TABLA DE CONTENIDO

.

INTRODUCCIÓN

El presente documento de Políticas de Seguridad de la Información establece los lineamientos y políticas administrativas, técnicas y legales, las cuales deben ser adoptadas por todos los funcionarios, contratistas, proveedores, y todo el personal externo que utilice los servicios de tecnologías de la información que ofrece la Alcaldía de Manizales.

Las políticas de seguridad descritas, se encuentran enfocadas al cumplimiento de la normatividad legal colombiana vigente y al modelo de seguridad y privacidad del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia – Mintic.

La Administración Municipal es consciente de las amenazas que enfrenta su información y de las consecuencias a las que se expone, cuando no cuenta con las medidas de seguridad y protección adecuadas. En ese sentido, la Alcaldía de Manizales debe tener una visión general de los riesgos de seguridad digital que pueden afectar la seguridad y privacidad de la información, donde se podrán establecer controles y medidas efectivos, viables y transversales con el propósito de realizar el aseguramiento de la disponibilidad, integridad y confidencialidad tanto de la información como de los datos de los servidores públicos, contratistas y partes interesadas.

Es preciso que la Administración Municipal realice una adecuada identificación, clasificación, valoración, gestión y tratamiento de los riegos de seguridad digital que puedan afectar la información de la entidad, con el propósito de implementar medidas y controles efectivos que permitan estar preparados ante situaciones en las que se vea comprometida tanto la seguridad física y lógica de sus instalaciones, personas, recursos y sistemas, como la seguridad de su información.

Teniendo en cuenta lo anterior, el presente documento tiene como finalidad establecer los principios orientadores en seguridad que buscan garantizar la disponibilidad, integridad, confidencialidad, privacidad, continuidad, autenticidad y no repudio de la información de la Alcaldía de Manizales, así como dar lineamientos para la aplicación de mecanismos que eviten la vulneración de la integralidad, seguridad, privacidad y criticidad de la información, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información – SGSI.

1. OBJETIVO

Instaurar lineamientos necesarios, con el fin de fortalecer las políticas (la gestión) de Seguridad y privacidad de la Información de la Alcaldía de Manizales, enmarcados en la implementación de un Sistema de Gestión de Seguridad de la Información, basado en la identificación y valoración de los riesgos asociados a ella, propendiendo por la protección de su confidencialidad, integridad, disponibilidad, privacidad, continuidad, autenticidad y criticidad.

2. ALCANCE

Los lineamientos contenidos en el presente documento son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por los servidores públicos, contratistas, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la Entidad a través de la recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información, con personal interno o externo, en el desarrollo de la misión institucional y el cumplimiento de sus objetivos estratégicos.

3. DEFINICIONES

Activo: Se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas) que tienen un valor para la entidad.

Activo crítico: Instalaciones, sistemas y equipos los cuales, si son destruidos, o es degradado su funcionamiento o por cualquier otro motivo no se encuentran disponibles, afectarán el cumplimiento de los objetivos estratégicos De la Administración Municipal.

Administración de Riesgos: Se entiende por administración de riesgos, como el proceso de identificación, control, minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar la información o impactar de manera considerable la operación. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la entidad.

Análisis de Impacto al Negocio (BIA - Business Impact Analysis): Es una metodología que permite identificar los procesos críticos que apoyan los productos y servicios claves, las interdependencias entre procesos, los recursos requeridos para operar en un nivel mínimo aceptable y el efecto que una interrupción del negocio podría tener sobre ellos.

Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Alta Dirección: Persona o grupo de personas que dirigen y controlan al más alto nivel una entidad.

Centro de cableado: El centro de cableado es el lugar donde se ubican los recursos de comunicación de tecnologías de información, como (Switch, patch, panel, UPS, Router, Cableado de voz y de datos).

Cifrado: Método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.

Control: Son todas aquellas políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Confiabilidad de la Información: Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Confidencialidad: Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Código malicioso: Es un código informático que crea brechas de seguridad para dañar un sistema informático.

Custodio: Es una parte designada de la entidad, un cargo o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación de privilegios de acceso, modificación y borrado.

Dato personal: Cualquier información vinculada o que pueda asociarse a una o a varias personas naturales determinadas o determinables. Debe entonces entenderse el “dato personal” como una información relacionada con una persona natural (persona individualmente considerada).

Dato personal público: Toda información personal que es de conocimiento libre y abierto para el público en general.

Dato personal privado: Toda información personal que tiene un conocimiento restringido, y en principio privado para el público en general.

Dato semiprivado: Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su Titular sino a cierto sector o grupo de personas o a la sociedad en general.

Datos sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así́ como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

Datacenter: Se denomina también Centro de Procesamiento de Datos (CPD) a aquella ubicación o espacio donde se concentran los recursos necesarios (TI) para el procesamiento de la información de una organización.

Disponibilidad: Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Dispositivos móviles: Equipo celular smartphone, equipos portátiles, tablets, o cualquiera cuyo concepto principal sea la movilidad, el cual permite almacenamiento limitado, acceso a internet y cuenta con capacidad de procesamiento.

Evento: Es el suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.

Evento de seguridad de la información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o falla de salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

Home Office: Oficina en casa o trabajo en casa

Incidente de Seguridad: Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad significativa comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Integridad: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento. **Impacto:** Resultado de un incidente de seguridad de la información.

Legalidad: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeta la entidad

Mesa de Ayuda: Constituye el único punto de contacto con los usuarios para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información.

No repudio: El emisor no puede negar que envió porque el destinatario tiene pruebas del envío. El receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor pueda negar tal envío**.**

Partes interesadas: Persona u organización que puede afectar o ser afectada o percibirse a sí misma como afectada por una decisión o actividad.

Plan de Continuidad de Negocio: Actividades documentadas que guían a la Entidad en la respuesta, recuperación, reanudación y restauración de las operaciones a los niveles predefinidos después de un incidente que afecte la continuidad de las operaciones.

Privacidad de la información: El derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de Gobierno Digital la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Propietario de la información (titular): Es la unidad organizacional o proceso donde se crean los activos de información.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Terceros: Personas naturales o jurídicas que tienen un contrato tercerizado y prestan un servicio a la entidad y hacen uso de la información y los medios tecnológicos dispuestos por la entidad.

Test de penetración: Es un ataque dirigido y controlado hacia componentes de infraestructura tecnológica para revelar malas configuraciones y vulnerabilidades explotables.

VPN: Red virtual privada por sus siglas en ingles Virtual Private Network, utilizada para acceder a los servicios de la entidad de manera remota.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

4. MARCO LEGAL

Constitución Política de Colombia. Artículo 15.

Ley 44 de 1993: Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor).

Ley 527 de 1999: Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 594 de 2000: Por medio de la cual se expide la Ley General de Archivos.

Ley 850 de 2003: Por medio de la cual se reglamentan las veedurías ciudadanas

Ley 1266 de 2008: Por la cual se dictan las disposiciones generales del Habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

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

Ley 1341 de 2009: Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones – TIC, se crea la agencia Nacional de espectro y se dictan otras disposiciones.

Ley 1437 de 2011: Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.

Ley 1474 de 2011: Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

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

Ley 1712 de 2014: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Ley 1915 de 2018: Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.

Ley 1952 de 2019: Por medio de la cual se expide el código general disciplinario

Decreto 2609 de 2012: Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

Decreto 0884 del 2012: Por el cual se reglamenta parcialmente la Ley 1221 del 2008.

Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

Decreto 886 de 2014: Por el cual se reglamenta el Registro Nacional de Bases de Datos.

Decreto 103 de 2015: Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

Decreto 1074 de 2015: Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.

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

Resolución 512 de 2019: Por la cual se adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios De la Administración Municipal/Fondo de Tecnologías de la Información y las Comunicaciones y se definen lineamientos frente al uso y manejo de la información.

CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.

CONPES 3854 de 2016. Política Nacional de Seguridad digital.

