Políticas operativas específicas de seguridad y privacidad de la información

Código SG/MIPG	127-PPPGI-08
Vigencia desde	27/12/2022
Versión	2

Proceso

Gestión de la Información y la Tecnología

ALCALDÍA MAYOR DE BOGOTÁ D.C.
DEPARTAMENTO ADMINISTRATIVO DE LA DEFENSORÍA DEL ESPACIO PÚBLICO
BOGOTÁ

Tabla de contenido

1. INTRODUCCIÓN

La información en sus múltiples ubicaciones (On premise o Cloud (Nube), medios y formas, así como los trámites y servicios que la Defensoría del Espacio Público provee a los usuarios y ciudadanos es el activo más importante y se considera un bien público, por consiguiente, los activos de información que conforman los bienes y servicios que proveen el DADEP son activos públicos y, por lo tanto, deben ser protegidos adecuadamente.

La protección de los activos de información, parten del concepto de seguridad de la información la cual comprende el conjunto de medios, procesos, procedimientos y controles establecidos para el manejo, gestión y control de la información durante el ciclo de vida de esta, para preservar su confidencialidad, integridad, y disponibilidad.

La Oficina de Tecnología de la Información y las Comunicaciones - OTIC del DADEP, consciente de que la seguridad informática se fundamenta en un conjunto de políticas que brindan instrucciones claras y lineamientos para definir estándares y procedimientos que aseguren que la información en cada uno de los procesos de la entidad cumplan con los criterios de confidencialidad, integridad y disponibilidad, ha venido trabajando para asegurar la custodia, la protección frente a accesos no autorizados, el control de acceso a otros sitios web y la adecuada utilización del correo electrónico de la Entidad. De igual manera, proporcionando hardware, software y equipos de comunicaciones, realizando revisiones periódicas de seguridad, y promoviendo el buen uso de los sistemas de información, para asegurar el cumplimiento de los criterios establecidos en la política general de seguridad de la información de la entidad como son: confidencialidad, integridad y disponibilidad

Atendiendo a los lineamientos de Gobierno en Línea, la Oficina de Tecnología de la Información y las Comunicaciones presentó al comité directivo el 19 de diciembre de 2016 la política general de seguridad de la información, la cual fue aprobada y posteriormente adoptada en el sistema integrado de gestión SIG, para ser desarrollada e implementada. Como resultado de la implementación se estructura este documento que se convierte en la columna vertebral de la seguridad de la información para la Defensoría del Espacio Público ya que en este se desarrollan los lineamientos establecidos en la política general de seguridad de la información de la entidad.

2. OBJETIVO GENERAL

Establecer los lineamientos que permiten proteger y salva guardar la confidencialidad, la integridad y disponibilidad de los activos de información, de acuerdo con los establecido en la Política General de Seguridad de la Información de la entidad, teniendo en cuenta procesos, la operación, los objetivos de la Entidad y los requisitos legales vigentes

3. ALCANCE

La política de seguridad de la información es aplicable a todo el ciclo de vida de los activos de información en el DADEP, incluyendo creación, distribución, almacenamiento y destrucción. De igual forma para todos los funcionarios, contratistas y terceros que desempeñan alguna labor para la Entidad. El alcance abarca desde el enunciado de la política, pasando por los lineamientos para la implementación del MSPI, la matriz de riesgos, la definición de los indicadores de monitoreo y cumplimiento de la política hasta la definición de la estrategia para su adopción.

4. TERMINOS

- **Acción correctiva**: Medida de tipo reactivo orientada a eliminar la causa de una no conformidad asociada a la implementación y operación del SGSI para prevenir su repetición.
- **Acción preventiva**: Medida de tipo proactivo orientada a prevenir potenciales no conformidades asociadas a la implementación y operación del SGSI.
- **Actualización de Base de Datos**: Necesidad de insertar, borrar o modificar información directamente en la base de datos cuando los sistemas de información no lo permiten.
- **Administración de incidentes de seguridad**: Un sistema de seguimiento de incidentes es un paquete de software que administra y mantiene listas de incidentes, conforme son requeridos por una institución. Para el caso de la Defensoría del Espacio Público, se administrarán con la herramienta GLPI creando una nueva categoría.
- **Antimalware**: Es una aplicación informática que encuentra y elimina el malware.
- **Antispyware**: Es un programa que puede ayudar a proteger su computadora de amenazas de seguridad causadas por spyware.
- **Antivirus**: Programa diseñado para identificar, aislar o eliminar un virus de los equipos de computado.
- **Alerta**: Una notificación formal de que se ha producido un incidente relacionado con la tecnología o la seguridad de la información que puede evolucionar hasta convertirse en desastre.
- **Amenaza**: Según [ISO/IEC 13335-1:2004): causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.
- **Análisis de riesgos**: Según [ISO/IEC Guía 73:2002): Uso sistemático de la información para identificar fuentes y estimar el riesgo.
- **Archivo de Archive**: Archivos que contienen todas las transacciones de la Base de datos con los que se puede hacer la recuperación a un tiempo anterior.
- **Backup**: Copia de seguridad o copia de respaldo con la que se puedan restaurar o recuperar información.
- **Características de la Información**: las principales características de la información son la disponibilidad, confidencialidad e integridad
- **Certificado Digital**: es un fichero informático generado por una entidad de servicios de certificación que asocia unos datos de identidad a una persona física, organismo o empresa, confirmando de esta manera su identidad digital en Internet.
- **Cifrado (CIPHER)**: Método de encriptación que utiliza una clave y un algoritmo para transformar texto simple en texto cifrado
- **Código malicioso (MALWARE)**: Tipo de software que tiene el objetivo de infiltrarse o dañar un computador o dispositivos de cómputo sin el consentimiento del usuario o propietario.
- **Contraseña o password**: Forma de autenticación que utiliza información secreta para controlar el acceso al recurso o sistema.

- **Control**: Las políticas, procedimientos, prácticas y estructuras de la organización para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.
- **Control correctivo**: Control que permite corregir un riesgo, error, omisión o acto deliberado antes de que produzca daño. Se supone que la amenaza ya se ha materializado pero que se corrige.
- **Control disuasorio**: Control que reduce la posibilidad de materialización de una amenaza.
- **Control preventivo**: Control que evita que se produzca un error, omisión o acto deliberado. No se materializa.
- **Cookie**: Tipo de almacenamiento de información guardado en el propio equipo que puede hacer normalmente el seguimiento de las preferencias en Internet dándole una clave que su creador podrá identificar para con ello tener una referencia de visitas con la finalidad de medir preferencias de mercado. Pero también por lo mismo puede ser usada por hackers para analizar qué páginas consulta un usuario regularmente, quitándole privacidad.
- **Copia incremental**: Copia de respaldo de los archivos que hayan sido modificados o se hayan creado desde la última copia realizada.
- **Copia total**: Copia completa de los datos o del sistema de archivos que compone el sistema que se está respaldando.
- **Cracker**: Persona interesada en saltarse la seguridad de un sistema informático.
- **Denegación de servicios**: Acción iniciada por una persona u otra causa que incapacite el hardware o el software, o ambos y después niegue el servicio quedando sin funcionamiento.
- **Desastre**: Evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una entidad.
- **Disponibilidad**: Característica o propiedad de la información de permanecer accesible y disponible para su uso cuando lo requiera una persona o entidad autorizada.
- **Dron**: Es una aeronave que vuela sin tripulación.
- **Evento**: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política general de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad. Según [ISO/IEC TR 18044:2004]
- **Encriptado, cifrado**: Conversión del texto claro a texto cifrado. Es un método para mantener la información sensible como confidencial mediante la modificación de los datos a un formato ilegible.
- **Equipo servidor**: Computador que, formando parte de una red, provee servicios a otras computadoras denominadas clientes. El término también puede referirse a un programa de computación que da servicios a otros programas de computación, ya sea en la misma máquina u otras.
- **Firewall**: Barrera de seguridad que protege segmentos de la red de accesos no deseados.
- **Firma Digital**: Es un mecanismo criptográfico que permite al receptor de un mensaje firmado digitalmente identificar el origen de dicho mensaje (autenticación de origen y

no repudio), y confirmar que el mensaje no ha sido alterado desde que fue firmado por el originador (integridad).

- **Formateo**: Acción mediante la cual un disco no usado es verificado y grabado con la información básica necesaria para su uso por el sistema. Para un disco con sectores fijos se graban todas las pistas de datos con identificadores de pista y las áreas de datos con un carácter fijo. Para un disco con sectores no fijos se graba la identificación del sector y de la pista al comienzo de cada sector en todas las pistas. Generalmente el sistema operativo incluye un programa para realizar esta función.
- **Grooming**: Es una práctica de acoso y abuso sexual en contra de niños y jóvenes que, en la mayoría de los casos, sucede a través de las redes sociales.
- **Hacker**: Persona con conocimientos técnicos que trata de esquivar, burlar o sobrepasar los controles y salvaguardias de un sistema de información, recurso tecnológico o de una persona de forma intencionada y sin permiso para hacerlo con el propósito de adquirir información.
- **Https**: Es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de Hipertexto.
- **Información**: La información constituye un importante activo, esencial para las actividades de una organización y, por lo tanto, necesita una protección adecuada. La información se encuentra en diferentes medios, puede estar impresa o escrita en papel, almacenada electrónicamente y tiene diferentes formatos.
- **Ingeniería** Social: Es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos ganando su confianza. Es una técnica que pueden utilizar investigadores privados, criminales, delincuentes computacionales (conocidos como cracker) para obtener información, acceso o privilegios en sistemas de información que les permiten realizar algún acto que perjudique o exponga a riesgos o abusos a personas o entidades.
- **Integridad**: Según [ISO 27000]: Es la Propiedad de la información relativa a su exactitud y completitud.
- **Keylogger**: Es un tipo de software o dispositivo hardware específico que se encarga de registrar las pulsaciones que se realizan en el teclado, para posteriormente memorizarlas en un fichero o enviarlas a través de internet.
- **Líder funcional**: Persona encargada de la toma de decisiones en cuanto a la manera como se estructura la funcionalidad de un software, es normalmente un experto en el manejo del procedimiento.
- **Logearse**: Es iniciar sesión mediante un nombre de usuario y contraseña.
- **Logs**: Registros cronológicos de las acciones realizadas en un sistema. Pueden ser de los usuarios que acceden o los procesos y ficheros que han intervenido. Se emplea con propósitos estadísticos y de control de la seguridad.
- **Modo archivelog**: Parámetro de configuración de la Base de datos de Oracle que al ser activado permite recuperar datos en el tiempo después de un error no recuperable (fallas humanas u otras).
- **Navegadores de internet**: Programas residentes en un computador empleado para visualizar información. Generalmente se aplica a programas que manejan páginas de

información Web y permiten el paso de una a otra de forma interactiva mediante el uso de hipertexto.

