PERSONERIA MUNICIPAL DE ITAGUI

POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

2018

Centro Administrativo Municipal de Itagüí (CAMI)
Cra. 51 No 51-55
Teléfono: +57 (4) 3764884
www.personeriaitagui.gov.co / info@personeriaitagui.gov.co

SC-CER 427888
GP-CER 427887

INTRODUCCIÓN

La información es un activo de alto valor para la Personería Municipal de Itagüí. A medida que los procesos de la entidad se hacen más dependientes de la información y de la tecnología que la soporta, se hace necesario contar con reglas de alto nivel que permitan el control y administración efectiva de los datos.

Los sistemas computarizados y aplicaciones están en permanente evolución, por tal razón pueden surgir nuevos puntos vulnerables y crear interrupciones o degradación de los servicios apalancados por las TI, porque a pesar de los avances en los sistemas de seguridad, los usuarios autorizados o no al uso y apropiación de las TI, con herramientas muy sofisticadas tienen grandes posibilidades de acceder las redes, los sistemas o sitios que sin políticas claras y ampliamente difundidas pueden llegar a materializarse alguno de los siguientes riesgos:

- Ataques a través de software malicioso o virus informáticos
- Ataque de intrusión
- Ingreso de correos no deseado con contenido malicioso (correo fraudulento)
- Uso de claves de acceso a la red sin la consciencia de su confidencialidad
- Instalación de software no institucional y/o no licenciado
- Pérdida de información crítica de la Entidad la cual debería estar respaldada en servidores de archivos destinados para ello
- Manejo de memorias USB con información confidencial o critica de la Entidad
- Accidente o desastre que interrumpa o degrade los servicios
- Mal uso de los privilegios de acceso a la información o entrega de información confidencial de manera accidental o deliberada.

El presente manual contiene los lineamientos que rigen el uso y apropiación de la información en formato físico o digital tanto para los usuarios internos como para contratistas externos o proveedores, en cumplimiento de las disposiciones legales vigentes, con el objeto de minimizar los riesgos y salvaguardar la información de la entidad.

PROPÓSITO

Proporcionar a los funcionarios, contratistas externos y usuarios de la Entidad un instrumento orientador para asegurar la información y el adecuado manejo de las TI, minimizando los riesgos en los que puede estar expuesta la información a fin de mantener su disponibilidad, integridad y confidencialidad y el uso de las TI de manera eficaz, eficiente y uniforme.

PRINCIPIOS

Las políticas contenidas en el presente manual se justifican y sustentan en los principios de la seguridad de la información, tales principios son:

Propuesta de explicar el detalle de cada principio

- Promover comportamientos de seguridad responsables.
- Exhortar las actuaciones profesionales y técnicas.
- Promover una cultura positiva para la seguridad.

- Tener un enfoque basado en los riesgos.
- Buscar el cumplimiento de los requisitos legales y regulatorios pertinentes.
- Promover la mejora continua.
- Proteger la información clasificada.
- Evaluar las amenazas actuales y futuras de la información.
- Proteger la organización.
- Soportar el actuar de la entidad.
- Enfocarse en la organización.
- Ofrecer calidad y valor a las partes interesadas.
- Ofrecer información puntual y precisa sobre la gestión de la seguridad
- Concentrarse en aplicaciones organizacionales críticas.
- Buscar el desarrollo sistemas de información de forma segura.

Dada la importancia del manual, deberá ser de estricto cumplimiento, evitando |todo trámite fuera de él. Este documento es un material de consulta permanente y útil en los procesos de inducción o reinducción de la Entidad.

ROLES Y RESPONSABILIDADES ASOCIADAS A LA PRESENTE POLÍTICA

Comité de Dirección de Seguridad de la Información (CDSI)
(La entidad reglamentará su creación)
Sus funciones son:

- Formular y mantener actualizadas las políticas de seguridad de la información para toda la entidad.
- Revisar, aprobar y promover el cumplimiento de las políticas, normas y procedimientos de seguridad de la información.

Asesores, Secretarios, Gerentes, Directores y profesionales con personal a cargo

- Asegurar que los servidores públicos y contratistas bajo su responsabilidad conozcan, entiendan y atiendan las políticas contenidas en el presente manual.
- Aplicar controles o medidas que garanticen el cumplimiento de las políticas de seguridad de la información dentro de los procesos del Sistema Integrado de Gestión que lideren.

Servidores públicos y contratistas externos

- Conocer y cumplir las políticas indicadas en este manual.
- Reportar las infracciones o incumplimientos que identifique.
- Apoyar a otros servidores en el cumplimiento de las políticas indicadas en este manual

Oficial de seguridad de la información

- Dirigir el plan estratégico de seguridad de la información y tomar las decisiones que permitan gestionar la seguridad de la información en el marco del cumplimiento de las políticas definidas y aprobadas por el Comité de Dirección de Seguridad de la Información (CDSI).

- Identificar oportunidades para la mejora de las políticas de seguridad de la información en función de las necesidades de la entidad y de los riesgos que sean identificados.
- Cumplimiento de requisitos legales y regulatorios

El presente manual de políticas fue construido para proteger la información y la plataforma de tecnologías de información de la Personería Municipal de Itagüí; en ningún momento la aplicación de las políticas de seguridad de la información podrá dañar los derechos fundamentales de las personas como el derecho a la intimidad o el derecho a la vida, la salud o la seguridad.
Así mismo, las políticas de seguridad de la información fueron definidas de conformidad a lo establecido en:

- La Ley 1712 de 2014. Ley de transparencia y del derecho de acceso a la información pública nacional.
- La Ley 1581 de 2012 y decreto 1377 de 2013. Ley de protección de datos personales.
- La Ley 1273. Ley de delitos informáticos y la protección de la información y de los datos.
- El Decreto 2693 DE 2012. Lineamientos generales de la estrategia de Gobierno en línea de la República de Colombia.
- 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.
- La Ley 527/1999. 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.

PROCESO DISCIPLINARIO Y SANCIONES

El desacato o incumplimiento a las presentes políticas por parte de un servidor público o contratista de la Personería Municipal de Itagüí puede acarrear sanciones disciplinarias. Dichas medidas se impartirán en coherencia con la ley vigente y el reglamento interno de trabajo de la Personería Municipal de Itagüí.
Una infracción o falta de estas políticas por parte de un contratista externo puede generar la terminación de su contrato con la Personería Municipal de Itagüí.

MANEJO DE EXCEPCIONES

En aquellas circunstancias en que las necesidades institucionales justifiquen la ejecución de acciones, que se encuentren en conflicto con las políticas definidas en el presente manual, se deberá informar por escrito al Oficial de Seguridad de la Información a través del formato respectivo del sistema de gestión de la calidad. La validez de la excepción se determinará mediante un análisis de los riesgos. Si la excepción es válida, se comunicará por escrito al interesado indicando el período válido de la excepción acorde con el riesgo asociado. Una vez pasado el período de excepción el equipo de seguridad de la información valorará si continúa siendo una excepción, caso en el cual deberá ser evaluada y aprobada nuevamente.

