PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES -PETI-, DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL ÁREA METROPOLITANA DE VALLEDUPAR

2024

CONTENIDO

1. DERECHOS DE AUTOR

Todas las referencias a los documentos del Modelo de Gestión de Riesgos de Seguridad Digital -**MGRSD**- son derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones -MINTIC-.
De igual forma, son derechos reservados por parte del MINTIC, todas las referencias a las políticas, definiciones o contenido relacionados con los documentos del MGRSD publicadas en el compendio de las normas técnicas colombianas vigentes.

En consecuencia, el MINTIC goza de los derechos de autor[1] establecidos en la ley 23 de 1982 y demás normas concordantes y complementarias, respecto de los documentos del MGRSD y su contenido.
Las reproducciones, referencias o enunciaciones de estos documentos deberán ir siempre acompañadas por el nombre o seudónimo del titular de los derechos de autor (Ministerio de Tecnologías de la Información y las Comunicaciones).
Lo anterior, sin perjuicio de los derechos reservados por parte de entidades tales como la *International Standard Organization* (ISO), ICONTEC, entre otras, respecto de referencias, definiciones, documentos o contenido relacionado en el MGRSD y sus documentos o anexos que son de su autoría o propiedad.

2. INTRODUCCIÓN

La política de gobierno digital en el Área Metropolitana de Valledupar, es una herramienta que permite no solo a la entidad sino también a los diferentes actores de la sociedad un desarrollo integral en donde las necesidades y problemáticas del contexto determinan el uso de la tecnología y la forma como ésta puede aportar en la generación de valor público.

Luego de varios años de implementación de la Estrategia de Gobierno en Línea en Colombia, las entidades públicas han tenido avances significativos en materia de eficiencia administrativa, participación y servicios al ciudadano por medios electrónicos, no obstante, la evolución constante de la sociedad y de la economía en donde la tecnología juega un papel fundamental, hace necesario dar el siguiente paso hacia la transformación digital del Estado, a fin de contar con entidades públicas orientadas a garantizar mejores condiciones de vida para los ciudadanos, así como satisfacer necesidades y problemáticas a través del aprovechamiento de la tecnología.

La política de Gobierno Digital establecida mediante el Decreto 1008 de 2018, forma parte del Modelo Integrado de planeación y Gestión (MIPG) y se integra con las políticas de Gestión y Desempeño Institucional en la dimensión operativa de Gestión para el Resultado con Valores, que busca promover una adecuada gestión interna de las entidades y un buen relacionamiento con el ciudadano a través de la participación y la prestación de servicios de calidad.

Es importante anotar que se toma información correspondiente del Manual De Gobierno Digital, para establecer elementos que permitan orientar y facilitar nuestro proceso de Gobierno Digital Institucional.

A partir de las necesidades actuales se formula la presente política como parte de la fase de planeación del modelo de gestión de seguridad de la información, siendo una herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios vigentes.

La presente Política define algunos lineamientos relacionados con Seguridad Digital que debe cumplir la Administración de la Entidad, orientado a preservar los pilares fundamentales de la seguridad de la información:

CONFIDENCIALIDAD: La información debe ser accesible sólo a aquellas personas autorizadas.

INTEGRIDAD: La información y sus métodos de procesamiento deben ser completos y exactos.

DISPONIBILIDAD: La información y los servicios deben estar disponible cuando se le requiera. Para ello es necesario considerar aspectos tales como:

- ✓ **Autenticidad:** Los activos de información los crean, editan y custodian usuarios reconocidos quienes validan su contenido.
- ✓ **Posibilidad de Auditoria:** Se mantienen evidencias de todas las actividades y acciones que afectan a los activos de información.

- ✓ **Protección a la Duplicación:** Los activos de Información son objeto de clasificación, y se llevan los registros de las copias generadas de aquellos catalogados como confidenciales.
- ✓ **No repudio:** Los autores, propietarios y custodios de los activos de información se pueden identificar plenamente.
- ✓ **Legalidad:** Los activos de información cumplen los parámetros legales, normativos y estatutarios de la entidad territorial.

3. DEFINICIONES Y ACRÓNIMOS

- **MSPI:** Modelo de Seguridad y Privacidad de la Información
- **Información:** Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.
- **Dato:** Es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.
- **Copias de respaldo:** Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.
- **Servidor:** Es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.
- **Activo de Información:** Es todo aquello que en la entidad es considerado importante o de alta validez para la misma ya que puede contener información importante como son en las Bases de Datos con usuarios, contraseñas, números de cuentas, etc.
- **Riesgo:** Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.
- **Vulnerabilidad:** Es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.
- **Amenaza:** Es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo.
- **Activo**: Cualquier cosa que tenga valor para la organización. Existen diversos tipos de activos en una organización como: información, software, programas de computador, físicos como los computadores, servicios, la gente y sus aptitudes, habilidades, y experiencia, intangibles como Reputación o Imagen.
- **Activo de Información**: en relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- **Arquitectura de T.I.:** De acuerdo con el Marco de referencia de Arquitectura empresarial del Estado, define la estructura y las relaciones de todos los elementos de TI de una organización. Se descompone en arquitectura de información, arquitectura de sistemas de información y arquitectura de servicios tecnológicos. Incluye además las arquitecturas de referencia y los elementos estructurales de la estrategia de TI (visión de arquitectura, principios de arquitectura, lineamientos y objetivos estratégicos). Arquitectura de T.I. sectorial: Es el análisis integral y estratégico de un sector de la administración pública (salud, educación, tic, entre otros) basado en los dominios del Marco de Referencia de Arquitectura Empresaria, con el propósito de obtener, evaluar y diagnosticar su estado actual y planificar la transformación necesaria que le permita a un sector evolucionar hasta la arquitectura empresarial objetivo.
- **Cadena de Trámites:** A partir de las necesidades identificadas por los ciudadanos se genera una contacto ciudadano-Estado que se resuelve mediante la ejecución de trámites. La relación que se establece entre estos trámites en función de los requisitos exigidos para su realización, los cuales se cumplen a través de otros trámites o servicios prestados por otras entidades, genera las cadenas de trámites. Esta relación puede darse intra e intersectorial, ya sea entre entidades del Estado o con particulares que desempeñan funciones administrativas.