- **No repudio**: Los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que el evento o acción no pueda ser negado posteriormente.
- **Plan de continuidad del negocio**: Plan orientado a permitir la continuación de las principales operaciones de la Entidad en el caso de un evento o siniestro imprevisto que inhabilite total o parcialmente los servicios.
- **Phishing**: Consiste en el intento de acceder a información confidencial de forma fraudulenta, como puede ser una contraseña, información financiera o cualquier otro tipo de información que pueda ser privada o sensible. El estafador se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica generalmente un correo electrónico, algún sistema de mensajería instantánea o llamadas telefónicas.
- **Política general de seguridad de la Información**: Documento que establece el compromiso de la alta dirección y el enfoque de la organización en la gestión de la seguridad de la información.
- **PL/SQL**: Lenguaje de programación que permite la manipulación de las estructuras y los datos de las bases de datos y construcción de procedimientos o funciones.
- **Ransomware**: Es un tipo de programa dañino que restringe (secuestra) el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción.
- **Red LAN**: Son redes de propiedad privada, de hasta unos cuantos kilómetros. Se usan para conectar computadoras personales o estaciones de trabajo, con el objeto de compartir recursos e intercambiar información.
- **Red DMZ**: Corresponde a un área segura donde están ubicados los servidores en donde se protegen de cualquier amenaza de seguridad (Zona desmilitarizada).
- **Restauración**: Proceso a través del cual se busca restituir datos o un Sistema de Información previamente guardados mediante una copia de respaldo, a un estado anterior.
- **RMAN**: Herramienta de Oracle que al configurarla genera copias de respaldo de la Base de Datos para futuras recuperaciones. (Recovery Manager).
- **Respondiente**: Persona encargada en la entidad de reportar, hacer seguimiento y administrar los incidentes de seguridad de la empresa.
- **SAN (Storage Área Network)**: Sistema de almacenamiento en Red, concebido para almacenar y disponer de grandes volúmenes de datos
- **Sistema de Gestión de la Seguridad de la Información**: Según [ISO/IEC 27000]: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

- **Sistemas de Información**: Un sistema de información es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.
- **Sniffers**: Programa que realiza captura de las tramas de red. Sirve para analizar la red, analizar los paquetes de datos y protocolos de comunicación y puede ser utilizada con fines maliciosos.
- **Spoofing**: Falsificación de la identidad origen en una sesión: la identidad es por una dirección IP o Mac Address.
- **Spam** (buzonear, bombardear): Correo electrónico no autorizado o no solicitado, normalmente con contenido publicitario que se envía masivamente. Este tipo de mensajes puede causar graves molestias y provocar pérdidas de tiempo y recursos.
- **Spammer (buzoneador)**: Programa que permite el envío masivo de mensajes de correo electrónico con contenido publicitario y la consiguiente recepción masiva de estos. Puede ser también empleado para el envío masivo de amenazas tales como gusanos y troyanos.
- **Spyware (software espía)**: Programas que registran sin permiso la actividad del usuario de un equipo, la navegación por Internet, las pulsaciones de teclado, y reenvían esta información a través de Internet a los creadores de los programas espía.
- **SSL**: Son las siglas de Secure Sockets Layer. SSL proporciona una conexión segura.
- **Troyano**: Aplicación que aparenta tener un uso legítimo pero que tiene funciones ocultas diseñadas para sobrepasar los sistemas de seguridad.
- **Usuario**: Servidor público (funcionario o contratista) que tiene a su cargo acceso a recursos tecnológicos (computador, cuenta de correo electrónico, sistemas de información entre otros) por medio de los cuales puede almacenar, procesar, transferir información.
- **Verificar**: Comprobar que el resultado del proceso es el esperado, ejemplo: se han incluidos todos los archivos requeridos, el medio funciona, no presenta errores, etc.
- **Virus**: Porción de código que se auto incluye en otros programas y de esta forma puede extenderse entre computadores. Algunos virus se auto encriptan (mutan) al extenderse evitando de esta forma su detección. Pueden llegar a destruir toda la información almacenada en el computador o reducir dramáticamente el rendimiento de una máquina o de un sistema completo.
- **Wifi**: Es un mecanismo de conexión de dispositivos electrónicos de forma inalámbrica.

5. DEFINICIONES Y SIGLAS

- **MSPI**: Modelo de Seguridad y Privacidad de la Información.
- **SGSI**: Sistema de Gestión de la Seguridad de la Información
- **TI**: Tecnología de la información.

- BD: Base de Datos
- DBA: Administrador de Base de Datos
- DDOS: Ataque distribuido de denegación de servicio.
- FUS: Formato único de sistemas (Formato para la solicitud de servicios de TIC)
- URL: Localizador uniforme de recursos
- TIC's: Tecnologías de la información y las comunicaciones
- MODELO DE TOMA DE DESICIONES: proceso por el cual se toman decisiones a partir de la experiencia y el juicio personal acumulado.
- PARTES INTERESADAS: cualquier individuo, grupo u organización que forme parte o se vea afectado por el mismo, obteniendo algún beneficio o perjuicio.

6. POLÍTICAS, PROCEDIMIENTOS Y CONTROLES

De los procedimientos de la Defensoría del Espacio Público, la Oficina de Tecnología de la Información y las Comunicaciones comparte con la Subdirección Administrativa Financiera y de Control Disciplinario, el liderazgo y responsabilidad del proceso "Gestión de la Información y la Tecnología", proceso que tiene seis procedimientos de los cuales tres son responsabilidad de la Oficina de Tecnología de la Información y las Comunicaciones:

- "Mantenimiento de la infraestructura tecnológica"
- "Seguridad de la información"
- "Sistemas de información"

El presente documento está enmarcado en el desarrollo de los tres procedimientos a cargo de la Oficina de Tecnología de la Información y las Comunicaciones y la información desde el punto de vista electrónico, digital por lo tanto el tema de la gestión documental desde el punto de vista físico es administrado y gestionado por la Subdirección Administrativa y Financiera como responsable de los procedimientos.

Las políticas desarrolladas en este documento pretenden identificar un objetivo, su aplicabilidad y las directrices que permitan de manera general establecer un conducto en el uso de las TICS y utilizar las buenas prácticas en busca de la confidencialidad, integridad y disponibilidad de la información y el uso adecuado de los recursos.

Por su parte, en cuanto a los controles se establecen los diferentes componentes y herramientas que permiten tener una trazabilidad y control de los diferentes mecanismos establecidos para dar cumplimiento a la política general de seguridad de la información.

6.1 POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Política general de Seguridad de la Información institucional, surge para sensibilizar a cada uno de los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con el DADEP, sobre la importancia de protección de la información, así como en los servicios críticos de la entidad, de tal manera que les permitan desarrollar adecuadamente sus labores en cumplimiento de la misión de esta.

Para la Defensoría del Espacio Público la información es el activo más importante para la prestación de servicios a la ciudadanía y toma de decisiones institucionales, por lo tanto, se ha definido como POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN, Proteger la confidencialidad, integridad, disponibilidad de sus activos de información.

a. Objetivo: Definir Los lineamientos generales para la protección de la información del DADEP, y servir como apoyo y orientación a la dirección con respecto a la seguridad de

la información, de acuerdo con las normas y/o lineamientos nacionales, distritales e institucionales.

b. Directrices:

- Verificar que se definan, implementen, revisen y actualicen las políticas específicas de seguridad y privacidad de la información.

- Planificar, diseñar y realizar los programas de auditoría interna del sistema de gestión de seguridad de la información, los cuales serán responsabilidad de la oficina de Control Interno.

- Todas las licencias de software deben ser comprados o aprobados por la Oficina de Tecnología de la Información y las Comunicaciones, de acuerdo con lo definido en el proceso de adquisiciones.

- El DADEP debe contar con mecanismos o dispositivos de seguridad perimetral para la conexión a Internet o para la conexión a otras redes en outsourcing o de terceros.

- Para un mayor control y fácil administración, los requerimientos de tecnología siempre deben gestionarse a través de la mesa de ayuda y con los formatos debidamente diligenciados cuando estos apliquen o mediante actas; las solicitudes a la mesa de ayuda pueden hacerse por correo electrónico a la cuenta mesadeayuda@dadep.gov.co, directamente en la herramienta GLPI en la URL mesadeayuda.dep.gov.co o telefónicamente a la extensión 2222.

- Los líderes de los procesos son las personas autorizadas para realizar la solicitud de creación de usuarios y privilegios para el uso de los componentes TIC's de la entidad. Los jefes o subdirectores pueden delegar a quién consideren, para el envío de las solicitudes a través de la mesa de ayuda mesadeayuda@dadep.gov.co y con el formato FUS debidamente diligenciado. Las personas delegadas deben ser informadas a la Oficina de Tecnología de la Información y las Comunicaciones a través de una comunicación, correo electrónico institucional, mesa de ayuda o acta tramitada o firmada por jefe de área.

  Hacen parte de las políticas específicas de seguridad y privacidad de la información de la Defensoría del Espacio Público las siguientes:

  - ✓ Política de Correo corporativo
  - ✓ Política para el uso de recursos tecnológicos
  - ✓ Política de control de acceso (usuario y contraseña)
  - ✓ Política de copias de seguridad

- ✓ Política de estaciones de trabajo
- ✓ Política de red corporativa y Wireless
- ✓ Política de uso de Internet
- ✓ Política de uso de sistemas de información
- ✓ Política de seguridad física y del entorno del centro de datos
- ✓ Política de acceso remoto
- ✓ Política de servidor de archivos
- ✓ Política de administración de Base de Datos
- ✓ Política de pistas de auditoría
- ✓ Política de transmisión y publicación de información
- ✓ Política de teletrabajo
- ✓ Política de derechos de autor y legalidad de software
- ✓ Política de usos de impresoras y servicios de impresión
- ✓ Política de gestión de archivos
- ✓ Política de seguridad de los recursos humanos
- ✓ Política de gestión de página web
- ✓ Política de gestión de comunicaciones y operaciones
- ✓ Política de control de acceso
- ✓ Política de adquisición, desarrollo y mantenimiento de sistemas de información
- ✓ Política de gestión de incidentes de seguridad de la información
- ✓ Política de gestión de continuidad del negocio
- ✓ Política para la gestión de dispositivos móviles
- ✓ Política de uso de controles criptográficos

Política de Correo Corporativo.

a. Objetivo: Definir los lineamientos y estándares para el adecuado seguimiento y administración de las cuentas de correo corporativo de la defensoría del Espacio Público.

b. Directrices:

- Las comunicaciones son una herramienta indispensable en las labores diarias a realizar en las instituciones públicas, razón por la cual es un deber de la entidad, proveer de una herramienta de correo electrónico a todos los funcionarios y contratistas para que estos realicen sus comunicaciones institucionales.

- La creación de las cuentas de correo debe ser solicitadas por el Líder de proceso o quién este designe, a través de la mesa de ayuda adjuntando el formato único de sistemas FUS debidamente diligenciado.

- Cuando un funcionario o contratista al que se le haya autorizado el uso de una cuenta de correo electrónico se retire de la entidad, su cuenta de correo será desactivada y solo se activará con la autorización del Líder de proceso o la persona que este autorice, a través de la mesa de ayuda.