DEFINICIONES

Activo de información: Todo aquello que tiene valor para la entidad y por lo tanto debe protegerse. De acuerdo con la norma ISO 27001 los activos de información se clasifican en: información, software, activos físicos, personas, servicios e intangibles como reputación, imagen de la entidad, etc.
Borrado seguro: procedimiento de eliminación de archivos que no permite la recuperación posterior de éstos.
Centro de Servicios Informáticos - CSI: equipo responsable de gestionar las solicitudes de servicio relacionadas con las plataformas de tecnologías de información de la Personería Municipal de Itagüí.
Comité de Dirección de Seguridad de la Información: Equipo interdisciplinario, conformado por servidores públicos de diferentes áreas la Personería Municipal de Itagüí que es presidido por el Director de Informática. Su función principal es la de gobernar y orientar gestión de la seguridad de la información en la Personería Municipal de Itagüí. Fue creado mediante resolución 108373 del 30/octubre/2013 y modificado mediante resolución 030836 del 21 de marzo de 2014.
Confidencialidad: Que la información solo sea accedida por las personas autorizadas para ello
Contratista externo: trabajador que sin tener una vinculación laboral directa con la Personería Municipal de Itagüí, presta sus servicios para la entidad (por ejemplo, a través de un contrato de prestación de servicios o por medio de una organización que tenga un contrato con la entidad).
Correo masivo: expresión usada en el presente manual de políticas para referirse a mensajes de correo electrónico enviado a 100 o más destinatarios que no formen parte de los dominios de la Personería Municipal de Itagüí.
Criterio de seguridad de la información de la Personería Municipal de Itagüí: conjunto de requisitos técnicos que deben considerarse para la planeación e implementación segura de infraestructura y aplicaciones de tecnología de información, así como para su posterior verificación.
Custodio de la información: es el usuario de la información que ejerza funciones de administración de sistemas de información. Sus responsabilidades incluyen:

- Garantizar que se cumplan los niveles de servicio definidos.
- Proporcionar asistencia al dueño de la información en la selección de soluciones técnicas apropiadas.
- Proveer operativamente el aseguramiento de la confidencialidad, integridad y disponibilidad de la información.

Derechos / Privilegios de acceso: conjunto de permisos dados a un usuario o a un sistema para acceder a un determinado recurso (repositorio información, aplicativo, datos).
Disponibilidad: La información estará lista para acceder a ella o utilizarse cuando se necesite
Dispositivos móviles: son aparatos con algunas capacidades de procesamiento y de conectividad. Su principal característica es su movilidad. Los dispositivos móviles abarcan una gran variedad de equipos como: teléfonos inteligentes, asistentes digitales personales (PDA), tabletas, y computadoras portátiles.
Dueño de activo de información: (o propietario). Servidor público de nivel directivo cuyo rol implica entender qué tipo de información es mantenida, creada, procesada o eliminada; cómo la información se desplaza en su área de responsabilidad y quien debe acceder a la información y por qué. Como resultado, son capaces de entender e identificar los riesgos a la información. Tiene la responsabilidad de asegurar la

clasificación de los activos y tomar decisiones sobre estos (por ejemplo: ubicación, acceso y controles de seguridad).

Entidad: término que se usa en el presente documento para identificar a la Personería Municipal de Itagüí cuando sea conveniente.

Equipos de trabajo de informática: equipos de trabajo de la Personería Municipal de Itagüí que son responsables de desarrollar, desplegar, mantener, proteger y administrar las plataformas de tecnología de información. Abarca a los integrantes de la Dirección de Informática y personal de otras áreas de la entidad con alguna de las responsabilidades mencionadas.

Equipo de seguridad de la información: grupo funcional adscrito a la Dirección de Informática, cuya función primordial es la de gestionar la seguridad de la información para el alcance previsto del Sistema de Gestión de Seguridad de la Información SGSI de la Personería Municipal de Itagüí, buscando que el nivel de riesgo de la información de la entidad permanezca en niveles aceptables.

Evento de seguridad de la información: Presencia identificada del estado de un sistema, servicio o red, que indica una posible violación de las políticas de seguridad de la información, una falla de los controles, o una situación desconocida previamente que puede ser relevante para la seguridad.

Incidente de seguridad de la información: Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. Todo incidente es un evento, más no todo evento es un incidente.

Integridad: La información debe estar completa y correcta en todo momento

Manual de protección de la información: Documento donde se establecen los lineamientos de seguridad para el manejo de la información de la Personería Municipal de Itagüí en función de la clasificación de dicha información. Según la Política de identificación y protección de la información la información de la entidad se clasifica en Pública, Clasificada y Reservada.

Plataforma de tecnologías de información / Plataforma de T.I.C.: Para propósitos del presente documento, las expresiones “plataforma de T.I.” y “plataforma de tecnologías de Información” hace referencia a todo el conjunto de recursos de tecnología de la información usados para generar, procesar, almacenar y transmitir información de la Personería Municipal de Itagüí. Lo que incluye por ejemplo: sistemas de información, equipos de escritorio, portátiles, sistemas operativos e infraestructura de red.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información:

- Confidencialidad: Propiedad que determina la condición de que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- Integridad: Propiedad de mantener la exactitud y estado completo de la información, en otras palabras, proteger la información para que no sea adulterada o alterada de forma indebida.
- Disponibilidad: Propiedad de mantener la información disponible y utilizable cuando lo requiera un individuo, proceso o entidad autorizada.

Seguridad informática: Rama de la seguridad de la información que se enfoca en la protección de la plataforma de tecnología de Información y de los datos que circulan, se procesan o almacenan en dicha plataforma.

Servidores Públicos: Término que se usa en el presente documento para identificar a empleados públicos, trabajadores oficiales y practicantes de la Personería Municipal de Itagüí.

Sistema de Gestión de Seguridad de la Información - SGSI: Sistema de gestión basado en un enfoque hacia los riesgos, cuyo fin es establecer, implementar, operar,

hacer seguimiento, revisar, mantener y mejorar la seguridad de la información. El SGSI se rige por los requisitos de la norma internacional de gestión ISO/IEC 27001.
Software malicioso: (También, código malicioso). Es un tipo de software que tiene como objetivo infiltrar o dañar un equipo de cómputo o sistema de información sin el consentimiento de su propietario. El software malicioso incluye virus, gusanos, troyanos, la mayor parte de los rootkits, scareware, spyware, adware intrusivo y crimeware. El término “software malicioso” también hace referencia a software hostil o molesto.
Usuario: Persona, proceso o aplicación de la entidad autorizada para acceder a la información de entidad o a los sistemas que la manejan.
Zonas restringidas de procesamiento: Son áreas, recintos o edificaciones ubicadas dentro de las sedes de la Personería Municipal de Itagüí destinadas a alojar Plataformas de tecnología de la información, recursos importantes o información de la entidad; razón por la que requieren controles especiales de seguridad física y control de acceso.

DOCUMENTOS RELACIONADOS

Documentos internos
(Por desarrollar)
- Manual de Protección de la Información.
- Procedimiento de Gestión de Peticiones de Servicios e Incidentes.
- Formato de plan de entrega de cargo.
- Formato de excepciones.
- Criterio de seguridad de la información.

Documentos externos
- 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 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013.
- 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”. Reglamentada parcialmente por el Decreto Nacional 103 de 2015.
- Decreto Nacional 2573 de 2014 “Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones”.
- Decreto 1078 del 26 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.
- * La Ley 527 de 1999 “Por medio de 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”.
- Norma Internacional de gestión ISO/IEC 27001:2013.
- Cobit 5 for information Security.

POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La información es un activo estratégico para las operaciones diarias de la Personería Municipal de Itagüí y a su vez un factor determinante para el éxito de su plan de desarrollo. Por ello, la entidad está comprometida con la adopción de buenas prácticas de seguridad de la información tendientes a implementar, mantener y mejorar su Sistema de Gestión de Seguridad de la Información SGSI.
Las Políticas y lineamientos de Seguridad de la Información y de las TI son de carácter obligatorio y deben ser conocidas y cumplidas por los servidores públicos, proveedores, contratistas y usuarios externos que hagan uso de la información y de los recursos tecnológicos de la entidad.

1. POLÍTICAS PARA SERVIDORES PÚBLICOS Y CONTRATISTAS EXTERNOS

Alcance

Estas políticas aplican tanto a los procesos realizados directamente por la Personería Municipal de Itagüí, como a los ejecutados a través de contratos o acuerdos con terceros.
Deben ser conocidas y cumplidas por los servidores públicos, proveedores, contratistas y usuarios externos de la entidad y de las sedes externas de la entidad que hagan uso de la información institucional y de sus recursos tecnológicos.
Comprende desde la explicación de los riesgos a los que están expuestos los activos de información, hasta la ejecución y seguimiento al cumplimiento de las normas y/o políticas informáticas.
Las políticas de seguridad de la información también aplican para los servidores públicos en modalidad de teletrabajo.

