MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

SECRETARÍA DISTRITAL DE DESARROLLO ECONÓMICO
BOGOTÁ D.C., OCTUBRE DE 2023

Contenido

1. INTRODUCCIÓN

La Secretaria Distrital de Desarrollo Económico tiene como misión liderar la formulación, gestión y ejecución de políticas de desarrollo económico, orientadas a fortalecer la competitividad, el desarrollo empresarial, el empleo, la economía rural y el abastecimiento alimentario, a través del diseño e implementación de estrategias efectivas que conlleven a la generación y mejora de ingresos de las personas, las empresas y el mejoramiento de la calidad de vida de los habitantes de la ciudad en general, fuente página www.desarrolloeconomico.gov.co, para esto la Secretaría Distrital de Desarrollo Económico cumple con las funciones estipuladas en el Decreto 437 de 2016 de la Alcaldía Mayor de Bogotá, D.C. " Por el cual se modifica la estructura organizacional de la Secretaría Distrital de Desarrollo Económico, estableciendo su objeto, funciones, estructura interna y funciones de las dependencias" y sus decretos modificatorios: Decreto 443 de 2021: "Por el cual se modifica la estructura organizacional de la Secretaría Distrital de Desarrollo Económico" y Decreto 100 de 2023: "Por medio del cual se modifica la estructura organizacional de la Secretaría Distrital de Desarrollo Económico y se dictan otras disposiciones".

En el desarrollo de sus actividades genera, preserva, compila, distribuye información, datos, documentos, entre otros. Esta información, al igual que la plataforma tecnológica son consideradas por la SDDE como activos valiosos para su funcionamiento y consecución de objetivos, por tal razón se hace necesario establecer políticas específicas como parte integral en la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI- y el cumplimiento de Resolución 399 de 2023 "Por la cual se adopta la Política de Seguridad y Privacidad de la Información de la SDDE" en el Marco de la Implementación del Modelo Integrado de Planeación y Gestión en la Política de Gestión y Desempeño de Seguridad Digital.

2. OBJETIVO

Establecer los lineamientos de implementación de la política de seguridad y privacidad de la información mediante componentes específicos.

3. ALCANCE

El presente manual de políticas aplica a funcionarios, contratistas, terceros, usuarios y visitantes de La Secretaría de Desarrollo Económico por alguna razón tengan cualquier tipo de interacción con los activos de información.

4. DEFINICIONES

- Activo de Información: se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, documentos, soportes, edificios, personas...) que tenga valor para la organización.
- Confidencialidad: Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.
- Integridad: Propiedad de la información que busca preservar su exactitud y completitud.
- Disponibilidad: Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.

- 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.
- Controles: Medida que permite reducir o mitigar un riesgo

5. CONTEXTO

En la búsqueda de mejorar la gestión de la SDDE se adoptó el Sistema Integrado de Gestión, el cual genera beneficios como el cumplimiento de normatividad legal, específicamente la implementación de la Política de seguridad digital que se encuentra establecida en la dimensión 3 -Gestión con valores para resultados-, establecida conforme el documento CONPES 3854 de 2016 el cual busca incorpora la Política Nacional de Seguridad Digital coordinada por la Presidencia de la República.

Con la política se fortalecen las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital, así como en la creación e implementación de instrumentos de resiliencia, recuperación y respuesta nacional en un marco de cooperación, colaboración y asistencia.

A través del mapa de procesos, se puede visualizar los procesos (Misionales, Estratégicos, de Apoyo y de Evaluación) sus interrelaciones, dentro de las cuales está contenida la base documental (procedimientos, manuales, formatos, guías e instructivos) para el desarrollo, mejora y logro de los objetivos institucionales.

Los procesos incluidos para el Sistema de Gestión de Seguridad de la Información corresponden a todos los definidos por la Secretaría Distrital de Desarrollo Económico que hacen uso de la información y de las herramientas tecnológicas como se observa en el mapa de procesos de la Entidad.

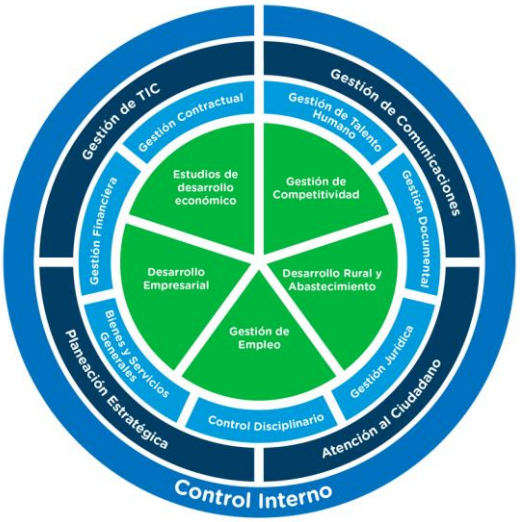

Imagen 1 – Mapa de Procesos de la Secretaría Distrital de Desarrollo Económico.

6. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

La Secretaria Distrital de Desarrollo Económico, establece a continuación, los siguientes lineamientos de seguridad de la información, los cuales deberán ser cumplidos conforme el alcance establecido.

Los lineamientos de seguridad están clasificados en diferentes temáticas, teniendo en cuenta el contexto interno y externo de la entidad:

6.1. Políticas Organizacionales

6.1.1. Política de estructura organizacional de seguridad de la información

- La Secretaría Distrital de Desarrollo Económico, en cumplimiento al compromiso de implementar el Sistema de Gestión de Seguridad de la Información - SGSI, establece un esquema de seguridad de la información definiendo roles y responsabilidades que involucren las actividades de operación, gestión y administración de la seguridad de la información a través de su Política de Seguridad y Privacidad de la información.
- A través de un acto administrativo de carácter general se adoptará la estrategia de seguridad digital, identificando el alcance y responsable de su implementación.
- Las políticas que componen el sistema de Gestión de Seguridad de la Información deben ser aprobadas por la Alta Dirección, en Comité Institucional de Gestión y Desempeño; publicadas, comunicadas y reconocidas por las partes interesadas; las actualizaciones serán a intervalos planificados no superiores a un año o si ocurren cambios significativos.
- El Subdirector de Informática y Sistemas y el oficial de seguridad tendrán la responsabilidad de proyectar, actualizar y/o modificar la Política de Seguridad y Privacidad de la Información, si a ello hubiere lugar y presentar al Comité Institucional de Gestión y Desempeño; para su aprobación.
- Todos los procedimientos y lineamientos que formen parte del SGSI deben ser aprobados, codificados, publicados en intranet y socializados a través de alguna estrategia de comunicación.