- Los correos electrónicos deben contener la siguiente nota respecto al manejo del contenido: "La información aquí contenida es para uso exclusivo de la persona o entidad de destino. Está estrictamente prohibida su utilización, copia, descarga, distribución, modificación y/o reproducción total o parcial, sin el permiso expreso de la Alcaldía Mayor de Bogotá, pues su contenido puede ser de carácter confidencial y/o contener material privilegiado. Si usted recibió esta información por error, por favor contacte en forma inmediata a quien la envió y borre este material de su computador. La Alcaldía Mayor de Bogotá no es responsable por la información contenida en esta comunicación, el directo responsable es quien la firma o el autor de esta."

- La Defensoría del Espacio Público permitirá a los funcionarios y contratistas, el intercambio de comunicaciones o mensajes, a través de una cuenta de correo electrónico institucional, que facilite el desarrollo de sus funciones y es un canal oficial de comunicación de la entidad.

- Los usuarios del correo electrónico corporativo son responsables de evitar prácticas o usos incorrectos 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 la entidad. Todos los correos electrónicos que se procesen en la infraestructura TIC de la Defensoría del Espacio Público deben ser de carácter institucional.

- El servicio de correo electrónico corporativo debe ser utilizado única y exclusivamente para comunicaciones institucionales y no debe ser utilizado para ningún otro fin.

- El envío de correos masivos, solo se permite a grupos específicos; el envío de correos a todo el personal de la entidad, deben ser realizado a través del Equipo de comunicaciones.

- El envío de correos con contenido que atenten contra la integridad y dignidad de las personas y el buen nombre de la entidad no está autorizado.

- Está prohibido utilizar el correo para el desarrollo de actividades políticas, comerciales, de entretenimiento o para la transmisión de mensajes vulgares u obscenos.

- Está restringido el envío de correos que lleven adjunto archivos con extensión .rar, .zip, .DMP y .DBF.

- Todos los mensajes pueden ser sujetos a análisis y conservación permanente por parte de la Entidad y en caso de requerirse pueden ser consultados por personas autorizadas para tal fin.

- Si el funcionario o contratista es el destinatario del mensaje, este debe dar un manejo adecuado a la información; de presentarse cualquier suceso anómalo, deberá reportarlo a la mesa de ayuda de la Entidad.

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

- Los mensajes cuyo origen es desconocido no deben ser contestados, ni abrir los archivos adjuntos y se deben reenviar al correo mesadeayuda@dadep.gov.co con la frase “correo sospechoso” en el asunto.

- El servicio de correo electrónico oficial de la entidad es el asignado por la Oficina de Tecnología de la Información y las Comunicaciones.

- Toda información creada, almacenada y/o compartida en las diferentes aplicaciones de la cuenta de correo electrónico institucional (por ejemplo, GOOGLE DRIVE, GOOGLE SITES), debe tener una copia de respaldo ubicada en las carpetas de almacenamiento compartido u otro medio que la Oficina de Tecnología de la Información y las Comunicaciones destine para tal fin.

- No se realizarán copias de los buzones para ser entregadas a los funcionarios o contratistas.

Política para el uso de recursos tecnológicos

Los recursos tecnológicos a los que se refiere este ítem son los componentes de tecnología que se asignen a los funcionarios o contratistas, como computadores de escritorio, portátiles, dispositivos externos de almacenamiento, así como los recursos lógicos de almacenamiento de información como carpetas compartidas para el almacenamiento de la información institucional.

a. Objetivo: Definir los lineamientos generales para asegurar el uso adecuado de los recursos tecnológicos de la Defensoría del Espacio Público, así como su distribución y balanceo de conformidad con la disponibilidad de los recursos tic de la entidad.

b. Directrices:

- Guardar la información institucional que se produzca en los procesos, por parte de funcionarios y contratistas, en el espacio de almacenamiento que corresponda a cada grupo de trabajo, en el servidor de archivos, al cual se le realizarán periódicamente copias de seguridad, para salvaguardar la información allí almacenada.

- El uso de dispositivos de almacenamiento externo (dispositivos móviles, DVD, CD, memorias USB, agendas electrónicas, celulares, u otros) está restringido. Para realizar copias de información en cualquier dispositivo de almacenamiento externo, se debe hacer la solicitud a través de la mesa de ayuda y debe estar autorizada por el Líder de proceso o supervisor del contrato.

- Los recursos tecnológicos (hardware y software) asignados a los funcionarios del DADEP son responsabilidad de cada funcionario o contratista.

- Los usuarios son los responsables de la información que administran en los equipos de escritorio o portátiles asignados por la entidad y deben abstenerse de almacenar en ellos información no institucional.

- Los usuarios tendrán acceso solamente a los datos y recursos autorizados por la entidad, de acuerdo lo solicitado por el jefe de área o la persona que este designó, y serán responsables disciplinaria y legalmente por la divulgación no autorizada de dicha información o al utilizarla para beneficio propio.

- Es responsabilidad de cada usuario proteger la información que está contenida en documentos, sistemas de información, formatos, listados, etc.; adicionalmente se deben proteger los datos de entrada de los procesos haciendo que esta sea integra y confiable.

- Los dispositivos periféricos como computadores, impresoras, fotocopiadoras, escáner, etc., solo deben utilizarse para los fines institucionales y autorizados por la entidad.

- Cualquier evento o posible incidente que afecte la seguridad de la información, debe ser reportado inmediatamente a la mesa de ayuda por los canales establecidos en el procedimiento de Mantenimiento y Soporte de la Infraestructura Tecnológica.

- La Oficina de Tecnología de la Información y las Comunicaciones se encargará de hacer las campañas correspondientes para que los usuarios estén enterados de los cambios tecnológicos, buenas prácticas en el uso de las TIC´s a través de los canales oficiales de comunicación de la entidad, así como de realizar las respectivas inducciones y capacitaciones en el uso de los diferentes sistemas de información de la entidad.

- El uso de firmas digitales es responsabilidad de las personas a quien se le asignen, teniendo en cuenta siempre que el usuario y contraseña es personal e intransferible, por lo tanto, el usuario de la firma digital se hace responsable de las transacciones que se realicen con el certificado digital asignado.

- Las cámaras fotográficas, de video, equipos de comunicaciones, carteleras digitales están a cargo de los funcionarios del área de comunicaciones, quienes son los responsables de su cuidado y buen uso.

- Se debe bloquear la sesión del equipo de cómputo siempre que el usuario se ausente. Para esto, oprima la tecla WINDOWS  y la tecla L.

- Al término de la jornada laboral se debe apagar la CPU y la pantalla. Exceptuando los equipos que tienen permitido el acceso remoto.

- Los recursos como papel, CD, DVD, entre otros, así como equipos topográficos, cámaras, impresoras y demás dispositivos electrónicos deben ser utilizados únicamente para el desarrollo de las funciones y no para uso y beneficio propio

Política de control de acceso (usuario y contraseña)

a. Objetivo: Definir los estándares y lineamientos generales para la creación de usuarios y contraseñas de los servicios de TIC's prestados por la Oficina se Sistemas, asegurando una fácil administración y organización de estos, a través del uso de contraseñas.

b. Directrices:

- La solicitud de creación de usuarios de directorio activo, correo electrónico, sistemas de información o cualquier otro servicio de TIC´s que se requieran para cada usuario, debe hacerse a través de la mesa de ayuda, enviando el formato único de sistemas FUS debidamente diligenciado y autorizado por el líder de proceso la persona que este designó. También se hará el mismo procedimiento para solicitar nuevos roles cuando el funcionario o contratista ya tenga un usuario creado.

- En los casos en que el usuario ya este creado y se encuentre deshabilitado por terminación de contrato u otra situación laboral, para su habilitación solo se requiere un correo a mesadeayuda@dadep.gov.co, solicitando la habilitación del usuario sin el formato FUS, este correo debe ser enviado por el líder de proceso o la persona que este designó.

- La Oficina de Tecnología de la Información y las Comunicaciones es la responsable de inactivar las cuentas de usuario de los sistemas de información y de directorio activo, cuando los funcionarios o contratistas soliciten a la Oficina de Tecnología de la Información y las Comunicaciones la firma de paz y salvo de entrega de puesto de trabajo y cuando reciba la relación de personal próximo a salir a vacaciones por parte de la oficina de talento humano, con el propósito de inactivar los servicios y no le asignen más correspondencia.

- La Oficina de Tecnología de la Información y las Comunicaciones se encargará de la creación de los usuarios solicitados, para lo cual se tendrá en cuenta la siguiente estructura: inicialmente, se tomará la primera letra del primer nombre seguida del primer apellido completo, en caso de que el nombre de usuario resultante exista, se tomarán las dos primeras letras del primer nombre seguidas del primer apellido completo y así sucesivamente hasta tomar todas las letras del primer nombre. Si tomando el primer nombre y apellido completos, el nombre de usuario resultante sigue presentando duplicidad, se deberá agregar un número consecutivo al final, iniciando desde el número 2 (dos), de modo que se pueda diferenciar de otro usuario existente.

Ejemplo:

No.	Nombres	Apellidos	Nombre de usuario resultante
1	Alicia	Pérez López	aperez
2	Andrés Felipe	Pérez Mendoza	anperez
3	Ana María	Pérez Díaz	anaperez
4	Ana	Pérez González	anaperez2

Para la creación de los usuarios administradores de SUMA o de SIDEP para usuarios externos, se utiliza el mismo estándar y formato FUS, pero se requieren datos adicionales relacionados con el correo electrónico y la entidad en la que labora el solicitante; el correo electrónico se requiere ya que es en esa cuenta de correo en la que se hará la notificación de la creación de usuario. Los usuarios de SUMA deben ser solicitados por el Instituto de Desarrollo Urbano - IDU, Instituto de Recreación y Deportes - IDRD o el Instituto Distrital de Artes - IDARTES a través del ingeniero líder técnico de SUMA, para el caso de SIDEP se hará a través de la persona delegada por la Subdirección de Registro Inmobiliario.

- La Oficina de Tecnología de la Información y las Comunicaciones notificará vía correo electrónico o de manera personal, sobre la creación de la cuenta y su contraseña, la cual debe ser cambiada en la primera sesión por parte del usuario.

- Las contraseñas de directorio activo y de los sistemas de información deben ser seguras, utilizando mayúsculas, minúsculas y números, para evitar que estas sean fácilmente vulneradas. Para el caso de los usuarios de Base de Datos Oracle, esta tiene implementado un perfil que tiene configurada esta contraseña segura y obliga a los usuarios a cumplirla.

- Las contraseñas deben ser cambiadas cada 30 días y no deben ser expuestas en papeles que queden a la vista o en lugares en donde otra persona la pueda encontrar.

- Los usuarios y contraseñas de todos los sistemas o servicios son personales e intransferibles, por lo tanto, no se deben prestar para ningún tipo de transacción.

- Las personas propietarias de los usuarios son responsables de las transacciones, alteraciones o modificaciones de que sea objeto la información, realizada con su usuario, con las consecuencias administrativas y legales a que haya lugar.

- En caso de olvidar su contraseña o que esta se encuentre bloqueada, debe solicitar a la mesa de ayuda su restablecimiento.

