ÁREA METROPOLITANA DEL VALLE DE ABURRÁ

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

CONTENIDO

INTRODUCCIÓN

La información definida como "datos dotados de significado y propósito", se ha convertido en un componente indispensable en la conducción de las entidades. En este contexto, un Sistema de Gestión de Seguridad de la Información-SGSI, contribuye a mantener la confidencialidad, integridad y disponibilidad de esta información mediante la aplicación de un proceso de gestión de riesgos basado en la norma ISO 27001, la cual ha sido desarrollada con el propósito de brindar un modelo que permita a las entidades, gestionar la seguridad de la información en el entorno corporativo.

En ese sentido, la implementación de un SGSI es una decisión estratégica de una entidad, adoptada con el fin de velar por la seguridad de la información en la ejecución de los procesos críticos del negocio.

El SGSI del Área Metropolitana del Valle de Aburrá ha sido desarrollado teniendo en cuenta el concepto de procesos y busca garantizar la seguridad de la información, así como definir el funcionamiento del sistema bajo un enfoque de mejora continua. Asimismo, la Entidad se ha comprometido a realizar diversas actividades para resguardar la seguridad de la información de sus procesos, mediante el análisis de los requisitos para la protección de los activos de información y la aplicación de los controles adecuados para garantizar la protección de estos activos de información.

1. OBJETIVO

Implementar el sistema de gestión de seguridad de la información del Área Metropolitana del Valle de Aburrá, basado en el estándar ISO-IEC 27001, alineado con los Decretos 2693 de 2012, 1078 de 2015 y 1499 de 2017, con el fin de aumentar los niveles de confianza en la información disponible en la Entidad y en la información entregada para el servicio de los ciudadanos, además por medio del modelo de la seguridad y privacidad de la información, se suscite la cultura de la seguridad de la información en la Entidad, buscando minimizar los riesgos identificados en la gestión, protegiendo los activos de información, fortaleciendo la integridad, confidencialidad y disponibilidad de los mismos.

2. ALCANCE

La política general de seguridad de la información de la Entidad cubre todos los procesos y dependencias que hacen parte de la organización administrativa, y se fundamenta en el modelo de seguridad y privacidad de la información y en el sistema de gestión de seguridad de la información, los cuales deben estar alineados con los sistemas de gestión de la Entidad, teniendo como cimiento los siguientes los principios:

3. PRINCIPIOS

Los principios de la política general de la privacidad y seguridad de la información se basan en el manual de políticas de seguridad y privacidad de la información de la Entidad, se aplican los controles descritos en el *Anexo A de la norma ISO/IEC 27001* bajo los siguientes principios sugeridos por *MINTIC*:

3.1. Principio sobre soporte de información: Las responsabilidades frente a la seguridad de la información son definidas, compartidas, publicadas y aceptadas por cada uno de los clientes internos, externos y partes interesadas.

3.2. Principio sobre las instalaciones: Proteger la información generada, procesada o resguardada por los procesos misionales, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (clientes internos, externos y partes interesadas).

3.3. Principio sobre la información: Proteger la información creada, procesada, transmitida o resguardada por los procesos misionales, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

3.4. Principio sobre el personal: Proteger su información de las amenazas originadas por parte del personal.

3.5. Principio sobre las instalaciones: Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

3.6. Principio sobre las aplicaciones: Controlar la operación de los procesos misionales garantizando la seguridad de los recursos tecnológicos y las redes de datos.

3.7. Principio sobre las comunicaciones: Garantizar a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

3.8. Principio sobre los procesos: Garantizar la disponibilidad de los procesos misionales y la continuidad de su operación basada en el impacto que pueden generar los eventos.

3.9. Principio de los sistemas operativos: Garantizar el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas, teniendo en cuenta el licenciamiento vigente.

3.10. Principio sobre el ciclo de vida de los sistemas de información: Garantizar que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

3.11. Principio de control de acceso: Implementar controles de acceso a la información y recursos de red.

3.12. Principio sobre normatividad: Garantizar el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

4. APLICABILIDAD DE LAS POLÍTIAS DE SEGURIDAD DE LA INFORMACIÓN

La política general de la seguridad de la información de la Entidad aplica a los clientes internos, externos y partes interesadas.

4.1. TÉRMINOS Y DEFINICIONES

4.1.1. Activo: Algo que tenga valor para la organización, puede ser tangible, intangible, humano, etc.
4.1.2. Confidencialidad: Propiedad para una determinada información, estar disponible y no ser divulgada a personas, entidades o procesos no autorizados.
4.1.3. Disponibilidad: Propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.
4.1.4. Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con relación al riesgo.
4.1.5. Integridad: La propiedad de salvaguardar la exactitud e integridad de los activos.
4.1.6. Tratamiento del riesgo: Proceso de tratamiento de la selección e implementación de medidas para modificar el riesgo.

Asimismo, para el caso específico del sistema de gestión de seguridad de la información, se consideran las siguientes definiciones:

1) **Acceso físico:** Significa poder ver, tocar y modificar una computadora y sus instalaciones.
2) **Acceso lógico:** Es un acceso en red a través de la Intranet, el Internet, redes, infraestructura, bases de datos.
3) **Acceso remoto:** Conexión a una computadora o servidor con conexión a una red o Internet sin importar las distancias, a través de programas virtuales, no siendo necesaria la presencia física.
4) **Activo de información:** Es toda la Información utilizada en la Entidad, la cual puede ser trasmitida vía oral, escrita o generada a través de medios informáticos.
5) **Administrador de red:** Persona responsable de mantener un LAN y de la implementación, monitoreo y ejecución de los controles de seguridad establecidos y autorizados por la Entidad.
6) **Amenaza:** Causa potencial de un incidente no deseado que puede resultar en daño al sistema u organización.
7) **Análisis de Sistemas:** Fase del desarrollo de los sistemas en la que se elaboran las especificaciones de los sistemas y los diseños conceptuales, basados en las necesidades y los requerimientos de los usuarios finales.
8) **Análisis del Impacto en el Negocio:** Proceso para determinar el impacto de perder la continuidad de un proceso crítico de una organización. Este estudio de evaluación establece el incremento de esa pérdida en el tiempo.
9) **Autenticación:** Acto de verificar la identidad y la elegibilidad de un usuario para tener acceso a la información computarizada.
10) **Backup:** Copia de respaldo de archivos o datos, que están disponibles en caso de pérdida de los originales. Esta acción evita numerosos y a veces irremediables problemas si se realiza de forma habitual y periódica.
11) **Base de datos:** Colección almacenada de los datos relacionados que necesitan las organizaciones y las personas para satisfacer sus requerimientos de procesamiento y recuperación de Información.
12) **Cambio regular:** Cambios planificados.
13) **Cambios de emergencia:** Cambios imprevistos.
14) **Control biométrico:** Cerradura de puertas y de entradas que son activadas por características biométricas como por ejemplo la voz, la retina del ojo, las huellas dactilares o la firma digital.
15) **Clasificación de la información:** Identificación y estructuración sistemática de las actividades de los documentos generados por la Entidad, en categorías, de acuerdo con métodos y normas de procedimiento, lógicamente estructurados y representados en un sistema de clasificación.
16) **Cláusulas de confidencialidad:** Acuerdo de confidencialidad, o cláusula de confidencialidad, se constituye en una manifestación de la voluntad de las partes encaminada a producir la obligación de guardar y no revelar a terceros información que una de las partes desea proteger, y que se puede desarrollar en una etapa precontractual o incluir dentro de un contrato.
17) **Código fuente:** Archivos de texto plano escritos en un lenguaje de programación.
18) **Computadoras portátiles:** Computadoras con batería que le proporciona la capacidad de trabajo sin estar enchufada a la red eléctrica. Son conocidas generalmente como Notebooks o Laptops.
19) **Contingencia:** Medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del negocio y las operaciones de la Entidad.

