tecnológicos	**34 controles** 8.1 Dispositivos de punto final de usuario 8.2 Derechos de acceso privilegiado 8.3 Restricción de acceso a la información 8.4 Acceso al código fuente 8.5 Autenticación segura 8.6 Gestión de capacidad 8.7 Protección contra malware 8.8 Gestión de vulnerabilidades técnicas 8.9 Gestión de la configuración 8.10 Eliminación de información 8.11 Enmascaramiento de datos 8.12 Prevención de fuga de datos 8.13 Copia de seguridad de la información 8.14 Redundancia de las instalaciones de procesamiento de información 8.15 Inicio sesión 8.16 Actividades de seguimiento 8.17 Sincronización de reloj 8.18 Uso de programas de utilidad privilegiados 8.19 Instalación de software en sistemas operativos 8.20 Seguridad en redes 8.21 Seguridad de los servicios de red. 8.22 Segregación de redes 8.23 Filtrado web 8.24 Uso de criptografía 8.25 Ciclo de vida de desarrollo seguro 8.26 Requisitos de seguridad de la aplicación 8.27 Principios de arquitectura e ingeniería de sistemas seguros 8.28 Codificación segura 8.29 Pruebas de seguridad en desarrollo y aceptación. 8.30 Desarrollo subcontratado 8.31 Separación de los entornos de desarrollo, prueba y producción 8.32 Gestión del cambio 8.33 Información de prueba 8.34 Protección de los sistemas de información durante las pruebas de auditoría

La Secretaría Distrital de Planeación debe mantener actualizados registros como por ejemplo evidencia de la evaluación de riesgos, resultados de las auditorías, evidencia de la gestión de incidentes, registros de configuración, evidencia de capacitación y socialización, Políticas y procedimientos, entre otros, creados y mantenidos como parte del Sistema de Gestión de Seguridad de la Información (SGSI), como evidencia tangible de que la entidad está cumpliendo con los requisitos de la norma y con sus propias políticas de seguridad.

3. OBJETIVO

Establecer lineamientos claros y concisos relacionados con la seguridad de la información abordando temáticas específicas, como complemento a lo definido en la "**Política General de Seguridad de la Información de la Entidad**" con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de la **Secretaría Distrital de Planeación**.

3.1.objetivos específicos

- Establecer los lineamientos generales definiendo los principios, estándares y procedimientos que deben seguir todos los miembros de la entidad para proteger la información.
- Alinear la seguridad de la información con los objetivos del negocio asegurando que las medidas de seguridad no obstaculicen las operaciones diarias, sino que las faciliten y protejan.
- Reducir el riesgo de incidentes de seguridad facilitando la identificación y mitigación de las posibles amenazas a la seguridad de la información, como ataques cibernéticos, pérdida de datos o accesos no autorizados.
- Cumplir con los requisitos legales y regulatorios, asegurando que la SDP cumpla con las leyes y normas aplicables en materia de protección de datos y seguridad de la información.
- Crear conciencia entre las personas vinculadas directa o indirectamente a la entidad sobre la importancia de la seguridad de la información y su papel en la protección de los activos de la organización.
- Servir como referencia y guía detallada para la implementación y el mantenimiento del sistema de gestión de seguridad de la información.

4. ALCANCE

El presente manual de políticas abarca a todos los funcionarios, contratistas, personal temporal, terceros, usuarios y visitantes de la **SECRETARÍA DISTRITAL DE PLANEACIÓN** que tengan acceso, utilicen o interactúen de cualquier forma con los sistemas de información, datos, equipos o cualquier otro activo de información de la entidad.

5. DEFINICIONES

- **Activo de Información:** se refiere a cualquier información o elemento relacionado con el tratamiento de la información (sistemas, documentos, soportes, edificios, personas...) que tenga valor para la organización.
- **Activo:** 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).
- **Acceso:** En relación con la seguridad de la información se refiere a la identificación, autenticación y autorización de un usuario a los sistemas, recursos y áreas de la Secretaría Distrital de Planeación en un momento dado.
- **Acceso físico:** Es el Ingreso a las áreas de misión crítica o instalaciones en general de un sitio de la Entidad.
- **Acceso lógico:** En general, el acceso lógico es un acceso electrónico o digital, por ejemplo: acceder a archivos, navegar en el servidor, enviar un correo electrónico o transferir archivos.
- **Amenaza:** Es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo.
- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo una actividad.
- **Certificado digital:** Es un documento o archivo en formato digital generado por una entidad certificadora, que conecta y relaciona los datos de una identidad, con una persona, organismo o empresa; confirmando absolutamente a nivel jurídico, que esa identidad ha firmado las transacciones electrónicas realizadas.
- **Entidad certificadora:** Entidad de confianza, responsable de emitir y revocar los certificados digitales, utilizando en ellos la firma electrónica, para lo cual se emplea la criptografía de clave pública.
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Confidencialidad:** Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.
- **Copias de respaldo:** Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

- **Controles:** Medida que permite reducir o mitigar un riesgo.
- **Clasificación de la Información:** Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados en la Entidad. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado.
- **Cliente:** Es el responsable de transmitir al equipo de desarrollo de software los objetivos que se desean cumplir en la entidad con el producto a ser desarrollado.
- **Dato:** Es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.
- **Desarrollador:** Profesional que apoya el desarrollo de alguna de las fases del ciclo de vida del desarrollo de software y que puede trabajar directamente para la SDP (planta, contratista directo) o a través de una empresa externa.
- **Dirección IP:** Significa «Dirección del Protocolo de Internet». Este protocolo es un conjunto de reglas para la comunicación a través de Internet, ya sea el envío de correo electrónico, la transmisión de vídeo o la conexión a un sitio web. Una dirección IP identifica una red o dispositivo en Internet.
- **Disponibilidad:** Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.
- **Estándar:** Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.
- **Estimación del riesgo:** Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.
- **Guía:** Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares, buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.
- **Herramienta de Mesa de Ayuda:** Sistema de información utilizado por la SDP para el registro, atención y seguimiento de incidencias de soporte tecnológico.
- **Identificación del riesgo:** Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.
- **Impacto:** Cambio adverso en el nivel de los objetivos del negocio logrados.
- **Incidencia:** Corresponde al reporte registrado en la herramienta de Mesa de Ayuda, genera un consecutivo para la atención y seguimiento.
- **Información:** Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.
- **Información institucional critica**: es aquella necesaria para mantener operativos los procesos de la entidad, puede ser almacenada en los servidores de la entidad ubicados en el centro de datos.
- **Freeware:** Software que se distribuye sin pago por licencia; es decir, sin costo por licencia. Por lo tanto, se puede utilizar por tiempo ilimitado.
- **Función Pública:** Garantiza la identidad de una persona natural titular del certificado, así como su vinculación a una entidad pública en virtud del cargo que ocupe como funcionario público.
- **Gestor de base de datos:** Un gestor de base de datos o SGBD, es una colección de programas cuyo objetivo es servir de interfaz entre la base de datos, el usuario y las aplicaciones. Se compone de un lenguaje de definición de datos, de un lenguaje de manipulación de datos y de un lenguaje de consulta. Un SGBD permiten definir los datos a distintos niveles de abstracción y manipular dichos datos, garantizando la seguridad e integridad de estos.
- **Hash:** Es una función computable mediante un algoritmo, que tiene como entrada un conjunto de elementos, que suelen ser cadenas, y los convierte (mapea) en un rango de salida finito, normalmente cadenas de longitud fija.
- **Información de Identificación Personal (PII):** Cualquier información que pueda utilizarse para identificar a una persona física, directa o indirectamente, como nombre, dirección, número de teléfono, dirección de correo electrónico, número de identificación, datos biométricos, registros financieros y cualquier otro dato que permita identificar a un individuo.
- **Integridad:** Propiedad de la información que busca preservar su exactitud y completitud.

- **Líder Funcional:** Es el responsable de coordinar en conjunto con el cliente la definición de las necesidades existentes en la Entidad y transformarlas en requerimientos.
- **Líder Técnico:** Es el profesional responsable de conectar la arquitectura planteada para un proyecto de software con la realidad del código y permite la dinámica de la construcción eficiente de software.
- **Log:** Es un registro oficial de eventos durante un rango de tiempo en particular. Se usa para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación.
- **Mejor Práctica:** Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.
- **MSPI de la SDP:** Es el Modelo de Seguridad y Privacidad de la Información definido por la Secretaría Distrital de Planeación con base en las recomendaciones del Ministerio de Tecnologías de la Información - MINTIC.
- **On-Premise:** Instalación de una solución informática llevada a cabo dentro de la infraestructura tecnológica de la Entidad.
- **One Drive:** Servicio de alojamiento de archivos que permite almacenar, crear, modificar, compartir y acceder a documentos, archivos y carpetas de todo tipo en la Nube. Permite el acceso a los archivos vía Web, desde el dispositivo móvil o desde el equipo de cómputo de escritorio o portátil.
- **Política:** Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.
- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000) y según Norma NTC-ISO 22301 del 20 de noviembre de 2019, Seguridad y resiliencia. Sistema de gestión de continuidad del negocio. Requisitos. Se define en el numeral 3.4 como: Información documentada que orienta a una organización para responder una interrupción y reanudar, recuperar y restaurar la oferta de productos y servicios de acuerdo con sus objetivos de continuidad del negocio.
- **Privilegio:**Derecho o autoridad de un usuario a realizar una tarea específica. Se asignan a los miembros mediante un rol predeterminado o un rol personalizado.
- **Procedimiento:** Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.
- **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 sea clasificada adecuadamente y mantenga una clasificación acorde con su nivel de confidencialidad.
- **Riesgo:** Es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.
- **Rol:** Papel, función que alguien o algo desempeña. Define el conjunto de privilegios asignado a un miembro.
- **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:** Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.
- **SharePoint:**herramienta diseñada para la gestión documental y trabajo en equipo.
- **Sistema de Gestión de Seguridad de la Información:** Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.
- **Software**: Componentes intangibles de un computador, necesarios para hacer posible la realización de una tarea específica, incluye el software licenciado, software libre autorizado y aplicaciones.

- **Software Autorizado**: En la SDP el software autorizado es el software libre que luego de ser solicitado mediante incidencia, siguiendo los lineamientos establecidos en los procedimientos, es evaluado por la Dirección TIC para revisar la conveniencia tanto técnica como de seguridad, en términos de vulnerabilidades y adicionalmente verificando que se ajuste a la infraestructura tecnológica con que cuenta la SDP en el momento.
- **Software propietario**: Software cuya copia, redistribución o modificación están restringidas por el propietario de los derechos de autor.
- **Software libre:** El software es libre cuando la licencia por la cual se distribuye exalta los valores de la libertad y garantiza que el usuario: (1) puede utilizar la obra de software para cualquier propósito, (2) puede distribuir el programa a otros usuarios, (3) tiene acceso al código fuente y puede modificarlo, (4) puede distribuir el programa modificado.
- **Software de Dominio Público**:Software cuyos derechos patrimoniales pertenecen a la comunidad y pueden ser utilizados sin ningún tipo de restricción. Algunos tipos de copia o versiones modificadas pueden no ser libres si el autor impone restricciones adicionales en la redistribución del original o de trabajos derivados.
- **Software de Código Abierto**:Un software es de código abierto cuando la licencia por la cual se distribuye garantiza que el usuario: (a) puede utilizar la obra software para cualquier propósito, (b) puede distribuir el programa a otros usuarios, (c) tiene acceso al código fuente y puede modificarlo, (d) puede distribuir el programa modificado.
- **Suscriptor:** Es aquella persona que ha adquirido un certificado de Función Pública emitido por una entidad certificadora para obrar en el entorno electrónico en su propio nombre y para el cumplimiento de las funciones de su cargo como servidor (a) público (a).
- **Token:** Dispositivo de almacenamiento de certificados digitales, utilizado para facilitar el proceso de autenticación de usuarios, tiene capacidad para generar claves públicas y privadas utilizadas para firma electrónica y/o para autenticación.
- **Tratamiento de la PII:** Cualquier operación o conjunto de operaciones realizadas sobre datos personales, como la recopilación, registro, organización, almacenamiento, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación, comparación o interconexión, bloqueo, supresión o destrucción.
- **URL** (Localizador de Recursos Uniforme): Es un identificador de recursos uniforme (Uniform Resource Identifier, URI) cuyos recursos referidos pueden cambiar, esto es, la dirección puede apuntar a recursos variables en el tiempo. Están formados por una secuencia de caracteres, de acuerdo a un formato modélico y estándar, que designa recursos en una red.
- **Usuario Funcional:** Es un profesional que se encarga esencialmente de ayudar a usar los sistemas de software para fines específicos, al mismo tiempo que actúa como un intermediario entre el equipo especializado y el usuario final.
- **Vulnerabilidad:** Es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

6. POLÍTICAS ESPECÍFICAS QUE HACEN PARTE DEL SGSI DE LA SDP

La Secretaría Distrital de Planeación (SDP), en su compromiso con la protección de la información y el cumplimiento de los más altos estándares de seguridad, presenta este manual de políticas de seguridad de la información. Este documento constituye el marco fundamental para garantizar la confidencialidad, integridad y disponibilidad de los activos de información de la entidad.

Las políticas contenidas en este documento definen las directrices para la aplicación de la Norma ISO/IEC 27001 versión 2022aprobadas por la alta dirección, publicadas, comunicadas y reconocidas por el personal y las partes interesadas relevantes.

Con la formulación, implementación y aplicación de las políticas de seguridad de la información, la Secretaría Distrital de Planeación busca esencialmente:

- **Proteger la información sensible:** Datos personales, información financiera, proyectos estratégicos y otros activos valiosos de la SDP deben estar resguardados de accesos no autorizados, modificaciones y divulgaciones.
- **Cumplir con la normatividad:** Las políticas de seguridad de la información se alinean con las regulaciones nacionales e internacionales aplicables, garantizando el cumplimiento legal de la SDP.
- **Fortalecer la confianza:** Al demostrar un compromiso sólido con la seguridad de la información, la SDP inspira confianza en

sus ciudadanos, colaboradores y socios.

- **Minimizar riesgos:** Las políticas identifican y mitigan los riesgos a los que está expuesta la información, reduciendo la probabilidad de incidentes de seguridad.

- **Optimizar los procesos:** Las políticas establecen los procedimientos y controles necesarios para gestionar de manera eficiente la seguridad de la información en todos los niveles de la entidad.

En el contexto anterior, **La SECRETARÍA DISTRITAL DE PLANEACIÓN**, establece a continuación, los lineamientos de seguridad de la información, los cuales deberán ser cumplidos por todos los funcionarios, contratistas, terceros, usuarios y visitantes. Los lineamientos de seguridad están clasificados en diferentes temáticas, teniendo en cuenta el contexto interno y externo de la entidad.

6.1.POLÍTICAS DE SEGURIDAD DE LOS RECURSOS HUMANOS

La SECRETARÍA DISTRITAL DE PLANEACIÓN en armonía con la Norma ISO 27001:2022, enfatiza la importancia del factor humano en la seguridad de la información. Al incorporar políticas robustas de seguridad de los recursos humanos, se propende fortalecer significativamente la postura de seguridad general. A continuación, se relacionan las políticas de seguridad de los recursos humanos establecidas por la entidad:

1. Compromiso con la Seguridad de la Información (Numeral 5.4)

- **Lineamiento:** La seguridad de la información es una prioridad para la SDP. Todo el personal debe aplicar y cumplir las políticas de seguridad de la información establecidas, demostrando un compromiso activo con la protección de los activos de información de la entidad. Este compromiso se refuerza mediante la comunicación continua, la capacitación y la asignación clara de responsabilidades.

2. Verificación de Antecedentes (Numeral 6.1)

- **Lineamiento:** Durante el proceso de selección de personal (planta o contratistas), se realizará una verificación de antecedentes disciplinarios de todos los candidatos, independientemente del cargo o posición a la que se postulen. Esta verificación se realizará de acuerdo con las leyes, reglamentos y consideraciones éticas aplicables, y será proporcional a los requisitos del puesto.

3. Continuidad en la Verificación de Antecedentes (Numeral 6.1)

- **Lineamiento:** Los controles de verificación de antecedentes se llevarán a cabo antes de la incorporación del personal y se mantendrán de forma continua durante la relación laboral o contractual, según sea necesario y permitido por la ley. Esto permite una gestión proactiva de riesgos y la detección temprana de posibles vulnerabilidades.

4. Acuerdos de Confidencialidad y Compromiso (Numeral 6.6)

- **Lineamiento:** Todo el personal que labore o preste servicios a la entidad deberá firmar:

  - Un acuerdo de confidencialidad que proteja la información sensible de la entidad.

  - Un documento de conocimiento y aceptación de las políticas del sistema de seguridad de la información.

  - Un compromiso sobre el buen uso de los activos de información a los que tenga acceso.

5. Gestión de Acuerdos de Confidencialidad (Numeral 6.6)

- **Lineamiento:** Los acuerdos de confidencialidad o no divulgación se identificarán, documentarán, revisarán periódicamente y se mantendrán actualizados para reflejar las necesidades de protección de la información de la entidad. Estos acuerdos deben ser firmados por el personal y otras partes interesadas relevantes.

6. Responsabilidades Contractuales en Seguridad de la Información (Numeral 6.2)

- **Lineamiento:** Los acuerdos contractuales de trabajo deben definir claramente las responsabilidades del personal y de la entidad en materia de seguridad de la información, incluyendo el manejo de la información durante y después de la relación laboral.

7. Concientización, Educación y Capacitación (Numeral 6.3)

- **Lineamiento:** El personal y las partes interesadas relevantes recibirán conciencia, educación y capacitación adecuadas en seguridad de la información, incluyendo actualizaciones periódicas sobre la política de seguridad de la información, políticas y procedimientos específicos, según sea relevante para su función laboral.

8. Proceso Disciplinario (Numeral 6.4)

- **Lineamiento:** La entidad formalizará y comunicará un proceso disciplinario para abordar las violaciones a la política de seguridad de la información por parte del personal y otras partes interesadas relevantes. Este proceso definirá las acciones a tomar en caso de incumplimiento.

9. Responsabilidades Post-Empleo (Numeral 6.5)

- **Lineamiento:** Se definirán, aplicarán y comunicarán al personal y otras partes interesadas las responsabilidades y deberes de seguridad de la información que sigan siendo válidos después de la terminación o el cambio de empleo.

10. Seguridad en el Trabajo Remoto (Numeral 6.7)

- **Lineamiento:** Se implementarán medidas de seguridad específicas para proteger la información a la que se acceda, procese o almacene fuera de las instalaciones de la entidad cuando el personal trabaje de forma remota. Estas medidas incluirán el uso de conexiones seguras, la protección de dispositivos y la concienciación sobre riesgos específicos del trabajo remoto.

11. Reporte de Incidentes de Seguridad (Numeral 6.8)

- **Lineamiento:** La entidad proporcionará un mecanismo claro y accesible para que el personal informe sobre eventos de seguridad de la información observados o sospechados a través de los canales apropiados y de manera oportuna. Se fomentará una cultura de reporte sin represalias.

12. Gestión de Identidades Digitales (Numeral 5.16)

- **Lineamiento:** La entidad establecerá procesos y controles para garantizar que las identidades digitales de usuarios, funcionarios, contratistas y personal temporal se creen, mantengan, utilicen y eliminen de manera segura y eficiente a lo largo de su ciclo de vida dentro de la organización. Esto incluye la gestión de contraseñas, privilegios de acceso y la revocación oportuna de accesos.

Estos lineamientos buscan fortalecer la seguridad de la información a través de la gestión del recurso humano, alineándose con las mejores prácticas establecidas en la norma ISO 27001:2022.

6.2.POLÍTICAS DE GESTIÓN DE ACTIVOS

Principios Generales:

- **Propiedad de la Información:** Toda información, física o digital, generada, almacenada o transformada por funcionarios, contratistas o proveedores de la SDP, utilizando recursos de la entidad o en desempeño de sus labores, es propiedad de la SECRETARÍA DISTRITAL DE PLANEACIÓN.

- **Uso de Activos:** Los activos dispuestos por la SDP solo se utilizarán para tareas laborales dentro del ámbito de la entidad.

- **Inventario y Gestión:** La SDP identificará, clasificará y gestionará su inventario de activos conforme a manuales y procedimientos formalizados, como la Guía para la Gestión de Activos en el Marco de Seguridad de la Información de la SDP - GTI-GA-001 y el formato GTI-FO-003 Formato Registro de Activos de Información (RAI). El RAI consolidado se publica como GTI-DI-001 - REGISTRO DE ACTIVOS DE INFORMACIÓN (RAI).

- **Mantenimiento:** La SDP mantendrá los equipos en buen estado, asegurando su disponibilidad e integridad mediante el GTI-PL-003 - Plan de Mantenimiento de Infraestructura Tecnológica.

Lineamientos Específicos:

1. Devolución de Activos (Numeral 5.11)

- **Lineamiento:** Al cambiar o terminar su empleo, contrato o acuerdo, el personal y otras partes interesadas devolverán todos los activos de propiedad la SDP que estén en su poder. Para servidores públicos, esto se realiza mediante el procedimiento de Desvinculación Laboral - GTH-PD-010 y los formatos GTH-FO-017 y GTH-FO-011. Para contratistas, se realiza en la liquidación del contrato con el Acta de Recibo Final GCO-FO-002 y su Anexo 2.

2. Emplazamiento y Protección de Equipos (Numeral 7.8)

- **Lineamiento:** El equipo se colocará de forma segura y protegida, previniendo accesos no autorizados y daños físicos. No se permite retirar equipos, información o software sin autorización previa. El traslado entre pisos lo realiza la Dirección de Tecnologías de la Información y las Comunicaciones o un servidor autorizado. Para la salida del edificio, se requiere el formato de la Secretaría Distrital de Hacienda y la notificación a la Dirección Administrativa. Los equipos de propiedad de la SDP deberán estar cubiertos por una póliza de seguro.

3. Seguridad de los Activos Fuera de las Instalaciones (Numeral 7.9)

- **Lineamiento:** Se protegerán los activos fuera del sitio mediante medidas de seguridad específicas. Los traslados requieren el formato GAD-FO-046 Autorización de Movimientos de Bienes de Consumo, Activos Fijos y otros, con verificación y firma autorizada de la Dirección Administrativa y radicación en Hacienda.

4. Medios de Almacenamiento (Numeral 7.10)

- **Lineamiento:** Los medios de almacenamiento (discos duros, SSD, cintas, dispositivos móviles, almacenamiento en la nube, etc.) se gestionarán a lo largo de su ciclo de vida:
    - **Adquisición:** Se adquirirán de proveedores confiables y cumplirán con estándares de seguridad.
    - **Uso:** Se asignarán a usuarios autorizados para fines autorizados, siendo responsables de su seguridad.
    - **Transporte:** Los medios con información sensible se transportarán de forma segura, con contenedores o bolsas de seguridad y rutas seguras, documentando los movimientos.
    - **Eliminación:** Los medios que ya no sean necesarios se eliminarán de forma segura, con métodos que garanticen la destrucción completa de los datos, documentando el proceso.

5. Mantenimiento de Equipo (Numeral 7.13)

- **Lineamiento:** Los equipos tecnológicos se mantendrán correctamente para garantizar la disponibilidad, integridad y confidencialidad de la información, según el GTI-PL-003.

6. Eliminación Segura o Reutilización de Equipos (Numeral 7.14)

- **Lineamiento:** Los equipos con medios de almacenamiento se verificarán para asegurar la eliminación o sobrescritura segura de datos confidenciales y software con licencia antes de su eliminación o reutilización, según el GTI-PD-002 - Soporte y Atención de la Mesa de Ayuda.

7. Dispositivos de Punto Final de Usuario (Numeral 8.1)

- **Lineamiento:** Se protegerá la información almacenada, procesada o accesible a través de los dispositivos finales del usuario. Los usuarios son responsables de la protección de los equipos asignados cuando estén desatendidos, bloqueando la sesión al retirarse, según la Política de Control de Acceso y la Política de Escritorio Limpio.

8. Gestión de Capacidad (Numeral 8.6)

- **Lineamiento:** El uso de los recursos se controlará y ajustará según los requisitos de capacidad actuales y previstos.

9. Eliminación de Información (Numeral 8.10)

- **Lineamiento:** La información almacenada en sistemas, dispositivos o cualquier otro medio se eliminará cuando ya no sea necesaria.

10. Directrices Adicionales para la Gestión de Activos:

- **Registro de Activos de Información:**Los responsables de los procesos (dueños de la información) registran los activos de información de tipo DATOS O INFORMACIÓN, de tipo SOFTWARE, HARDWARE, REDES Y COMUNICACIONES, INFRAESTRUCTURA, PERSONAS y SERVICIOS según la Guía GTI-GA-001 y el formato GTI-FO-003, considerando las premisas establecidas (documentos de archivo, registros originales, activos contenedores, etc.).

- **Premisas en el registro de Activos de Información:**

  - Todo documento de archivo (desde el punto de vista archivístico) es un registro (desde el punto de vista de calidad) y por consiguiente es un activo.

  - Los registros no son formatos como tal, son documentos que podrían o no ser diligenciados sobre un formato preestablecido.

  - Se debe relacionar un solo activo de información para los registros de los procedimientos que puedan tener varias versiones.