1.1. POLÍTICAS DE IDENTIFICACIÓN Y PROTECCIÓN DE LA INFORMACIÓN

Los activos de información dentro del alcance del Sistema de Gestión de Seguridad de la Información SGSI de la Personería Municipal de Itagüí deben ser identificados, clasificados y definidos los responsables de cada uno de ellos.
Busca asegurar que la información recibe el nivel de protección apropiado de acuerdo a la clasificación establecida.

1.1.1. Identificación y clasificación de la información

1.1.1.1 Los activos de información deben ser identificados y registrados en un inventario.

1.1.1.2 Los activos de información deben tener propietario designado.

1.1.1.3 El Propietario de un activo de información es responsable de:

- Definir los usuarios autorizados que pueden tener acceso al activo y sus privilegios de acceso.
- Determinar las clasificaciones correspondientes a la sensibilidad del activo.
- Asegurar que se gestione el riesgo de seguridad del activo.
- Establecer las reglas de uso del activo, cuando sea necesario.

- Solicitar la aplicación de controles para la protección del activo de información.

1.1.1.4 Cada activo de información debe tener un custodio designado, quien ha de protegerlo mediante la aplicación y el mantenimiento de los controles de seguridad autorizados por el propietario.

1.1.1.5 La información de la Personería Municipal de Itagüí se clasifica en:

- **Información pública.** Es toda información que la Personería Municipal de Itagüí genere, obtenga, adquiera, o controle en su calidad de obligado.
- **Información clasificada.** Es aquella información que estando en poder o custodia de la Personería Municipal de Itagüí en su calidad de obligado, pertenece al ámbito propio, particular y privado o semi-privado 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 6 de marzo de 2014 (ley de transparencia y del derecho de acceso a la información pública nacional).
- **Información reservada.** Es aquella información que estando en poder o custodia de la Personería Municipal de Itagüí en su calidad de obligado, 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 6 de marzo de 2014 (ley de transparencia y del derecho de acceso a la información pública nacional).

1.1.1.6 El manejo de la información de la Personería Municipal de Itagüí debe seguir los lineamientos del Manual de Protección de la Información.

1.1.1.7 Sólo se permite la transferencia de información Clasificada o Reservada cuando exista un acuerdo de confidencialidad o compromiso contractual que lo regule.

1.1.1.8 La Personería Municipal de Itagüí tiene control total sobre la información que se almacene en la infraestructura de tecnología de la información de la entidad; por lo tanto se reserva el derecho de mover, borrar, monitorear o tomar custodia de dicha información, para lo cual deberá contar con la aprobación del Director de Informática, del líder de proceso del tema en referencia y del Oficial de Seguridad.

1.1.1.9 Los servidores públicos y contratistas son responsables de proteger la información de su trabajo y solicitar a la Dirección de Informática el almacenamiento seguro de la información cuya pérdida pueda causar incumplimientos legales y/o la interrupción de los procesos de la entidad.

1.2. POLÍTICA DE GESTIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

En la Personería Municipal de Itagüí la gestión de los riesgos fundamenta la toma de decisiones de seguridad de la información.
Busca establecer la gestión del riesgo como eje principal de las actuaciones institucionales relacionadas con la seguridad de la información.

1.2.1. Lineamientos generales de la gestión del riesgo de seguridad informática
1.2.1.1 Servidores públicos y contratistas de la Personería Municipal de Itagüí, deben identificar y reportar condiciones que podrían indicar la existencia de riesgos de seguridad informática.

1.3. POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

En la Personería Municipal de Itagüí los eventos e incidentes de seguridad de la información son gestionados oportunamente con el fin de minimizar el impacto sobre la entidad.
Busca establecer las líneas de actuación de los servidores públicos frente a la ocurrencia (confirmada o sospechada) de situaciones que afecten la seguridad de la información.

1.3.1. Reporte de eventos, incidentes y debilidades de la seguridad informática.
1.3.1.1. Los servidores públicos y contratistas deben reportar inmediatamente al Centro de Servicios de Informática CSI, todas las situaciones que puedan afectar la seguridad de la información.

1.3.1.2. La información específica sobre Incidentes o vulnerabilidades de seguridad de la información, así como el detalle de las medidas para proteger las Plataforma de T.I.C., debe ser tratada como información Reservada.

1.3. POLÍTICA DE USO ADECUADO DE LOS RECURSOS DE LA PLATAFORMA DE TI

Toda la información de la Personería Municipal de Itagüí, así como los recursos para su procesamiento, almacenamiento y transmisión deben ser empleados únicamente para propósitos laborales o de la entidad; evitando su abuso, derroche, uso ilegal o desaprovechamiento.
Define las directrices para asegurar debido uso de los recursos de tecnologías de información y la comunicación de la entidad.

1.3.1. Requerimientos generales para el uso adecuado de la plataforma de TI.
1.3.1.1. Se prohíbe el uso de los recursos de plataforma de T.I. de la Personería Municipal de Itagüí para la realización de cualquier actividad ilegal.

1.3.1.2. Para verificar el cumplimiento de las presentes políticas; la Personería Municipal de Itagüí podrá monitorear y auditar las Plataforma de T.I.C. de la entidad que son facilitadas a servidores públicos y contratistas para el cumplimiento de sus deberes y funciones laborales.

1.3.1.3. Los servidores públicos y contratistas deben abstenerse de crear, acceder, almacenar o transmitir material ilegal, pornográfico, que promueva la violación de los derechos humanos o que atente contra la integridad moral de las personas o de las instituciones.

1.3.1.4. Está prohibida la realización de pruebas a los controles de seguridad de la información.

1.3.1.5. No está permitido aprovechar las vulnerabilidades de seguridad de las plataforma de TI

1.3.1.6. Solamente el grupo de Seguridad de la Información o un tercero autorizado por la Dirección de Informática puede utilizar herramientas de diagnóstico de la seguridad de la información (herramientas de hacking) sobre los activos de información de la Entidad.

1.3.1.7. Los programas informáticos desarrollados o adquiridos por Personería Municipal de Itagüí son para el uso exclusivo de la entidad.

1.3.2. Uso adecuado del correo electrónico

1.3.2.1. No está permitido enviar correos masivos sin la autorización del personal directivo de la dependencia.

1.3.2.2. La Dirección de Informática podrá establecer los límites en la cantidad de destinatarios y el tamaño de los mensajes de correo electrónico.

1.3.2.3. No está autorizado el envío de correos electrónicos con contenido que atente contra la integridad y la dignidad de las personas, así como con el buen nombre de la entidad.

1.3.2.4. Cuando un funcionario, contratista o colaborador al que le haya sido autorizado el uso de una cuenta de correo electrónico se retire de la Personería Municipal de Itagüí, su cuenta de correo será desactivada.

1.3.2.5. Las cuentas de correo electrónico son propiedad de la Personería Municipal de Itagüí, son asignadas para la realización tareas propias de la funciones laborales y no deben utilizarse para ningún otro fin.

1.3.2.6. Todos los mensajes pueden ser sujetos a análisis y conservación permanente por parte de la Entidad.

1.3.2.7. Cuando se detecte un correo fraudulento, con fines maliciosos o con contenido sospechoso se debe informar esta situación al Grupo de seguridad de la Información o a la mesa de ayuda del Centro de Servicios Informáticos (CSI).

1.3.3. Uso adecuado de equipos de cómputo asignados

1.3.3.1. No está permitida la instalación, ejecución y/o utilización de software diferente al preinstalado en los equipos de cómputo o al instalado por integrantes de los equipos de trabajo de informáTIa.

1.3.3.2. Los parámetros de configuración del sistema operativo solo deben ser modificados por integrantes de los equipos de trabajo de informáTIa.

1.3.4. Uso adecuado de los servicios de red

1.3.4.1. No deben almacenarse archivos personales en carpetas de la red y demás servicios de almacenamiento en internet suministrados por la Personería Municipal de Itagüí.