Política de copias de seguridad

Las copias de seguridad a los que se refiere este ítem son los aplicados a los activos de información de la entidad como lo son los servidores, bases de datos de los sistemas de información, equipos de comunicación, aplicaciones y sus fuentes.

a. Objetivo: Definir las estrategias para la realización de las copias de seguridad de la información institucional contenida en los sistemas de información y aplicaciones, asegurando la salvaguarda y fácil restauración en caso de requerirse y garantizar la operación del negocio.

b. Directrices:

Generales

- Se realizarán periódicamente copias de seguridad a los activos de información en producción.
- La Oficina de Tecnología de la Información y las Comunicaciones debe adelantar acciones administrativas y técnicas necesarias para asegurar la conectividad en los servicios y la información crítica de la entidad ante posibles contingencias.
- Los administradores de los servicios (Administrador de Base de Datos DBA o administrador de infraestructura), son los responsables de realizar el seguimiento para que la política de copia de seguridad se ejecute de acuerdo con los lineamientos acá definidos y sugerir ajustes a estas en caso de requerirse por cambios tecnológicos o mejores prácticas.
- La Oficina de Tecnología de la Información y las Comunicaciones debe mantener un inventario actualizado de las copias de respaldo de la información y los aplicativos de la entidad.
- Ningún tipo de información institucional puede ser almacenada en forma exclusiva en los discos duros de las estaciones de trabajo; por lo tanto, es obligación de los usuarios finales mantener la información de su trabajo y área en las carpetas compartidas destinadas para este fin.
- Los medios de respaldo que vayan a ser eliminados deben ser destruidos de forma adecuada, verificando que no quede información disponible, para su control histórico, esta actividad deberá ser registrada por el responsable del proceso y en todo caso informando a la Oficina de Tecnología de la Información y las Comunicaciones

- Es responsabilidad de cada dependencia, mantener depurada la información de las carpetas compartidas para la optimización del uso de los recursos de almacenamiento con que cuenta la entidad.

- Las copias de seguridad se realizan de acuerdo con lineamientos establecidos en el manual para la toma de backups.

Política de estaciones de trabajo

a. Objetivo: Garantizar que los usuarios finales hagan un uso adecuado de la información institucional y de los recursos de TIC asignados.

b. Directrices:

- La instalación de software en los computadores suministrados por el DADEP es una función exclusiva de la Oficina de Tecnología de la Información y las Comunicaciones, quién tiene el control del software autorizado para instalar en los computadores.

- Se definirán dos (2) perfiles de Administrador: Uno local con permisos para la instalación y configuración de software y aplicativos, así como para la configuración de periféricos. El segundo es un administrador de red, para uso de los funcionarios administradores de la Oficina de Tecnología de la Información y las Comunicaciones, este asume las políticas del directorio activo.

- En el Disco C:\ de las estaciones cliente se tiene configurado el sistema operativo, aplicaciones y perfil de usuario. El usuario deberá abstenerse de realizar modificaciones a estos archivos.

- Los usuarios deben bloquear la sesión del computador cada vez que se retiren de su puesto de trabajo.

- Los usuarios podrán trabajar sus documentos institucionales en borrador en la estación cliente asignada por la DADEP y deberán ubicar copias y documentos finales en las carpetas compartidas que se establezcan.

- El préstamo de computadores, portátiles y vídeo proyectores se debe solicitar a través de la mesa de ayuda con anticipación y se proveerán de acuerdo con la disponibilidad.

- Los equipos solicitados en préstamo deben ser devueltos a la Oficina de Tecnología de la Información y las Comunicaciones en el mismo estado en que se recibió por parte del solicitante, en caso de daños o averías, es responsabilidad del solicitante su reparación o reposición.

- Los equipos que ingresan temporalmente al DADEP que son de propiedad de terceros: deben ser registrados en las porterías de la entidad para poder realizar su retiro sin autorización, el DADEP no se hace responsable en caso de pérdida o daño de algún equipo informático de uso personal o que haya sido ingresado a las instalaciones.

- Los funcionarios o contratistas de la Oficina de Tecnología de la Información y las Comunicaciones no están autorizados para prestar servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo de información) a equipos que no sean del DADEP.

- Los usuarios son responsables del buen uso de los equipos asignados, por lo que se prohíbe el consumo de alimentos en los puestos de trabajo y la manipulación de sustancias que puedan afectar los elementos de cómputo.

- Los usuarios que utilicen activos de la entidad no los pueden desatender en lugares públicos.

- La información deberá almacenarse en las carpetas compartidas y no en las estaciones de trabajo (computadores).

- Los medios de almacenamiento deben guardarse en sitios seguros bajo llave, especialmente cuando los funcionarios se retiren de sus puestos de trabajo o la oficina esté desocupada.

Política de red corporativa y Wireless

a. Objetivo: Asegurar el buen uso de los puntos de red de la LAN y de la conexión inalámbrica de la entidad.

b. Directrices:

- Los usuarios deberán emplear los puntos de red para la conexión de equipos informáticos estándar. Los equipos de uso personal que no son de propiedad del DADEP, solo tendrán acceso a internet haciendo uso de la Wifi, previa autorización de la Oficina de Tecnología de la Información y las Comunicaciones quien configurará la conectividad de manera temporal.

- Para la conexión de los computadores se deben emplear los puntos de red habilitados en los módulos, los cuales están identificados en la etiqueta con la letra D (D mayúscula - DATOS); para utilizar los puntos de red identificados con V (V mayúscula- VOZ) deben informar a la Oficina de Tecnología de la Información y las Comunicaciones para habilitar el punto para red de datos.

- Las extensiones telefónicas deben estar conectadas en los puntos de voz, los cuales están identificados en la etiqueta con la letra V (V mayúscula), antes del número del punto de red.

- La contraseña de la red WIFI es de conocimiento de los funcionarios de la Oficina de Tecnología de la Información y las Comunicaciones delegados en este tema y siempre que se requiera una configuración, esta se debe hacer sin suministrar la contraseña a las demás personas, el uso de red Wifi es para operación única de internet y no cuenta con los permisos de conexión a la red del DADEP.

- La instalación, activación y gestión de los puntos de red es responsabilidad de la Oficina de Tecnología de la Información y las Comunicaciones.

Política de uso de Internet

a. Objetivo: Definir los lineamientos que garanticen la navegación segura y el uso adecuado de la internet por parte de los usuarios finales, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la internet.

b. Directrices:

- La navegación en Internet debe ser utilizada con propósitos laborales.
- Está prohibida la navegación a sitios con contenidos contrarios a la ley, como la ley 679 de 2001 u otras que representen peligro para la entidad como: pornografía, terrorismo, hacktivismo, segregación racial.
- También está restringida la navegación a YouTube, Facebook, u otras páginas sugeridas por la alta dirección del DADEP y su autorización de uso será controlada por la Oficina de Tecnología de la Información y las Comunicaciones en coordinación con la Subdirección Administrativa, Financiera y de Control Disciplinario.
- La descarga de archivos de Internet debe ser únicamente con propósitos laborales.

Política de uso de sistemas de información

a. Objetivo: Definir los lineamientos para asegurar el uso adecuado de los sistemas de información que permitan proteger la confidencialidad, integridad y disponibilidad de la información.

b. Directrices:

- Para poder acceder a un sistema de información de la entidad, se debe tener una cuenta de usuario personal, la cual se solicita a través de la mesa de ayuda diligenciando el Formato Único de Sistemas.
- No se debe hacer uso de usuarios genéricos, por ejemplo, el usuario consulta para todos los usuarios, estos deben ser individuales y personales.
- El uso de los sistemas de información debe hacerse luego de una capacitación que debe ser impartida por los líderes funcionales o por la Oficina de Tecnología de la Información y las Comunicaciones.
- Los cambios a los datos que se realicen en los sistemas de información son responsabilidad de los usuarios que abren la sesión, estos cambios quedan registrados en la base de datos identificando usuario, fecha, hora, y los datos cambiados, por lo que se recomienda especial cuidado de las contraseñas.
- En caso de requerirse una capacitación, esta debe solicitarse a los líderes funcionales o a la Oficina de Tecnología de la Información y las Comunicaciones.
- Es necesario realizar todas las actividades requeridas en los sistemas de información de acuerdo con el procedimiento ya que la falta de algún paso dentro del sistema puede ocasionar problemas en el proceso a los otros usuarios que hacen uso del sistema.
- En caso de desconocimiento de los procesos o procedimientos en los sistemas de información, se debe solicitar apoyo a los líderes funcionales, en caso de fallas técnicas se debe solicitar soporte a la oficina se sistemas a través de la mesa de ayuda.

Política de seguridad física y del entorno del centro de datos

a. Objetivo: Establecer los controles para proteger física y ambientalmente los componentes de Tecnologías de información y Comunicaciones TIC de la entidad, para garantizar la integridad, confidencialidad y disponibilidad de la información.

b. Directrices:

- El ingreso al centro de datos debe ser controlado, para lo cual se debe registrar la planilla "Formato Control de Acceso al centro de cómputo" en la que se registra la hora de entrada, hora de salida nombres y motivo de la visita o actividad realizada.

- La Oficina de Tecnología de la Información y las Comunicaciones debe garantizar que el control de acceso al centro de datos del DADEP, cuenta con dispositivos electrónicos de autenticación o sistema de control biométrico.

- Los equipos del centro de cómputo deben contar con un sistema de respaldo de suministro de energía.

- La limpieza y aseo del centro de datos estará a cargo del Área Administrativa y debe efectuarse en presencia de un funcionario o contratista de la Oficina de Tecnología de la Información y las Comunicaciones de la entidad. El personal de limpieza debe ser ilustrado con respecto a las precauciones mínimas a seguir que debe tener durante el proceso de limpieza y prohibirse el ingreso de maletas o elementos que no sean estrictamente necesarios para su labor de limpieza y aseo.

- En el centro de datos, no se debe fumar, comer o beber; de igual forma se debe eliminar la permanencia de papelería y materiales que representen riesgo de propagación de fuego, así como mantener el orden y limpieza en todos los equipos y elementos que allí se encuentran.

- El centro de datos debe estar provisto de:

    - Señalización de todos y cada uno de los diferentes equipos y elementos, así como luces de emergencia y de evacuación, cumpliendo las normas de seguridad industrial y de salud ocupacional.

    - Pisos falsos elaborados con materiales no combustibles.

    - Sistema de refrigeración por aire acondicionado de precisión. Este equipo debe ser redundante para que en caso de falla se pueda continuar con la refrigeración.

- Unidades de potencia ininterrumpida UPS, que proporcionen respaldo al mismo, con el fin de garantizar el servicio de energía eléctrica durante una falla momentánea del fluido eléctrico de la red pública.

- Alarmas de detección de humo y sistemas automáticos de extinción de fuego, conectada a un sistema central. Los detectores deberán ser probados de acuerdo con las recomendaciones del fabricante o al menos una vez cada 6 meses y estas pruebas deberán estar previstas en los procedimientos de mantenimiento y de control.

- Extintores de incendios o un sistema contra incendios debidamente probados y con la capacidad de detener el fuego generado por equipo eléctrico, papel o químicos especiales.

