MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - MSPI

1. INTRODUCCIÓN

La información es uno de los activos más importantes de toda entidad, por lo tanto, debe estar protegida en todo momento, independientemente de la manera en que se produzca, manipule, divulgue o se almacene.

La preservación de la confidencialidad, integridad y disponibilidad de la información para la Administración Municipal de Caldas Antioquia, constituye una prioridad y por tanto, es responsabilidad de todos velar por que no se realicen actividades que contradigan la esencia y el espíritu de cada una de estas políticas.

Las políticas de seguridad de la información incluidas en este manual constituyen una parte fundamental del Modelo de Seguridad y Privacidad de la Información (MSPI) de Gobierno en Línea (GEL) y se convierten en la base para la implantación de los controles, procedimientos y estándares definidos.

El Desarrollo del manual está basado en el Modelo de Seguridad de y Privacidad de la Información expuesto por el Ministerio de la Tecnologías de la Información y las Comunicaciones, el cual recopila las mejores prácticas para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo; lo anterior teniendo en cuenta las necesidades y objetivos, los requisitos de seguridad, los procesos misionales y el tamaño y estructura de la Administración Municipal de Caldas, Antioquia.

De esta forma estamos dando cumplimiento al decreto único reglamentario 1078 de 2015 en el componente de seguridad y privacidad de la Información como parte integral de la estrategia GEL.

El modelo a seguir está basado en las Normas técnicas NTC ISO/IEC 27000 y las ISO/ICONTEC, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otros. Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

Las políticas incluidas en este manual se convierten en la base para implementar controles en la Información misional de LA ADMINISTRACIÓN MUNICIPAL DE CALDAS, ANTIOQUIA.

2. OBJETIVO

Establecer las políticas de seguridad de la información para la Administración Municipal de Caldas Antioquia, con el fin de cumplir con los requisitos de seguridad, definidos en el MSPI, de GEL, que ayudarán, mediante su implementación, a preservar la Confidencialidad, Integridad y Disponibilidad de la información. De acuerdo a los lineamientos de buenas prácticas en Seguridad y Privacidad para las entidades del Estado, con el fin de regular la gestión de la seguridad de la información al interior de la entidad

3. ALCANCE

La política de seguridad de la información será aplicada a los procesos estratégicos, misionales, de apoyo y de seguimiento y control de la Administración Municipal, y deberá

ser conocida y cumplida por todos los funcionarios, contratistas, proveedores, ciudadanía en general y demás partes interesadas, que accedan a los sistemas de información e instalaciones físicas.

4. TÉRMINOS Y DEFINICIONES

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Activo de Información: cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la Administración Municipal y, en consecuencia, debe ser protegido. Se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Amenaza: es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática, los elementos de información. Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de riesgos de seguridad de la información: proceso sistemático de identificación de fuentes, estimación de impactos, probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

Autenticación: es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Confidencialidad: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datos Abiertos: Son todos 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 (Ley 1712 de 2014, art 6)

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales 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, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Disponibilidad: es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3).

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Integridad: es la protección de la exactitud y estado completo de los activos de información.

Ley de Habeas Data: Se refiere a la Ley Estatutaria 1266 de 2008.

Ley de Transparencia y Acceso a la Información Pública: Se refiere a la Ley Estatutaria 1712 de 2014.

Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

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

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Privacidad: En el contexto de este documento, por privacidad se entiende 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 GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Propietarios de los activos de información: son los responsables de cada uno de los activos de información (archivos, bases de datos, contratos y acuerdos, documentación del sistema, manuales de usuario, material de formación, aplicaciones, software del sistema, equipos informáticos, equipos de comunicaciones, servicios informáticos y de comunicaciones, las personas, etc. Esta persona se hará cargo de mantener la seguridad del activo.

Recursos tecnológicos: son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo.

Registro Nacional de Bases de Datos: Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

Responsabilidad Demostrada: Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Responsable del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Sistema de información (SI): es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo. Dichos elementos pueden ser personas, actividades o técnicas de trabajo, datos y recursos materiales en general.

Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

5. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la Administración Municipal de Caldas, Antioquia con respecto a la protección de la confidencialidad, integridad y disponibilidad de los activos de información que aportan valor para convertir al municipio de Caldas en un escenario de transformación para la paz y el progreso, con una perspectiva de derechos, incluyente, transparente y responsable con el medio ambiente y las necesidades de su comunidad, en condiciones de equidad y solidaridad. Esto se realiza a través de la implementación, mantenimiento y mejora del Modelo de Seguridad y Privacidad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

La Administración Municipal de Caldas Antioquia, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Gestionar el riesgo de seguridad de la información los procesos de la entidad.

- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

- Fortalecer la concientización de la seguridad de la información en los funcionarios, terceros, aprendices, practicantes y ciudadanía en general.