  - Se deben relacionar sólo los activos que correspondan a registros originales, es decir, no se deben incluir registros que sean borradores o documentos facilitativos o de apoyo.

  - Un proceso puede tener activos que no estén relacionados en los procedimientos, pero que requieren ser incluidos en el formato de registro de activos de tipo datos e información, porque son evidencias del cumplimiento de las funciones y marco normativo aplicable a la entidad.

  - Si un activo es generado por varias dependencias, la Dependencia responsable del proceso incluirá dicho activo en su registro de activos, consolidará y/o revisará y/o aprobará la información. Por ejemplo: Planes de mejoramiento, POA, para los cuales la Dirección de Planeación es el área responsable de reportar estos activos (procedimientos: gestión del plan de mejoramiento y gestión del Plan operativo anual POA de la SDP).

  - Un activo de información puede tener diferentes elementos de información, por lo cual se denomina activo contenedor, por ejemplo: la Encuesta Multipropósito tiene base de datos, documentación e investigaciones. Para el diligenciamiento de la matriz de registro de activos de tipo datos e información es necesario desagregar este activo en varios activos en caso de que los datos/información que lo componen tengan atributos, ubicación, valoración o clasificación diferentes.

- **Publicación de los Activos de Información:**El resultado consolidado del levantamiento de activos de información o inventario de activos de información de la Secretaría Distrital de Planeación será el REGISTRO DE ACTIVOS DE INFORMACIÓN (RAI) - GTI-DI-001 publicado en el Sistema de Gestión SG de la Entidad en el cual debe quedar claramente especificado el propietario de cada activo

- **Propiedad de los Activos de Información:** La propiedad recae en la SDP, representada por los roles definidos en GTI-MA-003 (Secretario(a), Jefes de Oficina Subsecretarios(as), Directores(as), Subdirectores (as) y Líderes(as) del Proceso).

- **Uso Aceptable de los Activos:** Se aplican las reglas y premisas definidas, incluyendo la responsabilidad de los propietarios de la información y los usuarios, la aplicación del modelo de gestión de riesgos y la concordancia con la valoración de Confidencialidad, Integridad y Disponibilidad (CID) en el RAI - GTI-DI-001.

  Las siguientes actividades sobre los activos de información de la SDP se consideran usos no autorizados que constituyen incidentes de seguridad, gestionados según el GTI-PD-008 procedimiento GESTIÓN DE INCIDENTES DE SEGURIDAD EN LA SDP.

- Modificación o acceso de la información sin contar con la autorización formal del propietario o dueño del activo de información.

- Divulgación de la información sin tener en cuenta la clasificación dada en términos de la Confidencialidad en el REGISTRO DE ACTIVOS DE INFORMACIÓN (RAI) - GTI-DI-001.

- Impedir el acceso a la información sin fundamento jurídico.

- Cualquier acción sobre la información que vaya en contravía de lo que se identifica en esta política como un uso aceptable del activo de información.

- **Premisas en el uso Aceptable de los Activos de información**

- El propietario o dueño de la información "*tiene responsabilidad aprobada de la dirección por el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos*"[2]; responsabilidad que cubre la gestión del activo de información dentro de todo su ciclo de vida que incluye su creación, asignación, procesamiento, almacenamiento, transmisión, eliminación y destrucción.
- Los propietarios o dueños de la información deben aplicar el modelo institucional de gestión de riesgos para identificar y tratar los riesgos que puedan afectar a los activos de información que hagan parte del inventario de activos de información a su cargo. Cada líder y responsable de proceso debe coordinar la aplicación del modelo institucional de gestión de riesgos sobre los activos de información a su cargo.
- Es responsabilidad de los usuarios de la SDP que participen en cualquier fase del ciclo de vida del activo de la información, realizar sus mejores esfuerzos para aplicar todos los controles y directrices establecidos en los procedimientos y políticas en el marco de la implementación del Sistema de Gestión de Seguridad de la Información para garantizar la preservación de la Confidencialidad, Integridad y Disponibilidad de la información que está a su cargo y a la que tengan acceso por la naturaleza misma de sus actividades.
- Todas las actividades de administración, operación y uso de la información, realizadas como parte del ciclo de vida[3] de cada activo de información que haga parte del inventario de activos de la SDP deben ser tratados en concordancia con la valoración de la Confidencialidad, Integridad y Disponibilidad reflejada en el REGISTRO DE ACTIVOS DE INFORMACIÓN (RAI) - GTI-DI-001 y consecuentemente la criticidad calculada para el activo.

- **Clasificación de la Información:** Se clasifica según los niveles de Confidencialidad (Pública Reservada, Pública Clasificada y Pública según la Ley 1712 de 2014), Disponibilidad (Alta, Media, Baja) e Integridad (Alta, Media, Baja), determinando la criticidad según la metodología del MinTIC (Guía 5).

  El nivel de confidencialidad del activo de información se determina si la información contiene datos personales y se puede categorizar su información como Pública Reservada, Pública Clasificada y Pública, teniendo en cuenta las definiciones establecidas en la Ley 1712 de 2014.

  Por su parte el nivel de **D**isponibilidad de cada activo reportado será identificado con el fin de identificar los riesgos y controles pertinentes, y se debe valorar la disponibilidad en Alta, Media o Baja según las siguientes consideraciones:

  - Alta: Si se considera que la no disponibilidad del activo de información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
  - Media: Si se considera que la no disponibilidad del activo de información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
  - Baja: Si se considera que la no disponibilidad del activo de información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.

  Finalmente se debe establecer la valoración de la **I**ntegridad de cada activo reportado con el fin de identificar los riesgos y controles pertinentes y se debe valorar la integridad en Alta, Media o Baja según las siguientes consideraciones:

  - Alta: Si se considera que la pérdida de exactitud y completitud del activo de información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
  - Media: Si se considera que la pérdida de exactitud y completitud del activo de información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
  - Baja: Si se considera que la pérdida de exactitud y completitud del activo de información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.

  De acuerdo al resultado de la valoración realizada de la Confidencialidad, Disponibilidad e Integridad, se debe clasificar el activo de información en términos de la criticidad según la metodología y los lineamientos establecidos por el MinTIC en su Guía 5 "*Guía para la Gestión y Clasificación de Activos de información: seguridad y privacidad de la información"*

  - Alta. Activos de información en los cuales la clasificación de la información en dos o todas las propiedades (confidencialidad, integridad, y disponibilidad) es *alta*.

- Media. Activos de información en los cuales la clasificación de la información es alta en una de sus propiedades (confidencialidad, integridad, y disponibilidad) o al menos una de ellas es de nivel *medio*.

- Baja. Activos de información en los cuales la clasificación de la información en todos sus niveles es *baja*.

- **Etiquetado de la Información:** La SDP desarrollará e implementará un procedimiento para el etiquetado de los activos de información en el RAI - GTI-DI-001.

- **Manejo de Activos:** Se aplicará el modelo institucional de gestión de riesgos para los activos clasificados con criticidad ALTA, alineado con la Guía de DAFP y la Guía 5 del MinTIC.

6.3.POLÍTICAS DE CONTROL DE ACCESO LÓGICO

Principios Generales:

La SDP establecerá medidas de control de acceso a toda la información de su propiedad, independientemente del medio de almacenamiento, procesamiento, uso o transmisión (recursos físicos y digitales; ambientes públicos, privados, propios, de terceros o en la nube; redes, sistemas operativos, aplicaciones, sistemas de información; servicios de TI, etc.). El objetivo es limitar y controlar el acceso a la información, estableciendo métodos de autenticación, autorización y auditoría para que solo sea accesible al personal autorizado. El responsable/dueño de la información determinará los privilegios de acceso según el rol autorizado.

Lineamientos Específicos:

1. Segregación de Deberes (Numeral 5.3)

- **Lineamiento:** Se separarán los deberes conflictivos y las áreas conflictivas de responsabilidad para prevenir fraudes, errores y accesos indebidos a la información.

2. Control de Acceso (Numeral 5.15)

- **Lineamiento:** Se establecerán e implementarán reglas para controlar el acceso físico y lógico a la información y otros activos asociados, basándose en los requisitos de seguridad de la información y de la entidad. Se implementarán procedimientos y políticas para el control de acceso a la red, sistemas de información e infraestructura física (instalaciones) para mitigar riesgos de acceso no autorizado. La Dirección de Tecnologías de la Información y las Comunicaciones y la Dirección Administrativa definirán, implementarán, verificarán la eficiencia y efectividad y monitorearán los controles de acceso adecuados para proteger la información y las instalaciones en donde se procesa, almacena, trata y se transmite.

3. Derechos de Acceso (Numeral 5.18)

- **Lineamiento:** Los derechos de acceso a la información y otros activos asociados se proporcionarán, revisarán, modificarán y eliminarán de acuerdo con la política y las reglas de control de acceso específicas. La Dirección de Tecnologías de la Información y las Comunicaciones permitirá el acceso solo a usuarios autorizados según sus funciones y responsabilidades, verificando los privilegios otorgados.

4. Derechos de Acceso Privilegiado (Numeral 8.2)

- **Lineamiento:** La asignación y el uso de derechos de acceso privilegiado se restringirán y gestionarán estrictamente. La Dirección de Tecnologías de la Información y las Comunicaciones gestionará las cuentas de usuario para el acceso a la configuración, sistemas operativos y programas utilitarios. Se realizará una depuración periódica de cuentas de usuario (privilegiadas, de aplicaciones y genéricas).

5. Restricción de Acceso a la Información (Numeral 8.3)

- **Lineamiento:** El acceso a la información y otros activos asociados se restringirá de acuerdo con la política específica sobre control de acceso.

6. Acceso al Código Fuente (Numeral 8.4)

- **Lineamiento:** El acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las bibliotecas de software se gestionará adecuadamente. La Dirección de Tecnologías de la Información y las Comunicaciones controlará el acceso al código fuente de los programas/aplicaciones bajo su administración, otorgándolo exclusivamente a los integrantes del equipo de software y a los administradores de bases de datos.

7. Autenticación Segura (Numeral 8.5)

- **Lineamiento:** Se implementarán tecnologías y procedimientos de autenticación segura en función de las restricciones de acceso a la información y la política específica sobre control de acceso.

8. Prevención de Fuga de Datos (Numeral 8.12)

- **Lineamiento:** Se aplicarán medidas de prevención de fuga de datos (DLP) a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.

9. Gestión de Cuentas de Usuario:

- **Responsabilidades de la Dirección de Tecnologías de la Información y las Comunicaciones:**
  - Establecer los mecanismos de control de acceso necesarios.
  - Analizar y realizar seguimiento permanente de las medidas de control de acceso.
  - Gestionar las cuentas de usuario.
  - Desactivar cuentas inmediatamente después de la desvinculación de usuarios.
  - Coordinar la depuración periódica de cuentas.
  - Asignar y configurar las VPN para acceso remoto seguro.
  - Crear un usuario genérico con clave para el personal de mesa de ayuda (uso exclusivo, con aprobación del usuario final para acceso remoto).
- **Responsabilidades de los Supervisores de Contrato:** Notificar el inicio y la liquidación de contratos y gestionar las cuentas de usuario y permisos correspondientes (según GTI-PD-004 - Gestión Cuentas de Usuario).
- **Responsabilidades de los Jefes:**
  - Guardar en reserva las claves de acceso (intransferibles, de uso institucional y personal, cambio al primer ingreso y actualización mensual).
  - Gestionar las cuentas de usuario para pares que cubran vacaciones, descansos y situaciones administrativas.
  - Delegar a un servidor público (no más de dos) cuando lo considere pertinente. de manera que sea posible la realización de las mismas actividades por parte del par que lo reemplazará, teniendo en cuenta que está delegando responsabilidades para definir el acceso a los activos de información a su cargo.
- **Gestión de Accesos a Sistemas/Aplicaciones:** Se realiza a través del GTI-PD-004 - Gestión Cuentas de Usuario y el GTI-PD-001 - Desarrollo, Instalación y Mantenimiento de Soluciones de Software.

10. Gestión de Perfiles y Privilegios (Numerales 5.15, 5.18, 8.2 y 8.3):

- **Lineamiento:** Los perfiles y privilegios de acceso a las soluciones de software se gestionarán según las funciones o rol del cargo. Los productos de software adquiridos a terceros con cuentas de usuario predeterminadas del proveedor deben ser revisados; si es posible, las cuentas deben ser eliminadas. Si no es posible, los permisos deben restringirse al mínimo necesario y documentarse en el manual técnico/de uso. Cada persona autorizada accederá con una única identificación (cuenta de usuario), con excepciones para administradores de sistemas operativos, bases de datos, equipos de red y seguridad, quienes ocasionalmente podrán usar usuarios propietarios.

11. Responsabilidad del Usuario (Numerales 5.10 y 5.15):

- **Lineamiento:** Todos los usuarios asumirán la responsabilidad sobre la información física o digital a la que accedan y procesen, dándole un uso adecuado para salvaguardar la confidencialidad, integridad y disponibilidad.

12. Gestión del Ciclo de Vida de las Cuentas de Usuario (Numerales 5.15, 5.16 y 5.18):

- **Lineamiento:** La entidad establecerá procedimientos claros para la creación, modificación y eliminación de cuentas de usuario. Todo acceso a sistemas, aplicaciones y/o servicios tecnológicos provistos por la SDP (usuarios internos, externos y terceros) debe ser solicitado y autorizado por el dueño/responsable de la información y/o del proceso, basándose en el principio de mínimos privilegios. Se otorgarán solo los permisos necesarios para las funciones. El responsable/dueño de la información o su delegado (mediante GTI-FO-002 - Solicitud Gestión Cuentas de Usuario) autorizará la creación/actualización/eliminación de cuentas, roles, permisos o privilegios, según los niveles de clasificación de la información (GTI-DI-001 - Registro de Activos de Información (RAI)). Se establecerá un procedimiento para solicitudes de creación, reinicio, cambio de contraseña, acceso a recursos, revisiones periódicas y eliminación de accesos.

13. Compromiso y Confidencialidad (Complemento de Numeral 6.6):

- **Lineamiento:** Todo servidor público o contratista es responsable del uso de la información a la que accede y debe conocer los compromisos adquiridos. Al recibir usuario y contraseña, firmará un acuerdo de compromiso y confidencialidad (GTI-FO-004 ACTA DE COMPROMISO PARA EL USO DE RECURSOS INFORMÁTICOS, GTI-FO-011 - ACTA DE COMPROMISO PARA USUARIOS PRIVILEGIADOS, GTI-FO-012 ACTA DE COMPROMISO PARA ADMINISTRADORES DE APLICACIONES DE LA SDP).

14. Estándares para Contraseñas (Numeral 5.17):

- **Lineamiento:** Todo funcionario, contratista, tercero y pasante con usuario institucional y contraseña para operar como usuario final un sistema, aplicación o servicio tecnológico de la SDP debe seguir los estándares y recomendaciones para la gestión de contraseñas.

15. Gestión de Usuarios Externos (Numeral 5.19 y 5.20):

- **Lineamiento:** Para usuarios externos, la Dirección de Tecnologías de la Información y las Comunicaciones informará por correo electrónico la información de autenticación (previa solicitud del responsable de la SDP), incluyendo los compromisos adquiridos (mínimo los del GTI-PD-004 - Gestión Cuentas de Usuario).

16. Revisiones Periódicas (Numeral 5.36):

- **Lineamiento:** Se realizarán revisiones periódicas de los permisos de acceso para garantizar su pertinencia.

17. Gestión de Accesos (Numeral 5.15 y 5.18):

- **Lineamiento:** La asignación, actualización, suspensión (por situaciones administrativas como vacancia temporal y licencias no remuneradas) o eliminación de accesos a sistemas, aplicaciones y/o servicios tecnológicos se realizará a través del GTI-PD-004 - Gestión Cuentas de Usuario.

18. Gestión de Administradores (Numeral 8.2):

- **Lineamiento:** Todo administrador de un sistema, aplicación, base de datos, equipos de red o cualquier servicio tecnológico debe seguir los estándares y recomendaciones para la gestión de contraseñas.

19. Traslado entre Dependencias (Numeral 5.18):

- **Lineamiento:** En caso de traslado entre dependencias, el jefe del área de destino solicitará la eliminación y/o creación de los permisos requeridos (GTI-FO-002 - Solicitud Gestión Cuentas de Usuario), registrando una incidencia en el sistema de mesa de ayuda.

20. Desvinculación de la Entidad (Numeral 5.11 y 5.18):

- **Lineamiento:** En caso de desvinculación, el jefe inmediato solicitará la cancelación de la cuenta de usuario (GTI-FO-002 - Solicitud Gestión Cuentas de Usuario), registrando una incidencia en el sistema de mesa de ayuda.

21. Ausencia Prolongada (Numeral 5.18):

- **Lineamiento:** En caso de ausencia prolongada (vacaciones, incapacidad, licencias, >15 días calendario), el jefe inmediato o supervisor solicitará la inhabilitación temporal de los accesos (GTI-FO-002 - Solicitud Gestión Cuentas de Usuario), registrando una incidencia en el sistema de mesa de ayuda.

22. Acceso a Salas de Reunión (Numeral 7.2 y 8.1):

- **Lineamiento:** Para el acceso a los equipos de las salas de reunión, se asigna una única cuenta genérica para la red (administrada por la Dirección de Tecnologías de la Información y las Comunicaciones). Para acceder a recursos compartidos, correo institucional o cualquier servicio tecnológico en nombre propio, se usará el usuario y contraseña personal.

23. Reporte de Incumplimientos (Numeral 5.24, 5.25 y 5.26):

- **Lineamiento:** Cualquier incumplimiento de las reglas de control de acceso que ponga en riesgo la CID de la información se reportará como un incidente de seguridad (GTI-PD-008 - Gestión de Incidentes de Seguridad y Privacidad en la SDP).

24. Requisitos de Seguridad en el Desarrollo de Software (Numeral 8.25, 8.26, 8.27, 8.28, 8.29 y 8.30):

- **Lineamiento:** Los procesos de construcción de software (internos o por terceros) incluirán en la definición de requerimientos los aspectos de seguridad de la información (CID, autenticidad, responsabilidad y fiabilidad), según el tipo de solución, contemplando perfiles, roles, rangos de acceso y manejo de contraseñas. Esta actividad estará a cargo del usuario funcional con la asistencia de la Dirección de Tecnologías de la Información y las Comunicaciones, según el GTI-PD-001 - DESARROLLO, INSTALACIÓN Y MANTENIMIENTO DE SOLUCIONES DE SOFTWARE y su artefacto GTI-FO-006 - SOLICITUD DE REQUERIMIENTO DE USUARIO (SISTEMAS DE INFORMACIÓN / SOLUCIONES DE SOFTWARE).

6.4.POLÍTICAS SOBRE CRIPTOGRAFÍA

En cumplimiento con la norma ISO/IEC 27001:2022, categoría A.8, control 8.24 (Uso de Criptografía), la SDP define esta política para establecer lineamientos y pautas para el uso y salvaguarda de las firmas digitales adquiridas y asignadas a los servidores públicos que lo requieran.

Lineamientos Específicos:

1. Implementación de Cifrado:

- **Lineamiento:** La SDP implementará herramientas de cifrado para proteger la confidencialidad, integridad y disponibilidad de la información. La Dirección de Tecnologías de la Información y las Comunicaciones determinará los equipos que requerirán controles criptográficos adicionales. Se utilizarán mecanismos de encriptación para proteger la información transportada por dispositivos móviles/removibles o a través de líneas de comunicación.

2. Adquisición y Gestión de Certificados de Firma Digital:

- **Lineamiento:** La Dirección de Tecnologías de la Información y las Comunicaciones gestionará la adquisición de certificados de firma digital según el presupuesto asignado. Gestionará ante la firma certificadora la asignación de la firma digital (token físico USB o virtual) según los protocolos y la documentación exigida. Controlará el inventario, la asignación y las fechas de entrega/vencimiento de las firmas digitales. Apoyará la instalación y configuración de los certificados, siguiendo los lineamientos de la firma certificadora. Proporcionará soporte técnico al suscriptor o gestionará el soporte ante la firma certificadora. Gestionará con la entidad certificadora la reposición en caso de pérdida o daño del certificado físico. Aplicará los protocolos de la entidad certificadora para la finalización del servicio.

3. Valoración de Riesgos en la Adquisición:

- **Lineamiento:** En la adquisición de certificados de firma digital, se realizará una valoración de riesgos para identificar el nivel de protección requerido, considerando el tipo, la fortaleza y la calidad del algoritmo de encriptación, y el impacto del uso de información encriptada en los controles que dependen de la inspección del contenido.

4. Roles y Responsabilidades en la Gestión de Certificados:

- **Lineamiento:** La Dirección de Tecnologías de la Información y las Comunicaciones establecerá los roles y las responsabilidades en la gestión de los certificados de firma digital, identificando al responsable de la implementación de la política y al responsable de la gestión de claves (incluyendo la generación).

5. Uso de Certificados Digitales:

- **Lineamiento:** La SDP utilizará certificados digitales de un prestador de servicios de certificación reconocido y homologado por la ONAC. Antes de emitir un certificado, se verificará la identidad de la entidad prestadora, validando la documentación que demuestre su reconocimiento por la ONAC.

6. Proceso de Generación y Emisión de Certificados:

- **Lineamiento:** La Dirección de Tecnologías de la Información y las Comunicaciones definirá el proceso para generar y emitir un certificado digital, incluyendo la generación de claves criptográficas y la firma del certificado por una autoridad de certificación (CA).

7. Políticas para la Gestión de Claves:

- **Lineamiento:** La Dirección de Tecnologías de la Información y las Comunicaciones establecerá políticas para la gestión de claves en los procesos de generación, almacenamiento y manejo seguro de las claves criptográficas asociadas a los certificados digitales.

8. Tiempo de Validez y Renovación:

- **Lineamiento:** La Dirección de Tecnologías de la Información y las Comunicaciones establecerá el tiempo de validez de un certificado digital antes de requerir su renovación.

9. Gestión de Llaves y Recuperación de Información:

- **Lineamiento:** La Dirección de Tecnologías de la Información y las Comunicaciones gestionará las llaves y los métodos para la protección de llaves criptográficas y la recuperación de información encriptada. Documentará el procedimiento de revocación de certificados (pérdida, compromiso o daño de claves privadas).

10. Publicación de Certificados:

- **Lineamiento:** La publicación de certificados emitidos se realizará a través de un repositorio o directorio de certificados.

11. Responsabilidades del Suscriptor:

- **Lineamiento:** El suscriptor debe:

  - Suministrar la documentación requerida por la entidad certificadora.
  - Responder a las comunicaciones de la entidad certificadora.
  - Recibir el certificado (token físico o virtual) según el protocolo definido.
  - Cambiar la contraseña inicial del certificado y seguir los lineamientos de gestión de contraseñas.
  - Usar el certificado exclusivamente para la gestión institucional en representación de la SDP.
  - Informar inmediatamente a la Dirección de Tecnologías de la Información y las Comunicaciones sobre cualquier inconveniente (bloqueos, pérdida o daño del token físico).
  - Conocer la fecha de vencimiento e informar a la Dirección de Tecnologías de la Información y las Comunicaciones al menos 5 días hábiles antes para la renovación.
  - Salvaguardar y custodiar el certificado, y entregarlo a la Dirección de Tecnologías de la Información y las Comunicaciones al renovarlo o al terminar su vinculación.

- Atender las recomendaciones de uso del certificado dadas por la firma certificadora.

12. Responsabilidades de la Entidad Certificadora:

- **Lineamiento:** La entidad certificadora debe:

  - Entregar a la SDP el procedimiento de solicitud de asignación del certificado, manuales de instalación y configuración, e información relevante.

  - Emitir o revocar los certificados solicitados por la SDP.

  - Entregar el certificado según el protocolo establecido en el contrato.

  - Dar soporte en la instalación, configuración y uso del certificado.

6.5.POLÍTICAS DE SEGURIDAD FÍSICA Y DEL ENTORNO

Principio General:

Esta política define las medidas para proteger la infraestructura física de la SDP, incluyendo accesos, sistemas de seguridad y control ambiental. Establece medidas efectivas para el control de acceso físico a las áreas e infraestructura donde se custodia y administra información sensible. Aplica a todos los funcionarios, contratistas y usuarios externos que ingresen a las instalaciones.

Lineamientos Específicos:

1. Perímetros Físicos de Seguridad (Numeral 7.1):

- **Lineamiento:** Los perímetros de seguridad se definirán y utilizarán para proteger las áreas que contienen información y otros activos asociados. En la SDP, los perímetros están delimitados por las recepciones y el sistema de control de acceso. Se definen áreas de acceso restringido, señalizadas y con control especial.

