INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL

ALCALDÍA MAYOR
DE BOGOTÁ D.C.
CULTURA, RECREACIÓN Y DEPORTE
Instituto Distrital del Patrimonio Cultural

Manual

Manual de Políticas de Seguridad y Privacidad de la Información

Proceso

Gestión Sistemas de Información y Tecnología

Vigencia: 19 de Noviembre 2021

Versión:2

1. INTRODUCCIÓN

Este documento describe el Manual de Políticas de Seguridad y Privacidad de la Información del Instituto Distrital de Patrimonio Cultural - IDPC, con base en la Norma ISO/IEC 27001:2013 y recomendaciones del Modelo de Seguridad y Privacidad de la Información (MSPI). Las políticas incluidas en este manual hacen parte fundamental del Sistema de Gestión de Seguridad de la Información (SGSI) y se convierten en la base para implantación de los controles, procedimientos y estándares para asegurar la información del Instituto.

Para el Instituto Distrital de Patrimonio Cultural - IDPC, la preservación de la Confidencialidad, Integridad y Disponibilidad de la información es una labor prioritaria y por tanto es responsabilidad de todos los funcionarios, contratistas, colaboradores y proveedores velar por el continuo cumplimiento de las políticas definidas en el presente documento.

2. OBJETIVO

Establecer un manual de políticas de seguridad y privacidad de la información que ayuden a asegurar y garantizar la confidencialidad, integridad y disponibilidad de la información del Instituto de Patrimonio Cultural - IDPC.

3. ALCANCE

Las políticas de seguridad y privacidad de la información se encuentran inmersas en el Sistema de Gestión de Seguridad de la Información – SGSI, las cuales aplican a todos los activos del Instituto Distrital de Patrimonio Cultural, en sus plataformas tecnológicas y procesos.

1. Los activos de información identificados y clasificados en los procesos del Instituto Distrital de Patrimonio Cultural.

2. Los contenedores donde se alojan los activos de Información.

3. Las sedes y oficinas del Instituto Distrital de Patrimonio Cultural.

4. Funcionarios, contratistas, colaboradores y proveedores.

El Sistema de Gestión de Seguridad de la Información - SGSI se encuentra alineado con el ciclo de mejoramiento continuo PHVA, NTC ISO/IEC 27001:2013 y los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI).

4. DEFINICIONES

TÉRMINO	DEFINICIÓN
Activo de Información	Es cualquier elemento que procese información, la almacene o ayude a protegerla, pero, además, que genere valor para la Entidad.
Amenaza	Ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).
Confidencialidad	Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
Contexto	Definición de los parámetros internos y externos (de la Entidad) que se tendrán en cuenta para la gestión del riesgo. El contexto se utiliza para la definición de la Política de gestión del Riesgo.[1]
contraseña	Código secreto que se introduce en una máquina para poder accionar un mecanismo o para acceder a ciertas funciones informáticas.
Control	Acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.
Continuidad del Negocio	Describe los procesos y procedimientos que una organización pone en marcha para garantizar que las funciones esenciales puedan continuar durante y después de un desastre.
Consecuencia	Resultado de un evento que afecta los objetivos. Lo que puede suceder si el riesgo se materializa.
Disponibilidad	Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
Evaluación de riesgos	Proceso de valoración de los riesgos y los controles para conocer el valor de riesgo inherente y posteriormente el riesgo residual.

[1] [Tomado de la norma NTC-ISO 31000. 2. Términos y definiciones 2.9 Establecimiento del contexto.]

Hardware	Se refiere a las partes físicas, tangibles, de un sistema informático; sus componentes eléctricos, electrónicos, electromecánicos y mecánicos
Impacto	consecuencias que genera un riesgo una vez se materialice
Información	Datos organizados de tal forma que tienen un significado
Integridad	Propiedad de la información relativa a su exactitud y completitud.
Internet	Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación.
Intranet	Una intranet es una red informática que utiliza la tecnología del Protocolo de Internet para compartir información, sistemas operativos o servicios de computación dentro de una organización.
Malware	Es un tipo de software que tiene como objetivo infiltrarse o dañar un computador o sistema de información
Monitoreo	Mesa de trabajo anual, la cual tiene como finalidad, revisar, actualizar o redefinir los riesgos de seguridad de la información en cada uno de los procesos, partiendo del resultado de los seguimientos y/o hallazgos de los entes de control o las diferentes auditorías de los sistemas integrados de gestión.
Phishing	Hace referencia a un modelo de abuso informático, que se comete mediante el uso de un tipo de ingeniería social, caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña, información detallada sobre tarjetas de crédito u otra información bancaria).
Probabilidad	Posibilidad de que la amenaza aproveche la vulnerabilidad para materializar el riesgo, en otras palabras, qué tan posible es que el riesgo se materialice.
Recursos Tecnológicos	Elementos de tecnología que pueden ser hardware y/o software, tales como equipos de cómputo, servidores, impresoras, teléfonos, faxes, programas y/o aplicativos de software, dispositivos USB, entre otros.
Respaldo de Información	Es la copia de los datos importantes de un dispositivo primario en uno ó varios dispositivos secundarios, ello para que en caso de que el primer dispositivo sufra una avería electromecánica ó un error en su estructura lógica, sea posible contar con la mayor parte de la información necesaria
Riesgo	Escenario de incertidumbre, bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitándole cumplir con sus objetivos.

