POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Este documento describe las políticas de seguridad de la información definidas por la Secretaría Distrital de Ambiente. Para la elaboración del mismo, se toman como base las leyes y demás regulaciones aplicables, la norma ISO 27001:2013, las recomendaciones del estándar ISO 27002:2013 y la NTD-SIG 001:2011, así como las determinaciones y guías dadas por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC).

Cubre todos los aspectos administrativos y de control que deben ser cumplidos por los funcionarios y contratistas de la Secretaría Distrital de Ambiente, para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada.

POLITICA GENERAL

Consciente de las necesidades derivadas de sus actividades, la Secretaría Distrital de Ambiente adopta el Subsistema de Gestión de Seguridad de la Información como una herramienta para garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información, administrando los riesgos, cumpliendo con la legislación vigente, y generando una cultura de seguridad de la información en los servidores públicos y demás partes interesadas.

OBJETIVO GENERAL

Mantener la confidencialidad, integridad, disponibilidad de los activos de información, y la protección de datos personales**,** mediante la gestión los riesgos, que permita establecer un marco de confianza a las partes interesadas en concordancia con la misión y visión de la entidad.

OBJETIVOS ESPECÍFICOS:

1. Proteger los activos de información, con base en los criterios de confidencialidad, integridad, disponibilidad, mediante la implementación de controles en los procesos de la entidad de manera coordinada con las partes interesadas.

2. Gestionar los riesgos asociados con la pérdida de confidencialidad, integridad, disponibilidad y privacidad de la información dentro del alcance del Subsistema de Gestión de Seguridad de la Información (SGSI).

3. Garantizar el tratamiento de los datos personales obtenidos en la entidad a los titulares de la información, en el ejercicio pleno de sus derechos.

4. Sensibilizar y entrenar al personal de la entidad en el Subsistema de Gestión de Seguridad de la Información (SGSI).

POLÍTICAS ESPECÍFICAS:

1. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La Secretaría Distrital de Ambiente establece como máxima autoridad del Subsistema de Gestión de Seguridad de la Información al Comité del Sistema Integrado de Gestión quien es responsable de la orientación estratégica para la administración de los activos de información, la sostenibilidad y mejora del Subsistema en la Entidad.

2. GESTIÓN DE ACTIVOS DE INFORMACIÓN

La Secretaría Distrital de Ambiente establece métodos de protección para la propiedad legal del contenido de cualquier documento (físico, electrónico y digital) que se genere, obtenga, adquiera, transforme o controle durante el desarrollo de sus funciones. La entidad se compromete de la mano con los procesos responsables, a identificar y proteger los activos de información, con el fin de garantizar su administración y control.

Los activos de información deberán ser identificados y/o actualizados cada vez que sea requerido por el líder de proceso asociado, y será asistido por el enlace SIG. Quienes deberán determinar la clasificación de los activos de información de acuerdo a la criticidad, sensibilidad y reserva de la misma, teniendo en cuenta la Ley 1581 de 2012, Decreto 1377 de 2013, Ley 1712 de 2014, Decreto 103 de 2015, entre otras que puedan aplicar de acuerdo a la naturaleza de la entidad. La identificación y/o actualización deberá registrarse en el formato establecido por el Sistema Integrado de Gestión.

2.1. Etiquetado de la Información:

Los documentos clasificados serán manejados, preparados, copiados y entregados sólo al personal autorizado. Se establecerán acuerdos periódicos para revisiones de seguridad en la producción y copiado.

En cada área se destinará un espacio físico adecuado para archivar los documentos de manera clasificada según la codificación definida por la Secretaria Distrital de Ambiente.

La utilización de equipos de reproducción tales como fotocopiadoras, impresoras, escáneres para documentos con clasificación RESERVADA o CONFIDENCIAL será debidamente autorizada por el supervisor o jefe del funcionario o contratista.

Se tratará como material clasificado los siguientes medios: discos, cintas, bocetos preliminares, notas o bocetos de trabajo, fotografías, plantillas y planos.

2.2. Devolución de los Activos

Todo funcionario o contratista que se desvincule de la Secretaría Distrital de Ambiente, deberá realizar la devolución de activos de información que tenga asignada y en custodia, en el formato de Paz y Salvo para funcionario y para contratista, de acuerdo con los procedimientos establecidos para tal fin.

2.3. Gestión De Medios Removibles

Para un adecuado uso y permiso de los medios removibles de la Secretaría Distrital de Ambiente se tendrán en cuenta los siguientes lineamientos de cumplimiento obligatorio.