6.1.2. Política de gestión de activos de información

- La entidad debe documentar, adoptar y divulgar un procedimiento formal para la gestión de activos de información.
- Los procesos institucionales deben identificar y mantener actualizados los activos de información que tengan a cargo.
- Los activos de información serán responsabilidad de los líderes de cada dependencia o proceso.
- Es responsabilidad de cada dependencia o proceso informar las novedades que puedan afectar la integridad, disponibilidad o confidencialidad de los activos de información.
- Se debe identificar y documentar la devolución de los activos, como, por ejemplo: información física, hardware de autenticación -token-, tarjetas de acceso a las instalaciones de la entidad, equipos y dispositivos tecnológicos.
- Toda información sea física o digital generada, almacenada o transformada por los funcionarios, contratistas y proveedores, utilizando los recursos dispuestos por la entidad para tal fin o en desempeño de sus labores o servicio contratado, son activos de información propiedad de La secretaria Distrital de Desarrollo Económico, por lo tanto, al finalizar su contrato, vínculo o acuerdo deberán devolverlos.

6.1.3. Política de uso de los activos

- La entidad implementará las directrices para mantener la protección adecuada y uso de los activos de información mediante la asignación de los usuarios finales que deban administrarlos de acuerdo con sus roles y funciones.
- La asignación de los activos de información es para uso exclusivo del desarrollo de las actividades misionales y contractuales que le sean asignadas en la entidad, por tal motivo la entidad no se hace responsable de la información personal que sea almacenada en los activos institucionales.
- El usuario de los recursos tecnológicos asignados por la entidad se debe comprometer a dar buen uso, de acuerdo con las políticas y lineamientos definidos por el SGSI.
- Todos los funcionarios, contratistas y proveedores que hagan uso de los activos de información institucionales tienen la responsabilidad de seguir las políticas establecidas para el uso adecuado de los activos de información, entendiendo que el uso no adecuado de los recursos puede poner en riesgo la disponibilidad de los servicios tecnológicos institucionales y la confidencialidad de la información y además generar acciones disciplinarias de ser el caso.
- Se debe capacitar a los funcionarios y contratistas cuando ingresen por primera vez a la entidad, en el manejo de los sistemas de información institucionales y las herramientas tecnológicas.
- No se debe consumir alimentos y bebidas mientras se esté haciendo uso o manipulación de los activos de información.

6.1.4. Política de uso de los recursos tecnológicos.

- Todos los funcionarios, contratistas y proveedores deben hacer buen uso de los activos de información a los cuales tienen acceso y que son propiedad de la entidad, de igual forma, son responsables de cualquier uso que se les dé.
- Los equipos de cómputo solo deben ser destapados y actualizados por el personal autorizado en la Subdirección de Informática y Sistemas.
- Los usuarios no deben almacenar en los discos duros de las estaciones cliente o discos virtuales de red, archivos de vídeo, música, fotos o cualquier tipo de archivo que no sean de carácter institucional.
- No está permitido realizar conexiones o derivaciones eléctricas que pongan en riesgo la disponibilidad de la información por fallas en el suministro eléctrico a los equipos de cómputo.

- La pérdida o daño de elementos o recursos tecnológicos, o de alguno de sus componentes, debe ser informada de inmediato a la Subdirección Administrativa y Financiera, de acuerdo con el procedimiento establecido para tal fin.
- El traslado de los recursos tecnológicos físicos estará a cargo de la Subdirección Administrativa y Financiera y su configuración se realizará a través de la Subdirección de Informática y Sistemas.
- Todo incidente de seguridad que comprometa la disponibilidad, integridad o confidencialidad de la información debe ser reportado a la Subdirección de Informática y Sistemas en la mayor brevedad posible, a través de la herramienta establecida para tal fin.
- La Subdirección de Informática y Sistemas es la única dependencia autorizada para la instalación del software, el cual no debe ser copiado, suministrado a terceros o utilizado para fines personales.
- Las estaciones de trabajo de usuario final deben quedar apagados cada vez que el colaborador no se encuentre en la entidad y no requiera realizar actividades vía remota.
- Definir y documentar la gestión de cambios en la infraestructura tecnológica y los sistemas de información.

- Los recursos tecnológicos son objeto de inspecciones, seguimiento y auditorías internas con el fin de gestionar, analizar e investigar posibles incidentes/eventos de seguridad que comprometan algún parámetro a nivel de integridad, disponibilidad y confidencialidad de los activos de información institucional.

6.1.5. Política de uso del correo electrónico

- El correo electrónico institucional es una herramienta de apoyo a las funciones y responsabilidades de los funcionarios y contratistas de la entidad.
- El servicio de correo electrónico institucional debe ser empleado únicamente para enviar y recibir mensajes de carácter institucional. En consecuencia, no puede ser utilizado con fines personales, económicos, comerciales y/o cualquier otro ajeno a los propósitos de la Secretaría Distrital de Desarrollo Económico
- En cumplimiento de la iniciativa del uso aceptable del papel y la eficiencia administrativa, se debe optar por el uso del correo electrónico al envío de documentos físicos, siempre que las disposiciones legales lo permitan. Esto teniendo en cuenta que, los mensajes de correo están respaldados por la Ley 527 de 1999 (por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.), en tal caso se funda la legalidad de los mensajes de datos y las implicaciones legales que conlleva el mal uso de estos.
- No se permite el uso de correos masivos tanto internos como externos, salvo a través de las cuentas autorizadas para tal fin.
- Todo mensaje sospechoso, SPAM o cadena debe ser inmediatamente reportado a la Subdirección de Informática y Sistemas como incidente/evento de seguridad de la información. No está permitido el envío y/o reenvío de mensajes en cadena, debido a que puede ser contentivo de virus, en especial si contiene archivos adjuntos con extensiones .exe, .bat, .prg, .bak, .pif,
- La cuenta de correo institucional no debe ser registrada en páginas o sitios publicitarios, de comercio electrónico, deportivos, casinos, o a cualquier otra ajena a los fines institucionales.
- No se permite el uso del correo para la transferencia de contenidos insultantes, ofensivos, injuriosos, obscenos, violatorios de los derechos de autor y/o que atenten contra la integridad moral de las personas o instituciones.
- No se dará uso del correo electrónico institucional para distribuir información de carácter reservado o clasificado, sin el previo análisis y autorización del líder de la dependencia y/o proceso.
- El envío de mensajes desde el correo electrónico debe contener una leyenda de confidencialidad y aplicarse en la firma institucional de todos los usuarios que tengan acceso a cuentas de correo electrónico con dominio de la entidad.