- **Capacidad Institucional:** Es una habilidad que debe tener una institución para poder cumplir con la misión y los objetivos que se propone. Se entiende que se tiene la capacidad cuando se posee procesos, infraestructura y talento humano con las competencias requeridas para prestar los servicios que debe proveer.
- **Ciudad o Territorio Inteligente:** Aquella que tiene una visión holística de sí misma, y en la cual sus procesos estratégicos y la provisión de servicios urbanos se basan en la promoción del desarrollo sostenible y la innovación, y en el uso y aprovechamiento de las TIC, con el propósito de aumentar la calidad de vida de los
- **Confidencialidad:** se refiere a que la información solo puede ser conocida por individuos autorizados.
- **Datos Abiertos:** son aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.
- **Digitalización:** Es el proceso mediante el cual se realiza la transformación de algo real (físico, tangible o análogo) a datos digitales (bits: unos y ceros), con el propósito de que dichos datos digitales puedan ser accedidos, manipulados y aprovechados para diferentes fines a través de equipos de cómputo (computadores, dispositivos móviles, entre otros). La digitalización es un paso o etapa dentro de un proceso de transformación digital, dado que este último implica elementos adicionales a la digitalización.
- **Estado Abierto:** es una modalidad de gestión pública más transparente, sujeta a rendición de cuentas, participativa y colaborativa, entre Estado y sociedad civil, donde el Estado hace posible una comunicación fluida y una interacción de doble vía entre gobierno y ciudadanía; dispone canales de diálogo e interacción, así como información para los ciudadanos con el fin de aprovechar su potencial contribución al proceso de gestión y la ciudadanía aprovecha la apertura de esos nuevos canales participativos, podrá colaborar activamente con la gestión de gobierno, promoviendo de este modo una verdadera democracia. El Estado no solo hace referencia a la
- **Gestión de T.I.:** Es una práctica, que permite operar, innovar, administrar, desarrollar y usar apropiadamente las tecnologías de la información (TI). A través de la gestión de TI, se opera e implementa todo lo definido por el gobierno de TI. La gestión de TI permite a una organización optimizar los recursos, mejorar los procesos de negocio y de comunicación y aplicar las mejores prácticas.
- **Gobierno Digital:** De forma general, consiste en el uso de las tecnologías digitales como parte integral de las estrategias de modernización de los gobiernos para crear valor público. Esto depende de un ecosistema de actores gubernamentales, ONGs, empresas, asociaciones ciudadanas e individuos que dan soporte a la producción de y acceso a datos, servicios y contenido a través de interacciones con el gobierno. En Colombia, Gobierno Digital es la política pública liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones - Min TIC, que tiene como objetivo “Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital”.
- **Gobierno de Arquitectura Empresarial:** Es una práctica orientada a establecer instancias de decisión, alinear los procesos institucionales o de negocio con los procesos, recursos y estrategias de TI, para agregar valor a las organizaciones

y apoyar el cumplimiento de sus objetivos estratégicos. El gobierno de Arquitectura empresarial gestiona y controla los riesgos, mide el desempeño de la arquitectura, define políticas de arquitectura, gestiona la evolución y cambios sobre los artefactos o productos de la arquitectura. El gobierno de la arquitectura, es parte del gobierno corporativo o empresarial.

- **Innovación Abierta:** Es un método específico para adelantar procesos de innovación, en el cual se distribuyen las tareas entre actores internos y externos de una organización, para la comprensión de problemáticas, generación de ideas o desarrollo de soluciones.
- **Integridad:** se refiere a la garantía de que una información no ha sido alterada, borrada, reordenada, copiada, etc., bien durante el proceso de transmisión o en su propio equipo de origen.
- **Responsive (término en inglés):** Técnica de diseño web adaptativo, que busca la correcta visualización de una misma página en distintos dispositivos computadores de escritorio, tabletas y dispositivos móviles.
- **Sede Electrónica**: Es una dirección electrónica que permite identificar la entidad y la información o servicios que provee en la web, a través de la cual se puede acceder de forma segura y realizar con todas las garantías legales, los procedimientos, servicios y trámites electrónicos que requieran autenticación de sus usuarios.
- **Servicios Ciudadanos Digitales:** Es el conjunto de servicios que brindan capacidades y eficiencias para optimizar y facilitar el adecuado acceso de los usuarios a la administración pública a través de medios electrónicos. Estos servicios se clasifican en básicos y especiales.
- **Sistema de Gestión Documental Electrónico de Archivo (SGDEA):** Es una herramienta informática destinada a la gestión de documentos electrónicos de archivo. También se puede utilizar en la gestión de documentos de archivo tradicionales.
- **Tecnologías Digitales:** Son herramientas, sistemas, dispositivos y recursos electrónicos que generan, almacenan o procesan datos en forma de bits (0 y 1). Estos incluyen redes sociales, juegos y aplicaciones en línea, multimedia, aplicaciones de productividad, computación en la nube, sistemas interoperables, dispositivos móviles, entre otros.
- **Trámite:** Conjunto o serie de pasos o acciones reguladas por el Estado, que deben efectuar los usuarios para adquirir un derecho o cumplir con una obligación prevista o autorizada por la ley. El trámite se inicia cuando ese particular activa el aparato público a través de una petición o solicitud expresa y termina (como trámite) cuando la administración pública se pronuncia sobre este, aceptando o denegando la solicitud.
- **Transformación Digital:** Es un proceso de reinvención o modificación en la estrategia o modelo del negocio, que responde a necesidades de supervivencia de las organizaciones y se apoya en el uso de Tecnologías de la Información y las comunicaciones.
- **Usabilidad:** es un anglicismo que apareció hace algunos años, que significa grado en que un producto puede ser usado por determinados usuarios para lograr sus propósitos con eficacia, eficiencia y satisfacción en un contexto de uso específico".
- **Valor Público:** se relaciona con la garantía de derechos, la satisfacción de necesidades y la prestación de servicios de calidad. Por ello, somos conscientes que no sólo es hacer uso de las tecnologías, sino cómo las tecnologías ayudan a resolver problemas reales. Este sería el fin último del uso de los medios digitales en la relación del Estado y el ciudadano.
- **Interoperabilidad**: Es la capacidad que tiene un producto o un sistema, cuyas

interfaces son totalmente conocidas, para funcionar con otros productos o sistemas existentes o futuros y eso sin restricción de acceso o de implementación.

CIO: Chief Information Officer (Directorio de Información)

DAFP: Departamento Administrativo de la Función Pública

DUR-TIC: Decreto Único Reglamentario del sector TIC

FURAG: Formulario Único de Reporte de Avances de la Gestión

MIPG: Modelo Integrado de Planeación y Gestión

Min TIC: Ministerio de Tecnologías de la Información y las Comunicaciones

MSPI: Modelo de Seguridad y Privacidad de la Información

PETI: Plan Estratégico de Tecnologías de la Información TIC: Tecnologías de la Información y la Comunicación

TI: Tecnologías de la Información

4. OBJETIVO

Establecer los lineamientos y protocolos de Seguridad y Privacidad de la Información para la ÁREA METROPOLITANA DE VALLEDUPAR, en el marco de los objetivos de la Seguridad de la información.

4.1. OBJETIVOS ESPECIFICOS DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

- ✓ Minimizar el riesgo en las funciones más importantes de la entidad.
- ✓ Cumplir con los principios de seguridad de la información.
- ✓ Cumplir con los principios de la función administrativa.
- ✓ Mantener la confianza de sus clientes, socios y empleados.
- ✓ Apoyar la innovación tecnológica.
- ✓ Implementar el sistema de gestión de seguridad de la información.
- ✓ Proteger los activos tecnológicos.
- ✓ Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- ✓ Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del Área Metropolitana de Valledupar.
- ✓ Garantizar la continuidad del Entidad frente a incidentes.

5. ALCANCE

Aplica a los funcionarios, contratistas y terceros que usan los recursos informáticos que se encuentran al servicio del ÁREA METROPOLITANA DE VALLEDUPAR, sean o no de propiedad del AMV, sea que estén compartidos o controlados individualmente, sea que estén aislados o interconectados a redes. Los recursos incluyen los datos y la información electrónica, el software y los equipos de cómputo y comunicaciones.

5.1. NIVEL DE CUMPLIMIENTO

Todas las personas que tengan que ver directa o indirectamente por el alcance de la política, deberán dar cumplimiento a un 100% de la misma.

6. MARCO LEGAL

NORMA	MATERIA
Decreto 1008 del 14 de junio de 2018	Política de Gobierno Digital.
Decreto 1078 de 2015 Articulo 2.2.17.7.1	Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1499 de 2017 Artículo 2.2.22.2.1.	Políticas de gestión y desempeño institucional.

7. POLITICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

En el ÁREA METROPOLITANA DE VALLEDUPAR la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes.

7.1. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION

El ÁREA METROPOLITANA DE VALLEDUPAR protegerá la información creada, procesada, transmitida, resguardada por sus procesos, 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. Para lo cual Conformara el comité un comité de seguridad de la información, el cual liderara la Gestión de la seguridad de la Información en el ÁREA METROPOLITANA DE VALLEDUPAR. Cuyo Objetivos serán:

- *Desarrollar, mantener y administrar operativa y técnicamente la seguridad de la información conforme con las políticas de seguridad adoptadas por el ÁREA METROPOLITANA DE VALLEDUPAR.*
- *Materializar las medidas de largo, mediano y corto plazo que permitan el desarrollo efectivo, estratégico y armónico de las políticas planteadas.*

Servidores Públicos, Contratistas y Particulares con acceso a Información son responsables de:

- *Cumplir con todas las políticas de seguridad adoptadas*
- *Actualizarse en los temas propios de seguridad de activos de la información aplicados en la administración pública.*

7.2. POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

- ✓ El ÁREA METROPOLITANA DE VALLEDUPAR protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- ✓ El ÁREA METROPOLITANA DE VALLEDUPAR implementará control de acceso a la información, sistemas y recursos de red en los casos que aplique.
- ✓ El ÁREA METROPOLITANA DE VALLEDUPAR verificará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- ✓ El ÁREA METROPOLITANA DE VALLEDUPAR realizará mejora continua al modelo de seguridad. Esta política será revisada con regularidad como parte del proceso de revisión estratégica, o cuando se identifiquen cambios en la Entidad, su estructura, sus objetivos o alguna condición que afecte la política, para asegurar que siga siendo adecuada y ajustada a los requerimientos identificados.
- ✓ Toda información que provenga de un archivo externo de la Entidad o que deba ser descargado tiene que ser analizado con el antivirus institucional vigente.
- ✓ Todo usuario de los recursos TIC, NO debe visitar sitios restringidos de manera explícita o implícita, o sitios que afecten la productividad de la Institución; como el acceso desde la Entidad a sitios relacionados con la pornografía, juegos, redes sociales no autorizadas, etc.

- ✓ Ningún usuario, debe descargar y/o utilizar información, archivos, imágenes, sonidos u otros que estén protegidos por derechos de autor de terceros sin la previa autorización de los mismos. En caso de que se requiera su uso, se debe dar su debido reconocimiento.
- ✓ Minimizar el uso de dispositivos extraíbles para compartir archivos aprovechando los recursos compartidos del servidor de la entidad o haciendo uso del servicio de internet.
- ✓ Todo usuario de los recursos TIC debe advertir e informar a la oficina de TIC qué información requiere medidas específicas de protección para evitar el acceso a personal no autorizado, y/o establecer el sistema de respaldo para la misma.

7.3. POLITICAS

7.3.1 GESTION DE ACTIVOS

7.3.1.1. Política de Gestion de Activos de Información

El ÁREA METROPOLITANA DE VALLEDUPAR es responsable de identificar los activos de información y definir las responsabilidades de protección apropiadas. Cada Dependencia y Oficinas asesoras son responsables de colaborar en las actividades relacionadas con la gestión de Activos de Información.

7.3.1.2. Política de Identificación de Activos de Información

Se identificarán los activos de información y se construirá el inventario de activos de Información, de acuerdo con los procedimientos y lineamientos definidos en el **Programa de Gestión Documental**, el cual estable los responsables y el instrumento.

Controles

- ✓ Se mantendrá actualizado los activos de información pública, que genere, obtenga, adquiera, transforme o controle, de acuerdo con los procedimientos y lineamientos definidos en el **Programa de Gestión Documental**
- ✓ Los activos de información pertenecen al ÁREA METROPOLITANA DE VALLEDUPAR y el uso de los mismos debe emplearse exclusivamente con propósitos laborales.
- ✓ Los datos/información creados, almacenados y recibidos, durante el ejercicio laboral serán propiedad del ÁREA METROPOLITANA DE VALLEDUPAR.
- ✓ Los funcionarios, y empleados públicos deberán documentar y entregar los conocimientos importantes que posee de la labor que ejecutan (activo de información), como requisito previo para su liquidación.
- ✓ Los funcionarios solo podrán realizar **BackUp** de sus archivos personales o de información pública.

7.3.1.3. Política De Organización de la Información

El ÁREA METROPOLITANA DE VALLEDUPAR realizara la organización de la

Información de acuerdo a los lineamientos definidos en el **Programa de Gestión documental**, y la normatividad vigente relacionada.

Controles

- ✓ Todos los servidores públicos del ÁREA METROPOLITANA DE VALLEDUPAR deben organizar la Información relevante que producen en la carpeta de la respectiva secretaría u oficina dispuesta en el servidor de almacenamiento de red para cumplir con el principio de Disponibilidad.
- ✓ Es responsabilidad de los líderes de proceso que la información esté debidamente organizada tanto física como digitalmente.
- ✓ Todos los usuarios que tengan acceso a la información la deben manejar de acuerdo a lo que establece la **Ley Estatutaria 1581 de 2012** y Reglamentada Parcialmente por el **Decreto Nacional 1377 De 2013**.

7.3.1.4. Politica de Clasificación de la Información

Todas las dependencias y oficinas asesoras del ÁREA METROPOLITANA DE VALLEDUPAR deben clasificar la información, determinar su sensibilidad y criticidad, de acuerdo a los lineamientos del **Programa de Gestión documental, y la normatividad vigente relacionada**. Para asegurar que la información reciba niveles de protección adecuados.

Controles

- ✓ Los jefes de dependencia, o área responsable de la generación, posesión, control o custodia de la información son los responsables de la calificación de la información pública, para su clasificación.
- ✓ La oficina de las TIC es encargada de administrar y hacer efectivos los controles de seguridad tales como: copias de seguridad, asignación de privilegios de acceso, modificación y borrado.
- ✓ La información clasificada, reservada, confidencial o de uso restringido, debe guardarse y transmitirse de acuerdo a los lineamientos del Programa de Gestión de Documentos.
- ✓ Es responsabilidad del usuario es evitar en todo momento la fuga de la información de la institución que se encuentre almacenada en los equipos de cómputo personal que tenga asignados o en la información de la red.
- ✓ Es responsabilidad de los líderes de procesos que los funcionarios guarden su información en la partición de almacenamiento en el servidor de datos o en la ubicación que el área de TIC configure o especifique para dicho fin.
- ✓ Se pedirá autorización a su jefe inmediato, o Secretario General para la copia de información clasificada o reservada y de acuerdo a los niveles de seguridad establecidos; Su copia, sustracción, daño intencional o utilización para fines distintos a las labores propias de la Institución, serán sancionadas de acuerdo con las normas y legislación vigentes.

7.3.1.5. Política de Devolución de Activos

Los funcionarios, contratistas y/o terceros deben realizar la entrega de los activos físicos y de información una vez finalice el empleo, acuerdo u contrato. Siguiendo los lineamientos del procedimiento **Gestion de Almacen.**

Controles

- ✓ Los funcionarios, y empleados públicos deberán realizar la devolución de todos los activos de información asignados por el ÁREA METROPOLITANA DE VALLEDUPAR en el proceso de desvinculación.
- ✓ Los usuarios o funcionarios deberán dar buen uso a los activos de información que tengan asignados.
- ✓ Los funcionarios, y empleados públicos seguirán los lineamientos de Disposición final de activos.
- ✓ Los líderes de los procesos son responsables de Mantener la protección adecuada de los activos de información mediante la asignación a los usuarios finales que deban administrarlos de acuerdo a sus roles y funciones.