Todos los medios removibles administrados por el data center que contengan información sensible o confidencial serán almacenados en un ambiente seguro y vigilado según las especificaciones del fabricante.

En los medios removibles que sean reutilizados por funcionarios o contratista se deberá realizar un borrado seguro de la información encontrada en dicho medio, antes de realizar alguna reasignación.

Se verificará los medios removibles que ya no se utilizaran, y que se dispongan para eliminar, retirar o trasladar de las instalaciones de la entidad. La información contenida en los medios removibles sera borrada con un procedimiento seguro y documentado. Para el retiro de dichos medios se debe contar con la autorización de la Dirección de Planeación y Sistemas de Información Ambiental, además se hace exclusión para medios removibles completamente en desuso.

La información crítica o sensible de la entidad que se encuentra almacenada en un medio removible cuya vida útil es menor al tiempo de retención de la información establecida por la entidad, deberá respaldarse en otro medio para evitar la pérdida de información.

Cuando se requiera transferir información de archivo de gestión al archivo central deberá almacenarse en el medio disponible para este fin y cuando se requiera pasar la información a archivo histórico se deberá disponer de los medios de transferencia documental para la información clasificada para este fin.

Es de exclusiva responsabilidad de cada funcionario tomar las medidas adecuadas para el almacenamiento y resguardo de los medios removibles, evitando accesos no autorizados, daños, pérdida de información o extravío del medio

En caso de ocurrir pérdida, modificación o daño de la información o del medio, se debe informar al responsable de seguridad de la información o quien haga sus veces.

2.4. Disposición De Los Activos:

La Secretaría Distrital de Ambiente establece que la destrucción del material clasificado se debe mantener hasta que sea completamente destruido y verificado. Siempre debe dejarse registro de la destrucción de material RESERVADO Y CONFIDENCIAL.

Los registros de destrucción deberían incluir: la fecha, la firma de la persona que realiza la destrucción y la autorización del procedimiento por parte del jefe inmediato. Para el caso de material RESERVADO Y CONFIDENCIAL, la firma de jefe de control interno será requisito para el procedimiento. Estos registros deberán retenerse de acuerdo a lo estipulado en las tablas de retención documental de la entidad. La destrucción de material clasificado debe realizarse bajo la estricta supervisión del Oficial de Seguridad de la Información o quien haga sus veces.

2.5. Dispositivos Móviles:

Los dispositivos móviles deben estar integrados a una plataforma de administración controlada por la Secretaría Distrital de Ambiente

Los dispositivos móviles deben tener contraseña de ingreso y bloqueo del equipo.

Los usuarios deben tener instaladas únicamente las aplicaciones distribuidas y autorizadas por el administrador de la plataforma y tener configurado únicamente la cuenta de correo electrónico de la entidad.

Es responsabilidad del usuario hacer buen uso del dispositivo suministrado por la SDA con el fin de realizar actividades propias de su cargo o funciones asignadas en la entidad.

Se debe activar la opción de cifrado de la memoria de almacenamiento de los dispositivos móviles institucionales haciendo imposible la copia o extracción de datos si no se conoce el método de desbloqueo.

La Secretaría Distrital de Ambiente debe contar con una solución de copias de seguridad para la información contenida en los dispositivos móviles institucionales; dichas copias deben acogerse a la Política de Copias de Respaldo de la Información.

La dependencia de la SDA quien efectúe la administración del sistema de información que involucre dispositivos móviles, debe proveer la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica, de forma remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.

En caso de requerir instalación de aplicaciones adicionales en el dispositivo móvil se debe solicitar al comité de seguridad informática para su aprobación.
Ante la pérdida del equipo, ya sea por sustracción o extravío, deberá dar cuenta en forma inmediata a la Dirección de Gestión Corporativa como dependencia que administra el Almacén de la Secretaría Distrital de Ambiente.

La Dirección de Gestión Corporativa debe instalar un software de antivirus para los dispositivos móviles institucionales.

Cada vez que los sistemas de los dispositivos móviles institucionales notifiquen una actualización disponible, los usuarios deben aceptar y aplicar la nueva versión.

Los usuarios deben evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.

3. CONTROL DE ACCESO

La Secretaría Distrital de Ambiente gestiona el control de acceso de los funcionarios, contratistas y terceros a las redes, aplicaciones, información física, sistemas de información, e instalaciones de procesamiento de información.

