POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

CONTENIDO

1 INTRODUCCION

Las políticas de seguridad definidas en el presente documento están dirigidas a los servidores públicos de la Alcaldía de Ibagué y partes interesadas, las cuales serán de obligatorio cumplimiento, a fin de proteger la información y otros activos informáticos, de amenazas y vulnerabilidades y garantizar la integridad, confidencialidad y disponibilidad de la información.

Con la definición de las políticas y estándares de seguridad informática, se busca establecer en el interior de la Alcaldía Municipal de Ibagué una cultura de calidad operando en una forma confiable,

Las políticas y controles establecidas son concordantes con lo el Anexo A de la norma ISO: 27001:2013, en el marco de la implementación del Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información de la política de Gobierno Digital de MIPG.

La información es considerada un activo esencial en las actividades de la organización, es por ello que se deben establecer estrategias que permitan el control y administración de los datos, así como el uso adecuado de los recursos informáticos tanto de Hardware como de Software. De ahí la importancia de definir y dar a conocer políticas y procedimientos de seguridad que permitan proteger los Activos de Información de las amenazas a las que se encuentra expuesto por el uso de tecnologías de la información, y de esta manera asegurar la continuidad de los procesos y el logro de los objetivos institucionales.

2 OBJETIVO

Las políticas de seguridad de la información, comprende un conjunto de reglas a ser aplicadas a todas las actividades relacionadas con los sistemas de información que soportan los procesos críticos de la Entidad, con el objeto de:

- Garantizar la integridad, confidencialidad y disponibilidad de la información
- Proteger los recursos tecnológicos.
- Minimizar el riesgo en los procesos críticos de la Entidad
- Cumplir con los principios de la función Administrativa
- Apoyar la innovación tecnológica
- Implementar el Sistema de Gestión de la Seguridad Informática SGSI
- Fortalecer la cultura de autocontrol de la información
- Garantizar la continuidad de los procesos frente a los incidentes.

3 ALCANCE

Las políticas de seguridad de la información y los controles son de obligatorio cumplimiento para todos los servidores públicos de planta, contratistas y terceros que generen, administren, custodien o hagan uso de los activos de información de la Alcaldía de Ibagué.

El incumplimiento a lo establecido en el presente documento, podrá presumirse como causa de responsabilidad administrativa y/o disciplinaria, dependiendo de su naturaleza y gravedad, cuya sanción será aplicada por las autoridades competentes.

Las excepciones al cumplimiento de las políticas de seguridad de la información serán autorizadas única y exclusivamente por la Secretaría de las TIC, cuando se considere que su impacto es negativo para la continuidad de los procesos o logro de los objetivos institucionales, y deberán ser documentadas formalmente.

4 TERMINOLOGIA Y DEFINICIONES

Activo: En relación con la seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Según [ISO/IEC 13335-1:2004]: Cualquier cosa que tiene valor para la organización.

Administrador de equipo: Persona responsable de configurar, administrar controladores de dominio o equipos locales, sus cuentas de usuario, asignar contraseñas, permisos y ayudar a los usuarios a solucionar problemas de red.

Administrador de Bases de Datos (DBA): Persona responsable de los aspectos ambientales de una base de datos.

Amenaza: Según [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Antivirus: Programa que busca y eventualmente elimina los virus informáticos que pueden haber infectado un disco rígido, o cualquier sistema de almacenamiento electrónico de información.

Ataque: Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Backup: Es una copia de los datos originales que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida.

Base de Datos: Es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados. Según [ISO/IEC 13335-1:2004]: Característica o propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

Control de Acceso: Es un mecanismo de seguridad diseñado para prevenir, salvaguardar y detectar acceso no autorizado y permitir acceso autorizado a un activo.

Criptografía: Protección de la información mediante el uso de códigos y cifrados. La información que se utiliza para el cifrado se conoce como la clave. La forma particular en que una clave cambia la información se denomina algoritmo.

Disponibilidad: Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran. Según [ISO/IEC 13335-1:2004]: Característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

Firewall: también llamado cortafuegos, es un sistema cuya función es prevenir y proteger una red privada, de intrusiones o ataques de otras redes, bloqueándole el acceso. Permite el tráfico entrante y saliente que hay entre redes u ordenadores de una misma red.

Hardware: Se refiere a las características técnicas y físicas de las computadoras.

Integridad: Se refiere a la pérdida o deficiencia en la autorización, totalidad o exactitud de la información de la organización. Es un principio de seguridad que

asegura que la información y los sistemas de información no sean modificados de forma intencional.

IP: Etiqueta numérica que identifica de manera lógica y jerárquica a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente un computador) dentro de una red que utilice el protocolo IP.

OFUSCAMIENTO: la ofuscación de datos, que también se conoce como enmascaramiento de datos, es el proceso de reemplazar información sensible existente en entornos de prueba o de desarrollo con la información que parece información real de producción, pero que no sirve para alguien que desee darle mal uso

ON SITE: En sitio**.**

Plan de Contingencia: Es un instrumento de gestión para el buen gobierno de las Tecnologías de la Información y las Comunicaciones en el dominio del soporte y el desempeño.

Redes: Es un término que se utiliza en informática para designar la conexión de nodos sin necesidad de una conexión física (cables), ésta se da por medio de ondas electromagnéticas. La transmisión y la recepción se realizan a través de puertos.

Riesgo: Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.

Servidores: Computador que responde peticiones o comandos de un computador cliente. El cliente y el servidor trabajan conjuntamente para llevar a cabo funciones de aplicaciones distribuidas. El servidor es el elemento que cumple con la colaboración en la arquitectura cliente-servidor.

SGSI: Sistema de Gestión de Seguridad de la Información

Sistemas de Información: 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 u objetivo.

Software: Programas y documentación de respaldo que permite y facilita el uso del pc. El software controla la operación del hardware.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

5 POLÍTICAS DE LA SEGURIDAD

5.1 Orientación de la dirección para la gestión de la seguridad de la información

Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.

5.1.1 Políticas para la seguridad de la información

La Alcaldía de Ibagué ha establecido las siguientes políticas de seguridad, las cuales representan el interés de la Administración de proteger los Activos de Información.

Las políticas de seguridad de la información estarán contenidas en un documento que surtirá el trámite de aprobación de conformidad con el procedimiento de control de documentos y será publicado y comunicado a todos los servidores públicos por la Secretaría de las TIC.

Las políticas de seguridad de la información serán objeto de evaluación anual, aplicando mecanismos de autocontrol y autoevaluación, para garantizar el mejoramiento continuo.

5.1.2 Revisión de las políticas para la seguridad de la información

Las políticas para la seguridad de la información serán revisadas por el comité de Seguridad anualmente o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúa.

6 POLITICAS DE ORGANIZACIÓN DE LA SEGURIDAD

6.1 Organización interna

.

Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización

6.1.1 Roles y responsabilidades para la seguridad de la información

Las responsabilidades y roles de la Seguridad de la información se encuentran definidas en la Política General del SGSI, el plan de Incidentes y Plan de Continuidad del Negocio,

6.1.2 Separación de deberes

Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.

6.1.3 Contacto con las autoridades

Se deben mantener contactos apropiados con las autoridades pertinentes, Fiscalía, Entes de control, Policía Nacional, entre otras.

6.1.4 Contacto con grupos de interés especial

Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad, tales como:

ColCERT (Grupo de respuesta a emergencias cibernéticas de Colombia)

CSIRT PONAL (Computer Security Incident Response Team -Centro de Centro de Respuesta a Incidentes de Seguridad cibernéticos de la Policía Nal),

CSIRT Gobierno

CPP (Centro Cibernético Policial de la Policía Nacional)

6.1.5 Seguridad de la información en la gestión de proyectos

La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.

6.2 Política para Uso de Dispositivos Móviles y Teletrabajo

Objetivo: Garantizar la seguridad del teletrabajo, y el uso de dispositivos móviles.

6.2.1 Política para dispositivos móviles

Todos los colaboradores y terceros son responsables de garantizar el buen uso de los dispositivos móviles (equipos portátiles, teléfonos móviles, tabletas entre otras) en redes seguras y con la protección adecuada para evitar acceso o divulgación de información no autorizada.

El almacén General de la Alcaldía llevará un registro y control de los dispositivos moviles que son asignados para el desempeño de las funciones laborales.

Los dispositivos moviles asignados para el desempeño de las funciones laborales, serán configurados por la Secretaría de las TIC, teniendo en cuenta los siguientes criterios:

- Los Dispositivos móviles contarán con un sistema de autenticación, como un patrón o contraseña
- Instalar y configurar el software de antivirus
- Bloqueo de pantalla para un mínimo de 3 minutos de inactividad
- Configurar la opción de borrado remoto de información en los dispositivos móviles.

El personal responsable del dispositivo móvil debe hacer periódicamente copias de respaldo.

Los usuarios de los dispositivos móviles no están autorizados para realizar instalación de aplicaciones, ni reinstalar el sistema operativo.

En caso de pérdida o hurto de dispositivos móviles que almacenen información de la Entidad, se debe reportar la perdida a la Secretaría de las TIC de manera inmediata.

En los dispositivos móviles de propiedad de la Alcaldía, no es permitido almacenar información personal.

Los colaboradores que utilicen dispositivos móviles diferentes a los asignados por la Entidad, deben aceptar en el instrumento que indique la Secretaría de las TIC, el cumplimiento de la política de dispositivos móviles, así como las configuraciones de seguridad establecidas,

La Secretaría de las TIC debe asegurarse que los dispositivos móviles de propiedad de terceros que sean configurados en la red de la Entidad cumplan con las configuraciones de seguridad establecidas.

La Secretaría de las TIC se reserva el derecho de realizar verificaciones de las configuraciones en dispositivos móviles y el cumplimiento de la política, en dispositivos móviles de propiedad de la Alcaldía o de terceros.