- El único servicio de correo electrónico autorizado para el manejo de la información institucional en la entidad es el asignado por la Subdirección de Informática y Sistemas, y que cuente con el dominio @desarrolloeconomico.gov.co, el cual cumple con todos los requerimientos técnicos y de seguridad.

6.1.6. Política para uso de dispositivos móviles y equipos portátiles

- Los dispositivos móviles que sean asignados por la entidad deberán mantener la configuración respectiva para restringir la instalación de software, así como un mecanismo que impida el robo o pérdida dentro de las instalaciones institucionales.

- Los dispositivos móviles deben estar configurados para acceder a través de credenciales de acuerdo con la asignación.
- Los dispositivos móviles de la entidad que sean retirados de las instalaciones deben contener mecanismo de cifrado de tal forma que evite divulgación de información en caso de pérdida o robo.
- Todos los dispositivos móviles asignados deben tener instalado el antivirus institucional.
- El uso de conexión a la red para los dispositivos móviles ajenos a la entidad deberá estar segmentada para proveer únicamente el servicio de internet, restringiendo el acceso a la data y navegación interna.

6.1.7. Política de uso de mensajería instantánea y redes sociales

- La información que se publique o divulgue -a título personal- por cualquier medio de internet por funcionarios, contratistas y proveedores de la entidad, en redes sociales como -pero sin limitarse a los siguientes: Twitter®, Facebook®, YouTube®, blogs, Instagram, se considera fuera del alcance del Sistema de Gestión de Seguridad de la Información y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que lo genere.
- Toda información distribuida en las redes sociales que sea originada por la entidad debe ser autorizada por los líderes de la dependencia y/o proceso para ser socializadas y divulgada por el grupo de comunicaciones de la Entidad.
- No se debe utilizar el nombre de la Secretaría Distrital de Desarrollo Económico en redes sociales para difamar o afectar la imagen y reputación de los seguidores cuando responden comentarios en contra de la filosofía de la Entidad.
- Las personas designadas para el manejo y gestión de contenido en las redes sociales de la entidad deben acatar las directrices dadas en el presente documento.
- Los responsables de cada red social deberán aplicar complejidad en las contraseñas de las cuentas institucionales, acatando los protocolos de seguridad de estas y realizando el cambio periódicamente.
- El Oficial de Seguridad de la Información realizará la verificación de las medidas y controles implementados de seguridad, encaminadas a evitar el acceso abusivo a la plataforma, que puedan afectar la imagen y la credibilidad de la entidad.
- No se deben vincular cuentas de correo electrónico personales en las redes sociales que se apertura bajo el dominio de la Secretaría Distrital de Desarrollo Económico.
- No se debe administrar y configurar las redes sociales la entidad en dispositivos móviles personales.
- Con el fin de evitar la fuga de información y descarga de contenido que pueda generar un riesgo de seguridad para la Entidad, se restringirá el acceso de mensajería instantánea como -pero sin limitarse a los siguientes: WhatsApp, Messenger que no se encuentre licenciada por la Secretaría Distrital de Desarrollo Económico. En caso de ser requerida alguna, se debe validar con la Subdirección de Informática y Sistemas el respectivo licenciamiento para su uso.

6.1.8. Política de clasificación de la información

- Las categorías de calificación de la información que se adoptaran son: Pública, Pública reservada y Pública clasificada.
- Todos los activos de información indiferente de su medio de almacenamiento deben ser clasificados de acuerdo con los lineamientos institucionales creados para tal fin. Esta actividad debe ser realizada por los responsables sobre la gestión de los activos de información, es decir los líderes de cada dependencia o proceso.

- Toda la documentación o información generada en la entidad debe ser clasificada en alguna de las categorías adoptadas.
- Desarrollar e implementar los lineamientos para el etiquetado de la información de acuerdo con las categorías definidas y adoptadas, las cuales permitirán reconocer fácilmente la clasificación del activo de información.
- En el caso de los sistemas de información que contienen información sensible se deben implementar mecanismos que indiquen la clasificación e identificación del contenido.

6.1.9. Política para la transferencia de información

- Proteger la información transferida al interior y fuera de la entidad.
- La Subdirección de Informática y Sistemas, realiza el control del uso de sistemas de transferencia de archivos vía FTP a terceros.
- Los canales de red usados para la transferencia de información deberán contar con un mecanismo que no permita la fuga o interceptación de información, en su defecto la información que viaja por estos deberá estar cifrada.
- Las transferencias de información deben estar amparadas por acuerdos interinstitucionales o de confidencialidad que permitan mantener los estándares de seguridad sobre esta.

6.1.10. Política de control y gestión de acceso a los activos de información

- La Subdirección de Informática y Sistemas establecerá los lineamientos para la gestión de usuarios dónde se detalle el uso de credenciales únicas, así mismo, para el uso de identificaciones compartidas o grupales por razones justificadas, establecer los tiempos de bloqueo o modificación de cuentas por inactividad, intentos fallidos, cambio de roles o retiro.
- Se debe mantener un registro centralizado de los accesos suministrados.
- Los accesos remotos se deben realizar por las herramientas autorizadas, no se permiten el uso de software de acceso remoto no licenciado por la entidad.
- Todo software debe ser validado o aprobado por la Subdirección de Informática y Sistemas
- El control de acceso a la Información se realiza aplicando el principio de mínimo privilegio necesario para la realización de las actividades asignadas.
- El acceso a la información se realiza de acuerdo con los niveles de calificación de la información y perfil asignado al usuario.
- Los accesos con privilegios especiales deben contar con la aprobación de la Subdirección de Informática y Sistemas y estar debidamente justificado por el solicitante.
- Los responsables del manejo de usuarios privilegiados deben aceptar su responsabilidad frente al uso del usuario asignado.
- Los administradores funcionales de los sistemas de información deben realizar revisiones periódicas por lo menos una semestral de los usuarios activos en los diferentes sistemas de información, dominio y red.
- Es responsabilidad de los supervisores y jefes de las dependencias notificar a la Subdirección de Informática y Sistemas la desvinculación de un funcionario, cesiones y terminaciones anticipadas del contratista para que sean retirados los accesos de todos los sistemas incluidos los accesos físicos a las diferentes instalaciones de la entidad, teniendo en cuenta el procedimiento establecido para tal fin.
- En el caso de los contratistas se debe realizar la configuración automática para que el día de la terminación del contrato sean inhabilitadas las credenciales asignadas.
- Para el acceso a los espacios de archivo tanto en las dependencias como el archivo central, se debe dar aplicación a los controles y lineamientos establecidos por la dependencia y/o proceso

encargado.