Es responsabilidad de la Dirección de Planeación y Sistemas de información Ambiental y la Dirección de Gestión Corporativa:

- Gestionar el control de acceso a los sistemas y servicios por medio de equipos de seguridad perimetral, Administración de aplicativos, sistemas de información, bases de datos, portal cautivo y controladores de dominio a servidores públicos y terceros
- Mantener los registros donde cada uno de los líderes responsables de los procesos que haya autorizado a los servidores públicos o terceros, el acceso a los diferentes sistemas de información de la entidad.

- Establecer y verificar que los datos de acceso a los sistemas están compuestos por un nombre de usuario, una contraseña y que sean únicos para cada servidor público o tercero.
- En caso de retiro, terminación, jubilación, suspensión, cesión o cambio de cualquier servidor público o tercero, se deberá deshabilitar o actualizar los privilegios en los sistemas a los que el usuario estaba autorizado.
- Asignar las contraseñas de acceso que deberán cumplir con un mínimo de 8 caracteres y la combinación de números, letras mayúsculas y minúsculas, en lo posible utilizar caracteres especiales.

Es responsabilidad de los usuarios de la secretaría de ambiente:

- Las contraseñas serán de uso personal e intransferible y no se deben escribir en medios físicos (documentos, notas o archivos)
- No se debe habilitar la opción – “recordar clave en este equipo”, que ofrecen los programas
- Cambia tu contraseña si piensas que alguien más la conoce y si ha tratado de dar mal uso de ella
- Selecciona contraseñas que no sean fáciles de descifrar
- No utilizar la opción de almacenar contraseñas en Internet.
- No utilizar contraseña con números telefónicos, nombre de familia etc.

La Secretaría Distrital de Ambiente se compromete a regular el acceso a la información bajo su control o custodia de acuerdo a su clasificación a través de disposiciones relacionadas con perfiles de usuario (y los ítems de seguridad que ello implique), delimitando y otorgando autorización para el acceso a la información de acuerdo a la labor propia de cada servidor público, así como la demarcación de perímetros de seguridad para zonas con infraestructura crítica de información, a estas áreas ingresarán únicamente personal autorizado y se tendrá e implementará los debidos controles para su uso y operación.

4. USO ADECUADO DE INTERNET

4.1. Dirección de Planeación y Sistemas de Información Ambiental

La Dirección de Planeación y Sistemas de Información Ambiental debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.

La Dirección de Planeación y Sistemas de Información Ambiental debe monitorear continuamente el canal o canales del servicio de Internet.

La Dirección de Planeación y Sistemas de Información Ambiental debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos y de alta peligrosidad.

La Dirección de Planeación y Sistemas de Información Ambiental debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de Internet.

4.2. Todos los Usuarios

Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores diarias.

No se permite el acceso a páginas relacionadas con pornografía, drogas, alcohol, violencia, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.

No se permite la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica de la entidad.

No se permite el intercambio no autorizado de información de propiedad de la Secretaría Distrital de Ambiente, de sus clientes y/o de sus funcionarios, con terceros.

5. NO REPUDIO

La Secretaria Distrital de Ambiente debe producir, validar, mantener, y poner a disposición de la entidad, pruebas o evidencias irrefutables respecto a la transferencia de información en cada uno

de sus procesos a nivel interno y externo, buscando información suficiente sobre la ocurrencia de un evento, el momento en el que ocurrió y las partes que intervinieron.

La Secretaria Distrital de Ambiente debe hacer uso de mecanismos criptográficos: firmas digitales, cifrado de mensajes, códigos de autenticación de mensajes, etc.

La Secretaria Distrital de Ambiente establecerá el procedimiento de ***No-repudio de Origen*** proporcionando al receptor de un objeto digital una prueba infalsificable del origen de dicho objeto, lo cual evitará que el emisor niegue el envío de la información o tenga éxito ante el juicio de terceros.

La Secretaria Distrital de Ambiente establecerá el procedimiento de ***No-repudio de Recepción*** proporcionando al emisor la prueba de que el destinatario legítimo de un mensaje u objeto digital genérico, realmente lo recibió, evitando que el receptor lo niegue posteriormente y consiga sus pretensiones.

Derivado de la ejecución de los dos procedimientos anteriores, la Secretaría Distrital de Ambiente deberá documentar las ***Evidencia de No-repudio,*** por medio de registros compuesto por cuatro fases distintas. En primer lugar, la fase de generación de la evidencia; en segundo lugar, la fase de transferencia; en tercer lugar, la fase de verificación y almacenamiento de la evidencia, que consiste en comprobar la firma digital y guardar la información para un uso posterior; y, por último, la fase de resolución de disputas, en caso de que éstas tengan lugar.