6.2.2 Política para el Teletrabajo

La Secretaría de las TIC, La Secretaría Administrativa y el líder de proceso y/o jefe inmediato del teletrabajador deben definir las medidas de seguridad para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo o el trabajo en casa, para lo cual se tendrá en cuenta:

- A qué servicios y entornos podrán acceder los teletrabajadores.
- A qué información podrán acceder, cumplimiento de la política y control de acceso.
- Qué controles de acceso adicionales se implementarán para los teletrabajadores. Esto incluye contraseñas o métodos de autenticación exclusivos para el teletrabajo.
- Qué mecanismos de protección (antivirus, restricciones de descarga de aplicaciones, control de actualizaciones entre otras) se implementarán para dispositivos utilizados para el teletrabajo.

- Responsabilidad de la custodia, preservación y almacenamiento de la información
- Protección de los recursos tangibles que son de propiedad de la Entidad y que quedan a cargo del trabajador.
- Análisis de riesgos de la actividad de teletrabajo o trabajo en casa.
- La Secretaría Administrativa llevará un control de las personas que se encuentran laborando en teletrabajo o trabajo en casa

7 POLITICA DE SEGURIDAD DE LOS RECURSOS HUMANOS

7.1 Antes de asumir el empleo

Objetivo: Asegurar que los empleados y contratistas de prestación de servicios profesionales y de apoyo a la gestión, comprendan sus responsabilidades y sean idóneos en los roles para los que se consideran.

7.1.1 Selección

Las verificaciones de los antecedentes de todos los candidatos a un Empleo independiente del tipo de vinculación, se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos del empleo o necesidad del servicio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.

7.1.2 Términos y condiciones del empleo

Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información, con el propósito de reducir los riesgos y de esta manera asegurar la integridad, confidencialidad y disponibilidad de la información.

La Oficina de contratación asegurará que las minutas de los contratos y convenios, independientemente de su naturaleza o modalidad, contenga cláusulas y obligaciones frente al cumplimiento de las políticas de seguridad de la información, y demás disposiciones del Sistema de Seguridad de la Información, las cuales deberán ser divulgadas a través de los supervisores de los contratos.

Los estudiantes, funcionarios, contratistas y proveedores deben dar aprobación a la Alcaldía de Ibagué, para el tratamiento de sus datos personales de conformidad con las disposiciones legales y acuerdo de confidencialidad, lo cual se realizará a la firma del contrato o posesión del cargo.

7.2 Durante la ejecución del empleo

Objetivo: Asegurarse de que los servidores públicos y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.

7.2.1 Responsabilidades de la dirección

La alta dirección debe exigir a todos los servidores públicos y contratistas la aplicación
de las disposiciones del Sistema de Gestión de seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la Entidad.

7.2.2 Toma de conciencia, educación y formación en la seguridad de la información

Todos los servidores públicos, pasantes y contratistas de prestación de servicios profesionales y de apoyo a la gestión, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.

La Dirección del Talento Humano incluirá en el programa de inducción, reinducción y capacitación, temáticas orientadas a generar conciencia y apropiación en los servidores públicos de la Entidad, sobre sus responsabilidades en el marco de la política de Seguridad de la información y demás disposiciones del Sistema de Gestión de Seguridad de la información.

La Secretaría de las TIC y los Administradores de los Sistemas de información implementarán mecanismos que garanticen que los usuarios de los sistemas de información han recibido la inducción, entrenamiento o capacitación en el manejo de la herramienta tecnológica con la cual va a interactuar en el desarrollo de sus funciones o del objeto contractual, según sea el caso.

7.2.3 Proceso disciplinario

La Alcaldía de Ibagué debe contar con un proceso o procedimiento formal de control disciplinario, que permita emprender acciones contra quienes hayan cometido violación a la seguridad de la información, se les aplicará lo establecido en la ley, particularmente en el Código Único Disciplinario, el Estatuto Anticorrupción y demás normas que las adicionen, modifiquen, reglamenten o complementen.

Dicho proceso o procedimiento, debe ser comunicado a todo el personal de planta, pasantes y de prestación de servicios profesionales y de apoyo a la gestión, en el desarrollo de los programas de inducción, reinducción y capacitación.

De los informes derivados del desarrollo del proceso de Gestión de Incidentes de Seguridad y teniendo en cuenta el impacto y las responsabilidades identificadas, se tomarán acciones y se realizará el respectivo traslado ante las instancias correspondientes.

7.3 Terminación y cambio de empleo

Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.

7.3.1 Terminación o cambio de responsabilidades de empleo

Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.

Todo el personal de planta, de prestación de servicios profesionales y de apoyo a la gestión, pasantes y demás proveedores, en el momento del retiro ya sea por desvinculación definitiva o temporal, traslado, terminación del contrato, o cualquier otra situación administrativa similar, entregará al jefe inmediato o supervisor según sea el caso, toda la información en medio físico o digital que en el ejercicio de sus funciones haya generado, procesado o almacenado, lo cual quedará registrado en el formato certificación entrega de elementos -paz y salvo, implementado en el proceso de Gestión del Talento Humano

8 POLITICA DE GESTION DE ACTIVOS DE INFORMACION

8.1 Responsabilidad por los activos

Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.

8.1.1 Inventario de activos

Los activos de información serán identificados conjuntamente por la Secretaría de las TIC, la Unidad Administrativa líder del proceso de Gestión Documental, Recursos físicos y Almacén, quienes mantendrán actualizado el inventario de activos de información.

Para la elaboración del inventario de activos de información, se deben realizar las siguientes actividades:

- Identificar los activos de información que dan soporte al negocio
- Clasificar los activos por su importancia
- Clasificar los activos por el tipo de activo o información
- Identificar al propietario del activo

Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.

8.1.2 Propiedad de los activos

El inventario de activos de información (tangibles e intangibles), en todo caso tendrá definido el propietario y el custodio para cada uno de los activos, el cual podrá ser una unidad administrativa de la entidad, un cargo, proceso, o grupo de trabajo que crea, gestiona su transferencia, almacenamiento o disposición final, es decir el que gestiona el activo debe ser el propietario.

El propietario del activo de información tiene la responsabilidad de:

- asegurar que los activos son inventariados, clasificados y protegidos adecuadamente.
- Definir y revisar periódicamente las restricciones de acceso y las clasificaciones de activos importantes, teniendo en cuenta la política de control de acceso.
- Garantizar el manejo adecuado cuando el activo es eliminado o destruido.

8.1.3 Uso aceptable de los activos

La Alcaldía de Ibagué, a través de la Secretaría de las TIC, establecerá y divulgará los lineamientos específicos para la identificación, clasificación, rotulado, valoración y buen uso de los activos de información.

La Secretaría de las TIC, diseñará una metodología que le permita identificar, clasificar, valorar y controlar los activos de información, para garantizar su uso, protección y recuperación ante desastres, discriminado por procesos y dependencias, y determinará su criticidad, clasificación, ubicación y responsable

8.1.4 Devolución de activos

Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.

El área de Talento Humano y de Contratación deben formalizar el proceso de finalización del vínculo laboral o contractual, incluyendo el requisito o cláusula de devolución de activos físicos y electrónicos, según sea el caso.

La Secretaría de las TIC, establecerá procedimientos de transferencia y borrado de información de forma segura, en el caso que sea pertinente por el uso de equipos de cómputo propios, transferencia y devolución de equipos.

8.2 Clasificación de la información

Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la Entidad

8.2.1 Clasificación de la información

La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.

La unidad Administrativa líder del proceso de Gestión Documental, será la responsable de mantener actualizado el índice de información clasificada y reservada, de conformidad con la normatividad vigente.

El esquema de clasificación de la información estará basado en los criterios de confidencialidad, integridad y disponibilidad.

La Clasificación del activo se revisará con una periodicidad anual y se mantendrá actualizada.

8.2.2 Etiquetado de la información

La Secretaría de las TIC y la unidad Administrativa líder del proceso de Gestión Documental, desarrollará e implementará un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado, el cual debe ser comunicado a todo el personal de planta, contratistas de prestación de servicios profesionales y de apoyo a la gestión, pasantes y proveedores.

La identificación de las carpetas y archivos debe ser lógico y de fácil identificación, y debe cumplir con los estándares de nombramiento establecidos por la Secretaría de las TIC.

8.2.3 Manejo de activos

Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la Entidad, los cuales incluyen el manejo de los activos, su procesamiento, almacenamiento y la forma de comunicar la información.

8.3 Manejo de medios

Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.

8.3.1 Gestión de medios removibles

Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación y Plan de preservación digital adoptado por la organización, los cuales deben contener:

- La necesidad de su uso
- los soportes reutilizables que deberían retirarse de la Entidad y hacerse irrecuperables
- Cuando sea práctico requerir autorización para su uso
- Mantener un registro de altas y bajas
- Considerar especificaciones de almacenamiento según especificaciones del fabricante
- Encriptar datos para proteger aquellos que se consideren importantes
- Renovar dispositivos con un periodo determinado para evitar la degradación de datos necesarios e importantes
- Proteger la información almacenada con copias de seguridad en soportes independientes
- Crear un registro de soportes extraíbles para limitar la posibilidad de pérdida de datos
- Controlar la transferencia de información hacia medios extraíbles
- Documentar los procedimientos de autorización

Los servidores públicos que contengan información confidencial de propiedad de la Entidad en medios de almacenamiento removibles, deben protegerlos del acceso lógico y físico, asegurándose además que el contenido se encuentre libre de virus y software malicioso, a fin de garantizar la integridad, confidencialidad y disponibilidad de la información.

Los medios de almacenamiento con información crítica que requieran ser enviados a un tercero en cumplimiento de la política de copias externas, deben ser manipulados única y exclusivamente por la persona asignada por el o la titular de la Secretaría de las TIC para hacer respaldos y salvaguardar información.