RESOLUCIÓN 1519 DEL 2020. Transparencia en el acceso a la información, accesibilidad web, seguridad digital web y datos abiertos.

5. POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

La Alcaldía de Manizales, en cumplimiento de sus funciones y comprendiendo la importancia de una adecuada gestión de la información, se ha comprometido a proteger, preservar y administrar la confidencialidad, integridad, disponibilidad de la información de la Entidad, mediante una gestión integral de riesgos, implementación de controles físicos y digitales, previniendo incidentes y dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua.

Para lograr el desarrollo de la política de seguridad de la información se hace necesario establecer los objetivos de seguridad de la información así:

- Implementar, operar y mejorar de forma continua el Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.
- Minimizar el riesgo de vulnerabilidad en la seguridad de la información en la ejecución de los procesos misionales de la entidad.

- Cumplir con los principios (Disponibilidad, Integridad y Confidencialidad) de seguridad de la información.
- Mantener la confianza de los servidores públicos, colaboradores y terceros.
- Apoyar la innovación tecnológica.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los servidores públicos, colaboradores y terceros, que hacen parte de la Administración Municipal.
- Verificar de manera periódica el cumplimiento de las políticas de seguridad de la información.
- Propender para que todos los servidores públicos, contratistas y terceros cumplan con las políticas, lineamientos, y buenas prácticas de seguridad de la información establecidas en el presente Manual de Políticas de Seguridad de la Información.

6. LINEAMINETOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

6.1 LINEAMIENTO DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

6.1.1 ORGANIZACIÓN INTERNA

Lineamientos:

a. Los activos de información deben estar bajo la custodia del responsable del activo, para evitar conflicto y reducir oportunidades de modificación (intencional o no), no autorizada o mal uso de los activos de información de la Alcaldía de Manizales.

b. La Unidad de Gestión Tecnológica de la Alcaldía de Manizales debe mantener y documentar los contactos con autoridades (Policía, bomberos, etc.) u otros especializados, con el fin de contactar en caso de que se presente un incidente de seguridad de la información y requiera de asesoría externa.

c. La Unidad de Gestión Tecnológica de la Alcaldía de Manizales es la única facultada para administrar y configurar el acceso a los recursos de la plataforma tecnológica en la entidad de acuerdo a la descripción de cargo.

d. Los proyectos que se Desarrollen en la Administración Municipal deben contemplar una gestión de los riesgos de seguridad asociados a la información del proyecto, lo cual incluye una identificación de los riesgos y la definición de la forma como serán gestionados.

6.1.2 DISPOSITIVOS MOVILES

Lineamientos:

a. La Unidad de Gestión Tecnológica, debe conocer el inventario actualizado de los dispositivos móviles autorizados
b. Los dispositivos móviles de propiedad de los de Servidores Públicos, contratistas, o terceros no deben estar incluidos en el dominio manizales.gov.co o cualquiera que funcione dentro de la entidad, para conectarse a los servicios de la red de datos deberán realizar solicitud a la mesa de ayuda y cumplir con los lineamientos referentes a seguridad de la información.
c. Todos los dispositivos móviles que almacenen información de la Administración Municipal deben tener instalado un software antivirus, y sistema operativo actualizado
d. En dispositivos móviles entregados por la Administración Municipal, los Servidores Públicos no están autorizados a cambiar la configuración, a desinstalar software, formatear o restaurar de fábrica.
e. En caso de pérdida o robo de un dispositivo móvil de propiedad del Municipio de Manizales, los Servidores Públicos, tendrán que realizar la respectiva denuncia ante la entidad competente, luego debe dar aviso inmediato a la oficina de bienes Municipales.

6.1.3 TRABAJO EN CASA

Lineamientos:

a. La Unidad de Gestión Tecnológica debe establecer los requerimientos para autorizar conexiones remotas a la infraestructura tecnológica necesaria para la ejecución de las funciones de los servidores públicos, contratistas e la Administración Municipal, garantizando las herramientas y controles para proteger la confidencialidad, integridad y disponibilidad de las conexiones remotas.
b. Toda información gestionada por funcionarios de la Administración Municipal, y que sea accedida remotamente debe ser utilizada solamente para el cumplimiento de las funciones del cargo o de las obligaciones contractuales.

6.2 LINEAMIENTO DE SEGURIDAD DE LOS RECURSOS HUMANOS

6.2.1 ANTES DE ASUMIR EL EMPLEO:

Lineamientos

a. La Unidad de Gestión Humana de la Alcaldía de Manizales, debe contar con procedimientos para la vinculación de personal, de acuerdo a la normatividad establecida para tal fin.
b. Desde los servicios Jurídicos se debe definir una lista de verificación que contenga los aspectos necesarios para la revisión de los antecedentes del personal a contratar por prestación de servicios de acuerdo con la normatividad vigente.
c. La Unidad de Gestión Humana y Servicios Jurídicos, deben establecer mecanismos o controles necesarios para proteger la confidencialidad y reserva de la información contenida en las historias laborales y expedientes contractuales.
d. Todo Servidor Público o contratista, debe firmar un documento o cláusulas en las que se establezcan acuerdo de confidencialidad y no divulgación de la información reservada del Municipio de Manizales, estos deben reposar en la historia laboral o expediente contractual según sea el caso.

6.2.2 DURANTE LA EJECUCIÓN DEL EMPLEO:

Lineamientos

a. Los Servidores Públicos y contratistas deben suscribir la autorización para el tratamiento de los datos personales de acuerdo con la Política de tratamiento de datos personales De la Administración Municipal y de acuerdo con lo establecido en la Ley 1581 de 2012 y sus decretos reglamentarios.
b. Una vez formalizado el proceso de vinculación, el jefe inmediato, supervisor o el delegado del área para tal fin, debe solicitar a través de la mesa de ayuda la apertura de los servicios tecnológicos que requiera el Servidor Público, contratista o tercero, para la ejecución de sus funciones u obligaciones contractuales.
c. La Unidad de Gestión Tecnológica y el personal de apoyo que se requiera, debe diseñar y ejecutar de manera permanente, un programa de concientización en seguridad de la información, con el fin de apoyar la protección adecuada de la información.
d. La Unidad de Gestión Tecnológica en conjunto con la Oficina de Divulgación y Prensa deben diseñar y ejecutar un plan de Uso y apropiación de comunicaciones en apropiación del

Sistema de Gestión de la Seguridad de la Información - SGSI, el cual se debe ejecutar durante la vigencia al interior de la Alcaldía de Manizales.

e. Es responsabilidad del Servidor Público, contratista o personal provisto por terceros, informar de los incidentes de seguridad de la información a través de la mesa de ayuda de la Unidad de Gestión Tecnológica.
f. En lo pertinente al incumplimiento de las políticas de la seguridad de la información, se aplicará lo establecido en los procedimientos destinados para tal fin, enmarcados en la normatividad vigente.

6.2.3 TERMINACIÓN Y CAMBIO DE EMPLEO

Lineamientos

a. Es de responsabilidad del Servidor Público realizar la entrega de la información propia de la entidad, que se encuentra en gestión del servidor público, cuando existe una novedad de retiro, investigación, inhabilidades, o cambio de funciones, utilizando para ello el formato de entrega de puesto de trabajo, publicado en la plataforma de gestión de la entidad.
b. El supervisor del contrato o a quien este delegue debe recoger y custodiar la información del Municipio de Manizales bajo la responsabilidad del contratista en caso de terminación anticipada, definitiva, temporal o cesión del contrato.
c. La Unidad de Gestión Tecnológica debe parametrizar en el directorio activo, la inactivación automática de los contratistas, teniendo en cuenta la fecha de terminación del contrato; la inactivación de los usuarios de los sistemas de información que no se autentican con el directorio activo, se debe hacer de forma manual.
d. La Unidad de Gestión Humana y los supervisores de contratos de prestación de servicios, deben informar a la Unidad de Gestión Tecnológica, a través de la Mesa de Ayuda, cualquier novedad de desvinculación administrativa, laboral o contractual del Servidor Público, contratista o tercero; una vez notificada la novedad la Unidad de Gestión Tecnológica, debe proceder a la inactivación de los y servicios accesos y servicios de red del Servidor Público, contratista o tercero
e. Se creará una copia de respaldo del buzón de correo electrónico una vez se dé por terminada la vinculación con el Municipio de Manizales.

f. Bajo ningún parámetro se podrán restablecer los accesos a correos electrónicos; solo se podrán restablecer buzones para consulta y no se podrán emitir correos ni notificaciones desde estos buzones.
g. Se deben inactivar todos los accesos a los sistemas de información.
h. La Unidad de Gestión Humana debe solicitar la devolución del carné o cualquier distintivo de autenticación, que lo acredita como Servidor Público, contratista o tercero del Municipio de Manizales.