7.3.1.6. Política de Gestión de Medios Removibles

Son medios removibles todos aquellos dispositivos electrónicos que almacenan información y pueden ser extraídos de los computadores.

Controles

- ✓ La información clasificada y reservada se deberá almacenar en el servidor, y no se autorizan copias en las computadoras personales ni en medios removibles.
- ✓ Está restringida la copia de archivos en medios removibles de almacenamiento, por lo cual se deshabilita la opción de escritura en dispositivos USB, unidades ópticas de grabación en todos los equipos de cómputo institucionales.
- ✓ La autorización de uso de los medios removibles debe ser tramitada a través de los líderes de los procesos y con aprobación de la Secretaría General como líder del proceso gestión de la Información y dichas autorizaciones será objeto de auditorías de seguridad en pro de la prevención de pérdidas de datos de la entidad.
- ✓ El servicio de acceso a Internet, Intranet, Sistemas de información, medio de almacenamiento, aplicaciones (Software), cuentas de red, navegadores y equipos de cómputo son propiedad de la Entidad y deben ser usados únicamente para el cumplimiento de la misión de la Entidad.

7.3.1.7. Política de Gestión de Dispositivos Móviles

Son dispositivos de comunicación que permiten el acceso a servicios de información del ÁREA METROPOLITANA DE VALLEDUPAR, como teléfonos móviles, teléfonos inteligentes “Smart Phones”, tabletas.

La Entidad asignará dispositivos móviles de comunicación institucionales (Teléfonos móviles, Smart Phones) a funcionarios, contratistas, de acuerdo a la disponibilidad de equipos y servicios, así como la función a desempeñar, previa aprobación de la Secretaria General.

Controles

- ✓ Los dispositivos móviles (teléfonos móviles, teléfonos inteligentes - Smart Phones, tabletas, entre otros), son una herramienta de trabajo que se deben utilizar únicamente para facilitar las comunicaciones de los usuarios de la entidad.
- ✓ Es responsabilidad del usuario hacer buen uso del dispositivo suministrado por el ÁREA METROPOLITANA DE VALLEDUPAR con el fin de realizar actividades

propias de su cargo o funciones asignadas en la entidad.

- ✓ En el caso del nivel directivo autoriza el uso de WhatsApp en los dispositivos suministrados por la entidad, no se permite por esta aplicación, el envío de fotografías, audios y videos clasificados como información pública reservada o información pública clasificada (privada o semiprivada).
- ✓ Los dispositivos móviles deben tener contraseña de ingreso y bloqueo del equipo de manera automática y manual, tener activado la función de borrado remoto, cifrar la memoria de almacenamiento.
- ✓ Los dispositivos móviles institucionales deben tener únicamente la tarjeta sim asignada por la entidad, de igual forma la tarjeta sim únicamente debe instalarse en los equipos asignados por la entidad.
- ✓ Los usuarios de dispositivos móviles institucionales NO deben hacer uso de redes inalámbricas públicas.

7.3.1.8. Política de Seguridad de los Recursos Humanos

El ÁREA METROPOLITANA DE VALLEDUPAR, se asegura de que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.

Controles

- ✓ El responsable de Talento Humano aplica sus procedimientos definidos en la selección de personal.
- ✓ El responsable de Talento Humano debe informar al personal que se vincule o se contrate por primera vez por la Entidad, la existencia de la Política de Seguridad de la Información e incluir en los contratos de estos últimos, el compromiso de confidencialidad de la información y la responsabilidad en materia de seguridad.
- ✓ Talento Humano debe realizar inducción y re-inducción permanentemente a los usuarios o clientes internos en materia de seguridad de la información y difundir las posibles amenazas y riesgos que afectan los recursos TIC de la Entidad de acuerdo al cronograma de capacitación. Para esto contará con el apoyo del grupo TIC de la entidad.
- ✓ Es responsabilidad del empleado o funcionario publico apropiar competencias minimas en el manejo de Ofimatica y nociones basicas de computo para el buen desempeño y cumplimiento de sus actividades.
- ✓ Las **responsabilidades** frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios, contratistas, proveedores, grupos de valor o terceros.
- ✓ El empleado y/o funcionario público como usuario de TIC deben proteger, respaldar y evitar **accesos de la información a personas no autorizadas**; es decir son responsables de cuidar todos los activos digitales de información sean o no propiedad del ÁREA METROPOLITANA DE VALLEDUPAR.
- ✓ El usuario debe asegurarse que los cables de conexión no sean pisados o pinchados al colocar otros objetos encima o contra ellos. Considerando que a través de éstos se le provee algunos servicios, por lo tanto, debe contribuir con su cuidado.

7.3.1.9. Política de Activos de Servicios (correo electrónico Institucional, claves de Internet, chat, página institucional)

El correo electrónico, claves de internet, y chat son de carácter personal e intransferible, es deber de cada uno de los usuarios mantener el uso de estas y de sus contraseñas, siguiendo estas dos premisas y por ningún motivo se debe permitir a otra persona acceder a estos recursos. El manejo, configuración, y actualización de la página institucional es exclusivamente de la oficina de las TIC, o del personal que esta misma delegue para tal fin.

Controles

- ✓ Los usuarios no deben usar cuentas de correo electrónico, claves de internet y chat asignadas a otras personas, ni recibir mensajes en cuentas de otros.
- ✓ Si fuera necesario leer el correo y/o chat de alguien más (mientras esta persona se encuentre fuera o de vacaciones) el usuario ausente debe redireccionar el correo y/o chat a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa a la institución, a menos que cuente con la autorización del departamento de informática.
- ✓ Los usuarios deben tratar los mensajes de correo electrónico, chat y archivos adjuntos como información de propiedad del ÁREA METROPOLITANA DE VALLEDUPAR.
- ✓ Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.
- ✓ Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando vayan de manera encriptado y destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones.
- ✓ Es prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico. Es prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.
- ✓ Cuando un funcionario que tiene asignada una cuenta de correo de la entidad, deberá entregar al Área de TIC los usuarios y password asignados, de igual manera dicha información debe entregarse cuando exista un proceso de empalme.
- ✓ Los usuarios del servicio de navegación en Internet del ÁREA METROPOLITANA DE VALLEDUPAR, al aceptar el servicio están aceptando que:

    1. Serán sujetos de monitoreo de las actividades que realiza en Internet.
    2. Saben que existe la prohibición al acceso de páginas no autorizadas.
    3. Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.
    4. Saben que existe la prohibición de descarga de software sin la autorización de la oficina de las TIC, especialmente juegos y programas que puedan traer archivos maliciosos.

- ✓ La utilización de Internet es para el desempeño de funciones y actividades contractuales y no para propósitos personales.
- ✓ Es responsabilidad de cada dependencia de la entidad hacer llegar la información a publicar en la página Institucional con oportunidad, y velar para que esté actualizada cuando se requiera.

7.3.2. CONTROL DE ACCESO

El ÁREA METROPOLITANA DE VALLEDUPAR limita el acceso a información y a instalaciones de procesamiento de información.

Se debe Controlar el acceso fisico o lógico, a los sistemas de información, bases de datos y servicios de información, así como el uso de medios de computación móvil. Autorizar a los usuarios por medio de técnicas de autenticación y autorización.