Todo medio de almacenamiento con copias de seguridad debe ser marcado de acuerdo a la información que almacena, detallando su contenido. Toda copia de respaldo que se encuentre en medios de almacenamiento removible deberá ser guardada bien sea en caja bajo llave o en un lugar seguro, al cual solo tendrá acceso el responsable de esta

No está autorizado el uso de los dispositivos de almacenamiento externos removibles que contenga información de la Entidad, en lugares de acceso público como cibercafés o en equipos que no garanticen la confiabilidad e integridad de la información.

La información de la Entidad clasificada como confidencial que sea transportada en medios de almacenamiento removible, debe ser protegida mediante cifrado o contraseñas, para garantizar que no pueda ser vista por terceros en caso de robo o extravío.

Los equipos servidores tendrán deshabilitada la reproducción automática de dispositivos externos de almacenamiento removibles.

8.3.2 Disposición de los medios

La Secretaría de las TIC debe establecer procedimientos para la eliminación segura de soportes a la finalización de su uso, para tal efecto es necesario:

- Identificar qué dispositivos requieren de un proceso de eliminación segura
- Controlar la utilización de empresas externas para la realización de tareas de eliminación segura estableciendo algún tipo de control
- Mantener un registro de dispositivos que han sido dados de baja de forma segura por contener información sensible

8.3.3 Transferencia de medios físicos

La Dirección de Recursos Físicos establecerá mecanismos de control para proteger la información contra acceso no autorizado, uso indebido o corrupción durante el

transporte, cuando los soportes necesitan ser trasladados entre distintas ubicaciones, los cuales contemplaran, entre otros:

- El registro de salida de los soportes para su cotejamiento con el transportista y el lugar de destino de mismo incluyendo un control de tiempos de transporte
- Control de transportistas (Utilizar transportistas de confianza)
- Mantener una lista de transportistas autorizados
- Controlar la identificación del transportista o mensajero
- Establecer un procedimiento de cifrado cuando sea necesario y posible
- Controlar los embalajes y las condiciones ambientales (Humedad, temperatura, polvo etc.) con las especificaciones del fabricante.

9 POLITICA CONTROL DE ACCESO

9.1 Requisitos del negocio para control de acceso

Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información para evitar el acceso no autorizado.

9.1.1. Control de acceso a los Sistemas de Información

Las tareas realizadas por los usuarios en cada uno de los sistemas de información de la Alcaldía de Ibagué, serán controladas por medio de la creación de cuentas de usuario a los cuales se les controlarán los privilegios de acceso, modificación y eliminación, de conformidad con los roles y perfiles establecidos.

9.1.2 Acceso a redes y a servicios en red

Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.

La Secretaría de las TIC contará con personal capacitado, responsable de la configuración y administración de las redes de tal forma que se garantice el control de acceso y la restricción de privilegios, dando aplicación al protocolo que se establezca para tal fin.

La Secretaría de las TIC implementará control de tráfico de red a través de firewall y será la responsable del control de asignación y del direccionamiento IP de cada uno de los equipos conectados que forman parte de la red con acceso a internet de la Alcaldía de Ibagué, dicho registro debe contener la siguiente información mínima:

1. Fecha en que es asignada la IP
2. Nombre del funcionario
3. Placa del equipo
4. Dependencia
5. Numero de IP
6. Firma de la persona a la que se le asignó la IP

Los usuarios de la Red de la Alcaldía de Ibagué no deben establecer redes de área local, conexión remota a redes internas o externas, o transferir archivos a través del FTP, utilizando la red de la Entidad sin autorización previa de la Secretaría de las TIC.

El acceso a la Red Inalámbrica de la Alcaldía de Ibagué a través de equipos de telefonía móvil será restringido por la Secretaría de las TIC, a fin de minimizar los riesgos y mejorar la velocidad en la navegación desde equipos portátiles, siendo este el fin principal de este tipo de tecnología.

9.1.2.1 Acceso a Internet, Intranet y edición Portal WEB

El acceso a Internet e Intranet es permitido a todos los servidores públicos para facilitar el desarrollo de los procesos propios de la Entidad, no obstante, están obligados a cumplir con los controles de acceso y uso implementados por la Secretaría de las TIC

La Secretaría de las TIC, será quien autorice el uso de servicios de computación en la nube, previa verificación de la seguridad de la información y siempre que esta no sea clasificada como confidencial.

La Secretaría de las TIC creará los siguientes perfiles de usuario, con los cuales se pretende controlar el acceso a internet, descongestionar el ancho de banda y garantizar la seguridad de la información.

Perfil No 1 Administrador: Corresponde a usuarios con funciones de Administradores de los sistemas de Información, con permisos para descargar archivos ejecutables

Perfil No 2. Comunicador: Usuarios de la oficina de prensa, cultura y otros que para el cumplimiento de sus funciones requieran acceso a redes sociales, reproducción de videos, emisoras en línea, sin permisos para descarga de archivos ejecutables

Perfil No 3 Comunicación General: Usuarios con acceso a redes sociales, reproducción de videos y restricción a emisoras en línea.

Perfil No 4 General: Corresponde a usuarios con acceso a internet y restricción a redes sociales, reproducción de videos y emisoras en línea.

Perfil No.5 Capacitación: Corresponde a usuarios con perfil general y acceso a reproducción de videos y redes sociales por un periodo de tiempo limitado.

Los canales de acceso a internet de la Entidad no podrán ser usados para fines diferentes a los requeridos en el desarrollo de las actividades propias de los cargos. Esta restricción incluye el acceso a páginas con contenido pornográfico, terrorismo, juegos en línea, actividades ilegales o que atenten contra la ética y el buen nombre del a Entidad o de las personas, redes sociales y demás cuyo contenido no sea obligatorio para desarrollar las labores encomendadas al cargo.

La Alcaldía de Ibagué se reserva el derecho a registrar los accesos y monitorear el contenido al que el usuario puede acceder a través de Internet desde los recursos y servicios de Internet de la Entidad.

El uso de Internet para la revisión de correo electrónico personal, en cumplimiento de actividades propias de la Entidad, está autorizado siempre y cuando se observen los mismos lineamientos estipulados para la utilización del servicio de correo interno.

La actividad de descarga de software estará a cargo de la persona o grupo de personas definido por la Secretaría de las TIC, por lo tanto, los usuarios de internet no están autorizados para descargar software, música, juegos, películas, protectores de pantalla, etc. Así como efectuar pagos, compras de bienes o

servicios a través de los canales de acceso a internet de la Alcaldía a título personal o de la Entidad, salvo cuando medie autorización.

Los Usuarios de Internet no están autorizados para descargar herramientas o aplicaciones que comprometan la seguridad con actos como monitoreo de datos, sondeo, copias, prueba de firewalls o hacking entre otros

9.1.2.2 Acceso y uso de la Intranet

Las cuentas de acceso a Intranet serán administradas por la Secretaría de las TIC y serán creadas para personal de planta.

El personal vinculado por prestación de servicios de apoyo a la Gestión y Profesional podrán ser usuarios de la Intranet con previa autorización del Director o Secretario de la Dependencia en la cual se desempeña.

Para el uso de Intranet se deben observar las mismas normas de comportamiento definidas para el uso de internet.

9.1.2.3 Publicación Portal Web

Administración de los Contenidos Institucionales de las Páginas: La administración de los contenidos de la página Institucional estará a cargo de la Oficina de Comunicaciones, quienes serán los encargados de verificar los contenidos que pueden o deben ser publicados. Todo contenido deberá respetar la ley de derechos de autor.

Ningún contenido del portal WEB se puede copiar con fines comerciales, ni se puede copiar y utilizar en otros sitios WEB.

Podrá asignarse permisos a editores por parte de las Unidades Administrativas, quienes serán responsables de la información que publiquen.

Cuando por omisión un editor del portal web revele sus contraseñas, se hará responsable de todo lo realizado con este usuario.

9.2 Gestión de acceso de usuarios

Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.

9.2.1 Registro y cancelación del registro de usuarios

Aprobaciones Requeridas para la Creación de Usuarios y Permisos: Para la creación, actualización o bloqueo de cuentas de usuario a los sistemas de información, las solicitudes para dichas actividades deben contener de forma clara y precisa la siguiente información

1. Nombre completo del funcionario
2. Documento de identidad
3. Correo electrónico Para notificación de Contraseñas.
4. Tipo de Permiso (Consulta, Ingreso de información, Actualización de Información, Facturación)
5. Tipo de vinculación: (Personal de Planta o Prestación de Servicios)
6. Si es personal de prestación de servicios, la fecha final del contrato
7. En caso de solicitar acceso a más de un aplicativo se debe especificar por cada uno de ellos los permisos a los que va a tener derecho
8. Los permisos deben ser solicitados por el Director o Secretario responsable de cada uno de los módulos.
9. Solo es permitido el acceso a las bases de datos a través de software de gestión de base de datos, a los usuarios autorizados por la Secretaría de las TIC.

9.2.2 Suministro de acceso de usuarios

La notificación de asignación de credenciales de acceso a los usuarios de los diferentes Sistemas de Información, se enviará al correo electrónico personal del

usuario final, y este deberá cambiarla de manera inmediata al ingresar por primera vez al aplicativo.

9.2.3 Gestión de derechos de acceso privilegiado

Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado, los cuales, en todo caso, cumplirán con los requisitos establecidos en el control 9.2.1

9.2.4 Gestión de información de autenticación secreta de usuarios

La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.

En los sistemas de información de desarrollo propio de la Entidad o adquirido, se debe asegurar que la contraseña no sea visible en la pantalla al momento de ser ingresada.

9.2.5 Revisión de los derechos de acceso de usuarios

Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, con periodicidad trimestral, y reportar las novedades respectivas al administrador de los sistemas de información, mediante comunicación interna a través de la herramienta tecnológica implementada para la Gestión Documental.

9.2.6 Retiro o ajuste de los derechos de acceso

Los derechos de acceso de todos los empleados y de usuarios externos, a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se presenten cambios.