Software	Creación intelectual que comprende los programas, los procedimientos, las reglas y cualquier documentación asociada pertinente a la operación de un sistema de procesamiento de datos.
Software Ilegal	El software ilegal es un programa que ha sido duplicado y distribuido sin autorización.
Tecnología de la Información	Hace referencia a las aplicaciones, información e infraestructura requerida por una entidad para apoyar el funcionamiento de los procesos y estrategia de negocio.
Vulnerabilidad	Falencia o debilidad que es inherente a los activos de información o a los controles.
VPN	(Virtual Private Network): es una tecnología de red que permite una extensión segura de la red privada de área local (LAN) sobre una red pública o no controlada como Internet.

5. NORMATIVIDAD

Ley 23 de 1982. Ley sobre derechos de autor

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.

Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado de la protección de la información y de los datos- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1450 de 2011. Por la cual se expide el Plan Nacional de Desarrollo, 2010-2014.

Ley Estatutaria 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales.

Ley 1712 de 2014, Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.

Decreto 1078 de 2015, Por medio del cual se expide el Decreto Único. Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

Resolución Distrital 305 de 2008, Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, caridad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre.

Resolución 004 de 2017, Por la cual se modifica la Resolución 305 de 2008 de la CDS.

Documento CONPES 3701 de 2011 - Lineamientos de Políticas sobre ciberseguridad y ciberdefensa.

Documento CONPES 3854 de 2016 - Política Nacional de Seguridad Digital.

Documento CONPES 3995 de 2020 - Política Nacional De Confianza y Seguridad Digital

NTC/ISO 27001:2013. Sistemas de la Información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

6. POLÍTICAS DE OPERACIÓN

Las políticas contenidas en el presente documento son de obligatorio cumplimiento por parte de todos los servidores públicos, contratistas de prestación de servicios, proveedores y terceros que tengan acceso a la información del Instituto, con el fin de proteger la información del Instituto, desde tres pilares fundamentales, confidencialidad, Integridad y Disponibilidad, lo que facilitará el cumplimiento de los objetivos estratégicos institucionales.

7. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

De acuerdo con lo establecido en la política general de Seguridad y Privacidad de la Información. El Instituto Distrital de Patrimonio Cultural se compromete a implementar, mantener y mejorar la seguridad y privacidad de la información, mediante una adecuada gestión de activos, riesgos e incidentes de seguridad de la información; con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de la información y los datos.

La Alta Dirección de la Entidad demostrará su compromiso a través de:

- La promoción activa de una cultura de seguridad.
- Facilitar la divulgación de este documento a todos los subdirectores, funcionarios, contratistas de la Entidad.
- El aseguramiento de los recursos adecuados para implementar y mantener la Política General de Seguridad de la Información

7.1 REGULACIÓN

La Política General de Seguridad de la Información contenida en este documento deberá ser conocida, aceptada y cumplida por todos los jefes de oficina, funcionarios, contratista del Instituto Distrital de Patrimonio Cultural. El incumplimiento de estas se considerará un incidente de seguridad, que de acuerdo con el caso podrá dar lugar a un proceso disciplinario para los funcionarios, y se podrá convertir en un incumplimiento del contrato respecto de los contratistas, que pueda dar lugar a la imposición de sanciones e incluso su terminación, sin perjuicio de la iniciación de otro tipo de acciones a las que haya lugar según la legislación vigente.

7.2 RESPONSABLES

- La Alta Dirección, jefes de Oficina, funcionarios, contratistas, terceros y todos los servidores públicos del Instituto Distrital de Patrimonio Cultural.
- Servidores Públicos de Órganos de Control y/o Entidades Gubernamentales que en cumplimiento de su función hagan uso de las tecnologías a las cuales aplica la presente Política.
- Terceros que utilicen equipos y herramientas informáticas propiedad de la entidad.

8. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

Con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de información, el IDPC establece el presente manual de políticas de seguridad de la información, las cuales son de obligatorio cumplimiento de acuerdo con el capítulo anterior.

8.1 Políticas para dispositivos móviles

El Instituto Distrital de Patrimonio Cultural establece la política para el uso y manejo de dispositivos móviles (teléfonos inteligentes y tabletas), y aplica tanto para los dispositivos

suministrados por el IDPC, como para los dispositivos personales en los que se consulte o almacene información de la Entidad teniendo en cuenta:

Se debe configurar un método para el bloqueo de la pantalla (PIN, Contraseña, etc) en el dispositivo móvil, para controlar el acceso de personas no autorizadas.

No se deben instalar aplicaciones de origen desconocido.

En caso de hallar algún malware y/o virus en los dispositivos móviles asignados por el IDPC debe reportarlo a través del Proceso de Gestión de Sistemas de Información y Tecnología. Para los usuarios que utilizan sus propios dispositivos y que hallaron algún malware o virus en él, deberán garantizar la eliminación de la amenaza, o la eliminación de la cuenta de correo e información institucional contenida en el dispositivo.

Se debe realizar la conexión a redes inalámbricas conocidas y evitar la conexión a redes públicas o de tipo libre.

Al terminar la relación contractual o laboral, el dispositivo móvil deberá ser sometido a un proceso de desvinculación de los servicios institucionales, así como el retiro de permisos, privilegios y configuraciones realizadas sobre dicho dispositivo.

8.2 Políticas de teletrabajo

El Instituto Distrital de Patrimonio Cultural establece esta política para las conexiones que se realizan a los servicios tecnológicos del Instituto, a través de una red pública como internet y desde lugares remotos, como por ejemplo los hogares de los colaboradores.

La conexión remota segura constituye un elemento técnico dentro de la modalidad de teletrabajo o trabajo en casa, razón por la cual todos los servidores públicos, contratistas o terceros que han sido autorizados a realizar sus actividades bajo esta modalidad deben saber que los servicios de TI serán controlados, restringidos y monitoreados tal como si estuviesen en cualquiera de las sedes físicas de la entidad.