6. NIVEL DE CUMPLIMIENTO

Todas las personas cubiertas por el alcance deberán dar cumplimiento de un 100% de la política.

7. SANCIONES

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno Nacional y Territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

8. COMPROMISO DE LA DIRECCIÓN

La Alta Dirección de ADMINISTRACIÓN MUNICIPAL DE CALDAS, ANTIOQUIA aprueba esta Política de Seguridad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la entidad, teniendo en cuenta el marco general del funcionamiento de la entidad, sus objetivos institucionales y sus procesos misionales.

La Alta Dirección demuestra su compromiso de apoyo a través de:

- La revisión y aprobación del Manual de Políticas de Seguridad de la Información para la Institución.
- La destinación de los recursos suficientes para desarrollar los programas de capacitación y sensibilización en seguridad de la información.
- La promoción activa de una cultura de seguridad de la información en los funcionarios, contratistas, proveedores y partes interesadas, que tengan acceso a los sistemas de información e instalaciones físicas.
- Facilitar la divulgación de este manual a todas las partes interesadas.
- El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad de la información, contenidas en el manual.
- La verificación del cumplimiento de las políticas aquí mencionadas.

9. NORMATIVIDAD

El manual de políticas de seguridad de la Información se ciñe a la normatividad legal vigente colombiana y de las Buenas Prácticas establecidas por la ISO 27000.

Año Emisión	Emisor	Norma	Asunto
2015	Presidencia de la República	Decreto 1078 del 26 de mayo de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
2006	ICONTEC	Norma Técnica Colombiana NTC-ISO/IEC 27001	Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos
2013	Organización Internacional de Normalización y la Comisión	ISO/IEC 27002:2013	Mejores prácticas en la gestión de la seguridad de la información

Año Emisión	Emisor	Norma	Asunto
	Electrotécnica Internacional.		
2007	IT Governance Institute	Marco de Trabajo COBIT 4.1	Estándares internacionales para la dirección y control de la tecnología de la información
2016	Ministerio de Tecnologías de la Información y las Comunicaciones	Modelo Guía	Modelo de Seguridad y Privacidad de la Información
2016	Ministerio de Tecnologías de la Información y las Comunicaciones	Guía No. 2	Elaboración de la política general de seguridad y privacidad de la Información
2016	Ministerio de Tecnologías de la Información y las Comunicaciones	Guía No. 3	Procedimientos De Seguridad De La Información
2016	Ministerio de Tecnologías de la Información y las Comunicaciones	Guía No. 8	Controles de Seguridad y Privacidad de la Información

Agradecimientos:

Al Ministerio de las Tecnologías de la Información y las Comunicaciones por la publicación de las guías (http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html) para construir el Sistema de Gestión de Seguridad de la Información (SGSI) para las entidades del Estado.

Al Instituto Colombiano de Crédito y Estudios Técnicos en el Exterior por su publicación del Manual de Políticas de Seguridad de la Información (https://www.icetex.gov.co/dnnpro5/en-us/elicetex/manualesdelaentidad.aspx) que sirvió como referente para el diseño del manual de seguridad de la Información de la Administración Municipal de Caldas, Antioquia.

MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - MSPI

Procedimientos de Seguridad y Privacidad de la Información

Política de Seguridad del Recurso Humano

En este dominio relacionado con el personal que labora dentro de la entidad, se pueden definir los siguientes procedimientos:

Capacitación y Sensibilización del Personal

- La Alta Dirección debe establecer una metodología para realizar la capacitación y sensibilización del personal en temas de seguridad de la información teniendo en cuenta los diferentes roles y responsabilidades, la periodicidad de dichas capacitaciones y sensibilizaciones, etc.

- La Alta Dirección, en cabeza de la Secretaría de Servicios Administrativos, debe proporcionar a todos los funcionarios un adecuado nivel de concienciación, educación y capacitación en procedimientos de seguridad y en el uso correcto de los medios disponibles para el procesamiento de la información con objeto de minimizar los posibles riesgos de seguridad.

- La Alta Dirección debe requerir a los funcionarios, contratistas y usuarios de terceras partes aplicar la seguridad en concordancia con las políticas y los procedimientos.

- Todos los funcionarios y contratistas de la Administración Municipal de Caldas, Antioquia deben recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.

Ingreso y desvinculación del personal:

La Alta Dirección debe gestionar de manera segura el ingreso y desvinculación, incluyendo temas como verificación de antecedentes, firma de acuerdos de confidencialidad, recepción de entregables requeridos para generar paz y salvos entre otras características.

Esta gestión está en cabeza de la Secretaría de Servicios Administrativos y va de la mano de la Dirección Financiera.

La Secretaría de Servicios Administrativos debe asegurar que, en la culminación de una relación laboral o contractual por parte de los funcionarios, contratistas o terceras personas, se controla el proceso de devolución de los equipos y se eliminan completamente todos los derechos de acceso. Adicionalmente, debe informar esta novedad por correo electrónico al Área de Informática para eliminar el acceso a estos usuarios a la plataforma tecnológica de la Administración Municipal.