Para retirar o modificar privilegios de acceso a usuarios, el líder de cada proceso debe remitir al área o dependencia que administra el Sistema de Información, una comunicación interna a través de la herramienta tecnológica implementada para la Gestión Documental, informando la novedad respectiva.

La Dirección de Talento Humano reportará a la Secretaría de las TIC y demás Secretarías que administren sistemas de información, el traslado o retiro de los servidores públicos, a fin de ejercer control sobre el estado de los usuarios.

La vigencia del usuario y contraseñas a personal de contrato estará sujeta a la fecha de finalización del contrato, siendo responsabilidad de los jefes de cada unidad administrativa reportar a la Secretaría de las TIC o los Administradores de otros Sistemas de información, la novedad de retiro.

Los Administradores de los diferentes Sistemas de Información, controlarán y eliminarán los usuarios redundantes, con una periodicidad trimestral.

9.3 Responsabilidades de los usuarios

Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.

9.3.1 Uso de información de autenticación secreta

Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.

9.4 Control de acceso a sistemas y aplicaciones

Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.

9.4.1 Restricción de acceso a la información

9.4.1.1 Restricción de horarios

Cuando el propietario del Activo de Información (Sistema de Información lo requiera), se implementará control de acceso a los aplicativos en horarios los horarios autorizados, de tal forma que, si se requiere el ingreso en horario adicional al señalado, debe mediar autorización escrita del Director o Secretario de Despacho líder del proceso propietario de la información, indicando la hora de inicio, finalización y los días que debe estar autorizado.

9.4.1.2 Bloqueo por intentos

Los intentos fallidos de acceso al sistema de información antes del límite de tres intentos, despliegan un mensaje de advertencia indicando que el usuario no ha podido iniciar sesión debido a que los datos de usuario o password son incorrectos. Cuando los intentos fallidos superan el máximo de tres, se desplegará un mensaje de bloqueo de usuario, lo que implica que debe comunicarse con el administrador del sistema para el desbloqueo respectivo.

Cuando se advierte un incidente de seguridad, como medida de contención, los Administradores realizarán el bloqueo de la cuenta de usuario.

9.4.1.3 Cierre de Sesión:

Todos los usuarios deben cerrar sesión cuando no van a hacer más uso del aplicativo, o cuando van a abandonar su estación de trabajo.

9.4.2 Procedimiento de ingreso seguro

Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro, para tal efecto las contraseñas deben cumplir los controles establecidos en el numeral 9.4.3

9.4.3 Sistema de gestión de contraseñas

9..4.3.1 Cambio Forzoso de Todas las Contraseñas del Administrador

Siempre que se detecte un ingreso no autorizado al sistema de información, los administradores del sistema deben cambiar inmediatamente cada una de sus contraseñas.

9.4.3.2 Cambios de Contraseñas Periódicas para el Administrador

Todos los administradores deben cambiar la contraseña en el sistema, con una periodicidad mínima mensual, o cuando se presente un incidente de seguridad o adviertan una situación que ponga en riesgo la seguridad de la información.

9.4.3.3 Control de Acceso al Sistema con Contraseña Individual para cada Usuario

Se precisa que el control de acceso al sistema, se debe realizar por medio de Usuario único, es decir que no se puede tener el acceso a la base de datos y otros recursos del sistema si no se encuentra privilegiado con uno.

9.4.3.4 Longitud de la Contraseña de Usuario

Se debe tener en la longitud de las contraseñas un mínimo diez caracteres y una longitud máxima de cuarenta y cinco (45) caracteres.

Combinación de Mayúsculas (A a Z), minúsculas (a a z), dígitos (0 al 9) y caracteres no alfabéticos o especiales. Para el caso particular de los usuarios de la plataforma PISAMI, las contraseñas no podrán iniciar con números.

La nueva contraseña debe diferir de las contraseñas anteriores

La nueva contraseña no debe permitir incremento secuencial de contraseñas anteriores

Las letras deben alternar aleatoriamente mayúsculas y minúsculas

Cambio de contraseñas trimestral

No se debe utilizar como contraseña, ni contener, el nombre de usuario asociado a la contraseña.

Después de 3 (tres) intentos no exitosos de ingreso de la contraseña el usuario deberá ser bloqueado de manera inmediata y deberá comunicarse con la mesa de ayuda para que lo habilite

La Contraseña no debe ser visible en la pantalla al momento de ser ingresada

El sistema no debe permitir el autoguardado de la contraseña.

La estructura y complejidad de las contraseñas debe aplicar para la creación del usuario, recuperación y actualización de las mismas.

La modificación de la contraseña debe ser obligatoria en los siguientes casos: Cuando se ingresa por primera vez, cuando se ingresa con contraseña recuperada, cuando ha expirado a los 90 días. EL sistema no permitirá actuación alguna hasta que se actualice la contraseña.

Las contraseñas asignadas por creación de usuario y recuperación expiran a las 24 horas.

9.4.3.5 Entrega de Contraseñas a Usuarios

Las contraseñas no se divulgan por medio de líneas telefónicas, se envían por correo electrónico, y el usuario debe cambiarla de manera inmediata al ingresar por primera vez al aplicativo.

9.4.3.6 Confidencialidad de las contraseñas

Se precisa que las contraseñas nunca deben ser compartidas o reveladas a nadie más que al usuario autorizado. Hacerlo expone al usuario a responsabilizarse de acciones que otras personas hagan con su cuenta.

Los servidores públicos serán responsables de la confidencialidad de las contraseñas y bajo ninguna circunstancia la darán a conocer a otras personas, o harán uso de contraseñas ajenas, ni de la opción de autoguardado de contraseñas.

9.4.3.7 Cambio de contraseña cuando se sospecha que ha sido descubierta

Ante la posibilidad o sospecha de la perdida de confidencialidad de la contraseña, esta debe ser cambiada de manera inmediata y reportado el evento a la Secretaría de las

9.4.3.8 Cambio de Contraseñas Periódicas para los usuarios en el Sistema

Se precisa que todos los usuarios cambien periódicamente la contraseña en el sistema, mínimo trimestral, lo cual será un control implementado en los sistemas de información.

9.4.4 Uso de programas utilitarios privilegiados

En la Alcaldía de Ibagué no está permitido el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.

Para tal efecto, el personal técnico de la Secretaría de las TIC, podrá realizar los monitoreos respectivos, y en caso de encontrar una inobservancia al control, se notificará al líder del proceso y se interpondrá la queja ante la Oficina de Control único disciplinario, dependiendo del caso.

En la Alcaldía de Ibagué, no está autorizado el uso de software de acceso remoto, salvo en casos especiales, los cuales estarán debidamente autorizados por el Secretario Líder de proceso.

9.4.5 Control de acceso a códigos fuente de programas

Acceso al código fuente de producción estará asignado a un solo servidor público adscrito a la planta de personal de la Alcaldía de Ibagué.

EL Acceso al código fuente de programas de propiedad de la Alcaldía, estará restringido, sólo tendrá permisos, el personal ingeniero desarrollador de Software, para acceder a la carpeta específica en ambiente de pruebas, dependiendo del componente del Sistema que tenga a cargo. Los privilegios en ambiente de pruebas serán de lectura, escritura y ejecución.

En el momento de asignar los permisos de acceso al código fuente, el autorizado firmará el compromiso de confidencialidad.

La asignación de permisos de acceso al código fuente será autorizado por el Secretario líder del proceso, mediante comunicación escrita radicada en el sistema de información de Gestión Documental.

10 POLITICA DE CONTROLES CRIPTOGRAFICOS

10.1 Controles Criptográficos

Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.

10.1.1 Política sobre el uso de controles criptográficos

La Secretaría de las TIC dispondrá de herramientas que permitan el cifrado de la información clasificada y reservada para proteger la confidencialidad, integridad y disponibilidad y autenticidad de la información, lo cual se realizará por solicitud de los usuarios interesados o de manera general cuando así lo disponga la Entidad.

Las contraseñas de usuario o claves para el control de acceso a los sistemas de información deberán hacer uso de mecanismos criptográficos, así como los documentos o archivos que las contengan.

Los documentos que se han sido objeto de cifrado, serán almacenados y tratados con mecanismos de seguridad requeridos conforme al nivel de clasificación de la información.

Identificar los sistemas de información que transmiten información pública reservada y pública clasificada, para garantizar que cuente con mecanismos de cifrado de datos.

.

10.1.2 Gestión de llaves

Objetivo: desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.

La entrega de la clave criptográficas debe realizarse a través de un medio diferente al del envío del archivo.

Se debe asegurar la disponibilidad operativa de las claves criptográficas y su continuidad el tiempo que lo requiera el servicio criptográfico correspondiente.

La Secretaría de las TIC, controlará la información de las claves criptográficas, la cual debe contener como mínimo los siguientes criterios: Tipo de llave, servicio de seguridad (Autenticidad, integridad, irrefutabilidad, confidencialidad etc.), datos asociados a proteger, garantía requerida, periodo de protección.

11 POLITICA DE SEGURIDAD FISICA Y DEL ENTORNO

11.1 Áreas seguras

Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.

11.1.1 Perímetro de seguridad física

Los visitantes, personal de planta, pasante, contratistas de prestación de servicios profesionales y de apoyo a la gestión deben portar el carnet o escarapela en lugar visible, mientras permanezcan dentro de las Instalaciones de la Alcaldía.

La Secretaría Administrativa, Dirección de Recursos Físicos es la competente para definir el horario autorizado para el ingreso y permanencia de personal de planta, contratistas, pasantes y visitantes a las diferentes sedes de la Alcaldía, en horarios distintos se requerirá la autorización del jefe inmediato del área.

11.1.2 Controles de acceso físicos

Todos los centros de procesamiento de datos de la Entidad, centros de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia, son de acceso restringido únicamente a personal autorizado, por lo tanto, sus puertas deben contar con mecanismos de seguridad efectivos.

Toda actividad que se realice por terceros en las áreas de servidores y de procesamiento debe ser supervisada por el responsable de la Dependencia.