Área	Acceso Restringido	• Señalizado y controlado por
Complejo CAD		
• Lobby de acceso a las torres A y B - Recepción	• Si. Control de ingreso de personal con tarjetas de proximidad o con cédula dependiendo del rol.	• SHD
• Lobby de acceso a las torres A y B - Ingreso a subestaciones y cuartos eléctricos	• Si. Únicamente para personal técnico y con autorización previa de la SHD.	• SHD
• Hall acceso ascensores	• Si. Control de ingreso de personal con tarjetas de proximidad o con cédula dependiendo del rol.	• SHD
• Puntos fijos para acceso (escaleras y pasillo zonas comunes)	• Si. Control de ingreso de personal con tarjetas de proximidad o con cédula dependiendo del rol.	• SHD
• Zonas de servicio (baños y cafetería)	• Si. Control de ingreso de personal con control biométrico para los baños. •	• SDP

	•	
• Puntos fijos para acceso (cuartos eléctricos en cada piso y ambos costados)	• Si. Únicamente para personal técnico y con autorización previa de la SHD. • •	• SHD
• Lobby de acceso a pisos	• Si. Control de ingreso de personal con control biométrico, tarjetas de proximidad o cédula dependiendo del rol. • •	• SDP
• Áreas internas de oficina - abierta	• Si. Personal autorizado o con carné. • •	• SDP
• Áreas internas de oficina abierta - áreas privadas (salas de juntas, oficinas de directivos, áreas técnicas controladas)	• Si. Personal autorizado o con carné. •	• SDP
• Áreas internas de archivos de gestión (Control Interno Disciplinario, Gestión Contractual, Gestión Financiera)	Si. Personal autorizado o con carné. • En todas las áreas se pide el carnet a los servidores y contratistas y se registran en las bitácoras de vigilancia. • Se siguen los controles de ingreso definidos por hacienda en el edificio. •	• SDP
• Área de atención al ciudadano - Notificaciones	• Si. Control de ingreso de personal con carné o con cédula dependiendo del rol. • •	• SDP
• Centros de cableado (uno por piso)	• Si. Únicamente para personal técnico y con autorización previa de la SDP, con control biométrico.	• SDP
• Centro de cómputo - piso 5	• Si. Únicamente para personal técnico y con autorización previa de la SDP, con control biométrico.	• SDP

• Centro de cómputo - piso 2 Supercade	• Si. Únicamente para personal técnico y con autorización previa de la SHD.	• SHD
• Oficina de ventanilla de radicación.	• Si. Únicamente para personal autorizado.	• SDP
• Oficina y zona de archivo para Planoteca, Biblioteca y Manzanas y Urbanismos.	• Si. Únicamente para personal autorizado.	• SDP
• Oficina y zona de archivo - Historias laborales	• Si. Únicamente para personal autorizado. •	• SDP
• Zonas de consulta	• Si. Control de ingreso de personal con carné o con cédula dependiendo del rol. Zona contralada por vigilancia adicional. • El usuario llega toma un turno y espera para ser atendido no tiene acceso a las áreas donde está la documentación • Si requiere copias las entrega el personal de fotocopiado, nadie toma los planos originales y hay un arquitecto de servicio al ciudadano • Se cuenta con cámaras de video.	• SDP
• Área de atención - Módulos de atención	• Si. Control de ingreso de personal con carné o con cédula dependiendo del rol.	• SHD
Archivo Central - Sede Montevideo		
• Lobby de acceso a la sede.	• Si. Control de ingreso de personal con carné o con cédula dependiendo del rol. • El control está documentado. •	• SDP
• Zonas de servicio (baño para público)	• Si. Control de ingreso de personal con carné o con cédula dependiendo del rol. • Se cuenta con baños para	• SDP

	• usuarios y otros para servidores públicos •	
• Zonas de consulta	• Si. Control de ingreso de personal con carné o con cédula dependiendo del rol. Zona contralada por vigilancia adicional.	• SDP
• Oficina de atención - archivo central de predios.	• Si. Únicamente para personal autorizado con carné. • •	• SDP
• Área de archivo central de predios. (Estantería de almacenamiento)	• Si. Únicamente para personal autorizado con carné.	• SDP
• Áreas internas de oficina - abierta	• Si. Personal autorizado o con carné.	• SDP
• Áreas internas de oficina abierta - áreas privadas (oficinas directivos y áreas técnicas controladas)	• Si. Personal autorizado o con carné.	• SDP
• Zonas de servicio (baños y cafetería)	• Si. Control de ingreso de personal con carné para los baños. •	• SDP
• Centros de cableado	• Si. Únicamente para personal técnico y con autorización previa de la SDP.	• SDP

2. Entrada Física (Numeral 7.2):

- **Lineamiento:** Las áreas seguras deben estar protegidas por controles de entrada y puntos de acceso apropiados. Se implementará control de ingreso con tarjetas de proximidad, cédula o control biométrico, según el rol y el área.

3. Asegurar Oficinas, Salas e Instalaciones (Numeral 7.3):

- **Lineamiento:** Se diseñará e implementará la seguridad física de las oficinas, salas e instalaciones. Se implementarán controles de acceso diferenciados según el tipo de área (ej. áreas de servicio, áreas internas de oficina, centros de cableado, centros de cómputo, archivos, etc.).

Área Segura	• Procedimiento y normatividad asociada	Dependencia a cargo
Complejo CAD		
• Lobby de acceso a las torres A y B - Ingreso a subestaciones y cuartos eléctricos	• Reglamento RETIE y RETILAP • NTC2050	• SHD - Administración
• Puntos fijos para acceso	• Reglamento RETIE y	• SHD - Administración

(cuartos eléctricos en cada piso y ambos costados)	RETILAP • NTC2050 Acta 31 de enero de 2011 DADEP GAD-PD-011 MANTENIMIENTO LOCATIVO.	• SDP - Dirección Administrativa
• Áreas internas de archivos de gestión	• GAD-MA-001 REGLAMENTO DE ARCHIVO • GAD-IN-003 INSTRUCTIVO PARA EL ALMACENAMIENTO DE EXPEDIENTES •	• SDP - Oficinas - Sitios destinados a la custodia de archivos de gestión.
• Centros de cableado (uno por piso)	• Reglamento RETIE y RETILAP • NTC2050 Acta 31 de enero de 2011 DADEP GAD-PD-011 MANTENIMIENTO LOCATIVO	• SDP - Dirección de Tecnologías de la Información y las Comunicaciones. • SDP - Dirección Administrativa
• Centro de cómputo - piso 5	• ANSI/TIA-942 - Tier 2.	• SDP - Dirección de Tecnologías de la Información y las Comunicaciones.
• Centro de cómputo - piso 2 Supercade	• ANSI/TIA-942 - Tier 3.	• SHD • SDP - Dirección de Tecnologías de la Información y las Comunicaciones.
• Oficina de ventanilla de radicación.	• GAD-MA-001 REGLAMENTO DE ARCHIVO • GAD-IN-003 INSTRUCTIVO PARA EL ALMACENAMIENTO DE EXPEDIENTES	• SDP - Dirección Administrativa
• Oficina y zona de archivo para Planoteca, Biblioteca y Manzanas y Urbanismos.	• GAD-MA-001 REGLAMENTO DE ARCHIVO • GAD-IN-003 INSTRUCTIVO PARA EL ALMACENAMIENTO DE EXPEDIENTES	• SDP - Dirección Administrativa
• Oficina y zona de archivo - Historias laborales	• GAD-MA-001 REGLAMENTO DE ARCHIVO GAD-IN-003 INSTRUCTIVO	• SDP - Dirección de Talento Humano •

	PARA EL ALMACENAMIENTO DE EXPEDIENTES	•
Archivo Central - Sede Montevideo		
• Área de archivo central de predios. (Estantería de almacenamiento)	• GAD-MA-001 REGLAMENTO DE ARCHIVO • GAD-IN-003 INSTRUCTIVO PARA EL ALMACENAMIENTO DE EXPEDIENTES •	• SDP - Dirección Administrativa
• Centros de cableado	• Reglamento RETIE y RETILAP • NTC2050 Acta 31 de enero de 2011 DADEP GAD-PD-011 MANTENIMIENTO LOCATIVO	• SDP - Dirección de Tecnologías de la Información y las Comunicaciones. • SDP - Dirección Administrativa

4. Monitoreo de Seguridad Física (Numeral 7.4):

- **Lineamiento:** Los locales deberán ser monitoreados continuamente para el acceso físico no autorizado, mediante personal de vigilancia, sistemas de CCTV y bitácoras de registro.

5. Protección contra Amenazas Físicas y Ambientales (Numeral 7.5):

- **Lineamiento:** Se debe diseñar e implementar la protección contra amenazas físicas y ambientales, como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura. Las instalaciones con información reservada o restringida contarán con sistemas de alarmas, cámaras de seguridad y sistemas de detección y extinción de incendios. Los equipos se mantendrán aislados de amenazas como fuego, agua, polvo, vibración e interferencia electromagnética. Los equipos del Centro de Cómputo tendrán control de temperatura y humedad.

6. Trabajar en Áreas Seguras (Numeral 7.6):

- **Lineamiento:** Se diseñarán e implementarán medidas de seguridad para trabajar en áreas seguras. Se definen áreas seguras con acceso autorizado por la dependencia a cargo, que deben mantenerse en orden, limpieza y con elementos exclusivos para la operación del área. Se definen procedimientos y normatividad asociada para cada área segura (ej. Reglamento RETIE y RETILAP, NTC2050, GAD-MA-001, GAD-IN-003, ANSI/TIA-942).

7. Control de Acceso a Áreas de Despacho y Carga:

- **Lineamiento:** Se garantizarán controles de seguridad para el acceso a las áreas de despacho y de carga, aislándolas de las zonas de trabajo y de aquellas donde se custodie información reservada o restringida.

8. Acceso a Instalaciones de Procesamiento de Información:

- **Lineamiento:** Tendrán acceso a las instalaciones de procesamiento de información (infraestructura tecnológica) los administradores y operadores de infraestructura y los proveedores de servicio técnico autorizados, cumpliendo las normas de acceso físico de la Dirección Administrativa (Numeral 7 - Controles Físicos) y de la Secretaría Distrital de Hacienda (para el Data Center).

9. Mecanismos de Seguridad en Instalaciones:

- **Lineamiento:** Se implementarán mecanismos de seguridad en las instalaciones mediante infraestructura física, recurso humano y medios tecnológicos (autenticación biométrica, tarjetas de proximidad, CCTV, etc.).

6.6.POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES

Principio General:

Con el fin de asegurar las operaciones realizadas en los recursos tecnológicos que soportan la operación del negocio, la SDP planea, gestiona, respalda y monitorea la infraestructura tecnológica siguiendo los lineamientos de los procedimientos del SGSI.

Lineamientos Específicos:

1. Procedimientos Operativos Documentados (Numeral 5.37):

- **Lineamiento:** Los procedimientos operativos para las instalaciones de procesamiento de información deben documentarse y ponerse a disposición del personal que los necesite.

2. Gestión de Capacidad (Numeral 8.6):

- **Lineamiento:** El uso de los recursos se controlará y ajustará de acuerdo con los requisitos de capacidad actuales y previstos.

3. Protección contra Malware (Numeral 8.7):

- **Lineamiento:** La protección contra el malware se implementará y respaldará mediante la conciencia adecuada del usuario.

4. Gestión de Vulnerabilidades Técnicas (Numeral 8.8):

- **Lineamiento:** Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información, evaluar la exposición de la organización y tomar las medidas apropiadas.

5. Gestión de la Configuración (Numeral 8.9):

- **Lineamiento:** Las configuraciones (incluidas las de seguridad) de hardware, software, servicios y redes deben establecerse, documentarse, implementarse, monitorearse y revisarse.

6. Eliminación de Información (Numeral 8.10):

- **Lineamiento:** La información almacenada en los sistemas de información, dispositivos o en cualquier otro medio se eliminará cuando ya no sea necesaria.

7. Prevención de Fuga de Datos (Numeral 8.12):

- **Lineamiento:** Las medidas de prevención de fuga de datos se aplicarán a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.

8. Redundancia de las Instalaciones de Procesamiento de Información (Numeral 8.14):

- **Lineamiento:** Las instalaciones de procesamiento de información se implementarán con suficiente redundancia para cumplir con los requisitos de disponibilidad.

9. Actividades de Seguimiento (Numeral 8.16):

- **Lineamiento:** Las redes, los sistemas y las aplicaciones deberán ser monitoreados por comportamiento anómalo y se tomarán las acciones apropiadas para evaluar posibles incidentes de seguridad de la información.

10. Sincronización de Reloj (Numeral 8.17):

- **Lineamiento:** Los relojes de los sistemas de procesamiento de información deben estar sincronizados con las fuentes de

tiempo aprobadas.

11. Instalación de Software en Sistemas Operativos (Numeral 8.19):

- **Lineamiento:** Se implementarán procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas operativos.

12. Seguridad en Redes (Numeral 8.20):

- **Lineamiento:** Las redes y los dispositivos de red se asegurarán, administrarán y controlarán para proteger la información en los sistemas y aplicaciones.

13. Seguridad de los Servicios de Red (Numeral 8.21):

- **Lineamiento:** Se identificarán, implementarán y controlarán los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red.

14. Segregación de Redes (Numeral 8.22):

- **Lineamiento:** Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en las redes de la organización.

15. Filtrado Web (Numeral 8.23):

- **Lineamiento:** El acceso a sitios web externos se gestionará para reducir la exposición a contenido malicioso.

6.7.POLÍTICAS COPIAS DE RESPALDO Y RECUPERACIÓN DE LAINFORMACIÓN INSTITUCIONAL

En cumplimiento con la norma ISO/IEC 27001:2022, categoría A.8, numeral 8.13 (Copia de seguridad de la información), la SDP establece esta política para definir los lineamientos y directrices para la realización de copias de respaldo de la información alojada en su infraestructura y su restauración efectiva ante fallas, errores o eventos malintencionados, asegurando la continuidad y seguridad de la información crítica y mitigando el riesgo de pérdida.

Lineamientos Específicos:

1. Identificación de Activos de Información:

- **Lineamiento:** La SDP debe definir y documentar los activos críticos de información que requieren respaldo. La información en equipos de cómputo de servidores públicos solo se respaldará por demanda, mediante el procedimiento de Gestión de Copias de Respaldo y previa solicitud en la mesa de ayuda. Las copias de respaldo de sistemas de información y aplicaciones incluirán la información de configuración y datos necesarios para la recuperación completa, con guías documentadas en el sistema de versionamiento, incluyendo manuales de instalación y configuración. La información en carpetas compartidas se respaldará según los lineamientos para la Gestión de Carpetas Compartidas. Los dueños de la información son responsables de definir los lineamientos de custodia y salvaguarda, concertados con la Dirección de Tecnologías de la Información y las Comunicaciones y ajustados a los recursos disponibles.

2. Frecuencia y Programación de Copias de Respaldo:

- **Lineamiento:** La Dirección de Tecnologías de la Información y las Comunicaciones establecerá la frecuencia regular de las copias de respaldo, considerando la criticidad de la información. Los dueños de la información definirán la frecuencia para su información. La Dirección de Tecnologías de la Información y las Comunicaciones programará y automatizará los procesos de respaldo, garantizando su consistencia y cumplimiento. En la configuración de nuevos respaldos, el responsable de la información definirá el nivel adecuado según las necesidades y recursos, indicando la frecuencia (diaria, semanal, mensual, anual o por demanda, siendo mensual por defecto para la información en servidores) y el período de retención, según las necesidades del área, la legislación y la normatividad aplicable.

3. Almacenamiento Seguro:

- **Lineamiento:** La información de las copias de respaldo custodiada por la Dirección de Tecnologías de la Información y las Comunicaciones se alojará en la infraestructura tecnológica de la SDP (servidores y equipos de almacenamiento). Se procurará almacenar los medios magnéticos en un sitio diferente y alejado de las sedes de la entidad (cintoteca y/o contrato de guarda custodia), llevando un registro de las acciones. Las copias de respaldo no se entregarán a servidores y contratistas sin autorización del dueño de la información o jefe de la dependencia. La Dirección de Tecnologías de la Información y las Comunicaciones establecerá mecanismos para restringir el acceso a las copias de respaldo a personal autorizado.

4. Procedimientos de Recuperación:

- **Lineamiento:** Anualmente, se elaborará e implementará un plan de restauración de copias de respaldo, con pasos específicos y roles responsables, con aprobación del Director de Tecnologías de la Información y las Comunicaciones y los líderes de los equipos de trabajo, incluyendo al equipo de seguridad de la información. La Dirección de Tecnologías de la Información y las Comunicaciones elaborará, aprobará y mantendrá actualizado el procedimiento para la generación de copias de respaldo y recuperación de la información (GTI-PD-003 Copias de Seguridad Y Recuperación de Información). Se realizarán pruebas regulares (simulacros periódicos) para verificar la efectividad del plan y garantizar la idónea generación y restauración de copias de respaldo, considerando la disponibilidad de recursos.

5. Análisis de Entornos y Recursos:

- **Lineamiento:** La Dirección de Tecnologías de la Información y las Comunicaciones identificará y garantizará la disponibilidad de los recursos tecnológicos necesarios para las actividades de respaldo y recuperación. Realizará un análisis de los entornos donde reside la información (desarrollo, pruebas, producción y recursos compartidos), identificando los recursos tecnológicos necesarios y procurando su disponibilidad y adaptabilidad a los cambios en la infraestructura y las mejores prácticas de seguridad.

6. Protección de Registros:

- **Lineamiento:** Para la protección de registros contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, se garantizará la copia de la base de datos de las herramientas de copias de respaldo, dejando los registros para garantizar la restauración y el acceso posterior. La Dirección de Tecnologías de la Información y las Comunicaciones salvaguardará los medios de respaldo fuera de las instalaciones de la SDP para garantizar la disponibilidad de la información en caso de desastre.

7. Responsabilidades (Numeral 5.10):

- **Lineamiento:** Para la aplicación de esta política, se tendrán en cuenta los roles y responsabilidades definidos en el GTI-MA-003 - Roles y Responsabilidades de Seguridad de la Información en la SDP.

    - **Dueño de la información:** Identificar y describir los activos de información que requieren respaldo, recibir la información almacenada en SharePoint al retiro de servidores y contratistas (asegurando la transferencia a una cuenta corporativa o la administración por personal de planta), y definir los niveles de protección, acceso y frecuencia requeridos según la criticidad.

    - **Usuarios Privilegiados (Administrador de la herramienta de copias de respaldo):** Generar el plan de restauración, configurar las políticas/jobs en las herramientas de respaldo, asegurar el respaldo de la información según los recursos disponibles y las especificaciones de los dueños de la información, asegurar el respaldo de las bases de datos (en coordinación con el administrador de bases de datos), monitorear la ejecución de las copias de respaldo, alertar sobre errores, depurar la información temporal, etiquetar los medios de almacenamiento, realizar pruebas de recuperación (con el apoyo de los líderes de la Dirección de Tecnologías de la Información y las Comunicaciones, según GTI-PD-003), velar por el cumplimiento del procedimiento, generar y actualizar la guía de copias de respaldo (incluyendo la guía de recuperación), y realizar un chequeo periódico de las políticas configuradas vs el inventario de infraestructura.

    - **Administrador de bases de datos:** Generar los scripts para las copias de respaldo en disco, ejecutar los scripts para las solicitudes por demanda, asegurar la disponibilidad de las copias de respaldo en disco para llevar a cinta, informar al administrador de la herramienta de copias de respaldo sobre novedades de bases de datos, participar en el plan de restauración, y generar las guías de recuperación de la infraestructura que administra.

    - **Administrador de sistemas operativos:** Instalar los agentes de copia de respaldo al desplegar una máquina en la

infraestructura, e informar al administrador de la herramienta de copias de seguridad sobre modificaciones en los servidores.

- **Líder de Software de la Dirección de Tecnologías de la Información y las Comunicaciones:** Participar en la generación y ejecución del plan de restauración para las pruebas de restauración.

- **Líder de infraestructura de la Dirección de Tecnologías de la Información y las Comunicaciones:** Gestionar la actualización del licenciamiento de la herramienta de copias de respaldo y participar anualmente en el plan de restauración.
- **Líder de soporte de la Dirección de Tecnologías de la Información y las Comunicaciones:** Participar anualmente en la generación del plan de restauración, gestionar el contrato de Guarda custodia (si aplica), y liderar la gestión de los servicios relacionados con la generación de copias de respaldo y recuperación por demanda siguiendo el procedimiento creado para tal fin.

6.8.POLÍTICAS SOBRE LAINFRAESTRUCTURAFÍSICA, INSTLACIONES ELECTRICAS Y DE DATOS

Principio General:

Con el fin de asegurar las operaciones realizadas en los recursos tecnológicos que soportan la operación de la entidad, la SDP planea, gestiona, respalda y monitorea la infraestructura tecnológica siguiendo los lineamientos establecidos en los procedimientos del SGSI. Esta política se centra en la protección de las instalaciones de procesamiento de información contra interrupciones y la seguridad del cableado.

Lineamientos Específicos:

1. Utilidades de Apoyo (Numeral 7.11):

- **Lineamiento:** Las instalaciones de procesamiento de información deben estar protegidas contra cortes de energía y otras interrupciones causadas por fallas en los servicios públicos de apoyo. La SDP debe contar con un Sistema de Energía Interrumpible (UPS) y/o plantas eléctricas para asegurar el apagado regulado y sistemático de los equipos de cómputo, garantizando la continuidad de las operaciones durante el restablecimiento del suministro eléctrico y contrarrestando el riesgo de pérdida de información y daño de equipos.

2. Seguridad del Cableado (Numeral 7.12):

- **Lineamiento:** Los cables que transportan energía, datos o servicios de información de apoyo deben estar protegidos contra intercepciones, interferencias o daños. La SDP debe contar con:

  - Tableros eléctricos de control de circuitos plenamente marquillados e identificados, con breakers para el corte general o parcial de energía en caso de emergencia.

  - Cumplimiento de los requisitos técnicos de la normatividad vigente, principalmente los Reglamentos RETIE y RETILAP y la norma NTC2050.

  - Iluminación de emergencia en caso de falla en el suministro principal de energía.

  - Protección contra descargas eléctricas (sistema de puesta a tierra).

  - Conexiones adecuadas para la energía eléctrica y la red de datos.

  - Protección del cableado de red contra intercepción no autorizada, utilizando conductos como canaletas.

  - Separación del cableado eléctrico y el cableado de red para evitar interferencias.

3. Restricciones en la Conexión de Dispositivos:

- **Lineamiento:** Ningún usuario diferente a los profesionales encargados en la Dirección de Tecnologías de la Información y las Comunicaciones o la Dirección Administrativa deberá conectar aparatos o dispositivos eléctricos diferentes a los equipos de

cómputo y teléfono asignados por la entidad para la realización de sus labores.

Detalle de los Lineamientos:

- **Continuidad del Negocio (Relacionado con 7.11):** La implementación de UPS y/o plantas eléctricas, junto con procedimientos de apagado regulado, busca minimizar el impacto de interrupciones en el suministro eléctrico sobre las operaciones de la SDP, asegurando la disponibilidad de los servicios y la integridad de la información.

- **Seguridad Eléctrica (Relacionado con 7.11 y 7.12):** El cumplimiento de RETIE, RETILAP y NTC2050 garantiza la seguridad de las instalaciones eléctricas, minimizando riesgos de accidentes y daños a los equipos. El marquillado e identificación de los tableros eléctricos facilita la gestión y el control de la energía. La iluminación de emergencia asegura la visibilidad y la seguridad en caso de corte de energía.

- **Protección contra Interferencia y Daños (Relacionado con 7.12):** La separación del cableado eléctrico y de red, el uso de canaletas y la protección contra descargas eléctricas minimizan el riesgo de interferencias electromagnéticas, daños físicos al cableado y la intercepción no autorizada de datos.

- **Control de Conexiones (Relacionado con 7.12):** La restricción en la conexión de dispositivos eléctricos no autorizados previene sobrecargas, cortocircuitos y otros problemas eléctricos que podrían afectar la infraestructura.

6.9.POLITICAGESTIÓN DE CARPETAS COMPARTIDAS

Principio General:

La SDP establece estos lineamientos para la gestión de carpetas compartidas (servidores on-premise y SharePoint), permitiendo administrar la información contenida en estos recursos. Este lineamiento se alinea con la Norma ISO/IEC 27001 versión 2022 - Categoría A.8 Controles tecnológicos, Control 8.2 (Derechos de acceso privilegiado) y Control 8.3 (Restricción de acceso a la información).

Lineamientos Específicos:

1. Espacios Compartidos:

- **Lineamiento:** Las áreas o usuarios que requieran compartir información institucional podrán utilizar los siguientes espacios compartidos: \Areas\Privada, \Areas\Pública, \[Tema_Específico], y \Unidades Compartidas\Drive.

2. Carpetas Privadas (\Areas\Privada):

- **Consideraciones Generales:**

  - **Lineamiento:** Se crean subcarpetas por cada Dependencia. El acceso se otorga con la creación de la cuenta en Directorio Activo. Los usuarios pueden crear, actualizar, eliminar y compartir información dentro de su subcarpeta. La responsabilidad de la seguridad de la información es compartida. Se permiten máximo tres niveles de subcarpetas, con nombres cortos (máximo 30 caracteres). Cada servidor público es responsable de la información y su administración. La organización y administración del contenido es competencia de los administradores asignados por cada dependencia.

- **Capacidad de Almacenamiento:**

  - **Lineamiento:** Cada subcarpeta de área tiene una cuota máxima de 12 Gigas. La cuota por usuario es de máximo 2 Gigas, compartida entre \Areas\Privada y \Areas\Pública.

- **Depuración de la Información:**

  - **Lineamiento:** Cada área es responsable de depurar la información almacenada, manteniendo solo información institucional importante. Se avisará al usuario cuando se alcance la cuota individual o de la Dependencia.