Se debe tener actualizado y verificado regularmente el inventario de los activos cargados a cada funcionario, con el fin de que al momento de desvinculación la devolución de los activos sea más sencilla.

Política de Gestión de Activos de Información

Este dominio está relacionado con la identificación y clasificación de activos de acuerdo a su criticidad y nivel de confidencialidad.

Identificación y clasificación de activos:

La Alta Dirección debe indicar la manera como los activos de información son identificados e inventariados por la entidad, así como también se debe especificar como son clasificados de acuerdo a su nivel de confidencialidad o criticidad, como se asignan y se devuelven los activos una vez se termina la relación laboral con la entidad.

Adicionalmente se debe explicar cómo se hace una correcta disposición de los activos cuando ya no se requieran y su transferencia hacia otros lugares de manera segura.

Algunos ejemplos de activos son:

- Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad y contingencia, información archivada, etc.

- Recursos de software: software de aplicaciones y sistemas operativos.

- Activos físicos: equipamiento informático (servidores, CPU, monitores, computadoras portátiles), equipos de comunicaciones (routers, PBX, máquinas de fax, switches de datos, etc.), medios magnéticos (discos, dispositivos móviles de almacenamiento de datos – discos externos, etc.), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado, etc.), mobiliario, etc.

- Servicios: servicios informáticos y de comunicaciones, utilitarios generales (iluminación, energía eléctrica, etc.)

Responsabilidad por los activos

Identificar los activos en la Administración Municipal y definir las responsabilidades para una protección adecuada.

- La Administración Municipal de Caldas, Antioquia es propietaria tanto de la información física como de la información generada, procesada, almacenada y transmitida con su plataforma tecnológica, y debe otorgar responsabilidad a las dependencias sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.

- La información, archivos físicos, los sistemas, los servicios y los equipos (ej. estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos, entre otros) propiedad de la Administración Municipal, son activos de la Administración Municipal y se proporcionan a los funcionarios y terceros autorizados, para cumplir con la misión de la Administración Municipal.

- Toda la información sensible de la Administración Municipal, así como los activos donde ésta se almacena y se procesa deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y los criterios que dicte la Secretaría de Planeación. Los propietarios de los activos de información deben llevar a cabo el levantamiento y la actualización permanente del inventario de activos de información al interior de sus procesos o áreas.

- Los propietarios de los activos de información se encuentran sujetos a auditorías y a revisiones de cumplimiento por parte de la Oficina de Control Interno.

- La Secretaría de Servicios Administrativos, apoyada en el Área de Informática, es la propietaria de los activos de información correspondientes a la plataforma tecnológica de la Administración Municipal y, en consecuencia, debe asegurar su apropiada operación y administración.

- El Área de Informática debe autorizar la instalación, cambio o eliminación de componentes de la plataforma tecnológica de la Administración Municipal.

- El Área de Informática debe establecer una configuración adecuada para los recursos tecnológicos, con el fin de preservar la seguridad de la información y hacer uso adecuado de ellos.

- El Área de Informática es responsable de preparar los equipos de cómputo y/o portátiles de los funcionarios y de hacer entrega de los mismos.

- El Área de Informática es responsable de recibir los equipos de cómputo y/o portátiles y generar copias de seguridad de la información de los funcionarios que se retiran o cambian de labores, cuando les es formalmente solicitado.

- El Área de Bienes, es responsable de recibir los equipos de cómputo y/o portátiles para su reasignación o disposición final.

- Los Secretarios de Despacho y Jefes de Oficina deben autorizar a sus funcionarios el uso de los recursos tecnológicos, previamente preparados por el Área de Informática.

- Todos los funcionarios de la Administración Municipal deben utilizar los recursos tecnológicos, de forma ética y en cumplimiento de las leyes y reglamentos vigentes, con el fin de evitar daños o pérdidas sobre la operación o la imagen de la Administración Municipal.

- Los recursos tecnológicos provistos a funcionarios, son proporcionados con el único fin de llevar a cabo las labores misionales; por consiguiente, no deben ser utilizados para fines personales o ajenos a ésta.

- Los funcionarios no deben utilizar sus equipos de cómputo y dispositivos móviles personales para desempeñar las actividades laborales.

- Los funcionarios no deben utilizar software no autorizado o de su propiedad en la plataforma tecnológica de la Administración Municipal.

- En el momento de retiro, los funcionarios deben realizar la entrega de su puesto de trabajo al Jefe Inmediato o quien este delegue; así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.

Clasificación de la información

El objetivo es el de asegurar que se aplica un nivel de protección adecuado a la Información.