- Los servidores que, tengan bajo su responsabilidad la custodia de información física almacenada en archivadores que se encuentren en las oficinas, deben mantener el control de acceso a esta información; por lo tanto, debe estar bajo llave, la cual se debe guardar en un sitio seguro, dando cumplimiento a lo establecido en el presente manual.
- Se debe controlar que la información física clasificada como reservada o confidencialidad no se encuentre expuesta en sitios tales como cajones sin llave o sobre el escritorio, esto con el fin de mantener la confidencialidad.
- La Subdirección de Informática y Sistemas y el grupo de Gestión Documental deberá definir los lineamientos para la creación de repositorios de información dentro las herramientas que dispone la entidad, con el fin de establecer la estructura de la información generada y procesada de cada dependencia que se debe almacenar -Gestor documental y almacenamiento en la nube a través Drive asignado a cada área-

6.1.11. Política de establecimiento, uso y protección de claves de acceso

- Ningún usuario deberá acceder a la red o a los servicios de la entidad utilizando una cuenta de usuario o credenciales de otro usuario.
- Toda acción realizada usando la clave de acceso es responsabilidad directa del usuario al que se le asignaron las credenciales.
- La Subdirección de Informática y Sistemas suministrará a los usuarios las claves iniciales respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados. Las claves son de uso personal e intransferible.
- La Subdirección de Informática y Sistemas Implementará mecanismos para que los usuarios cambien su contraseña de acceso al usarla por primera vez en los sistemas de información o servicios a los que se les permita el acceso; así como implementar una política de red que solicite cambio de credenciales en periodos definidos.
- El desbloqueo y asignación de nueva contraseña solo debe ser solicitado por el titular de la cuenta, comunicándose a la Subdirección de Informática y Sistemas, en donde se llevará a cabo la validación de los datos personales, y se asignará una contraseña temporal.
- Los usuarios no deben dejar visibles las credenciales asignadas.
- Las contraseñas de acceso deben contener los siguientes requisitos de seguridad:
  - ✓ Tener mínimo ocho (8) caracteres alfanuméricos y especiales.
  - ✓ Cada vez que se cambien estas deben ser distintas por lo menos de las últimas cuatro (4) anteriores.
  - ✓ La contraseña debe ser cambiada máximo cada noventa (90) días.
  - ✓ No debe contener el nombre de usuario y caracteres consecutivos como -abcd,123456

Manejo de contraseñas para administradores de TI

- Se debe garantizar en las plataformas de tecnología que, el ingreso a la administración se realice con la vinculación directa de las credenciales del directorio activo.
- Las contraseñas referentes a las cuentas “predefinidas” incluidas en los sistemas o aplicaciones adquiridas deben ser desactivadas. De no ser posible su desactivación, las contraseñas deben ser cambiadas después de la instalación del producto.
- Los administradores de TI pertenecientes a la Subdirección de Informática y Sistemas no deben dar a conocer sus credenciales institucionales de acceso a los sistemas de información a terceros, sin previa autorización escrita del Subdirector de Informática y Sistemas
- Los Administradores de TI pertenecientes a la Subdirección de Informática y Sistemas deben

emplear obligatoriamente contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación que posee la entidad de acuerdo con el rol asignado.

6.1.12. Política en la relación con proveedores

- Mantener la seguridad de la información y de los servicios de procesamiento, a los cuales tienen acceso las terceras partes, entidades externas o que son procesados, comunicados o dirigidos por estas.
- Se deben establecer obligaciones dentro de los contratos con terceros que contemplen aplicación de estándares y mejores prácticas de gestión de seguridad y otros criterios que resulten de un análisis de riesgos de la selección y los criterios establecidos por la entidad.
- Se debe establecer mecanismos de control en las relaciones contractuales, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por los proveedores o contratistas, cumplan con las políticas de seguridad de la información de la entidad, las cuales deben se divulgadas por los funcionarios responsables de la realización y/o firma de contratos o convenios.
- Los contratistas, oferentes y/o proveedores deben aceptar y firmar el acuerdo de confidencialidad establecido por la entidad.
- Los funcionarios de la entidad que tengan responsabilidad como supervisores de contratos relacionados con sistemas de información deberán realizar seguimiento, control y revisión de los servicios suministrados por los proveedores y/o contratistas, propendiendo por el cumplimiento de las políticas de seguridad de la información.
- Todo proveedor y/o contratista debe informase de las políticas y lineamientos que componen el Sistema de Gestión de Seguridad de la Información -SGSI y establecerse como una obligación contractual.
- Todo proveedor y/o contratista debe realizar la devolución de los activos de información asignados por la entidad para el cumplimiento de las obligaciones contractuales.
- Se deben establecer mecanismos o condiciones con los contratistas y proveedores en donde estos informen y puedan realizar la gestión de cambios en los servicios suministrados.

6.1.13. Política para el uso de servicios en la nube

- En el uso de servicios en la nube contratados por la entidad se deben gestionar los riesgos de seguridad.
- Se debe identificar y definir la responsabilidad compartida de la seguridad de la información y los esfuerzos de colaboración entre el proveedor del servicio y la Secretaría Distrital de Desarrollo Económico. En caso de que los acuerdos de servicios estén predefinidos y no están abiertos a negociación la entidad debe revisar los definidos y validar que se contemplen los requisitos de confidencialidad, integridad, disponibilidad y manejo de la información institucional.
- La entidad, actuando como cliente del servicio en la nube definirá si debe exigir al proveedor de servicio que se notifique antes de realizar cambios sustanciales que afecten la continuidad del servicio contratado, como los relacionados a continuación, pero sin limitarse:
  - ✓ Cambios de hardware o software, reconfiguraciones y demás que afecten o cambien la oferta de servicios en la nube.
  - ✓ Realizar tratamiento de información en una nueva jurisdicción geográfica o legal.
  - ✓ Uso de proveedores de servicios similares o subcontratados.