20) **Contraseña:** Hilera de caracteres protegidos, generalmente encriptados por computadora que autentican a un usuario de computadora ante un sistema de información.
21) **Control:** Herramienta de gestión de riesgo, incluido políticas, pautas, estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, gerencial o legal.
22) **Control de acceso:** Mecanismos que permiten prevenir, detectar o remediar el acceso de personal no autorizado.
23) **Control de cambios:** Permite evaluar cualquier petición de cambio, incluye coordinar cambios correctivos y preventivos para evitar problemas adicionales.
24) **Declaración de aplicabilidad:** Documento que describe los objetivos de control y controles que son relevantes y aplicables al SGSI de la organización.
25) **Disco duro:** Dispositivo de almacenamiento más importante de la computadora en el que se guardan los archivos y programas.
26) **Equipo compartido:** Opción de compartir información o algunos dispositivos de las computadoras en red, para ser accedidas por otros equipos que no posean dicha información o recurso. Generalmente se puede compartir directorios o carpetas, impresoras, lectoras de CD/DVD.
27) **Equipos de cómputo:** Ordenadores y dispositivos creados para conectarse a estos o a una red informática.
28) **Dispositivos removibles:** Equipos que pueden ser trasladados fácilmente de un lugar a otro por ser pequeños y livianos, estos pueden ser entre otros:

    - ✓ Computadoras portátiles.
    - ✓ Tabletas.
    - ✓ Teléfonos celulares
    - ✓ USB (Memoria USB): Es un pequeño dispositivo de almacenamiento de información sin necesidad de baterías.
    - ✓ Discos externos, medios de almacenamiento instalados externamente a las computadoras y pueden ser removidos fácilmente por el usuario interno y otros clientes externos.

29) **Extintor:** Aparato a presión que contiene un agente (agua, polvo, espuma física, anhídrido carbónico u otro químico) que puede ser proyectado y dirigido sobre fuego por acción de una presión interna o externa, con el fin de proceder a su extinción.
30) **Firewall:** Dispositivo utilizado en redes de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas. Forma una barrera entre un ambiente seguro y uno abierto.
31) **Firmas de virus:** Pequeñas muestras de partes de virus que el antivirus usa para identificar uno o varios ejemplares de malware.
32) **Hardware:** Conjunto de elementos materiales que conforman una computadora, es decir, los dispositivos físicos tales como el disco duro, CD-ROM, disquetera, entre otros.
33) **Incidente de seguridad de la información:** Una serie de eventos no deseados que tienen una probabilidad significativa de comprometer operaciones del negocio y amenazar la seguridad de la información.
34) **Instalaciones de procesamiento de la información:** Ubicación donde se concentran todos los recursos necesarios para el procesamiento de información de una organización. También se conoce como Centro de Proceso de Datos o Data Center.

Dichos recursos consisten en dispositivos debidamente acondicionados, servidores, computadoras y redes de comunicaciones.

35) **Intrusión:** También conocido como "Ingreso no autorizado a sistemas". Cometida por quien ingresa a un sistema informático sin autorización para acceder, por violación o desactivación de mecanismos de autenticación y seguridad, con el objeto de robar información crítica o atentar contra la integridad de ella.
36) **Intruso:** Persona que trata maliciosamente de tener acceso no autorizado a un sistema de información.
37) **Malware**: Programa o archivo dañino para la computadora que intenta conseguir algún objetivo, como podría ser el de recoger información sobre el usuario o sobre el ordenador en sí.
38) **Medio de almacenamiento:** Accesorios utilizados para guardar información (discos duros, cintas de backup, CD-ROM, disquetes, memorias USB, entre otros).
39) **Monitorear:** Acción de supervisar y vigilar las actividades de usuarios de recursos de TI. También conocido como el procedimiento de verificar o evaluar la ejecución de algún proceso manual o automático.
40) **Periféricos:** Equipo auxiliar de una computadora usado para entrada, salida y procesamiento de datos, por ejemplo, una impresora.
41) **Phishing:** Capacidad de duplicar una página web para hacer creer al visitante que se encuentra en la página original y acceder a sus datos personales tales como número de cuentas, claves secretas, etc.
42) **Pista de auditoría:** Pista visible de evidencias que permite que se rastree información contenida en sentencias o declaraciones o en reporte, permitiendo llegar a la fuente original donde se ingresó la Información.
43) **Política:** Directriz general y formal expresada por la alta dirección y acatada por todos los usuarios internos y externos.
44) **Portal Web:** Página principal de una persona natural o jurídica que permite el acceso a las distintas secciones de un sitio web, con información pública de la Entidad.
45) **Red de Área Ancha (WAN):** Red de computadoras que se conecta a diferentes lugares remotos que puede incluir desde distancias cortas, como por ejemplo un piso o un edificio, hasta transmisiones extremadamente largas que abarcan una región grande o varios países.
46) **Red de Área Local (LAN):** Redes de computadoras que sirven a varios usuarios dentro de un área geográfica específica.
47) **Plataforma tecnológica:** Infraestructura informática utilizada para el intercambio de información en una red privada integrada por computadoras, servidores, impresoras y cableado.
48) **Radiación electromagnética:** Es un tipo de campo electromagnético variable, es decir una combinación de campos eléctricos y magnéticos oscilantes, que se propagan a través del espacio transportando energía de un lugar a otro.
49) **Respaldo:** Archivos, equipos, datos y procedimientos disponibles para su uso en el caso de una falla o pérdida, si se destruyen los originales o si se está en el sitio alterno.
50) **Riesgo:** Combinación de la probabilidad de un evento y sus consecuencias.
51) **Router:** Dispositivo informático responsable de gestionar adecuadamente los caminos más rápidos y adecuado para la conexión a Internet.
52) **Segregación de funciones:** Control básico que previene o que detecta errores e irregularidades mediante la asignación de la responsabilidad de iniciar y de registrar

transacciones y la custodia de los activos. Se utiliza para que ninguna persona esté en posición de introducir códigos fraudulentos o maliciosos sin ser detectada.