1.3.4.2. No se permite el uso de servicios de descarga o intercambio de archivos que funcionan bajo el esquema P2P (person to person). Por ejemplo: Torrent, Ares, eMule, Limewire, GNUnet, entre otros.

1.3.4.3. No está permitida la descarga de archivos de audio y/o video a menos que lo requieran en virtud de sus responsabilidades laborales.

1.3.4.4. La Personería Municipal de Itagüí podrá controlar y limitar la navegación a ciertos sitios, recursos o servicios de internet con el fin de proteger la seguridad y la disponibilidad del servicio de internet.

1.3.4.5. No está permitido deshabilitar o evadir los controles de navegación en internet.

1.3.4.6. En horarios laborales, está prohibido el uso del servicio de internet de la entidad para acceder a páginas de transmisión de películas, programas de televisión y eventos deportivos.

1.3.4.7. El acceso remoto a los equipos y dispositivos de la plataforma de T.I. solo está permitido para labores de soporte técnico autorizado.

1.3.4.8. El acceso remoto a equipos de cómputo debe contar con la aprobación del servidor público o contratista responsable de dicho equipo.

1.3.4.9. Solo se permite el acceso remoto a estaciones de trabajo de la entidad si el servidor público o contratista responsable del equipo de cómputo lo aprueba.

1.3.4.10. Solo está permitido el uso de servicios de almacenamiento de información suministrados por la entidad.

1.3.4.11. La red de visitantes está dispuesta únicamente para las personas que visitan temporalmente la Personería Municipal de Itagüí.

1.3.4.12. Solo equipos matriculados en el directorio activo institucional pueden ser ingresados a la red de la Personería Municipal de Itagüí.

1.3.4.13. No se permite la inclusión de equipos de cómputo personales (tales como PCs, computadores portátiles, celulares, tabletas, impresoras, cámaras, y wearables) en la red corporativa.

1.3.4.14. Todo equipo Tecnológico debe ser revisado, registrado y aprobado por la Dirección de Informática antes de conectarse a cualquier nodo de la Red de corporativa. Aquellos dispositivos que no estén aprobados deben ser desconectados de la red, eventos de conexión de equipos no autorizados a la red institucional se deben reportar como eventos/incidentes de seguridad.

1.3.5. Uso de material protegido por derechos de autor

1.3.5.1. Se prohíbe el almacenamiento de archivos multimedia (videos, música, imágenes o libros electrónicos) y cualquier otro tipo de contenido que viole las leyes y regulaciones vigentes de propiedad intelectual (derechos de autor y propiedad industrial) en las carpetas de red y demás servicios de almacenamiento en internet suministrados por la entidad.

1.3.5.2. Se prohíbe el almacenamiento, uso, instalación y/o ejecución de software que viole las leyes y regulaciones vigentes de propiedad intelectual (derechos de autor y propiedad industrial) y/o licenciamiento en la plataforma tecnológica de la entidad.

1.4. POLÍTICA DE PERSONAS Y CULTURA FRENTE A LA SEGURIDAD INFORMÁTICA

Se deben aplicar medidas de control antes, durante y después de finalizada la relación laboral, con el fin de mitigar los riesgos de seguridad de la información asociados al factor humano.
Procura que los servidores públicos y contratistas, entiendan sus responsabilidades y las funciones de sus roles como usuarios de la información con el fin de reducir el riesgo de hurto, fraude o filtraciones.

1.4.1. Antes del empleo

1.4.1.1. Toda persona a ser contratada como servidor público, debe aceptar formalmente el cumplimiento de las políticas del presente manual.

1.4.2. Durante el empleo o la vigencia del contrato

1.4.2.1. Los servidores públicos y contratistas de la Personería Municipal de Itagüí son responsables por desempeñar sus funciones cumpliendo las políticas definidas en el presente manual.

1.4.2.2. Los servidores públicos y contratistas de la Personería Municipal de Itagüí son responsables por desempeñar sus funciones sin descuidar, ignorar o desestimar los controles de seguridad establecidos.

1.4.2.3. Los servidores públicos y contratistas que tengan acceso a la información de la Personería Municipal de Itagüí deben participar en las actividades o iniciativas de concientización en materia de seguridad de la información a las que sea convocado.

1.4.2.4. El incumplimiento de las políticas consignadas en el presente manual podrá generar sanciones disciplinarias.

1.4.2.5. Las políticas de seguridad informática forman parte integral de los contratos de trabajo de los servidores públicos.

1.4.3. Terminación del contrato o cambio de cargo

1.4.3.1. Servidores públicos y contratistas que finalicen su relación laboral con la Personería Municipal de Itagüí deben entregar a su superior inmediato o responsable, la información de la entidad que se encuentre bajo su responsabilidad y/o manejo. Debe quedar registro de lo anterior en el formato “PLAN DE ENTREGA DEL CARGO” del Sistema Integrado de Gestión.

1.4.3.2. La información y el conocimiento desarrollado por los servidores públicos de la Personería Municipal de Itagüí durante el horario laboral y dentro de la vigencia del contrato laboral es propiedad de la entidad, por lo tanto se prohíbe el borrado o la copia de dicha información por parte de servidores públicos y contratistas en proceso de retiro o por personal retirado.

1.4.3.3. Ante la finalización de la relación laboral o contractual de un servidor público o contratista con la Personería Municipal de Itagüí, se deben suspender inmediatamente los permisos de acceso a la plataforma de T.I. de la entidad.

1.4.3.4. La Dirección de Personal debe informar inmediatamente a la Dirección de Informática, los retiros o traslados de los servidores públicos, trabajadores oficiales y practicantes, con el fin de revocar o modificar los privilegios de acceso asignados a dicho personal.

1.4.3.5. El superior inmediato de servidores públicos y contratistas es el responsable de gestionar el retiro o modificación de los derechos de acceso ante novedades laborales como la terminación o cambio del contrato.

1.4.3.6. El superior inmediato es el responsable de gestionar el respaldo de la información de los equipos de cómputo de los servidores públicos y contratistas en proceso de retiro.

1.5. POLÍTICA DE SEGURIDAD INFORMÁTICA PARA CONTRATACIÓN

La información de la Personería Municipal de Itagüí debe ser protegida en el proceso de contratación.
Busca proteger los procesos de contratación frente a situaciones que comprometan la disponibilidad, la integridad y la confidencialidad de la información de dichos procesos; resguardando así su legalidad y transparencia.

1.5.1. Disposiciones generales

1.5.1.1. Los servidores públicos y contratistas responsables por los servicios de contratistas o proveedores, son responsables de identificar y valorar los riesgos de la información asociados al acceso de éstos.

1.5.1.2. Los contratos celebrados entre la Personería Municipal de Itagüí y contratistas o proveedores con acceso a la información de la entidad, deben incluir cláusulas para mitigar riesgos de seguridad de la información.

1.5.1.3. Con el fin de proteger la información de ambas partes, se debe formalizar un acuerdo de confidencialidad. El acuerdo deberá definir claramente el tipo de información que intercambiarán las partes, los medios, la frecuencia y los procedimientos a seguir.

1.5.1.4. Siempre que haya un proceso de selección que implique la entrega de información Clasificada o Reservada de la entidad, los proponente participantes deben firmar previamente un acuerdo de confidencialidad.

1.6. POLÍTICA DE SEGURIDAD FÍSICA DE LA INFORMACIÓN Y LOS EQUIPOS DE CÓMPUTO

Se debe brindar seguridad física a la información de la entidad y a los recursos de la plataforma de T.I., de modo que se encuentren en condiciones ambientales adecuadas y a su vez, sean protegidos de situaciones como acceso no autorizado, robo, destrucción o desconexión.
Se pretende proteger la información, así como las tecnologías de información y la comunicación de la entidad frente a incidentes de seguridad causados por condiciones inadecuadas protección física, sean estas ambientales o que faciliten el acceso indebido a los activos de información.