6.1.14. Política de gestión de los incidentes de la seguridad de la información

- Garantizar que los eventos e incidentes de seguridad que se presenten con los activos de información sean comunicados y atendidos oportunamente, empleando los procedimientos definidos, con el fin de tomar oportunamente las acciones correctivas.
- Establecer los respondientes para la atención de incidentes de seguridad dentro de la Secretaría Distrital de Desarrollo Económico.
- Identificar y documentar contacto con autoridades, grupos de interés que manejen temas relacionados con seguridad de la información e incidentes.
- Asegurar una gestión consistente y eficaz de la evidencia relacionada con incidentes de seguridad de la información para efectos de acciones disciplinarias y legales.
- Fortalecer y mejorar los controles de seguridad de la información a través de la documentación y conocimiento de los incidentes de seguridad que se presenten en la entidad.

6.1.15. Política de seguridad de la información durante la interrupción de los servicios institucionales

- La entidad debe definir el conjunto de procedimientos y estrategias para contrarrestar las interrupciones en las actividades misionales de la entidad, proteger sus procesos críticos contra fallas mayores en los servicios tecnológicos y asegurar que las operaciones se recuperen oportuna y ordenadamente, generando un impacto mínimo o nulo ante una contingencia.
- Prevenir interrupciones en las actividades de la plataforma tecnológica de la entidad que, van en detrimento de los procesos críticos de TI afectados por situaciones no previstas o desastres.
- Los proveedores de servicios TI críticos deberán contar con planes de continuidad, los cuales deben ser de conocimiento de la Subdirección de Informática y Sistemas.
- Se debe desarrollar e implementar un Plan de Continuidad TI para asegurar que los procesos misionales de la entidad los cuales serán restaurados dentro de escalas de tiempo razonables. El plan de acción que permitirá mantener la continuidad se desarrollará teniendo en cuenta los siguientes aspectos como mínimo:
  - ✓ Identificación y asignación de prioridades a los procesos críticos de la entidad de acuerdo con su impacto en el cumplimiento de la misión institucional.
  - ✓ Documentación de la estrategia de continuidad TI.
  - ✓ Documentación del plan de recuperación del negocio de acuerdo con la estrategia definida anteriormente.
  - ✓ Plan de pruebas de la estrategia de continuidad TI.
- Los requisitos de seguridad de la información deben incluirse en los procesos de gestión de la continuidad del negocio.

6.1.16. Política de cumplimiento de requisitos legales, estatutarios, reglamentarios y contractuales

- La entidad debe gestionar riesgos para prevenir el incumplimiento de obligaciones legales relacionadas con seguridad de la información.
- Todos los sistemas de información que capturen datos personales deben cumplir con la política de tratamiento y protección de datos personales definidas por la entidad.
- La entidad debe identificar, documentar y actualizar los requisitos legales y reglamentados relacionados con seguridad de la información.
- La Subdirección de Informática y Sistemas deberá garantizar que todo el software que se ejecute

esté protegido por derechos de autor o en su defecto contenga licencia de uso o software de libre distribución y uso.

- La entidad debe mantener prueba y evidencia de propiedad del licenciamiento adquirido.
- Los servidores institucionales deben cumplir con las Leyes de derechos de autor y acuerdos de licenciamiento de software, se recuerda que es ilegal duplicar software y documentación sin la autorización del propietario bajo los principios de derechos de autor y, la reproducción no autorizada es una violación a la Ley.

6.1.17. Política de tratamiento de datos personales

La Secretaría Distrital de Desarrollo Económico realizará el tratamiento de datos personales conforme la Ley 1581 de 2012, sus Decretos reglamentarios y la Política de Tratamiento y Protección de Datos Personales definida en la entidad.

6.1.18. Política de revisión independiente de la seguridad de la información.

- Garantizar el funcionamiento del sistema de gestión de seguridad de la información de acuerdo con las políticas y procedimientos implementados en la Entidad.
- A través de la Oficina de Control Interno se realizarán las verificaciones del cumplimiento de objetivos, controles, políticas y procedimientos de seguridad de la Información.
- Todos los líderes de proceso y dependencias deben verificar y supervisar el cumplimiento de las políticas de seguridad de la información con el personal a cargo.
- La Subdirección de Informática y Sistemas a través del Oficial de Seguridad de la Información –o quien haga sus veces- realizará revisiones esporádicas no programadas con el fin verificar el cumplimiento de las políticas de seguridad de la información en las instalaciones de la entidad.

6.1.19. Política de cumplimiento en materia de seguridad de la información

- Los diferentes aspectos contemplados en este documento son de obligatorio cumplimiento para todos los funcionarios, contratistas y proveedores de la Secretaría Distrital de Desarrollo Económico. En caso de que se infrinjan las políticas de seguridad de forma intencional o por desconocimiento, la entidad tomará las acciones disciplinarias y legales correspondientes.
- Con la aplicabilidad de las políticas establecidas se debe prevenir el incumplimiento de las leyes, estatutos, regulaciones y obligaciones contractuales que se relacionen con los controles de seguridad.

6.2. Política de seguridad del recurso humano

- Se debe asegurar que los funcionarios y contratistas, adopten sus responsabilidades en relación con las políticas de seguridad de la información y actúen de manera consistente frente a las mismas, con el fin de reducir los riesgos.
- Los acuerdos laborales y contractuales deben establecer la responsabilidad del colaborador en cuanto a seguridad de la información -derechos de autor, confidencialidad y no divulgación de la información durante y después del empleo; así como el conocimiento y cumplimiento de las políticas del SGSI.
- Establecer estrategias para que los funcionarios y contratistas tomen conciencia con lo relacionado a los temas de seguridad de la información.
- Articular los procedimientos disciplinarios en situaciones de incumplimiento y/o violaciones de las

políticas de seguridad de la información, conforme a las normas que lo reglamenten en el sector público.

- Implementar procedimientos que permitan identificar las novedades, desvinculaciones, terminaciones o cesiones de contrato y demás, con el fin de retirar o modificar los accesos físicos y lógicos en la entidad.