53) **Seguridad de datos:** Controles que tratan de mantener la confidencialidad, la integridad y la disponibilidad de la información.
54) **Seguridad de la información**: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad.
55) **Servidor:** Computadora de alto poder, que pone recursos o servicios a disposición de otras computadoras. Estos recursos pueden ser datos, aplicaciones, etc.
56) **Servidor de archivos:** Servidor que almacena datos centralmente para los usuarios de la red y que administra el acceso a esos datos.
57) **Sesiones activas:** Conexiones a la red que no han sido cerradas.
58) **Sistema de gestión de seguridad de la información:** Es un sistema de seguridad basado en un enfoque de riesgos del negocio para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.
59) **Sistema operativo:** Programa de control principal que opera la computadora y que actúa como un creador de cronogramas y controlador de tráfico. Es el primer programa copiado a la memoria de la computadora después de que ésta es encendida y debe residir en la memoria todo el tiempo. Fija las normas para los programas de aplicación que se ejecutan en la misma.
60) **Software:** Colección de programas de computadora usados en el diseño, procesamiento y control de todas las aplicaciones. Incluye el sistema operativo y los programas utilitarios.
61) **Software de seguridad:** Software usado para administrar la seguridad lógica. Usualmente incluye autenticación de usuarios, otorgamiento de acceso conforme a reglas predefinidas, funciones de monitoreo y reporte.
62) **Spam:** Recepción de correos no solicitados, normalmente de publicidad engañosa, y en grandes cantidades que tienen la posibilidad de contener virus o programas espías, o replicas masivas de mensajes de datos.
63) **Spyware:** Aplicaciones ocultas que recopilan información sobre una persona u organización sin su conocimiento para distribuirlo a empresas publicitarias u otras organizaciones interesadas.
64) **Switch:** Dispositivos inteligentes que permiten conectar recursos de TI tales como computadoras, impresoras, etc.
65) **Terceros:** Proveedores de bienes o servicios que tienen convenios o razones contractuales con el Área Metropolitana del Valle de Aburra, que generalmente requieren tener acceso a la información o recursos de la organización mientras desempeña sus labores en la misma.
66) **Terminal:** Dispositivo para enviar y recibir datos computarizados por medio de líneas de transmisión.
67) **Tomas eléctricas:** Conocidos como tomacorrientes, lugar donde se conectan los artefactos eléctricos.
68) **Topología:** Disposición física de cómo las computadoras están conectadas en red.
69) **Tratamiento de la información:** Operaciones que las personas ejecutan con la información, las cuáles pueden ser muy variadas, como lectura, escritura, copia, traducción, transmisión, ordenación, comparación, archivo, etc.

70) **Unidad de red:** Es un directorio compartido desde otro equipo por medio de la red y que se encuentra conectado a una computadora como si fuera una unidad más, como un disco duro o una memoria USB.
71) **UPS (Fuente de Poder Ininterrumpido):** Equipo electrónico utilizado para almacenar energía durante operaciones normales a través de una batería y entregar la energía acumulada en forma estable cuando ocurren fallos en la red eléctrica.
72) **Usuario:** Cualquier persona que utilice información, programas, sistemas y equipos del Área Metropolitana del Valle de Aburra.
73) **Valoración del riesgo:** Proceso de comparación del riesgo estimado contra el criterio del riesgo dado para determinar el significado de este.
74) **Virus informático:** Es un programa de computadora, que tiene como objetivo causar una alteración en un sistema de cómputo. Al igual que otras amenazas, un virus puede causar la alteración total de programas e información, o comprometer su integridad
75) **Vulnerabilidad:** Debilidad de un activo o grupo de activos que pueden ser explotados por una o más amenazas.

5. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La Dirección del Área Metropolitana del Valle de Aburrá, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información-SGSI, buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la planeación estratégica de la Entidad.

El Área Metropolitana del Valle de Aburrá, con la protección de los activos de información, busca la disminución del impacto generado por los riesgos identificados de manera sistemática, asegurando la integridad, confidencialidad y la disponibilidad de los mismos, acorde con las necesidades de los clientes internos, externos y partes interesadas.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se define en su alcance y está basada en las siguientes premisas:

a. Minimizar el riesgo en las funciones de la Entidad.
b. Cumplir con los principios de seguridad de la información.
c. Mantener la confianza de los clientes internos, externos y partes interesadas.
d. Apoyar la innovación tecnológica.
e. Proteger los activos tecnológicos.
f. Cumplir con los principios de la función pública.
g. Establecer las políticas, manuales, procedimientos e instructivos en materia de seguridad de la Información.
h. Fortalecer la cultura de seguridad de la información en los clientes internos, externos y partes interesadas.
i. Garantizar la continuidad del negocio frente a incidentes.

Es por esto que el Área Metropolitana del Valle de Aburrá ha decidido definir, implementar, operar y mejorar de forma continua el SGSI basado en el estándar ISO-IEC 27001, soportado en lineamientos claros alineados a las necesidades institucionales, y a los

requerimientos regulatorios.

6. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

6.1. Política de estructura organizacional de seguridad de la información

Actualmente la Entidad viene implementando el sistema de gestión de seguridad de la información, basado en el estándar ISO-2700, dando cumplimento a la normatividad vigente, con el objetivo claro de preservar y dar seguridad al inventario de los activos de información, definiendo y estableciendo roles y responsabilidades que involucren las actividades de operación, gestión y administración de la seguridad de la información, el SGSI se articula plenamente con el Sistema de Gestión de Calidad.

6.2. Política para uso de dispositivos móviles

La Entidad establece las directrices de uso y manejo de dispositivos móviles (teléfonos móviles, teléfonos inteligentes, tabletas), entre otros, suministrados por el AMVA y los personales para el uso de los servicios de información de la Entidad. Los dispositivos entregados por el AMVA a sus funcionarios sólo podrán ser utilizados con fines laborales y se prohíbe el envío de cualquier información que sea clasificada como información pública reservada o información pública clasificada (privada o semiprivada).

Los usuarios no están autorizados a cambiar la configuración, a desinstalar o instalar software, formatear o restaurar de fábrica los equipos móviles institucionales, cuando se encuentran a su cargo, únicamente se deben aceptar y aplicar las actualizaciones.

Los dispositivos móviles personales sólo podrán conectar a la red Wi-Fi de invitados disponible y con fines laborales.

La Entidad tiene dispuestos 2 perfiles de conexión a la red Wi-Fi:

- ✓ ***InvitadoAMVA***
- ✓ ***AMVAInstitucional***.

InvitadoAMVA: está configurado para atender los requerimientos de los visitantes a la Entidad, los cuales deberán aceptar los términos y condiciones de uso del servicio e ingresar la contraseña disponible para tal fin, debido a lo anterior, esta es la red que alcanza el límite de su capacidad más rápido.

Se tiene como política cambiar la contraseña de la red ***InvitadoAMVA*** cada tres meses.