- El Acceso al centro de cómputo está controlado por acceso biométrico y la información de los registros de acceso están bajo la custodia de la Oficina de Tecnología de la Información y las Comunicaciones, los usuarios autorizados son restringidos a algunos funcionarios de la Oficina de Tecnología de la Información y las Comunicaciones.

- El cableado de la red debe ser protegido de interferencias por ejemplo usando canaletas que lo protejan.

- Las actividades de soporte y mantenimiento dentro del centro de datos siempre deben ser supervisadas por un funcionario o contratista autorizado del DADEP.

- Cuando se requiera realizar alguna actividad sobre algún armario (rack), este debe quedar ordenado, cerrado y con llave, cuando se finalice la actividad.

- Los equipos del centro de datos que lo requieran deben estar monitoreados para poder detectar las fallas que se puedan presentar.

- La destrucción y/o disposición final de los medios de almacenamiento, computadores o servidores debe hacerse de forma adecuada, eliminando primero la información antes de su disposición final.

Política de acceso remoto

a. Objetivo: Definir los canales y restricciones que se deben tener en cuenta para acceso remoto a los componentes TIC´s de la entidad, manteniendo la integridad, disponibilidad y confidencialidad de la información.

b. Directrices:

- El acceso remoto a los computadores y/o servidores de la entidad, se deben solicitar a través de la mesa de ayuda de la entidad, según lo definido en el procedimiento de Mantenimiento y Soporte de la Infraestructura Tecnológica.

- El canal de acceso remoto es la VPN, el acceso para esta debe contar con el visto bueno del jefe inmediato, el jefe de la Oficina de Tecnología de la Información y las Comunicaciones y el encargado de la seguridad de la información de la entidad.

- Si es un usuario especializado (soporte de Oracle, soporte de DELL, soporte de Royal) se le creará un acceso VPN, que establece una conexión a la red desde su máquina remota, para poder operar debe haber gestionado los permisos para hacer uso de los recursos que requiera, de lo contrario solo operarán los servicios públicos a los que tenga acceso.

- Para acceso a proveedores, podrían permitirse accesos remotos, ya sea para mantenimientos o nuevas instalaciones, éste debe contar con a la aprobación del jefe de la Oficina de Tecnología de la Información y las Comunicaciones, el líder de infraestructura y el visto bueno del encargado de la seguridad de la información de la entidad, los periodos de tiempo de conexión deberán ser controlados por el líder de infraestructura.

Política de servidor de archivos

a. Objetivo: Definir los lineamientos para la administración, buen uso y optimización de los recursos de almacenamiento en los servidores de archivos dispuestos para la centralización de la información institucional, manteniendo la integridad, disponibilidad y seguridad de la información en las carpetas compartidas.

b. Directrices:

- Las carpetas compartidas en el DADEP están organizadas por dependencia, una general para todas las áreas y otras por temas para grupos de trabajos específicos. También se cuenta con una unidad de almacenamiento, para las imágenes documentales de royal.

- Para que los usuarios tengan acceso a la información ubicada en los discos de red, se debe enviar el formato único de sistemas (FUS), solicitando el usuario de directorio activo, en el que se indica el área en la que va a trabajar, por ende, tiene acceso a la carpeta del área correspondiente, a la carpeta pública general y si se requiere permiso a otra carpeta en particular se debe especificar en el formato, el cual debe ser enviado a la mesa de ayuda.

- Los usuarios tendrán permisos de escritura, lectura o modificación de información en las carpetas de red del área a la que pertenecen, en la pública general con permisos de lectura, modificación, copiado, eliminación y en otras dependiendo del rol solicitado. Para el caso de la carpeta documentos electrónicos de royal, para los usuarios de captura cuentan con permisos de escritura y lectura, para los demás solo de lectura.

- La información institucional que se trabaje en las estaciones cliente de cada usuario debe almacenarse finalmente en las carpetas compartidas, esta tarea es de responsabilidad de cada funcionario y contratista.

- Los documentos no institucionales no deben ser copiados en las carpetas compartidas.

- Está prohibido almacenar archivos con contenido que atente contra la moral y las buenas costumbres de la entidad o las personas, como pornografía, propaganda racista, terrorista o cualquier software ilegal o malicioso, ya sea en medios de almacenamiento de estaciones de trabajo, computadores de escritorio o portátiles, tabletas, celulares inteligentes, etc. o en los discos de red.

- No está permitido extraer, divulgar o publicar información sin expresa autorización de la Entidad.

- La responsabilidad de generar las copias de respaldo de la información de las carpetas compartidas está a cargo de la Oficina de Tecnología de la Información y las Comunicaciones, de acuerdo con la política de copias de seguridad.

- En caso de que un usuario requiera la restauración de información de las carpetas compartidas, debe solicitarla en el formato "Solicitud de Información o Modificación a la Base de Datos de los Sistemas de Información" debidamente diligenciado y enviarlo a la mesa de ayuda.

Política de administración de Base de Datos

a. Objetivo: Definir los lineamientos a tener en cuenta para el control y administración de las bases de datos institucionales, a fin de optimizar el uso de los recursos y garantizar la confidencialidad, integridad y disponibilidad de la información.

b. Directrices:

- La administración de las bases de datos es responsabilidad de los funcionarios o contratistas de la Oficina de Tecnología de la Información y las Comunicaciones delegados para tal fin, estos deben cumplir con un perfil de Administrador de Base de Datos.

- La Oficina de Tecnología de la Información y las Comunicaciones proveerá Bases de Datos para los aplicativos de producción y ambientes separados para pruebas y/o desarrollo, para llevar a cabo las labores correspondientes por parte de los ingenieros de desarrollo de software y usuarios.

- En las Bases de datos, los usuarios tienen acceso restringido a través de roles definido en las aplicaciones, cumpliendo con unos perfiles funcionales establecidos.

- Para la creación de nuevos esquemas, tablas, índices, vistas, procedimientos almacenados, sinónimos u otros objetos de base de datos, estos deben ser solicitados a través de la mesa de ayuda con el formato "Solicitud de Información o Modificación a la Base de Datos de los Sistemas de Información" debidamente diligenciado.

- Para la creación de una nueva instancia de Base de Datos, esta debe ser solicitada a través de la mesa de ayuda con el formato "Solicitud de Información o Modificación a la Base de Datos de los Sistemas de Información", justificando la razón por la que se solicita y su creación estará sujeta a verificación de licenciamiento (ORACLE, MySQL o al que corresponda) y a disponibilidad de infraestructura.

- Para las Bases de Datos de desarrollo y pruebas, los ingenieros de desarrollo contarán con acceso de los usuarios propietarios de los objetos (esquemas), también con su cuenta de usuario configurado para que les permita el control de ciertos recursos, para la creación y/o modificación de sus objetos y realizar las pruebas.

- Cuando por necesidad de la dependencia usuaria se requiere insertar, borrar o modificar información directamente en la base de datos, se deberá realizar la solicitud requerida a la mesa de ayuda, siguiendo lo definido en el procedimiento de Mantenimiento y Soporte de la Infraestructura Tecnológica. Esto se puede presentar por fallas en las operaciones internas del sistema, fallas en la funcionalidad del sistema, error humano, caídas del sistema por diferentes causas que no permiten la sincronización de la información, u otras.

Política de pistas de auditoría

a. Objetivo: Definir los lineamientos a tener en cuenta en la realización y administración de la auditoría de las bases de Datos y de las transacciones, para los ambientes de producción que contribuyan con la confidencialidad, integridad, disponibilidad, y trazabilidad de las operaciones realizadas.

b. Directrices:

- La administración de la auditoría será responsabilidad de los funcionarios o contratistas de la Oficina de Tecnología de la Información y las Comunicaciones delegados para tal función.
- La auditoría se realizará solamente en la base de datos de producción.
- Para configurar la auditoría de las aplicaciones se deben definir las tablas y los campos a auditar en cada aplicación, esto se define conjuntamente los responsables de cada aplicativo, y de acuerdo con la importancia y la sensibilidad de los datos.
- La auditoría de las aplicaciones registrará las transacciones de inserción, actualización y borrado de datos en las tablas de la base de datos, registrando el usuario, nombre de la tabla, esquema, fecha de la transacción en formato dd/dd/yyyy hh:mm:ss, dato anterior y dato nuevo.
- Los registros de auditoría no podrán ser eliminados ni alterados, por lo tanto, se debe conservar copia de estos de manera continua.
- Dada la gran cantidad de registros de auditoría, para facilitar su consulta estos deben ser organizados por vigencia en diferentes esquemas.
- Los backup's de los registros de auditoría están inmersos en los backup's de la base de datos del ambiente de producción.
- Los requerimientos de datos de auditoría deben solicitarse por la mesa de ayuda, en el formato de "Solicitud de Información o Modificación a la Base de Datos de los Sistemas de Información" debidamente diligenciado.

Política de transmisión y publicación de información

a. Objetivo: Definir los canales y responsables de la transmisión y publicación de información institucional de la entidad, contribuyendo con la confidencialidad, integridad y disponibilidad de la información.

b. Directrices:

- Las personas encargadas de actualizar información en los canales oficiales de comunicación de la entidad son: funcionarios o contratistas del área de comunicaciones y de la Oficina de Tecnología de la Información y las Comunicaciones delegados para esta función, los cuales tiene rol de administrador otorgado en las respectivas plataformas.

- El usuario administrador de portales web, se debe solicitar a través de la mesa de ayuda siguiendo las instrucciones definidas en el numeral 4.11 Gestión de los servicios de administración, creación y eliminación de cuentas de usuarios en el servidor de dominio, del instructivo de mantenimiento y Soporte de la Infraestructura Tecnológica.

- El formato y el estilo de la información a publicar se regirá por las directrices estipuladas en el Plan de comunicaciones.

- La veracidad y la calidad de la información publicada en los canales oficiales, será responsabilidad de las áreas donde se origine.

- Todos los contenidos publicados en los canales oficiales deben cumplir con las directrices estipuladas en el Plan de comunicaciones.

- Los terceros que tengan acceso a información del DADEP, deberán firmar un acuerdo de confidencialidad y buen uso de la información a la que tengan acceso.

Política de trabajo en casa

a. Objetivo: Definir las directrices con el establecimiento de los mecanismos de uso de los componentes TIC, para la implementación del trabajo en casa en el DADEP.

b. Directrices:

- Los permisos para el uso de las herramientas TIC en la modalidad de trabajo en casa, deberán ser solicitados en el formato único de sistemas FUS. Esto debe ser solicitado por la Subdirección Administrativa, Financiera y de Control Disciplinario, siguiendo las instrucciones definidas en el numeral 4.11 Gestión de los servicios de administración, creación y eliminación de cuentas de usuarios en el servidor de dominio, del instructivo de mantenimiento y Soporte de la Infraestructura Tecnológica.

- De acuerdo con los servicios solicitados en el FUS, la Oficina de Tecnología de la Información y las Comunicaciones asignará y parametrizará la correspondiente VPN.

- El equipo o equipos utilizados por los funcionarios para trabajo en casa debe contar con una solución de seguridad (firewall), tener instaladas las actualizaciones, implementar contraseñas de bloqueo y realizar mantenimientos regulares.