6.3 LINEAMIENTO DE GESTIÓN DE ACTIVOS

6.3.1 RESPONSABILIDAD POR LOS ACTIVOS

Lineamientos

a. Todos los procesos del Municipio de Manizales que aplique, deben contar con un inventario de sus activos de información y se debe evidenciar a través de los instrumentos dispuestos.
b. Todos los activos de información mantenidos en el inventario deben tener un propietario
c. La Unidad de Gestión Tecnológica, debe establecer una configuración adecuada para los recursos tecnológicos, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información
d. Los Servidores Públicos, contratistas o terceros, no deben usar software no autorizado o de su propiedad en activos de la Alcaldía de Manizales.
e. Todo aquel elemento o equipo de hardware retirado de las instalaciones de la entidad debe tener su respectiva orden de salida y la Unidad de Gestión Tecnológica deberá hacer un seguimiento periódico al destino de los mismos.
f. Los Servidores Públicos, contratistas o terceros de la Alcaldía de Manizales, deben hacer entrega de los activos bajo su responsabilidad de acuerdo con el formato de Entrega de puestos de trabajo.

6.3.2 CLASIFICACIÓN DE LA INFORMACIÓN

Lineamientos

a. La Unidad de Gestión Tecnológica será la encargada de recolectar y actualizar el inventario de activos de información que involucren componentes tecnológicos.
b. Las Tablas de Retención Documental (TRD) deben indicar el tipo de clasificación de las series, subseries y documentos en ella contenidas.
c. Los Servidores Públicos, contratistas o terceros De la Administración Municipal deben aplicar la clasificación de la información de la Alcaldía de Manizales, las TRD, el inventario de activos de información y lineamientos para la administración de los archivos.
d. Cada propietario del activo de Información debe velar por el cumplimiento de su clasificación de acuerdo con lo establecido en lineamientos para la administración de los archivos y activos de Información
e. Para el intercambio de información se debe tener en cuenta su clasificación para su debida protección en términos de confidencialidad.

6.3.3 MANEJO DE MEDIOS

Lineamientos

a. La Unidad de Gestión Tecnológica debe definir un procedimiento para el uso de medios removibles.
b. La Unidad de Gestión Tecnológica debe proveer a los usuarios De la Administración Municipal los métodos de cifrado de la información, así como administrar el software o herramienta utilizado para tal fin, y generar la guía de uso para el usuario.
c. Todo medio removible debe ser escaneado mediante las soluciones de seguridad, suministrado por La Unidad de Gestión Tecnológica cada vez que se conecte a un equipo De la Administración Municipal.
d. Es responsabilidad de cada Servidor Público, contratista o tercero tomar las medidas para la protección de la información contenida en medios removibles, para evitar acceso físico y lógico no autorizado, daños, pérdida de información o extravío del mismo.
e. Se prohíbe el uso de medios removibles que contengan información reservada o clasificada De la Administración Municipal
f. La Unidad de Gestión Tecnológica debe crear o actualizar si fuere necesario el procedimiento o documento donde se establezca la disposición final de residuos de aparatos eléctricos y electrónicos (RAEE).

g. Cuando se requiera transferir un medio de almacenamiento de información De la Administración Municipal a otras entidades se debe establecer un acuerdo de confidencialidad y seguridad, entre las partes.
h. La Unidad de Gestión Tecnológica debe generar y aplicar lineamientos para la disposición segura de los dispositivos que almacenen información de la entidad, ya sea cuando son dados de baja o asignados a un nuevo usuario.
i. La Unidad de Gestión Tecnológica debe autorizar el uso de periféricos o medios de almacenamiento externo, de acuerdo con las necesidades requeridas para el cumplimiento de las funciones y del perfil del cargo de los servidores públicos o Contratistas
j. Los servidores públicos, Contratistas o personal provisto por terceras partes deben acoger las condiciones de uso de periféricos y medios de almacenamiento establecidos por La Unidad de Gestión Tecnológica.
k. Se deben emplear herramientas de borrado seguro y demás mecanismos de seguridad pertinentes en los medios de propiedad de la Administración Municipal que sean reutilizados o dados de baja, con el fin de controlar que la información de la Administración Municipal contenida en estos medios no se pueda recuperar.
l. Cuando se requiera transferir un medio de almacenamiento se debe tener en cuenta el registro de contenido de los medios, la protección aplicada, al igual que los tiempos de transferencia a los responsables durante el transporte y el recibido.
m. El transporte para los medios de almacenamiento debe contar con las condiciones apropiadas para salvaguardar la integridad, confidencialidad y disponibilidad de la información de la Administración Municipal.

6.4 LINEAMIENTO CONTROL DE ACCESOS

6.4.1 REQUISITOS DE LA ENTIDAD PARA EL CONTROL DE ACCESO

Lineamientos:

a. La Unidad de Gestión Tecnológica debe suministrar y garantizar el cambio de contraseña, a los usuarios las credenciales para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, según su perfil y rol, las credenciales de acceso son de uso personal e intransferible.

b. La conexión remota a la red de área local De la Administración Municipal debe establecerse a través de una conexión VPN, la cual debe ser aprobada, registrada y monitoreada por La Unidad de Gestión Tecnológica.
c. La Unidad de Gestión Tecnológica debe establecer una segregación de las redes, separando los entornos de red de usuarios de los entornos de red de servidores y servicios publicados.
d. La Unidad de Gestión Tecnológica debe asegurar que las redes inalámbricas de la Entidad cuenten con métodos de autenticación que evite accesos no autorizados.
e. La Unidad de Gestión Tecnológica debe realizar el cambio de contraseña de la red inalámbrica de la Entidad mínimo tres (3) veces al año.
f. La Unidad de Gestión Tecnológica para los eventos que se realicen en la Entidad debe generar usuario y clave de red Wifi, el cual debe expirar una vez finalizado el evento
g. La Unidad de Gestión Tecnológica debe revisar que los equipos personales de los Servidores Públicos, contratistas o terceros De la Administración Municipal que se conecten a las redes de datos De la Administración Municipal cumplan con todos los requisitos o controles para autenticarse y únicamente podrán realizar las tareas para las que fueron autorizados.