- **Respaldo de la Información:**

- **Lineamiento:** Se realiza copia de respaldo según el procedimiento GTI-PD-003 Copias de Seguridad y Recuperación de Información. Se recomienda trasladar la información importante de los equipos de usuario final a la carpeta del área para garantizar su protección.

3. Carpetas Públicas (\Areas\Pública):

- **Consideraciones Generales:**

  - **Lineamiento:** Contiene carpetas por Despacho, Subsecretaría y Oficina (sin subcarpetas para Dirección ni Subdirección). La información se cataloga como información de paso. Los usuarios pueden crear, actualizar y eliminar información en su subcarpeta. Los usuarios de otras áreas tendrán acceso de lectura. Se recomienda máximo tres niveles de subcarpetas. Cada área es responsable de la información. No se debe publicar información confidencial. Se debe borrar la información una vez cumplida su función.

- **Capacidad de Almacenamiento:**

  - **Lineamiento:** La cuota máxima para \Areas\Pública es de 100 Gigas. La cuota por usuario es de máximo 2 Gigas, compartida entre \Areas\Privada y \Areas\Pública.

- **Depuración de la Información:**

  - **Lineamiento:** La información es de carácter temporal y se borra mensualmente (archivos con más de 45 días sin actualizar) sin previo aviso por la Dirección de Tecnologías de la Información y las Comunicaciones los días 15 de cada mes.

- **Respaldo de la Información:**

  - **Lineamiento:** No se realiza respaldo de la información en \Areas\Pública. Es responsabilidad del usuario tener una copia en otro medio o solicitar un respaldo por demanda (GTI-PD-003).

4. Carpetas Específicas (\[Nombre_Tema_Específico]):

- **Consideraciones Generales:**

  - **Lineamiento:** Se crean previa solicitud del Jefe de área (GTI-FO-002) a través de la Mesa de Ayuda (GTI-PD-004), indicando el nombre, los usuarios, el tipo de acceso y la justificación. El Grupo de Infraestructura evalúa la viabilidad. Los nuevos usuarios se incluyen con solicitud del Jefe solicitante. Se recomienda máximo tres niveles de subcarpetas y nombres cortos. Cada usuario es responsable de la información. La administración del contenido es competencia del Jefe solicitante o su delegado.

- **Capacidad de Almacenamiento:**

  - **Lineamiento:** La capacidad se asigna según la disponibilidad de recursos y el requerimiento del Jefe solicitante.

- **Depuración de la Información:**

  - **Lineamiento:** El equipo de trabajo autorizado es responsable de depurar la información, manteniendo solo información institucional importante. Se informa a los usuarios cuando se alcanza la capacidad.

- **Respaldo de la Información:**

  - **Lineamiento:** Se realiza copia de respaldo según el procedimiento GTI-PD-003.

5. Carpetas Compartidas en SharePoint:

- **Consideraciones Generales:**

  - **Lineamiento:** Los servidores públicos y contratistas pueden crear recursos compartidos en SharePoint para temas institucionales transversales. Los nuevos miembros se gestionan por el Administrador de la carpeta. Se recomienda máximo tres niveles de subcarpetas. Cada miembro es responsable de la información. La administración del contenido es responsabilidad del equipo de trabajo autorizado por el Administrador.

- **Capacidad de Almacenamiento:**

  - **Lineamiento:** La capacidad es de 5 Teras de almacenamiento compartido por usuario con cuenta @sdp.gov.co.

- **Depuración de la Información:**

  - **Lineamiento:** El equipo de trabajo autorizado por el Administrador es responsable de depurar la información.

- **Respaldo de la Información:**

  - **Lineamiento:** El propietario debe ceder la propiedad de los archivos a otro funcionario vinculado al retirarse (GTH-FO-017) o registrarlo en el informe final (contratistas). La información eliminada en SharePoint tiene 25 días para su restauración.

6. Otras Consideraciones para la Gestión de Carpetas Compartidas (Aplicable a todas las carpetas compartidas):

- **Lineamiento:**

  - **Uso de caracteres:** Alfanuméricos (sin tilde ni eñe). No usar solo mayúsculas.

  - **Otros caracteres permitidos:** "_" o "-". No usar espacios.

  - **Nombre:** Separar componentes con mayúsculas, "_" o "-". Usar nombres temáticos.

  - **Longitud de nombres:** Máximo 30 caracteres.

  - **Formato de fecha:** Usar aaaammdd al inicio para archivos periódicos o versionados.

  - **Evitar artículos:** (el, las, los, de).

El cumplimiento de estas consideraciones permite realizar los respaldos de manera efectiva. El incumplimiento puede generar errores en las copias de respaldo, por lo cual la Dirección de Tecnologías de la Información y las Comunicaciones no se hará responsable de la copia y su recuperación.

6.10.POLÍTICAS PARA MESA DE AYUDA

Principio General:

Estos lineamientos definen el uso de la Herramienta de Mesa de Ayuda GLPI para la gestión de solicitudes de soporte en la SDP, asegurando un registro adecuado, la asignación de responsabilidades y la aplicación de las políticas y procedimientos correspondientes. Se busca asegurar que la información importante para la SDP reciba un nivel apropiado de protección, tal como se establece en la guía para la gestión de activos en el marco de seguridad de la información en la SDP (GTI-GA-001).

Lineamientos Específicos:

1. Registro de Solicitudes:

- **Lineamiento (Numeral 5.37 - Procedimientos operativos documentados):** Toda solicitud de soporte que no implique Desarrollo de Software debe ser registrada en la Herramienta de Mesa de Ayuda GLPI directamente por el usuario que la requiera. Este registro documentado permite el seguimiento, la trazabilidad y la gestión eficiente de las solicitudes.

2. Delegación de Solicitudes (Numerales 5.10 - Responsabilidades, y 8.2 - Derechos de acceso privilegiado):

- **Lineamiento:** La única solicitud de servicio que se puede delegar es la referente a la gestión de usuarios (GTI-PD-004), cuyo objeto es "Desarrollar las actividades necesarias para la gestión (creación, actualización o eliminación) de cuentas de usuario y sus contraseñas sobre los diferentes recursos informáticos (red, correo electrónico, bases de datos, sistemas de información/aplicaciones y recursos compartidos de la entidad)". Esta delegación debe realizarse siguiendo los procedimientos establecidos y respetando los principios de mínimo privilegio.

3. Solicitudes Relacionadas con el Uso de Software (Numerales 8.3 - Restricción de acceso a la información, y otros aplicables según el software):

- **Lineamiento:** Para el uso del software en la SDP, se deben seguir los lineamientos establecidos en la Política de uso del software. Para toda incidencia que tenga que ver con ello, es directamente el jefe del área quien debe realizar la solicitud a la mesa de ayuda. Esto asegura la coherencia con las políticas de software y la autorización adecuada para las solicitudes relacionadas.

4. Solicitudes Relacionadas con Copias de Respaldo y Recuperación de Información (Numeral 8.13 - Copia de seguridad de la información):

- **Lineamiento:** Las incidencias de copias de respaldo y recuperación de información seguirán los lineamientos establecidos en el procedimiento GTI-PD-003 Copias de Seguridad y Recuperación de la Información y la Política para la Gestión de Copias de Respaldo y Recuperación de la Información Institucional. Esto asegura la aplicación consistente de las políticas y procedimientos específicos para la gestión de respaldos.

5. Responsabilidad de los Procesos Institucionales (Numeral 5.10 - Responsabilidades):

- **Lineamiento:** Cada uno de los responsables de los procesos institucionales debe asegurar que la información importante para la SDP relacionada con su proceso y sus medios de procesamiento (activos) reciban un nivel apropiado de protección. La aplicación de estos niveles de protección o controles puede ser delegada, pero el responsable del proceso sigue siendo responsable de la protección adecuada de la información de su proceso durante todo el ciclo de vida de la información, según la guía para la gestión de activos en el marco de seguridad de la información en la SDP (GTI-GA-001). Este lineamiento refuerza la responsabilidad de la gestión de la información en todos los niveles de la organización.

Relación con otros numerales de la ISO 27001:2022:

Además de los numerales mencionados explícitamente, los lineamientos para la Mesa de Ayuda se relacionan implícitamente con otros numerales de la ISO 27001:2022, dependiendo del tipo de solicitud. Por ejemplo:

- **Gestión de incidentes de seguridad de la información (Numerales 5.24, 5.25 y 5.26):** Las solicitudes relacionadas con incidentes de seguridad deben gestionarse a través de la Mesa de Ayuda, siguiendo los procedimientos de gestión de incidentes.

- **Gestión de la configuración (Numeral 8.9):** Las solicitudes relacionadas con cambios en la configuración de sistemas y aplicaciones deben gestionarse a través de la Mesa de Ayuda, siguiendo los procedimientos de gestión de cambios.

- **Instalación de software en sistemas operativos (Numeral 8.19):** Las solicitudes de instalación de software deben gestionarse a través de la Mesa de Ayuda, siguiendo los procedimientos de instalación de software.

- **Seguridad en redes (Numeral 8.20):** Las solicitudes relacionadas con problemas de red deben gestionarse a través de la Mesa de Ayuda.

6.11.POLÍTICAS DE SEGURIDAD DE LAS COMUNICACIONES

Principio General:

Estas políticas establecen los lineamientos para asegurar la protección de las comunicaciones de la SDP, tanto internas como externas, garantizando la confidencialidad, integridad y disponibilidad de la información transmitida. Se busca controlar el acceso lógico a las redes y definir procedimientos para la transferencia segura de información.

Lineamientos Específicos:

1. Controles de Acceso Lógico y Protección de Redes (Numeral 8.1 - Control de acceso, 8.20 - Seguridad en redes, 8.21 - Seguridad de los servicios de red, 8.22 - Segregación de redes y 8.23 - Filtrado web):

- **Lineamiento:** El Grupo de Tecnológica de la Información y las Comunicaciones establecerá los controles para el acceso lógico y la protección de las redes de la SDP. Estos controles deben asegurar el cumplimiento de los acuerdos de niveles de servicio (ANS) que se establezcan para los servicios de red y que deberán ser acordados con la alta dirección. Esto implica:

    - **Control de acceso (8.1):** Implementar mecanismos de autenticación y autorización robustos para controlar el acceso

a la red y a los sistemas.

- **Seguridad en redes (8.20):** Asegurar, administrar y controlar las redes y los dispositivos de red para proteger la información en los sistemas y aplicaciones. Esto incluye la configuración segura de firewalls, routers, switches y otros dispositivos de red.

- **Seguridad de los servicios de red (8.21):** Identificar, implementar y controlar los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red, como DNS, DHCP, VPN, etc.

- **Segregación de redes (8.22):** Segregar los grupos de servicios de información, usuarios y sistemas de información en las redes de la organización para limitar el impacto de posibles incidentes de seguridad.

- **Filtrado web (8.23):** Gestionar el acceso a sitios web externos para reducir la exposición a contenido malicioso.

2. Procedimientos y Lineamientos para la Transferencia Segura de Información (Numerales 8.1 - Control de acceso, 8.12 - Prevención de fuga de datos, 8.20 - Seguridad en redes, y otros aplicables según el tipo de transferencia):

- **Lineamiento:** La SDP definirá procedimientos y lineamientos para la transferencia segura de información interna o externamente, garantizando la integridad y confidencialidad de la información. Esto incluye:

  - **Control de acceso (8.1):** Controlar el acceso a la información durante la transferencia, asegurando que solo las personas autorizadas puedan acceder a ella.

  - **Prevención de fuga de datos (8.12):** Implementar medidas para prevenir la fuga de datos durante la transferencia, como el cifrado de la información y el control de los canales de comunicación.

  - **Seguridad en redes (8.20):** Utilizar protocolos seguros para la transmisión de información a través de la red, como HTTPS, SFTP o VPN.

  - **Cifrado (8.24):** Utilizar técnicas de cifrado para proteger la confidencialidad de la información durante la transmisión y el almacenamiento.

  - **Acuerdos de confidencialidad:** Establecer acuerdos de confidencialidad con terceros que tengan acceso a información sensible durante la transferencia.

  - **Procedimientos para la transferencia de información sensible:** Definir procedimientos específicos para la transferencia de información sensible, como información personal, financiera o estratégica.

  - **Clasificación de la información (5.21):** Clasificar la información según su nivel de sensibilidad para aplicar los controles de seguridad adecuados durante la transferencia.

Detalle de los Lineamientos:

- **Acuerdos de Niveles de Servicio (ANS):** Los ANS deben definir los parámetros de calidad del servicio de red, incluyendo la disponibilidad, el rendimiento, la seguridad y el soporte. Deben ser acordados con la alta dirección para asegurar el compromiso y la asignación de recursos necesarios.

- **Transferencia Segura de Información:** Los procedimientos y lineamientos para la transferencia segura de información deben considerar diferentes escenarios, como la transferencia de archivos, el correo electrónico, las comunicaciones en línea y el acceso remoto. Deben especificar los controles de seguridad que se deben aplicar en cada caso, como el cifrado, la autenticación, la autorización y el registro de auditoría.

6.12.POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Principio General:

Esta política define los parámetros y controles de seguridad en los procesos de implementación, mantenimiento, adquisición y uso de aplicaciones/sistemas de información en la SDP, tanto a nivel interno como externo. Su objetivo es garantizar la integridad, confidencialidad y disponibilidad de la información y servicios críticos. La Dirección de Tecnologías de la Información y las

Comunicaciones es responsable de planificar, desarrollar y ejecutar las actividades relacionadas con el desarrollo, actualizaciones, mantenimiento e instalaciones de aplicaciones, software y sistemas de información, así como de la ejecución de las pruebas no funcionales y de seguridad previas a la puesta en producción.

Lineamientos Específicos:

1. Lineamientos Generales:

- **Seguridad en la Implementación:** Se establecerán y aplicarán reglas para el desarrollo seguro de software y sistemas, abarcando todas las fases del ciclo de vida(8.25 - Ciclo de vida de desarrollo seguro). Todos los procesos de la entidad deberán informar a la Dirección de Tecnologías de la información y las comunicaciones sobre sus proyectos de desarrollo o adquisición de sistemas de información, con el fin de brindar las observaciones correspondientes y revisar los aspectos técnicos necesario para su desarrollo e implementación. Los requisitos de seguridad de la información se identificarán, especificarán y aprobarán al desarrollar o adquirir aplicaciones, incluyendo aspectos como confidencialidad, integridad, disponibilidad, autenticación, autorización, gestión de vulnerabilidades, pruebas de seguridad, gestión de logs y cumplimiento normativo. (8.26 - Requisitos de seguridad de la aplicación). Se establecerán y aplicarán reglas para el desarrollo seguro de software y sistemas. Los cambios a los sistemas se controlarán mediante procedimientos formales de control de cambios (8.32 - Gestión del cambio). Se revisarán y probarán las aplicaciones críticas del negocio al cambiar las plataformas de operación para asegurar que no haya impacto adverso en las operaciones o la seguridad. Se limitarán las modificaciones a los paquetes de software y se controlarán estrictamente todos los cambios (8.32 - Gestión del cambio). Se establecerán, documentarán y mantendrán principios para la construcción de sistemas seguros (8.27 - Principios de arquitectura e ingeniería de sistemas seguros). Se establecerán y protegerán adecuadamente los ambientes de desarrollo seguros (8.31 - Separación de los entornos de desarrollo, prueba y producción). Se supervisará y hará seguimiento de la actividad de desarrollo de sistemas contratados externamente (8.30 - Desarrollo subcontratado). Se establecerán programas de prueba para aceptación y criterios de aceptación para nuevas aplicaciones, software y sistemas de información, actualizaciones y nuevas versiones (8.29 - Pruebas de seguridad en desarrollo y aceptación). Se establecerá y documentará el cumplimiento con las leyes y regulaciones de seguridad de la información. Se proporcionará formación y concienciación en seguridad a los desarrolladores y personal involucrado en el proceso de desarrollo. Se establecerán políticas de control de acceso a sistemas y aplicaciones. Se implementará una gestión de identidades y accesos sólida. Se cumplirá con la regulación de protección de datos personales. Se establecerán procedimientos para detectar, informar y responder a incidentes de seguridad. Se revisará y mejorará regularmente la política de desarrollo seguro.

2. Acceso al Código Fuente (8.4):

- **Lineamiento:** El acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las bibliotecas de software se gestionará adecuadamente, implementando controles de acceso basados en roles y el principio de mínimo privilegio. Se utilizarán repositorios de código seguros y se auditará el acceso al código.

3. Eliminación de Información (8.10):

- **Lineamiento:** La información almacenada en los sistemas de información, dispositivos o en cualquier otro medio de almacenamiento se eliminará cuando ya no sea necesaria, siguiendo procedimientos seguros de borrado o destrucción, según la clasificación de la información. Se documentarán los procedimientos de eliminación y se capacitará al personal.

4. Enmascaramiento de Datos (8.11):

- **Lineamiento:** El enmascaramiento de datos se debe utilizar de acuerdo con la política específica del tema de la organización sobre el control de acceso y otras políticas relacionadas, y los requisitos comerciales, teniendo en cuenta la legislación aplicable, especialmente para datos sensibles o personales. Se definirán los métodos de enmascaramiento a utilizar según el tipo de dato y el contexto.

5. Principios de Codificación Segura (8.28 - Codificación segura):

Lineamiento: Se aplicarán principios de codificación segura, como: Validación de entradas, gestión de errores, autenticación y autorización, gestión de sesiones, cifrado, gestión de contraseñas, control de acceso y pruebas de seguridad.

6. Pruebas de Seguridad en Desarrollo y Aceptación (8.29):

Lineamiento: Los procesos de pruebas de seguridad se definirán e implementarán en el ciclo de vida del desarrollo, incluyendo pruebas de penetración, análisis de vulnerabilidades, pruebas de seguridad de aplicaciones web y pruebas de seguridad de redes.

Se documentarán los resultados de las pruebas y se gestionarán las vulnerabilidades encontradas.

7. Desarrollo Subcontratado (8.30):

- **Lineamiento:** La entidad debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas subcontratados, incluyendo la definición de requisitos de seguridad en los contratos, la revisión del código fuente, las pruebas de seguridad y la gestión de la configuración. Se establecerán acuerdos de confidencialidad y se auditará el cumplimiento de los requisitos de seguridad.

8. Separación de los Entornos de Desarrollo, Prueba y Producción (8.31):

- **Lineamiento:** Los entornos de desarrollo, prueba y producción deben estar separados y protegidos (8.31 - Separación de los entornos de desarrollo, prueba y producción), implementando controles de acceso y segregación de redes. Se evitará la utilización de datos de producción en los entornos de desarrollo y prueba.

9. Información de Prueba (8.33):

- **Lineamiento:** La información de las pruebas se seleccionará, protegerá y gestionará adecuadamente, utilizando datos anonimizados o sintéticos siempre que sea posible. Se evitará el uso de datos reales de producción en los entornos de prueba, a menos que sea estrictamente necesario y se cuente con las autorizaciones correspondientes.

10. Protección de los Sistemas de Información durante las Pruebas de Auditoría (8.34):

- **Lineamiento:** Las pruebas de auditoría y otras actividades de aseguramiento que involucren la evaluación de los sistemas operativos deben planificarse y acordarse entre el evaluador y la dependencia (o gerente del proyecto) correspondiente, minimizando el impacto en la operación de los sistemas y protegiendo la confidencialidad de la información.

11. Requisitos de Seguridad en el Ciclo de Desarrollo de Software (8.26 - Requisitos de seguridad de la aplicación):

- **Lineamiento:** Se establecerán requisitos de seguridad de la información, como: Confidencialidad (cifrado, control de acceso, protección contra divulgación no autorizada), Integridad (protección contra modificaciones no autorizadas, mecanismos de detección y corrección de errores, control de versiones y gestión de cambios), Disponibilidad (planes de continuidad del negocio y recuperación ante desastres, redundancia, protección contra ataques de denegación de servicio), Autenticación y autorización (mecanismos de autenticación fuertes, control de acceso basado en roles, gestión de identidades y accesos), Gestión de vulnerabilidades (escaneo y análisis, parcheo y actualización, gestión de incidencias), Pruebas de seguridad (pruebas de penetración, pruebas de seguridad de aplicaciones web, pruebas de seguridad de redes), Gestión de logs (recopilación y análisis, alerta temprana) y Cumplimiento normativo.

12. Lineamientos de Seguridad para los Desarrolladores:

- **Lineamiento:** Los mantenimientos, modificaciones o actualizaciones se realizarán en ambientes independientes de desarrollo y pruebas. Se planificarán las etapas de paso a producción, incluyendo respaldos, recursos, pruebas y la aceptación del usuario funcional (8.29). Los datos para las pruebas se generarán. La información de las pruebas se seleccionará, protegerá y gestionará adecuadamente (8.33). Los desarrolladores no tendrán acceso a datos sensibles del ambiente de producción. Los desarrollos por terceros requerirán la suscripción de un acuerdo de confidencialidad.

13. Normas de Seguridad para la Gestión de Vulnerabilidades (8.29 - Pruebas de seguridad en desarrollo y aceptación):

- **Lineamiento:** Se llevarán a cabo pruebas de funcionalidad de la seguridad. Se definirá un proceso de gestión de riesgos para identificar, evaluar y mitigar vulnerabilidades. Se implementarán evaluaciones regulares de seguridad, pruebas de penetración y análisis de vulnerabilidades. Se realizará la gestión de vulnerabilidades técnicas. Se establecerá un plan de actualización del software base.

14. Normas de Seguridad para la Documentación del Software:

- **Lineamiento:** El diccionario de datos mantendrá una descripción actualizada de las definiciones de datos. Los comentarios en el código fuente no divulgarán información de configuración innecesaria. Se generará un protocolo de las condiciones de autenticación. La documentación se generará durante el ciclo de vida, será revisada por los usuarios finales, se actualizará si el programa cambia y se almacenará en el sistema de control de versiones.

15. Normas de Seguridad para Proyectos de Desarrollo de Software:

- **Lineamiento:** En la fase de levantamiento de requerimientos, se describirán los requerimientos de seguridad.

16. Normas de Seguridad para la Especificación Detallada de Requerimientos:

- **Lineamiento:** Los requerimientos incluirán autenticación, roles, privilegios, riesgos y criterios de aprobación. Se considerará el nivel de criticidad del sistema y el nivel de protección de seguridad. Los requerimientos de seguridad serán compatibles con las demás políticas de seguridad de la información de la SDP.

17. Normas de Seguridad para el Diseño de Sistema:

- **Lineamiento:** Se definirá el nivel de confidencialidad de todos los elementos del software. Se emplearán las herramientas de seguridad necesarias en los gestores de bases de datos. Las soluciones de software críticos incluirán la generación de registros de auditoría. Se proyectará el rendimiento esperado.

18. Normas de Seguridad para la Codificación y Pruebas:

- **Lineamiento:** No se modificarán programas sin el registro de un requerimiento. No se escribirá código malicioso. Las pruebas incluirán instalación, volumen, stress, rendimiento, almacenamiento, configuración, funcionalidad, seguridad y recuperación ante errores. Las pruebas unitarias y funcionales se ejecutarán en los ambientes correspondientes y se registrarán sus resultados según el procedimiento GTI-PD-001 - Desarrollo, Instalación y Mantenimiento de Soluciones de Software. Se realizarán validaciones de datos de entrada y salida, manejo de logs y errores, y validación de la información suministrada por los usuarios. Se establecerán controles para la autenticación, la validación de sesiones, el manejo de operaciones sensibles, el manejo de errores, el manejo de archivos, la conexión a bases de datos, la información en los encabezados de respuesta, la transferencia de archivos, los parámetros, la liberación de memoria, la protección del código fuente y la ejecución de comandos en el sistema operativo. Se implementará el control de integridad (hash). En lo posible se deberá asegurar el manejo de operaciones sensibles en los aplicativos desarrollados, permitiendo el uso de dispositivos adicionales como "tokens" o el ingreso de parámetros adicionales de verificación.

19. Normas de Seguridad para la Implementación:

- **Lineamiento:** Se implementarán los controles de seguridad al mismo tiempo que los componentes, funciones o módulos. Todas las aplicaciones contarán con un sistema de autenticación de usuario. Las aplicaciones contarán con manejo de diferentes roles con permisos de acceso y operaciones asociados. Las aplicaciones deberán contar con manejo de doble factor de autenticación.

20. Normas de Seguridad Posterior a la Puesta en Producción:

- **Lineamiento:** Se revisará y auditará la existencia de los controles de seguridad definidos. Se realizará un escaneo anual de las aplicaciones más recientes en busca de vulnerabilidades.

21. Responsabilidades (5.10 - Responsabilidades):

- **Lineamiento:** Las responsabilidades se contemplan en el procedimiento GTI-PD-001 para cada rol (Cliente, Usuario Funcional, Líder Funcional, Líder Técnico, Profesional Grupo de Software, Profesional Grupo de Infraestructura). Los desarrolladores son responsables de la confidencialidad del código fuente, el versionamiento y la custodia segura, la confidencialidad de la información de pruebas y el paso a producción de los requerimientos aprobados.

6.13.POLÍTICA DE USO DE SOFTWARE DE LA SDP

Principio General:

El objetivo general de esta política es establecer los lineamientos mínimos necesarios y aplicables al interior de la entidad en el uso de software, garantizando el cumplimiento de la Norma ISO/IEC 27001 versión 2022 - Categoría A.5, Controles organizacionales, Control 5.32 (Derechos de propiedad intelectual), la Directiva Presidencial 002 de 2002 y la legislación nacional vigente sobre derechos de autor.