- La Administración Municipal definirá con el apoyo de cada Secretaría y de cada dependencia, los niveles más adecuados para clasificar su información de acuerdo con su sensibilidad y generará una guía de Clasificación de la Información para que los propietarios de la misma la cataloguen y determinen los controles requeridos para su protección, además de identificar el acervo documental con que cuenta cada uno de los procesos.

- Toda la información de la Administración Municipal debe ser identificada, clasificada y documentada de acuerdo con las guías de Clasificación de la Información establecidas por la Ley de Transparencia.

- La Administración Municipal proporcionará los recursos necesarios para la aplicación de controles en busca de preservar la Confidencialidad, Integridad y Disponibilidad de la misma, con el fin de promover el uso adecuado por parte de los funcionarios.

- El Área de Informática debe efectuar la eliminación segura de la información, a través de los mecanismos necesarios en la plataforma tecnológica, ya sea cuando son dados de baja o cambian de usuario.

- El Área de Archivo debe utilizar los medios de los cuales está dotada para destruir o desechar correctamente la documentación física, con el fin de evitar la reconstrucción de la misma, acogiéndose a procedimiento establecido para tal fin.

- El Área de Archivo debe realizar la destrucción de información cuando se ha cumplido su ciclo de almacenamiento.

- La información física y digital de la ADMINISTRACIÓN MUNICIPAL debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado en las tablas de retención documental y cuando se cumpla el periodo de expiración, toda la información debe ser eliminada adecuadamente.

- Los usuarios deben verificar que cuando impriman, escaneen o saquen copias, no queden documentos confidenciales para evitar su divulgación no autorizada.

- Los funcionarios deben asegurarse que en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.

- La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.

Política de Control de Acceso

Este dominio está relacionado con el acceso a la información y a las instalaciones de procesamiento de la información.

Para impedir el acceso no autorizado a los sistemas de información se deberán implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto, es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento

Ingreso seguro a los sistemas de información

El objetivo es impedir el acceso no autorizado a la información mantenida por los sistemas y aplicaciones

- El Área de Informática debe gestionar el acceso a sus sistemas de información de manera segura, validando los datos completos para ingreso a los sistemas y restringiendo el acceso a la información a través de la red.

- El Área de Informática debe restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida.

- El Área de Informática debe definir procedimientos seguros de inicio de sesión, es decir, cuando sea requerido por la política de control de accesos se debera controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de log-on

- El Área de Informática debe realizar la gestión de contraseñas de usuario las cuales deben ser interactivos, asegurando contraseñas de calidad.

- El Área de Informática debe hacer uso de herramientas de administración de sistemas. El uso de utilidades software que sean capaces de anular o evitar controles en aplicaciones y sistemas que deban estar restringidos y estrechamente controlados.

- El Área de Informática debe asegurar que las redes inalámbricas cuenten con métodos de autenticación que evite accesos no autorizados.

- Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos de la ADMINISTRACIÓN MUNICIPAL deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

- El Área de Informática debe restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado, de acuerdo con las labores desempeñadas.

- El Área de Informática debe mantener actualizado un listado de las cuentas administrativas de los recursos de la plataforma tecnológica.

Gestión de usuarios y contraseñas

- El Área de Informática debe realizar la creación de usuarios y la asignación de contraseñas (las cuales deberán tener un nivel de seguridad aceptable, con base a una política de contraseñas seguras definida previamente), prohibiendo su reutilización posterior, permitiendo a los usuarios cambiarla regularmente. Teniendo en cuenta el rol que cada usuario requiera en los determinados sistemas, para brindar el acceso necesario.

- El Área de Informática debe definir lineamientos para la configuración de contraseñas que aplicarán sobre la plataforma tecnológica, los servicios de red y los sistemas de información; dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico y cambio de contraseña en el primer acceso, entre otros.

- El Área de Informática debe establecer un procedimiento para gestionar de altas/bajas en el registro de usuarios con el objeto de habilitar la asignación de derechos de acceso con el fin de asignar o revocar derechos de acceso para todos los sistemas y servicios, adicionalmente establecer los privilegios especiales que son de caracter restringido y controlado. Este procedimiento incluye retirar o adaptar los derechos de acceso a aquellos funcionarios, contratistas o usuarios de terceros que hacen uso de la información y a las instalaciones del procesamiento de información y que llegan a un estado de finalización del empleo, contrato o acuerdo.

- Los usuarios deben ser conscientes de sus responsabilidades en el mantenimiento de controles de acceso eficaces, en particular respecto al uso de contraseñas y seguridad en los equipos puestos a su disposición.

- La Alta Dirección debe implantar una política para mantener mesas de escritorio y monitores libres de cualquier información con objeto de reducir el riesgo de accesos no autorizados o el deterioro de documentos, medios y recursos para el tratamiento de la información.