Se prohíbe el ingreso a través de cualquiera de las aplicaciones de libre distribución para acceso remoto (Teamviewer, Weezo, AMMYY, RealVNC, LogMeIn, AnyDesk entre otros), sin la debida autorización del Instituto.

Las conexiones remotas hacia la red o los servicios informáticos del Instituto se deben realizar mediante servicios seguros, tal como una VPN.

8.3 Políticas de seguridad de los recursos humanos

La siguiente política tiene como propósito reducir los riesgos de error humano, robo, fraude, ingeniería social y utilización indebida de los equipos, mediante la formación, capacitación y sensibilización de la seguridad de la información, para tal fin se tiene en cuenta:

El IDPC comprobará los antecedentes de los funcionarios, contratistas y terceros, para verificar la identidad, idoneidad, ética profesional y conducta del personal.

A cada funcionario, contratista o tercero que tenga acceso a la información del IDPC se le debe hacer firmar un acuerdo confidencialidad, el cual debe ir más allá de la finalización de la relación laboral o contractual, este término de tiempo se define dependiendo del tipo de activo de información al que tendrá acceso cada persona.

Los funcionarios y contratistas deben asistir a las capacitaciones, charlas e inducciones acerca de la seguridad de la información, las cuales deberán ser coordinadas y ejecutadas entre el Proceso de Gestión de Sistemas de Información y Tecnología y Talento Humano

8.4 Política de criptografía

Teniendo en cuenta la información de acuerdo con su clasificación y criticidad, normatividad vigente aplicable (Ley 1712 de 2014) y/o acuerdos contractuales, debe estar protegida con mecanismos de cifrado, contemplando y sin limitarse a:

- Información transmitida por canales de comunicación.
- Información contenida en medios de almacenamiento (USB, Discos, CDs, DVDs, Cintas, otros).
- Copias de Respaldo.
- Información propia del IDPC transmitida a otras entidades.
- Información propia de la entidad correspondiente a ideas, estrategias, conceptos, propuestas, costos e información contable en general, cuando sea transmitida a destinatarios externos a la compañía.
- Información que se tenga almacenada en los datacenter internos o externos (datacenter, proveedores, cloud).
- Las páginas web publicadas a Clientes o en Internet deberán contar con certificado digital.

Para garantizar lo anterior se debe identificar qué información debe ser cifrada y proteger la misma, ya sea incluyéndola en un archivo protegido por una contraseña ó utilizando un software que permita su resguardo mediante la aplicación de un algoritmo de cifrado robusto.

8.5 Política de gestión de usuarios

Los responsables y/o dueños de la información deben determinar las reglas de control de acceso apropiadas de acuerdo con las actividades que desarrolla cada uno de los funcionarios, según su rol dentro de la entidad y evaluando los riesgos asociados al uso de esta. Por lo tanto, son ellos quienes autorizan o retiran los permisos para el uso de un activo de información teniendo en cuenta lo establecido en:

- Los procedimientos de control de acceso físico definidos.
- El acceso a servidores, bases de datos, Internet, correo electrónico y aplicaciones deben realizarse bajo los lineamientos definidos y establecidos por el Proceso de Gestión de Sistemas de Información y Tecnología.
- La administración de usuarios debe realizarse bajo los lineamientos definidos por el Proceso de Gestión de Sistemas de Información y Tecnología.
- Se debe garantizar en las plataformas de tecnología que el ingreso a la administración en lo posible se realice con la vinculación directamente de las credenciales de los usuarios de directorio activo.
- Los usuarios SuperAdministradores y sus correspondientes contraseñas a las consolas administrables se dejan en custodia en sobre sellado y digitalmente en un gestor de contraseñas en un área segura, las credenciales allí contenidas deben ser modificadas de manera frecuente o cuando amerite ante una amenaza de compromiso de estas.
- Todas las contraseñas utilizadas por usuarios y administradores de sistemas deben cumplir con los lineamientos definidos por el Proceso de Gestión de Sistemas de Información y Tecnología.
- La interconexión con redes externas debe ser configurada bajo los lineamientos definidos por el Proceso de Gestión de Sistemas de Información y Tecnología.

Para la implementación de controles de acceso que no estén descritos en este documento, se tendrá como referencia la legislación vigente aplicable a la SuperVigilancia y la necesidad de conocer.

Todos los funcionarios, contratistas o terceros que tengan acceso a la infraestructura tecnológica o a los sistemas de información de la entidad, deben contar con una definición clara de los roles y funciones sobre estos para reducir y evitar el uso no autorizado o modificación no intencional sobre los activos de información.

La segregación de funciones sobre la infraestructura tecnológica y sobre los sistemas de información deberá ser revisada periódicamente por el Proceso de Gestión de Sistemas de Información y Tecnología con el fin de mantener actualizada dicha información y acorde con la realidad de cada una de las dependencias del IDPC.

Los usuarios son responsables de realizar un adecuado uso de las herramientas de seguridad y de las actividades realizadas con sus cuentas de usuario o mecanismos de autenticación asignados que se ponen a su disposición.

8.6 Políticas gestión de activos

En el IDPC la información estará clasificada dentro los niveles definidos y se deberá mantener un inventario actualizado de los activos de información que facilite el uso aceptable, la manipulación correcta y adecuada de los mismos, entendiéndose como “activos de información”, aquellos elementos que pueden contener, procesar o proteger información relevante o de valor para el Instituto, para lo cual se tiene en cuenta:

La identificación de los activos de información por parte de funcionarios y contratistas se debe realizar mínimo una vez al año, o cuando se identifiquen cambios significativos en alguno de los procesos. Esta actividad se deberá realizar en los instrumentos que disponga la entidad.