Lineamientos Específicos:

1. Directrices Generales para el Uso del Software:

- **Procedimiento de Uso y Administración (Relacionado con 5.37 - Procedimientos operativos documentados):** La Dirección TIC definirá y propenderá por el cumplimiento del procedimiento para el uso y administración del software de la SDP.

- **Cumplimiento de la Legislación (5.32 - Derechos de propiedad intelectual):** Todo software instalado y utilizado en los equipos propiedad de la SDP debe cumplir con los principios constitucionales (Artículo 61), los acuerdos internacionales y la legislación nacional vigente sobre derechos de autor, respetando los derechos o la voluntad expresada por el autor en documentos físicos o digitales de licenciamiento.

- **Condiciones de Licenciamiento (5.32 y 8.18 - Software instalado por el usuario):** Toda instalación de software debe realizarse a partir de fuentes obtenidas legalmente con la autorización de su autor, según el modo y vigencia de licenciamiento, derecho de uso de software o condiciones por transferencia de terceros, en concordancia con los lineamientos de la Dirección TIC. Se prohíbe la instalación de software sin la debida licencia.

- **Administración y Control del Software (8.19 - Instalación de software en sistemas operativos):** La Dirección TIC es la encargada de administrar y controlar el software como activo institucional. Debe mantener un repositorio centralizado y definir un catálogo de software de la Entidad.

- **Muestreo de Software (5.37 - Procedimientos operativos documentados y 9.2 - Auditoría interna):** La Dirección de TIC realizará al menos una vez al año un muestreo del software instalado en los equipos de la SDP para validar el cumplimiento de los lineamientos.

- **Software Legal en Productos Desarrollados (5.32 y 8.28 - Codificación segura):** Todo producto construido para la SDP debe elaborarse con software legal, ya sea propietario, de código abierto, Freeware o de dominio público. Se dará preferencia al uso de software con licencias que permitan la auditoría del código fuente cuando sea necesario.

- **Solicitudes de Instalación (8.19 y 5.10 - Responsabilidades):** Las solicitudes de instalación de software las debe realizar exclusivamente el responsable de la dependencia o área (Directivo), mediante registro en la herramienta de mesa de ayuda, con la respectiva justificación de su uso. Esta responsabilidad no puede ser delegada.

2. Responsabilidades:

- **Dirección TIC (5.10 - Responsabilidades, 8.19 y 5.37):**

  - La instalación de software será realizada exclusivamente por la Dirección TIC, previo registro y justificación del responsable de la dependencia, evaluación y aprobación por parte de la Dirección TIC, siguiendo los procedimientos establecidos.

  - La Dirección TIC será responsable de controlar, evaluar y aprobar la instalación del licenciamiento de software, tanto adquirido por la SDP como de uso libre.

  - La Dirección TIC será responsable de realizar la evaluación técnica y emitir concepto para el uso de software específico (propietario, freeware y software libre), previa solicitud del Directivo del área, siguiendo el procedimiento definido.

- **Usuarios de la SDP (5.10 y 8.18):**

  - Los servidores públicos, contratistas y personal temporal de la SDP pueden utilizar exclusivamente software debidamente licenciado y autorizado por la Dirección TIC, tanto en los equipos de cómputo de la SDP como en los de su propiedad que se utilicen para funciones y actividades inherentes a la SDP.

  - Los desarrolladores de soluciones de software deben usar herramientas debidamente licenciadas y contar con la aprobación de la Dirección TIC, cumpliendo los procedimientos establecidos. El software utilizado por los contratistas debe estar licenciado, presentando la copia de la licencia o evidencia verificable.

  -

- **Grupo Directivo de la SDP (5.10 y 8.19):**

- Los Directivos de la SDP son los únicos autorizados para solicitar la instalación de software en los equipos de la SDP. La solicitud se realiza registrando una incidencia en la mesa de ayuda, con la justificación, número de placa del equipo y usuario que lo utilizará.

- En el desarrollo de productos y servicios de software, los directivos son responsables de asegurar que los productos se hayan elaborado con software legal y aprobado por la Dirección TIC.

Relación con otros numerales de la ISO 27001:2022:

- **5.21 (Clasificación de la información):** La clasificación de la información puede influir en la selección y el uso del software, especialmente en lo que respecta al cifrado y otras medidas de seguridad.
- **8.2 (Derechos de acceso privilegiado):** El acceso a la instalación y configuración del software debe restringirse a personal autorizado de la Dirección TIC.
- **8.3 (Restricción de acceso a la información):** El acceso al software y a los datos que procesa debe restringirse según las políticas de control de acceso.
- **8.13 (Copia de seguridad de la información):** Se deben realizar copias de seguridad del software y de los datos que procesa.
- **8.24 (Cifrado):** Se debe considerar el uso de cifrado para proteger la información almacenada y transmitida por el software.
- **8.28 (Codificación segura):** En el caso de software desarrollado internamente, se deben aplicar principios de codificación segura.
- **9.1 (Seguimiento, medición, análisis y evaluación):** Se debe realizar un seguimiento del uso del software para asegurar el cumplimiento de la política.

6.14.POLÍTICAS DE RELACIONES CON LOS PROVEEDORES

Principio General:

Estas políticas establecen los lineamientos para gestionar los riesgos de seguridad de la información asociados con el uso de productos o servicios de proveedores, incluyendo la cadena de suministro de TIC y los servicios en la nube. Se busca asegurar que los requisitos de seguridad de la información se establezcan, se acuerden y se monitoreen a lo largo de la relación con el proveedor.

Lineamientos Específicos:

1. Seguridad de la Información en las Relaciones con los Proveedores (5.19):

- **Lineamiento:** La SDP establecerá políticas y requisitos de seguridad de la información para mitigar los riesgos asociados a cada proceso de contratación. Se definirán e implementarán procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor. Esto incluye la evaluación de riesgos de seguridad de la información antes de la contratación, la definición de controles de seguridad en los contratos y el monitoreo del cumplimiento de estos controles durante la vigencia del contrato.

2. Abordar la Seguridad de la Información en los Acuerdos con los Proveedores (5.20):

- **Lineamiento:** Antes de iniciar la ejecución de contratos con terceras partes, deberán suscribirse los respectivos acuerdos de confidencialidad que incluyan las cláusulas de confidencialidad y los aspectos de seguridad de la información necesarios durante y después del contrato. Los requisitos de seguridad de la información pertinentes se establecerán y acordarán con cada proveedor en función del tipo de relación y los riesgos identificados. Estos requisitos se documentarán en los contratos y acuerdos de nivel de servicio (ANS).

3. Gestión de la Seguridad de la Información en la Cadena de Suministro de TIC (5.21):

- **Lineamiento:** Se definirán e implementarán procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de TIC. Esto incluye la evaluación de los riesgos de seguridad de los proveedores de TIC, la definición de controles de seguridad en los contratos con los proveedores de TIC y el monitoreo del cumplimiento de estos controles. Se considerarán aspectos como la seguridad del desarrollo, la gestión de vulnerabilidades y la gestión de incidentes.

4. Seguimiento, Revisión y Gestión de Cambios de Servicios de Proveedores (5.22):

- **Lineamiento:** La SDP debe monitorear, revisar, evaluar y gestionar periódicamente los cambios en las prácticas de seguridad de la información del proveedor y la prestación de servicios. Se establecerán mecanismos de seguimiento y comunicación con los proveedores para asegurar que se mantengan los niveles de seguridad acordados. Se gestionarán los cambios en los servicios del proveedor para minimizar el impacto en la seguridad de la información de la SDP.

5. Seguridad de la Información para el Uso de Servicios en la Nube (5.23):

- **Lineamiento:** Los procesos de adquisición, uso, gestión y salida de los servicios en la nube se deben establecer de acuerdo con los requisitos de seguridad de la información de la SDP. Se evaluarán los riesgos de seguridad asociados con el uso de servicios en la nube y se definirán los controles de seguridad necesarios, incluyendo aspectos como la seguridad de los datos, el control de acceso, la gestión de identidades y la gestión de incidentes. Se considerarán las responsabilidades compartidas entre la SDP y el proveedor de servicios en la nube.

6.Requisitos Legales, Estatutarios, Reglamentarios y Contractuales (5.31):

- **Lineamiento:** Los requisitos legales, estatutarios, reglamentarios y contractuales relevantes para la seguridad de la información y el enfoque de la SDP para cumplir con estos requisitos deben identificarse, documentarse y mantenerse actualizados. Estos requisitos se considerarán en la gestión de las relaciones con los proveedores, incluyendo la definición de los requisitos de seguridad en los contratos y el monitoreo del cumplimiento de estos requisitos.

Detalle de los Lineamientos:

- **Evaluación de Riesgos:** Se realizará una evaluación de riesgos de seguridad de la información antes de contratar cualquier proveedor que tenga acceso a información de la SDP. Esta evaluación considerará factores como el tipo de información a la que tendrá acceso el proveedor, los servicios que proporcionará y la ubicación del proveedor.

- **Acuerdos de Confidencialidad:** Los acuerdos de confidencialidad deben incluir cláusulas que especifiquen las responsabilidades del proveedor en materia de seguridad de la información, incluyendo la protección de la confidencialidad, la integridad y la disponibilidad de la información.

- **Controles de Seguridad en los Contratos:** Los contratos con los proveedores deben incluir controles de seguridad específicos, como la exigencia de certificaciones de seguridad (ej. ISO 27001), la definición de niveles de servicio de seguridad (SLAs), la obligación de notificar incidentes de seguridad y el derecho de la SDP a realizar auditorías de seguridad.

- **Monitoreo del Cumplimiento:** Se establecerán mecanismos para monitorear el cumplimiento de los requisitos de seguridad por parte de los proveedores, incluyendo revisiones periódicas, auditorías y pruebas de seguridad.

- **Gestión de Incidentes:** Se definirán procedimientos para la gestión de incidentes de seguridad que involucren a proveedores, incluyendo la notificación, la investigación y la resolución de incidentes.

6.15.POLÍTICAS DE SEGURIDAD DE LAINFORMACIÓN EN LACONTINUIDAD DE NEGOCIO

Principio General:

Estas políticas establecen los lineamientos para asegurar la continuidad de las operaciones de la SDP ante interrupciones, con un enfoque específico en la preservación de la seguridad de la información. Se busca planificar cómo mantener la seguridad de la información durante una interrupción y asegurar la preparación de las TIC para la continuidad del negocio.

Lineamientos Específicos:

1. Seguridad de la Información durante la Interrupción (5.29):

- **Lineamiento:** La SDP establecerá un plan de continuidad tecnológica que incluya la continuidad de la seguridad de la

información y la restauración oportuna de los servicios en un escenario de contingencia. Este plan debe definir los controles de seguridad que se implementarán durante una interrupción para mantener un nivel adecuado de protección de la información. Esto implica:

- **Identificación de activos críticos:** Identificar los activos de información críticos para la operación de la SDP que deben protegerse durante una interrupción.

- **Definición de controles alternativos:** Definir controles de seguridad alternativos que se puedan implementar durante una interrupción en caso de que los controles normales no estén disponibles.

- **Procedimientos de seguridad durante la interrupción:** Documentar procedimientos claros para el personal sobre cómo mantener la seguridad de la información durante una interrupción, incluyendo el manejo de accesos, la protección de la información sensible y la gestión de incidentes de seguridad.

- **Comunicación:** Establecer protocolos de comunicación para informar al personal y a las partes interesadas sobre el estado de la seguridad de la información durante una interrupción.

2. Preparación de las TIC para la Continuidad del Negocio (5.30):

- **Lineamiento:** La Dirección de Tecnologías de la Información y las Comunicaciones generará dicho plan de continuidad tecnológica con base en Planes de Recuperación de Desastres (DRP) y Análisis de Impacto al Negocio (BIA). La preparación de las TIC debe planificarse, implementarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC. Esto implica:

  - **Análisis de Impacto al Negocio (BIA):** Realizar un BIA para identificar los procesos críticos de la SDP y el impacto que tendría una interrupción en estos procesos. El BIA debe considerar los requisitos de seguridad de la información.

  - **Plan de Recuperación de Desastres (DRP):** Desarrollar un DRP que defina los procedimientos para la recuperación de los sistemas y servicios de TIC en caso de un desastre. El DRP debe incluir la recuperación de los controles de seguridad y la restauración de la información.

  - **Pruebas del DRP:** Probar periódicamente el DRP para asegurar su efectividad y realizar ajustes según sea necesario. Las pruebas deben incluir la verificación de la restauración de la seguridad de la información.

  - **Mantenimiento del DRP:** Mantener actualizado el DRP para reflejar los cambios en los sistemas, los procesos y los requisitos de seguridad de la información.

  - **Infraestructura redundante:** Implementar infraestructura redundante para asegurar la disponibilidad de los sistemas y servicios críticos durante una interrupción.

  - **Copias de seguridad:** Realizar copias de seguridad regulares de la información y probar su restauración.

  - **Sitio alterno de trabajo:** Establecer un sitio alterno de trabajo para el personal en caso de que las instalaciones principales no estén disponibles.

Detalle de los Lineamientos:

- **Plan de Continuidad Tecnológica:** Este plan debe ser un documento integral que abarque todos los aspectos de la continuidad del negocio relacionados con la tecnología, incluyendo la seguridad de la información. Debe definir los roles y responsabilidades del personal, los procedimientos de recuperación, los recursos necesarios y los criterios de éxito.

- **Análisis de Impacto al Negocio (BIA):** El BIA debe identificar el tiempo máximo tolerable de inactividad (RTO) y el punto objetivo de recuperación (RPO) para cada proceso crítico. Estos parámetros se utilizarán para definir los requisitos de recuperación de las TIC y la seguridad de la información.

- **Planes de Recuperación de Desastres (DRP):** Los DRP deben ser específicos para cada sistema o servicio crítico y deben incluir instrucciones detalladas para la recuperación, incluyendo la restauración de la configuración de seguridad, la recuperación de las contraseñas y la verificación de la integridad de la información.

- **Seguridad de la información durante la recuperación:** Se debe asegurar que los procesos de recuperación no comprometan la seguridad de la información. Se deben implementar controles para prevenir el acceso no autorizado a la

información durante la recuperación y para asegurar la integridad de la información restaurada.

- **Capacitación y Concienciación:** Se debe capacitar al personal sobre los procedimientos de continuidad del negocio y la seguridad de la información durante las interrupciones. Se deben realizar simulacros periódicos para probar la efectividad de los planes.

6.16.POLÍTICAS DE GESTIÓN DE INCIDENTES

Principio General:

Estas políticas establecen los lineamientos para la gestión de incidentes de seguridad de la información en la SDP, desde la planificación y preparación hasta el aprendizaje posterior a los incidentes. Se busca asegurar una respuesta efectiva y la mejora continua de los controles de seguridad.

Lineamientos Específicos:

1. Planificación y Preparación de la Gestión de Incidentes de Seguridad de la Información (5.24):

- **Lineamiento:** La SDP debe planificar y prepararse para la gestión de incidentes de seguridad de la información definiendo, estableciendo y comunicando procesos, roles y responsabilidades de gestión de incidentes. Esto implica:

  - **Definición de un Plan de Gestión de Incidentes:** Documentar un plan que describa los procedimientos a seguir ante diferentes tipos de incidentes, incluyendo la identificación, clasificación, contención, erradicación, recuperación y actividades posteriores al incidente.

  - **Establecimiento de un Equipo de Respuesta a Incidentes de Seguridad de la Información (CSIRT):** Designar un equipo con roles y responsabilidades claras para la gestión de incidentes.

  - **Comunicación:** Establecer canales de comunicación internos y externos para la notificación y gestión de incidentes.

  - **Capacitación y Concienciación:** Capacitar al personal en la identificación y reporte de incidentes, así como en los procedimientos de respuesta.

2. Evaluación y Decisión sobre Eventos de Seguridad de la Información (5.25):

- **Lineamiento:** La SDP debe evaluar los eventos de seguridad de la información y decidir si se clasificarán como incidentes de seguridad de la información. Esto implica:

  - **Definición de criterios de clasificación:** Establecer criterios claros para determinar si un evento se considera un incidente, basándose en su impacto potencial en la confidencialidad, integridad y disponibilidad de la información.

  - **Proceso de evaluación:** Definir un proceso para la evaluación de eventos, incluyendo la recopilación de información, el análisis y la toma de decisiones sobre la clasificación.

3. Respuesta a Incidentes de Seguridad de la Información (5.26):

- **Lineamiento:** Se debe responder a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados en el Plan de Gestión de Incidentes. Esto implica:

  - **Contención:** Implementar medidas para detener la propagación del incidente y minimizar su impacto.

  - **Erradicación:** Eliminar la causa raíz del incidente.

  - **Recuperación:** Restaurar los sistemas y servicios afectados a su estado normal de operación.

  - **Comunicación:** Mantener informadas a las partes interesadas durante todo el proceso de respuesta.

4. Aprender de los Incidentes de Seguridad de la Información (5.27):

- **Lineamiento:** El conocimiento obtenido de los incidentes de seguridad de la información se utilizará para fortalecer y mejorar los controles de seguridad de la información. Esto implica:

    - **Análisis post-incidente:** Realizar un análisis posterior a cada incidente para identificar las causas raíz, las lecciones aprendidas y las áreas de mejora.

    - **Implementación de mejoras:** Implementar las mejoras identificadas en los controles de seguridad, los procesos y la capacitación.

5. Recolección de Evidencia (5.28):

- **Lineamiento:** La organización debe establecer e implementar procedimientos para la identificación, recolección, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información. Esto implica:

    - **Definición de procedimientos de recolección de evidencia:** Documentar procedimientos para la recolección y preservación de evidencia digital, asegurando la cadena de custodia y la admisibilidad legal.

    - **Herramientas forenses:** Utilizar herramientas forenses adecuadas para la recolección y análisis de evidencia.

    - **Capacitación en forense digital:** Capacitar al personal en la recolección y preservación de evidencia digital.

- **Reporte de Incidentes:** Cada vez que se detecta un evento, incidente o debilidad relacionados con la seguridad de la información por parte de un funcionario, contratista o terceras partes, se deberá reportar a la Dirección de Tecnologías de la Información y las Comunicaciones a través de la mesa de ayuda de la Dirección TIC. Este reporte debe incluir la mayor cantidad de detalles posible sobre el evento.

- **Responsabilidad de la Dirección TIC:** Será responsabilidad de la Dirección de Tecnologías y las Comunicaciones seguir los procedimientos establecidos para la gestión de los incidentes que puedan presentarse, incluyendo la coordinación del CSIRT, la comunicación con las partes interesadas y la implementación de las acciones de respuesta.

Relación con otros numerales de la ISO 27001:2022:

- **5.10 (Responsabilidades):** Se deben definir las responsabilidades del personal en la gestión de incidentes.
- **5.21 (Clasificación de la información):** La clasificación de la información influye en la prioridad y el impacto de los incidentes.
- **8.3 (Restricción de acceso a la información):** Los controles de acceso ayudan a prevenir y contener incidentes.
- **8.13 (Copia de seguridad de la información):** Las copias de seguridad son esenciales para la recuperación ante incidentes.
- **9.2 (Auditoría interna):** Las auditorías internas pueden identificar debilidades que podrían dar lugar a incidentes.
- **10.1 (Mejora continua):** La gestión de incidentes es un proceso de mejora continua.

6.17.POLÍTICAS DE CUMPLIMIENTO

Principio General:

Estas políticas establecen los lineamientos para asegurar el cumplimiento de los requisitos legales, reglamentarios, contractuales y de propiedad intelectual relacionados con la seguridad de la información en la SDP. Se busca garantizar la protección de la información, la privacidad de los datos personales y la adecuada gestión de los derechos de propiedad intelectual, así como la revisión independiente y el cumplimiento de las políticas internas.

Lineamientos Específicos:

1. Derechos de Propiedad Intelectual (5.32):

- **Lineamiento:** La SDP debe implementar procedimientos apropiados para proteger los derechos de propiedad intelectual,

incluyendo:

- **Inventario de activos de propiedad intelectual:** Mantener un inventario actualizado de los activos de propiedad intelectual de la SDP, incluyendo software, documentación, marcas, patentes, etc.
- **Políticas de uso de software y licencias:** Establecer políticas claras sobre el uso de software y la gestión de licencias, asegurando el cumplimiento de los términos de las licencias y evitando el uso de software no autorizado.
- **Acuerdos de confidencialidad:** Implementar acuerdos de confidencialidad con empleados, contratistas y terceros que tengan acceso a información confidencial o protegida por derechos de propiedad intelectual.
- **Procedimientos para la gestión de derechos de autor y patentes:** Establecer procedimientos para la gestión de derechos de autor y patentes, incluyendo la presentación de solicitudes, el seguimiento y la protección de los derechos.

2. Privacidad y Protección de la Información de Identificación Personal (PII) (5.34):

- **Lineamiento:** La SDP deberá identificar y cumplir los requisitos relacionados con la preservación de la privacidad y la protección de la PII de acuerdo con las leyes y reglamentos aplicables y los requisitos contractuales. Esto implica:
  - **Identificación de PII:** Identificar los tipos de PII que maneja la SDP.
  - **Evaluación de impacto en la privacidad (EIP):** Realizar EIPs para los procesos que involucran el tratamiento de PII.
  - **Implementación de controles de privacidad:** Implementar controles técnicos y organizativos para proteger la PII, incluyendo el cifrado, el control de acceso, la minimización de datos y la seudonimización.
  - **Aviso de privacidad:** Proporcionar avisos de privacidad claros y concisos a los titulares de los datos.
  - **Gestión de solicitudes de los titulares de los datos:** Establecer procedimientos para atender las solicitudes de los titulares de los datos, como el acceso, la rectificación, la cancelación y la oposición.

3. Revisión Independiente de la Seguridad de la Información (5.35):

- **Lineamiento:** El enfoque de la organización para gestionar la seguridad de la información y su implementación, incluidas las personas, los procesos y las tecnologías, se revisará de forma independiente a intervalos planificados o cuando se produzcan cambios significativos. Esto implica:
  - **Planificación de las revisiones independientes:** Definir la frecuencia y el alcance de las revisiones independientes.
  - **Selección de revisores independientes:** Seleccionar revisores independientes con la competencia y la objetividad necesarias.
  - **Ejecución de las revisiones:** Realizar las revisiones de acuerdo con un plan establecido y documentar los resultados.
  - **Seguimiento de las acciones correctivas:** Realizar un seguimiento de la implementación de las acciones correctivas identificadas en las revisiones.

4. Cumplimiento de Políticas, Normas y Estándares de Seguridad de la Información (5.36):

- **Lineamiento:** El cumplimiento de la política de seguridad de la información de la organización, las políticas, las reglas y los estándares específicos de cada tema se revisará periódicamente. Esto implica:
  - **Definición de indicadores de cumplimiento:** Definir indicadores para medir el cumplimiento de las políticas, normas y estándares.
  - **Monitoreo del cumplimiento:** Monitorear periódicamente el cumplimiento de los indicadores.
  - **Acciones correctivas:** Implementar acciones correctivas cuando se identifiquen desviaciones.
  - **Informes de cumplimiento:** Generar informes periódicos sobre el estado del cumplimiento.

Lineamiento Adicional (integrando la información proporcionada):

- **Cumplimiento Legal y Normativo:** La Secretaría Distrital de Planeación velará por el cumplimiento de la legislación vigente respecto a los requisitos establecidos en la seguridad y privacidad de la información, derechos de propiedad intelectual, protección de datos personales, transparencia y del derecho de acceso a la información pública. Esto implica:

  - **Identificación de requisitos legales y normativos:** Mantener un registro actualizado de los requisitos legales y normativos aplicables a la SDP en materia de seguridad de la información.

  - **Implementación de controles para el cumplimiento:** Implementar controles para asegurar el cumplimiento de los requisitos legales y normativos.

  - **Seguimiento del cumplimiento legal y normativo:** Monitorear el cumplimiento de los requisitos legales y normativos y realizar ajustes según sea necesario.

Relación con otros numerales de la ISO 27001:2022:

- **4.2 (Comprensión de las necesidades y expectativas de las partes interesadas):** Se deben considerar las necesidades y expectativas de las partes interesadas en materia de cumplimiento.
- **5.1 (Liderazgo y compromiso):** La alta dirección debe demostrar su liderazgo y compromiso con el cumplimiento.
- **6.1.3 (Tratamiento de los riesgos para la seguridad de la información):** Se deben considerar los riesgos de incumplimiento.
- **9.3 (Revisión por la dirección):** La revisión por la dirección debe incluir una revisión del estado del cumplimiento.

6.18.POLÍTICAS DE PROTECCIÓN DE DATOS PERSONALES

Esta política establece los lineamientos para la recolección, almacenamiento, uso y tratamiento de datos personales de acuerdo con la ley colombiana y da a conocer las políticas de protección de datos personales establecidas en la SDP, para preservar los derechos del titular de la información cuando suministra los datos a través de los diferentes canales habilitados para la respectiva captura.