- El Área de Informática debe definir una buena estrategia y documentar claramente las responsabilidades relativas a seguridad de la información en las descripciones o perfiles de los puestos de trabajo, las cuales deben ser sensibilizadas a través de campañas institucionales, asegurando de que se establecen las responsabilidades de seguridad y que son entendidas por el personal afectado.

- Los usuarios de la plataforma tecnológica, los servicios de red y los sistemas de información de la Administración Municipal deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a éstos.

- Los funcionarios y contratistas de la Administración Municipal no deben compartir sus cuentas de usuario y contraseñas con otros funcionarios o con personal provisto por terceras partes.

- Cada Secretario de Despacho y Jefe de Oficina, debe solicitar al Área de Informática la creación, modificación, bloqueo y eliminación de cuentas de usuario, a través del correo electrónico establecido para tal fin.

- Los Jefes de área deben solicitar al Área de Informática la definicion de perfiles de usuario para el acceso a los recursos tecnológicos de los funcionarios a su cargo.

Política seguridad física y del entorno:

Este dominio está relacionado con la prevención del acceso a áreas no autorizadas, el daño a la infraestructura, las instalaciones o de la información. Se pueden generar los siguientes procedimientos:

Control de acceso físico

La Alta Dirección debe garantizar el control de acceso seguro a las instalaciones al personal autorizado.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido.

- Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas por funcionarios del Área de Informática autorizados; no obstante, los visitantes siempre deberán estar acompañados de un funcionario de dicha dependencia durante su visita.

- El Área de Informática debe registrar el ingreso de los visitantes al centro de cómputo y a los centros de cableado que están bajo su custodia, en una bitácora ubicada en la entrada de estos lugares de forma visible.

- El Área de Informática debe descontinuar o modificar de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de un funcionario autorizado.

- El Área de Informática debe proveer las condiciones físicas necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo; deben existir implementos de control de temperatura, extinción de incendios, protección de descarga eléctrica y cámaras vigilancia. Estos sistemas se deben monitorear de manera permanente.

- El Área de Informática debe velar porque los recursos de la plataforma tecnológica de la Administración Municipal ubicados en el centro de cómputo se encuentran protegidos contra fallas o interrupciones eléctricas.

- El Área de Informática debe certificar que el centro de cómputo y los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.

- El Área de Informática 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; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.

- La Dirección Administrativa y Financiera y la Secretaría de Hacienda deben proporcionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implantados en las instalaciones de la Administración Municipal.

- La Secretaría de Servicios Administrativos, con el acompañamiento del Área de Informática, debe verificar que el cableado se encuentra protegido con el fin de disminuir las intercepciones o daños.

- Los funcionarios y contratistas deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de la Administración Municipal; en caso de pérdida del carné, deben reportarlo a la mayor brevedad posible a la Secretaría de Servicios Administrativos.

- Los funcionarios de la Administración Municipal y el personal provisto por terceras partes no deben intentar ingresar a áreas a las cuales no tengan autorización.

Protección de activos:

Se incluyen los pasos con los cuales los equipos son protegidos por la entidad. Se recomienda indicar cómo se determina la ubicación de los equipos que procesan información confidencial, cómo se aseguran dichas las instalaciones, los controles que se aplican para minimizar riesgos de desastres naturales, amenazas físicas, daños, por polvo, agua, interferencias, descargas eléctricas, etc.

- El Área de Informática debe proveer los mecanismos y estrategias necesarios para proteger la Confidencialidad, Integridad y Disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de la Administración Municipal.

- El Área de Informática debe generar estándares de configuración segura para los equipos de cómputo de los funcionarios de la Administración Municipal y configurar dichos equipos acogiendo los estándares generados.

- El Área de Informática debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los funcionarios de la Administración Municipal, ya sea cuando son dados de baja o cambian de usuario.

- El Área de Bienes debe velar porque los equipos que se encuentran sujetos a traslados físicos fuera de la Administración Municipal, posean pólizas de seguro.

- Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a los funcionarios se deben acoger las instrucciones técnicas que proporcione el Área de Informática.

- Cuando se presente una falla o problema de hardware o software en una estación de trabajo u otro recurso tecnológico propiedad de la Administración Municipal el usuario responsable debe informar al Área de Informática donde se atenderá o escalará, con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.

- La instalación, reparación o retiro de cualquier componente de hardware o software

de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos del Municipio, solo puede ser realizado por los funcionarios del Área de Informática, o personal externo autorizado por dicha dependencia.

- Los funcionarios y contratistas de la Administración Municipal deben bloquear sus estaciones de trabajo en el momento de abandonar su puesto de trabajo.

- Los funcionarios y contratistas de la Administración Municipal no deben dejar encendidas las estaciones de trabajo u otros recursos tecnológicos en horas no laborables.

- Los equipos de cómputo, bajo ninguna circunstancia, deben ser dejados desatendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados.

- Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.

- En caso de pérdida o robo de un equipo de cómputo de la Administración Municipal, se debe informar de forma inmediata al Jefe inmediato para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.