6.4.2 GESTIÓN DE ACCESO DE USUARIOS

Lineamientos:

a. La creación de usuarios para los diferentes accesos en la entidad, deberá ser solicitada por su jefe inmediato mediante la mesa de ayuda de la Unidad de Gestión Tecnológica.
b. La Unidad de Gestión Tecnológica debe definir un procedimiento que contemple la creación, actualización, activación e inactivación de cuentas de usuario.
c. La Unidad de Gestión Tecnológica sólo otorgará a los usuarios, los accesos solicitados y autorizados por el jefe inmediato, supervisor del contrato o un jefe de mayor jerarquía.
d. Por defecto los usuarios creados no tienen permisos de administrador. En caso de requerirlo deben realizar la solicitud por medio de la mesa de ayuda de la Unida de gestión tecnológica. Sólo se otorgan los privilegios para la administración de recursos tecnológicos, servicios de red, sistemas operativos y sistemas de información a aquellos usuarios que cumplan dichas actividades.

e. El usuario y la contraseña asignados para el acceso a los diferentes servicios tecnológicos, es personal e intransferible. Cualquier actividad que se realice con el usuario y clave será responsabilidad del servidor público y contratista al cual le fue asignado.
f. La Unidad de Gestión Tecnológica debe garantizar que las estaciones de trabajo con perfil de administrador local sean las que estén autorizadas, en caso contrario se debe modificar el permiso en la configuración de la estación de trabajo.
g. Una vez finalizada la gestión de servicios prestados por terceras partes para la Entidad, el supervisor de contrato debe garantizar que los accesos queden cerrados al finalizar el proceso o contrato.
h. La Unidad de Gestión Tecnológica, con el apoyo de Mesa de Ayuda Unidad de Gestión Tecnológica, debe garantizar que los usuarios, realicen el cambio de contraseña de acceso a los servicios de la Administración Municipal, cada vez que sea requerido.
i. La Unidad de Gestión Tecnológica de Información debe deshabilitar los servicios o funcionalidades no utilizadas de los sistemas operativos, el firmware, bases de datos y demás recursos tecnológicos.
j. La Unidad de Gestión Tecnológica debe mantener un listado actualizado con las cuentas que administren todos los recursos tecnológicos.
k. La contraseña para la autenticación se debe suministrar a los usuarios de manera segura, y el sistema debe solicitar el cambio inmediato de la misma al ingresar.
l. La Unidad de Gestión Tecnológica debe establecer controles para que los usuarios finales de los servicios tecnológicos no tengan instalado en sus equipos de cómputo software o herramientas que permitan la obtención de privilegios no autorizados.

6.4.3 RESPONSABILIDADES DE LOS USUARIOS

Lineamientos:

a. La Unidad de Gestión Tecnológica debe garantizar que para el ingreso a los servicios tecnológicos de la entidad las contraseñas no sean visibles en texto claro.
b. Las contraseñas deben poseer algún grado de complejidad y no deberán ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, por tanto:
c. Los administradores de los servicios tecnológicos o Sistema de Información deben de entregar de manera adecuada las credenciales de acceso.

6.4.4 CONTROL DE ACCESOS A SISTEMAS Y APLICACIONES

Lineamientos:

a. La Unidad de Gestión Tecnológica, deben velar por que los servicios tecnológicos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico, teniendo en cuenta la matriz de roles y perfiles para cada sistema de información.
b. La Unidad de Gestión Tecnológica, se debe acoger a las buenas prácticas de desarrollo seguro en los productos entregados, controlando el acceso lógico cuando estos estén en producción.
c. La Unidad de Gestión Tecnológica, deben revisar los perfiles definidos, de acuerdo con la matriz de roles y perfiles, en los casos cuando exista novedades de gestión de cuenta (creación, traslado, inactivación, incapacidades y licencias).
d. La Unidad de Gestión Tecnológica debe establecer ambientes separados a nivel físico y lógico para el desarrollo-pruebas y producción; contando con su plataforma, servidores, aplicativos, dispositivos y versiones independientes de los otros ambientes, para evitar así que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad, confidencialidad y disponibilidad de la información de los servicios en producción.
e. La Unidad de Gestión Tecnológica debe asegurar mediante los controles necesarios, que los usuarios utilicen diferentes cuentas de usuario para los ambientes pruebas y producción y así mismo que los menús muestren los mensajes de identificación apropiados para reducir el riesgo de error.
f. Los desarrolladores deben asegurar que no se desplieguen en pantalla las contraseñas ingresadas.
g. Los desarrolladores deben, a nivel de los aplicativos, restringir el acceso a archivos u otros recursos, a direcciones URL protegidas, a funciones protegidas, a servicios, a información de las aplicaciones, a atributos y políticas utilizadas para los controles de acceso y a la información relevante de la configuración, solamente a usuarios autorizados.

6.5 LINEAMIENTO SEGURIDAD FÍSICA Y DEL ENTORNO

6.5.1 ÁREAS SEGURAS

Lineamientos

a. La Unidad y de Gestión Tecnológica y el Archivo General Municipal, deberán señalizar las áreas seguras de acuerdo con el inventario de áreas seguras.
b. Las puertas y ventanas de las áreas seguras deben permanecer cerradas y bloqueadas cuando no haya supervisión o estén desocupadas.
c. Todos los puntos de acceso deben tener un nivel de seguridad para controlar el acceso físico al sitio o instalación.
d. El personal de vigilancia debe establecer mecanismos para inspeccionar y examinar los morrales, bolsos, cajas, etc. que ingresen los Servidores Públicos y Contratistas o visitantes a las instalaciones de la Administración Municipal.
e. El personal de vigilancia debe registra en una bitácora o sistema de información el ingreso y retiro de todo equipo cómputo elemento informático (pc o portátil, mouse, teclado, cargador, etc.), servidores, equipos activos de red o cualquier equipo electrónico diferentes a smartphone.
f. La Unidad de Gestión Tecnológica, debe controlar el ingreso a los centros de datos y centros de cableado de la Administración Municipal.
g. Cuando la Unidad de Gestión Tecnológica, autorice el ingreso a personal ajeno a la entidad, a los centros de datos y centros de cableado, este debe estar acompañado por quien sea autorizado, éste se hará responsable de la estadía durante el tiempo que permanezca en las instalaciones.
h. Todo el personal que ingrese a las áreas seguras debe tener permiso del ingreso a la misma. Este debe estar acompañado por quien sea autorizado.
i. La Unidad de Gestión Tecnológica debe proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia, monitoreo y alarmas en caso de detectarse

condiciones ambientales inapropiadas. Estos sistemas deben monitorearse de manera permanente.

j. La Unidad de Gestión Tecnológica debe velar por que los recursos de la plataforma tecnológica de la Entidad ubicado en el centro de cómputo se encuentren protegidos contra fallas o interrupciones eléctricas.

k. La Unidad de Gestión Tecnológica y El Archivo General del Municipio establecen los lineamientos para los controles contra amenazas externas y ambientales y quedarán enmarcadas en los planes de contingencia, de emergencia y de continuidad del negocio.

l. La Unidad de Gestión Tecnológica debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado.

m. La Unidad de Gestión Tecnológica debe realizar mantenimientos preventivos al centro de cómputo y centros de cableado que estén bajo su custodia; así mismo, se debe llevar el control al plan de mantenimiento de servicios tecnológicos.

n. Las puertas del centro de cómputo deben permanecer cerradas.

o. En el centro de cómputo y centro de cableado está prohibido: (Fumar, Ingresar comidas o bebidas, el porte de armas de fuego, corto punzantes o similares, mover, desconectar y/o conectar equipos sin autorización, modificar la configuración del equipo o interconectarlo sin autorización, Alterar software instalado en los equipos sin autorización, Alterar o dañar las etiquetas de identificación de los sistemas de información o sus conexiones físicas, Extraer información de los equipos en dispositivos externos sin previa autorización)

p. La Unidad de Gestión Tecnológica debe velar por que los cables de potencia estén separados de los de comunicaciones siguiendo las normas técnicas pertinentes.

q. La Unidad de Gestión Tecnológica debe controlar el acceso de visitantes a los centros de cómputo y centros de cableado que estén bajo su custodia.