Mediante esta política se aplica lo establecido en la Norma ISO/IEC 27001 versión 2022 - Categoría A.5, Controles organizacionales, Control 5.34 Privacidad y protección de la información de identificación personal (PII), control: La organización deberá identificar y cumplir los requisitos relacionados con la preservación de la privacidad y la protección de la información de identificación personal PII de acuerdo con las leyes y reglamentos aplicables y los requisitos contractuales.

¿PARA QUÉ UNA POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES?

Para preservar el derecho ciudadano a la adecuada protección de su información personal, suministrada a través de los diferentes instrumentos disponibles por la Secretaría Distrital de Planeación, entre ellos:

- Caracterización de ciudadanos y/o grupos de interés.
- Tratamiento y respuesta a las peticiones, quejas, reclamos, sugerencias y denuncias (PQRSD).
- Información registrada en el Sistema de Información y Gestión de Empleo Público (SIGEP).
- Información registrada en el Sistema de Información Distrital del Empleo y la Administración Pública (SIDEAP) del Departamento Administrativo del Servicio Civil Distrital.
- Consulta de datos en las bases de entidades públicas o privadas.
- Capacitaciones o encuestas de satisfacción y/o percepción.
- Envío de información de interés general.
- Comunicaciones a través de los diferentes canales (presencial, virtual o telefónico) para la realización de trámites o servicios.

¿QUIÉN LIDERA EL PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES EN LA SDP?

EL OFICIAL DE PROTECCIÓN DE DATOS PERSONALES, de acuerdo con el Artículo 12 del Acuerdo Distrital 822 del 2021, este Oficial estará a cargo de estructurar, diseñar y administrar las capacidades que les permita a todas las entidades cumplir las normas sobre protección de datos personales, así como mitigar las vulnerabilidades asociadas a los mismos en cumplimiento de los lineamientos establecidos por la Superintendencia de Industria y Comercio - SIC para tales fines.

¿CUÁL ES EL ALCANCE DE ESTA POLÍTICA?

Esta política aplica para todas las bases de datos o archivos manuales o automatizados de la Secretaría Distrital de Planeación, cuyo contenido corresponda a datos personales de los ciudadanos. En este sentido, el responsable del tratamiento de esta información será la Secretaría Distrital de Planeación, por lo que hará uso de ella únicamente para las finalidades que se presentarán en el desarrollo de la pregunta ¿CÓMO ES EL TRATAMIENTO DE LOS DATOS Y CUÁL ES SU FINALIDAD? de la presente política.

¿CUÁLES SON LOS PRINCIPIOS DE ESTA POLÍTICA?

Principio de legalidad: El tratamiento de datos personales se realizará con base en lo dispuesto por la ley y velará por el efectivo ejercicio de los derechos fundamentales con base en lo dispuesto en la Constitución Política de Colombia y la normatividad vigente, con el fin de velar por el efectivo ejercicio de los derechos fundamentales.

Principio de finalidad: El tratamiento de datos personales cumple una finalidad legítima enmarcada en la ley, la cual será informada al titular; quien, a su vez, podrá conocer el uso que se le ha dado a sus datos, previa solicitud.

Principio de veracidad o calidad: La información sujeta a tratamiento de datos personales debe ser veraz, completa, exacta, actualizada, comprobable y comprensible, lo que implica la prohibición del tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

Principio de transparencia: En el tratamiento de datos personales la Secretaría Distrital de Planeación le garantiza al titular de la información el derecho a obtenerla en cualquier momento y sin restricciones.

Principio de acceso y circulación restringida: Los datos personales no podrán estar disponibles en internet u otros medios de comunicación masiva, a menos que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados.

Principio de seguridad: Los datos personales sujetos a tratamiento por la Secretaría Distrital de Planeación serán objeto de protección en la medida en que los recursos técnicos y estándares adoptados así lo permitan. En este sentido, se adoptarán medidas administrativas y tecnológicas para evitar su adulteración, modificación, pérdida, consulta, y, en general, cualquier uso o acceso no autorizado o fraudulento.

Principio de confidencialidad: Todas las personas que, en ejercicio de sus funciones, administren, manejen, actualicen o tengan acceso a información de bases o bancos de datos, se comprometen a conservarla y mantenerla de manera estrictamente confidencial y no revelarla a terceros. Esta obligación se mantiene después de finalizada su relación con alguna de las labores que comprende el tratamiento.

¿QUIÉN ES EL RESPONSABLE DEL TRATAMIENTO DE LOS DATOS PERSONALES?

- Responsable: Secretaría Distrital de Planeación - SDP, en cabeza del (la) Representante Legal.

NIT: 899999061-9

Domicilio: Bogotá D.C., Colombia. Dirección: Cra. 30 N° 25-90 Pisos 5, 8, 13

¿CUÁLES SON LOS CANALES HABILITADOS POR LA SECRETARÍA PARA EL REGISTRO DE PETICIONES CIUDADANAS?

Para la radicación de peticiones, consultas y reclamos a través del cual el ciudadano o un tercero puede conocer, actualizar, rectificar y suprimir algún dato, la Secretaría Distrital de Planeación tiene dispuestos los siguientes canales de atención:

- Canal Presencial. Ventanilla de radicación en correspondencia, ubicada en el primer piso del SuperCade CAD (Cra. 30 N° 25-90).
- Canal Virtual: Virtual: En el enlace de interés http://www.sdp.gov.co/enlace-de-interes, puede realizar solicitudes o peticiones:
    - Radicación virtual: https://sipa.sdp.gov.co/webfile/
    - Bogotá te escucha: https://sdqs.bogota.gov.co/sdqs/login
    - Contáctenos: https://bogota.gov.co/sdqs/crear-peticion
    - Correo electrónico: servicioalciudadanoGEL@sdp.gov.co

Las respuestas a estas solicitudes, así como la obtención de información acerca del procedimiento de consultas y reclamaciones se darán en el medio escogido por el ciudadano, de acuerdo con los canales disponibles:

- Telefónico: PBX 3358000 o directamente a la Línea 195 opción 8

En todos los canales habilitados para el servicio, se dará a conocer la política de protección de datos personales.

Todas las dependencias de la Secretaría Distrital de Planeación, obedeciendo al tipo de información que manejan en el cumplimiento de sus funciones, son encargadas y garantes del tratamiento de los datos personales según lo establecido en las normas vigentes.

¿CÓMO ES EL TRATAMIENTO DE LOS DATOS Y CUÁL ES SU FINALIDAD?

La información y datos personales, suministrados por el ciudadano titular de estos, serán utilizados por la Secretaría Distrital de Planeación para el desarrollo de las funciones propias de la entidad, por lo que debe tenerse en cuenta que:

- El titular reconoce que la información personal que brinda a la Secretaría Distrital de Planeación se da de manera voluntaria cuando presenta requerimientos específicos para realizar un trámite, queja o reclamo, a través de los diferentes canales.
- El titular acepta que la Secretaría Distrital de Planeación recolecta datos personales, a través del registro de información por los diferentes canales de atención al ciudadano y/o a través de cualquier medio utilizado en desarrollo de la gestión de los procesos de la entidad.

En este sentido, la recolección y tratamiento de los datos personales tiene las siguientes finalidades de acuerdo al grupo de interés:

CIUDADANOS

1. Responder las Consultas, Peticiones y Reclamos que allegue cualquier ciudadano a través de los mecanismos de comunicación de la Secretaría Distrital de Planeación.
2. Realizar trámites y servicios que sean de competencia de la Secretaría Distrital de Planeación y que sean solicitados por la ciudadanía.
3. Gestionar, controlar y mantener la trazabilidad de las operaciones que se realicen con ocasión al cumplimiento del objeto principal de la Secretaría Distrital de Planeación.
4. Establecer un canal de comunicación con el ciudadano, a fin de informar las novedades que, con respecto a los servicios y beneficios ofrecidos por la Entidad, así como proporcionar nuevos servicios a través de las campañas institucionales que se desarrollen.
5. Transmitir información personal a terceros de orden gubernamental en el ejercicio de sus funciones y misionalidad que puedan complementar la prestación de un servicio de calidad ofrecido por la Secretaría Distrital de Planeación.
6. Elaborar estudios de estadísticas para propósitos internos de la entidad.
7. Permitir el acceso a las instalaciones de la Secretaría Distrital de Planeación.

CANDIDATOS A FUNCIONARIOS

1. Enviar a través de la dirección de correo electrónico suministrado por el titular, información relacionada con el proceso de selección, contrato de trabajo o de prestación de servicios, pagos y en general información de carácter laboral o contractual que requiera ponerse en su conocimiento.
2. Para fines de seguridad, registro y control de acceso a las instalaciones con los datos recolectados a través de puntos de seguridad, así como, los datos tomados de los documentos suministrados por el Titular al personal de seguridad física y los obtenidos de las videograbaciones que se realizan dentro de las instalaciones de la Entidad y todas sus sedes, serán utilizados

para fines de seguridad y vigilancia de las personas, los bienes e instalaciones de la Entidad, y podrán ser utilizados como prueba en cualquier tipo de proceso judicial o administrativo.

3. Realizar, directa o indirectamente, transmisión o transferencia nacional o internacional de datos, cuando resulte imprescindible para el correcto funcionamiento de la Entidad, circunstancia que el Titular, al autorizar el tratamiento del dato, acepta con dicho acto tal proceder.
4. Elaborar estudios de estadísticas para propósitos internos de la entidad.
5. Dar acceso a su historia laboral o contractual, incluyendo certificados de aptitud médica ocupacional y demás documentos relacionados con estos para manejo interno en la Entidad.
6. Acceder y consultar la información del Titular del dato que repose o esté contenida en bases de datos o archivos de cualquier Entidad Privada o Pública ya sea nacional, internacional o extranjera.
7. Solicitar a las entidades prestadoras de servicios de salud (EPS y/o ARL), copia de su historia clínica para efectuar los trámites que establezcan como necesaria esta información, sin limitarse a la transcripción de incapacidades.
8. Realizar el tratamiento de sus datos personales con los fines necesarios en la administración y gestión de la planta de personal y contratistas de la Entidad.

FUNCIONARIOS

En caso de llegar a ser seleccionado y vinculado efectivamente por la Entidad, el titular permitirá realizar el siguiente tratamiento adicional de los datos personales:

1. Para realizar procesos de capacitación, sensibilización, entrenamiento, trasferencia de conocimiento e inducción de los diferentes colaboradores de la Entidad, sobre procesos, políticas, procedimientos, sistemas de gestión y reglamentos establecidos por la entidad.
2. Establecer, mantener, modificar y terminar las relaciones contractuales que sean necesarias con los funcionarios que sean necesarias para ejecutar las funciones que le fueron asignadas por ley; así como también gestionar y mantener la trazabilidad de todos los contratos que hayan sido suscritos y se encuentren vigentes.
3. Registro en los sistemas de información de la entidad para el desarrollo de procedimientos contables y financieros de la Entidad.
4. Publicar imágenes, videos y demás contenidos de publicidad y eventos en redes sociales, el sitio web de la entidad y carteleras digitales internas.
5. Generación y legalización de pólizas de cumplimiento y calidad del servicio.
6. Gestión de la hoja de vida del funcionario: verificación de formación académica, referencias laborales, personales y familiares, antecedentes judiciales y demás requisitos del cargo a proveer;
7. Vinculación, afiliación o reporte de novedades asociadas al sistema de seguridad social, pensiones, cesantías y riesgos laborales;
8. Gestión administrativa del contrato laboral;
9. Solicitar a las entidades prestadoras de servicios de salud (EPS y/o ARL), copia de su historia clínica para efectuar los trámites que establezcan como necesaria esta información, sin limitarse a la transcripción de incapacidades;
10. Gestionar pagos de nóminas, primas, horas extras, bonificaciones y/o liquidaciones;
11. Concesión y gestión de permisos, licencias y autorizaciones al trabajador;
12. Control de horario laboral;
13. Gestión de programas de formación y capacitación acorde a los requerimientos de los roles y responsabilidades de la función encomendada;
14. Afiliación de las personas a cargo a la caja de compensación para el acceso a subsidios;
15. Desarrollar actividades de bienestar y desarrollo integral de los funcionarios y su núcleo familiar;
16. Gestión de procedimientos administrativos internos, tales como: procesos disciplinarios, sanciones, descargos, entre otros;
17. Gestión de información de salud necesaria para el desarrollo del Sistema de Gestión de Seguridad y Salud en el Trabajo - SGSST;
18. Seguridad, registro y control de acceso a las instalaciones de la entidad;
19. Inscripción a programas, actividades lúdicas, eventos deportivos y/o culturales.
20. Campañas de actualización de datos e información de cambios en el tratamiento de datos personales.

CONTRATISTAS

1. Realizar las verificaciones que sean necesarias en desarrollo del proceso de contratación para corroborar la veracidad de la información contenida en la hoja de vida, documentos entregados y formularios propios de la entidad;
2. Gestión de la hoja de vida del contratista;
3. Verificación de afiliación al sistema de seguridad social y régimen de pensiones;
4. Enviar a través de la dirección de correo electrónico que haya suministrado, información relacionada con el proceso para el contrato de prestación de servicios;
5. Registro en los sistemas de información de la entidad para el desarrollo de procedimientos contables y financieros;
6. Inducción de los contratistas sobre procesos, políticas, procedimientos, sistemas de gestión y reglamentos establecidos por la entidad;
7. Gestionar y realizar actividades de pago de honorarios como contratista;
8. Establecer, mantener, modificar y terminar las relaciones contractuales que sean necesarias para ejecutar las funciones que le fueron asignadas; así como también gestionar y mantener la trazabilidad de todos los contratos que hayan sido suscritos y se encuentren vigentes;
9. Seguridad, registro y control de acceso a las instalaciones;

PROPONENTES, PROVEEDORES Y COLABORADORES

1. Realizar las verificaciones que sean necesarias en desarrollo del proceso de contratación para corroborar la veracidad de la información contenida en los documentos entregados y formularios propios de la entidad;
2. Verificación de antecedentes comerciales, reputacionales, administrativos y judiciales;
3. Vinculación jurídica y comercial de proveedores;
4. Acreditación de condiciones financieras de los proveedores;
5. Generación de solicitudes de cotización y otras actividades relacionadas con el proceso de adquisición de bienes o servicios;
6. Gestión administrativa del contrato;
7. Registro en los sistemas de información de la entidad para el desarrollo de procedimientos contables y financieros;
8. Gestión de facturación, cobros y pagos;
9. Seguimiento y control al cumplimiento de las actividades correspondientes al contrato;
10. Declaración y pago de aportes de seguridad social a los colaboradores de proveedores;
11. Verificación del cumplimiento de estándares relacionados con la prestación del servicio;

VISITANTES

1. Seguridad, registro y control de acceso a las instalaciones;
2. Gestión de información de salud necesaria para el desarrollo del Sistema de Gestión de Seguridad y Salud en el Trabajo - SGSST;
3. Elaborar estudios de estadísticas para propósitos internos de la entidad.

Para los grupos de interés, candidatos a funcionarios, funcionarios, contratistas, proponentes, proveedores y colaboradores y los ciudadanos que sean usuarios de trámites o servicios que estén priorizados en el Sistema de Administración del Riesgo de Lavado de Activos, Financiación del Terrorismo y Financiación de la Proliferación de Armas de Destrucción Masiva - SARLAFT de la Entidad; la recolección de datos personales tiene como finalidad la consulta de listas restrictivas, vinculantes y fuentes de información pública, en el marco de la aplicación de las medidas de debida diligencia del SARLAFT, así como la generación de reportes a nivel nacional y distrital. La gestión de la información anteriormente mencionada estará a cargo del rol del Oficial de Cumplimiento del SARLAFT de la Entidad, o quien haga sus veces.

Cualquier otro tipo de finalidad que se pretenda dar a los datos personales deberá ser informado previamente en el aviso de privacidad y en la respectiva autorización otorgada por el titular del dato, según sea el caso, y siempre teniendo en cuenta los principios rectores para el tratamiento de los datos personales establecidos por la Ley, el presente documento y las demás normas que desarrollen la materia.

¿CÓMO ES EL TRATAMIENTO DE LOS DATOS DE LAS NIÑAS, NIÑOS Y ADOLESCENTES?

Es posible que la Secretaría Distrital de Planeación reciba o haya recibido datos de niñas, niños y adolescentes. En este caso, el suministro de esta información será de carácter facultativo; es decir, no será obligatorio, tanto para ellos, como para quienes actúen en su nombre.

En todo caso, la Secretaría Distrital de Planeación velará por el uso adecuado de los datos personales de esta población y respetará y asegurará la protección de sus derechos fundamentales y, en lo posible, teniendo en cuenta su opinión como titulares de sus datos personales, bajo las siguientes finalidades:

1. Generar comunicaciones al interior y exterior de la SDP que tengan como objetivo dar visibilidad al propósito misional de la Entidad.
2. Utilizar las fotografías y videograbaciones para ser publicadas en el sitio web de la Entidad, en redes sociales como Twitter, Facebook, Instagram y YouTube e inclusive para piezas de publicidad internas y externas impresas o digitales.
3. Generar evidencia de realización y participación en eventos.
4. Fotos y/o videograbaciones podrán tratarse en formato o soporte material, en ediciones impresas o en medio electrónico, óptico, magnético, en redes, (Intranet e Internet), mensajes de datos o similares y en general para cualquier medio o soporte conocido.

¿A QUIÉNES SE LES PUEDE SUMINISTRAR INFORMACIÓN?

La información que reúna las condiciones establecidas en la Ley podrá suministrarse a las siguientes personas:

- A los titulares, sus causahabientes (personas que han sucedido o sustituido al titular) cuando aquellos falten, o sus representantes legales.
- A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial.
- A los terceros autorizados por el titular o por la ley.

¿CUÁLES SON LOS DERECHOS DE LOS TITULARES DE LOS DATOS PERSONALES?

La Secretaría Distrital de Planeación dará a conocer al titular de la información la existencia de bases de datos que contienen datos personales y le garantizará el goce efectivo de sus derechos para que pueda:

- Acceder, conocer, rectificar, actualizar y eliminar sus datos ante la Secretaría Distrital de Planeación, como responsable de su tratamiento. Lo que incluye datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o que no hayan sido autorizados.
- Recibir información por parte de la Secretaría Distrital de Planeación, previa solicitud, respecto del uso que se les ha dado a sus datos personales.
- Acudir ante las autoridades legalmente constituidas (por ejemplo: superintendencias) y presentar quejas por incumplimiento a la normatividad vigente, previo trámite de consulta o requerimiento ante el responsable del tratamiento, en este caso, la Secretaría Distrital de Planeación.
- Solicitar la eliminación del dato cuando en su tratamiento no se respeten los principios, derechos y garantías constitucionales y legales vigentes.
- Tener conocimiento y acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento.

El titular podrá ejercer estos derechos a través de los canales citados en el numeral 8 de este documento.

¿CUÁLES SON LOS DEBERES DE LOS RESPONSABLES Y ENCARGADOS DEL TRATAMIENTO DE DATOS PERSONALES EN LA SECRETARÍA DISTRITAL DE PLANEACIÓN?

Los deberes de los responsables y encargados del tratamiento de los datos personales en la Secretaría Distrital de Planeación, de conformidad con lo establecido en la Ley 1581 de 2012, son los siguientes:

"**Artículo 17.** Deberes de los responsables del Tratamiento. Los Responsables del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;
b) Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular;
c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización

otorgada; Departamento Administrativo de la Función Pública Ley 1581 de 2012 5 EVA - Gestor Normativo;

d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible;
f) Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada;
g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento;
h) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley;
i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular;
j) Tramitar las consultas y reclamos formulados en los términos señalados en la presente ley;
k) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos;
l) Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo;
m) Informar a solicitud del Titular sobre el uso dado a sus datos;
n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
o) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

Artículo 18. Deberes de los Encargados del Tratamiento. Los Encargados del Tratamiento deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la presente ley y en otras que rijan su actividad:

a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;
b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
c) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la presente ley;
d) Actualizar la información reportada por los Responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo;
e) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente ley;
f) Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los Titulares;
g) Registrar en la base de datos la leyenda "reclamo en trámite" en la forma en que se regula en la presente ley;
h) Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal;
i) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio;
j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella;
k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares;
l) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

Parágrafo. En el evento en que concurran las calidades de Responsable del Tratamiento y Encargado del Tratamiento en la misma persona, le será exigible el cumplimiento de los deberes previstos para cada uno."1. Artículo 17 Ley 1581/2012.

¿CUÁL ES EL ÁREA RESPONSABLE DE LA ATENCIÓN DE PETICIONES, CONSULTAS Y RECLAMOS DE DATOS PERSONALES?

En la Secretaría Distrital de Planeación, el área responsable de administrar los servicios de la ventanilla única de radicación y las notificaciones de la Secretarla de acuerdo con los procedimientos establecidos es la Dirección Administrativa, de la Subsecretaria de Gestión Institucional, la cual, a través de la ventanilla de radicación de correspondencia, da al titular de la información la garantía de conocer, actualizar, rectificar y suprimir sus datos.

Por su parte la Dirección de Servicio a la Ciudadanía es la responsable de analizar, gestionar, direccionar, tramitar y/o responder las

peticiones, quejas, reclamos, sugerencias, denuncias, solicitudes y felicitaciones presentadas por los ciudadanos o usuarios, de conformidad con los acuerdos de niveles de servicio establecidos por la Secretaría Distrital de Planeación. Así mismo, le corresponde realizar el seguimiento de las solicitudes de Habeas Data, con el fin de velar por la atención oportuna de estas.

En el marco del Decreto 432 de 2022 se estableció la responsabilidad a la Dirección de Información y Estadística de diseñar la política y lineamientos respecto de los estándares y mejores prácticas en materia gobierno y protección de datos para la Secretaría.

Las solicitudes serán asignadas a las áreas que en ejercicio de sus funciones hayan realizado la recolección y el tratamiento del dato personal objeto de consulta o reclamo, para que realicen directamente la atención y resolución de las peticiones o solicitudes ciudadanas.

¿CUÁL ES EL PROCEDIMIENTO PARA QUE LA CIUDADANÍA PUEDA EJERCER SU DERECHO DE HABEAS DATA?

La Secretaría Distrital de Planeación garantizará los medios y mecanismos necesarios para ejercer este derecho, que serán los mismos para la recepción y atención de peticiones, quejas, reclamos, sugerencias y denuncias. En este sentido, el titular de los datos personales tiene derecho a presentar ante la Secretaría Distrital de Planeación, consultas y/o reclamos, previa validación de su identidad.

Posteriormente, la Secretaría Distrital de Planeación responderá la consulta y/o reclamo por el medio disponible que sea seleccionado por el titular de la información para recibir la respuesta.

A continuación, se presentan los procedimientos, de acuerdo con la necesidad del ciudadano o titular de la información (acceder, conocer, rectificar, actualizar y eliminar sus datos):

a) Consulta de información de datos personales:

- Los titulares o sus causahabientes (personas que han sucedido o sustituido al titular) podrán solicitar la consulta de la información personal de las bases de datos o archivos de la Secretaría Distrital de Planeación.
- La Secretaría Distrital de Planeación consultará en los sistemas de información especializados en donde reposa la información personal para atender la solicitud.
- La Secretaría Distrital de Planeación suministrará al titular toda la información que esté vinculada con su identificación, de acuerdo con la legislación vigente.
- La consulta será atendida en un término máximo de 10 días hábiles, contados a partir de la fecha de recibo de esta. Si no es posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en la que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término[4].

b) Actualización y rectificación de datos personales

- La Secretaría Distrital de Planeación rectificará y actualizará, a solicitud del titular o su representante, toda información que de éste resulte incompleta o inexacta.
- El titular o su representante señalará las actualizaciones y rectificaciones necesarias, junto con la documentación que soporta dicha solicitud.

c) Supresión o eliminación de datos personales

- Los titulares podrán solicitar la eliminación de sus datos personales mediante una petición, cuando consideren que los datos no están recibiendo un tratamiento adecuado o no son pertinentes o necesarios para la finalidad para la cual fueron

recolectados.

- Si vencido el término legal respectivo, no se han eliminado los datos personales, el titular tendrá derecho a solicitar a la Superintendencia de Industria y Comercio que ordene la supresión de los datos personales de las bases de datos de la entidad.
- No obstante, la solicitud de eliminación de datos no podrá realizarse cuando el titular tenga un deber legal o contractual de permanecer en la base de datos o la eliminación de los datos represente un impedimento en actuaciones administrativas o judiciales relacionadas a obligaciones fiscales, investigación de delitos o actualización de sanciones administrativas.

d) Reclamos de tratamiento de datos personales

- El titular o su representante que considere que la información contenida en una base de datos de la Secretaría Distrital de Planeación debe ser objeto de corrección, actualización o eliminación, o cuando note el presunto incumplimiento de cualquiera de los deberes contenidos en la Ley Estatutaria 1581 de 2012 (Ley de protección de datos personales), podrá presentar un reclamo ante la entidad, el cual debe contar como mínimo con la siguiente información:

  - Nombres y apellidos completos.
  - Número de identificación del titular.
  - Datos de contacto (dirección física o electrónica y número telefónico).
  - Área que realizó la recolección de la información.
  - Medios en los que desea recibir la respuesta (dirección de envío de correspondencia o correo electrónico).
  - Descripción de los motivos o hechos que dan lugar al reclamo.
  - Documentos que desea hacer valer.
  - Firma (si aplica).