Retiro de activos

En este procedimiento debe especificarse cómo son retirados los activos de la entidad con previa autorización. Se debe indicar el flujo de las solicitudes, autorizaciones y el control que tendrá el activo fuera de la entidad, así como también los controles de seguridad que deberá incluir el equipo cuando esté por fuera.

La Secretaría de Servicios Administrativos es la única dependencia autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos de la Administración Municipal.

Procedimiento de Mantenimiento de Equipos

Este procedimiento debe especificar como se ejecutan mantenimientos preventivos o correctivos dentro de la entidad, indicando los intervalos en que estos deberán realizarse, con base a las sugerencias de los proveedores o si existen seguros atados a los equipos y los mantenimientos sean requisitos. Se debe especificar el modo en que los mantenimientos se llevarán a cabo y el personal que deberá ejecutarlo, llevando el registro apropiado.

El Área de Informática debe realizar mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica de la Administración Municipal.

El procedimiento está descrito en el formato P-RF-03 de la ISO

Gestión de Cambios

Se deben especificar aspectos como identificación y registro de cambios significativos en los aplicativos que se manejan en la Administración Municipal de manera segura, valoración de impactos, tiempos de no disponibilidad del servicio; comunicando a las áreas pertinentes.

- El Área de Informática debe tener conocimiento de todos los cambios en aplicativos, procedimientos, procesos, parámetros de sistema y servicio, con el fin de manejar de manera estándar todas las solicitudes (incluyendo mantenimiento y parches).

- El Área de Informática debe garantizar que todas las solicitudes de cambio se evalúan de manera estructurada en cuanto a impactos en el sistema operacional y su funcionalidad. Esta evaluación deberá incluir categorización y priorización de los cambios.

- El Área de Informática siempre que se implantan cambios al sistema, debe actualizar el sistema asociado y la documentación de usuario y procedimientos correspondientes y realizar la revisión para garantizar la implantación completa de los cambios.

Protección contra códigos maliciosos

La entidad debe proteger la información contra códigos maliciosos haciendo uso de hardware y/o software para tal fin, haciendo las configuraciones y actualizaciones pertinentes sobre las plataformas de detección, permitiendo el reporte y recuperación de ataques contra software malicio y recolección de información de manera regular como suscripción a listas de correo.

Se debe tener en cuenta que: ¡No sirve de mucho tener el mejor software antivirus del mercado si los empleados siguen abriendo e-mails de remitentes desconocidos o descargando ficheros de sitios no confiables!

- El Área de Informática debe proveer herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica de la Administración Municipal y los servicios que se ejecutan en la misma.

- El Área de Informática debe asegurar que el software de antivirus, antimalware, antispam y antispyware cuente con las licencias de uso requeridas, certificando así su autenticidad y la posibilidad de actualización periódica de las últimas bases de datos de firmas del proveedor del servicio.

- El Área de Informática debe certificar 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.

- El Área de Informática, a través de sus funcionarios y contratistas, debe asegurarse de que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware.

- El Área de Informática, a través de sus funcionarios y contratistas, debe certificar que el software de antivirus, antispyware, antispam, antimalware, posea las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.

- Los usuarios deben asegurar que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.

- Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar al Área de Informática para que tome las medidas de control correspondientes.

Aseguramiento de Servicios en la Red

- El Área de Informática, establecerá los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas; así mismo, velará por que se cuente con los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos. De igual manera, propenderá por el aseguramiento de las redes de datos, el control del tráfico en dichas redes y la protección de la información reservada y restringida de la Administración Municipal.

- El Área de Informática debe adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red de la Administración Municipal.

- El Área de Informática debe implantar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.

- El Área de Informática debe establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red de la plataforma tecnológica, acogiendo buenas prácticas de configuración segura.

- El Área de Informática debe velar por la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos.

- El Área de Informática debe diseñar y divulgar las directrices técnicas para la administración y uso del correo electrónico.

- La cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún funcionario bajo ninguna circunstancia debe utilizar una cuenta

de correo que no sea la suya.

- Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada usuario en apoyo al objetivo misional. El correo institucional no debe ser utilizado para actividades personales.

- No es permitido el envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.

- El Área de Informática debe proporcionar los recursos requeridos para la prestación segura del servicio de Internet de acuerdo a los perfiles de los usuarios.

- El Área de Informática debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.

- El Área de Informática debe monitorear continuamente de los canales del servicio de Internet.

- El Área de Informática debe implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.

- El Área de Informática debe realizar informes de la navegación y los accesos de los usuarios a Internet, así como establecer y monitorear el uso del servicio de Internet.

- El Área de Informática y la Oficina de Comunicaciones deben implementar campañas de sensibilización para todos los funcionarios y contratistas referente a las precauciones que deben tener en cuenta cuando utilicen el servicio de Internet, en el intercambio de información sensible por medio de correo electrónico.