6.5.2 EQUIPOS

Lineamientos

a. La Unidad de Gestión Tecnológica velará que los equipos de cómputo, escáneres e impresoras estén situados y protegidos en áreas para reducir el riesgo contra amenazas ambientales y de acceso no autorizado.

b. La Unidad de Gestión Tecnológica, debe propender que los equipos de cómputo portátiles suministrados por la entidad se protejan mediante mecanismos que no permitan su pérdida.
c. La Unidad de Gestión Tecnológica establece los lineamientos para el uso de la red de energía regulada en los puestos de trabajo en los cuales solo se deben conectar equipos como computadores de escritorio, portátiles y pantallas; los otros elementos deben conectarse a la red eléctrica no regulada.
d. La Unidad de Gestión Tecnológica debe proteger el cableado que transporta voz, datos y suministro de energía eléctrica contra la interceptación, interferencia o daños de cualquier tipo dentro del perímetro de la Administración Municipal.
e. La Unidad de Gestión Tecnológica debe definir mecanismos para que los cables de energía eléctrica estén separados de los cables de comunicaciones para evitar interferencia y ruido.
f. La Unidad de Gestión Tecnológica debe definir mecanismos de soporte y mantenimiento a los equipos de cómputo, servidores y equipos activos de red y debe llevar registro de estos.
g. Cuando un equipo o medio extraíble sea reasignado o retirado de servicio, La Unidad de Gestión Tecnológica debe garantizar la eliminación de toda información mediante mecanismos de borrado seguro teniendo en cuenta que previo a esta actividad debe realizarse una copia de seguridad de esta.
h. Es responsabilidad de los usuarios registrar el ingreso o salida de los equipos portátiles ya sean propios o de la entidad.
i. La Unidad de Gestión Tecnológica debe configurar como política general que todos los equipos de cómputo que se encuentren en los dominios de la Administración Municipal bloqueen automáticamente su sesión después de tres (3) minutos de inactividad.
j. Los Servidores Públicos, contratista o terceros de la Administración Municipal, durante su ausencia no deben conservar sobre el escritorio información propia de la Administración Municipal como: documentos físicos o medios de almacenamiento, por lo tanto, se requiere guardar en un lugar seguro para impedir su pérdida, daño, copia o acceso por parte terceros o personal que no tenga autorización para su uso o conocimiento.
k. Los Servidores Públicos, contratista o terceros de la Administración Municipal, deben bloquear la pantalla del computador a su cargo cuando se ausenten de su puesto de trabajo, para impedir el acceso de terceros no autorizados a la información almacenada en el equipo de cómputo.

l. Los documentos que impriman los Servidores Públicos, contratista o terceros con clasificación (Clasificada – Reservada), deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.

m. No se debe reutilizar documentos impresos con clasificación (Clasificada – Reservada), estos deben ser destruidos y no deben estar como papel reciclable.

6.6 LINEAMIENTO SEGURIDAD DE LAS OPERACIONES

6.6.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES

Lineamientos

a. La Unidad de Gestión Tecnológica con el apoyo de la Oficina de Transparencia debe documentar y mantener actualizados todos sus procedimientos operativos para garantizar la disponibilidad, integridad y confidencialidad de la información.

b. La Unidad de Gestión Tecnológica debe establecer un procedimiento que permita asegurar la gestión de cambios a nivel de infraestructura, aplicativos y servicios tecnológicos para que estos sean desarrollados bajo estándares de eficiencia, seguridad, calidad y permitan determinar las actividades y responsables en la gestión de cambios.

c. La Unidad de Gestión Tecnológica debe establecer mesas de trabajo de gestión de cambios, quien se encargará de evaluar, aprobar o negar la implementación de los cambios y este a su vez será presidido por el Gestor de Cambios.

d. La Unidad de Gestión Tecnológica debe documentar la gestión de capacidad de la plataforma tecnológica, definir su responsable y mantenerla actualizada.

e. La Unidad de Gestión Tecnológica debe velar por la capacidad de procesamiento requerida en los recursos tecnológicos de la información de la entidad, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica con una periodicidad definida.

f. La Unidad de Gestión Tecnológica debe realizar las tareas de optimización de servicios tecnológicos y sistemas de información, al igual que la verificación de capacidad de los servicios de red de la entidad.

g. La Unidad de Gestión Tecnológica debe definir y documentar las reglas para la transferencia de software del ambiente de pruebas a producción.

h. La Unidad de Gestión Tecnológica debe garantizar que todo cambio que se deba realizar en los sistemas de información en producción deba ser probados en un ambiente de pruebas

antes de aplicarlos a los sistemas en producción, de acuerdo a la metodología de desarrollo de la Entidad, salvo que sean cambios de emergencia.

i. La Unidad de Gestión Tecnológica debe garantizar que los compiladores, editores y otras herramientas de desarrollo y utilitarios del sistema, no sean accedidos desde sistemas de producción cuando no se requieren.

6.6.2 PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS

Lineamientos

a. La Unidad de Gestión Tecnológica debe definir y documentar los controles para la detección, prevención y recuperación contra códigos maliciosos. Además, proporcionará los mecanismos para generar cultura de seguridad entre los Servidores Públicos, contratistas y terceros frente a los ataques de software malicioso.
b. La Unidad de Gestión Tecnológica debe contar con herramientas tales como antivirus, antimalware, antispam y antispyware que reduzcan el riesgo de contagio de software malicioso.
c. La Unidad de Gestión Tecnológica debe asegurar que el software de antivirus, antimalware, antispyware y antispam cuente con las licencias de uso requeridas, certificando su autenticidad y la posibilidad de actualización periódica de las últimas bases de datos de firmas del proveedor de servicios.
d. La Unidad de Gestión Tecnológica debe velar por que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.
e. La Unidad de Gestión Tecnológica, debe asegurar que no se pueda realizar cambios en la configuración del software de antivirus, antispyware, antispam y antimalware.
f. La Unidad de Gestión Tecnológica debe velar que el software de antivirus, antispyware, antispam y antimalware posea las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.
g. Los Servidores Públicos, contratista o terceros de la Administración Municipal, deben abstenerse de abrir o ejecutar archivos y/o documentos de fuentes desconocidas, especialmente los que se encuentran en medios de almacenamiento externo o que provienen de correos electrónicos desconocidos.

h. Los Servidores Públicos, contratista o terceros de la Administración Municipal no deben descargar archivos de internet de fuentes desconocidas, en caso de requerirlo, debe generar la solicitud a La Unidad de Gestión Tecnológica a través de la Mesa de Ayuda Unidad de Gestión Tecnológica.
i. Los Servidores Públicos, contratista o terceros de la Administración Municipal que sospechen o detecten alguna infección por software malicioso deben notificar de inmediato a La Unidad de Gestión Tecnológica a través de la Mesa de Ayuda Unidad de Gestión Tecnológica, con el fin de ejercer los controles correspondientes.

6.6.3 COPIAS DE RESPALDO

Lineamientos

a. La Unidad de Gestión Tecnológica debe definir y documentar un plan o procedimiento de copias de respaldo y restauración de la información de la Administración Municipal, donde se establezca el esquema, de qué, cómo, quién, con qué periodicidad, tipo de respaldo y nivel de criticidad.
b. La Unidad de Gestión Tecnológica, velará por que los medios magnéticos que contienen la información sean almacenados en una ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguarden las copias de respaldo debe contar con la seguridad física y medioambientales apropiados.
c. La Unidad de Gestión Tecnológica debe disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.
d. La Unidad de Gestión Tecnológica debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.
e. Gestión Documental debe definir las condiciones de transporte, transmisión o custodia de las copias de respaldo de la información que son almacenadas externamente.
f. La Unidad de Gestión Tecnológica debe proporcionar los lineamientos para la definición de las estrategias de generación, retención y rotación de las copias de respaldo de los activos de información de la entidad.

g. La Unidad de Gestión Tecnológica debe velar por que el software de respaldo esté instalado en las estaciones de trabajo y servidores para los cuales sea necesario la realización de Backup. Se debe contar con las licencias necesarias para garantizar continuidad en el proceso.
h. Es responsabilidad de los procesos dueños de las aplicaciones, definir la frecuencia de la generación de copias de respaldo adicionales a las definidas por La Unidad de Gestión Tecnológica
i. Es responsabilidad de los Servidores Públicos, contratistas y terceros de la Administración Municipal, guardar la información crítica de sus funciones en unidades de almacenamiento destinadas para tal fin, garantizando su respaldo.
j. Es responsabilidad de los Servidores Públicos, contratistas y terceros de la Administración Municipal, guardar la información para el desarrollo de sus funciones, en la carpeta “Institucionales” en sus estaciones de trabajo. La información que no se aloje en esta carpeta no se respaldará y cualquier pérdida de esta será responsabilidad del usuario.
k. Los Servidores Públicos, contratistas y terceros de la Administración Municipal son responsables de hacer buen uso de los servicios tecnológicos de la Administración Municipal y en ningún momento pueden ser usados para beneficio propio o para realizar prácticas ilícitas o mal intencionadas que atenten contra otros Servidores Públicos, contratistas y terceros,
l. Por ningún motivo se permite alojar en servidores información catalogada como personal, música, videos, etc.
m. La Unidad de Gestión Tecnológica garantizará el respaldo de los archivos con extensión .pdf .doc, .docm, .docx, .dot, .dotm .xls, .xlsm, .xlsx, .xlt, .xltm, .xltx, .bmp, .gif, .jpg, .odp, .png, .pot, .potm, .potx, .pps, .ppt, .pptm, .jpeg. , que sea requerido por los usuarios cuando se consideren de alta prioridad.