- Si la información del reclamo está incompleta, la Secretaría Distrital de Planeación le solicitará al interesado, dentro de los cinco (5) días siguientes a la recepción del reclamo, que complete lo necesario. Si pasados dos (2) meses, el solicitante no ha presentado la información requerida, se entenderá que ha desistido del reclamo. Artículo 15 Ley 1581/2012.
- En caso de que quien reciba el reclamo no sea competente para resolverlo, la Secretaría Distrital de Planeación dará traslado a quien corresponda en un término máximo de los cinco (5) días hábiles se informará de la situación al interesado en concordancia a la Ley 1755 del 2015.
- Una vez recibido el reclamo completo, se incluirá en el Sistema de Información de Procesos Automáticos - SIPA para la atención y deberámantenerse abierto hasta que el reclamo sea decidido, cuyo estado será *"Finalizado"*.
- El término máximo para atender el reclamo será de quince (15) días hábiles, contados a partir del día siguiente a la fecha de su recibo. Si no es posible atender el reclamo dentro de dicho término, la Secretaría Distrital de Planeación le informará al interesado los motivos de la demora y la fecha en la que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término[5].
- Todas las peticiones, consultas y reclamos relacionadas con el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar la información que se haya recolectado sobre ellas en bases de datos o archivos (Art. 15 Constitución Política de Colombia) se clasificarán como solicitudes de *habeas data* en las diferentes herramientas de registro o gestión documental de la entidad.
- El reclamo podrá ser atendido a favor; es decir, de acuerdo con lo solicitado; o en contra, para lo cual se explicarán las razones de su no aplicación.

Nota: Requisito de Procedibilidad[6]: Los interesados podrán elevar la queja frente a la Superintendencia de Industria y Comercio

(Ente que regula el cumplimiento de la Ley 1581/2012), si su derecho ha sido vulnerado o haya agotado el trámite de consulta o reclamo ante la Secretaría Distrital de Planeación.

¿CUÁLES SON LAS MEDIDAS DE SEGURIDAD DE LOS DATOS PERSONALES?

En desarrollo del principio de seguridad establecido en la normatividad vigente, la Secretaría Distrital de Planeación adoptará las medidas técnicas, humanas y administrativas para garantizar la seguridad de la información registrada en las bases de datos, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, lo anterior, dando cumplimiento al Modelo de Seguridad y Privacidad de la Información - MSPI, expedido por MinTic.

La Alcaldía Mayor de Bogotá emitió la Directiva 001 del 03 de marzo de 2021 (https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=108172), a través de la cual se establecen las directrices para la protección de identidad del denunciante, estableciendo que, en los canales de atención al ciudadano, se deberá garantizar la protección de identidad del denunciante y reservar la información suministrada, así como las pruebas allegadas; para ello, los funcionarios y/o contratistas de la entidad que colaboren con la recepción, registro, tipificación, direccionamiento y gestión de una denuncia de posibles actos de corrupción, y/o inhabilidades, incompatibilidades o conflictos de intereses, deberán suscribir un compromiso de confidencialidad y no divulgación de dicha información.

¿CUÁL ES LA VIGENCIA DE ESTA POLÍTICA?

A partir de su publicación oficial en el Sistema de Gestión de la Secretaría Distrital de Planeación y en su Portal web: www.sdp.gov.co.

6.19.POLITICA ESCRITORIO LIMPIO Y PANTALLA LIMPIA

Principio General:

En aplicación de la norma ISO/IEC 27001 versión 2022 - Categoría A.7 Controles físicos, numeral 7.7 - Escritorio despejado y pantalla despejada, la Secretaría Distrital de Planeación (SDP) establece las directrices generales para prevenir el acceso no autorizado, la pérdida y/o daño de la información que produce o gestiona, tanto en formato físico como digital, dentro y fuera del horario laboral.

Lineamientos Específicos:

1. Lineamientos Generales (7.7 - Escritorio despejado y pantalla despejada):

- **Escritorio Físico y Virtual Limpios:** No deberán dejarse documentos críticos en el escritorio físico ni en el escritorio virtual (espacio digital en los equipos de cómputo). Se deben emplear cajoneras o archivos para el almacenamiento de información sensible o crítica.
- **Bloqueo de Equipos:** Cada vez que los funcionarios se retiren del lugar de trabajo, deben bloquear los equipos de cómputo (Windows + L).
- **Orden y Limpieza:** Los puestos de trabajo deben permanecer limpios y ordenados. Los dispositivos de impresión y digitalización deben permanecer libres de documentos.
- **Apagado de Dispositivos:** Todos los equipos de cómputo y dispositivos de impresión y digitalización deben apagarse cuando no estén en uso.
- **Ubicación de Puestos de Trabajo (7.1 - Perímetros de seguridad física):** Los lugares de trabajo que manejan información confidencial, clasificada o reservada deben ubicarse preferiblemente en sitios con acceso restringido y control de entrada. Los puestos de trabajo cercanos a zonas de atención o tránsito no deben exponer documentos con información sensible.
- **Bloqueo de Sesiones (8.3 - Restricción de acceso a la información):** Toda sesión de trabajo en los equipos de cómputo debe bloquearse con un mecanismo de bloqueo de pantalla y teclado controlado por contraseña cuando no estén siendo atendidos. Se configurará el bloqueo automático de la sesión luego de un tiempo límite de inactividad de máximo 5 minutos.

- **Cierre de Gabinetes y Archivadores:** Los gabinetes, cajones y archivadores que contengan documentos o medios extraíbles con información sensible deben quedar cerrados durante la hora de almuerzo y al finalizar la jornada laboral.

- **Control de Acceso a las Áreas de Trabajo (7.2 - Controles de entrada física):** Todo usuario o persona externa que ingrese a un área donde se encuentran los puestos de trabajo debe ser anunciado y su ingreso debe ser autorizado y acompañado por un funcionario.

- **Limpieza de Equipos en Préstamo:** Los equipos de cómputo o portátiles solicitados en préstamo deben quedar libres de información al finalizar el préstamo. El personal de soporte realizará periódicamente el mantenimiento y depuración de archivos en estos equipos.

- **Limpieza de Salas de Reunión:** Las salas y áreas de reunión, una vez utilizadas, deben quedar libres de todo material y los tableros deben quedar limpios de información confidencial.

- **Seguridad en Impresión y Copiado (7.4 - Protección contra amenazas físicas y ambientales):** Los equipos de reproducción de información deben utilizarse con un sistema de claves. Los funcionarios deben garantizar la confidencialidad e integridad de los documentos reproducidos, retirándolos, almacenándolos o eliminándolos apropiadamente.

- **Política Cero Papel:** Los servidores públicos deben velar por la aplicación de la política cero papel, sustituyendo los flujos documentales en papel por medios electrónicos.

2. Responsabilidades (5.10 - Responsabilidades):

- **Usuarios (Funcionarios, Contratistas y Personal Temporal):**

  - Cumplir con esta política.

  - Asegurar que al levantarse del puesto de trabajo y al finalizar la jornada laboral, el escritorio esté despejado y libre de documentos y/o medios extraíbles con información protegida.

  - Eliminar la información en los portátiles antes de devolverlos.

  - Retirar inmediatamente los documentos impresos o digitalizados.

  - Mantener el escritorio de su perfil limpio, almacenando los archivos en las unidades locales o recursos compartidos.

  - Bloquear su estación de trabajo al ausentarse (Windows + L).

  - Reportar cualquier incumplimiento que ponga en riesgo la seguridad de la información (procedimiento GTI-PD-008).

- **Dirección de Tecnologías de la Información y las Comunicaciones:**

  - Apoyar, definir normas y procedimientos para mantener el escritorio limpio y la pantalla despejada.

  - Establecer las condiciones y controles para el acceso seguro a la información.

  - Configurar el bloqueo automático de la sesión de trabajo.

  - Aplicar un protector de pantalla estándar.

  - Divulgar periódicamente esta política.

- **Dirección Administrativa:**

  - Institucionalizar y socializar la Política de Gestión Documental (GAD-PO-001).

  - Establecer y actualizar los mecanismos y controles para la reproducción de documentos.

  - Gestionar los controles de seguridad relacionados con los accesos físicos a las instalaciones (Política de Seguridad Física y del Entorno).

- Garantizar el servicio de vigilancia y la provisión de muebles para archivos y puestos de trabajo seguros.

- **Líder de Seguridad de la Información:**

  - Actualizar y velar por el cumplimiento de esta política.

- **Directivos y Líderes de Procesos:**

  - Apoyar y fomentar el cumplimiento de esta política entre sus colaboradores.

Relación con otros numerales de la ISO 27001:2022:

- **7.3 (Seguridad física perimetral):** Relacionado con la ubicación de puestos de trabajo que manejan información sensible.
- **8.5 (Información de respaldo):** Se debe considerar la seguridad de la información en las copias de seguridad.
- **8.10 (Eliminación de información):** Se relaciona con la eliminación segura de documentos impresos y archivos digitales.

6.20.POLÍTICAS PARA EL USO ADECUADO DE INTERNET

Principio General:

El internet es un recurso valioso para el desempeño de las labores de todos los funcionarios. Esta política define los lineamientos para su uso adecuado, buscando equilibrar la productividad con la seguridad de la información y el cumplimiento legal.

Lineamientos Específicos:

1. Restricciones de Acceso a Sitios Web (8.23 - Filtrado web):

- **Contenido Inapropiado o Ilegal:** Se limitará el acceso a portales de juegos, pornografía, drogas, terrorismo, segregación racial, hacking, malware, software gratuito o ilegal y/o cualquier otra página que vaya en contra de las leyes vigentes. Este control se implementará mediante soluciones de filtrado web y otras herramientas técnicas.
- **Redes Sociales:** Se limitará el acceso a redes sociales en general, salvo autorización expresa y justificada por necesidades del cargo y con la implementación de controles de seguridad adicionales. Se debe definir una lista de redes sociales permitidas y los casos de uso autorizados.
- **Servicios de Nube e Intercambio de Información Masiva (8.26 - Uso de servicios de red):** Se restringirá el acceso a portales de nube e intercambio de información masiva (exceptuando la nube corporativa o institucional). Se debe promover el uso exclusivo de las plataformas corporativas para el almacenamiento e intercambio de información.

2. Monitoreo y Registros de Navegación (8.16 - Monitoreo):

- **Revisión de Logs:** El grupo/oficina de TIC podrá verificar los logs o registros de navegación cuando así se solicite o se requiera para las investigaciones o requerimientos que puedan generarse, respetando siempre la legislación vigente en materia de privacidad y protección de datos personales. Se debe definir un procedimiento para la revisión de logs que incluya la autorización, el alcance y la confidencialidad de la información.

3. Uso Aceptable (Relacionado con 5.10 - Responsabilidades y 5.21 - Clasificación de la información):

- **Propósito Laboral:** El acceso a Internet debe estar principalmente orientado al desarrollo de las funciones laborales. El uso personal debe ser mínimo y no debe interferir con las responsabilidades laborales ni comprometer la seguridad de la información.
- **Seguridad de la Información:** Se prohíbe la descarga e instalación de software no autorizado, así como la divulgación de información confidencial de la SDP a través de Internet.
- **Protección contra Malware:** Se deben seguir las recomendaciones de seguridad para evitar la descarga de malware, como no abrir correos electrónicos sospechosos ni descargar archivos de fuentes no confiables.

- **Uso de Contraseñas Seguras (8.4 - Gestión de contraseñas):** Se deben utilizar contraseñas seguras y cambiarlas periódicamente para proteger las cuentas de usuario y el acceso a Internet.

4. Responsabilidades (5.10 - Responsabilidades):

- **Usuarios:** Son responsables de cumplir con esta política y de utilizar Internet de manera responsable y segura.
- **Grupo/Oficina de TIC:** Es responsable de implementar los controles técnicos para restringir el acceso a sitios web no autorizados, monitorear el uso de Internet y gestionar los incidentes de seguridad relacionados.
- **Líder de Seguridad de la Información:** Es responsable de mantener actualizada esta política y de coordinar las acciones relacionadas con la seguridad de Internet.

Relación con otros numerales de la ISO 27001:2022:

- **5.21 (Clasificación de la información):** El uso de Internet debe considerar la clasificación de la información que se maneja.
- **8.3 (Restricción de acceso a la información):** Se deben implementar controles de acceso para restringir el acceso a información sensible a través de Internet.
- **8.13 (Copia de seguridad de la información):** Se deben realizar copias de seguridad de la información importante que se almacena o se transmite a través de Internet.
- **8.28 (Codificación segura):** En el caso de aplicaciones web desarrolladas por la SDP, se deben aplicar prácticas de codificación segura.

6.21.POLÍTICAPARAEL USO DE DISPOSITIVOS MÓVILES EN LASDP

Principio General:

En aplicación de la Norma ISO/IEC 27001 versión 2022 - Categoría A.8 Controles tecnológicos, Control 8.1, Dispositivos de punto final de usuario, se protegerá la información almacenada, procesada o accesible a través de los dispositivos finales del usuario, ya sean institucionales o personales (BYOD - Bring Your Own Device). El objetivo principal es establecer las condiciones para el manejo seguro y responsable de estos dispositivos.

Lineamientos Específicos:

1. Gestión de Dispositivos Móviles (8.1 - Dispositivos de punto final de usuario):

- **Inventario y Registro (8.2 - Gestión de activos):** Se mantendrá un inventario actualizado de los dispositivos móviles institucionales, incluyendo información como el tipo de dispositivo, el propietario, el número de serie y el software instalado. Para los dispositivos personales que accedan a información de la SDP, se requerirá un registro con información básica y la aceptación de las políticas de seguridad.
- **Configuración Segura (8.3 - Restricción de acceso a la información, 8.4 - Gestión de contraseñas, 8.24 - Gestión de vulnerabilidades técnicas):** Se establecerán configuraciones de seguridad obligatorias para todos los dispositivos móviles que accedan a información de la SDP, incluyendo:
  - **Contraseñas robustas:** Se exigirá el uso de contraseñas complejas y se implementará el bloqueo automático del dispositivo tras un número determinado de intentos fallidos.
  - **Cifrado del dispositivo (8.18 - Cifrado):** Se requerirá el cifrado del almacenamiento del dispositivo para proteger la información en caso de pérdida o robo.
  - **Software antivirus y antimalware (8.22 - Protección contra malware):** Se exigirá la instalación y actualización regular de software antivirus y antimalware.
  - **Actualizaciones del sistema operativo y aplicaciones (8.24 - Gestión de vulnerabilidades técnicas):** Se requerirá

la instalación oportuna de las actualizaciones de seguridad del sistema operativo y las aplicaciones.

- **Borrado remoto (8.1 - Dispositivos de punto final de usuario):** Se implementará la capacidad de realizar un borrado remoto de la información en caso de pérdida, robo o finalización de la relación laboral.

- **Control de aplicaciones (8.25 - Gestión de la configuración):** Se podrá restringir la instalación de aplicaciones no autorizadas o que representen un riesgo para la seguridad de la información.

- **Acceso a la Red Corporativa (8.26 - Uso de servicios de red):** El acceso a la red corporativa desde dispositivos móviles, ya sean institucionales o personales, se realizará a través de una red privada virtual (VPN) segura. Se controlará el acceso a los recursos de la red según el principio de mínimo privilegio.

- **Gestión de Aplicaciones Móviles (8.25 - Gestión de la configuración):** Se establecerá un catálogo de aplicaciones móviles autorizadas para su uso en dispositivos institucionales. Se evaluará la seguridad de las aplicaciones antes de su autorización.

- **Uso de Dispositivos Personales (BYOD) (8.1 - Dispositivos de punto final de usuario):** Se definirá una política específica para el uso de dispositivos personales (BYOD) que accedan a información de la SDP. Esta política deberá incluir los requisitos de seguridad que deben cumplir los dispositivos, las responsabilidades del usuario y las limitaciones de acceso a la información.

2. Uso Aceptable (Relacionado con 5.10 - Responsabilidades y 5.21 - Clasificación de la información):

- **Propósito Laboral:** El uso de dispositivos móviles para acceder a información de la SDP debe estar principalmente orientado al desarrollo de las funciones laborales.

- **Protección de la Información (8.3 - Restricción de acceso a la información):** Se prohíbe el almacenamiento de información confidencial de la SDP en dispositivos personales que no cumplan con los requisitos de seguridad establecidos.

- **Seguridad Física (7.6 - Seguridad de los equipos):** Se deben tomar precauciones para proteger físicamente los dispositivos móviles contra robos, pérdidas o daños.

- **Reporte de Incidentes (5.24 a 5.28 - Gestión de incidentes de seguridad de la información):** Se debe reportar inmediatamente cualquier incidente de seguridad relacionado con dispositivos móviles, como pérdida, robo o sospecha de acceso no autorizado.

3. Responsabilidades (5.10 - Responsabilidades):

- **Usuarios:** Son responsables de cumplir con esta política, de mantener la seguridad de sus dispositivos móviles y de reportar cualquier incidente de seguridad.

- **Dirección de Tecnologías de la Información y las Comunicaciones:** Es responsable de implementar y mantener los controles técnicos de seguridad para los dispositivos móviles, de gestionar el inventario de dispositivos y de brindar soporte a los usuarios.

- **Líder de Seguridad de la Información:** Es responsable de mantener actualizada esta política y de coordinar las acciones relacionadas con la seguridad de los dispositivos móviles.

Relación con otros numerales de la ISO 27001:2022:

- **7.3 (Seguridad física perimetral):** Se debe considerar la seguridad física de las áreas donde se utilizan dispositivos móviles.

- **8.5 (Información de respaldo):** Se deben realizar copias de seguridad de la información importante almacenada en dispositivos móviles institucionales.

- **8.10 (Eliminación de información):** Se deben establecer procedimientos para la eliminación segura de la información de los dispositivos móviles, especialmente al finalizar su vida útil o al cambiar de usuario.

6.22.POLÍTICAS PARA EL USO ADECUADO DE CORREO ELECTRÓNICO:

Principio General:

Los buzones de correo electrónico asignados a los funcionarios, contratistas o terceros pertenecen a la entidad (SDP), y por lo tanto, su contenido también es propiedad de la misma. Esta política define el uso adecuado del correo electrónico institucional, buscando proteger la información, prevenir riesgos de seguridad y asegurar el cumplimiento de las normativas.

Lineamientos Específicos:

1. Propiedad y Uso del Correo Electrónico (Relacionado con 5.10 - Responsabilidades):

- **Propiedad de la Entidad:** Los buzones de correo y su contenido son propiedad de la SDP.
- **Uso Institucional Exclusivo:** El correo electrónico institucional (dominio sdp.gov.co) debe emplearse única y exclusivamente para temas laborales y el desempeño de las funciones correspondientes a cada cargo. Se prohíbe el uso para fines personales, comerciales o financieros.
- **Separación de Cuentas:** Los temas personales deben ser gestionados con cuentas de correo electrónico personales.

2. Monitoreo y Acceso a Buzones (8.16 - Monitoreo):

- **Verificación de Contenido:** La oficina/grupo de tecnología podrá verificar el contenido de los buzones de correo en los casos que se requiera acceder a información para continuar con la prestación del servicio o para investigaciones específicas, siempre respetando la legislación vigente en materia de privacidad y protección de datos personales. Se debe contar con un procedimiento formal para estas acciones que defina las autorizaciones, el alcance y la trazabilidad.

3. Seguridad de las Cuentas (8.4 - Gestión de contraseñas):

- **Responsabilidad del Usuario:** Los usuarios son completamente responsables de todas las actividades realizadas con sus cuentas de acceso y, por ende, del contenido de su buzón de correo electrónico.
- **Cambio de Contraseñas:** Si un usuario sospecha que la seguridad de su cuenta se ha visto comprometida, debe reiniciar su contraseña inmediatamente. Se recomienda cambiar las contraseñas al menos una vez al mes.
- **Complejidad de Contraseñas:** Las contraseñas deben tener un mínimo de ocho (8) caracteres y ser alfanuméricas.

4. Uso Correcto y Prohibiciones (8.23 - Filtrado web, 8.26 - Uso de servicios de red, 8.22 - Protección contra malware):

- **Uso Exclusivo del Usuario:** La cuenta de correo electrónico es de uso exclusivo del servidor o dependencia para quien fue creada y no es transferible.
- **Prohibición de Difusión Masiva:** El correo electrónico institucional no es una herramienta de difusión de información masiva tipo *spam* o cadenas.
- **Actividades Prohibidas:** Se prohíben las siguientes actividades:
    - Utilizar el correo electrónico para cualquier propósito comercial o financiero.
    - Participar en la propagación de "cartas en cadenas" ni en esquemas piramidales.
    - Distribuir de forma masiva grandes cantidades de mensajes con contenidos inapropiados.
    - Enviar archivos adjuntos con extensión ejecutable (.exe, .lnk, .bat, .com, .dll, .PS1, .MSI, .SYS) u otras extensiones potencialmente peligrosas.
- **Tamaño de Archivos Adjuntos:** Se permite el envío de datos adjuntos (Attachments), siempre y cuando el tamaño total del archivo no exceda los 25 MB (tanto de entrada como de salida).
- **Precaución con Correos Desconocidos:** No se deben abrir correos de cuentas desconocidas, con temas llamativos u ofrecimientos grandiosos, ya que normalmente contienen *software* malicioso.
- **Phishing (8.22 - Protección contra malware):** Se debe capacitar a los usuarios para identificar correos electrónicos de

phishing y reportarlos al área de tecnología.

5. Responsabilidades (5.10 - Responsabilidades):

- **Usuarios:** Son responsables de cumplir con esta política, de mantener la confidencialidad de sus contraseñas y de reportar cualquier incidente de seguridad relacionado con el correo electrónico.
- **Oficina/Grupo de Tecnología:** Es responsable de implementar y mantener los controles técnicos de seguridad para el correo electrónico, de monitorear su uso y de gestionar los incidentes de seguridad relacionados.
- **Líder de Seguridad de la Información:** Es responsable de mantener actualizada esta política y de coordinar las acciones relacionadas con la seguridad del correo electrónico.

Relación con otros numerales de la ISO 27001:2022:

- **7.6 (Seguridad de los equipos):** Se debe asegurar la seguridad física de los equipos desde donde se accede al correo electrónico.
- **8.5 (Información de respaldo):** Se deben realizar copias de seguridad del correo electrónico institucional.
- **8.10 (Eliminación de información):** Se deben establecer procedimientos para la eliminación segura de correos electrónicos, especialmente aquellos que contienen información sensible.
- **5.24 a 5.28 (Gestión de incidentes de seguridad de la información):** Se deben gestionar los incidentes de seguridad relacionados con el correo electrónico de acuerdo con los procedimientos establecidos.

6.23.POLÍTICAS PARA EL USO DE USUARIOS Y CONTRASEÑAS:

Principio General:

Los buzones de correo electrónico asignados a los funcionarios, contratistas o terceros pertenecen a la entidad (SDP), y por lo tanto, su contenido también es propiedad de la misma. Esta política define el uso adecuado del correo electrónico institucional, buscando proteger la información, prevenir riesgos de seguridad y asegurar el cumplimiento de las normativas.

Lineamientos Específicos:

1. Propiedad y Uso del Correo Electrónico (Relacionado con 5.10 - Responsabilidades):

- **Propiedad de la Entidad:** Los buzones de correo y su contenido son propiedad de la SDP.
- **Uso Institucional Exclusivo:** El correo electrónico institucional (dominio sdp.gov.co) debe emplearse única y exclusivamente para temas laborales y el desempeño de las funciones correspondientes a cada cargo. Se prohíbe el uso para fines personales, comerciales o financieros.
- **Separación de Cuentas:** Los temas personales deben ser gestionados con cuentas de correo electrónico personales.

2. Monitoreo y Acceso a Buzones (8.16 - Monitoreo):

- **Verificación de Contenido:** La oficina/grupo de tecnología podrá verificar el contenido de los buzones de correo en los casos que se requiera acceder a información para continuar con la prestación del servicio o para investigaciones específicas, siempre respetando la legislación vigente en materia de privacidad y protección de datos personales. Se debe contar con un procedimiento formal para estas acciones que defina las autorizaciones, el alcance y la trazabilidad.

3. Seguridad de las Cuentas (8.4 - Gestión de contraseñas):

- **Responsabilidad del Usuario:** Los usuarios son completamente responsables de todas las actividades realizadas con sus cuentas de acceso y, por ende, del contenido de su buzón de correo electrónico.

- **Cambio de Contraseñas:** Si un usuario sospecha que la seguridad de su cuenta se ha visto comprometida, debe reiniciar su contraseña inmediatamente. Se recomienda cambiar las contraseñas al menos una vez al mes.

- **Complejidad de Contraseñas:** Las contraseñas deben tener un mínimo de ocho (8) caracteres y ser alfanuméricas.

4. Uso Correcto y Prohibiciones (8.23 - Filtrado web, 8.26 - Uso de servicios de red, 8.22 - Protección contra malware):

- **Uso Exclusivo del Usuario:** La cuenta de correo electrónico es de uso exclusivo del servidor o dependencia para quien fue creada y no es transferible.

- **Prohibición de Difusión Masiva:** El correo electrónico institucional no es una herramienta de difusión de información masiva tipo *spam* o cadenas.