- Los funcionarios y contratistas de la Administración Municipal deben adstenerse de descargar software desde Internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.

- No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.

- Está prohibido el acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Kazaa, MSN, Yahoo, Sype y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a la misión de la Administración Municipal.

- Está prohibida la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas

que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.

- Esta prohibido el intercambio no autorizado de información de propiedad de la Administración Municipal entre sus funcionarios y contratistas con terceros.

Transferencia de Información

La entidad deberá indicar como realiza la transmisión o transferencia de la información de manera segura dentro de la entidad o con entidades externas, donde se apliquen métodos para proteger la información de interceptación, copiado, modificación y/o destrucción.

Se deben tener en cuenta acuerdos de confidencialidad y no divulgación, que deberán ser actualizados y revisados constantemente, donde se incluyan condiciones sobre la información que se va a proteger, la duración del acuerdo, responsabilidades, propietarios de la información, acciones en caso de incumplimiento, entre otros.

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

- Los propietarios de los activos de información, o a quien ellos deleguen, deben verificar que el intercambio de información con terceros deje registro del tipo de información intercambiada, el emisor y receptor de la misma y la fecha de entrega/recepción.

- Los propietarios de los activos de información deben asegurar que el intercambio de información (digital) solamente se realice si se encuentra autorizada.

- La Oficina de Archivo, en cabeza de la Secretaría de Sevicios Administrativos, debe acoger el procedimiento para el intercambio, de información (medios de almacenamiento y documentos) con terceras partes y la adopción de controles a fin de proteger la información sensible contra divulgación, pérdida o modificaciones.

- La Oficina de Archivo, en cabeza de la Secretaría de Sevicios Administrativos, debe certificar que todo envío de información física a terceros (documento o medio magnético) utilice únicamente los servicios de transporte o servicios de mensajería autorizados por la Administración Municipal, y que éstos permitan ejecutar rastreo de las entregas.

- Los terceros con quienes se intercambia información de la Administración Municipal deben darle manejo adecuado a la información recibida, en cumplimiento de las condiciones contractuales establecidas para el intercambio de información.

- Los terceros con quienes se intercambia información de la Administración Municipal deben destruir de manera segura la información suministrada, una vez esta cumpla con la función para la cual fue enviada y demostrar la realización de las actividades

de destrucción.

- Los funcionarios de la Administración Municipal no deben utilizar el correo electrónico como medio para enviar o recibir información sensible de la Administración Municipal o de sus beneficiarios.

- No está permitido el intercambio de información sensible de la Administración Municipal por vía telefónica.

Política de Relaciones con los Proveedores

Este dominio está relacionado con la protección de los activos de la organización a los cuales los proveedores o terceros tienen acceso.

Tratamiento de la Seguridad en los Acuerdos con los proveedores

Se debe indicar como la entidad establece, acuerda, aprueba y divulga los requerimientos y obligaciones relacionados con la seguridad de la información, tanto con los proveedores como con la cadena de suministros que estos tengan (es decir algún intermediario). Dichos acuerdos deben tener características como: aspectos legales, descripción de la información a la que ambas partes tendrán acceso, reglas de uso aceptable e inaceptable de la información, requerimientos en gestión de incidentes, resolución de conflictos, informes periódicos por parte del proveedor, auditorías al servicio y gestión de cambios.

- El Área de Informática, la Oficina Asesora Jurídica y la Secretaría de Servicios Administrativos deben generar un modelo base para los requisitos de Seguridad de la Información, con los que deben cumplir terceras partes o proveedores de servicios; dicho modelo, debe ser divulgado a todas las áreas que adquieran o supervisen recursos y/o servicios tecnológicos.

- La Oficina Asesora Jurídica debe elaborar modelos de Acuerdos de Confidencialidad y Acuerdos de Intercambio de Información con terceras partes. De dichos acuerdos deberá derivarse una responsabilidad tanto civil como penal para la tercera parte contratada.

- El Área de Informática debe establecer las condiciones de conexión adecuada para los equipos de cómputo y dispositivos móviles de los terceros en la red de datos del Municipio.

- Los Supervisores de contratos con terceros deben divulgar las políticas, normas y procedimientos de seguridad de la información a dichos terceros, así como velar porque el acceso a la información y a los recursos de almacenamiento o procesamiento de la misma, por parte de los terceros se realice de manera segura, de acuerdo con las políticas, normas y procedimientos de seguridad de la información.

- Los Supervisores de contratos con terceros, deben administrar los cambios en el suministro de servicios por parte de los proveedores, manteniendo los niveles de cumplimiento de servicio y seguridad establecidos con ellos y monitoreando la aparición de nuevos riesgos.