6. PRIVACIDAD Y CONFIDENCIALIDAD

La Secretaría Distrital de Ambiente establece controles, instalando las medidas técnicas y organizativas necesarias para evitar la pérdida, mal uso, alteración, acceso no autorizado y robo de los datos facilitados por los usuarios, en cumplimiento de la Ley Estatutaria 1581 de 2012, Decreto 1377 de 2013 y demás normativa vigente en el tema. La Entidad, bajo ninguna circunstancia utilizará la información recopilada para otra acción diferente a su misionalidad y al objeto de recolección, previa autorización informada del titular de los datos a excepción de los terceros autorizados por el titular o por la ley.
Entiéndase como datos personales los siguientes tipos de datos:

De Identificación: Nombre, apellido, tipo de identificación, número de identificación, fecha y lugar de expedición, nombre, estado civil, sexo, firma, nacionalidad, datos de familia, firma electrónica, otros documentos de identificación, lugar y fecha de nacimiento o muerte, edad, huella, ADN, iris, Geometría facial o corporal, fotografías, vídeos, fórmula dactiloscópica, voz, etc.

De Ubicación: como los relacionados con la actividad comercial o privada de las personas como dirección, teléfono, correo electrónico, etc.

De contenido socioeconómico: como estrato, propiedad de la vivienda, Datos financieros, crediticios y/o de carácter económico de las personas, Datos patrimoniales como bienes muebles e inmuebles, ingresos, egresos, inversiones, historia laboral, experiencia laboral, cargo, fechas de ingreso y retiro, anotaciones, llamados de atención, nivel educativo, capacitación y/o historial académico de la persona, etc.

Sensibles: como los relacionados con la salud de la persona en cuanto a órdenes y relación de pruebas complementarias como laboratorio, imágenes diagnósticas, endoscópicas, patológicas, estudios, etc. diagnósticos médicos, generales o especializados, psicológicos o psiquiátricos, medicamentos y/o tratamientos médicos o terapéuticos de cualquier tipo, los relacionados con la pertenencia a sindicatos, organizaciones sociales, de derechos humanos, religiosas, políticas; datos relacionados con las convicciones religiosas, filosóficas y/o políticas, los datos de preferencia, identidad y orientación sexual de la persona, origen étnico-racial, personas de la tercera edad o menores de 18 años en condición de pobreza, datos sobre personas en situación de discapacidad personas con limitaciones psicomotoras, auditivas y visuales en condiciones de pobreza, personas víctimas de la violencia, personas en situación de desplazamiento forzado por violencia, madres gestantes o lactantes o cabeza de familia en situación de vulnerabilidad, menores en condición de abandono o protección, etc.

6.1 Responsabilidades de los funcionarios y contratistas de la Entidad

Es responsabilidad de funcionarios y contratistas garantizar la protección de los datos personales que se obtengan del ejercicio misional de los usuarios y ciudadanía en general, tal y como lo establece la circular SDA no. 1 de 2013.

6.2. Manejo de datos personales para ingreso a la Entidad

La Secretaría Distrital de Ambiente, como responsable del tratamiento de los datos personales de las personas naturales que ingresan a la entidad, solicitará la autorización al usuario para el tratamiento, recolección, almacenamiento, gestión y eliminación de sus datos personales.

Los datos personales que se entregan por parte de las personas al ingreso de la SDA, tales como huella digital e imágenes (datos sensibles), nombre y número de cédula, sólo serán usados para efectos de control de acceso de visitantes a las instalaciones y por ende no serán transferidos ni comercializados con terceros. Solo se solicitarán datos personales estrictamente necesarios para los fines mencionados y tales datos serán obtenidos bajo los principios de finalidad, calidad, circulación restringida en la ley 1581 de 2012.

6.3. Derechos de los Titulares de los Datos Personales

Los titulares de la información cuyos datos personales sean objeto de tratamiento por parte de Secretaría Distrital de Ambiente podrán conocer en cualquier momento los datos personales sobre los cuales la SDA está realizando el tratamiento. De igual manera, el titular puede solicitar en cualquier momento, que sus datos sean actualizados o rectificados.

El titular de la información debe ser informado por la SDA, previa solicitud, respecto del uso que ésta le ha dado a sus datos personales.