1.6.1. Seguridad en las instalaciones

1.6.1.1. Fuera del horario laboral normal o cuando se alejen de sus estaciones de trabajo, los Servidores públicos y contratistas deben despejar sus pantallas, escritorios y áreas de trabajo, de tal manera que los datos, bien sean físicos (como documentos impresos y carpetas) o electrónicos (como memorias USB, Discos Duros Externos, CDs y DVDs), estén resguardados adecuadamente.

1.6.1.2. Cuando un servidor público se percate de la presencia de personas sospechosas en las instalaciones de entidad, debe reportar dicha situación a la Dirección de Seguridad Interna.

1.6.1.3. No se deben prestar ni descuidar los elementos de identificación y acceso a las instalaciones de la Personería Municipal de Itagüí (tales como tarjetas de acceso, carnets, llaves y tokens).

1.6.1.4. Cuando se imprima información clasificada o reservada, las impresiones deben ser retiradas inmediatamente.

1.6.1.5. Siempre que sea posible, las impresiones deben ser protegidas por medio de una clave de seguridad.

1.6.1.6. Las reuniones y sesiones de videoconferencias de la Personería Municipal de Itagüí no deben ser grabadas en audio o video a menos que todos los participantes estén al tanto de dicha grabación. En el acta de la reunión debe registrarse que la sesión fue grabada.

1.6.1.7. No está permitido fumar, ingerir alimentos o bebidas en las aulas con equipos de cómputo.

1.6.2. Seguridad de los equipos

1.6.2.1. Los servidores públicos y contratistas de la Personería Municipal de Itagüí son responsables de garantizar la debida protección de los equipos asignados (computadores de escritorio y dispositivos móviles) dentro y fuera de la entidad, lo que contempla su vigilancia, el debido cuidado en su transporte y el uso de cualquier otra medida de seguridad física necesaria.

1.6.2.2. Los equipos suministrados por la Personería Municipal de Itagüí, como computadores de escritorio y dispositivos móviles (incluye computadores portátiles), no deben ser objeto de alteraciones en su hardware. Toda modificación a los equipos debe ser autorizada y realizada por personal de soporte técnico de los equipos de trabajo de informática.

1.6.2.3. Se debe bloquear la sesión cuando el usuario se aleje del computador.

1.6.2.4. La salida de los computadores (de escritorio o portátiles) de la entidad debe ser autorizada por el secretario general.

1.6.2.5. Toda pérdida de equipos de cómputo o de alguno de sus componentes, debe ser informada inmediatamente al centro de servicios informáticos CSI.

1.6.2.6. Los equipos de cómputo externos (no entregados por la Personería Municipal de Itagüí) no deben conectarse a la red de datos de la entidad, a menos que cumplan con los requisitos definidos por la Dirección de Informática. (Requisitos por definir).

1.6.2.7. Solo personal de la mesa de ayuda (Centro de Servicios Informáticos CSI) debe tener privilegios de administración sobre las equipos de cómputo.

1.7. POLÍTICA DE CONTROL DE ACCESO A PLATAFORMAS DE TECNOLOGÍA DE LA INFORMACIÓN

La Personería Municipal de Itagüí otorga el nivel de acceso necesario a la información y su plataforma de T.I. para el cabal cumplimiento de las funciones de los servidores públicos y contratistas.
Se busca evitar y mitigar riesgos que comprometan la confidencialidad de la información y de las plataformas T.I.C. institucionales.

1.7.1. Gestión de acceso a usuarios

1.7.1.1. Los dueños de los sistemas de información deben verificar que los privilegios de acceso de los usuarios en las Plataformas de tecnología de la información se han otorgado de acuerdo con la necesidad laboral legítima.

1.7.1.2. Los privilegios de acceso otorgados a los usuarios de las Plataformas de tecnología de la información deben ser autorizados por el superior inmediato.

1.7.1.3. Los privilegios de acceso otorgados a los usuarios de las Plataformas de Tecnología de Información deben ser revisados al menos anualmente por los jefes inmediatos de los usuarios.

1.7.1.4. No están permitidas las cuentas de usuarios genéricas para el ingreso a la Plataforma de T.I.

1.7.1.5. Todas las cuentas de usuario son personales e intransferibles.

1.7.1.6. Servidores públicos y contratistas de la Personería Municipal de Itagüí deben reportar a su Jefe cuando tengan más derechos de acceso de los necesarios.

1.7.1.7. A excepción de las carpetas de red, los usuarios deben abstenerse de ingresar a los servidores de la plataforma tecnológica de la Personería Municipal de Itagüí, a menos que lo requieran en virtud de sus funciones laborales (como los Administradores de plataforma de T.I. de la entidad).

1.7.1.8. En la eventualidad de requerirse el ingreso a un equipo o a alguna de las cuentas de los sistemas de información de la entidad asignadas a un servidor público ausente, el jefe directo respectivo será el único autorizado para solicitar el acceso.

1.7.1.9. Los servidores públicos y contratistas son los responsables de todas las transacciones o acciones efectuadas con su cuenta de usuario.

1.7.1.10. Ningún servidor público, contratista deberá acceder a la red o a los servicios de T.I.C. de la Personería Municipal de Itagüí utilizando una cuenta de usuario diferente a la que le fue asignada.

1.7.2. Manejo de contraseñas

1.7.2.1. Los usuarios de las Plataformas de Tecnologías de la Información de la Personería Municipal de Itagüí deben abstenerse de escribir las contraseñas en medios físicos o electrónicos.

1.7.2.2. Las contraseñas de acceso a las Plataformas de Tecnologías de la Información son personales e intransferibles, cada usuario es responsable de su uso y de preservar su confidencialidad.

1.7.2.3. El préstamo de contraseñas está prohibido bajo cualquier circunstancia, en caso de hacerlo el usuario de la información responsable de la cuenta asume las consecuencias generadas por dicha situación.

1.7.2.4. Los usuarios de las Plataforma de T.I.C. tienen la responsabilidad de cambiar su contraseña (o solicitar su cambio, si es el caso) en el evento que fuese revelada o existiese alguna sospecha de ello.

1.7.2.5. Todos los usuarios de Las Plataformas de Tecnología de Información de la entidad deben emplear contraseñas seguras, es decir, que cumplan las siguientes características:

- 10 Caracteres como mínimo.
- Deben incluir letras mayúsculas y minúsculas.
- Deben incluir números.
- Deben incluir caracteres especiales, por ejemplo !@#$%&*.
- No deben basarse en información personal como: fechas de cumpleaños, direcciones, números telefónicos, nombres de personas, números de documentos de identificación, nombre de la entidad, etc.
- No deben basarse en información de la entidad, es decir, no deben hacer referencia al nombre de la entidad, sus procesos, dependencias, áreas o funciones.

1.8. POLÍTICA DE OPERACIÓN DE PLATAFORMAS DE TECNOLOGÍA DE INFORMACIÓN

La Personería Municipal de Itagüí aplica controles para el funcionamiento correcto y seguro de las Plataformas de tecnología de la información y la comunicación.
Se busca proteger la operación de las plataformas de T.I.C. institucionales, garantizando la continuidad y la seguridad de los procesos institucionales.

1.8.1. Requisitos para la planeación y operación de las plataformas de TI.

1.8.1.1. Todas las adquisiciones de software y hardware deben estar avaladas técnicamente por la Dirección de Informática.

1.8.1.2. Los componentes y sistemas de la infraestructura de seguridad de la información, no deben ser inhabilitados, desviados, apagados o desconectados sin la previa autorización de la Dirección de Informática.

1.8.2. Protección contra software malicioso

1.8.2.1. No está permitido el ingreso intencionado de software malicioso a los equipos y redes de la Personería Municipal de Itagüí.

1.8.2.2. La presencia identificada o sospechada de software malicioso debe ser reportada al Centro de servicios de Informática CSI.

1.8.3. Intercambio de información

1.8.3.1. Todo intercambio de información con terceras partes debe ser realizado de conformidad a lo dispuesto en el Manual de Protección de la Información. (Por desarrollar).

1.8.3.2. Se deben implementar controles que aseguren la confidencialidad de las conexiones de red a través de las cuales se realice intercambio de información sensible con redes externas o a través de internet.