La clasificación de los activos de información se realizará de acuerdo con la metodología de activos de información de la entidad y demás lineamientos y leyes como la Ley 1712 de 2014 y la Ley 1581 de 2012.

Una vez terminada la vinculación laboral o contractual cada funcionario o contratista realizara la respectiva devolución de sus activos de información.

Las unidades de medios removibles (CD´s, memorias y/o pendrive USB, discos duros) se encuentran restringidas en las áreas que gestionan información clasificada o reservada.

Ningún funcionario o contratista podrá compartir archivos o carpetas de un equipo de cómputo a otro sin la respectiva autorización del Proceso de Gestión de Sistemas de Información y Tecnología o del jefe de cada dependencia.

8.6.1 Gestión de activos de Información

- El IDPC tiene la custodia sobre todo dato, información y mensaje generado, procesado y contenido por sus sistemas de cómputo, así como también de todo aquello transmitido a través de su red de telecomunicaciones o cualquier otro medio de comunicación físico o electrónico y se reserva el derecho de conceder el acceso a dicha información.

- El IDPC debe identificar los activos asociados a cada sistema de información, sus respectivos propietarios y su ubicación a fin de elaborar y mantener un inventario actualizado de los activos de información.

- El IDPC debe realizar la clasificación y control de activos con el objetivo de garantizar que los mismos reciban un apropiado nivel de protección, clasificar la información para señalar su sensibilidad y criticidad y definir los niveles de protección y medidas de tratamiento, evaluando las tres características de la información en las cuales se basa la Seguridad de la Información: confidencialidad, integridad y disponibilidad.

- El IDPC deberá definir procedimientos para el rotulado y manejo de información de acuerdo con el esquema de clasificación definido.

8.6.2 Competencias mínimas para el manejo de información sensible

El I En el Instituto Distrital de Patrimonio Cultural, la información se encuentra asociada o contenida en los activos de información que ha identificado la entidad, con base en la clasificación y el análisis de riesgos se identifican controles para proteger la información allí contenida-

Dentro de los controles propuesto se establece los criterios que se deben tener en cuenta por parte de los funcionarios y contratistas es las competencias mínimas para manipular la información sensible.

Para ello se deben tener en cuenta los siguientes aspectos:

- Conocer y entender la ley 1712 de 2014 y las actualizaciones que se hayan presentado a la misma.
- Haber realizado el proceso de contratación definido por la entidad aportando los soportes requeridos de acuerdo con el rol o cargo a desempeñar.
- Información académica relacionada con los criterios mínimos para desempeñar el cargo
- Tener conocimiento de proceso de gestión documental y las tablas de retención documental definidas por la entidad.
- Tener los conocimientos necesarios que permitan garantizara que la información asociada a su cargo o rol desempeñado se encuentra bien catalogada.
- Conocer las políticas de seguridad de la información (debe asistir a las capacitaciones que se programen de acuerdo con la temática a tratar y estar pendiente de las últimas modificaciones o actualizaciones de dicha política.)
- Tener conocimiento de la ley de protección de datos personales de la entidad y de la normatividad asociada.
- Cumplir con el código de tica de la entidad.
- Firmar el acuerdo de confidencialidad definido por le entidad

Adicional a lo mencionado anteriormente debe asegurarse que los activos de información que se encuentren bajo su responsabilidad cuenten con todos los controles de que permitan garantizar la confidencialidad, la integridad y la disponibilidad d ellos mismos.

Finalmente debe reportar al oficial de seguridad de la información o que ejecute sus funciones todo evento o incidente que ponga en riesgo los activos o la información sensible que se encuentre a su cargo.

8.6.3 Uso de recursos tecnológicos

El Instituto Distrital de Patrimonio Cultural asignará diferentes recursos tecnológicos como herramientas de trabajo para uso exclusivo de sus funcionarios y contratistas autorizados.

El uso adecuado de estos recursos se reglamenta bajo las siguientes políticas:

La instalación de cualquier tipo de software en los equipos de cómputo del IDPC, debe ser realizada por el Proceso de Gestión de Sistemas de Información y Tecnología y por tanto son los únicos autorizados para realizar esta labor.

Los usuarios no deberán realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz, protector de pantalla corporativo o traslado de hardware. Estos cambios podrán ser realizados únicamente por las oficinas autorizadas.

El Proceso de Gestión de Sistemas de Información y Tecnología definirá la lista actualizada de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios; así mismo, realizará el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.

Sólo personal autorizado podrá realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información del IDPC; las conexiones establecidas para este fin utilizarán los esquemas de seguridad definidos.

Está expresamente prohibido el consumo alimentos y bebidas en el puesto de trabajo y más aún, sobre el computador (incluyendo su teclado y/o mouse).

El usuario debe evitar usar CD, DVD o memorias o discos extraíbles USB de fuentes desconocidas, y si es necesario hacer uso de estos medios, primero deberá revisarlos con el programa de Antivirus, para ello debe pedir apoyo del Proceso de Gestión de Sistemas de Información y Tecnología.

Los funcionarios de la entidad son responsables de hacer buen uso de los recursos tecnológicos del IDPC y en ningún momento podrán ser usados para beneficio propio o para realizar prácticas ilícitas o malintencionadas que atenten contra otros funcionarios, terceros, el Instituto en sí mismo, la legislación vigente y las políticas y lineamientos de seguridad de la información del IDPC.