- Es obligatorio que los funcionarios que realizan trabajo en casa conozcan y apliquen las políticas específicas de seguridad y privacidad de la información definidas en este documento.

- La Oficina de Tecnología de la Información y las Comunicaciones del DADEP, podrá monitorear y hacer seguimiento a la trazabilidad de las actividades realizadas por los funcionarios para modalidad de trabajo en casa.

Política de derechos de autor y legalidad de software

a. Objetivo: Definir los lineamientos para dar cumplimiento a la ley 23 de 1982 de derechos de autor.

b. Directrices:

- Los funcionarios de la Oficina de Tecnología de la Información y las Comunicaciones del DADEP instalarán copia de los programas que han sido adquiridos legalmente. No está autorizado el uso de programas sin su respectiva licencia y autorización del DADEP, ni el uso de archivos como: imágenes, vídeos, software o música, obtenidos a partir de otras fuentes (internet, dispositivos de almacenamiento externo, correo), ya que estos pueden implicar amenazas legales y de seguridad de la información para la entidad.

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

- Los programas instalados en los equipos son de propiedad del DADEP o la entidad está autorizada para su uso, la copia no autorizada de programas o de su documentación, implica una violación a las normas de derechos de autor. Los funcionarios, contratistas o demás colaboradores que utilicen copias no autorizadas de programas o su respectiva documentación, quedarán sujetos a las acciones disciplinarias establecidas por la entidad o las sanciones que especifique la ley.

- El DADEP 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 de la entidad. Estos controles pueden incluir valoraciones periódicas en todos los equipos del uso de los programas y auditorías.

- La instalación y uso de aplicaciones de terceros que se requieran y se puedan utilizar bajo el cumplimiento de las restricciones establecidas por el fabricante deberá contar con la autorización de la Oficina de Tecnología de la Información y las Comunicaciones.

Política de usos de impresoras y servicios de impresión

a. Objetivo: definir los lineamientos para asegurar la adecuada, correcta y segura operación de las impresoras y del servicio de impresión y plotter.

b. Directrices:

- Los documentos, planos o mapas que se impriman o plotean en las impresoras o plotter del DADEP deben ser de carácter institucional.

- Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (impresoras, escáner, plotter y fotocopiadora) para que no se afecte su correcto funcionamiento, en caso de desconocimiento debe apoyarse en funcionarios de la mesa de ayuda de la Oficina de Tecnología de la Información y las Comunicaciones.

- Ningún usuario debe realizar labores de reparación o mantenimiento de los equipos (impresoras, escáner, plotter y fotocopiadora). En caso de presentarse alguna falla, esta se debe reportar a la mesa de ayuda de la Oficina de Tecnología de la Información y las Comunicaciones.

- El acceso a los servicios de impresoras es configurado por áreas o grupos de trabajo.

- Para garantizar el uso racional de papel, así como cumplir con la directiva presidencial 04 del 3 de abril de 2012. Se debe realiza la impresión de los documentos finales luego de ser revisados y se estos deben ser impresos a doble cara.

- El papel con información confidencial o sensible que ya no se requiera, no se debe reciclar, deberá destruirse inmediatamente.

Política de gestión de archivos

Los activos de información a los que hace referencia en este ítem corresponden a los archivos físicos y electrónicos cualquiera que sea su formato, información de los sistemas de información, software, licencias, manuales y los componentes tic como equipos, impresoras, entre otros.

a. Objetivo: Proteger adecuadamente los activos de información de la entidad mediante la asignación de estos a los usuarios finales, quienes deben responsabilizarse de su administración de acuerdo con sus roles y funciones asignadas.

b. Directrices:

- Los activos de información pertenecen al DADEP y el uso de estos debe emplearse exclusivamente con propósitos laborales institucionales.

- Los usuarios deberán utilizar únicamente los equipos y programas autorizados por la Oficina de Tecnología de la Información y las Comunicaciones.

- La entidad proporcionará al usuario, los equipos informáticos e instalará los programas que se requieran; la información creada, procesada, enviada y recibida, serán propiedad del DADEP y deberá almacenarse en las carpetas compartidas asignadas. Para copiar cualquier tipo de información clasificada o reservada debe pedir autorización a su jefe inmediato; la copia, sustracción, daño intencional o utilización para fines distintos a labores propias de la entidad, se sancionarán de acuerdo con las normas vigentes.

- Todos los requerimientos de información de los sistemas de información, archivos y equipos informáticos deben ser solicitados a través de la mesa de ayuda de la Oficina de Tecnología de la Información y las Comunicaciones.

- La Oficina de Tecnología de la Información y las Comunicaciones será la responsable de custodiar los medios magnéticos/electrónicos (DVDs, CDs u otros) que vengan originalmente con el software y sus respectivos manuales y licencias de uso, adicionalmente las contraseñas y códigos de autorización para descargar el software de fabricantes de sus páginas web o portales en internet y las contraseñas de administración de los equipos informáticos, sistemas de información o aplicativos.

- Los recursos de TI del DADEP no podrán ser utilizados para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, juegos en línea, publicidad política o cualquier otro uso que no esté autorizado.

- Ningún usuario deberá acceder a la red o a los servicios TIC del DADEP utilizando una cuenta de usuario o contraseña de otro usuario, este es personal e intransferible,

por lo tanto, es responsabilidad del usuario cualquier cambio o afectación que se realice sobre los activos con sus credenciales.

- Todos los archivos que provengan de fuentes externas al DADEP, deben ser examinados para detección de virus, antes de ser utilizados en la red de la entidad.

- Todos los cambios que se realicen a la infraestructura informática deben ser controlados y ejecutado por la Oficina de Tecnología de la Información y las Comunicaciones del DADEP.

- La información de la entidad debe ser respaldada de forma frecuente dando cumplimiento a lo establecido en la política de copias de seguridad de este documento.

Política de seguridad de los recursos humanos

a. Objetivo: Asegurar que los funcionarios, contratistas y demás colaboradores del DADEP, entiendan sus responsabilidades y las funciones de sus roles y usuarios, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información, de los recursos de TI y de las instalaciones de la entidad.

b. Directrices:

- Todos los funcionarios y/o contratistas serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido

- Todos los funcionarios, contratistas y usuarios externos, recibirán formación adecuada en concientización y actualizaciones regulares sobre las políticas y los procedimientos de la entidad, según sea pertinente para sus funciones laborales. El proceso de gestión del Talento Humano, junto con la Oficina de Tecnología de la Información y las Comunicaciones se encargará de ejecutar un plan de capacitación de seguridad en la información que garantice el uso adecuado de los sistemas.

- El funcionario, contratista y/o usuario externo que haga mal uso de los sistemas de información, o de la información que le ha sido entregada para su gestión, acarreará las sanciones disciplinarias pertinentes que han sido establecidas por la ley.

- Todos los funcionarios, contratistas o usuarios externos deben devolver todos los activos que estén en su poder, pertenecientes a la entidad, al finalizar su contratación laboral, contrato o acuerdo. Así mismo la Oficina de Tecnología de la Información y las Comunicaciones será la encargada de llevar a cabo los procedimientos necesarios para finalizar los derechos de acceso que hayan sido otorgados.

- Se prohíbe a los funcionarios, contratistas o usuarios externos la realización de pruebas de seguridad y los cambios en los activos fijos de información asignados, esta es una actividad de responsabilidad exclusiva de la Oficina de Tecnología de la Información y las Comunicaciones.

- Está prohibido el uso de dispositivos de almacenamiento externo (dispositivos móviles, DVD, CD, memorias USB, agendas electrónicas, celulares, etc.) que no sean de la entidad, ya que se puede generar riesgos de seguridad de la información por lo que cualquier extracción de información debe hacerse a través de la mesa de ayuda de la Oficina de Tecnología de la Información y las Comunicaciones.

- Los programas instalados por la Oficina de Tecnología de la Información y las Comunicaciones, en los equipos asignados a los funcionarios o contratistas, son de propiedad del DADEP. Adicionalmente, ningún funcionario o contratista debe realizar

instalación de software sin la autorización de la Oficina de Sistema. De ser necesario, estas instalaciones solo se realizarán por el personal de la Oficina de Tecnología de la Información y las Comunicaciones.

- Los recursos tecnológicos y de software asignados a los funcionarios y contratistas del DADEP son responsabilidad de cada uno de ellos.

- Los funcionarios son responsables disciplinaria y legalmente de la divulgación no autorizada de información institucional.

- Es responsabilidad de cada usuario proteger la información de la entidad que está contenida en documentos, formatos, listados, etc.

- Los dispositivos electrónicos (computadores, impresoras, fotocopiadoras, escáner, etc.) solo deben utilizarse para los fines institucionales.

- Cualquier evento o posible incidente que afecte la seguridad de la información, debe ser reportado a la mesa de ayuda mesadeayuda@dadep.gov.co.

- La fuente de la información para dar respuestas a peticiones debe ser la que reposa en los sistemas de información y no de archivos personales.

Política de gestión de página web

a. Objetivo: Asegurar que los sitios web de la entidad cumplan con los estándares establecidos por Govimentum, el cual busca facilitar el uso, implementación y estandarización de los portales web del Distrito.

b. Directrices:

- La Oficina de Tecnología de la Información y las Comunicaciones aplicará en la estructuración de los sitios web de la entidad, los lineamientos y estándares de Govimentum, para facilitar el uso de los sitios por parte de la ciudadanía en todos los portales del Distrito, de una forma más segura.

- La oficina de comunicaciones en acompañamiento de la Oficina de Tecnología de la Información y las Comunicaciones será la responsable de los diseños y contenidos de la página web de la entidad, teniendo en cuenta siempre los estándares establecidos por gobierno en línea y ley de transparencia, todos los contenidos publicados en la página serán avalados por la oficina de comunicaciones.

- La Oficina de Tecnología de la Información y las Comunicaciones fomentará el uso de las tecnologías de seguridad en autenticación, cifrado, uso de protocolos http seguros, certificados SSL y TLS, en la medida de los posible.

Política de gestión de comunicaciones y operaciones

a. Objetivo: Asegurar que los usuarios de los servicios de TIC identifiquen fácilmente donde encontrar la documentación y tengan claridad en la forma de proceder para utilizar los servicios.

b. Directrices:

- La Oficina de Tecnología de la Información y las Comunicaciones documentará y adoptará formalmente los instructivos, guías y/o manuales necesarios para desplegar cada una de las políticas asociadas a los temas de seguridad de la información, de los que habla el presente documento. Estos serán públicos para cualquier funcionario o contratista que los requiera en el sistema integrado de gestión SIG, en la URL http://sgc.dadep.gov.co.

- Todos los requerimientos de TIC deben ser escalados a través de la mesa de ayuda y con los formatos en los casos en los que se requiere.

- Cualquier cambio en los servicios o sistema de información, debe ser conocido, documentado y autorizado por la Oficina de Tecnología de la Información y las Comunicaciones.

- Los sistemas de información que se encuentran en periodo de prueba deben ser controlados con usuarios autorizados para evitar riesgos de acceso o cambios no autorizados.

- Se asegurará que los controles de seguridad, las definiciones del servicio y los niveles de prestación del servicio de terceros sean implementados, mantenidos y operados por los terceros.