AMVAInstitucional: la experiencia de navegación es superior ya que está configurada para dar prioridad y beneficio a las personas que tienen vínculo directo con la Entidad, por lo cual la velocidad de conexión es mayor.

Se tiene como política cambiar la contraseña de la red ***AMVAInstitucional*** cada 6 meses.

6.3. Política de seguridad para los recursos humanos

Una gran parte de los incidentes de seguridad provienen de errores humanos, el objetivo de esta política es la de establecer los términos del empleo a fin de concienciar y capacitar al personal en el desarrollo de sus actividades enfocados a la seguridad de la información.

La Entidad debe garantizar que los funcionarios y contratistas conocen y entienden sus responsabilidades y deberá:

1) Investigar los antecedentes de las personas antes de tomar posesión del cargo o el inicio del contrato, según lo establecido por las normas vigentes.
2) Incluir en los manuales de funciones y contratos las obligaciones y responsabilidades de ambas partes en lo relacionado a seguridad de la información.
3) Asegurar que los funcionarios y contratistas son conscientes de las políticas de seguridad establecidas en la entidad y que las cumplan, para ello se debe establecer:

    - Planes de concienciación y formación que se renueven periódicamente.
    - Medidas y comunicaciones de las acciones disciplinarias que la entidad podrá llevar a cabo ante el incumplimiento de las políticas establecidas.

6.4. Políticas de gestión de activos de información

1) Los equipos de cómputo (estaciones de trabajo, portátiles, impresoras, dispositivos móviles, Internet, redes, servidores, aplicaciones, entre otros) son activos de la Entidad y son asignados a los funcionarios y a terceros autorizados con el fin de ser utilizados como herramienta de trabajo en el ejercicio de las funciones o actividades relacionadas, estos activos deben ser inventariados, clasificados y asignados a un responsable de acuerdo al procedimiento del sistema de gestión de calidad, P-GLO-01 Administración de Bienes y Servicios.
2) Cada líder de proceso debe actuar como responsable de la información física y electrónica de la dependencia a cargo, ejerciendo así la facultad de aprobar o revocar el acceso a su información con los perfiles adecuados para tal fin.
3) La Oficina de Sistemas de Información debe levantar un inventario con el software y sistemas de información que se encuentran permitidos en las estaciones de trabajo para el desarrollo de las actividades laborales, así como verificar periódicamente que el software instalado en dichas estaciones de trabajo o equipos móviles corresponda únicamente al permitido y posee el debido licenciamiento.
4) Los supervisores deben verificar el estado y calidad de los activos de información entregados al contratista al momento del inicio del contrato y en su liquidación.
5) Sólo el Líder de la Oficina de Sistemas de Información puede autorizar la instalación de software en cualquier estación o dispositivo, por lo tanto, cualquier necesidad debe ser tramitada ante él de manera formal utilizando el procedimiento establecido para este fin.
6) Si los funcionarios o contratistas necesitan utilizar equipos propios, diferentes a los proporcionados por la Entidad, deben solicitar la autorización, verificación y registro del Líder de la Oficina de Sistemas de Información.

    El equipo de un externo debe tener iguales o superiores características de seguridad a las que poseen los equipos de la Entidad, así se puede autorizar la conexión a la red de

trabajo, mínimo debe poseer una licencia de antivirus legal y actualizada, sistema operativo legal con sus parches actualizados de lo contrario conlleva a la propagación de riesgos informáticos. Es responsabilidad del funcionario, contratista y/o tercero cumplir con dichas normas de propiedad intelectual y piratería, de los contrario no se le podrá dar autorización de uso.

Al iniciar el contrato, el supervisor debe gestionar para el contratista la autorización de uso ante la Oficina de Sistemas de Información, soporte técnico, quienes deberán implementar un control a nivel de switch o por medio de la MAC del equipo.

6.5. Política de uso de estaciones cliente

Las estaciones de trabajo son herramientas fundamentales y de uso cotidiano por parte de los funcionarios y contratistas de la Entidad. El correcto uso y adecuada administración de estas herramientas permite aumentar la productividad de todos y contribuye a garantizar la seguridad de la información.

- ✓ Solicitud: la asignación de elementos informáticos se hará con base en la solicitud de cada dependencia, previa aprobación de la alta dirección y según las funciones establecidas.
- ✓ Aprovisionamiento de hardware y software básico: Una vez aprobada la solicitud, el alistamiento y asignación del equipo debe hacerse siguiendo el procedimiento establecido por Oficina de Logística y la Oficina de Sistemas de Información siguiendo los procedimientos establecidos en el sistema de gestión de calidad de la Entidad.
- ✓ Entrega: La entrega formal al funcionario quien utilizará el equipo, en el sitio preestablecido, debe hacerse mediante firma del acta de responsabilidad, en la que se indica las condiciones y buenas prácticas para el buen uso establecidas en este manual.

6.6. Políticas de uso de Internet

La Entidad proporcionará los recursos necesarios que permitan garantizar y asegurar la disponibilidad de acceso a internet como herramienta de trabajo, para esto, la Oficina de Sistemas de Información deberá:

1) Proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de internet, bajo las restricciones de los perfiles de acceso establecidos.
2) Diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de internet en caso de contingencia interna.
3) Establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de internet y evitar el acceso a sitios catalogados como restringidos.
4) Generar registros de la navegación y los accesos de los usuarios a internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de internet.
5) Generar campañas para concientizar tanto a los funcionarios como a los contratistas, respecto a las precauciones que deben tener en cuenta cuando utilicen el servicio de internet.

6) Monitorear continuamente el canal o canales del servicio de internet, en cuanto a carga y tráfico.

6.6.1. **Los usuarios de internet dentro de la Entidad deben abstenerse de:**

a. Descargar material no autorizado, así como su instalación en las estaciones de trabajo asignados para el desempeño de sus labores, a menos que sean autorizados por la Oficina de Sistemas de Información.
b. Acceder a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y cualquier página que vaya en contra de la ética y la moral, las leyes vigentes del país o las políticas establecidas en este documento.
c. Utilizar el servicio de internet para el acceso y uso de servicios interactivos o mensajería instantánea como Facebook y otros similares, con el fin de intercambiar información confidencial o de uso interno de la institución o para actividades que no corresponden con el desempeño de las funciones asignadas.
d. Descargar, usar, intercambiar o instalar juegos, música, películas, información que de alguna manera atenten contra la propiedad intelectual de sus autores.
e. Intercambiar información confidencial de la Entidad sin la debida autorización.

6.7. Políticas de clasificación de la información

- ✓ La Entidad define los niveles más adecuados para clasificar su información, de acuerdo con su sensibilidad, la Oficina de Sistemas de Información genera una **Guía de Clasificación de la Información** para que los propietarios de esta la cataloguen y determinen los controles requeridos para su protección.
- ✓ Toda la información debe ser identificada, clasificada y documentada de acuerdo con la **Guía de Clasificación de la Información** establecida por el Comité para la Gestión de la Información.
- ✓ **La Guía de Clasificación de la Información** define los controles técnicos y administrativos que se implantan en la Entidad con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos en función de su nivel de clasificación.