- **Actividades Prohibidas:** Se prohíben las siguientes actividades:

  - Utilizar el correo electrónico para cualquier propósito comercial o financiero.

  - Participar en la propagación de "cartas en cadenas" ni en esquemas piramidales.

  - Distribuir de forma masiva grandes cantidades de mensajes con contenidos inapropiados.

  - Enviar archivos adjuntos con extensión ejecutable (.exe, .lnk, .bat, .com, .dll, .PS1, .MSI, .SYS) u otras extensiones potencialmente peligrosas.

- **Tamaño de Archivos Adjuntos:** Se permite el envío de datos adjuntos (Attachments), siempre y cuando el tamaño total del archivo no exceda los 25 MB (tanto de entrada como de salida).

- **Precaución con Correos Desconocidos:** No se deben abrir correos de cuentas desconocidas, con temas llamativos u ofrecimientos grandiosos, ya que normalmente contienen *software* malicioso.

- **Phishing (8.22 - Protección contra malware):** Se debe capacitar a los usuarios para identificar correos electrónicos de *phishing* y reportarlos al área de tecnología.

5. Responsabilidades (5.10 - Responsabilidades):

- **Usuarios:** Son responsables de cumplir con esta política, de mantener la confidencialidad de sus contraseñas y de reportar cualquier incidente de seguridad relacionado con el correo electrónico.

- **Oficina/Grupo de Tecnología:** Es responsable de implementar y mantener los controles técnicos de seguridad para el correo electrónico, de monitorear su uso y de gestionar los incidentes de seguridad relacionados.

- **Líder de Seguridad de la Información:** Es responsable de mantener actualizada esta política y de coordinar las acciones relacionadas con la seguridad del correo electrónico.

Relación con otros numerales de la ISO 27001:2022:

- **7.6 (Seguridad de los equipos):** Se debe asegurar la seguridad física de los equipos desde donde se accede al correo electrónico.

- **8.5 (Información de respaldo):** Se deben realizar copias de seguridad del correo electrónico institucional.

- **8.10 (Eliminación de información):** Se deben establecer procedimientos para la eliminación segura de correos electrónicos, especialmente aquellos que contienen información sensible.

- **5.24 a 5.28 (Gestión de incidentes de seguridad de la información):** Se deben gestionar los incidentes de seguridad relacionados con el correo electrónico de acuerdo con los procedimientos establecidos.

6.24.USO DE UTILITARIOS DE SISTEMA

Principio General:

En aplicación del control 8.18 (Uso de programas de utilidad privilegiados) de la norma ISO/IEC 27001:2022, se establece que el uso de programas de utilidad que puedan anular los controles del sistema y de la aplicación debe estar restringido y estrictamente controlado. Dado que estos programas pueden comprometer la seguridad de la información, la SDP implementa esta política para mitigar los riesgos asociados.

Lineamientos Específicos:

1. Control y Restricción de Utilitarios (8.18 - Uso de programas de utilidad privilegiados, 8.3 - Restricción de acceso a la información, 8.25 - Gestión de la configuración):

- **Autenticación para Utilitarios y Funciones Administrativas (8.4 - Gestión de contraseñas):** Se implementarán procedimientos de autenticación robustos, como la autenticación multifactor (MFA) cuando sea posible, para el acceso a utilitarios del sistema y programas con funciones administrativas. Se exigirá el uso de contraseñas complejas y su cambio periódico.

- **Separación y Segregación (8.3 - Restricción de acceso a la información):** Se separarán los utilitarios de las aplicaciones del sistema y se segregarán las funciones siempre que sea posible, aplicando el principio de mínimo privilegio. Esto significa que los usuarios solo tendrán acceso a las funciones y utilitarios estrictamente necesarios para el desempeño de sus funciones.

- **Limitación a Usuarios Autorizados (8.3 - Restricción de acceso a la información, 5.10 - Responsabilidades):** El uso de utilitarios del sistema se limitará únicamente a usuarios fiables y expresamente autorizados por la Dirección de Tecnologías de la Información y las Comunicaciones (TIC). Se mantendrá un registro de los usuarios con privilegios administrativos.

- **Confidencialidad de la Existencia y Uso (8.3 - Restricción de acceso a la información):** Se evitará que personas ajenas a la Entidad tomen conocimiento de la existencia y modo de uso de los utilitarios instalados en los recursos informáticos. La información sobre la configuración y el uso de estos utilitarios se tratará como información confidencial.

- **Inventario y Gestión de Cambios (8.2 - Gestión de activos, 8.25 - Gestión de la configuración):** Se mantendrá un inventario actualizado de los utilitarios de sistema instalados, incluyendo su versión y configuración. Cualquier cambio en la configuración o instalación de nuevos utilitarios deberá ser autorizado y documentado a través de un proceso de gestión de cambios formal.

- **Monitoreo y Auditoría (8.16 - Monitoreo, 9.2 - Auditoría interna):** Se implementarán mecanismos de monitoreo y auditoría para registrar el uso de los utilitarios del sistema. Los registros de auditoría se revisarán periódicamente para detectar cualquier actividad sospechosa o no autorizada.

2. Clasificación y Control de Utilitarios:

- **Clasificación:** Se clasificarán los utilitarios según su nivel de riesgo y los privilegios que otorgan. Los utilitarios con mayor nivel de riesgo requerirán controles de acceso más estrictos.

- **Control de Instalación:** La instalación de nuevos utilitarios estará restringida y requerirá la autorización de la Dirección de TIC. Se evaluará la necesidad y el riesgo de cada utilitario antes de su instalación.

3. Responsabilidades (5.10 - Responsabilidades):

- **Dirección de Tecnologías de la Información y las Comunicaciones (TIC):** Es responsable de la gestión, configuración, control y monitoreo de los utilitarios del sistema, así como de la autorización de usuarios con privilegios administrativos.

- **Líder de Seguridad de la Información:** Es responsable de mantener actualizada esta política y de coordinar las acciones relacionadas con la seguridad de los utilitarios del sistema.

- **Usuarios con Privilegios Administrativos:** Son responsables de utilizar los utilitarios de sistema de manera responsable y de acuerdo con esta política, así como de mantener la confidencialidad de sus credenciales de acceso.

Relación con otros numerales de la ISO 27001:2022:

- **7.6 (Seguridad de los equipos):** Se debe asegurar la seguridad física de los equipos donde se ejecutan los utilitarios.

- **8.10 (Eliminación de información):** Se deben establecer procedimientos para la eliminación segura de información generada

por los utilitarios, cuando corresponda.

- **8.13 (Copia de seguridad de la información):** Se deben realizar copias de seguridad de la configuración de los sistemas y los datos generados por los utilitarios.

- **8.22 (Protección contra malware):** Se deben implementar medidas para prevenir la instalación de malware a través de los utilitarios.

6.25.SENSIBILIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LAINFORMACIÓN

SENSIBILIZACIÓN Y COMUNICACIÓN

1. ALCANCE (4.2 - Comprensión de las necesidades y expectativas de las partes interesadas):

Esta política aplica a todos los servidores públicos, contratistas, pasantes, grupos de valor y grupos de interés de la Secretaría Distrital de Planeación (SDP).

2. OBJETIVO GENERAL:

Establecer los lineamientos para la capacitación y sensibilización en temas relacionados con la seguridad de la información, con la finalidad de disminuir las vulnerabilidades y amenazas relacionadas con el factor humano en la SDP.

3. OBJETIVOS ESPECÍFICOS:

- **Cumplimiento Normativo (6.3 - Concientización, educación y capacitación en seguridad de la información):** Dar cumplimiento a los lineamientos del Modelo de Seguridad y Privacidad de la Información de la SDP (GTI-MA-006) y a lo establecido en las normas ISO 27001 e ISO 27002:2022, específicamente el control 6.3, que describe la necesidad de proporcionar conciencia, educación y capacitación adecuadas en seguridad de la información y actualizaciones periódicas de las políticas y procedimientos relevantes.

- **Compromiso de la Alta Dirección (5.1 - Liderazgo y compromiso):** Lograr el compromiso de la Alta Dirección para la implementación de la política, asegurando que los participantes cuenten con los conocimientos, educación, formación o experiencia adecuada, se sensibilicen y tomen conciencia de la importancia de la protección de la información, así como del conocimiento de instrumentos y herramientas para la identificación de posibles amenazas y vulnerabilidades.

- **Implementación de Estrategias:** Definir e implementar las estrategias necesarias para capacitar y sensibilizar a los participantes en la aplicación de los lineamientos, políticas, procedimientos y demás instrumentos que hacen parte del Modelo de Seguridad y Privacidad de la Información de la SDP.

- **Concientización sobre Buenas Prácticas (5.10 - Responsabilidades):** Involucrar, sensibilizar y concientizar con información oportuna y clara a los participantes en la observancia, adopción y apropiación de buenas prácticas, los deberes y las obligaciones frente a la seguridad de la información y la conservación de sus atributos de integridad, confidencialidad y disponibilidad.

- **Cultura de Seguridad y Privacidad:** Generar en todos los participantes la cultura de la seguridad y privacidad de la información institucional, con base en la normatividad vigente y las políticas establecidas por la entidad.

- **Compromiso con el SGSI (5.1 - Liderazgo y compromiso):** Lograr que todos los participantes, desde su rol, se comprometan a seguir los lineamientos del Sistema de Gestión de Seguridad de la Información (SGSI).

- **Agentes Activos del SGSI:** Lograr que todos los participantes sean agentes activos del SGSI y aporten en la construcción y disponibilidad de información institucional organizada, confiable y robusta.

4. LINEAMIENTOS PARALAIMPLEMENTACIÓN DE LAPOLÍTICA:

- **Plan Anual de Capacitación (6.3 - Concientización, educación y capacitación en seguridad de la información):** El Oficial de Seguridad de la Información elaborará anualmente un plan de capacitación y sensibilización en temas de seguridad y privacidad de la información, incluyendo estrategias para los diferentes grupos de valor y grupos de interés.

- **Inclusión en el PIC:** El Líder de la Política de Gobierno Digital enviará las necesidades de capacitación a la Dirección de Talento Humano para su inclusión en el Plan Institucional de Capacitación (PIC).

- **Gestión con Talento Humano:** La capacitación se gestionará con la Dirección de Talento Humano según el procedimiento establecido.

- **Aprobación del Plan (5.1 - Liderazgo y compromiso):** Las estrategias de capacitación y sensibilización se llevarán a aprobación del Comité Institucional de Gestión y Desempeño.

- **Medios de Sensibilización:** Se utilizarán medios virtuales y presenciales para la sensibilización.

- **Asistencia Obligatoria (5.10 - Responsabilidades):** La participación en los eventos y procesos de capacitación, sensibilización, inducción y reinducción en temas de seguridad y privacidad de la información es obligatoria.

- **Acta de Compromiso (5.10 - Responsabilidades):** Todo nuevo integrante debe diligenciar el GTH-FO-026 ACTA DE COMPROMISO SEGURIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES.

- **Capacitación Específica para Administradores Técnicos (6.3 - Concientización, educación y capacitación en seguridad de la información):** Los administradores técnicos de infraestructura, plataformas o *software* deben recibir capacitación del fabricante y transferencia de conocimiento, incluyendo esto como un entregable contractual.

- **Participación en Jornadas de Sensibilización:** El personal de servicios logísticos (aseo, vigilancia, atención al público, etc.) debe participar en las jornadas de sensibilización programadas.

- **Revisión Periódica del Plan (6.3 - Concientización, educación y capacitación en seguridad de la información):** Se realizará una revisión periódica (al menos anual) del plan de capacitación y sensibilización.

- **Roles y Responsabilidades Definidos (5.10 - Responsabilidades):** Se definirán los roles y responsabilidades para el diseño, la comunicación y la ejecución de las actividades de capacitación y sensibilización.

- **Contenidos de Capacitación (6.3 - Concientización, educación y capacitación en seguridad de la información):** Los contenidos de capacitación y sensibilización deben incluir políticas relevantes como la de escritorio y pantalla limpios, medios removibles, control de acceso y carpetas compartidas.

5. ESTRATEGIAS PARA LA IMPLEMENTACIÓN DE LA POLÍTICA:

Se definen las siguientes estrategias:

- **5.1.1 Sesiones de Sensibilización:** Sesiones periódicas para socializar las políticas institucionales, normas y buenas prácticas, especialmente en los procesos de inducción y reinducción. (Liderado por el Representante de la Alta Dirección y el Director(a) de TIC, apoyado por el Oficial de Seguridad de la Información y la Dirección de Talento Humano).

- **5.1.2 Campañas de Seguridad y Privacidad de la Información:** Campañas mediante medios electrónicos y audiovisuales, con piezas informativas (ej. "ASEGÚRATE") enviadas por correo electrónico (seginfosdp@sdp.gov.co), intranet y otros medios. (Liderado por el Representante de la Alta Dirección y el Director(a) de TIC, apoyado por el Oficial de Seguridad de la Información y la Oficina Asesora de Comunicaciones).

- **5.1.3 Píldoras de Seguridad y Privacidad de la Información:** Piezas informativas concisas dirigidas a directivos sobre temas de interés gerencial, enviadas por correo electrónico (seginfosdp@sdp.gov.co), *chat* y otros medios. (Liderado por el Representante de la Alta Dirección y el Director(a) de TIC, apoyado por el Oficial de Seguridad de la Información y la Oficina Asesora de Comunicaciones).

- **5.1.4 Encuesta en Seguridad y Privacidad de la Información (9.1 - Seguimiento, medición, análisis y evaluación):** Encuestas para medir el grado de apropiación del conocimiento y la satisfacción sobre los temas de seguridad y privacidad, siguiendo la metodología de la GUÍA PARA MEDIR LA SATISFACCIÓN DE LOS GRUPOS DE VALOR Y DE LOS GRUPOS DE INTERÉS O PARTES INTERESADAS DE LA SDP (DEI-GA-001). (Actividad liderada por el Representante de la Alta Dirección y el Director(a) de TIC, apoyado por el Oficial de Seguridad de la Información y el Líder de Sistemas de Información y Aplicaciones).

- **5.1.5 Socialización de Políticas, Guías e Instrumentos del SGSI:** Socialización de los documentos del SGSI mediante su

publicación en el Sistema de Gestión de Calidad y la creación de piezas de conocimiento enviadas por correo electrónico (seginfosdp@sdp.gov.co), intranet y otros medios. (Actividad liderada por el Director(a) de TIC, apoyado por el Oficial de Seguridad de la Información, la Oficina Asesora de Comunicaciones y los Enlaces SG-MIPG).

- **5.1.6 Boletines con Temas de Actualidad:** Boletines digitales con información actual sobre seguridad de la información, enviadas por correo electrónico (seginfosdp@sdp.gov.co), intranet y otros medios. (Liderado por el Director(a) de TIC, apoyado por el Oficial de Seguridad de la Información y la Oficina Asesora de Comunicaciones).

6. PLAN DE ACCIÓN ANUAL:

Durante el primer bimestre del año, se elaborará un plan de acción que permita el cumplimiento de los objetivos y el seguimiento a la implementación de la política de capacitación y sensibilización en temas de seguridad de la información de la SDP. Este plan deberá incluir:

- **Cronograma de Actividades:** Detallar las fechas, la duración y los responsables de cada actividad de capacitación y sensibilización.
- **Recursos Asignados:** Especificar los recursos financieros, humanos y técnicos necesarios para la ejecución del plan.
- **Indicadores de Seguimiento (9.1 - Seguimiento, medición, análisis y evaluación):** Definir indicadores medibles para evaluar la efectividad de las actividades de capacitación y sensibilización, como el número de participantes, los resultados de las encuestas de satisfacción y las evaluaciones de conocimiento.
- **Mecanismos de Evaluación (9.1 - Seguimiento, medición, análisis y evaluación):** Establecer cómo se evaluará el impacto de la capacitación y sensibilización en el comportamiento de los usuarios y en la reducción de incidentes de seguridad.
- **Revisión y Actualización (10.2 - No conformidad y acción correctiva):** El plan de acción se revisará y actualizará periódicamente, al menos una vez al año, o cuando sea necesario, para asegurar su pertinencia y eficacia. Se tomarán acciones correctivas en caso de desviaciones o incumplimientos.

7. ROLES Y RESPONSABILIDADES (5.10 - Responsabilidades):

- **Oficial de Seguridad de la Información:** Es responsable de la elaboración, implementación, seguimiento y evaluación del plan de capacitación y sensibilización.
- **Líder de la Política de Gobierno Digital/Director(a) de TIC:** Es responsable de coordinar las actividades de capacitación y sensibilización con las diferentes áreas de la SDP y de asegurar la asignación de recursos.
- **Dirección de Talento Humano:** Es responsable de gestionar la logística de las capacitaciones, incluyendo la convocatoria, la gestión de espacios y la certificación de la participación.
- **Oficina Asesora de Comunicaciones:** Es responsable de apoyar la difusión de las actividades de sensibilización a través de los diferentes canales de comunicación de la SDP.
- **Directivos y Líderes de Procesos:** Son responsables de promover la participación de su personal en las actividades de capacitación y sensibilización y de reforzar los mensajes clave en sus equipos de trabajo.
- **Todos los Servidores Públicos, Contratistas y Pasantes:** Son responsables de participar activamente en las actividades de capacitación y sensibilización y de aplicar los conocimientos adquiridos en su trabajo diario.

8. MEJORACONTINUA(10.1 - Mejora):

La SDP se compromete a la mejora continua de la Política de Capacitación y Sensibilización en Seguridad de la Información. Se realizarán revisiones periódicas de la política y del plan de acción, y se tomarán en cuenta las lecciones aprendidas y las mejores prácticas para fortalecer las actividades de capacitación y sensibilización.

9. VIGENCIA:

Esta política entra en vigencia a partir de su publicación y deroga cualquier otra disposición que le sea contraria.

6.26.POLITICA SOBRE CAPACITACIONES EN SEGURIDAD

La SECRETARÍA DISTRITAL DE PLANEACIÓN, a través de sus áreas/procesos de Talento Humano y Contratos, incluirá dentro de sus capacitaciones e inducciones las temáticas de seguridad de la información, con el objetivo de que cualquier funcionario y/o contratista que se vincule a la entidad tenga pleno conocimiento de las políticas de seguridad de seguridad de la información, el grupo TIC y/o el Oficial de Seguridad de la Información apoyará en dichas inducciones.

7. OTROS LINEAMIENTOS:

1. Gestión de Incidentes de Seguridad de la Información (5.24 a 5.28 - Gestión de incidentes de seguridad de la información):

- **Reporte de Incidentes (5.24 - Notificación de eventos de seguridad de la información):** La Dirección de Tecnologías de la Información y las Comunicaciones (TIC) es responsable de establecer y mantener un proceso para que los empleados, contratistas y otras partes interesadas reporten cualquier incidente de seguridad de la información de manera oportuna, utilizando canales de comunicación claros y accesibles.

- **Investigación y Medidas Correctivas (5.25 - Evaluación de eventos de seguridad de la información, 5.27 - Respuesta a incidentes de seguridad de la información):** La Dirección de TIC es responsable de liderar las investigaciones de todos los incidentes reportados para determinar la causa raíz, el impacto y tomar las medidas correctivas y preventivas necesarias para evitar su recurrencia.

- **Aprendizaje de los Incidentes (5.28 - Aprendizaje de la seguridad de la información):** Se analizarán los incidentes para identificar las lecciones aprendidas y mejorar continuamente los controles de seguridad, documentando las lecciones aprendidas y difundiendo la información relevante dentro de la organización.

2. Gestión de Recursos Humanos (6.13 - Detección de antecedentes, 6.2 - Términos y condiciones de empleo, 6.4 - Proceso disciplinario):

- **División de Responsabilidades (8.3 - Restricción de acceso a la información):** Se separarán las responsabilidades clave dentro de los procesos de negocio para reducir el riesgo de fraude, errores y conflictos de interés, aplicando el principio de segregación de funciones.

- **Rotación de Tareas (6.2 - Términos y condiciones de empleo):** Se implementará un programa de rotación de tareas, cuando sea aplicable y viable, para reducir la dependencia de un solo individuo en funciones críticas y para detectar posibles actividades fraudulentas.

- **Gestión de Terminación/Cambio de Rol (6.5 - Terminación o cambio de empleo):** Se establecerá un procedimiento formal para la gestión de la terminación de la relación laboral o el cambio de rol de un empleado, incluyendo la revocación de accesos, la recuperación de activos de la empresa (equipos, tarjetas de acceso, credenciales, etc.), y la firma de acuerdos de confidencialidad post-empleo, cuando sea necesario.

3. Gestión de Contratistas y Proveedores (5.22 - Gestión de la seguridad de la información en la cadena de suministro):

- **Evaluación de Riesgos (5.22 - Gestión de la seguridad de la información en la cadena de suministro):** Se evaluarán los riesgos de seguridad de la información asociados con los contratistas y proveedores antes de otorgarles acceso a la información o a los sistemas de la organización, considerando la criticidad de la información a la que accederán.

- **Acuerdos de Nivel de Servicio (SLA) (5.22 - Gestión de la seguridad de la información en la cadena de suministro):** Se establecerán Acuerdos de Nivel de Servicio (SLA) que especifiquen los requisitos de seguridad de la información que deben cumplir los contratistas y proveedores, incluyendo confidencialidad, integridad y disponibilidad de la información. Estos acuerdos se revisarán y actualizarán periódicamente.

4. Gestión de Dispositivos Personales (8.1 - Dispositivos de punto final de usuario):

- **Política de BYOD (Bring Your Own Device) (8.1 - Dispositivos de punto final de usuario):** Se implementará una política clara y concisa para el uso de dispositivos personales (BYOD) que accedan a información o a los sistemas de la

organización, estableciendo los requisitos mínimos de seguridad que deben cumplir los dispositivos, las responsabilidades de los usuarios y las medidas de seguridad que se aplicarán.

5. Cultura de Seguridad y Mejora Continua (5.1 - Liderazgo y compromiso, 6.3 - Concientización, educación y capacitación en seguridad de la información, 10.1 - Mejora):

- **Cultura de Seguridad (6.3 - Concientización, educación y capacitación en seguridad de la información):** Se fomentará una cultura de seguridad de la información en la que todos los empleados se sientan responsables de proteger la información de la organización, a través de programas de concientización, capacitación y comunicación continua.

- **Evaluación y Mejora Continua (10.1 - Mejora):** Se realizarán evaluaciones periódicas de las políticas de seguridad de los recursos humanos y de la eficacia de los controles implementados, realizando los ajustes necesarios para garantizar su continua adecuación y eficacia. La política se revisará formalmente al menos una vez al año, o con mayor frecuencia si es necesario, para reflejar los cambios en el entorno de la organización, las amenazas y las mejores prácticas.

6. Auditoría de Cumplimiento (9.2 - Auditoría interna):

Para garantizar el cumplimiento de esta política y de los controles implementados, la Oficina de Control Interno incluirá la revisión de estos aspectos en las auditorías de seguimiento al Modelo de Seguridad y Privacidad de la Información.

8. APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS

Las políticas aquí definidas se harán efectivas a partir de su aprobación por la Alta Dirección y serán revisadas por lo menos anualmente, cuando existan incidentes de seguridad de la información o cuando se produzcan cambios estructurales considerables, esto con el fin de asegurar su vigencia y aplicabilidad dentro de **SECRETARÍA DISTRITAL DE PLANEACIÓN.**

9. SANCIONES

La falta de conocimiento de los presentes lineamientos no libera al personal de **SECRETARÍA DISTRITAL DE PLANEACIÓN** de las responsabilidades establecidas en ellos por el mal uso que hagan de los recursos de TIC o por el incumplimiento de los lineamientos aquí descritos.

a. Se aplicarán sanciones de acuerdo con el Código Único Disciplinario.
b. Pueden aplicarse sanciones de tipo penal según sea el caso y la gravedad de este, si así lo consideran los entes investigativos y judiciales correspondientes.
c. La Dirección de Tecnologías de la Información y las comunicaciones será la encargada de recopilar y entregar a la Oficina de Control Disciplinario las evidencias de incumplimiento de los lineamientos, informes de impactos y consecuencias y cualquier otro insumo requerido para formalmente manejar la investigación inicialmente a nivel interno, así mismo, el grupo TIC será el encargado de registrar y gestionar el Incidente de seguridad derivado con el incumplimiento de las políticas.

---

[1] Norma NTC-IEC-ISO 27001:2022 en la cual se establece 4 categorías de controles de seguridad de la información y 93 controles.

[2] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. (Norma NTC-ICO/IEC 27002:2022).

[3] creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción

[4] Ley Estatutaria 1581 de 2012, artículo 14°. Consultas.

[5] Ley Estatutaria 1581 de 2012, artículo 15°. Reclamos.

[6] Ley Estatutaria 1581 de 2012, artículo 16°. Recurso de Procedibilidad

VERSIÓN	FECHA	CONTROL DE CAMBIOS

ELABORÓ	REVISÓ	APROBÓ
Nombre: Marisol Rubiano Casas **Cargo:** Profesional Universitario **Fecha:** 31/Dic/2024	**Nombre:** Gabriel Andres Solorza Sanabria **Cargo:** Profesional Especializado **Fecha:** 31/Dic/2024	**Nombre:** Lina Maria Cruz Silva **Cargo:** Director Tecnico **Fecha:** 31/Dic/2024

TXT_PataDocumento