7.3.2.1. Gestión de acceso de usuarios

Controles

- ✓ Cada funcionario contratista o tercero debe tener un usuario y contraseña para acceder a los servicios de TIC.
- ✓ El funcionarioempleado publico o contratista tiene acceso a los servicios de red para los que hayan sido autorizados especificamente.
- ✓ Los derechos e acceso de todos los empleados y funcionrios publicos a la informacion e instlaciones de procesamiento de informacion se retiran al terminar su empleo o contrato.
- ✓ El acceso a la informacion y funciones de los sistemas de las aplicaciones esta autorizado en a los profesionales del area de TIC y es restrigido a los demas empleados y funcionarios publicos.
- ✓ Es responsabilidad del usuario el manejo apropiado a las claves asignadas de los servicios de red y de acceso a la red estas claves de acceso y usuarios son personales e intransferibles.
- ✓ Se controlará el acceso a la información en horario no laboral.

7.3.2.2. Suministro del control de acceso

Se debe determinar los procedimientos formales y directrices que se deben construir para la gestión de asignación, modificación, revisión o revocación de derechos y/o privilegios a cada uno de los usuarios (ID) creados, igualmente para los usuarios (ID) con privilegios superiores utilizados para la administración de infraestructura, aplicaciones y sistemas de información.

Controles

- ✓ La dependencia propietaria de la información debe solicitar a la oficina de las TIC a través de email institucional sistemas@areametrovalledupar.gov.co con Asunto: AUTORIZO USUARIO Y CONTRASEÑA, el acceso autorizado a los sistemas de información que opera cuando se requiera.
- ✓ Para que los usuarios tengan acceso a la información ubicada en los discos de red, el Líder del proceso o jefe inmediato deberá enviar un correo autorizando el acceso y permisos, correspondientes al rol y funciones a desempeñar, al Área de TIC. Los usuarios tendrán permisos de escritura, lectura o modificación de información en los discos de red, dependiendo de sus funciones y su rol.
- ✓ La información institucional que se trabaje en las estaciones cliente de cada usuario debe ser trasladada periódicamente a los discos de red por ser información institucional. Es responsabilidad del líder del proceso asegurar su cumplimiento.
- ✓ Se realizara asignación, modificación, revisión o revocación de derechos y/o privilegios a cada uno de los usuarios (ID) creados de acuerdo a los procedimientos establecidos en el Modelo integrado de Planeación y Gestión.
- ✓ El personal del Área de Tecnología y Sistemas de la Información debe emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad y utilizar los criterios de autenticación fuerte de acuerdo al rol asignado.

- ✓ Los administradores de los sistemas de información deben seguir las políticas de cambio de clave y utilizar procedimiento de salvaguarda o custodia de las claves o contraseñas en un sitio seguro.
- ✓ Los funcionarios del Área de Tecnología y Sistemas de Información se obligan a no revelar a terceras personas, la información a la que tengan acceso en el ejercicio de sus funciones de acuerdo con la guía de clasificación de la información según sus niveles de seguridad. En consecuencia, se obligan a mantenerla de manera confidencial y privada y a protegerla para evitar su divulgación
- ✓ El acceso a cualquier servicio, servidor o sistema de información debe ser autenticado y autorizado.
- ✓ Los funcionarios encargados de realizar la instalación o distribución de software, sólo instalarán productos con licencia y software autorizado.
- ✓ Se suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados.
- ✓ El restringido al área de TIC el acceso a los códigos fuentes de los programas y elementos asociados como (diseños, especificaciones, librerías de fuentes de programas, planes de verificación y planes de validación). no se podrá realizar ninguna actividad de tipo remoto sin la debida aprobación del líder del Área de TIC.

7.3.2.3. Responsabilidades de los usuarios

Los usuarios DEBEN aplicar buenas prácticas por la salvaguarda de su información de autenticación.

Controles

- ✓ La contraseña o password debe Poseer algún grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, ni productos a resaltar de su entidad.
- ✓ Nunca utilice sus contraseñas personales en el entorno laboral Tener mínimo ocho caracteres alfanuméricos.
- ✓ Cambiar su contraseña obligatoriamente la primera vez que el usuario ingrese al sistema.
- ✓ Cambiar su contraseña periódicamente..
- ✓ Cambiar su contraseña si ha estado bajo riesgo o se ha detectado anomalía en la cuenta de usuario.
- ✓ No debe ser visible en la pantalla, al momento de ser ingresada o mostrarse o compartirse.
- ✓ El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta o su jefe inmediato.
- ✓ El empleado y/o funcionario público como usuario de TIC es responsable de la protección de la información a su cargo y no debe compartir, publicar o dejar a la vista, datos sensitivos como Usuario y Password, Direcciones IP entre otros.
- ✓ Los empleados y/o funcionarios públicos; NO deben guardar su contraseña en una forma legible en archivos del disco duro sin protección debida, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente o solicitar al área de TIC su cambio.
- ✓ El empleado y/o funcionario público es responsable de todas las transacciones o acciones efectuadas con su “cuenta de usuario”. Nunca debe compartirse la contraseña o revelarla a otros.

- ✓ Prevenir el acceso no autorizado. Usando un sistema de contraseñas robusto, activando el protector de pantalla, configurando el protector de pantalla para que se active al cabo de 15 minutos de inactividad y que requiera una contraseña para continuar la actividad.
- ✓ Los empleados y/o funcionarios públicos no tienen AUTORIZACION para abrir, desarmar o manipular de manera inadecuada los equipos de cómputo de la Entidad. Instalar o desinstalar dispositivos, y software que no esté debidamente licenciados.
- ✓ No deben hacer mal uso de los recursos tecnológicos como envíos o reenvíos masivos de correos electrónicos o spam, practica de juegos en línea, uso permanente de redes sociales personales, conexión de periféricos o equipos que causen molestia a compañeros de trabajo, etc

7.3.2.4. Areas seguras

Se deben definir perimetros fisicos de seguridad donde se encuentra información critica, sensible o se realice almacenamiento y/o procesamiento de informacion.

Controles

- ✓ Sólo el personal autorizado puede acceder áreas restringidas.
- ✓ Son áreas restringidas : los cuartos de máquinas y cuarto de Procesamiento de Datos, archivos de Gestión, Archivo Central en las instalaciones de la ÁREA METROPOLITANA DE VALLEDUPAR.
- ✓ El profesional responsable del Área de tecnologías de información y comunicaciones autoriza el acceso a cuartos de máquinas y centros de procesamiento de datos.
- ✓ El Secretario General autoriza el acceso a archivos de Gestión y Archivo central.
- ✓ El Área de Tecnología y Sistemas de Información, realizará la Gestión del sistema de video seguridad (Circuito cerrado de televisión CCTV), así mismo administrará estas plataformas.
- ✓ El acceso a la información del CCTV se hará previa solicitud y autorización del líder del Proceso.
- ✓ El ÁREA METROPOLITANA DE VALLEDUPAR a través de la Secretaría General debe garantizar la seguridad física en todas las sedes de la Entidad para prevenir e impedir accesos no autorizados, daños e Interferencia a las sedes, instalaciones, así como a la información que recibe y genera.
- ✓ **La conexión remota y el acceso** a los sistemas de información de la Entidad debe ser en la oficina de las TIC o autorizada con el fin de minimizar el riesgo de accesos no autorizados.
- ✓ **Se Restringirá la administración remota de equipos** conectados a Internet, salvo que se cuente con la autorización y con un mecanismo de control de acceso seguro autorizado por el dueño de la información y de la oficina de las TIC
- ✓ Todos los recursos físicos inherentes a los sistemas de información del ÁREA METROPOLITANA DE VALLEDUPAR deben estar protegidos, como las instalaciones, equipos, cableado, expedientes, medios de almacenamiento, etc...
- ✓ El área de Seguridad y Salud en el Trabajo implementará y mantendrá en operación sistemas de control de incendio, así como planes integrales a las instalaciones para prevenir inundaciones o humedad en los centros de datos y centros de cableado.
- ✓ Los empleados y funcionarios públicos deben mantener su escritorio limpio para

los papeles y medios de almacenamiento removibles, y sus pantallas limpias y organizadas.