8.6.4 Trabajo en Áreas Protegidas

- En las áreas donde se encuentren activos informáticos, se debe cumplir como mínimo con los siguientes lineamientos:
    - No se deben consumir alimentos ni bebidas.
    - No se deben ingresar elementos inflamables.
    - No se debe permitir el acceso de personal ajeno sin que este acompañado por un funcionario durante el tiempo que dure su visita.
    - No se deben almacenar elementos ajenos a la funcionalidad de la respectiva zona segura.
    - No se permite tomar fotos o grabaciones de las áreas seguras sin la previa autorización del área responsable de cada una de ellas.
    - No se permite el ingreso de equipos electrónicos, así como maletas o contenedores, a menos que haya una justificación para esto. En ese caso, deberán ser registradas al ingreso y salida para minimizar la posibilidad de ingreso de elementos no autorizados o la extracción de elementos.
- Las áreas protegidas deben contar con las condiciones ambientales que garanticen la correcta operación de los equipos y el estado de los medios que contienen información, así como un sistema de detección y control de incendios.

8.7 Políticas control de acceso

Esta política determina los mecanismos de protección, los límites y procedimientos frente a la administración y responsabilidad, relacionados con los accesos a la información.

El IDPC suministrará a los usuarios las claves respectivas para el acceso a los servicios tecnológicos a los que hayan sido autorizados, las claves son de uso personal e intransferible.

Ningún usuario deberá acceder a la red o a los servicios TIC del IDPC, utilizando las credenciales de otro usuario.

El cambio de contraseña sólo podrá ser solicitado por el titular de la cuenta, comunicándose a la extensión del Proceso de Gestión de Sistemas de información y Tecnología, en donde se llevará a cabo la validación de los datos personales; en caso de ser solicitado el cambio de contraseña para otra persona. Solo se podrá mediante orden judicial.

La conexión remota a la red de área local del IDPC debe ser hecha a través de una conexión VPN segura suministrada por el Instituto, la cual debe ser aprobada, registrada y auditada. El acceso a cualquier servicio, servidor o sistema de información debe ser autenticado y autorizado.

Se debe suspender temporalmente el acceso a los servicios de TI cuando un funcionario está disfrutando de sus vacaciones, de licencias remuneradas o no remuneradas, o en caso de sanción disciplinaria. Por otro lado, el acceso a los servicios de TI será desactivados de manera inmediata y definitiva, a partir de la fecha en la cual la persona termine oficialmente su vinculación con la entidad o cuando la dependencia deje de existir, o por solicitud del jefe de la dependencia correspondiente.

Se debe suspender temporalmente el acceso a los servicios de TI cuando un contratista de prestación de servicios pide la suspensión de su contrato.

8.7.1 Gestión de contraseñas

Se debe garantizar en las plataformas de tecnología que el ingreso a la administración en lo posible se realice con la vinculación directamente de las credenciales de los usuarios de 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.

El personal del Proceso de Gestión de Sistemas de Información y Tecnología no debe dar a conocer su clave de usuario a terceros de los sistemas de información, si algún tercero requiere acceder a los sistemas informáticos del Instituto, se le deberán generar nuevas credenciales de acceso adecuadas.

El personal del Proceso Gestión de Sistemas de Información y Tecnología debe emplear obligatoriamente claves o contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación fuerte que posee la entidad de acuerdo con el rol asignado.

De acuerdo con lo anterior el IDPC establece las siguientes condiciones para la gestión de las contraseñas:

Longitud mínima de contraseña: La contraseña debe tener una longitud mínima de 12 caracteres alfanuméricos

Expiración de la contraseña: El tiempo de expiración (cambio de contraseñas) debe ser máximo cada 60 días calendario

Vigencia de la contraseña: Una contraseña deberá tener una vigencia mínima de 2 días, antes de que se pueda volver a cambiar.

Historial de contraseñas: 5 contraseñas recordadas, definiendo cuantas veces debe ser cambiada una contraseña para poder volver a utilizarla.

Bloqueo de cuenta: Intentos que el usuario intenta ingresar una contraseña sin ser bloqueado. Para lo cual se define 3 intentos de ingreso de contraseña, después del cuarto intento se bloquea el usuario.

Tiempo de inactividad: Aplica cuando un usuario no hacer uso d ele los recursos. Después de 30 días si un usuario no utiliza la cuenta será inactivada.

Desconexión de sesión: El tiempo de desconexión estará configurado a 2 minutos, asociados al bloqueo de pantalla.

8.7.2 Carpetas de red, discos de red, carpetas virtuales

Para que los usuarios tengan acceso a la información ubicada en los discos o carpetas de red, el subdirector, jefe de oficina o Asesor deberá enviar un correo autorizando el acceso y permisos, correspondientes al rol y funciones a desempeñar al Proceso de Gestión de Sistemas de Información y Tecnología del IDPC. Los usuarios tendrán permisos de escritura, lectura o modificación de información en los discos o carpetas de red, dependiendo de sus funciones y su rol.

La información almacenada en cualquiera de los discos o carpetas de red debe ser de carácter institucional.

Está prohibido almacenar archivos con contenido que atente contra la moral y las buenas costumbres del Instituto o las personas, como pornografía, propaganda racista, terrorista o cualquier software ilegal o malicioso.

Se prohíbe extraer, divulgar o publicar información de cualquiera de los discos o carpetas de red sin expresa autorización del subdirector o Jefe de Oficina de la dependencia correspondiente.

Se prohíbe el uso de la información de los discos o carpetas de red con fines publicitarios, de imagen negativa, lucrativa o comercial.

8.8 Políticas seguridad física y del entorno

Las siguientes políticas tienen como propósito impedir el ingreso no autorizado, deterioro y perturbación de la infraestructura tecnológica, las instalaciones y los datos, teniendo en cuenta:

Se debe contar con un área de recepción y/o vigilancia para controlar el acceso físico a las sedes, escenarios, y áreas seguras (restringidas) del IDPC.