Los responsables de los centros de datos mantendrán un registro de todas las personas ajenas que ingrese a las áreas de servidores y de procesamiento de información, indicando, fecha, hora, nombre, actividad realizada, y nombre de quien autorizó

Las Instalaciones de procesamiento de información administradas por la Alcaldía de Ibagué se encontrarán separadas de las administradas por terceros.

Se debe impedir el ingreso a las áreas restringidas, de equipos de cómputo móvil, fotográfico, videos, dispositivos removibles o cualquier otro equipo que registre información, a menos que sea autorizado por el responsable de dicha área.

La Secretaría Administrativa – Dirección de Recursos Físicos, asegurará que los centros de procesamiento de datos de la Entidad, centros de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia cuenten con los mecanismos de protección física y ambiental adecuados para la protección de la información física y digital, tales como protección contra descargas eléctricas, ubicación libre de daño por plagas, humedad, goteras, inundaciones y demás efectos del clima.

En las áreas seguras de procesamiento de datos de la Entidad, centros de cableado, áreas de archivo, áreas de recepción y entrega de correspondencia no se permite fumar, consumir alimentos, ni almacenar material inflamable.

Las actividades de limpieza en las áreas seguras deben ser controladas y supervisadas por personal adscrito al proceso.

La Secretaría Administrativa – Dirección de Recursos Físicos debe garantizar que el personal de limpieza se capacite acerca de las precauciones mínimas a seguir durante el proceso de limpieza en las áreas seguras y se prohíbe el ingreso de maletas, bolsos u otros objetos que no sean propios de las tareas de aseo

11.1.3 Seguridad de oficinas, recintos e instalaciones

Con el propósito de garantizar la seguridad física a oficinas, recintos e instalaciones se establece:

Se prohíbe fumar y el consumo de alimentos y bebidas cerca a los equipos tecnológicos y documentación física.

La Secretaría Administrativa – Dirección de Recursos Físicos debe garantizar el mantenimiento preventivo y correctivo de la red eléctrica y de las instalaciones y, garantizar su protección física, a fin de evitar incidentes de seguridad que pongan en riesgo el recurso tecnológico (Hardware, software y comunicaciones) y la información.

Se debe cumplir con los controles de acceso físico estipulados en el control del 11.1.2

11.1.4 Protección contra amenazas externas y Ambientales

Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.

Los equipos que hacen parte de la infraestructura tecnológica de la Alcaldía de Ibagué, tales como servidores, estaciones de trabajo, centro de cableado, aires acondicionados, UPS, dispositivos de almacenamiento, entre otros, deben estar protegidos y ubicados en sitios libres de amenazas como robo, incendio, inundaciones, humedad, agentes biológicos, explosiones, vandalismo y terrorismo.

11.1.5 Trabajo en áreas seguras

La Dirección de Talento Humano - Grupo de Seguridad y Salud en el Trabajo y la Secretaría de las TIC, establecen los lineamientos para los controles contra amenazas externas y ambientales, los cuales quedarán enmarcadas en los planes de contingencia, de emergencia y de continuidad del negocio, para garantizar el trabajo en áreas seguras.

11.1.6 Áreas de despacho y carga

Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.

11.2 Equipos

Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.

11.2.1 Ubicación y protección de los equipos

Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.

Todos los equipos que cuenten con puertos de transmisión y recepción de infrarrojo y bluetooth estos deben estar deshabilitados.

Los Servidores Públicos a quienes se les asignen equipos de cómputo portátiles deberán adoptar las medidas de seguridad necesarias que garantizar la seguridad física del recurso tecnológico y salvaguardar la información.

Los servidores públicos deben dar aviso de inmediato al Almacén, de la pérdida o hurto del recurso tecnológico a su cargo, para que se surta el procedimiento establecido.

Los servidores públicos deben comunicar de manera inmediata a la Secretaría de las TIC cuando detecte posibles riesgos por factores tales como humedad, inundaciones, choques eléctricos, robo, calentamientos etc.

11.2.2 Servicios de suministro

Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.

11.2.3 Seguridad del cableado

El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño

La Secretaría de las TIC a través del equipo de soporte técnico realizará inspecciones a la red eléctrica de las dependencias, para garantizar el uso correcto de la energía regulada, es decir que no se encuentren conectados electrodomésticos, multitomas, regletas o equipos que puedan inducir variaciones en la corriente, a fin de evitar una descarga de corriente que pueda causar inestabilidad y daño al recurso Tecnológico. En caso de detectar conexiones inapropiadas, desconecta los elementos que no corresponden y registra en el servicio la actuación. La evidencia de esta actuación queda registrada en el software de soporte técnico.

La Secretaría de las TIC a través del equipo de soporte técnico realizará inspecciones a la red de cableado estructurado, para garantizar su uso correcto, y en ningún caso se permitirá las derivaciones o cascadas de la red con switches.

11.2.4 Mantenimiento de equipos

Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continua.

Todo equipo servidor que proporcione servicios a través de la red debe:

- Funcionar las 24 horas al día los 365 días del año
- Tener mantenimiento preventivo mínimo dos veces al año
- Ser objeto de Mantenimiento semestral donde se realizará la depuración de bitácoras
- Hacerle revisión de su configuración semestral
- Ser Monitoreado diariamente por la persona encargada

Los usuarios no están autorizados para instalar o desinstalar dispositivos, o hacer mantenimiento a los equipos sin previa autorización de la Secretaría de las TIC.

El Servidor Público que requiera soporte técnico debe dar aviso a la Secretaría de las TIC para que allí el encargado envíe el personal especializado a diagnosticar el equipo; en caso que se presente un daño mayor el funcionario debe enviar el equipo con memorando autorizado para que ingrese al taller de mantenimiento.

11.2.5 Retiro de activos

Los equipos, información o software no se deben retirar de su sitio sin autorización previa del jefe inmediato y del Almacén General de la Alcaldía

Todo recurso tecnológico (hardware) debe ser registrados al ingreso y salida de las instalaciones de la Alcaldía.

11.2.6 Seguridad de equipos y activos fuera de las instalaciones

Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.

El recurso tecnológico asignado será de uso exclusivo para labores propias de la Entidad y será responsabilidad del usuario que los retire de las instalaciones sin la respectiva autorización del jefe inmediato y registro de la novedad en la minuta de vigilancia

11.2.7 Disposición segura o reutilización de equipos

Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reúso.

Cuando un equipo de cómputo sea reasignado o dado de baja, se debe realizar una copia de respaldo de la información y posteriormente realizar un procedimiento de borrado seguro de información y del software instalado.

11.2.8 Equipos de usuario desatendido

Todos los equipos de cómputo deben ser configurados para bloqueo automático por inactividad.

Los usuarios al finalizar sus actividades diarias o cuando se retiren de sus puestos de trabajo por algún motivo, deben salir de todas las aplicaciones y apagar las estaciones de trabajo.

11.2.9 Política de escritorio limpio y pantalla limpia

Todo el personal de la Alcaldía de Ibagué, debe conservar su escritorio libre de información propia de la Entidad, que pueda ser copiada, utilizada y accedida por personas no autorizadas.

11.2.10 Política de adquisición de equipos

La Secretaría de las TIC verificará las características y el estado de todos los equipos digitales y análogos que ingresan a la Alcaldía de Ibagué, previo al ingreso a almacén.

Todos los dispositivos adquiridos deben contar con la garantía de fábrica. Esta debe ser tipo ON-SITE y debe acreditarse con documento equivalente a certificación o documento expedido por la casa fabricante de cada dispositivo, la cual debe tener el tiempo de garantía, tipo de garantía y tipo de cubrimiento, además el centro autorizado para efectos de la garantía debe estar ubicado en la Ciudad de Ibagué.

Los equipos que hayan sido importados deben contar con el certificado de manifiesto de aduana.

La CPU y los periféricos como son monitor, mouse y teclado que adquiera la Entidad, deben ser de la misma marca. En ese sentido la entidad requiere que tanto los computadores de escritorio y equipos portátiles sean de la misma casa fabricante. Los componentes internos que conforman la CPU deberán ser respaldados por la casa fabricante de los equipos de cómputo.

Cuando los equipos de cómputo e impresoras adquiridas sean de marca de fabricación extranjera, se deberá garantizar que el respaldo de repuestos y suministros en Colombia. Mínimo para cinco (5) años (Anexar documento).

12 POLÍTICA DE SEGURIDAD DE LAS OPERACIONES DE TIC

12.1 Procedimientos operacionales y responsabilidades

Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.

12.1.1 Procedimientos de operación documentados

Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.

12.1.2 Gestión de cambios

Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.

Se debe definir un procedimiento de gestión de cambios, el cual debe contener los canales autorizados, los niveles de autorización, la clasificación de los cambios, el tratamiento de los cambios de emergencia, las diferentes fases del cambio, entre otros

La Secretaría de las TIC y Dirección de Recursos Físicos debe planear el traslado de instalaciones contando con el concepto y soporte técnico de la Secretaría de las TIC, a fin de garantizar la continuidad de los servicios de conectividad, la seguridad del recurso tecnológico y la continuidad de los procesos.

Toda solicitud de cambio de los sistemas de información se debe realizar por escrito por los canales autorizados y se debe llevar una trazabilidad de los cambios solicitados, los cuales deben ser registrados y documentados.

Los cambios o actualizaciones a las versiones de los sistemas de información deben ser autorizados única y exclusivamente por el propietario de la información o líder del proceso que hace uso de la herramienta tecnológica que va a ser objeto de cambio.

El cambio de un sistema de información o la decisión de no continuar su operación, en todo caso debe estar debidamente justificado, y soportada la causa de la decisión, ya sea por obsolescencia, fallas de seguridad comprobada, vencimiento de licencia de uso, mal funcionamiento, incumplimiento normativo, entre otros, concepto técnico que debe contar con el aval de la Secretaría de las TIC.

Los cambios de los sistemas de información deben ser planeados y en todo caso se debe contar con un proceso de transición que garantice la integridad de la información y la continuidad de los procesos.