6.6.4 REGISTRO DE EVENTOS Y SEGUIMIENTO

Lineamientos

a. La Unidad de Gestión Tecnológica debe generar registros de auditoría que contengan excepciones o eventos relacionados a la seguridad en los sistemas de información que se consideren.

b. La Unidad de Gestión Tecnológica debe salvaguardar los registros de auditoría que se generen de cada sistema.
c. La Unidad de Gestión Tecnológica debe monitorear excepciones o los eventos de la seguridad de información.
d. La Unidad de Gestión Tecnológica debe monitorear la infraestructura tecnológica para verificar que los usuarios sólo la usen para actividades propias de su labor y la Misión de la Administración Municipal.
e. La Unidad de Gestión Tecnológica, debe garantizar que todos los sistemas de procesamiento de información, los equipos y demás servicios tecnológicos que lo ameriten se sincronicen con una única fuente de referencia de tiempo, con el fin de garantizar la exactitud de los registros de auditoría.

6.6.5 CONTROL DE SOFTWARE OPERACIONAL

Lineamientos

a. La Unidad de Gestión Tecnológica designará responsables y establecerá instructivos y guías para controlar la instalación de software operativo, se cerciorará de contar con el soporte de los proveedores de dicho software y asegurará la funcionalidad de los sistemas de información que operan sobre la plataforma tecnológica cuando el software operativo sea actualizado.
b. La Unidad de Gestión Tecnológica debe establecer responsabilidades y procedimientos para controlar la instalación del software operativo.
c. La Unidad de Gestión Tecnológica debe conceder accesos temporales y controlados a los fabricantes y terceros autorizados para realizar actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones.
d. La Unidad de Gestión Tecnológica debe establecer las restricciones y limitaciones para la instalación del software operativo en los equipos de cómputo de la Administración Municipal.
e. La Unidad de Gestión Tecnológica debe generar un plan de actualizaciones para el software, aplicaciones y librerías de programas que deberán llevar a cabo los administradores, bajo la autorización de la dirección de la Oficina.
f. La Unidad de Gestión Tecnológica debe manejar un sistema de control de configuración para mantener el control de todo el software implementado, al igual que se debe mantener la documentación del sistema.

6.6.6 GESTIÓN DE VULNERABILIDADES TÉCNICAS

Lineamientos

a. La Unidad de Gestión Tecnológica debe realizar mínimo una vez al año una revisión de vulnerabilidades técnicas a los sistemas de información críticos y misionales por medio de ethical hacking y/o pruebas de penetración.
b. La Unidad de Gestión Tecnológica debe documentar, informar, gestionar y corregir las vulnerabilidades encontradas, adoptando acciones correctivas para mitigar los hallazgos, minimizar el nivel de riesgo y reducir el impacto.
c. La Unidad de Gestión Tecnológica debe restringir a los usuarios finales la instalación de software en los equipos de la Administración Municipal.
d. La Unidad de Gestión Tecnológica debe establecer y monitorear que la infraestructura tecnológica sea usada exclusivamente para el desempeño laboral, o para el desarrollo de las funciones, actividades y obligaciones acordadas o contratadas.
e. La Unidad de Gestión Tecnológica debe controlar la instalación y uso de máquinas virtuales y sólo podrá realizarse siempre y cuando sea una necesidad para el uso de las funciones o labor contratada.
f. La Unidad de Gestión Tecnológica debe realizar de manera periódica una inspección del software instalado en los equipos de la Administración Municipal y debe desinstalar el software no autorizado.
g. La Unidad de Gestión Tecnológica a través de la Mesa de Ayuda Unidad de Gestión Tecnológica es la responsable de instalar, configurar y dar soporte a los equipos de la Administración Municipal.
h. Sólo está permitido el uso de software licenciado por la Administración Municipal y/o aquel que sin requerir licencia de uso comercial sea expresamente autorizado.

6.6.7 CONSIDERACIONES SOBRE AUDITORIAS DE SISTEMAS DE INFORMACIÓN

Lineamientos

a. La Unidad de Gestión Tecnológica debe planificar periódicamente actividades que involucren auditorias de los sistemas críticos en producción.

b. La Unidad de Gestión Tecnológica debe documentar los resultados de las auditorias de los sistemas de Información De la Administración Municipal.

6.7 LINEAMIENTO SEGURIDAD DE LAS COMUNICACIONES

6.7.1 GESTIÓN DE SEGURIDAD DE LAS REDES

Lineamientos

a. La Unidad de Gestión Tecnológica debe disponer de controles para realizar transferencias completas, sin alteraciones y visualizaciones no autorizadas de la información entre las aplicaciones de la Administración Municipal.
b. La Unidad de Gestión Tecnológica debe proporcionar recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación del servicio de internet.
c. La Unidad de Gestión Tecnológica debe monitorear continuamente el canal o canales que prestan el servicio de internet, con el fin de prevenir y atender cualquier incidente que se presente tan pronto como sea posible.
d. La Unidad de Gestión Tecnológica debe generar registros de navegación y los accesos de los usuarios a Internet, así como establecer e implementar procedimientos de monitoreo sobre la utilización del servicio de internet.
e. La Unidad de Gestión Tecnológica debe implementar controles que eviten el ingreso a páginas con código malicioso incorporado o sitios catalogados como peligrosos.
f. La Unidad de Gestión Tecnológica debe proporcionar una plataforma Tecnológica que soporte los sistemas de información, esta debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a internet. La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad.
g. La Unidad de Gestión Tecnológica debe realizar segmentación de Redes para Servidores Públicos, Contratistas y visitantes de la Administración Municipal.
h. La Unidad de Gestión Tecnológica debe establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.

i. La Unidad de Gestión Tecnológica debe 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.
j. La Unidad de Gestión Tecnológica debe instalar protección entre las redes internas y cualquier red externa, que este fuera de la capacidad de control y administración de la Entidad.
k. La Unidad de Gestión Tecnológica debe permitir el acceso a redes inalámbricas mediante un portal de acceso en donde permita al usuario ingresar un usuario y contraseña.
l. La Unidad de Gestión Tecnológica debe realizar de manera periódica el cambio de las claves de acceso a la red WIFI de la Administración Municipal.