6.2.1. Política de trabajo a distancia

- La Subdirección de Informática y Sistemas velará por la identificación de necesidad y licenciamiento de la VPN - Virtual Private Network
- Las actividades de acceso remoto (uso de VPN - Virtual Private Network) a los activos de información electrónicos/digitales de la entidad, se autorizan de acuerdo con las necesidades específicas de la dependencia solicitante.
- Se recomienda que mientras se haga uso de VPN desde un equipo personal, éste tenga instalado y actualizado el antivirus y que el sistema operativo cuente con las actualizaciones de seguridad y esté licenciado.
- La Subdirección de Informática y Sistemas realizará las configuraciones de seguridad, aprovisionamientos y revocación de acceso a la VPN según corresponda.

6.3. Política de seguridad física

6.3.1. Política de perímetros y entrada física

- La entidad debe implementar un sistema de seguridad física para las instalaciones de la entidad.
- Se deben implementar alarmas de detección de intrusos a los centros de datos y centros de cableado de la entidad u otros mecanismos que permitan mantener alertas.
- Definir y usar perímetros de seguridad para proteger las dependencias de procesamiento de información sensible o critica, teniendo en cuenta:
  - ✓ Todas las puertas externas deberían tener mecanismos de control que eviten el acceso no autorizado.
  - ✓ Las puertas y ventanas se deben mantener cerradas con llave cuando no hay supervisión.
  - ✓ Prohibir el uso de equipo fotográfico, de video, audio u otro equipo de grabación cuando no se cuente con autorización para ello
- Los visitantes deben registrarse en la entrada, ser autorizados por un colaborador para ingresar y durante su estancia y hasta su retiro deben estar acompañados por el funcionario o contratista con el cual están desarrollando su actividad.
- Los controles de acceso físico a las instalaciones deben permitir el acceso únicamente al personal autorizado.
- Todos los colaboradores deben portar el carné en lugar visible, en caso de ser visitante se debe portar una escarapela que lo identifique.
- Para el caso de las dependencias del despacho y carga se debe:
  - ✓ Inspeccionar el material que ingresar para detectar presencia de materiales peligrosos.
  - ✓ Restringir para el personal identificado y autorizado

6.3.2. Política de escritorio despejado y pantalla limpia

- Los funcionarios y contratistas que tienen algún vínculo con la entidad deben conservar su escritorio libre de información, propia de la entidad, que pueda ser vista, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

- Todos los equipos y sistemas de información deben configurarse con una función de tiempo de espera o cierre de sesión automático.
- Los usuarios de los sistemas de información institucionales deben bloquear la pantalla de su computador, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.
- Los usuarios de los sistemas de información deben cerrar las aplicaciones y servicios de red cuando ya no los necesite.
- Al imprimir documentos con información pública reservada y/o pública clasificada, deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia

6.3.3. Política de protección contra amenazas físicas y ambientales

- Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.
- Contar con herramientas que permitan registrar y restringir el acceso de los servidores a estas dependencias.
- En las instalaciones del centro de datos o de los centros de cableado, No está permitido:
  - ✓ Fumar dentro de las instalaciones.
  - ✓ Introducir alimentos o bebidas.
  - ✓ El porte de armas de fuego, corto punzantes o similares.
  - ✓ Mover, desconectar y/o conectar equipos de cómputo sin autorización
  - ✓ Modificar la configuración del equipo o intentarlo sin autorización.
  - ✓ Alterar software instalado en los equipos sin autorización.
  - ✓ Alterar o dañar las etiquetas de identificación de los elementos tecnológicos o sus conexiones físicas.
  - ✓ Extraer información de los equipos en dispositivos externos sin previa autorización.
  - ✓ Abuso y/o mal uso de los recursos tecnológicos físicos.
  - ✓ Toda persona debe hacer uso únicamente de los equipos y accesorios que les sean asignados y para los fines que se les autorice.

- Revisar y actualizar periódicamente los derechos de acceso.
- Cada Gabinete o armario de almacenamiento debe contener llave y/o tarjeta de acceso, las cuales deben permanecer custodiadas por el colaborador designado para tal fin.
- Considerar la implementación de controles contra incendios, inundaciones, sobretensiones eléctricas y en general de las posibles amenazas físicas y ambientales.
- Los medios y equipos donde se almacena procesan o comunica la información (física o electrónica), deben mantenerse con las medidas de protección físicas y lógicas.

6.3.4. Política de medios de almacenamiento

- Los medios de almacenamiento extraíble pueden generar riesgos para la entidad al ser conectados a los computadores, ya que son susceptibles de transmisión de virus informáticos o pueden ser utilizados para la extracción de información no autorizada.
- Está restringida la copia de archivos en medios removibles de almacenamiento, por lo cual se deshabilita la opción de escritura en dispositivos USB, unidades ópticas de grabación en todos los equipos de cómputo institucionales; la autorización de uso de los medios removibles debe ser tramitada a través de la Subdirección de Informática y Sistemas y será objeto de auditorías de seguridad mediante las herramientas consideradas para tal fin.

- Solo se habilitarán los puertos de conexión de medios de almacenamiento extraíbles si existe una razón institucional para su uso y es autorizado por el jefe inmediato.
- Se debe realizar monitoreo a la transferencia de información cuando sea necesario utilizar medios de almacenamiento extraíble.

6.3.5. Política de seguridad del cableado

- Se deben implementar controles que permitan proteger las líneas eléctricas y de telecomunicaciones de cortes accidentales.
- Los cables de alimentación y comunicación deben estar separados para evitar interferencias.
- Implementar conductos blindados, cajas cerradas y alarmas en los puntos de terminación.
- Establecer mecanismos de acceso controlado a los paneles de conexión y centros de cableado.
- Se debe propender por el uso de cables de fibra óptica.

6.3.6. Política de eliminación segura o reutilización de equipos

- Cuando no se requiera la información contenida en un medio de almacenamiento reusable, se debe borrar para que no sea recuperable y registrar los resultados como prueba de la eliminación. En caso de los equipos en condición de alquiler, se debe realizar el borrado antes de la devolución.
- La información almacenada con nivel alto de confidencialidad o integridad en medios removibles debe contar con técnicas de cifrado para evitar accesos no autorizados.
- Para los medios que contienen información confidencial, se deben almacenar y disponer de forma segura, mediante incineración, destrucción a través de máquinas destinadas para tal fin o proceso de borrado seguro, de acuerdo con las directrices de la Subdirección de Informática y Sistemas

  En cualquiera sea el caso de realizar destrucción de algún componente tecnológico, se ejecutará bajo los lineamientos del Sistema de Gestión Ambiental.