Los cambios en los Sistemas de información deben cumplir con la fase de pruebas y se debe verificar que cumple el propósito por el cual fue solicitado.

Se debe disponer de un roll-back en la implementación de los cambios, a fin de garantizar que de ser necesario se puede volver al estado anterior.

El software que ha sido declarado técnicamente obsoleto o que ya cumplió su ciclo y no está en uso, debe darse de baja de conformidad con los procedimientos establecidos por el Almacén General del Municipio para los activos intangibles.

12.1.3 Gestión de capacidad

Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.

12.1.4 Separación de los ambientes de desarrollo, pruebas, y operación

Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.

La Entidad debe establecer un procedimiento de mantenimiento y desarrollo de software seguro, en el cual se establezcan las actividades a seguir para hacer la transición del ambiente de pruebas a producción.

No es permitido realizar pruebas, instalaciones o desarrollos de software directamente en ambiente de producción.

En los ambientes de desarrollo y pruebas no se pueden utilizar datos reales sin que previamente se haya hecho un proceso de ofuscamiento, a fin de proteger la confidencialidad de la información y cumplir con la política de tratamiento de datos.

Se deben aplicar controles de acceso independientes para los diferentes ambientes.

12.2 Protección contra códigos maliciosos

Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.

12.2.1 Controles contra códigos maliciosos

Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.

Toda la infraestructura de procesamiento de información de la Entidad, debe contar con un sistema de detección y prevención de intrusos, herramientas anti-Spam y sistemas de control de navegación.

La Secretaría de las TIC es la responsable de la configuración apropiada e instalación de mecanismos de detección de intrusos y sistemas de protección del Hardware (firewalls), Software base, aplicativos, redes y sistemas de comunicación, a fin de evitar la intrusión y los ataques físicos.

La Secretaría de las TIC garantizará la instalación de software contra virus y código malicioso y su actualización, para protección a nivel de la red y de estaciones de trabajo, los cuales no podrán ser removidos ni reemplazados por los usuarios de los sistemas de información.

El antivirus se debe instalar con opción de actualización automática

La Secretaría de las TIC se reserva el derecho de monitorear las comunicaciones y/o información que se genere, comunique o transmita por cualquier medio, en busca de virus o código malicioso,

El único servicio de antivirus permitido, es el instalado por personal autorizado por la Secretaría de las TIC, por lo tanto, está prohibido que los usuarios desinstalen el antivirus de su equipo, modifiquen o eliminen las configuraciones de seguridad que previenen la propagación de virus

Los equipos de terceros conectados a la Red de la Alcaldía deben tener antivirus y contar con las medidas de seguridad apropiadas.

Todos los equipos conectados a la Red de la Alcaldía deben ser monitoreados y supervisados por la Secretaría de las TIC

El servicio de correo electrónico institucional contratado debe contar con análisis automático de virus en los archivos adjuntos.

Los usuarios deben asegurarse que todos los medios de almacenamiento tanto internos como externos están libres de virus o software malicioso, mediante la ejecución del software antivirus autorizado.

Los usuarios que tengan conocimiento del alojamiento de un virus en su PC deben comunicar de manera inmediata a la Secretaría de las TIC para que le brinden el soporte técnico de erradicación del virus.

Los usuarios de la red de la Alcaldía deben garantizar el análisis de virus en los archivos adjuntos en los correos electrónicos personales.

12.3 Copias de respaldo

Objetivo:

Proteger contra la pérdida de datos.

12.3.1 Respaldo de la información

Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, de conformidad con el plan de backups y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.

La Secretaría de las TIC debe establecer y documentar el procedimiento para la realización y restauración de copias de seguridad, el cual debe contener el esquema de rotulado de las copias de respaldo, el procedimiento de reemplazo de los medios de almacenamiento, disposición final de los medios de almacenamiento y copias externas,

En ningún caso las copias de seguridad serán almacenadas en el mismo equipo donde se encuentra la información. Los medios de almacenamiento de las copias de seguridad estarán ubicados en sitios seguros para impedir el acceso a la información a personal no autorizado.

La Secretaría de las TIC conservará las copias de seguridad en un lugar externo a los del origen de la información, el cual debe contar con las medidas protección y seguridad física adecuadas

Las medidas de seguridad a los Activos de TI en el sitio principal se deben extender al sitio donde se encuentren las copias externas.

La Secretaría de las TIC, el responsable de Seguridad, junto con los administradores de los sistemas de información y propietarios de la información, debe analizar las necesidades de información por lo menos con una periodicidad semestral, para determinar la información crítica que debe ser respaldada y la frecuencia con la que se debe realizar.

El propietario de la información es el responsable de definir el periodo de retención de las copias de seguridad, para lo cual debe tener en cuenta las TRD y las disposiciones de la ley general de archivo.

La Secretaría de las TIC debe disponer, controlar la ejecución del plan de backup, así como las pruebas periódicas de restauración, mínimo tres al año.

Los Administradores de los Sistema de información que soportan los procesos de la Entidad deben:

- Verificar diariamente o con la periodicidad establecida para la realización de copias de respaldo, su correcta ejecución.

- Efectuar copias de información de los servidores, cada vez que se realice un cambio significativo en los Sistemas Operativos o configuraciones básicas.

- Garantizar que las copias de respaldo se realicen en horario no hábil.

- Realizar pruebas de restauración de los backups con la periodicidad establecida en el plan de copias de seguridad, para garantizar que las copias son leídas y restauradas correctamente

Los usuarios finales son los responsables de realizar copias de seguridad de información relevante generada en el desarrollo de sus funciones, en los medios de almacenamiento autorizados por la Entidad y en ningún caso podrá realizarlo en medios removibles personales.

Los servidores públicos efectuaran copias de seguridad cuando los equipos de cómputo sean enviados a mantenimiento, previniendo así la perdida de información o en su defecto la Secretaría de las TIC realizará dichas copias de seguridad antes de hacer el mantenimiento al equipo.

La Secretaría de las TIC y los administradores de los Sistemas de información que soportan la operación de los procesos de la Entidad, deben llevar un registro de los respaldos de información realizada, de acuerdo a la periodicidad establecida en el plan de backup, del ingreso y retiro de las copias del sitio de almacenamiento externo, y de la comprobación de la integridad de la información.

La Dirección de Recursos Físicos proveerá a las Dependencias de las herramientas o recursos necesarios para efectuar las copias de seguridad.

12.4 Registro y seguimiento

Objetivo: Registrar eventos y generar evidencia.

12.4.1 Registro de eventos

Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la

información, que permitan contar con información necesaria para la gestión de incidentes de seguridad.

Todos los Sistemas de información que soportan la operación de los procesos de la Entidad deben contar con log de auditoría, los cuales deben ser revisados con la periodicidad establecida por el dueño de la información, dependiendo de su criticidad.

Los Log de auditoría deben proporcionar información relevante para soportar procesos de auditoría y para contribuir al cumplimiento de las políticas de seguridad de la información.

Los líderes de los procesos propietarios de la información definirán los criterios a auditar de acuerdo con los requerimientos internos o externos o con los datos que considere sensibles a hechos fraudulentos.

El acceso a los logs de auditoría será restringido solo a los administradores del Sistema y a los propietarios de información o a quien estos autoricen por medios escritos.

Los administradores de los sistemas de información realizarán monitoreos trimestrales al log de auditoría, emitiendo un acta como evidencia de la actuación y reportando las presuntas irregularidades

Se deben hacer copias de respaldo de los logs de auditoría, para que estén disponibles en caso de un incidente de seguridad.

Los soportes documentales de las modificaciones a los datos de manera directa por los usuarios Administradores, deben conservarse de conformidad con las TRD aprobadas

12.4.2 Protección de la información de registro

Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.

La Secretaría de las TIC debe garantizar que los respaldos de información se conserven en sitios seguros.

Ningún usuario puede realizar copias de respaldo en medios de almacenamiento removibles personales, ya que esto puede desencadenar en fuga de información.

12.4.3 Registros del administrador y del operador

Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.

Los Administradores de los sistemas de información que soportan los procesos de la Entidad deben tener asignada una cuenta de usuario, a través de la cual realizarán las actividades de administración, la cual será entregada a través de un proceso formal.

La transferencia de la responsabilidad de administración de los sistemas de información con ocasión de situaciones administrativas como vacaciones, ausencia temporal a retiro definitivo, se debe realizar a través de un proceso formal y las claves deben ser modificadas por quien asume dichas funciones.

El Administrador de bases de datos, no podrá manipular directamente los datos, salvo en circunstancias en las cuales los aplicativos no lo permitan, y solo lo realizará cuando medie autorización escrita del líder del proceso propietario de la información, y con el debido soporte que requiera de la actualización respectiva

12.4.4 Sincronización de relojes

Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la Entidad o ámbito de seguridad, se deben sincronizar con la hora legal colombiana.

12.5 Control de software operacional

Objetivo: Asegurar la integridad de los sistemas operacionales.

12.5.1 Instalación de software de sistemas operativos

La Secretaría de las TIC implementará controles para la instalación de software en sistemas operativos, actividad que es competencia exclusiva de esta Secretaría.

Los equipos servidores o los que hagan sus veces, deben contar con el software para realizar el chequeo de integridad del sistema operativo y del hardware. La periodicidad de su ejecución estará definida por el o la titular de la Secretaría de las TIC. Esto aplica para todos los equipos de cómputo (ej.: equipos de escritorio y portátiles)

12.6 Gestión de la vulnerabilidad técnica

Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.

12.6.1. Gestión de las vulnerabilidades técnicas

Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.

Los Administradores de las bases de datos deben programar todas las tareas de afinamiento y los sistemas de información de manera periódica, de acuerdo con la cantidad de solicitudes o quejas de los usuarios respecto de la disponibilidad de las aplicaciones.