6.7.2 TRANSFERENCIA DE INFORMACIÓN

Lineamientos

a. Cada dependencia será responsable del intercambio de información con los diferentes terceros que, hacen parte de la operación de la Administración Municipal, por lo que deberán establecer mecanismos donde se contemple la recepción o envío de la información, utilización de medios de transmisión confiables y la adopción de controles, con el fin de proteger la confidencialidad e integridad de esta.
b. La Unidad de Gestión Tecnológica, debe ofrecer servicios o herramientas de intercambio de información seguros, así como adoptar controles como el cifrado de información, que permitan el cumplimiento del procedimiento para el intercambio de información (digital o medio magnético), con el fin de proteger dicha información contra divulgación o modificaciones no autorizadas.
c. El grupo interno de trabajo de apoyo, logística y documental debe dictar directrices sobre retención, disposición y transferencia de la información física de la Administración Municipal, de acuerdo con la normatividad vigente.
d. La Unidad de Gestión Tecnológica debe establecer controles para proteger la información que se transmite como documentos adjuntos a través del correo electrónico de la Administración Municipal.
e. Los mensajes y la información contenida en los buzones de correo son propiedad de la Administración Municipal y cada responsable, el cual debe mantener únicamente los mensajes relacionados con el desarrollo de sus actividades.

f. El único servicio de correo electrónico controlado por la Alcaldía de Manizales es el asignado directamente por la Unidad de Gestión Tecnológica, el cual cumple con todos los requerimientos técnicos y de seguridad para evitar ataques informáticos, virus, spyware y otro tipo de software o código malicioso.
g. Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por la Administración Municipal y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.
h. Los usuarios de correo electrónico tienen prohibido el envío de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los servidores públicos de la entidad y el personal provisto por terceras partes.
i. Está prohibido el envío de o intercambio de mensajes con contenido que atente contra la integridad de las personas o instituciones, tales como: ofensivo, obsceno, pornográfico, chistes, información terrorista, cadenas de cualquier tipo, racista, o cualquier contenido que atente con la integridad de las personas.
j. Es responsabilidad del usuario etiquetar el mensaje de correo electrónico de acuerdo con los niveles de clasificación teniendo en cuenta el tipo de información que se pretende compartir.
k. Es responsabilidad del usuario reportar un correo electrónico cuando crea que es de dudosa procedencia a La Unidad de Gestión Tecnológica, con el fin de que el administrador tome las medidas necesarias para evitar su propagación dentro de la entidad.
l. Es responsabilidad de cada usuario asegurar los destinatarios a los cuales va dirigida una comunicación, si estas son listas de distribución, también debe revisarlas con el fin de evitar compartir información a personas no autorizadas.
m. El servicio de correo electrónico debe ser usado de manera ética, razonable, eficiente, responsable, no abusiva y sin generar riesgos para la operación de equipos, sistemas de información e imagen de la Entidad.
n. No es permitido el envío o recepción de archivos que contengan extensiones ejecutables, en ninguna circunstancia.
o. Es obligación del usuario realizar la activación de las repuestas automáticas en el servicio de correo de la Entidad, cuando su ausencia sea mayor a tres (3) días, igualmente, esta deberá

indicar quién es la persona asignada para cubrir su ausencia. Nota: La persona encargada de cubrir la ausencia debe estar autorizada por parte del jefe inmediato o supervisor del contrato.

p. La Unidad de Gestión Tecnológica define las pautas generales para asegurar un adecuado uso de la Suite de correo (correo electrónico, grupos, servicio de nube, calendario, sitios y formularios) por parte de los usuarios.
q. Está prohibida la divulgación no autorizada de información de propiedad de la Administración Municipal a través de la plataforma de correo.
r. Está prohibido la creación, almacenamiento o intercambio de mensajes que atenten contra las leyes de derechos de autor.
s. Se deben establecer acuerdos de confidencialidad o de no divulgación de Información.
t. Para el personal externo que ejecute tareas propias de la Administración Municipal y haya sido contratado en el marco de un contrato o convenio con la Administración Municipal, debe firmar un acuerdo de confidencialidad y no divulgación de la información firmado entre el Supervisor del Contrato y el Representante Legal, y este debe reposar en la carpeta de ejecución del contrato.

6.7.3 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Lineamientos

a. Las diferentes dependencias de la Administración que vayan a adquirir servicios de desarrollo de software o arrendamiento, deberán solicitar la autorización al grupo interdisciplinario de compras tecnológicas.
b. En aras de garantizar que lo aprobado en el grupo interdisciplinario de compras tecnológicas cumpla con los requisitos objeto del contrato, el supervisor del contrato deberá socializar el informe final con la Unidad de Gestión Tecnológica, quien los apoyará en la verificación de los entregables.
c. Las áreas técnicas propietarias de sistemas de información en conjunto con La Unidad de Gestión Tecnológica incluirán requisitos de desarrollo seguro en la definición de requerimientos y, posteriormente se asegurarán de que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido.

d. La Unidad de Gestión Tecnológica debe establecer metodologías para el desarrollo de software seguro, que incluyan la definición de requerimientos de seguridad y las buenas prácticas, con el fin de proporcionar a los desarrolladores una visión clara de lo que se espera.
e. Las áreas técnicas responsables de la administración de los sistemas de información en acompañamiento con La Unidad de Gestión Tecnológica deben establecer las especificaciones de adquisición o desarrollo de sistemas de información considerando siempre los requerimientos de Seguridad de la Información.
f. El área técnica responsable de la administración de los sistemas de información puede definir qué perfiles deben contener los sistemas de información a desarrollar, igualmente, deben aprobar la asignación de estos perfiles cuando sea necesario.
g. La Unidad de Gestión Tecnológica debe liderar la definición de requerimientos de seguridad de los sistemas de información, teniendo en cuenta aspectos como la estandarización de herramientas de desarrollo, controles de autenticación, la arquitectura de aplicaciones, entre otros. Igualmente, el área técnica debe definir los controles de acceso
h. La Unidad de Gestión Tecnológica debe asegurar que cada vez que se pretenda implementar un sistema de información ya sea propio o de terceros, este sea sometido a un análisis de vulnerabilidades supervisadas las cuales deberán ser remediadas antes del despliegue en producción por las áreas encargadas.
i. La Unidad de Gestión Tecnológica debe establecer mecanismos que permitan deshabilitar las funcionalidades de autocompletar en formularios de solicitud que requieran información sensible.
j. La Unidad de Gestión Tecnológica debe asegurar que no se permitan conexiones recurrentes con el mismo usuario a los sistemas de información construidos, garantizando la seguridad de las conexiones a los sistemas de información mediante mecanismos que aseguren una única autenticación.
k. La Unidad de Gestión Tecnológica debe exigir la documentación relacionada con el código fuente para los desarrollos propios.

6.7.4 SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y DE SOPORTE

Lineamientos

a. La Unidad de Gestión Tecnológica debe velar por que el desarrollo interno o externo de los sistemas de información cumpla con las buenas prácticas para el desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado.
b. La Unidad de Gestión Tecnológica debe establecer y mantener ambientes separados de Desarrollo/Pruebas y Producción, dentro de la infraestructura de la Administración Municipal.
    - El ambiente de desarrollo/pruebas se debe utilizar para propósitos de implementación, modificación, ajuste y/o revisión de código fuente; además se debe utilizar para realizar el conjunto de validaciones funcionales y técnicas del software, aplicación o sistema de información, teniendo como base los criterios de aceptación y los requerimientos de desarrollo.
    - El ambiente de producción debe utilizarse para la prestación de un servicio que involucra el manejo de datos reales y que tiene un impacto directo sobre las actividades realizadas como parte de un proceso de la Administración Municipal.
c. Los administradores de los sistemas de información (Líder Funcional) con el apoyo de La Unidad de Gestión Tecnológica son responsables de asegurar que la calidad de los entregables cumpla con los requerimientos de seguridad y establecidos, antes del paso a producción de los sistemas utilizando metodologías para este fin, documentando las pruebas realizadas y aprobando los pasos a producción.
d. La Unidad de Gestión Tecnológica debe incluir dentro del procedimiento los controles de gestión de cambios el manejo de los cambios en el software, aplicativos y sistemas de información de la Administración Municipal.
e. Los desarrolladores internos y externos de los sistemas de información deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de estos, pasando desde el diseño hasta la puesta en marcha.
f. Los desarrolladores internos y externos deben proporcionar un nivel adecuado de soporte para solucionar los problemas en los sistemas de información de la Entidad; de acuerdo a los niveles de servicio acordados entre las partes.
g. Los desarrolladores internos y externos deben construir los sistemas de información de tal manera que efectúen las validaciones de datos de entrada y la generación de datos de salida de manera confiable, utilizando rutinas de validación centralizada y estandarizadas.