Debe haber un listado con las personas autorizadas a ingresar a la sala de cómputo y a los centros de cableado, que estará a cargo del jefe del Proceso de Gestión de Sistemas de Información y Tecnología.

Los equipos ubicados en el centro de cómputo (Data Center) y centros de cableado deben estar protegidos de amenazas potenciales de orden físico.

Está prohibido en el centro de cómputo y cuartos de comunicaciones (servidores) fumar, ingerir bebidas alcohólicas o cualquier tipo de estupefaciente.

Está prohibido que terceros, como personal de mantenimiento, auditores o contratistas de suministro tomen fotografías del centro de cómputo.

La dependencia de bienes e infraestructura es la encargada por la seguridad física.

8.8.1 Política de escritorio y pantalla limpia

Se entiende por escritorio, el puesto de trabajo de cada funcionario o contratista de prestación de servicios e incluye la mesa principal donde se ubica el computador.

Sobre el escritorio solamente deben estar los documentos con los cuales está trabajando.

Procure no tener en el puesto de trabajo fotografías personales o portarretratos digitales con imágenes que puedan suministrar información sobre sus hábitos o su familia (sus nombres entre otros).

Los funcionarios y contratistas deben evitar tener archivos y carpetas en la pantalla principal del computador (Escritorio).

Cuando un usuario se ausente de su computador de trabajo, debe realizar el bloqueo de la sesión.

No se deben escribir las contraseñas en las notas rápidas del escritorio, mantenerlas a la vista de los demás usuarios, ni escribirlas en documentos físicos.

8.9 Políticas transferencia de información

Toda transferencia de información perteneciente al IDPC a la cual se tenga acceso por razones técnicas o comerciales debe ser susceptible de trazabilidad.

El IDPC, en caso de tener un servicio de transferencia de archivos deberá realizarlo empleando protocolos seguros. Cuando el origen sea el IDPC hacia entidades externas, el IDPC establecerá los controles necesarios para preservar la seguridad de la información; cuando el origen de la transferencia sea una entidad externa, se acordarán las políticas y controles de seguridad de la información con esa entidad. En todo caso se deben revisar y proponer controles en concordancia con las políticas de seguridad de la información del IDPC;

los resultados de la revisión de requerimientos de seguridad se documentarán y preservarán para futuras referencias o para demostrar el cumplimiento con las políticas y con los controles de seguridad del IDPC.

Los usuarios de las Subdirecciones y Oficinas del IDPC no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red del Instituto, sin la autorización de la Subdirección de Gestión Corporativa.

La Oficina Asesora Jurídica del IDPC debe establecer en los contratos que se creen con los funcionarios y contratistas, los Acuerdos de Confidencialidad o Acuerdos de intercambio dejando explícitas las responsabilidades y obligaciones legales asignadas por la divulgación no autorizada de información de beneficiarios del instituto que les ha sido entregada en razón del cumplimiento de los objetivos misionales del IDPC.

No está permitido el intercambio de información clasificada o reservada del instituto por vía telefónica o mensajería instantánea.

Los propietarios de los activos de información deben asegurar la validación y garantizar que el Intercambio de información solamente se realice si se encuentra autorizada y dando cumplimiento a las Políticas de Seguridad.

Los propietarios de los activos de información deben velar porque la información del IDPC sea protegida de divulgación no autorizada por parte de los terceros a quienes se entrega esta información, verificando el cumplimiento de las cláusulas relacionadas en los contratos, Acuerdos de confidencialidad o Acuerdos de intercambio establecidos.

8.10 Políticas de copias de respaldo

Proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y el software, se pueda recuperar después de una falla, garantizando que la información y la infraestructura de software crítica de la entidad, sean respaldadas y puedan ser restauradas en caso de una falla y/o desastre.

El administrador de los servidores, los sistemas de información o los equipos de comunicaciones, es el responsable de definir la frecuencia de respaldo y los requerimientos de seguridad de la información y el asignado por el subdirector de gestión corporativa es el responsable de realizar los respaldos periódicos.

Las copias de respaldo se guardarán únicamente con el objetivo de restaurar el sistema luego de un virus informático, defectos en los discos de almacenamiento, problemas de los servidores o computadores, materialización de amenazas, catástrofes y por requerimiento legal.

Cada usuario final es responsable de realizar la copia de seguridad de su información laboral en las carpetas destinadas para este fin.

La Subdirección de Gestión Corporativa debe mantener un inventario actualizado de las copias de respaldo de la información y los aplicativos o sistemas del IDPC.

Los medios que vayan a ser eliminados deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada.

Es responsabilidad de cada dependencia mantener depurada la información de las carpetas de red para la optimización del uso de los recursos de almacenamiento que entrega el IDPC a los usuarios.

8.11Políticas seguridad en las operaciones

Las siguientes políticas tienen como propósito garantizar el funcionamiento seguro de equipos y dispositivos usados para el manejo, procesamiento y almacenamiento de la información.

Los servidores, equipos activos y demás componentes son administrados por el Proceso de Gestión de Sistemas de Información y tecnología.

El Proceso de Gestión de Sistemas de Información y Tecnología debe aplicar de forma obligatoria las actualizaciones a sistemas operativos y/o aplicaciones de los servidores que tengan relaciones con posibles vulnerabilidades de seguridad.

El Proceso de Gestión de Sistemas de Información y tecnología debe sincronizar la infraestructura tecnológica con la hora legal para Colombia.

El IDPC debe implementar herramientas para la detección, bloqueo y eliminación de virus, malware y demás software malicioso.

El Antivirus corporativo debe estar operativo en todos los computadores y servidores del Instituto en todo momento.

Los equipos de cómputo de terceros que son autorizados para conectarse a la red de datos del IDPC deben tener antivirus y contar con las medidas de seguridad mínimas.