- ✓ La oficina de las TIC debe administrar, controlar los perímetros de seguridad que implemente mediante la instalación y configuración de "gateways" con funcionalidades de "firewall" o redes privadas virtuales, para filtrar el tráfico entre los dominios y bloquear el acceso no autorizado.
- ✓ La oficina de las TIC establecerá los filtros de páginas no autorizadas a través del firewall, Realizando periódicamente monitoreo de acceso y generando los informes respectivos.
- ✓ Se Restringirá el manejo de dispositivos de computación móvil y trabajo remoto para contribuir el acceso seguro a las redes, optimización del servicio de internet.
- ✓ Los cuartos de máquinas que contienen los equipos de comunicación (Routers, switches, etc.), centro de Sistema Regulado deben tener una temperatura apropiada y estar bajo llave. Se restringe el acceso a personas no autorizadas. Por ningún motivo se deben utilizar para archivos, almacenamiento de inservibles, y/o almacén de herramientas.

7.3.3. NO REPUDIO

Los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.

Controles

Son responsables los líderes de proceso seguir los lineamientos del programa de Gestión Documental en la elaboración del registro de Activos de información, de modo que estos se identifique su trazabilidad, fiabilidad, confiabilidad, retención, auditoria, intercambio electrónico de información.

Para ingresar a los sistemas de información que opera la entidad, los funcionarios y contratistas deben tener su propio usuario y contraseña, se entenderá que las transacciones que se generen con este, son avaladas por el servidor que tiene a su cargo dicho usuario.

Se elaborará el procedimiento de No-repudio de Origen proporcionando al receptor de un objeto digital una prueba infalsificable del origen de dicho objeto, lo cual evitará que el emisor niegue el envío de la información o tenga éxito ante el juicio de terceros. Y el procedimiento de No-repudio de Recepción proporcionando al emisor la prueba de que el destinatario legítimo de un mensaje u objeto digital genérico, realmente lo recibió, evitando que el receptor lo niegue posteriormente y consiga sus pretensiones.

7.3.4. PRIVACIDAD Y CONFIDENCIALIDAD

7.3.4.1. Política de Tratamiendo de Datos Personales

El Tratamiento de los datos se realizará con la finalidad de obtener y generar datos históricos, estadísticas en cumplimiento a la naturaleza de las funciones del ÁREA METROPOLITANA DE VALLEDUPAR.

Controles

- ✓ **El Tratamiento de los datos** se realizará para:

- La vinculación, desempeño de funciones o prestación de servicios, retiro o terminación, (incluye, entre otros, funcionarios, ex funcionarios, pasantes, practicantes y aspirantes a cargos).
- Para seguridad de las personas, los bienes e instalaciones de gobierno.
- Para los fines relacionados con el desarrollo el proceso de gestión contractual de productos o servicios que la entidad requiera para su funcionamiento de acuerdo a la normatividad vigente.

✓ **Datos sensibles:** el Titular tiene derecho a optar por no suministrar cualquier información sensible solicitada por el ÁREA METROPOLITANA DE VALLEDUPAR, relacionada, entre otros, con datos sobre su origen racial o étnico, la pertenencia a sindicatos, organizaciones sociales o de derechos humanos, convicciones políticas, religiosas, de la vida sexual, biométricos o datos de salud.

✓ **Derechos de los titulares:**

- Conocer, actualizar y rectificar sus datos personales frente al responsable y encargado del tratamiento. Este derecho se podrá ejercer entre otros ante datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
- Solicitar prueba de la autorización otorgada al ÁREA METROPOLITANA DE VALLEDUPAR como responsable y encargado del tratamiento, salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la Ley 1581 de 2012.
- Ser informado por el ÁREA METROPOLITANA DE VALLEDUPAR como responsable del tratamiento y encargado del tratamiento, previa solicitud, respecto del uso que le ha dado a los datos personales del Titular.
- Presentar ante el ÁREA METROPOLITANA DE VALLEDUPAR quejas por infracciones a lo dispuesto en la Ley 1581 de 2012 y las demás normas que la modifiquen, adicionen o complementen.
- Revocar la autorización y/o solicitar la supresión del dato personal cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando el ÁREA METROPOLITANA DE VALLEDUPAR haya determinado que en el tratamiento el responsable o encargado han incurrido en conductas contrarias a la Ley 1581 de 2012 y a la Constitución.
- Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento.

✓ Autorización del titular:

✓ Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa, expresa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta y verificación posterior.

✓ Casos en que no se requiere la autorización: La autorización del Titular no será necesaria cuando se trate de:

✓ Información requerida por el ÁREA METROPOLITANA DE VALLEDUPAR en ejercicio de sus funciones legales o por orden judicial.

✓ Datos de naturaleza pública.

✓ Casos de urgencia médica o sanitaria.

✓ Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.

✓ Datos relacionados con el Registro Civil de las Personas.

✓ **Datos de menores de edad**: El suministro de los datos personales de menores

de edad es facultativo y debe realizarse con autorización de los padres de familia o representantes legales del menor.

- La autorización del Titular no será necesaria cuando se trate de:
- Información requerida por el ÁREA METROPOLITANA DE VALLEDUPAR en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el Registro Civil de las Personas.

✓ **Se deberá firmar un compromiso o acuerdo de confidencialidad**: implica que la información conocida por todo funcionario, contratista y/o tercero, bajo ninguna circunstancia deberá ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total ni parcialmente, sin contar con previa autorización.

7.3.5. INTEGRIDAD

Controles

✓ Todos los funcionarios públicos son responsables de la integridad de Toda información verbal, física o electrónica, debe ser adoptada, procesada y entregada o transmitida integralmente, coherentemente, exclusivamente a las personas correspondientes y a través de los medios correspondientes, sin modificaciones ni alteraciones.

✓ El compromiso de integridad, deberá incluirse en una de las cláusulas del respectivo contrato, bajo la denominación de Cláusula de integridad de la información, para el caso de vinculación contractual.

7.3.6. DISPONIBILIDAD DEL SERVICIO E INFORMACION

Prevenir interrupciones en las actividades de la plataforma informática del ÁREA METROPOLITANA DE VALLEDUPAR que van en detrimento de los procesos críticos de TI afectados por situaciones no previstas o desastres. Se debe desarrollar e implantar un Plan de Continuidad para asegurar que los procesos misionales de TI puedan ser restaurados dentro de escalas de tiempo razonables.

El ÁREA METROPOLITANA DE VALLEDUPAR deberá tener definido un plan de acción que permita mantener la continuidad del negocio teniendo en cuenta los siguientes aspectos:

- Identificación y asignación de prioridades a los procesos críticos de TI del ÁREA METROPOLITANA DE VALLEDUPAR de acuerdo con su impacto en el cumplimiento de la misión de la entidad.
- Documentación de la estrategia de continuidad del negocio.
- Documentación del plan de recuperación del negocio de acuerdo con la estrategia definida anteriormente.
- Plan de pruebas de la estrategia de continuidad del negocio.