12.6.2 Restricciones sobre la instalación de software

Todo software instalado en equipos de la Entidad, será autorizado o instalado por la Secretaría de las TIC, la cual tiene autonomía para desinstalar o borrar software no autorizado, en desarrollo de actividades de control de uso de software legal.

Los Servidores públicos no están autorizados para instalar en los equipos de cómputo de propiedad de la Alcaldía, Software no autorizado por la Secretaría de las TIC.

El servidor Público asumirá la responsabilidad por el software instalado en el computador que le sea asignado o que esté utilizando.

Toda aplicación que esté instalada debe estar debidamente licenciada. La Secretaría de las TIC será la responsable del control e inventario de las licencias de software y del manejo de los medios de instalación.

El líder de los procesos serán los responsables de planear y disponer del recurso presupuestal para la adquisición y renovación de las licencias, y la Secretaría de las TIC soporte técnico en la etapa precontractual y la supervisión de los contratos.
.

12.7 Consideraciones sobre auditorías de sistemas de información

Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.

12.7.1 Controles de auditorías de sistemas de información

Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.

Las pistas de auditoría deben permitir monitorear las conexiones a las bases de datos, las modificaciones al modelo de datos y las modificaciones a los datos, de manera directa o por medio de aplicativos.

13 POLITICAS DE SEGURIDAD DE LAS COMUNICACIONES

13.1 Gestión de la seguridad de las redes

Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.

13.1.1 Controles de redes

Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.

La Secretaría de las TIC contará con personal capacitado, responsable de la configuración y administración de las redes de tal forma que se garantice el control de acceso y la restricción de privilegios, dando aplicación al protocolo que se establezca para tal fin.

La Secretaría de las TIC es la responsable de establecer los controles lógicos para el acceso a los diferentes recursos tecnológicos.

El uso de aplicaciones de acceso remoto a la red de la Alcaldía, solo se autorizará de acuerdo a la política de Teletrabajo o trabajo en casa establecida por la Entidad.

Los usuarios de la Red de la Alcaldía de Ibagué no deben establecer redes de área local, conexión remota a redes internas o externas, o transferir archivos a través del FTP, utilizando la red de la Entidad sin autorización previa de la Secretaría de las TIC.

13.1.2 Seguridad de los servicios de red

Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.

La Secretaría de las TIC es la responsable de verificar la instalación y configuración de todo servidor que sea conectado a la red, y de implementar mecanismos de seguridad física y lógica.

13.1.3 Separación en las redes

Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.

La Secretaría de las TIC debe establecer un esquema de segregación de redes, con el fin de controlar el acceso a los diferentes segmentos de la red.

El acceso a la Red Inalámbrica de la Alcaldía de Ibagué a través de equipos de telefonía móvil será restringido por la Secretaría de las TIC, a fin de minimizar los

riesgos y mejorar la velocidad en la navegación desde equipos portátiles, siendo este el fin principal de este tipo de tecnología.

Se deben seguir los procedimientos de acceso o retiro de componentes tecnológicos para la solicitud de servicios de red, y establecer los estándares mínimos para la implementación de cableado estructurado certificado, switches administrables etc.

Se deben establecer parámetros técnicos para la conexión segura de la red con los servicios de red.

Se deben establecer mecanismos de autenticación seguros para el acceso a la red.

Se deben separar las redes inalámbricas de las redes internas, para garantizar los principios de la seguridad de la información.

13.2 Transferencia de información

Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

13.2.1 Políticas y procedimientos de transferencia de información

Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.

13.2.2 Acuerdos sobre transferencia de información

Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.

En todos los Contratos o Acuerdos con terceras partes, que implique un intercambio, uso o procesamiento de información de la Entidad, se deben realizar Acuerdos de confidencialidad sobre el manejo de la información.

Los Acuerdos de confidencialidad de la información deben hacer parte integral de los contratos o documentos que legalicen la relación del negocio.

Dentro del contrato o acuerdo se deben definir claramente el tipo de información que se va a intercambiar por las partes.

La Entidad identificará los riesgos para la información y servicios de procesamiento de información que involucran a terceros e implementará los controles adecuados antes de autorizar el acceso.

13.2.3 Mensajería electrónica

Se debe proteger adecuadamente la información incluida en la mensajería electrónica.

La Secretaría de las TIC es la encargada de Administrar el servicio de correo electrónico, de definir los nombres, estructura, tamaño del buzón, tamaño de los archivos enviados y plataforma que se debe utilizar para la cuenta de correo Institucional de cada Dependencia o programa.

El uso del correo institucional es de carácter corporativo, siendo responsabilidad de los Secretarios y Directores su Administración y control.

Los Secretarios y Directores podrán delegar por escrito al funcionario que se encargará de la administración del correo.

En instante en que la Secretaría de las TIC asigne un correo electrónico y establezca la contraseña de acceso, la persona responsable de gestionar el correo ingresara por primera vez y este automáticamente le solicitara el cambio de contraseña. La confidencialidad y el uso de las credenciales de acceso será responsabilidad de la persona a quien se le asigne.

Todo correo institucional debe ser descargado periódicamente de la bandeja de entrada para así liberar y dar capacidad al servidor, previa realización de copia de seguridad garantizando la seguridad de la información.

La Secretaría de las TIC debe garantizar las copias de seguridad de todas las cuentas a través del servidor de correo.

El intercambio de información entre la Entidad y terceros a través de correos electrónicos, se hará única y exclusivamente por medio de los correos institucionales, y en ningún caso por medio de correos personales.

La información contenida en archivos generados en suite ofimáticas, será enviada en formatos no editables utilizando el software que indique la Secretaría de las TIC.

El usuario responsable del correo institucional debe evitar abrir los adjuntos de correos de origen desconocido o que contengan palabras en Ingles a fin de evitar los virus, a menos que haya sido analizado previamente por el antivirus autorizado.

El correo institucional será de uso exclusivo para fines propios de la Entidad y en su uso se dará aplicación al código de ética; En consecuencia, es prohibido utilizar el correo institucional para divulgar información confidencial, reenviar mensajes que falten al respeto o atenten contra la dignidad e intimidad de las personas, difundir propaganda política, comercial, religiosa, racista, sexista o similares y reenviar contenido y anexos que atenten contra la propiedad intelectual.

Los usuarios del correo institucional deben evitar enviar respuestas a todos los destinatarios del correo inicial, salvo en los casos que sea absolutamente necesario, sobre todo en los casos en los cuales el correo original fue enviado de manera masiva.

La Secretaría de las TIC y de Comunicaciones definirán el texto de exoneración de responsabilidad que se debe incluir en los correos electrónicos, para proteger a la Entidad de los contenidos de los correos electrónicos.

13.2.4 Acuerdos de confidencialidad o de no divulgación

Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.

Todos los servidores públicos que manipulen información en cumplimiento de sus funciones, y terceros tales como proveedores de redes y servicios de telecomunicaciones, personal de entes de control entre otros, deben aceptar acuerdos de uso y manejo de la información reservada o confidencial definida por la Entidad, donde se comprometen a no revelar, modificar, dañar, eliminar o usar inapropiadamente la información confidencial a la que tengan acceso, so pena de las investigaciones penales y disciplinarias a las que haya lugar.

La Entidad identificará la información considerada clasificada o reservada, índice que deberá ser divulgada de conformidad con la normatividad vigente.

La información clasificada reservada confidencial solo se debe transmitir por medios seguros.

14 POLITICA DE ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACION

14.1 Requisitos de seguridad de los sistemas de información

Objetivo: Garantizar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.

14.1.1 Análisis y especificación de requisitos de seguridad de la información

Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.

La Secretaría de las TIC será la responsable de definir y establecer los estándares y procedimientos para el desarrollo, mantenimiento y adquisición de sistemas de información, incluyendo la custodia del código fuente, ambientes de desarrollo, pruebas y producción, y de toda la infraestructura tecnológica relacionada, de conformidad con las mejores prácticas y reglas internacionales de seguridad informática.

En el marco del Plan Estratégico de la Información (PETI) y de sus competencias, la Secretaría de las TIC es la única Dependencia con la capacidad técnica para adquirir, desarrollar e implementar soluciones tecnológicas para la Alcaldía de Ibagué, así como de avalar la adquisición o recepción de software dentro del marco de convenios y contratos con terceros, con el fin de garantizar la conveniencia, soporte, mantenimiento y seguridad de la información.

En caso que alguna Dependencia adquiera, desarrolle o realice mantenimientos a sistemas de información dentro de su marco misional, deberá cumplir con lo establecido en las políticas y estándares, y deberá solicitar el acompañamiento de la Secretaría de las TIC.

14.1.2 Seguridad de servicios de las aplicaciones en redes Públicas

La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.

14.1.3 Protección de transacciones de los servicios de las aplicaciones

La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.

14.2 Seguridad en los procesos de desarrollo y soporte.

Objetivo: garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo de los sistemas de información y de esta manera se garantice la calidad del producto entregado y en consecuencia su uso, apropiación y continuidad de uso.

14.2.1. Política de desarrollo seguro de software Control: la Entidad velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, se asegurará que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido por la Entidad.

Cualquier solicitud para el Desarrollo de aplicativos nuevos debe tener un proyecto de viabilidad el cual deberá estar debidamente sustentado, una vez sea aprobado por el comité de desarrollo de software se ordenará iniciar con las fases del ciclo de vida del sistema de información.

La Secretaría de las TIC documentará las buenas prácticas para el desarrollo seguro de Software, que garanticen la integridad, confidencialidad y disponibilidad de la información.

14.2.2. Procedimientos de control de cambios en los sistemas.

La Secretaría de las TIC debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información de la Entidad. La realización de un cambio tecnológico que no considere los requerimientos de seguridad de la Información hace que la Entidad esté expuesta a riesgos. Por lo tanto, cada cambio tecnológico debe asegurar el cumplimiento de la Política de Seguridad de la Información y sus respectivas normas, y en caso de exponer a la Entidad a un riesgo en seguridad de la información, éste debe ser identificado, evaluado, documentado, asumido y controlado por el respectivo dueño de la información.