6.8. Políticas de control de acceso

- ✓ Garantizar que los espacios u oficinas cuenten con los controles de acceso idóneos, los cuales aseguren el perímetro, así como en entornos abiertos para evitar el acceso no autorizado a ellos.
- ✓ Las Oficinas de Logística y Sistemas de Información controlan las amenazas físicas externas y velan por proveer las condiciones medioambientales requeridas para el funcionamiento de la plataforma tecnológica y para la preservación de sus activos de información digitales y físicos.
- ✓ La Oficina de Sistemas de Información debe asegurar la implantación y efectividad de mecanismos de seguridad física, controles de acceso físico y condiciones medioambientales con los que se debe contar.
- ✓ La Oficina de Logística conjuntamente con la Oficina de Sistemas de Información (funcionario con el rol de Oficial de Seguridad de la Información tienen la responsabilidad de vigilar y garantizar que se cumplan las siguientes medidas de seguridad:

- ❖ Las áreas que se catalogan como seguras deben permanecer cerradas y custodiadas.
- ❖ El acceso a áreas seguras donde se procesa o almacena información confidencial, de uso interno y público, es limitado únicamente a personas autorizadas.

6.8.1. **Política de establecimiento, uso y protección de claves de acceso**

Los usuarios de los recursos tecnológicos y los sistemas de información realizan un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual se les ha permitido el acceso.

Ninguna persona debe compartir sus cuentas de usuario y contraseñas asignadas para el ingreso a los servicios de red y los sistemas de información con otras personas y deben acogerse a las normas establecidas para la configuración de contraseñas designadas por la Entidad.

6.8.2. **Políticas de uso de puntos de red de datos (red de área local – LAN)**

La Oficina de Sistemas de Información debe:

- ✓ Proporcionar los recursos, el **procedimiento de autorización y controles** para proteger el acceso a las redes de datos y los recursos de red de la Entidad.
- ✓ Asegurar que las redes inalámbricas de la Entidad cuenten con métodos de autenticación que evite accesos no autorizados.
- ✓ Cumplir con todos los requisitos o controles para autenticarse y realizar las tareas para las que fueron autorizados según lo establecido en el SGSI es responsabilidad del usuario final que se conecten o deseen conectarse a las redes de datos de la Entidad.

6.8.3. **Política de uso de impresoras y del servicio de Impresión**

Los funcionarios o contratistas utilizan el carnet de la Entidad para acceder a los servicios de impresión, los mismos deben remover impresiones antes de dejar el lugar de trabajo, revisar que no queden documentos en cola de impresión y verificar que en las impresoras no queden trabajos impresos, fax, escáner y demás máquinas donde pueda haber papel con información confidencial, privada o restringida. Se deben triturar impresiones con datos sensibles una vez utilizados y que no se necesiten.

Sólo se podrá imprimir documentos relacionados con las actividades o funciones contractuales, está estrictamente **prohibido** utilizar los recursos de impresión para documentos personales.

6.8.4. **Políticas de controles criptográficos**

La Oficina de Sistemas de Información debe:

- ✓ Proporcionar los mecanismos y protocolos de seguridad y cifrado necesarios para asegurar que la transmisión de información confidencial de forma interna o externa se realice de forma segura.

- ✓ Proporcionar los mecanismos o herramientas necesarias para cifrar la información confidencial de la Entidad, resguardada por los propietarios de la información (Dirección, Secretaría General, Subdirecciones, Oficinas).
- ✓ Proporcionar los mecanismos o herramientas necesarias para asegurar la protección de claves de acceso a la red de datos, los sistemas de información, datos y servicios de la Entidad, de igual forma, debe proteger y salvaguardar los algoritmos o programas de cifrado y descifrado junto con las claves y/o semillas utilizadas por estos algoritmos utilizados por cualquier sistema de información utilizado por la Entidad.

6.8.5. **Políticas de seguridad física**

- ✓ El sitio escogido para colocar los equipos de cómputo y comunicaciones debe estar protegido por barreras y controles físicos, para evitar intrusión física, inundaciones, y otro tipo de amenazas que afecten su normal operación.
- ✓ Todos los sitios en donde se encuentren sistemas de procesamiento informático o de almacenamiento, deben ser protegidos de accesos no autorizados, utilizando tecnologías de autenticación, monitoreo y registro de entradas y salidas.
- ✓ Debe existir un área de recepción que solo permita la entrada de personal autorizado.
- ✓ Debido al posible robo, vandalismo y uso no autorizado de los sistemas de información, se debe considerar restringir el acceso de personas a las áreas consideradas seguras.

6.8.6. **Políticas de seguridad del centro de datos y centros de cableado**

- ✓ El Centro de Cómputo se debe establecer como área restringida y debe contar con un sistema de control de acceso el cual registre la información relacionada con la entrada y la salida de todas las personas que ingresan al mismo.
- ✓ Se debe realizar procedimientos de limpieza constantes al Centro de Cómputo con el fin de evitar la acumulación de polvo, el mismo que puede provocar daños a la infraestructura.
- ✓ El Centro de Cómputo debe poseer los **planos actualizado**s de las instalaciones eléctricas y de comunicaciones.
- ✓ Se deben adoptar procedimientos que permitan verificar constantemente las condiciones adecuadas ambientales como temperatura y humedad.

6.8.7. **Políticas de seguridad de los equipos**

- ✓ Ningún funcionario o contratista de la Entidad está autorizado a mover o reubicar los equipos de cómputo, instalar o desinstalar dispositivos sin la autorización del Líder de la Oficina de Logística o del Líder de la Oficina de Sistemas de Información.
- ✓ La Oficina de Logística debe resguardar los activos de información que se le asignan a los funcionarios o contratistas mediante la firma del usuario como responsable de estos.
- ✓ Los equipos de cómputo sólo pueden ser utilizados para uso exclusivo de las funciones asignadas.
- ✓ Ningún funcionario o contratista está autorizado para abrir o destapar los equipos de cómputo de la Entidad. Solo el personal de la Oficina de Sistemas de Información está autorizado para realizar esta labor.

6.8.8. **Políticas de escritorio y pantalla limpia**

La política de escritorio y pantalla limpia define las medidas preventivas de protección y las buenas prácticas, con respecto a las estaciones de trabajo y escritorio de todos los funcionarios y contratistas que desarrollan sus actividades en las instalaciones de la Entidad.

La finalidad de esta política es proteger los documentos de la Entidad, tanto los físicos como los digitales, y todo tipo de almacenamiento, al reducir los riesgos de acceso no autorizado a la información, y la pérdida y/o daño de esta.

Esta política se basa en las buenas prácticas que permiten mantener el orden y la limpieza en el puesto de trabajo.