Controles

✓ Identificación y asignación de prioridades a los procesos críticos de TI del ÁREA METROPOLITANA DE VALLEDUPAR de acuerdo con su impacto en el

cumplimiento de la misión de la entidad

- ✓ la alta dirección del ÁREA METROPOLITANA DE VALLEDUPAR será la responsable de velar por la implantación de las medidas relativas a la disponibilidad del servicio de información. Igualmente, es responsable proveer los recursos para el desarrollo de las tareas necesarias para el mantenimiento de estas medidas.
- ✓ Los proveedores de servicios de TI deben proveer acuerdos de niveles de servicios (ANS).
- ✓ La alta dirección deberá proveer los recursos para establecer la segregación de ambientes para minimizar los riesgos de puesta en funcionamiento de aplicaciones con el fin de minimizar el impacto de la indisponibilidad del servicio.

7.3.7. REGISTRO Y AUDITORIA

Controles

- ✓ La Oficina de Control Interno y similares, tiene la responsabilidad de llevar a cabo auditorías periódicas a los sistemas y actividades relacionadas a la gestión de activos de información, así como la responsabilidad de dicha Oficina de informar los resultados de las auditorías. Estas se incluirán dentro del programa anual de auditorías. Orientadas mejorar la eficiencia de los sistemas, el cumplimiento de las políticas y procedimientos de la Entidad; así como recomendar las deficiencias detectadas.

7.3.8. GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

Prevenir el incumplimiento de obligaciones legales relacionadas con seguridad de la información.

- ✓ El ÁREA METROPOLITANA DE VALLEDUPAR, respeta y acata las normas legales existentes relacionadas con seguridad de la información, para lo cual realizará una continua revisión, identificación, documentación y cumplimiento de la legislación y requisitos contractuales aplicables para la entidad, relacionada con la seguridad de la información.
- ✓ Se establecerá el procedimiento para protección de derechos de autor y propiedad intelectual, razón por la cual propenderá porque el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.
- ✓ El Área de TIC deberá realizar la gestión de incidentes de seguridad de la información, los cuales se informarán al email oficial del área, y documentara el incidente hasta su solución.
- ✓ Los líderes de proceso son co-responsables de garantizar que todo el software que se ejecute los activos de información de la ÁREA METROPOLITANA DE VALLEDUPAR estén protegido por derechos de autor y/o licencia de uso, o sea software de libre distribución y uso.
- ✓ El Área TIC realizará el procedimiento de Copias de respaldo (BackUp) de los registros alojados en los sistemas de información.
- ✓ Los usuarios y/o funcionarios deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software, se recuerda que es ilegal duplicar software, duplicar documentación sin la autorización del propietario bajo los principios de derechos de autor y, la reproducción no autorizada es una violación a la ley.
- ✓ Ningún empleado del ÁREA METROPOLITANA DE VALLEDUPAR puede

intentar probar fallas en la Seguridad, a menos que estas pruebas sean controladas y aprobadas por el área de TIC.

7.4. OTRAS POLITICAS

7.4.1. Política de uso de impresoras y del servicio de impresión

Asegurar la operación correcta y segura de las impresoras y del servicio de impresión.

Controles

- ✓ Los documentos que se impriman en las impresoras del AMV deben ser de carácter institucional.
- ✓ Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner y fotocopiado) para que no se afecte su correcto funcionamiento.
- ✓ Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras. En caso de presentarse alguna falla, esta se debe reportar al Área de TIC.
- ✓ Los funcionarios en el momento de realizar impresiones de documentos con clasificación pública reservada o información pública clasificada (privada o semiprivada), debe mantener control de la impresora, por lo cual no la deberán dejar desatendida, preservando la confidencialidad de la información.

7.4.2. Política de computadores y portátiles

Lograr una óptima operación y salvaguarda de computadores y portátiles.

Controles

- ✓ Los computadores de mesa, portátiles, y cualquier activo de tecnología de información, podrán salir de las instalaciones únicamente con la aprobación del líder de la dependencia.
- ✓ El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones del ÁREA METROPOLITANA DE VALLEDUPAR.
- ✓ Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del computador.
- ✓ Únicamente la oficina de las TIC está autorizada para llevar a cabo los servicios de mantenimiento y reparaciones a los equipos de cómputo.
- ✓ Los usuarios deberán asegurarse de respaldar la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previniendo así la pérdida involuntaria de información, derivada del proceso de reparación.
- ✓ Los equipos del ÁREA METROPOLITANA DE VALLEDUPAR sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.
- ✓ Debe respetarse y no modificar la configuración de hardware y software establecida por la oficina de las TIC.
- ✓ Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems en computadores que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado. Todas las

comunicaciones de datos deben efectuarse a través de la LAN o WAN del ÁREA METROPOLITANA DE VALLEDUPAR.

- ✓ A menos que se indique lo contrario, los usuarios deben asumir que todo el software de la institución está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.
- ✓ Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente a la oficina de las TIC y poner el computador en cuarentena hasta que el problema sea resuelto.
- ✓ No debe utilizarse software descargado de Internet y en general software que provenga de una fuente no confiable, a menos que haya sido comprobado en forma rigurosa y que esté aprobado su uso por la oficina de las TIC del ÁREA METROPOLITANA DE VALLEDUPAR.
- ✓ Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario.
- ✓ No deben usarse USB u otros medios de almacenamiento en cualquier computador de la institución a menos que haya sido previamente verificado que están libres de virus u otros agentes dañinos.
- ✓ El personal que utiliza un computador portátil que contenga información confidencial de la institución, no debe dejarlo desatendido, sobre todo cuando esté de viaje.
- ✓ El Área de TIC no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo e información) a equipos que no sean del ÁREA METROPOLITANA DE VALLEDUPAR.
- ✓ Se prohíben que los equipos estén en contacto con piso, el usuario debe disponerlo (computador y/o Portátil) sobre el escritorio.
- ✓ Los recursos TIC utilizados para el procesamiento de la información deben ser ubicados en sitios estratégicos, que faciliten el trabajo compartido, el trabajo colaborativo, la optimización de recursos.
- ✓ Toda persona ajena al ÁREA METROPOLITANA DE VALLEDUPAR debe realizar registro en portería de sus equipos tecnológicos para poder acceder a cualquier lugar de las instalaciones de la Entidad. De igual forma debe tramitar la autorización de salida de dichos equipos.

7.4.3. Política de Switch y Routers

La Oficina de las TIC es el único responsable del manejo de los dispositivos de red, entiéndase por Routers y Switches de los que dispone el ÁREA METROPOLITANA DE VALLEDUPAR y son de propiedad de la misma, velando porque estén dispuestos en lugares seguros y protegidos a nivel físico, así como también a nivel lógico.

Controles

- ✓ Las contraseñas predefinidas que traen los dispositivos nuevos, deben cambiarse inmediatamente al ponerse en servicio el dispositivo.
- ✓ Se debe disponer de la información de los proveedores de servicios en la oficina de las TIC.
- ✓ Se deberán enumerar protocolos, puertos y servicios a ser permitidos o filtrados en cada interface, así como los procedimientos para su autorización.
- ✓ Se deberán identificar los servicios de configuración dinámica de los Routers, y las redes permitidas para accesar a dichos servicios.