El titular de la información podrá solicitar a la Secretaría Distrital de Ambiente la eliminación de sus datos personales o revocar la autorización otorgada para el tratamiento de los mismos, mediante la presentación de una solicitud. No obstante, la supresión de la información y la revocatoria de la autorización no procederán cuando el Titular de la información tenga un deber legal o contractual de permanecer en la Base de Datos y/o Archivos, ni mientras se encuentre vigente la relación entre el Titular y la Secretaría Distrital de Ambiente, en virtud de la cual fueron recolectados sus datos.

El titular de la información podrá acceder de forma gratuita a sus datos personales objeto de Tratamiento por parte de la Secretaría Distrital de Ambiente.

Así mismo la entidad no cederá a terceros los datos personales de los usuarios que se obtengan a través de cualquier mecanismo sin su consentimiento expreso. Sin perjuicio de lo anterior, el usuario consiente en que se cedan sus datos personales cuando así sea requerido por las autoridades administrativas competentes o por mandato judicial.

6.4. Formato de autorización para el tratamiento de datos personales.

Para efectos del tratamiento de los datos personales recolectados, la SDA, como responsable de los datos personales obtenidos a través de sus distintos canales de atención, solicitará a todas las personas su autorización para que, de manera libre, previa, expresa y voluntaria permitan continuar con su tratamiento. Para lo cual deberá utilizarse el siguiente formato tanto en los canales presenciales como en los canales tecnológicos:

Autorización de tratamiento de datos personales

Declaro de manera libre, expresa, inequívoca e informada, que AUTORIZO a la SECRETARIA DISTRITAL DE AMBIENTE para que, en los términos del literal a) del artículo 6 de la Ley 1581 de 2012, realice la recolección, almacenamiento, uso, circulación, supresión, y en general, tratamiento de mis datos personales, incluyendo datos sensibles, como mis huellas digitales, fotografías, videos y demás datos que puedan llegar a ser considerados como sensibles de

conformidad con la Ley, para que dicho Tratamiento se realice con el fin de lograr las finalidades relativas a ejecutar el control, seguimiento, monitoreo, y, en general todos los trámites y servicios; así como para garantizar la seguridad de sus instalaciones.

Declaro que se me ha informado de manera clara y comprensible que tengo derecho a conocer, actualizar y rectificar los datos personales proporcionados, a solicitar prueba de esta autorización, a solicitar información sobre el uso que se le ha dado a mis datos personales, y denunciar por el uso indebido de mis datos personales, a revocar esta autorización o solicitar la supresión de los datos personales suministrados y a acceder de forma gratuita a los mismos.
Declaro que la información por mí proporcionada es veraz, completa, exacta, actualizada y verificable. Mediante la aceptación del presente documento, manifiesto que reconozco y acepto que cualquier consulta o reclamación relacionada con el tratamiento de mis datos personales podrá ser elevada verbalmente o por escrito ante la SDA, como Responsable del Tratamiento, cuyo portal web es: www.ambientebogota.gov.co, teléfono de atención: +57 (1) 3778879, Sede Principal ubicada en la Av Caracas No 54 - 38.

NOMBRE: *
EMPRESA: *
DIRECCIÓN: *
CORREO ELECTRÓNICO: *
¿AUTORIZA EL TRATAMIENTO DE SUS DATOS PERSONALES SENSIBLES? *

7. CRIPTOGRAFÍA Y GESTIÓN DE LLAVES

Con el fin de conservar la confidencialidad, integridad, privacidad, autenticidad y no repudio de la información, la Secretaría Distrital de Ambiente utiliza controles criptográficos en los siguientes casos:

- Uso de aplicativos, enlaces de comunicaciones, y protección de dispositivos portables.
- Protección de claves de acceso a sistemas, datos y servicios.
- Transmisión de información clasificada, fuera del ámbito de la entidad

La gestión de claves criptográficas se realiza a través del Directorio Activo durante todo su ciclo de vida.

Las claves criptográficas que por alguna razón se vuelven no seguras o aquellas que ya no son usadas por algún usuario o grupo deben ser eliminadas del sistema para evitar comprometer la información.

8. SEGURIDAD FÍSICA Y AMBIENTAL

La Secretaría Distrital de Ambiente se compromete a proteger las áreas destinadas al procesamiento o almacenamiento de información sensible y aquellas donde se encuentra la infraestructura de servidores que dan soporte a los sistemas de información y comunicaciones, considerándolas áreas de acceso restringido a través de medidas de control de acceso físico, así como estableciendo métodos de protección para la infraestructura tecnológica al servicio de la Entidad, con el fin de prevenir su pérdida o daño por situaciones internas, externas, ambientales, de seguridad perimetral o de uso.