No descargar programas (software) o archivos de sitios desconocidos o con mala reputación, ni del correo, cuando se trata de remitentes desconocidos o el contenido es sospechoso.

El Proceso de Gestión de Sistemas de Información y Tecnología debe implementar procedimientos y adquirir las herramientas necesarias para la supervisión y monitoreo de la infraestructura de TI y sistemas de información.

El Proceso de Gestión de Sistemas de Información y tecnología debe formular y aplicar una metodología de rotación de eventos (logs). Así como la asignación del espacio para su almacenamiento, de acuerdo con la capacidad de los recursos tecnológicos involucrados

Los responsables o líderes de los procesos y dependencias son los responsables de la información producida o manejada en dichos procesos, así como del manejo que se le dé a la misma.

8.12 Política de seguridad de las comunicaciones

8.12.1 Uso de internet

La navegación en Internet debe realizarse de forma razonable y con propósitos laborales.

No se permite la navegación a sitios con contenidos contrarios a la ley o a las políticas del IDPC o que representen peligro para el Instituto como: pornografía, terrorismo, hacktivismo, segregación racial u otras fuentes definidas por el IDPC.

La descarga de archivos de Internet debe ser con propósitos laborales y de forma razonable para no afectar el canal de servicio de Internet.

8.12.2 Uso de correo electrónico

Los usuarios del correo electrónico corporativo son responsables de evitar prácticas o usos del correo que puedan comprometer la seguridad de la información.

Los servicios de correo electrónico corporativo se emplean para servir a una finalidad operativa y administrativa en relación con el instituto.

Todos los correos electrónicos procesados por los sistemas, redes y demás infraestructura TIC del IDPC se consideran bajo el control del Instituto.

Cada subdirector o Jefe de Oficina deberá solicitar la creación de las cuentas de correo electrónico por medio de la Mesa de Ayuda.

El área de Talento Humano para funcionarios de planta y temporales y el respectivo subdirector para los contratistas del IDPC son los responsables de solicitar la modificación o cancelación de las cuentas electrónicas al proceso de Gestión de Sistemas de Información y Tecnología del IDPC.

El envío de cadenas de correo, envío de correos masivos con archivos adjuntos de gran tamaño que puedan congestionar la red, no está autorizado.

No está autorizado, el envío de correos con contenido que atenten contra la integridad y dignidad de las personas y el buen nombre del Instituto.

Cuando un funcionario, contratista o colaborador al que le haya sido autorizado el uso de una cuenta de correo electrónico y se retire del IDPC, su cuenta de correo será desactivada y conservada para futuras referencias.

Las cuentas de correo electrónico son propiedad del IDPC, las cuales son asignadas a personas que tengan algún tipo de vinculación laboral con el instituto, ya sea como personal de planta, contratistas, consultores o personal temporal, quienes deben utilizar este servicio única y exclusivamente para las tareas propias de la función desarrollada en el Instituto y no debe utilizarse para ningún otro fin.

Cada usuario es responsable del contenido del mensaje enviado y de cualquier otra información adjunta al mismo.

Todos los mensajes pueden ser sujetos a análisis y conservación permanente por parte del Instituto.

Todo usuario es responsable por la destrucción de los mensajes cuyo origen sea desconocido y por lo tanto asumirá la responsabilidad y las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En estos casos no se debe contestar dichos mensajes, ni abrir los archivos adjuntos y se debe reenviar el correo a la cuenta sistemas@idpc.gov.co con la frase "correo sospechoso" en el asunto.

8.13 Políticas adquisición, desarrollo y mantenimiento de sistemas

Esta política aplica durante la adquisición, desarrollo y mantenimiento de soluciones de software y permite brindar seguridad a todos los componentes que se van generando durante el ciclo de vida de desarrollo.

Se debe utilizar una metodología de desarrollo seguro, y además requerirla a las empresas con quienes se contrate el servicio de desarrollo de software.

Para dar viabilidad a las solicitudes de desarrollo y actualización de software se debe tener en cuenta los recursos técnicos, financieros y humanos disponibles en el instituto

En caso de que la solicitud de desarrollo y actualización de software requiera la contratación de un tercero, esta será coordinada por el Proceso de Gestión de Sistemas de Información y Tecnología con el acompañamiento del área u oficina que hace el requerimiento.

El equipo de desarrollo en conjunto con el usuario funcional debe definir los requerimientos de desarrollo según las características de la solicitud.

La documentación es construida a lo largo del proceso de desarrollo y actualización de software y es entregada al final de las pruebas.

El control de versiones del código fuente se debe hacer por medio de un repositorio centralizado que se encuentre en los servidores administrados por el instituto.

Los contratos de desarrollo de software deben ser supervisados por el responsable del Proceso de Gestión de Sistemas de Información y Tecnología.

Se deben realizar pruebas de seguridad en las aplicaciones, teniendo en cuenta las recomendaciones del proyecto abierto de seguridad de aplicaciones web – OWASP.

8.14 Políticas relaciones con los proveedores

La Oficina Asesora Jurídica del IDPC debe definir los modelos de Acuerdos de Confidencialidad y/o de Intercambio de Información entre el instituto y proveedores incluyendo los compromisos adquiridos y las penalidades civiles o penales por el incumplimiento de dichos acuerdos.

Los Supervisores de contratos deben monitorear periódicamente, el cumplimiento de los Acuerdos de Niveles de Servicio, Acuerdos de Confidencialidad, Acuerdos de Intercambio de información y los requisitos de Seguridad de la Información de parte de los terceros proveedores de servicios.