- ✓ Se deben identificar los algoritmos criptográficos autorizados para levantar VPN's, cuando se requiera.

7.4.4. Política de gestión de bases de datos

Es obligación de la Oficina TIC controlar todo tipo de manejo que se efectué sobre la base de datos y velar por mantenerla protegida contra todo tipo de ataque daño o intrusión que sean de naturaleza externa o interna, y en caso de presentarse este tipo de situaciones deben aplicarse los procedimientos correctivos necesarios para restaurar el funcionamiento de la misma.

Controles

- ✓ Es función del administrador especificar los privilegios que un usuario tiene sobre la base de datos
- ✓ Registrar todos los ingresos, cada vez que un usuario entra se debe chequear cuándo y desde dónde entró la vez anterior.
- ✓ La base de datos debe estar protegida contra el fuego, el robo y otras formas de destrucción.
- ✓ Se debe garantizar que los datos sean reconstruidos en caso de daño, efectuando periódicamente un respaldo de la información.
- ✓ Los datos deben poder ser sometidos a procesos de auditoria. La falta de auditoria en los sistemas de computación ha permitido la comisión de grandes delitos.
- ✓ El sistema debe tener capacidad para verificar que sus acciones han sido autorizadas. Las acciones de los usuarios deben ser supervisadas, de modo tal que pueda descubrirse cualquier acción indebida o errónea.
- ✓ Manejo de la tabla de usuarios con código y contraseña, control de las operaciones efectuadas en cada sesión de trabajo por cada usuario y anotadas en la bitácora, lo cual facilita la auditoría de la BD.

7.4.5. Politica de gestión de comunicaciones

Controles

- ✓ El responsable de las comunicaciones designado por el ÁREA METROPOLITANA DE VALLEDUPAR impartirá directrices y asesorará, cuando lo consideré oportuno, a cada una de las dependencias en el análisis de contenidos, y las estrategias efectivas para su divulgación y/o socialización.
- ✓ El Área de TIC, asesorará en temas de su competencia, a las dependencias que en desarrollo de actividades misionales requieran el despliegue de un sitio Web, o el desarrollo y/o actualización de Sistemas de información.
- ✓ El Área de Comunicaciones validará la información que las dependencias, en cumplimiento de la normativa existente y planes internos de socialización, soliciten disponer a la ciudadanía y/o funcionarios de la Entidad.
- ✓ Todos los usuarios que manejan comunicaciones oficiales electrónicas debe aplicar respeto y buen trato cumpliendo con los lineamientos establecidos y normas vigentes.
- ✓ La oficina de las TIC, es la única responsable de administrar permisos para el ingreso a redes sociales.
- ✓ Las redes sociales se usarán de manera adecuada, respetuosa y siempre procurando mejorar y mantener la imagen institucional.
- ✓ La oficina de las TIC es la única encargada de definir las responsabilidades

funcionales y operativas con relación al Data Center o Centro de datos.

8. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El Plan de implementación para la dimensión de Seguridad y Privacidad de la Información comprende el siguiente cronograma y se le hace seguimiento mes a mes.

GESTIÓN	ACTIVIDADES	TAREA	RESPONSABLE	FECHAS PROGRAMACIÓN	
				FCHA INICIO	FECHA FINAL
Activos de Información	Definir lineamientos para el levantamiento de activos de información	Elaboración metodología e instrumento de levantamiento de activos de información	PROFESIONAL UNIVERSITARIO CÓDIGO 219 GRADO 01	3-mar-24	27-mar-24
	Levantamiento Activos de Información	Socializar la guía de activos de Información.	PROFESIONAL UNIVERSITARIO CÓDIGO 219 GRADO 01	06-abr-24	17-abr-24
		Validar activos de información en el instrumento levantado en la vigencia anterior	PROFESIONAL UNIVERSITARIO CÓDIGO 219 GRADO 01	20-abr-24	24-abr-24
		Identificar nuevos activos de información en cada dependencia	PROFESIONAL UNIVERSITARIO CÓDIGO 219 GRADO 01	04-may-24	8-may-24
		Realizar informe de actualización a los activos de información por alguna de las siguientes novedades: Actualizaciones al proceso al que pertenece el activo, Adición de actividades al proceso, Inclusión de un nuevo activo, Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados, Materialización de riesgos que cambien la criticidad del activo.	PROFESIONAL UNIVERSITARIO CÓDIGO 219 GRADO 01	11-may-24	29-may-24
	Publicación de Activos de Información	Validar y aceptar los activos de información para su publicación en SIMIG por cada líder de proceso.	PROFESIONAL UNIVERSITARIO CÓDIGO 219 GRADO 01	01-jun-24	5-jun-24

		Publicar los instrumentos de activos de información consolidado en SIMIG	PROFESIONAL UNIVERSITARIO CÓDIGO 219 GRADO 01	15-jun-24	30-jun-24
	Reporte Datos Personales	Reportar al Oficial de Datos personales o Seguridad de la Información la información recolectada en el instrumento de activos de información, correspondiente a bases de datos	PROFESIONAL UNIVERSITARIO CÓDIGO 219 GRADO 01	01-jul-24	17-jul-24
Gestión de Riesgos	Actualización de lineamientos de riesgos	Actualizar política y metodología de gestión de riesgos	PROFESIONAL UNIVERSITARIO CÓDIGO 219 GRADO 01	03-ago-24	6-ago-24
	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación	Identificación, Análisis y evaluación de Riesgos - Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	PROFESIONAL UNIVERSITARIO CÓDIGO 219 GRADO 01	10-ago-24	14-ago-24
	Aceptación de Riesgos Identificados	Aceptación, aprobación Riesgos identificados y planes de tratamiento	PROFESIONAL UNIVERSITARIO CÓDIGO 219 GRADO 01	18-ago-24	31-ago-24
	Publicación	Publicación Matriz de riesgos - SIMIG	PROFESIONAL UNIVERSITARIO CÓDIGO 219 GRADO 01 -- SUBDIRECCIÓN DE PLANEACIÓN	14-sep-24	18-sep-24
	Seguimiento Fase de Tratamiento	Seguimiento Estado planes de tratamiento de riesgos identificados y verificación de evidencias	PROFESIONAL UNIVERSITARIO CÓDIGO 219 GRADO 01	21-sep-24	30-sep-24
	Evaluación de riesgos residuales	Evaluación de riesgos residuales	PROFESIONAL UNIVERSITARIO CÓDIGO 219 GRADO 01	05-oct-24	30-oct-24
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	PROFESIONAL UNIVERSITARIO CÓDIGO 219 GRADO 01	05-oct-24	30-oct-24
	Monitoreo y Revisión	Generación, presentación y reporte de indicadores	PROFESIONAL UNIVERSITARIO CÓDIGO 219 GRADO 01	05-oct-24	15-oct-24

Protección de datos personales	Recolectar bases de datos	Elaborar y emitir un memorando para la recolección de bases de datos personales de acuerdo a los estándares emitidos por la SIC	PROFESIONAL UNIVERSITARIO CÓDIGO 219 GRADO 01	03-nov-24	13-nov-24
	Revisión de bases de datos	Revisar y realimentar la información recolectada por las áreas para el registro de las bases de datos	PROFESIONAL UNIVERSITARIO CÓDIGO 219 GRADO 01	17-nov-24	21-nov-24
	Registro y actualización de las bases de datos	Registrar o actualizar las bases de datos teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de información	PROFESIONAL UNIVERSITARIO CÓDIGO 219 GRADO 01	23-nov-24	6-dic-24