1.8.3.3. Personal de la mesa de ayuda del Centro de servicios Informáticos no está obligado a realizar procedimientos de recuperación de información borrada, debido a que no puede garantizarse la eficacia (el éxito) de la realización de estas actividades de recuperación. De ser realizado este tipo de servicios, el personal del CSI no se compromete con la cantidad ni con la calidad de la información recuperada.

1.8.3.4. La Personería Municipal de Itagüí no está obligada a prestar soporte técnico a equipos de cómputo que no sean propiedad de la entidad.

1.9. POLÍTICAS DE CIFRADO DE LA INFORMACIÓN

Deben aplicarse mecanismos de cifrado cuando exista un alto riesgo de comprometer la confidencialidad de la información clasificada o reservada de la entidad.
Busca establecer lineamientos tendientes a la protección de la confidencialidad de la información a través de mecanismos de cifrado.

1.9.1. Cifrado

1.9.1.1. Servidores públicos y contratistas que sean responsables de llaves (o claves) de cifrado deben reportar al Equipo de Seguridad de la información, novedades acerca del manejo de dichas llaves (por ejemplo: cambio de dueños, cambio de custodia, pérdidas, acceso no autorizado).

1.9.1.2. Cada vez que se utilice el cifrado, los servidores públicos y contratistas no deben borrar la única versión legible de los datos, a menos que hayan probado que el proceso de des-cifrado puede restablecer una versión legible de los datos.

1.9.1.3. Se deben utilizar mecanismos de cifrado cuando se requiera el almacenamiento de información reservada o clasificada en medios removibles (como memorias USB, discos duros externos, CD y DVD).

1.9.1.4. Se deben utilizar mecanismos de cifrado cuando se requiera enviar información reservada o clasificada a través de redes externas (internet).

1.10. POLÍTICA DE DISPOSITIVOS MÓVILES

El acceso a los datos y sistemas de información de la Personería Municipal de Itagüí a través de dispositivos móviles debe ser realizado de forma regulada y controlada con el fin de evitar incidentes de seguridad de la información.
Procura proteger la información institucional que se almacena en dispositivos móviles de la entidad.

1.10.1. Computadores portátiles

1.10.1.1. Los usuarios que tengan bajo su responsabilidad computadores portátiles de la Personería Municipal de Itagüí son responsables de su protección dentro y fuera de las instalaciones de la entidad.

1.10.1.2. Todo usuario al que se le asigne o facilite un computador portátil de la Personería Municipal de Itagüí debe asegurarlo adecuadamente al puesto de trabajo con la guaya de seguridad.

1.10.1.3. Los usuarios de computadores portátiles de la Personería Municipal de Itagüí deben emplear medidas de seguridad para su adecuado manejo fuera de las instalaciones de la entidad. Las medidas de protección incluyen, pero no se limitan a:

- Llevar los computadores portátiles como equipaje de mano en viajes terrestres y aéreos.
- Mantener a la vista y vigilar el computador portátil en todo momento que se esté fuera de las instalaciones de la entidad o de la vivienda del servidor público.
- Ocultar el computador portátil de la vista de personas externas cuando se esté transportando en un vehículo.
- Utilizar la guaya de seguridad.

1.10.1.4. Los computadores portátiles están cubiertos por la sección “Seguridad física de los equipos” del presente manual de políticas.

1.10.2. Dispositivos móviles diferentes a computadores portátiles
Nota: esta sección hace referencia a dispositivos como teléfonos móviles inteligentes y tabletas.

1.10.2.1. Los usuarios de dispositivos móviles entregados por la Personería Municipal de Itagüí son responsables de su protección dentro y fuera de las instalaciones de la entidad.

1.10.2.2. Los usuarios de dispositivos móviles entregados por la Personería Municipal de Itagüí deben abstenerse de modificar las configuraciones de seguridad de dichos dispositivos.

1.10.2.3. Los usuarios de dispositivos móviles entregados por la Personería Municipal de Itagüí deben reportar inmediatamente el robo o pérdida de dicho dispositivo al personal de los equipos de trabajo de informática.

1.10.2.4. No está permitido el envío de información Clasificada o Reservada a través de servicios de mensajería instantánea no institucionales (como WhatsApp, LIME o Blackberry BBN PIN).

1.10.2.5. La Personería Municipal de Itagüí no está obligada a prestar soporte técnico a dispositivos móviles que sean de propiedad de los usuarios o cualquier otro que no sea propiedad de la entidad.

1.10.2.6. Los usuarios que accedan a los servicios de la plataforma de T.I. (por ejemplo, al correo electrónico) a través de un dispositivo móvil propio, deben reportar inmediatamente el robo, cambio o pérdida de dicho dispositivo al centro de servicios informáticos CSI.

1.11. POLÍTICA DE CUMPLIMIENTO

La Personería Municipal de Itagüí cumple la regulación y legislación vigente aplicable en materia de seguridad de la información.
Busca identificar y asegurar el cumplimiento de los requisitos regulatorios y legales aplicables a la entidad en cuanto a la seguridad de la información.

1.11.1. Cumplimiento legal y normativo

1.11.1.1. Será sancionado con las acciones disciplinarias y legales correspondientes, al que utilizare registros informáticos, software u otro medio para ocultar, alterar o distorsionar información requerida para una actividad de la entidad, para el cumplimiento de una obligación respecto al Estado o para ocultar los estados contables o la situación de un proceso, área o persona física o jurídica.

1.11.1.2. Toda la información de ciudadanos o servidores públicos y contratistas que incluya cédulas de identidad, datos de contacto o información financiera debe ser sólo accesible al personal de la entidad que necesite ese acceso en virtud de su trabajo.

1.11.1.3. La realización de auditorías (verificaciones o pruebas de seguridad) no deben afectar la normal operación de los sistemas de información o plataformas.

1.12. POLÍTICA DE SEGURIDAD PARA REDES SOCIALES INSTITUCIONALES

Las redes sociales institucionales deben ser protegidas de situaciones de acceso indebido y publicaciones no autorizadas.

1.12.1. Asegurar el manejo seguro de las redes sociales institucionales, evitando situaciones que puedan afectar la reputación de la entidad derivadas del su uso no autorizado.

1.12.2. Las credenciales de acceso (usuario y contraseña) de una cuenta institucional de redes sociales, solo pueden ser conocidas por un único responsable designado.

1.12.3. Las contraseñas de acceso a las redes sociales institucionales deben cumplir los lineamientos para contraseñas establecidos en el presente documento.

1.12.4. Las contraseñas de redes sociales institucionales deben ser cambiadas cada tres meses como mínimo.

1.12.5. No debe establecerse la misma contraseña a más de una cuenta de redes sociales institucionales.

1.12.6. Se deben cambiar las contraseñas de acceso cada vez que se cambien los responsables del manejo de las redes sociales institucionales.

1.12.7. Copias de las credenciales de acceso a las redes sociales institucionales (usuarios y contraseñas) deben ser puestas en sobres firmados y sellados (un sobre por cada cuenta de redes sociales) estos sobres deben permanecer en un sitio seguro, como una caja de seguridad; de modo que puedan ser utilizados en caso de contingencias con el (los) responsable(s) de las redes sociales.

2. POLÍTICAS PARA EL PERSONAL DE LOS EQUIPOS DE TRABAJO DE INFORMÁTICA

Alcance

Estas Políticas aplican exclusivamente a personal de los equipos de Informática de la Personería Municipal de Itagüí ya sea interno o externo, en el ámbito del proceso de Planeación y Administración de las TI.

2.1. **POLÍTICA DE GESTIÓN DEL RIESGO DE SEGURIDAD INFORMÁTIA**

En la Personería Municipal de Itagüí, la gestión de los riesgos fundamenta la toma de decisiones de seguridad de la información en la Personería Municipal de Itagüí.
Busca establecer la gestión del riesgo como eje principal de las actuaciones institucionales relacionadas con la seguridad de la información.