- ✓ Los puestos de trabajo deben permanecer limpios y ordenados, y deben contar con los implementos básicos para poder desarrollar las funciones propias las actividades desempeñadas. No se debe comer o ingerir bebidas en el puesto de trabajo.
- ✓ El bloqueo estándar de Windows debe activarse máximo con una espera de cinco minutos de inactividad en los equipos de cómputo. Además, es necesario cerrar aplicaciones y bloquear la pantalla cuando se aleje de su escritorio. (Cerrar sesión de inicio de Windows y bloquear el equipo con comandos como Control + Alt + Supr, o la tecla de Windows +L).
- ✓ Todo funcionario o contratista es responsable por el cumplimiento de las normas y estándares establecidas en esta política, además, tiene la obligación de informar, a la Oficina de Sistemas de Información si observan incumplimiento de esta política por parte de otras personas, o informar a la Oficina de Logística en caso de que se esté exponiendo la confidencialidad, integridad y disponibilidad de la información. La omisión de esta norma se considera incumplimiento de las obligaciones laborales por parte del funcionario o contratista.
- ✓ En los lugares de trabajo deben existir medidas de seguridad física y digital tendientes a la protección de la información que impidan el acceso libre por parte de personas externas. Deben existir controles que detecten e impidan situaciones de acceso no autorizados a los lugares de trabajo, y proteger tanto el equipo tecnológico como los documentos que utilizan los colaboradores. Los documentos en papel o medios magnéticos que contengan información confidencial o sensible se deberán guardar en lugar seguro.

6.8.9. **Políticas de seguridad de las operaciones de TIC**

a. Todos usuarios de servicios y terceros serán responsables por las credenciales (usuario y contraseña) que le sean asignadas y que reciben para el uso y acceso de los recursos.
b. Ningún usuario recibirá credenciales de acceso a la plataforma tecnológica, los servicios de red y los sistemas de información o aplicaciones, hasta que no acepte formalmente la Política de Seguridad de la Información vigente.
c. Todos los funcionarios, contratistas y otros terceros, deben autenticarse en los mecanismos de control de acceso provistos por la Oficina de Sistemas de Información antes de poder usar cualquier elemento de la infraestructura tecnológica.

6.8.10. **Política de adquisición, desarrollo y mantenimiento de sistemas de información**

La Oficina de Sistemas de Información debe:

a. Implementar los controles necesarios para asegurar que el acceso al código fuente de los aplicativos desarrollados sea limitado. Solamente el personal del grupo de desarrollo podrá contar con acceso a esta información y hará un uso moderado de la misma, además, debe proporcionar las herramientas necesarias para realizar control de cambios sobre el código fuente de los aplicativos desarrollados por la misma, las cuales permitirán retroceder a una versión anterior del código.
b. Aprobar, supervisar y modificar los códigos fuente de los aplicativos.
c. Implementar los estándares de diseño y desarrollo de software de la entidad que están disponibles bajo las siguientes nomenclaturas en el sistema de gestión de calidad:

   - ✓ P-GIN-10 Procedimiento Estándares software Modelo de clases.
   - ✓ P-GIN-11 Procedimiento Estándares software nombramiento bases de datos.
   - ✓ P-GIN-12 Procedimiento Estándares software web application Java html5.
   - ✓ P-GIN-13 Procedimiento Atención a Requerimientos Desarrollo o Ajustes.

6.8.11. **Políticas de respaldo y restauración de información**

La Oficina de Sistemas de Información debe:

a. Proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y el software, se pueda recuperar después de una falla, garantizando que la información y la infraestructura de software crítica de la Entidad, sean respaldadas y puedan ser restauradas en caso de una falla y/o desastre.
b. Elaborar el **Plan de Respaldo y Pruebas de Restauración** el cual debe contener el alcance que define a que información se le saca copia de seguridad, cómo se almacena la información, la periodicidad de respaldo y la programación de las pruebas de restauración, y establecer las actividades que verifiquen el éxito en el proceso de respaldo y restauración.
c. Restaurar las copias de respaldo en ambientes de producción y deben estar debidamente aprobada por el propietario de la información y solicitadas a través de la herramienta de mesa de servicios Help Desk.
d. Generar tareas de restauración aleatorias de la información y documentarlas inmediatamente es responsabilidad del administrador de la plataforma de backup.
e. Definir las directrices de respaldo y restauración de información, en el procedimiento P-GIN-08 Copias de seguridad de la información electrónica.

6.8.12. **Políticas de registro y seguimiento de eventos de sistemas de información y comunicaciones**

La Oficina de Sistemas de Información debe:

a. Disponer de una herramienta de mesa de servicios Help Desk, la cual debe ser utilizada desde la intranet por todos los funcionarios y contratistas que requieren la solución a

eventos e incidencias presentadas en el uso de las herramientas o elementos suministrados para el ejercicio de sus actividades.

b. Atender las incidencias que solo están reportados en la herramienta de mesa de servicios Help Desk, es responsabilidad de los funcionarios o contratistas que dan soporte y estos deben realizar de manera oportuna el registro de la solución suministrada de acuerdo a los plazos establecidos en los respectivos acuerdos de niveles de servicio.

6.8.13. **Políticas de control de software operacional**

La Oficina de Sistemas de Información debe:

a. Asegurar que el software operativo instalado en la plataforma tecnológica de la Entidad cuenta con soporte de los proveedores y el software esté debidamente licenciado.
b. Conceder accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones.
c. Validar los riesgos que genera la migración hacia nuevas versiones del software operativo.
d. Asegurar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software operativo es actualizado.
e. Establecer las restricciones y limitaciones para la instalación de software operativo en los equipos de cómputo de la Entidad.

6.8.14. **Políticas de gestión de vulnerabilidades**

La Oficina de Sistemas de Información debe:

a. Revisar, valorar y gestionar periódicamente la aparición de vulnerabilidades sobre los recursos de la plataforma tecnológica, con el objetivo de realizar la corrección sobre los hallazgos arrojados por dichas pruebas.
b. Adelantar los trámites correspondientes para la realización de pruebas de vulnerabilidades y hacking ético con una periodicidad establecida, por un ente independiente al área objeto de las pruebas, con el fin de garantizar la objetividad del desarrollo de estas.
c. Revisar periódicamente la aparición de nuevas vulnerabilidades y reportarlas a los administradores de la plataforma tecnológica y los desarrolladores de los sistemas de información, prevengan la exposición al riesgo.
d. Generar, ejecutar o monitorear planes de acción para la mitigación de las vulnerabilidades detectadas en la plataforma tecnológica.
e. Revisar, valorar y gestionar las vulnerabilidades encontradas, apoyándose en herramientas tecnológicas para su identificación.