h. Los desarrolladores internos y externos deben asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.
i. Los desarrolladores internos y externos deben suministrar opciones de desconexión o cierre de sesión de los sistemas de información (Logout) que permitan terminar completamente con la sesión o conexión asociada.
j. Los desarrolladores internos y externos deben asegurar el manejo de operaciones sensibles o críticas de los aplicativos desarrollados permitiendo el uso de dispositivos adicionales como tokens o el ingreso de parámetros adicionales de verificación.
k. Los desarrolladores internos y externos deben asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.
l. Los desarrolladores internos y externos deben garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.
m. Los desarrolladores internos y externos deben remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.
n. Los desarrolladores internos y externos deben prevenir la revelación estricta de directorios de los sistemas de información construidos.
o. Los desarrolladores internos y externos deben remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.
p. Los desarrolladores internos y externos deben evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas independientes, los cuales se recomienda que estén cifrados.
q. Los desarrolladores internos y externos deben certificar el cierre de la conexión con las bases de datos desde los aplicativos tan pronto como estas sean requeridas.
r. Los desarrolladores deben implementar controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los

archivos transferidos en el repositorio destinado para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos solo tengan privilegios de lectura.

s. Ni los desarrolladores ni terceros deben realizar pruebas, instalaciones o desarrollos de software, directamente sobre el entorno de producción. Esto puede conducir a fraude o inserción de código malicioso.
t. Los desarrolladores deben proteger el código fuente de los aplicativos construidos, de tal forma que no pueda ser descargado ni modificado por usuarios no autorizados.
u. Los desarrolladores deben asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.
v. La Unidad de Gestión Tecnológica en conjunto con los desarrolladores, debe crear e implementar una guía de desarrollo seguro usando metodologías de desarrollo seguro.
w. Todo desarrollo realizado por el equipo de La Unidad de Gestión Tecnológica o terceros debe estar alineado con los lineamientos de desarrollo seguro para Sistemas Información

6.7.5 PROTEGER LOS DATOS USADOS PARA PRUEBAS.

Lineamientos:

a. La Unidad de Gestión Tecnológica protegerá los datos de prueba que se entregarán a los desarrolladores, asegurando que no revelen información confidencial de los ambientes de producción.
b. La Unidad de Gestión Tecnológica debe certificar que la información a ser entregada a los desarrolladores para sus pruebas será enmascarada y no revelará información confidencial de los ambientes de producción.
c. La Unidad de Gestión Tecnológica debe eliminar la información de los ambientes de pruebas una vez estas hayan concluido.
d. Cada vez que se realicen copias de información de producción se debe contar con un registro que permita realizar auditoria.

6.8 LINEAMIENTO SEGURIDAD DE RELACIÓN CON PROVEEDORES

Lineamientos

a. Gestión Contractual debe establecer lineamientos para el cumplimiento de las obligaciones contractuales de la dimensión de Seguridad y Privacidad de la Información con terceros o proveedores.
b. Gestión Contractual debe establecer en el momento de suscribirse contratos de cualquier tipo los riesgos asociados a la seguridad y privacidad de la información, los compromisos establecidos de confidencialidad de la información y el cumplimiento de las políticas de seguridad de la información de la Administración Municipal.
c. Gestión Contractual debe establecer en los contratos con terceros y proveedores los requisitos legales y regulatorios relacionados con la protección de datos personales, los derechos de propiedad intelectual y derechos de autor.
d. La Unidad de Gestión Tecnológica debe documentar, establecer controles y permisos cuando un tercero o proveedor requiera tener accesos a la información por medio de la infraestructura tecnológica de la Administración Municipal.
e. La Unidad de Gestión Tecnológica debe verificar mensualmente el cumplimiento de Acuerdos de Nivel de Servicio establecidos con sus proveedores de tecnología.
f. La Unidad de Gestión Tecnológica debe establecer un procedimiento que permita asegurar la gestión de cambios a nivel de infraestructura, aplicativos y servicios tecnológicos que son soportados por terceros y/o proveedores, para garantizar estándares de eficiencia, seguridad, calidad y que permitan determinar los responsables y tareas a seguir para garantizar el éxito en la gestión de cambios.
g. Gestión Contractual debe incluir en las guías de contratación y supervisión obligaciones generales sobre seguridad y privacidad de la información y los formatos para su cumplimiento y verificación por parte del supervisor de contrato.

6.9 LINEAMIENTO GESTIÓN DE INCIDENTES DE SEGURIDAD

Lineamientos

a. La Unidad de Gestión Tecnológica en conjunto con el responsable de Seguridad de la Información debe definir un procedimiento para la gestión de incidentes de seguridad de la información.
b. La Unidad de Gestión Tecnológica debe definir los canales para que los Servidores Públicos, contratistas y terceros de la Administración Municipal puedan reportar los incidentes de Seguridad de la Información.

c. La Unidad de Gestión Tecnológica es la encargada de la evaluación de eventos de seguridad de la información y la decisión tomada sobre los mismos.
d. La Oficina de Tecnologías de la Información es la encargada para la recolección de evidencias de los incidentes de seguridad de la información.
e. La Unidad de Gestión Tecnológica debe contar con los mecanismos para el cumplimiento de los tiempos en la respuesta de incidentes establecido en los lineamientos para la Gestión de Incidentes.
f. La Unidad de Gestión Tecnológica deberá dar a conocer a los Servidores Públicos, contratistas y terceros de la Administración Municipal los lineamientos establecidos para la Gestión de Incidentes de Seguridad de la Información.
g. La Unidad de Gestión Tecnológica debe velar por que la recolección de evidencia tenga en cuenta la cadena de custodia, la seguridad del personal, los roles y responsabilidades del personal involucrado, la competencia del personal, y la documentación.

6.10 LINEAMIENTO GESTIÓN CONTINUIDAD DEL NEGOCIO

6.10.1 CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN

Lineamientos

a. Establecer un análisis de impacto al negocio (BIA por sus siglas en ingles), por medio del cual se identifiquen los servicios críticos de la Administración Municipal.
b. Diseñar las estrategias y tiempos de recuperación de la operación de los servicios críticos de la Administración Municipal.
c. La Unidad de Gestión Tecnológica debe disponer de planes de contingencia de los servicios Tecnológicos de Información y un plan de recuperación ante desastres, enfocados a lograr el retorno a la operación normal.

6.14 LINEAMIENTO DE CUMPLIMIENTO

6.14.1 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES

Lineamientos

La Alcaldía de Manizales gestiona la seguridad y privacidad de la información dando cumplimiento adecuado a la legislación vigente. Analizando los requisitos legales aplicables a la

información de derechos de autor y propiedad intelectual, protección de datos personales, ley de transparencia y del derecho de acceso a la información pública nacional. Igualmente, velará por la protección de los registros ante cualquier pérdida, destrucción, falsificación acceso o liberación no autorizada de acuerdo con los requisitos legislativos, de reglamentación y contractuales de la Administración Municipal.

6.14.2 REVISIONES DE SEGURIDAD DE LA INFORMACIÓN

Lineamientos

a. La Oficina de Control Interno, debe realizar de manera periódica auditorías internas para comprobar el correcto funcionamiento del Sistema de Gestión de Seguridad de la Información en cuanto a los objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información.
b. Los líderes de los procesos deben asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad se realicen correctamente, con el fin de cumplir las políticas y normas de seguridad; en caso de incumplimiento se evaluarán y propondrán acciones correctivas
c. La Unidad de Gestión Tecnológica debe realizar revisiones mínimo una vez al año del cumplimiento de las políticas de Seguridad y Privacidad de la Información.
d. Es un deber de los servidores públicos contratistas y terceros de la Administración Municipal, conocer esta Política y realizar todos los actos conducentes para su cumplimiento, implementación y mantenimiento.

Responsables: Secretaria de Servicios Administrativos, Unidad Tecnológica.