2.1.1. Lineamientos generales de la gestión del riesgo de seguridad informática
2.1.1.1. Se deben identificar los riesgos a los que se encuentran expuestos los activos de información de la entidad.

2.1.1.2. Los criterios de evaluación y aceptación de riesgos de seguridad de la información deben estar alineados con los criterios y políticas de gestión del riesgo de la entidad.

2.1.1.3. Los riesgos de seguridad de la información analizados deben ser objeto de tratamiento (mitigar, transferir, evitar, aceptar), dicho tratamiento debe ser coherente con los criterios de aceptación de riesgos.

2.1.1.4. Los riesgos deben ser monitoreados después de su tratamiento para asegurar que siguen estando en niveles aceptables para la entidad.

2.1.1.5. En los casos que se realice la estimación económica de los riesgos, se debe asegurar que el valor de la aplicación de medidas de mitigación sea inferior al costo de las consecuencias de la materialización de los riesgos.

2.2. **POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA**

En la Personería Municipal de Itagüí los eventos e incidentes de seguridad de la información son gestionados oportunamente con el fin de minimizar el impacto sobre la entidad.

Busca establecer las líneas de actuación de los servidores públicos frente a la ocurrencia (confirmada o sospechada) de situaciones que afecten la seguridad de la información.

2.2.1. Gestión de incidentes de seguridad de la información
2.2.1.1. Debe conformarse y mantenerse un equipo multidisciplinario para la respuesta y tratamiento a los incidentes de seguridad de la información.

2.2.1.2. La atención de incidentes debe seguir el procedimiento descrito en el sistema de gestión de la calidad Gestión de Peticiones de Servicios e Incidentes.

2.3. POLÍTICA DE SEGURIDAD INFORMÁTICA ASOCIADA A CONTRATISTAS

La información de la Personería Municipal de Itagüí debe ser protegida de los riesgos generados por el manejo o acceso de contratistas y proveedores.
Busca mantener la seguridad de los activos de información accedidos por contratistas, evitando situaciones como:

- Abuso de privilegios de acceso.
- Fuga de información.
- Negación de responsabilidades de incidentes de seguridad por parte del contratista.

2.3.1. Requisitos de seguridad de la información asociados a contratistas y terceros

2.3.1.1. El acceso de contratistas y proveedores a información o a plataformas de tecnología de Información de la Personería Municipal de Itagüí, se concede

solamente cuando se demuestre la necesidad de su uso y esté expresamente autorizado por el propietario del activos de información o sistema de información respectivo.

2.3.1.2. Únicamente debe concederse acceso remoto a plataformas de TI a contratistas y proveedores cuando estos tengan una necesidad legítima que lo justifique. El acceso remoto debe limitarse al tiempo requerido para cumplir con las actividades, debe ser autorizado por el propietario del activo respectivo, y posteriormente gestionado por personal autorizado de la Dirección de Informática.

2.3.1.3. El tercero que ejerza funciones de administración y soporte de sistemas de información, debe garantizar que se generan registros automáticos (logs de auditoría) de dichas labores.

2.3.1.4. El tercero que ejerza funciones de administración y soporte de sistemas de información, debe garantizar que se generan registros automáticos (logs de auditoría) de dichas labores.

2.4. SEGURIDAD FÍSICA DE LA INFORMACIÓN Y LOS EQUIPOS DE CÓMPUTO

Se debe brindar seguridad física a la información de la entidad y a los recursos de la plataforma de T.I., de modo que se encuentren en condiciones ambientales adecuadas y a su vez, sean protegidos de situaciones como acceso no autorizado, robo, destrucción o desconexión.

Se busca proteger la información, así como las tecnologías de información y la comunicación de la entidad frente a incidentes de seguridad causados por condiciones inadecuadas protección física, sean estas ambientales o que faciliten el acceso indebido a los activos de información.

2.4.1. Zonas restringidas de procesamiento

2.4.1.1. Se deben identificar y especificar las zonas restringidas de procesamiento de la Personería Municipal de Itagüí destinadas a alojar equipos y dispositivos de la plataforma de T.I. de la entidad.

2.4.1.2. Cada zona restringida de procesamiento debe tener un responsable.

2.4.1.3. Las zonas restringidas de procesamiento deben contar al menos con mecanismos de control de acceso y vigilancia.

2.4.1.4. Se deben definir las reglas para el trabajo al interior de las zonas restringidas de procesamiento, dichas reglas deben ser documentadas y publicadas en un lugar visible de cada una de estas zonas.

2.4.1.5. Todo sistema, equipo, dispositivo, o medio crítico para la transmisión, procesamiento y almacenamiento de la información de la Personería Municipal de Itagüí debe ser ubicado dentro de zonas restringidas de procesamiento. Si no se pudiera ubicar algún equipo dentro de estas zonas, dicho equipo debe ser objeto de controles complementarios de acceso físico.

2.4.1.6. Sólo personal autorizado por el responsable de cada zona restringida de procesamiento puede ingresar a dicha zona.

2.4.1.7. Se debe generar y mantener registro de los accesos de personal externo a las zonas restringidas de procesamiento que contengan infraestructura crítica de TI. El periodo de retención para estos registros es de tres meses como mínimo.

2.4.1.8. En el caso particular del centro de cómputo, se debe generar y mantener registro de los accesos de personal tanto interno como externo. El periodo de retención para estos registros es de tres meses como mínimo.

2.4.1.9. El personal no autorizado interno o externo sin acompañamiento dentro de las zonas restringidas de procesamiento debe ser retirado de dicho lugar y además debe notificarse al responsable de la zona restringida de procesamiento respectiva.

2.4.1.10. Los privilegios de acceso a las zonas restringidas de procesamiento deben ser revisados al menos cada trimestre.

2.4.1.11. Las zonas restringidas de procesamiento deben estar dispuestas para brindar condiciones ambientales adecuadas (como temperatura y humedad) para mantener de forma óptima los recursos y la información allí alojados.

2.4.2. Seguridad física de los equipos

2.4.2.1. Siempre que se reutilice un servidor, computador portátil o un computador de estación de trabajo, se requiere la realización previa de un formateo de la información almacenada en dichos equipos antes que sean entregados a los nuevos usuarios.

2.4.2.2. Debe realizarse Borrado Seguro de los equipos de forma previa al proceso de disposición final (por ejemplo: venta, donación o destrucción).

2.4.2.3. Los servidores deben estar ubicados de modo que se reduzcan los riesgos generados por amenazas del entorno (es decir, evitando daños derivados de situaciones como manifestaciones sociales, inundaciones, humedad o incendio).

2.4.2.4. Todos los equipos de procesamiento críticos deben tener controles para evitar caídas de la plataforma de TI causadas por fallas en el servicio eléctrico.

2.5. CONTROL DE ACCESO A PLATAFORMAS DE TECNOLOGÍA DE LA INFORMACIÓN

La Personería Municipal de Itagüí otorga el nivel de acceso a la información necesario para el cabal cumplimiento de las funciones.
Busca evitar y mitigar riesgos que comprometan la confidencialidad de la información y de las plataformas T.I.C. institucionales.

2.5.1. Proceso de control de acceso

2.5.1.1. El control de acceso es una característica indispensable para las plataformas de tecnología de la información de la Personería Municipal de Itagüí.

2.5.1.2. Todo proceso de control de acceso debe tener un responsable de su gestión.

2.5.1.3. La gestión del proceso de control de acceso debe comprender las actividades de solicitud, aprobación, asignación, modificación y revocación del acceso.

2.5.1.4. Cuando aplique, las medidas de control de acceso a las plataformas de tecnología de la información deben cumplir el Criterio de seguridad de la información.

2.5.1.5. El acceso remoto a plataformas de tecnología de la información de la Personería Municipal de Itagüí debe ser autorizado por los dueños de las plataformas respectivas.

2.5.1.6. El acceso remoto a plataformas de tecnología de la información de la Personería Municipal de Itagüí debe ser realizado a través de VPN u otros medios que garanticen la seguridad en la comunicación.