6.4. Política de las operaciones de las Tecnologías de la Información y las Comunicaciones

6.4.1. Política de dispositivos tecnológicos y redundancias

- Definir y documentar las actividades operacionales especificando los lineamientos para:
  - ✓ Copias de seguridad
  - ✓ Reinicio y recuperación del sistema en caso de falla
  - ✓ Contactos de soporte en caso de dificultades técnicas inesperadas.
- Realizar seguimiento al uso de recursos y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema, considerando documentar planes de gestión de capacidad para los sistemas críticos de la misionalidad.
- Los servicios y dispositivos tecnológicos deben estar monitoreados en cuanto a: seguimiento de intentos de accesos fallidos y compartimientos anómalos.
- Los funcionarios y contratistas no tienen permitido descargar, utilizar e instalar software externo en los recursos tecnológicos institucionales a menos que sea aprobado e instalado por la Subdirección de Informática y Sistemas.
- Implementar controles de detección, prevención y recuperación para proteger los activos de información contra ataques de código malicioso.
- La asignación de dispositivos tecnológicos deberá realizarse a través de registro y entregar con

las configuraciones de: dominio, cifrado de disco, restricción de instalación de software, protección contra virus, bloqueo remoto -en caso de no requerirse accesibilidad a través de VPN, partición del disco duro y demás consideradas en las políticas anteriores.

- La Subdirección de Informática y Sistemas velará por:
  - ✓ Adquirir y mantener actualizadas las licencias de software de protección contra código malicioso en todos sus servidores, equipos de cómputo y los archivos intercambiados por correo electrónico tanto entrantes como salientes.
  - ✓ Establecer mecanismos para mantener actualizados todos los sistemas de procesamiento de información (parches de software y actualizaciones).
  - ✓ Presentar las necesidades tecnológicas en materia de seguridad digital ante las instancias correspondientes.

6.4.2. Política de accesos con privilegios elevados.

- La asignación de los accesos con privilegios debe controlarse a través de un procedimiento.
- Las solicitudes deben ser realizadas y aprobadas por el responsable del activo de información.
- Los accesos con privilegios deben estar limitadas por un rango de tiempo específico.
- Revisar regularmente los accesos con privilegios otorgados.
- Se debe tener en cuenta que los accesos con privilegios elevados son exclusivamente para realizar tareas de gestión y administración de los componentes tecnológicos y en ningún momento para realizar actividades de uso personal del usuario.
- Los accesos con privilegios deben estar asociados a un usuario específico, si la cuenta contiene una identificación genérica no se debe hacer uso por varios administradores.

6.4.3. Política de acceso a sistemas y aplicaciones

- El acceso a la información y a las funcionalidades de las aplicaciones se debe restringir, de acuerdo, con los niveles de autorización para cada usuario o grupo de usuarios.
- El acceso a los sistemas de información se debe iniciar con el principio de accesos mínimos.
- Los sistemas y aplicaciones deben mantenerse monitoreados y auditados.
- Las credenciales para acceder a los ambientes de pruebas y producción se deben diferenciar de forma que permitan identificar cada usuario para cada ambiente.
- Se debe controlar el acceso a códigos fuente de programas y elementos asociados (diseños, especificaciones, planes de prueba, resultados), para evitar la introducción de funcionalidades no autorizadas o cambios involuntarios, así mismo, para mantener la confidencialidad de la propiedad intelectual, por tal motivo:
  - ✓ Las librerías de programas fuente deben almacenarse en el repositorio de control de versiones dispuesta por la entidad para tal fin, no deberían estar contenidas en los ambientes de producción.
  - ✓ Establecer un repositorio formal para el almacenamiento de código fuente y control de versiones.
  - ✓ Controlar los cambios para el mantenimiento y copia de las librerías de fuentes de programas.
  - ✓ Mantener un registro de auditoría de todos los accesos con su respectiva acción.
- Se debe mantener los siguientes lineamientos, pero sin limitarse;
  - ✓ Validar las credenciales de acceso al completar todos los datos de entrada, en caso de error el sistema no deberá informar cual es el dato correcto o incorrecto.

- ✓ Proteger contra intentos de ingreso mediante ataques de fuerza bruta.
- ✓ Mantener registro de intentos exitosos y fallidos de acceso.
- ✓ No mantener visible la contraseña que se está ingresando.
- ✓ Todos los sistemas de información expuestos públicamente o en el portal web de la entidad deben contar con certificado de sitio seguro.
- ✓ No transmitir contraseñas en texto claro en las redes o medios de comunicación.
- ✓ No dar la opción al usuario de recordar las credenciales
- ✓ Datos de acceso (fecha y hora de inicio de sesión exitoso)
- ✓ Finalizar las sesiones inactivas después de un periodo de inactividad de tiempo, con especial rigurosidad para lugares públicos, externos o dispositivos móviles.
- ✓ Bloqueo de credenciales tras 4 intentos máximos erróneos.
- ✓ Bloqueo de los equipos de cómputo tras 5 minutos de inactividad.

6.4.4. Política de gestión de vulnerabilidades

- Identificar y definir las estrategias de monitoreo de vulnerabilidades técnicas.
- Realizar pruebas planificadas y documentadas para evaluar vulnerabilidades mínimo una vez al año.
- Validar riesgos del despliegue de actualizaciones de firmware o sistemas operativos antes de su instalación

6.4.5. Política de controles criptográficos

- Implementar controles para proteger activos de información reservados, fortaleciendo la confidencialidad, disponibilidad e integridad, mediante el uso de herramientas criptográficas.
- La entidad no establece un lineamiento de ciclo de vida de llaves criptográficas, toda vez que, la asignación de la clave para el cifrado de la información en la herramienta, la establece el usuario que genera o administra la información a cifrar, teniendo siempre presente que, en caso de olvidar la clave, la información cifrada no es recuperable.
  Se debe contar con herramientas que permitan el cifrado de información en medios de almacenamiento.
- Se debe instalar y configurar herramientas de cifrado de información en los portátiles institucionales

6.4.6. Política de respaldo y restauración de información

- Proporcionar medios de respaldo adecuados para asegurar que la información misional y el software, se pueda recuperar después de una falla, garantizando que esta y la infraestructura crítica de la entidad, sean respaldadas y puedan ser restauradas en caso de una falla y/o desastre.
- Los administradores de la plataforma que realizan las copias de seguridad verificarán la correcta ejecución de estos procesos.
- Los administradores de la plataforma de copias de respaldo de la entidad, trimestralmente deben generar tareas de restauración aleatorias de la información, incluidas las bases de datos definidas por el Subdirector de Informática y Sistemas; estas restauraciones deben ser documentadas, con el fin de garantizar la continuidad de las actividades realizadas en la entidad, usando las herramientas tecnológicas en caso de presentarse la no disponibilidad de la información almacenada en las bases de datos.
- Es responsabilidad de los funcionarios y contratistas almacenar la información en los medios

dispuestos por la Subdirección de Informática y Sistemas, el medio contará con un límite de espacio de almacenamiento. Cuando la información almacenada supere la capacidad de almacenamiento límite asignado, el usuario deberá revisar y depurar su información.