Con relación a las instalaciones de la Entidad, la Secretaría Distrital de Ambiente se compromete a gestionar constantemente sistemas de vigilancia y seguridad perimetral, así como planes de mantenimiento para la salvaguarda de un ambiente seguro e idóneo para las actividades desarrolladas en cada una de sus sedes.

9. TELETRABAJO

La Secretaria Distrital de Ambiente implementará los controles adecuados para proteger la confidencialidad, integridad, disponibilidad y privacidad de los activos de información en un ambiente de teletrabajo, asignando permisos, generando autenticaciones y conexiones seguras de acuerdo a la sensibilidad de la información por acceder, verificando los aspectos de seguridad física, del entorno y el suministro de elementos tecnológicos.

10. ESCRITORIO LIMPIO Y PANTALLA LIMPIA

La Secretaría Distrital de Ambiente promoverá la cultura de escritorio y pantalla limpios, donde cada servidor público de la entidad se compromete a mantener protegida la información en sus áreas de trabajo a través de la correcta custodia y disposición de documentos, CD, dispositivo USB y cualquier otro medio de almacenamiento, así como bloqueando la sesión de su estación de trabajo en el momento en que se ausente. De igual forma existe el compromiso de mantener la pantalla de inicio del equipo de cómputo libre de archivos, salvo los accesos directos a las aplicaciones necesarias para su labor.

Al imprimir documentos de carácter confidencial, estos deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.

11.GESTIÓN DE SEGURIDAD EN DATA CENTER Y REDES

11.1.Data Center

La Secretaría Distrital de Ambiente garantiza que el Data Center se encuentre separado de áreas que tengan líquidos inflamables o estén en riesgo de inundaciones e incendios, implementando mecanismos de revisión y control del ingreso de cual-quier tipo de material al Centro de Cómputo, además deben existir sistemas de detección y extinción automáticas de incendios e inundación y alarmas en caso de detectarse condiciones inapropiadas.

Los niveles de temperatura y humedad relativa en el Data Center deben ser mantenidos dentro de los límites requeridos por la infraestructura de cómputo allí instalada, para lo cual se deben usar sistemas de aire acondicionado.

Se debe monitorear y revisar de manera permanente el estado de los componentes de soporte físico, eléctrico y ambiental que hacen parte del Centro de Cómputo, como son el sistema de aire acondicionado y el sistema de detección y extinción de incendios, entre otros.
Cuando se realicen trabajos de mantenimiento correctivo en redes eléctricas, cableados de da-tos y voz, deben ser realizados por personal especializado y debida-mente autorizado e identificado.

Se deben realizar mantenimientos preventivos y pruebas de funciona-lidad del sistema de UPS, plantas eléctricas, y sistema de aire acondicio-nado.

Se deben realizar mantenimientos preventivos y correctivos de los ser-vidores, equipos de comunicaciones y de seguridad que conforman la plataforma tecnológica de la Secretaría Distrital de Ambiente.

11.2. Redes

Las redes deben ser administradas y controladas para proteger la información en los sistemas y aplicaciones. Además, cuentan con dispositivos de seguridad y niveles de servicio apropiados. Se establecerán mecanismos de identificación automática de equipos en la red, como medio de autenticación de conexiones.

La Secretaría Distrital de Ambiente debe contar con segmentos de red físicos y lógi-cos e independientes de los segmentos de red de usuarios, de cone-xiones con redes con terceros y del servicio de acceso a Internet. La división de estos segmentos debe ser realizada por medio de disposi-tivos perimetrales e internos de enrutamiento y de seguridad si así se requiere.

La SDA por medio de la Dirección de Planeación y Sistemas de Información garantiza que los puertos físicos y lógicos de diagnóstico y configu-ración de plataformas que soporten sistemas de información estarán restringidos y monitoreados con el fin de prevenir acce-sos no autorizados.

12. AMBIENTE DE DESARROLLO SEGURO

La SDA debe garantizar un ambiente de desarrollo seguro durante la ejecución de los proyectos, arquitecturas, software o sistemas, estableciendo metodologías que incluya requisitos de seguridad en cada una de las fases del proyecto, acuerdos de soporte y niveles de servicio a terceros, y separación física y virtual en los ambientes de operación, todo a través de técnicas de programación seguras. Así mismo, cada sistema de información deberá contar con sus manuales de uso y técnicos disponibles de acuerdo a los niveles de protección de la información dados para estos datos.