2.5.2. Gestión de acceso a usuarios

2.5.2.1. Las cuentas de administración de las Plataformas de tecnología de la información sólo deben ser usadas cuando sea necesario dicho privilegio.

2.5.3. Manejo de contraseñas

2.5.3.1. Los nombres de usuario y contraseñas se rigen por el Criterio de seguridad de la información de la Personería Municipal de Itagüí.

2.5.3.2. No se permite el uso de contraseñas fijas. Todos los funcionarios sin excepción deben cambiar su password según lo establecido en el Criterio de seguridad de la Información.

2.5.3.3. Las contraseñas de administración de las Plataformas de tecnología de la información de la Personería Municipal de Itagüí podrán ser escritas en medios físicos o electrónicos únicamente si son objeto de medidas de seguridad física y/o lógica, según lo establecido en el Criterio de seguridad de la información de la Personería Municipal de Itagüí.

2.5.3.4. Las contraseñas de administración de las Plataforma de T.I.C. de tener un tiempo de caducidad, o en su defecto, deben ser cambiadas periódicamente. El periodo de vigencia de las contraseñas de administración de plataforma de T.I. se establece en el Criterio de Seguridad de la Información. (A desarrollar por la entidad).

2.6. OPERACIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

La Personería Municipal de Itagüí aplica controles para el funcionamiento correcto y seguro de las Plataformas de tecnología de la información y Telecomunicaciones.
Busca proteger la operación de las plataformas de T.I.C. institucionales, garantizando la continuidad y la seguridad de los procesos institucionales.

2.6.1. Requisitos para la planeación y operación de las plataformas de TI

2.6.1.1. Las nuevas plataformas o soluciones de tecnologías de la información de la Personería Municipal de Itagüí deben ser analizadas en la fase de planificación con el fin de identificar los requisitos funcionales y de seguridad de la información.

2.6.1.2. Toda intervención a las Plataformas de Tecnologías de la Información que impliquen modificaciones o cambios debe ser ejecutada de conformidad a lo establecido en el procedimiento de control de cambios.

2.6.1.3. Las Plataformas Tecnológicas de la Entidad deben ser configuradas de conformidad con el Criterio de seguridad de la información de la Personería Municipal de Itagüí.

2.6.1.4. La realización de auditorías, verificaciones o pruebas de seguridad de la información no deben afectar la normal operación de las Plataformas de tecnología de la información.

2.6.2. Protección contra software malicioso y móvil

2.6.2.1. La plataforma de T.I de la Personería Municipal de Itagüí debe ser objeto de protección frente software malicioso.

2.6.3. Respaldo de la información

2.6.3.1. La información importante de la entidad alojada en los repositorios de red y los sistemas de información críticos deben ser respaldados a intervalos programados.

2.6.3.2. Los respaldos de información deben ser probados regularmente, para verificar que la información si es recuperable ante un incidente.

2.6.3.3. Los respaldos de información deben almacenarse además en un lugar externo a la Personería Municipal de Itagüí, evitando que ante la posibilidad de un desastre al interior de la misma, se pierda por completo la información.

2.6.4. Intercambio de información

2.6.4.1. Las direcciones IP internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la entidad, deberán ser considerados y tratados como información clasificada.

2.6.4.2. La creación de una conexión directa entre las Plataformas de tecnología de la información de la Personería Municipal de Itagüí y las organizaciones externas a través de Internet o cualquier otra red pública, debe estar autorizada por el Grupo de Seguridad de la Información.

2.7. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Los aplicativos y sistemas de información de la Personería Municipal de Itagüí deben ser asegurados en sus fases de planeación, adquisición, desarrollo, implementación y operación.
Se busca mitigar los riesgos de seguridad asociados a la existencia de seguridad en los aplicativos y sistemas de información de la entidad.

2.7.1. Requerimientos de seguridad de los sistemas de información

2.7.1.1. Durante la etapa de definición de requisitos para desarrollar, adquirir o modificar un aplicativo, se deben especificar claramente todos aquellos requisitos concernientes a la seguridad. Debe existir un registro que evidencie la documentación de tales requisitos.

2.7.1.2. Los requisitos de seguridad de los aplicativos deben incorporar los lineamientos del Criterio de seguridad de la información de la Personería Municipal de Itagüí aplicables o aquellos que sean definidos por el grupo de seguridad de la información.

2.7.1.3. La contratación de un desarrollo a medida, adquisición de software o sistemas de información debe incluir entrenamiento en administración de las funciones de seguridad de dichas aplicaciones.

2.7.1.4. La contratación de un desarrollo a medida, adquisición o modificación de software o sistemas de información debe incluir la entrega de la documentación y la transferencia de conocimiento técnico y operativo suficiente al personal de soporte de la Personería Municipal de Itagüí.

2.7.1.5. Deben definirse requisitos previos a la contratación de proveedores de desarrollo o soporte de software y sistemas de información que incluyan:

- Aseguramiento de la disponibilidad y continuidad del servicio.
- Condiciones para la entrega de código fuente a la Personería Municipal de Itagüí (por ejemplo: ante el incumplimiento del proveedor) cuando el código fuente no sea propiedad de la entidad.
- Acuerdos de niveles de servicio (ANS) adecuados a la criticidad de la aplicación desarrollada o soportada por el proveedor.
- Requisitos de seguridad, al menos los listados en el instructivo “Requisitos de seguridad para desarrollo de aplicaciones Web”, en el caso desarrollo de aplicativos web.
- La realización de verificaciones de la seguridad a la aplicación; ya sean estas auditorías al código fuente o pruebas de seguridad.

2.7.2. Gestión de vulnerabilidades técnicas

2.7.2.1. Se debe verificar que el procesamiento del aplicativo es correcto, tanto en ambiente de pruebas como de producción, así como el cumplimiento de los requisitos definidos en la etapa de planeación.

2.7.2.2. Los administradores de las plataforma de T.I.C. son responsables de remediar las vulnerabilidades de seguridad que sean identificadas en las tecnologías bajo administración.

2.7.2.3. Las vulnerabilidades técnicas de las Plataformas de tecnología de la información deben ser objeto de un procedimiento de gestión orientado a la remediación de dichas vulnerabilidades.

2.7.3. Cifrado

2.7.3.1. Los controles de cifrado empleados en la entidad deben seguir los requerimientos del Criterio de seguridad de la información de la Personería Municipal de Itagüí.

2.7.3.2. Las llaves criptográficas deben tener un custodio designado.

2.7.3.3. Se debe mantener un inventario de las llaves criptográficas que son responsabilidad de informática.

2.7.4. Seguridad de los archivos del sistema

2.7.4.1. El personal de desarrollo de sistemas de información no debe tener facultad para trasladar o modificar software al ambiente de pruebas ni al ambiente de producción.

2.7.4.2. A menos que se obtenga un permiso por escrito del propietario de la información (dueño de las bases de datos) toda prueba a sistemas de

información (o a funcionalidades de estos) diseñados para manejar información reservada o clasificada:

- Debe llevarse a cabo con datos que no sean clasificados o reservados.
- Deben emplearse soluciones de ofuscación datos, que impidan la correlación de la información por parte de eventuales atacantes.

2.7.4.3. Sólo el personal responsable del desarrollo de software debe tener acceso al código fuente.

2.8. DISPOSITIVOS MÓVILES

El acceso a los datos y sistemas de información de la Personería Municipal de Itagüí a través de dispositivos móviles debe ser realizado de forma regulada y controlada con el fin de evitar incidentes de seguridad de la información.
Busca evitar que las actividades de teletrabajo generen situaciones que amenacen la disponibilidad, la integridad y la confidencialidad de la información de la Personería Municipal de Itagüí.

2.8.1. Computadores portátiles

2.8.1.1. Los computadores portátiles de la entidad deben tener instalada una herramienta de cifrado de datos que impida la fuga de información en caso de robo, pérdida o intentos de acceso no autorizado al equipo.

KENY WILLER GIRALDO SERNA
Personero Municipal