- Ningún usuario final debe realizar copias de la información contenida en la estación de trabajo a medios extraíbles de información, sin autorización del responsable del activo de información.
- Teniendo en cuenta que, la información generada, producida y tratada por el funcionario/contratista es producto de la ejecución de actividades institucionales no se entregaran copias de respaldo de la información contenida en correos electrónicos, sistemas de información, estaciones de trabajo y unidades de almacenamiento; en todo caso se validará la autorización de entrega de la información previa solicitud del responsable del activo indicando el motivo, tipo de información se requiere, la clasificación establecida en la matriz de activos de información. Es responsabilidad del usuario entregar el medio de almacenamiento en el cual será almacenada la información.
- Mantener custodiadas copias idénticas de sistemas operativos que respondan a eventos de contingencia y disminuyan el impacto en caso de falla irreversible.
- La entidad debe evaluar mecanismos externos para generar copias de seguridad.

6.4.7. Política de seguridad de las comunicaciones

- Implementar mecanismos de control que permitan mantener la disponibilidad de las redes de datos, sistemas de comunicaciones e instalaciones de procesamiento de la entidad.
- Segmentar los servicios de información, usuarios y sistemas, controlando así el tráfico.
- Los servicios de red deben estar protegidos a través de medios de autenticación.
- Implementar los mecanismos técnicos requeridos para la conexión segura con los servicios de red.
- Disponer de zona DMZ entre la red interna y externa con el objetivo limitar conexiones desde la red interna hacia Internet y conexiones desde internet hacia la red interna.
- Restringir la conectividad de la red cableada a los equipos que no son propiedad de la entidad.
- Se debe disponer de servicio de internet para visitantes de la entidad.

6.4.8. Política de registro y seguimiento de eventos de sistemas de información y comunicaciones

- Identificar los sistemas críticos de la entidad y documentar una metodología de revisión y escritura de eventos (Event Logs), que permita evidenciar las actividades por usuario, excepciones, fallas y eventos de seguridad que no den espacio a la alteración, uso no autorizado o repudio, en caso de presentarse materialización del riesgo y ser utilizados como medio probatorio.
- Mantener los relojes de todos los dispositivos tecnológicos con una única fuente de referencia, esto con el fin de mantener la exactitud del tiempo y permita correlacionar los eventos y logs.

6.4.9. Política de adquisición, desarrollo y mantenimiento de sistemas de información

- Garantizar que la seguridad es parte integral del ciclo de vida de los sistemas de información.
- Documentar lineamiento de control de instalación y cambios de los sistemas, para mantener operativas las aplicaciones basadas en estos y que permitan procedimientos de retroceso (RollBack) exitosos.
- Definir y documentar los requisitos de seguridad para la adquisición, desarrollo de los sistemas y mejoras de los existentes.

- Se debe aplicar mecanismos de auditoría a todos los sistemas de información en producción y se evaluara su tiempo de retención teniendo en cuenta la capacidad de almacenamiento institucional, en todo caso, este no debe ser inferior a 3 meses.
- Garantizar la separación de los entornos de desarrollo, pruebas y producción de los sistemas de información.
- Definir y documentar los entornos para el almacenamiento de los códigos y sus versiones.
- Ejecutar revisiones periódicas al licenciamiento de software y desinstalar de los equipos de cómputo, el software que no se encuentre licenciado.
- Establecer, documentar y ejecutar las prácticas seguras, criterios de solicitud y pruebas de calidad y aceptación sobre el desarrollo
- Las solicitudes para uso de software libre serán avaladas previo concepto del oficial de seguridad.
- Asegurar en la medida de lo posible que las bases de datos utilizadas en ambientes de pruebas sobre las etapas de desarrollo de soluciones de información no corresponden a información real o la misma debe ser modificada para tales fines.
- El desarrollo de aplicativos o sistemas de información diseñado por terceros debe estar bajo estándares de desarrollo de la Subdirección de Informática y Sistemas y alineado a las políticas de seguridad de la información.
- Los datos de prueba no deben contener datos personales o información sensible, de ser necesario este contenido se deben utilizar mecanismos de enmascaramiento o sustitución de datos.

6.4.10. Política de protección de la información durante auditorias

Cuando se considere realizar auditorías a los sistemas de información y demás componentes de almacenamiento como bases de datos, se tendrá en cuenta:

- La auditoría debe contemplar de manera específica el sistema al cual requiere acceso.
- Los accesos solo serán autorizados en modo lectura.
- Si se requiere un acceso diferente al modo lectura, se otorgará para copias aisladas del sistema con todos los parámetros de seguimiento de seguridad -logs.
- Si las pruebas afectan la disponibilidad estas deben realizarse fuera del horario laboral.

7. DECLARACIÓN DE APLICABILIDAD

La Declaración de Aplicabilidad (Statement of Applicability - SOA), será el documento que lista los controles a implementar en la Secretaría Distrital de Desarrollo Económico, así como la justificación de aquellos controles que no serán implementados.

Este análisis se hace evaluando los requisitos de la norma ISO 27002:2022, para cada uno de los controles establecidos en los dominios o temas relacionados con la gestión de la seguridad de la información que allí se especifica.

CAMBIOS EN EL DOCUMENTO	RESPONSABLE	FECHA	VERSIÓN
Creación del documento	Subdirección Informática y Sistemas	19 de octubre de 2023	1

No.	ELABORÓ	REVISÓ	APROBÓ	REVISIÓN TÉCNICA	APROBACIÓN TÉCNICA:	FECHA
1	Maria Alejandra Suarez Contratista	Adriana Montoya/ Subdirector de Informática y Sistemas	Gloria Edith Martínez Sierra/ Directora de Gestión Corporativa	Diana Karina Ruiz Perilla Profesional Esp. OAP	Carolina Chica/ Jefe Oficina OAP	19 octubre de 2023