6.8.15. **Políticas de seguridad de las comunicaciones**

La Oficina de Sistemas de Información debe:

a. Adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red de la Entidad.

b. Implantar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.
c. Mantener las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier otra tipificación que se considere conveniente para la Entidad.
d. Identificar los mecanismos de seguridad y los niveles de servicio de red requeridos e incluirlos en los acuerdos de servicios de red, cuando estos se contraten externamente.
e. Establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red de la plataforma tecnológica de la Entidad, acogiendo buenas prácticas de configuración segura.
f. Identificar, justificar y documentar los servicios, protocolos y puertos permitidos por la Entidad en sus redes de datos e inhabilitar o eliminar el resto de los servicios, protocolos y puertos.
g. Instalar protección entre las redes internas y cualquier red externa, que este fuera de la capacidad de control y administración de la Entidad.
h. Velar por la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos de la Entidad.

6.8.16. **Políticas para la transferencia de información**

La Oficina de Sistemas de Información debe:

a. Proteger la información transferida al interior y exterior del AMVA.
b. Realizar el control del uso de sistemas de transferencia de archivos vía FTP y accesos de escritorio remoto a terceros.
c. Comunicar los sistemas de información pertenecientes a la Entidad con sistemas de información externos utilizando servicios web Rest-Full que implementen mecanismos de seguridad para la transferencia de información y por medio de la utilización de protocolos seguros.

6.8.17. **Política de uso de correo electrónico**

El correo electrónico institucional sólo debe ser utilizado con fines laborales, no se permite el envío de correos que incorporen como archivo anexos archivo de tipo: .EXE .BAT.JAR.

Los usuarios y claves del contratista administrador de la plataforma tecnológica y los desarrolladores de la Oficina de Sistema de Información son de uso personal e intransferible.

El Líder de Gestión Humana debe informar a la Oficina de Sistemas de Información, los funcionarios vinculados para la creación de su cuenta de correo electrónico; así también oportunamente los retiros para la suspensión de este servicio.

El Área Metropolitana del Valle de Aburrá como organización debe poseer una regla de renuncia (disclaimer) que debe utilizarse siempre en los mensajes con el fin de evitar reclamaciones legales. El disclaimer para su aprobación debe decir: *La información contenida en este mensaje y en sus anexos es estrictamente confidencial. Si usted recibió por error esta comunicación, por favor notificar inmediatamente esta circunstancia mediante reenvío a la dirección electrónica del remitente y bórrela puesto que su uso no autorizado*

acarreará las sanciones y medidas legales a que haya lugar. La Entidad no se hace responsable por la presencia en este mensaje o en sus anexos, de algún virus o malware que pueda generar o genere daños en sus equipos, programas o afecte su información.

La capacidad máxima para almacenamiento de correo electrónico está definida por el Líder de la Oficina de Sistemas de Información y depende del tipo de usuario. No obstante, en caso de necesidades especiales, el interesado podrá solicitar la ampliación de la capacidad. Por razones organizacionales o técnicas, las capacidades máximas de los buzones podrán ser modificadas unilateralmente por parte del Líder de la Oficina de Sistemas de Información.

Es responsabilidad del funcionario y/o contratista solicitar al Líder de la Oficina de Sistemas de Información con copia a la mesa de ayuda la asesoría de cómo realizar el Backup de su correo electrónico.

Las bandejas de correo electrónico están activas durante el tiempo que dure la vinculación del funcionario o contratista con la Entidad, excepto en casos de fuerza mayor o mala utilización que eventualmente puedan causar la suspensión o cancelación de la misma. Una vez se produzca la desvinculación de la persona, la cuenta será dada de baja en el servidor mediante una solicitud enviada a la mesa de ayuda.

El sistema de monitoreo filtra los archivos anexos a los mensajes de correo electrónico, para verificar la ausencia de virus. La entrega de todo mensaje a su destinatario final está sujeta a que esta comprobación sea exitosa.

La comunicación por correo electrónico entre los usuarios internos y usuarios externos (públicos de interés) debe hacerse a través del correo homologado y proporcionado por la Entidad. No es permitido utilizar cuentas personales para comunicarse con los públicos de interés, ni para transmitir cualquier otro tipo de información del AMVA.

El buzón de correo electrónico del funcionario debe ser corresponsable y velar por la seguridad protegiendo su clave de acceso. El usuario es el único responsable por el buen uso de su cuenta de correo electrónico. En consecuencia el usuario se compromete a:

1. Respetar la privacidad de las cuentas de otros usuarios del servicio, tanto dentro como fuera de la red corporativa. El usuario no podrá utilizar identidades ficticias o pertenecientes a otros usuarios para el envío de mensajes. El titular de correo o cuenta asignada usará el correo electrónico para enviar y recibir mensajes necesarios para el desarrollo de las labores propias de su cargo o de las investigaciones que tenga asignadas. La Oficina Asesora de Comunicaciones es la única dependencia autorizada para el envío de correos masivos.

2. Usar el correo electrónico propiedad del AMVA con extensión *@metropol.gov.co* solamente para fines propios a la organización siempre con respeto y cortesía; no podrá crear, distribuir o reenviar mensajes que ofenda la dignidad, intimidad y buen nombre de las personas, de las instituciones, o para realizar algún tipo de acoso, difamación, calumnia, con intención de intimidar, insultar o cualquier otra forma de actividad hostil; de igual forma se prohíbe difundir ideas políticas, religiosas, propagandas entre otros.

3. Evitar enviar o recibir los mensajes de sus usuarios con contenido impropio, difamatorio, ilícito, obsceno, indecente o que contenga difusión de noticias sin identificar plenamente su autor; adicionalmente, los colaboradores no podrán enviar anónimos, propagandas o literatura de cualquier índole, encuestas, concursos, esquemas piramidales, cartas en cadena, mensajes no deseados, o cualesquiera que contenga mensajes duplicativos o no solicitados, u otra información ajena a las labores que desempeñan en su cargo.

4. Evitar el uso de la cuenta para el envío o reenvío de mensajes spam (no solicitados, no deseados o de remitente desconocido, habitualmente de tipo publicitario, enviados en grandes cantidades), o intento de hacer creer que algo falso es real, con contenido que pueda resultar ofensivo o dañino para otros usuarios (como virus o pornografía), o que sea contrario a las políticas y normas institucionales.

5. Depurar mensualmente por parte del funcionario responsable el contenido del buzón de entrada en el servidor para evitar que los mensajes permanezcan en él un tiempo excesivo que conduzca a la congestión o al bloqueo de este.

6. Evitar el envío de respuestas con copia a todos los destinatarios de un mensaje recibido, y en particular cuando se trata de mensajes que originalmente hayan sido dirigidos a un grupo grande de usuarios; salvo cuando se trate de una respuesta que por su naturaleza o contenido necesariamente requiera ser conocida por todos ellos.

7. Evitar abrir mensajes no esperados que contengan archivos adjuntos, aunque provengan de personas conocidas. En particular, no abrir mensajes cuyo asunto contenga palabras en inglés a menos que lo esté esperando, podría tratarse de un virus.

8. Evitar usar letras mayúsculas, especialmente en el campo de “Asunto:”, al igual que el uso excesivo de signos de exclamación (&, %, $, #, ?, ¡, !, ¿), esto puede hacer que los sistemas de correo electrónico lo identifiquen como correo no deseado o spam, y el mensaje posiblemente no llegue al destinatario, o llegue con identificación de correo no solicitado.