- Para los sistemas de información nuevos o actualizaciones, se establecerán criterios de aceptación por parte de los usuarios, entre los que se deben incluir funcionalidad, cumplimiento de criterios de data definidos en el requerimiento y validaciones.

- Se implementarán acciones de sensibilización a usuarios frente a los controles de detección, prevención y recuperación de datos contra códigos maliciosos.

- La Oficina de Tecnología de la Información y las Comunicaciones generará las copias de respaldo de la información y del software, realizando pruebas periódicas de acuerdo con la política de respaldo acordada.

- Para evitar la divulgación, modificación, retiro o destrucción de activos no autorizada, se asegurará que su eliminación se haga de forma segura y sin riesgo.

Política de control de acceso

a. Objetivo: Establecer los controles y directrices a seguir para la adecuada administración del control de acceso a los recursos informáticos de la Defensoría del Espacio Público.

b. Directrices:

- Cada funcionario, contratista o usuario externo contará con un usuario únicamente para su uso personal, es exclusivo y no debe ser compartido con otros usuarios.

- Las sesiones inactivas se deben bloquear después de un periodo de inactividad definido por la Oficina de Tecnología de la Información y las Comunicaciones.

- Se llevará a cabo el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información. Esta tarea está a cargo de la Oficina de Tecnología de la Información y las Comunicaciones quién controlará la asignación de privilegios y contraseñas y revisará periódicamente dichos derechos.

- Las cuentas de los usuarios retirados de la entidad serán bloqueadas y posteriormente su posterior eliminación deberá ser aprobada por el jefe de la Oficina de Tecnología de la Información y las Comunicaciones.

- Es responsabilidad de los funcionarios, contratistas o usuario externos generar buenas prácticas en la selección de usos de contraseñas de acuerdo con lo establecido en los documentos internos de la entidad, para tal fin. De igual forma será su responsabilidad, llevar a cabo buenas prácticas de escritorio despejado y política de pantalla despejada.

- La Oficina de sistema otorgará accesos a los servicios, de acuerdo con las autorizaciones específicas solicitadas por el líder del proceso o quien este delegue, solicitud que se debe escalar a la mesa de ayuda mesadeayuda@dadep.gov.co, en el formato único de sistemas FUS, debidamente diligenciado por el líder de proceso.

- La Oficina de Tecnología de la Información y las Comunicaciones establecerá los controles para acceso lógico y físico a los puertos de configuración y de diagnóstico, redes compartidas, enrutamiento en las redes y sistemas operativos.

Política de adquisición, desarrollo y mantenimiento de sistemas de información

a. Objetivo: Definir los lineamientos y controles en la adquisición, desarrollo y mantenimiento de los sistemas de información, haciendo uso de las mejores prácticas en el desarrollo y mantenimiento de software.

b. Directrices:

- La adquisición, desarrollo y mantenimiento de los sistemas de información, deberán adelantarse dando cumplimiento a lo establecido en la guía de "Sistemas de información", del proceso de Gestión de la Información y la Tecnología.

- Los sistemas de información contendrán validaciones de los datos de entrada, que permitan mantener la integridad de los datos, también deben asegurar que el formato de visualización sea estándar para los usuarios para evitar distintas interpretaciones.

- Los sistemas de información deben implementar mecanismos de integridad referencial para asegurar la persistencia correcta de los datos.

- La instalación y configuración de los sistemas de información en los computadores será coordinada y realizada por la Oficina de Tecnología de la Información y las Comunicaciones como único responsable. A su vez se generarán los mecanismos necesarios para garantizar la protección y control de datos de prueba y códigos fuente de los programas.

- En cuanto a la seguridad en el desarrollo y soporte de software, se establecerán los procedimientos necesarios para el control de cambios, revisando y sometiendo a prueba las aplicaciones críticas para la entidad, antes de pasarla a producción. Estas políticas aplican de igual forma a los contratos externos que estén relacionados con el tema.

- La entidad llevará a cabo el diagnóstico de las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluando la exposición de la organización a dichas vulnerabilidades y tomando las acciones apropiadas para tratar los riesgos asociados.

- Las máquinas virtuales para pruebas y desarrollo deben ser máximo 30 GB para máquinas con sistema operativo Linux y 70 GB para máquinas con sistema operativo Windows.

- Para cada proyecto de software deberá tenerse solamente una máquina para el desarrollo y otra para pruebas.

- Los ambientes de desarrollo y pruebas serán proporcionados por la ENTIDAD teniendo en cuenta que a estos ambientes se les aplica procedimientos de seguridad (control de acceso, copias de seguridad, mantenimiento).

- La solicitud de ambientes de desarrollo y pruebas deberán solicitarse a la mesa de ayuda y solo será aprobada por la jefe de la Oficina de Tecnología de la Información y las Comunicaciones.

- El Sr. Ariosto tendrá la responsabilidad de preparar los servidores y el Ingeniero Enrique coca deberá facilitar el ambiente de bases de datos.

- Los desarrolladores deben gestionar los requerimientos, el código fuente y el versionamiento de los desarrollos en el servidor GITEA (GIT).

- El líder de infraestructura establecerá las tareas automatizadas (JOB) para copiar las máquinas de desarrollo y pruebas a nube de AZURE y la información tendrá copias incrementales).

Política de gestión de incidentes de seguridad de la información

Los delitos informáticos cuando se clasifican dentro de los establecidos en la ley 1273 de 2009, deben ser reportados al centro cibernético de la policía nacional COLCERT, en la url https://www.policia.gov.co/denuncia-virtual/delitos-informaticos, de no hacerlo la entidad o el funcionario responsable (respondiente), se convierte en cómplice del delito.

a. Objetivo: Definir el mecanismo para gestionar los incidentes de seguridad de la información que se presenten en la Defensoría del Espacio Público.

b. Directrices:

- Detección de Incidente: Siempre que un usuario detecte alguna amenaza que atente contra la seguridad de la información como: descarga de virus, suplantación de sitios web, estafas, violación de derechos de autor o ataques a sistemas de información, infraestructura, página web o cualquier otro componente TIC, violando la ley 1273 de 2009, deberá reportarla a la mesa de ayuda para iniciar su respectivo tratamiento.

- Clasificación: Una vez comunicado el incidente detectado, un técnico experto pasará a clasificarlo de acuerdo con la ley 1273 de 2009.

- Resolución del incidente: Se debe hacer un diagnóstico de la gravedad del incidente y evaluar el tiempo estimado para resolverlo. El técnico designado ejecutará las acciones necesarias para dar solución. Una vez resuelto el incidente, se procederá a dar respuesta al funcionario que reportó y se documentará en la mesa de ayuda para conformar una base de conocimiento que permita dar solución de nuevos incidentes.

- Trámite: En caso de que el incidente reportado se encuentre clasificado dentro de los delitos de la ley 1273 de 2009, este debe ser reportado por el respondiente al centro cibernético de la Policía Nacional, a través de la Secretaría Jurídica del Distrito. Para reportarlo se deben tener las evidencias.

- Seguimiento: El respondiente es el encargado de hacer seguimiento al incidente reportado en el centro cibernético de la Policía Nacional hasta lograr una respuesta de fondo por parte de la Policía Nacional.

- Cierre al incidente: Resuelto el incidente por parte de la Policía Nacional, se documentará en la mesa de ayuda el tratamiento dado de cara a saber cómo actuar frente a incidentes similares futuros y se comunica a los directivos de la entidad el resultado.

- Si el incidente lo requiere, se debe implementar las medidas necesarias para realizar el trabajo de informática forense el cual sirva y contenga validez jurídica. De lo contrario se contratará a expertos para llevar a cabo esta función.

Política de gestión de continuidad del negocio

a. Objetivo: Definir el mecanismo que permita la continuación de las principales operaciones de la Entidad en el caso de un evento o siniestro imprevisto que inhabilite total o parcialmente los servicios críticos prestados por la entidad.

b. Directrices:

- Debe existir un inventario de los activos de información que se consideren críticos, que sean objeto de inclusión en el plan de continuidad del negocio.
- Deben establecerse los responsables y sus funciones para la ejecución del plan de continuidad del negocio en cada uno de los procesos o áreas.
- Debe definir los recursos requeridos para la implementación del plan de continuidad del negocio.
- El plan de continuidad del negocio del DADEP debe estar documentado.
- La entidad deberá realizar las pruebas y simulacros del plan de continuidad del negocio que permitan que su ejecución sea más efectiva, dejando registro de estas.
- La alta dirección debe aprobar, adoptar y socializar el plan de continuidad de negocio definido para el DADEP.
- La entidad deberá ejecutar el plan de continuidad del negocio en las situaciones que se haga necesario, dando aplicación a lo establecido en este, dejando registro de las actividades de su implementación.
- La entidad deberá realizar un análisis de resultado luego de que se termine la contingencia para hacer una mejora continua al plan establecido.
- La entidad deberá registrar las restauraciones periódicas que se e realicen a las copias de respaldo.

Política de gestión de activos de Información

a. Objetivo: Identificar los activos de la organización, definir los responsables y establecer los mecanismos de protección apropiados.

b. Directrices:

- Los activos de información del DADEP, serán identificados, clasificados y asignados como propiedad de algún proceso de la entidad para establecer los responsables y los mecanismos de protección necesarios. Cada dependencia, deberá elaborar y mantener actualizado el inventario de los activos de información (procesada y producida).

- El área de archivo determinará los requerimientos legales de retención a la documentación física y digital de la entidad en cualquiera de sus procesos.

- La clasificación de los niveles de privacidad, publicación, divulgación y nivel de riesgo será una labor conjunta entre la Oficina Jurídica, la Oficina Asesora de Planeación y el responsable de los riesgos.

- Identificar y mantener actualizado el Registro de Activos de Información para los procesos que lideran, diligenciando el formato de Inventario de Activos de Información con toda la información requerida para cada uno de los activos.

- Informar a la OTIC los cambios realizados enviando el Inventario actualizado cada vez que se registren novedades en él.

Política de seguridad física y del entorno

a. Objetivo: Definir y divulgar a toda la entidad los lineamientos que deben ser implementados para prevenir el acceso físico no autorizado a las instalaciones de procesamiento de información y evitar la materialización de daños o fallas que puedan afectar la seguridad de la información y las operaciones del DADEP.

b. Directrices:

- Está prohibido el paso al personal no autorizado al centro de cómputo, área que contiene los servicios de procesamiento de la información. Este acceso será autorizado por el director y/o jefe de Oficina de Tecnología de la Información y las Comunicaciones únicamente.

- La entidad diseñará y aplicará las protecciones físicas necesarias para garantizar la protección de la información contra formas de desastre natural o artificial.

- Todo funcionario de la Oficina de Tecnología de la Información y las Comunicaciones deberá aplicar las directrices establecidas y utilizar la protección física adecuada para trabajar en áreas seguras.

- Los equipos que contiene la información de la entidad estarán protegidos para reducir el riesgo por amenazas o peligros del entorno, accesos no autorizados o fallas en los servicios de suministro; recibirán mantenimiento periódico para asegurar su continua disponibilidad e integridad y serán verificados para garantizar que no se eliminan datos sensibles.