8.14.1 Tercerización u outsourcing

Mantener la seguridad de la información y los servicios de procesamiento de información, a los cuales tienen acceso terceras partes, entidades externas o que son procesados, comunicados o dirigidos por estas.

Se deben establecer criterios de selección que contemplen la experiencia y reputación de terceras partes, certificaciones y recomendaciones de otros clientes, estabilidad financiera de la compañía, seguimiento de estándares de gestión de calidad y de seguridad y otros criterios que resulten de un análisis de riesgos de la selección y los criterios establecidos por la entidad.

Se deben 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 del IDPC, las cuales deben se divulgadas por los funcionarios responsables de la realización y/o firma de contratos o convenios.

El proceso de Gestión de Sistemas de Información y Tecnología deberá mitigar los riesgos de Seguridad y privacidad de la información teniendo en cuenta lo definido en el Manual de Gestión de Riesgos del IDPC.

Se debe identificar y monitorear los riesgos relacionados con los contratistas o proveedores en relación con los objetos contractuales, incluyendo la cadena de suministro de los servicios de tecnología y comunicación.

Los funcionarios del IDPC que se asignen 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.

Se deben establecer mecanismos o condiciones con los contratistas o proveedores que permitan realizar la gestión de cambios en los servicios suministrados.

8.15 Políticas gestión de incidentes

El personal del IDPC y los terceros que tengan acceso a la información institucional, deberán reportar cualquier evento o incidente relacionado con la seguridad de los datos o de la información institucional, para lo cual podrán utilizar el mismo método que se emplea para el reporte de casos de tecnología.

El Oficial de Seguridad de la Información deberá realizar la clasificación y asignación de responsables para la atención de cada evento o incidente reportados.

Para iniciar la investigación de un evento o incidente de seguridad de la información reportado, se tomarán en cuenta los reportes, alarmas, alertas o notificaciones manuales o de algún sistema o dispositivo que indiquen mal uso o mal funcionamiento del activo de información.

8.16 Políticas cumplimiento

Los funcionarios, contratistas y terceros deben cumplir siempre con la legislación vigente, las políticas, normas, directrices y controles internos establecidos en el Instituto, en lo que tiene que ver con la seguridad de la información.

Los monitoreos de la red efectuados por personas no autorizadas representan una seria amenaza a la disponibilidad, integridad y confidencialidad de la información y a los recursos de cómputo, por lo tanto, esta situación debe evitarse.

Se debe asegurar la privacidad y la protección de datos personales, como se exige legalmente en Colombia de acuerdo con la Ley estatutaria 1581 de 2012.

8.16.1 Cumplimiento de propiedad intelectual de software

Se deben realizar campañas de sensibilización respecto al cumplimiento de derechos de propiedad intelectual, en las cuales se informe la intención de tomar acciones disciplinarias contra el personal que las incumpla.

El IDPC mantendrá la propiedad intelectual de cualquier producto o servicio que haya sido desarrollado en el marco de la labor de sus funcionarios y/o contratistas.

El IDPC instalará los programas que han sido adquiridos legalmente en los equipos asignados en las cantidades requeridas para suplir las necesidades. El uso de programas sin su

respectiva licencia y autorización del IDPC (imágenes, vídeos, software o música), obtenidos a partir de otras fuentes (internet, dispositivos de almacenamiento externo), puede implicar amenazas legales y de seguridad de la información para el Instituto, por lo que esta práctica no está autorizada.

Todo el software usado en la plataforma tecnológica del IDPC debe tener su respectiva licencia y acorde con los derechos de autor.

Los programas instalados en los equipos son de propiedad del IDPC, la copia no autorizada de programas o de su documentación, implica una violación a la política general del IDPC. Aquellos funcionarios, contratistas o demás colaboradores que utilicen copias no autorizadas de programas o su respectiva documentación, quedarán sujetos a las acciones disciplinarias establecidas por el IDPC o las sanciones que especifique la ley.

El IDPC se reserva el derecho de proteger su buen nombre y sus inversiones en hardware y software, fomentando controles internos para prevenir el uso o la realización de copias no autorizadas de los programas de propiedad del Instituto. Estos controles pueden incluir valoraciones periódicas del uso de los programas, auditorías anunciadas y no anunciadas.

Los recursos tecnológicos y de software asignados a los funcionarios del IDPC son responsabilidad de cada funcionario y/o Contratista.

Los usuarios solo tendrán acceso a los datos y recursos autorizados por el IDPC, y serán responsables disciplinaria y legalmente de la divulgación no autorizada de esta información.

Es responsabilidad de cada usuario proteger la información que está contenida en documentos, formatos, listados, etc., los cuales son el resultado de los procesos informáticos; adicionalmente se deben proteger los datos de entrada de estos procesos.

9. CONTROL DE CAMBIOS

Fecha	Versión	Cambios Introducidos	Simplificación o mejora	Origen
24/03/2021	01	Creación del documento.	Mejora	Norma ISO/IEC 27001:2013
12-11-2021	02	Actualización, se agrega las políticas de Gestión de Usuarios, Gestión de activos y criptografía, se incluye el numeral 8.6.2 que establece las competencias mínimas para el manejo de información sensible	Mejora	Norma ISO/IEC 27001:2013

10. CRÉDITOS

Elaboró	Revisó	Aprobó
Eusebio Cordero Orjuela Contratista – Oficial de Seguridad de la Información Subdirección de Gestión Corporativa Carlos Mario Santos Pinilla Contratista- Oficina Asesora de Planeación- Acompañamiento	Mary Rojas Contratista – Líder TI Subdirección de Gestión Corporativa	Juan Fernando Acosta Mirkow Subdirector de Gestión Corporativa
Aprobado	Comité Institucional de Gestión y Desempeño del 12/11/2021	