9. Utilizar el servicio de correo sin dejar mensajes almacenados por mucho tiempo en el servidor de correo. Tenga presente descargarlos con una frecuencia diaria, debido a que el tamaño de su buzón de correo es limitado; una vez superado este tope el sistema no le procesará más correos.

10. No utilizar la plataforma institucional para el envío de correos de tipo spam (masivos). Se entiende por correo masivo aquel que es remitido a más de 25 destinatarios.

6.8.18. **Política específica para funcionarios y contratistas de la Oficina de Sistemas de Información**

Los funcionarios adscritos a la Oficina de Sistemas de Información deben mantener completa y estricta confidencialidad de la información a la que tienen acceso debido a los permisos y roles que sobre las bases de datos y fuentes de información poseen para soportar la

infraestructura tecnológica y brindar soporte a las incidencias presentadas, además, deben garantizar en cada actividad la preservación e integridad en la información accedida.

El no cumplimiento de los procedimientos establecidos en esta política del SGSI constituye una falta grave que será sancionada de acuerdo a lo establecido en el P-GJU-08 Procedimiento Disciplinario Interno.

6.8.19. **Políticas de tercerización u outsourcing**

La Oficina de Sistemas de Información debe:

a. Mantener la seguridad de la información y los servicios de procesamiento de información, a los cuales tienen acceso terceras partes, entidades externas o que son procesados, comunicados o dirigidos por estas.
b. Garantizar el cumplimiento de la normatividad vigente en los procedimientos de contratación.
c. Establecer criterios de selección que contemplen la experiencia y reputación de terceras partes, certificaciones y recomendaciones de otros clientes, estabilidad financiera de la compañía, seguimiento de estándares de gestión de calidad y de seguridad y otros criterios que resulten de un análisis de riesgos de la selección, Resolución Metropolitana No. 144 de 2014 Manual de Interventoría y Resolución Metropolitana 1129 de 2016 Manual Contratación.
d. Establecer mecanismos de control en las relaciones contractuales, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por los proveedores o contratistas, cumplan con las políticas de seguridad de la información establecidas por el SGSI del AMVA.
e. Incluir en los contratos o acuerdos con los proveedores y/o contratistas una causal de terminación del acuerdo o contrato de servicios, por el no cumplimiento de las políticas de seguridad de la información o el no cumplimiento de los procesos establecidos en el SGSI. Los contratistas, oferentes y/o proveedores deben aceptar y firmar el acuerdo de confidencialidad establecido por el AMVA.
f. Mitigar los riesgos de seguridad con referencia al acceso de los proveedores y/o contratistas a los sistemas de información SIM, G+, SICOF y demás herramientas a los que estos tengan permisos para ingresar.
g. Identificar los riesgos para la información y los servicios de procesamiento de información que involucren partes externas al AMVA. El resultado del análisis de riesgos será la base para el establecimiento de los controles y debe ser presentado al Comité para la Gestión de la Información antes de iniciar el estudio de mercado y publicación del proyecto de pliegos del contrato de outsourcing en el portal de contratación.

6.8.20. **Política de gestión de los incidentes de la seguridad de la información**

La Oficina de Sistemas de Información debe:

- ✓ Asegurar que los eventos e incidentes de seguridad que se presenten con los activos de información sean comunicados y atendidos oportunamente, empleando los procedimientos definidos, con el fin de tomar oportunamente las acciones correctivas.

- ✓ Aplicar el P-GIN-02 Procedimiento de Gestión de Incidentes y Debilidades, las directrices de gestión de incidentes de seguridad de la información.

6.8.21. **Políticas de cumplimiento de requisitos legales y contractuales**

La Oficina de Sistemas de Información debe:

a. Velar por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información, entre ellas la referente a derechos de autor y propiedad intelectual, razón por la cual estará pendiente de que el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.
b. Identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a la Entidad y relacionados con seguridad de la información. Es responsabilidad de la Oficina de Sistemas de Información, con el apoyo de la Oficina Asesora Jurídica Administrativa.
c. Certificar que todo el software que se ejecuta en la institución esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso.
d. Instalar software en las estaciones de trabajo suministradas para el desarrollo de las actividades de los funcionarios acogiéndose al buen uso y licenciamiento del software que se está utilizando.
e. Cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software es responsabilidad de los funcionarios y demás terceros.

6.8.22. **Políticas de revisión de seguridad de la información**

Esta política tiene como objetivo garantizar el funcionamiento del sistema de gestión de seguridad de la información de acuerdo a las políticas y procedimientos implementados.

La Oficina de Sistemas de Información debe:

a. Adelantar auditorías periódicas internas del sistema de gestión de seguridad de la información, para la verificación y cumplimiento de objetivos, controles, políticas y procedimientos de seguridad de la Información.
b. Verificar y supervisar el cumplimiento de las políticas de seguridad de la información es la responsabilidad de los líderes de cada proceso.
c. Establecer el procedimiento para revisar periódicamente los sistemas de información con las herramientas automáticas y especialistas técnicos.

6.8.23. **Política de retención y archivo de datos**

Tiene como objetivo mantener la integridad y disponibilidad de la información almacenada de forma centralizada en la Oficina de Atención al Usuario y Gestión Documental y la información especializada en el Centro de Información Documental, garantizando el cumplimiento de la Ley 594 del 2000 y los Decretos reglamentarios del Archivo General de Nación, mediante la implantación de programas de gestión de documentos PGD,

implementación de tablas de retención TRD, valoración documental TVD y mecanismos de preservación documental digital a lo largo del tiempo.

6.8.24. **Políticas de uso de mensajería instantánea y redes sociales**

La Oficina Asesora de Comunicaciones debe:

a. Publicar u divulgar por cualquier medio de Internet, redes sociales como: twitter®, facebook®, youtube® likedink®, blogs, instagram, etc, una vez sea autorizada por el Director de la Entidad en caso contrario se considera fuera del alcance del SGSI y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.
b. Distribuir en las redes sociales solo la información que sea originada por la Entidad con un vocabulario institucional.
c. Utilizar el nombre de la Entidad en las redes sociales para difamar o afectar la imagen y reputación de los seguidores cuando responden comentarios en contra de la filosofía de la institución, es una práctica indebida. Resolución Metropolitana 1308 Política Institucional de Comunicaciones.

6.8.25. **Política de tratamiento de datos personales**

La Resolución Metropolitana 156 del 30 enero del 2019 establece y adopta las políticas de protección de datos personales.

7. CUMPLIMIENTO

Todos aspectos contemplados en este Manual son de obligatorio cumplimiento para todos los funcionarios y contratistas.

En caso de que se violen las políticas de seguridad ya sea de forma intencional o por negligencia, la Entidad tomará las acciones disciplinarias y legales correspondientes, P-GJU-08 Procedimiento Disciplinario Interno.