- Ningún equipo, información, ni software se deben retirar sin autorización previa y con el acompañamiento de la Oficina de Tecnología de la Información y las Comunicaciones.

Política de cumplimiento

c. Objetivo: Definir el mecanismo para hacer seguimiento y controlar el cumplimiento de la normatividad y actualización de la documentación asociada a la seguridad de la información.

d. Directrices:

- Es deber de cada funcionario, contratista o usuario externo conocer, adoptar e implementar los controles y políticas definidas en el documento de POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

- La Oficina de Tecnología de la Información y las Comunicaciones se encargará de definir explícitamente, documentar y mantener actualizados para cada sistema de información los requisitos estatutarios, reglamentarios y contractuales pertinentes.

- Será responsabilidad de las áreas competentes imponer las penalizaciones respectivas en caso de incumplimiento o trasladarlas a las entidades competentes.

- La entidad se compromete a implementar todas las acciones de seguridad de la información que garanticen la protección contra pérdida, destrucción y falsificación de la información, la protección de los datos y la privacidad de acuerdo con la legislación y los reglamentos pertinentes.

- Es responsabilidad de la dirección garantizar que todos los procedimientos de seguridad dentro de sus procesos se lleven a cabo correctamente para lograr el cumplimiento con las políticas y las normas de seguridad.

- Periódicamente la Oficina de Tecnología de la Información y las Comunicaciones revisará los procesos, procedimientos, manuales, guías y formatos asociados a la seguridad de la información y determinará el nivel de cumplimiento de las normas de implementación de la seguridad de la información al interior del DADEP.

- Es responsabilidad de cada funcionario, contratista o usuario externo no utilizar los servicios de procesamiento de información para propósitos no autorizados.

Política para la gestión de dispositivos móviles

a. Objetivo: Definir los lineamientos técnicos, funcionales, regulatorios y de seguridad para que los colaboradores, contratistas y terceras partes autorizados, puedan conectar sus dispositivos móviles a la red del DADEP.

b. Directrices:

- La entidad es responsable de contar y proporcionar una infraestructura física y lógica que garantice conexiones seguras a los dispositivos móviles autorizados.
- Con previa aprobación del líder de proceso la asignación de los dispositivos móviles se realiza de acuerdo con las responsabilidades.
- Cada dispositivo móvil se entregará únicamente con los accesorios originales propios.
- La Oficina de Tecnología de la Información y las Comunicaciones debe entregar los dispositivos móviles configurados con los controles de acceso lógico, las aplicaciones y servicios autorizados por la entidad.
- Los dispositivos móviles solo podrán ser intervenidos físicamente por personal autorizado por la entidad.
- La configuración de aplicaciones y servicios de la entidad dispositivos móviles que no sean de la entidad deberán ser autorizados por la misma.
- Los colaboradores no podrán retirar de las instalaciones del DADEP sin previa aprobación y autorización de la entidad.
- El uso de los dispositivos móviles debe ser racional y debe orientarse estrictamente para el desarrollo de sus funciones.
- Si en el periodo de tiempo de 48 horas el colaborador no reporta la pérdida o el daño del dispositivo móvil a su cargo, será su responsabilidad de reposición el 100% del valor.
- Cuando se retire un colaborador de la entidad debe retornar los dispositivos móviles y se deberá verificar su buen estado.
- No está permitido que los funcionarios realicen labores que generen costos adicionales, descarguen e instalen software no autorizado en los dispositivos móviles de la entidad.

- Los colabores se acogen a los lineamientos de navegación que imparte la entidad, las cuales prohíben la consulta de páginas violentas, pornográficas o que atenten contra los principios, ética y moral de los colaboradores.

- El no cumplimiento a esta política por parte de los colaboradores a los que se les asigne un dispositivo móvil dará lugar a las sanciones definidas en el Reglamento Interno de Trabajo, las cláusulas que apliquen al incumplimiento dentro del Contrato y demás normativas que resulten aplicables.

- Los servicios técnicos y de soporte solo se podrá solicitar a la Mesa de Ayuda.

Política de uso de controles criptográficos

a. Objetivo: Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad e integridad de la información digital etiquetada como Confidencial.

b. Alcance

La Política de Controles Criptográficos será dirigida por la Oficina de Tecnología de la Información y las Comunicaciones y aplicada por los desarrolladores Internos y Externos, que diseñen y desarrollen sistemas de información para el DADEP.

c. Directrices:

Directrices para la DADEP

1. Para el cumplimiento de esta política se debe tener previamente establecido el inventario de activos de tipo información junto a su clasificación y etiquetado.

2. La información digital etiquetada como confidencial debe ser almacenada y/o transmitida bajo técnicas de cifrado, con el propósito de proteger su confidencialidad e integridad.

3. Debe verificar que todo sistema de información o aplicativo que almacene o transmita información confidencial cuente con mecanismos de cifrado de datos.

4. Debe definir e implementar estándares para la aplicación de controles criptográficos.

5. Utilizar controles criptográficos en los siguientes casos:

    - Para la protección de contraseñas de acceso a sistemas, datos y servicios.
    - Para la transmisión de información clasificada como confidencial.
    - Para proteger la información cuando la evaluación de riesgos lo indique.

6. Definir:

    - Procedimiento para la gestión de contraseñas
    - Procedimiento para la recuperación de información cifrada en caso de pérdida, compromiso o daño de las contraseñas.
    - Procedimiento para el cambio o restauración de las contraseñas de cifrado.

7. Definir y asignar el rol de responsable de la gestión de contraseñas.

8. Establecer los algoritmos de cifrado a utilizar para los distintos escenarios, así como la longitud de las contraseñas.

Directrices para desarrolladores:

- Los Desarrolladores Internos y Externos deben utilizar mecanismos de cifrado en las aplicaciones que procesen información confidencial.

- Los Desarrolladores Internos y Externos deben asegurar que los controles criptográficos de los sistemas de información desarrollados para el DADEP, cumplen con los estándares establecidos por la entidad.

Política de gestión de activo

a. Objetivo: Identificar los activos de la organización, definir los responsables y establecer los mecanismos de protección apropiados.

b. Directrices:

- Los activos de información del DADEP, serán identificados, clasificados y asignados como propiedad de algún proceso de la entidad para establecer los responsables y los mecanismos de protección necesarios. Cada dependencia, deberá elaborar y mantener actualizado el inventario de los activos de información (procesada y producida).
- Identificar y mantener actualizado el Registro de Activos de Información para los procesos que lideran, diligenciando el formato de Inventario de Activos de Información con toda la información requerida para cada uno de los activos.
- Informar a la Oficina de Tecnología de la Información y las Comunicaciones – Seguridad de la Información, los cambios realizados enviando el Inventario actualizado cada vez que se registren novedades en él.
- El área de archivo determinará los requerimientos legales de retención a la documentación física y digital de la entidad en cualquiera de sus procesos.
- La clasificación de los niveles de privacidad, publicación, divulgación y nivel de riesgo será una labor conjunta entre la Oficina Jurídica, la Oficina Asesora de Planeación y el responsable de los riesgos.

6.2 PROCEDIMIENTOS QUE APOYAN A LAS POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Los procedimientos son la parte fundamental dentro de la estructuración y la manera de hacer las cosas en una organización.

Un procedimiento describe de forma más detallada las actividades de un proceso, en él se especifica cómo se debe desarrollar una actividad, el alcance, los recursos, entradas, salidas y el objetivo que se pretende lograr y caracteriza el proceso.

Para llegar a un mayor detalle de las actividades descritas en este manual, se hará uso de instructivos, Guías y formatos que permitirán de manera puntual detallar aún más las tareas, controles y acciones puntuales que se deben desarrollar dentro de un procedimiento.

Los usuarios de la Defensoría del Espacio Público pueden consultar la documentación asociada al proceso de "Gestión de la Información y la Tecnología", a través del sistema integrado de gestión SIIG, en la que encontrará la caracterización del proceso, procedimientos, manuales, guías, instructivos y formatos asociados al proceso y en el que se encuentra de manera detallada las actividades del proceso.

Procedimiento de Soporte y mantenimiento de la Infraestructura Tecnológica

Este procedimiento tiene como objetivo Garantizar la disponibilidad de la infraestructura tecnológica de la entidad, para lo cual se contará con servicios externos para el mantenimiento preventivo y correctivo de la infraestructura, entendiéndose esta como los componentes del centro de cómputo, sistemas de información, equipos de escritorio, portátiles, impresoras, escáner, video proyector y plotters. Se programarán un número específico de mantenimientos y el suministro de repuestos cuando se requiera.

Los casos de soporte de infraestructura que se presenten cotidianamente y los casos de soporte de software y otros componentes de TI, serán resueltos por el personal adscrito a la Oficina de Tecnología de la Información y las Comunicaciones y siempre serán registrados, gestionados y administrados a través de la mesa de ayuda y haciendo uso de los formatos establecidos según el caso; si hay casos de infraestructura o de sistemas de información propietarios que no se puedan resolver internamente, se escalarán al servicio externo (proveedores).

Procedimiento de seguridad de la Información

Este procedimiento tiene como objetivo mantener la confidencialidad, integridad y disponibilidad de la información, haciendo uso adecuado de las políticas específicas de seguridad y privacidad de la información establecidas en el documento de la 'Política General de Seguridad y Privacidad de la Información y los documentos que la desarrollan.

La seguridad de la información es un tema trasversal a todos los procesos, funcionarios y contratistas de la entidad y es responsabilidad de todos unir esfuerzos y hacer uso de las buenas prácticas para evitar siniestros que terminen con la puesta en riesgo de la integridad, disponibilidad y confidencialidad de la información.

La Oficina de Tecnología de la Información y las Comunicaciones se encargará de documentar, actualizar, socializar e implementar los mecanismos a que haya lugar para el desarrollo e implementación de la política general de seguridad de la información.

Procedimiento de Sistemas de Información

Este procedimiento tiene como objetivo realizar actualizaciones, soporte y mantenimiento a los sistemas de información, que contribuyen al cumplimiento de las diferentes actividades del DADEP.

Los casos de soporte de los sistemas de información que se presenten cotidianamente serán resueltos por el personal adscrito a la Oficina de Tecnología de la Información y las Comunicaciones y siempre serán registrados, gestionados y administrados a través de la mesa de ayuda y haciendo uso de los formatos establecidos cuando aplique.
Para el mantenimiento, actualización y nuevos desarrollos de los sistemas de información, se dará aplicación a lo establecido en la guía de sistemas de información, actividades que serán priorizadas y asignadas a los ingenieros para su desarrollo.

Actualizó: Carlos De la Ossa – Contratista OTIC

Revisó: Syrus Pacheco – Jefe OTIC

Aprobó: Syrus Pacheco – Jefe - OTIC

CONTROL DE CAMBIOS		
VERSIÓN	**FECHA**	**DESCRIPCIÓN DE MODIFICACIÓN**
2	27/12/2022	Se adicionan directrices al numeral Política de Gestión de Activo Aprobado mediante Acta 006/2022 Comité Institucional de Gestión y Desempeño 27/12/2022