Los propietarios de los sistemas de información son responsables de realizar las pruebas para asegurar que cumplen con los requerimientos de funcionamiento establecidos antes del paso a producción de los sistemas. Estas pruebas deben realizarse por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica.

Los propietarios de los sistemas de información deben aprobar las migraciones entre los ambientes de desarrollo, pruebas y producción de sistemas de información nuevos y/o de cambios o nuevas funcionalidades.

La Secretaría Distrital de Ambiente debe implantar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios. Se debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información.
Los desarrolladores de los sistemas de información de la SDA deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el diseño hasta la puesta en marcha.

Los desarrolladores de la SDA deben construir los aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.

Se deben asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de

datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.

Los aplicativos desarrollados proporcionarán la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.

Se debe garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.

Las funcionalidades y archivos que no sean necesarios para los aplicativos se removerán, previo a la puesta en producción, además se debe prevenir la revelación de la estructura de directorios de los sistemas de información construidos.

Los desarrolladores de la SDA deben desarrollar los controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos sólo tengan privilegios de lectura.

Se debe proteger el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios. Además, no se debe permitir que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

13. SEGURIDAD EN LAS OPERACIONES

La Secretaría Distrital de Ambiente deberá generar acciones de seguridad constantes basadas en la planificación de la operación, controlando los procesos y ejecutando los planes que permitan cumplir con los objetivos propuestos por el Subsistema de Gestión de Seguridad y Privacidad de la Información, con base a la valoración y tratamiento de los riesgos evidenciados para cada uno de los activos de información de la entidad. Toda labor realizada debe contar con la correcta documentación sobre los planes ejecutados y los métodos usados para garantizar la salvaguarda de la información.

14. GESTIÓN DEL CAMBIO

La Secretaría Distrital de Ambiente debe establecer una metodología sobre las labores de control de cambio sobre para el software en producción, comunicaciones y en general cualquier modificación de la infraestructura tecnológica, con el objetivo de no afectar la seguridad de los

activos de información, evaluando los riesgos ante los cambios previstos y verificar su correcta implementación, reduciendo lo máximo posible la afectación en la operatividad de la entidad.

15. TRANSFERENCIA DE INFORMACIÓN

Con el fin de mantener la seguridad de los activos de información de la entidad, la Secretaría Distrital de Ambiente establecerá acuerdos de confidencialidad con los funcionarios, contratistas y partes interesadas que por diferentes razones requieran conocer o intercambiar información clasificada y reservada, de acuerdo a los niveles y perfiles de autorización para acceso, modificación, divulgación y eliminación de la información dada por los propietarios. De igual forma el supervisor del contrato o jefe inmediato debe asegurar que todos los activos sean devueltos y la información pertinente sea transferida, de acuerdo con los procedimientos establecidos para tal fin.

Los terceros con quienes se intercambia información sensible de la Secretaría Distrital de Ambiente deben destruir de manera segura la información suministrada, una vez esta cumpla con la función para la cual fue enviada y demostrar la realización de las actividades de destrucción.

No está permitido el intercambio de información sensible de la Secretaría Distrital de Ambiente por vía telefónica y/o correo electrónico.

La Secretaria Distrital de Ambiente debe garantizar soluciones de intercambio de información seguros, así como adoptar controles de cifrado de información que permitan el cumplimiento del procedimiento para el intercambio de información en cada uno de los medios utilizados.

16. PROVEEDORES

La Secretaría Distrital de Ambiente deberá establecer métodos y requisitos para el control de la información con relación al acceso, procesamiento, almacenamiento, comunicación o suministro componentes de infraestructura de TI para la información de la organización, garantizando el aislamiento de los sistemas de información ante posibles conexiones y accesos inseguros. Durante la ejecución del contrato, todas las actividades realizadas en los sistemas de información por parte de los contratistas, deben ser monitoreadas por el supervisor o el profesional encargado a quien se le presta el servicio. En caso de evidenciar abuso en los accesos se reportará el incidente respectivo conforme al procedimiento de gestión de incidentes.

17. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La Secretaria Distrital de Ambiente comprometida con la mejora continua del **SGSI**, establecerá y ejecutará procedimientos para identificar, analizar, valorar, tratar y aprender de los incidentes de seguridad de la información que se presenten en la Entidad. Todo funcionario público deberá reportar los eventos o incidentes de seguridad que se presenten junto a todos los registros que se posean, realizando la correcta identificación, recolección, adquisición y preservación de los mismos, según el procedimiento de gestión de incidentes vigente.
La Alta Dirección o a quien delegue, serán los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas.