Política de Adquisición y Mantenimiento de Sistemas de Información

Adquisición y Mantenimiento de Software

La entidad debe realizar la gestión de la seguridad de la información en los sistemas adquiridos a un tercero, verificando que cada uno de ellos preserve la confidencialidad, Integridad y Disponibilidad de la Información. Dicha gestión y control también debe ser especificada para los sistemas ya existentes que son actualizados o modificados en la entidad.

Control Software

La entidad deberá realizar el control de software, es decir, cómo limita el uso o instalación de software no autorizado, quiénes están autorizados para realizar la instalación de software, como se realizaría la gestión de las solicitudes de instalación de software para los usuarios, cómo se realiza el inventario de software dentro de la entidad entre otros aspectos.

- El Área de Informática debe asegurase que los sistemas de información adquiridos o desarrollados por terceros, cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.

- El Área de Informática, a través de sus funcionarios y contratistas, se debe asegurar que la plataforma tecnológica esté actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.líticas de Gestión de incidentes de Seguridad de la Información

Gestión de incidentes de Seguridad de la Información

Deben especificarse los roles, las responsabilidades y acciones requeridas para identificar, contener, documentar, recolectar evidencias y mejorar la respuesta ante un incidente de seguridad de la información.

La Alta Dirección o a quien delegue, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas.

- Los propietarios de los activos de información deben informar a la Oficina de Control Interno, los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización.

- La Oficina Control Interno debe establecer responsabilidades y procedimientos para

asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.

- El Área de Informática debe crear bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento.

- Es responsabilidad de los funcionarios de la Administración Municipal y del personal provisto por terceras partes reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos con la mayor prontitud posible.

- Los funcionarios y contratistas de la Administración Municipal, en caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno, reservada o restringida, deben notificarlo al superior inmediato para que se registre y se le dé el trámite necesario.

Políticas en Aspectos de Seguridad de la Información de la Gestión de Continuidad de Negocio

Gestión de la Continuidad de Negocio

La entidad debe indicar la manera en que garantizará la continuidad para todos sus procesos (de ser posible o por lo menos los misionales), identificando los procesos críticos que tendrán mayor prioridad en las fases de recuperación ante algún desastre o incidente crítico. Indicando los pasos a seguir cuando existan estas situaciones adversas, quienes deberán actuar (incluyendo las terceras partes o proveedores), los tiempos a cumplir, los procesos alternos o que permitan continuar con el proceso de manera temporal.

- El Área de Informática debe elaborar un plan de recuperación ante desastres para el centro de cómputo y un conjunto de procedimientos de contingencia, recuperación y retorno a la normalidad para cada uno de los servicios y sistemas prestados.

- La Oficina de Control Interno debe validar que los procedimientos de contingencia, recuperación y retorno a la normalidad incluyan consideraciones de seguridad de la información.

- La Oficina de Control Interno debe asegurar la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de negocio, verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.

- Los Directivos de cada una de las dependencias de la Administración Municipal deben identificar y, al interior de sus áreas, generar la documentación de los procedimientos de continuidad que podrían ser utilizados en caso de un evento adverso, teniendo en cuenta la seguridad de la información. Estos documentos deben ser probados para certificar su efectividad.

Bibliografía

Ministerio de las Tecnologías de la Información y las Comunicaciones, (2016). Modelo de Seguridad y Privacidad de la Información - Seguridad y Privacidad dela Información – Modelo - – Versión 3.0.2.

Ministerio de las Tecnologías de la Información y las Comunicaciones, (2016). Elaboración de la política general de seguridad y privacidad de la Información. – Seguridad y Privacidad dela Información – Guía No. 2 - Versión 1.

Ministerio de las Tecnologías de la Información y las Comunicaciones, (2016). Procedimientos De Seguridad De La Información. – Seguridad y Privacidad dela Información – Guía No. 3 - Versión 1.

Ministerio de las Tecnologías de la Información y las Comunicaciones, (2016). Controles de Seguridad y Privacidad de la Información. - Seguridad y Privacidad dela Información – Guía No. 8 - Versión 3.0.1.

ICONTEC, (2006). Norma Técnica Colombiana NTC-ISO/IEC 27001. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos.

Organización Internacional de Normalización y la Comisión Electrotécnica Internacional, (2013). ISO/IEC 27002:2013. Mejores prácticas en la gestión de la seguridad de la Información.

IT Governance Institute, (2007). Marco de Trabajo COBIT 4.1. Estándares internacionales para la dirección y control de la tecnología de la Información.

Instituto Colombiano de Crédito Educativo y Estudios Técnicos en el Exterior –ICETEX. (2014). Manual de Políticas de Seguridad de la Información – Recuperado el 1 de septiembre de 2016, de https://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/manuales/Manualseguridadinformacion.pdf

ISO 27002. Recuperado el 1 de septiembre de 2016, de http://www.iso27000.es/iso27002.html

Proyectó: Claudia Marcela García González

Vo.bo.