18. GESTIÓN DE VULNERABILIDADES TÉCNICAS

La Secretaría Distrital de Ambiente identificará vulnerabilidades técnicas del conjunto de plataformas tecnológicas, de comunicaciones y de seguridad que soporten los activos de información, con el fin de proponer actividades para gestionarlas, de acuerdo a los controles establecidos.

19. GESTIÓN DE CONTINUIDAD DE NEGOCIO.

La Entidad establecerá una estructura de gestión adecuada para mitigar y responder a una crisis, desastre o incidente, usando personal con la autoridad, experiencia y competencia necesarias, desarrollando y aprobando planes, procedimientos de respuesta, retorno y recuperación, poniéndolos a prueba para asegurar que son coherentes con los objetivos de seguridad en la continuidad de negocio, con el fin de lograr que los procesos críticos tengan instalaciones alternas y sus activos de información cuando se requieran.

20. COPIAS DE RESPALDO DE LA INFORMACIÓN

La información definida y contenida en la plataforma tecnológica de la organización, como servidores, archivo de configuración, dispositivos de red, estaciones de trabajo, entre otros, debe ser periódicamente resguardada mediante mecanismos y controles adecuados que garanticen la confidencialidad, integridad y disponibilidad de la información, realizándolas conforme al procedimiento adoptado por la entidad; Las áreas encargadas de la información en conjunto con la Dirección de Planeación y Sistemas de Información Ambiental deberán definir la estrategia a seguir para el respaldo y almacenamiento de la información, validando las copias a intervalos regulares.

La Secretaria Distrital de Ambiente velará porque los medios magnéticos que contienen la información crítica sea almacenada en una ubicación diferente a las instalaciones donde se

encuentra dispuesta. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados.

21. CUMPLIMIENTO

La Secretaria Distrital de Ambiente sancionará cualquier violación a esta política o procedimiento establecido en el Sub Sistema de Gestión de la Seguridad y Privacidad de la información SGSPI, de acuerdo a lo establecido en la ley de delitos informáticos 1273 del 2009 y demás aplicables.

La Secretaria Distrital de Ambiente velará por el cumplimiento de la legislación relacionada con la seguridad de la información, entre ella la referente a derechos de autor y propiedad intelectual.

Todo funcionario en la SDA es responsable de registrar y reportar las violaciones a la seguridad, confirmadas o sospechadas, además será responsable de preservar la confidencialidad, integridad y disponibilidad de los activos de información en cumplimiento de la presente política.

22. RECURSOS HUMANOS Y CAPACITACIÓN

La Secretaría Distrital de Ambiente garantizará procesos de selección de personal de acuerdo a los lineamientos dados por la norma vigente, realizando las verificaciones necesarias para confirmar la veracidad de la información suministrada por el funcionario o contratista candidato a contratar.

La Dirección de Gestión Corporativa debe certificar que los contratos de trabajo de los funcionarios, proveedores y contratistas que desarrollen dentro de sus actividades el manejo de información sensible de la entidad cuenten con cláusulas respecto a la propiedad intelectual, cláusulas de confidencialidad y manejo de seguridad de información perteneciente a la SDA. Además, se debe anexar un documento de aceptación de las Políticas de Seguridad y Privacidad de la información de la Secretaría Distrital de Ambiente.

El personal provisto por terceras partes que realicen labores en o para la Secretaría Distrital de Ambiente, deben firmar un Acuerdo o Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad de la Información, antes de que se les otorgue acceso a las instalaciones y a la plataforma tecnológica.

De igual forma, la entidad propenderá por la generación de la cultura de los funcionarios y contratistas de la SDA con relación a la seguridad de la información, con el fin de reducir el riesgo, gestionar adecuadamente los activos y proteger las instalaciones, así como con los demás

procedimientos y puntos de control generados dentro del marco del Subsistema de Gestión de Seguridad de la Información.

23. CONTROLES DE REVISIÓN Y AUDITORÍA

La Secretaría Distrital de Ambiente a través de la Oficina de Control Interno o quien haga sus veces, realizará seguimiento y auditoría a la gestión de los riesgos y activos de información del Subsistema de Gestión de Seguridad y Privacidad de la Información, de acuerdo a los lineamientos dados en el procedimiento de Auditoría Interna de la Entidad.

El incumplimiento de las determinaciones dadas en el presente documento estará sujeto a tratamientos disciplinarios.