Se debe dar cumplimiento a los controles establecidos en el numeral 12.1.2

14.2.3. Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.

La Secretaría de las TIC, debe realizar pruebas de todos los sistemas, cuando se presente un cambio de sistema operativo en los equipos de cómputo de la Entidad, con el fin de revisar los posibles impactos en las operaciones o en la seguridad de la información

14.2.4. Restricciones a los cambios en los paquetes de software.

La realización de un cambio tecnológico en un paquete de software entregado por un tercero, que no considere los requerimientos de seguridad de la Información hace que la Entidad esté expuesta a riesgos. Por lo tanto, cada cambio tecnológico debe asegurar el cumplimiento de la Política de Seguridad de la Información y sus respectivas normas, y en caso de exponer a la Entidad a un riesgo en seguridad de la información, éste debe ser identificado, evaluado, documentado, asumido y controlado por el respectivo dueño de la información.

14.2.5. Uso de principios de ingeniería en protección de sistemas.

La Entidad establecerá mecanismos de control en la labor de implementación en el sistema de información, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por las mismas, cumplan con las políticas, normas y procedimientos de seguridad de la información.

14.2.6. Seguridad en entornos de desarrollo.

La Entidad establecerá y protegerá adecuadamente los entornos para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de vida de desarrollo del sistema.

14.2.7. Externalización del desarrollo de software.

La Secretaría de las TIC debe establecer el procedimiento y los controles de acceso a los ambientes de desarrollo de los sistemas de información; así mismo, debe asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.

14.2.8. Pruebas de funcionalidad durante el desarrollo de los sistemas.

Los desarrolladores de los sistemas de información deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el diseño hasta la puesta en marcha.

Para la publicación y puesta en marcha de aplicativos nuevos estos deben estar correctamente diseñados, evaluados de forma minuciosa para evitar la redundancia en las salidas de información, supervisados y autorizados por el Secretario(a) de las TIC y líder del proceso.

14.2.9. Pruebas de aceptación.

La Secretaría de las TIC debe generar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.

14.3 Datos de prueba.

Objetivo: garantizar la protección de los datos que se utilizan para procesos de pruebas.

14.3.1. Protección de los datos utilizados en prueba

La Secretaría de las TIC de la Entidad protegerá los datos de prueba que se entregarán a los desarrolladores, asegurando que no revelan información confidencial de los ambientes de producción. La Secretaría de las TIC mediante acuerdos de confidencialidad, debe asegurar que la información a ser entregada a los desarrolladores para sus pruebas será enmascarada y no revelará información confidencial de los ambientes de producción

15. POLITICAS DE RELACIONES CON LOS PROVEEDORES

15.1 Seguridad de la información en las relaciones con los proveedores

Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.

15.1.1 Política de seguridad de la información para las relaciones con proveedores

Establecer un plan de relación con proveedores que documente la decisión adoptada por el nivel directivo de adquirir un producto o servicio relacionado con activos de información, así como las consideraciones de seguridad de la información relacionadas con esta contratación.

Planificar la selección de los proveedores de productos o servicios de seguridad de la información, Gestionar la relación durante la ejecución del contrato y Planificar el cierre contractual con los proveedores de productos o servicios de seguridad de la información.

Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con éstos y se deben documentar.

15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores

Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.

Los documentos sobre los acuerdos para la seguridad de la información deben estar firmados por las partes y deben contener como mínimo los siguientes requisitos de seguridad que se deben exigir a los proveedores son:

- Designación de un responsable de seguridad, quien será el interlocutor y el responsable del cumplimiento de los controles pactados.
- Control de personal. El proveedor debe establecer comunicación directa con el supervisor del contrato, a quien mantendrá informado de manera escrita sobre los cambios de personal que hace parte de la prestación del servicio

contratado, de tal forma que el personal que ha sido retirado, le sean revocado los permisos de acceso tanto físico a las instalaciones como a los sistemas de información.

- Cumplimiento de los requisitos legales, protección de datos, derechos de autor, entre otros.
- Uso correcto de los activos de información para la finalidad prevista e implementación de controles para evitar el daño o revelación de la información y accesos no autorizados.
- Condiciones para la disponibilidad del contratista para la realización de auditorías de seguridad.
- El proveedor debe establecer, implementar y mantener procesos de seguridad (Procesos de contratación, devolución o destrucción de información, planes de formación en seguridad, proceso control de cambios, tratamiento de incidencias, actualización de software y programas de seguridad, planes de continuidad del negocio, entre otros)
- El proveedor debe tener implementado controles de software malicioso y virus en los equipos que se conecten a la red de la Entidad y debe mantener el antivirus actualizado.
- Cualquier equipo que se conecte a la red de la entidad debe tener instalado software debidamente licenciado.
- Obligación a ceñirse a las políticas, controles y procedimientos de gestión de cambios y desarrollo de software seguro establecidos en la Entidad.
- Cumplimiento de las políticas y controles establecidos para el cifrado de información y autenticación.
- Cumplimiento de las políticas y protocolos seguros para la transmisión segura de información reservada o clasificada.
- Establecer criterios técnicos para la configuración y funcionalidad de los firewalls.
- Cumplir con las políticas de seguridad de acceso y demás políticas de seguridad que le sean aplicables.

15.1.3 Cadena de suministro de tecnología de información y comunicación

Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación, es decir por los servicios que nuestros proveedores subcontraten.

El proveedor debe garantizar que sus proveedores son de confianza y la aplicación de controles de seguridad sobre sus proveedores.

Exigir al proveedor la trazabilidad de los procesos críticos y la garantía de la comunicación con los proveedores y su cadena de suministro.

15.2 Gestión de la prestación de servicios de proveedores

Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.

15.2.1 Seguimiento y revisión de los servicios de los proveedores

Las Unidades Administrativas que celebren contratos de prestación de servicios tecnológicos tales como alojamiento de servidores, aplicaciones de datos y servicios de comunicación entre otros, deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.

La relación con los proveedores estará regulada por un contrato de prestación de servicios o convenio, en el cual se debe especificar las condiciones para el manejo adecuado de la información de la Entidad y de terceros, con los requisitos de seguridad que se han definido entre los cuales se encuentran las cláusulas de confidencialidad.

Estas condiciones de seguridad serán acordadas con los proveedores con anterioridad a la firma de los contratos y quedará documentada en los anexos que se establezcan.

Todo tipo de contrato de servicios digitales (aplicación, servicio, tareas o procesos) debe contar con el análisis de riesgos de seguridad digital de los activos de información que estarán afectados con la contratación o cesión de datos a terceros, dando aplicación a la metodología establecida en la política de riesgos.

En la definición de controles se incluirá la investigación de los antecedentes de los proveedores, verificando información financiera, antecedentes penales, auditoría de controles, procesos de seguridad del proveedor, control de accesos, entre otros.

La investigación de los antecedentes se mantendrá dentro de la legalidad vigente y en cumplimiento de las leyes de protección de datos.

Los controles de seguridad serán contenidos en los acuerdos de confidencialidad.

En los controles de acceso, se deben definir los límites de la información a la cual el proveedor tendrá acceso para el desarrollo de la ejecución del contrato.

Se deben incluir controles para la devolución de los activos de información, eliminación o destrucción de datos, cancelación y revocación de accesos.

15.2.2 Gestión de cambios en los servicios de los proveedores

Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos.

Se debe Contar con un plan de migración o de terminación avalado y probado para la entrega de los productos o servicios de seguridad de la información a la entidad o al proveedor entrante.

Documento con la evaluación de los riesgos existentes en los procesos de entrega o migración de los servicios o productos de seguridad de la información.

Activación del plan de continuidad del negocio, verificación de controles existentes y respaldo de información o dispositivos según corresponda

Acta de finalización del contrato debe estar avalada y firmada por el supervisor, en el cual certifica el cierre de la relación contractual al igual que el informe de lecciones aprendidas durante el tiempo del servicio y en el cierre del contrato.

15 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

15.1 Gestión de Incidentes y mejoras en la Seguridad de la Información.

Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

16.1.1 Responsabilidades y procedimientos

Las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información, se encuentran definidas en el plan de gestión de incidentes.

16.1.2 Reporte de eventos de seguridad de la información

Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.

Los servidores públicos deben comunicar de manera inmediata a los contactos de la Secretaría de las TIC indicados en el plan de incidente, cuando detecte posibles riesgos por factores tales como humedad, inundaciones, choques eléctricos, robo, calentamientos, acceso no autorizado y demás incidentes de seguridad etc.

16.1.3 Reporte de debilidades de seguridad de la información

Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.

16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos.

Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.

16.1.5 Respuesta a incidentes de seguridad de la información

Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.

16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información

El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.

16.1.7 Recolección de evidencia

En el plan de Gestión de Incidentes se deben definir procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia, los cuales la Entidad debe aplicar.

Sólo la Secretaría de las TIC está autorizada para reportar incidentes de seguridad ante las autoridades de defensa nacional, policía, Entes de Control, así mismo son los únicos autorizados para hacer pronunciamientos oficiales ante Entidades externas, medios de comunicación y ciudadanía en general.

16 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO

16.1 Continuidad de seguridad de la información

Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.

17.1.1 Planificación de la continuidad de la seguridad de la información

La Alcaldía de Ibagué, debe documentar en el plan de continuidad de negocio, los requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.

La Entidad debe garantizar la disponibilidad de los recursos indicados en el plan de continuidad de negocio.

17.1.2 Implementación de la continuidad de la seguridad de la información

La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.

17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información

La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.

16.2 Redundancias

Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.

17.2.1 Disponibilidad de instalaciones de procesamiento de información.

Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.

17 CUMPLIMIENTO

17.1 Cumplimiento de los requisitos legales y contractuales

Objetivo: Evitar los incumplimientos de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y con los requisitos de seguridad.

18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales

La Alcaldía de Ibagué debe identificar y documentar en el normograma, todos los requisitos legales y contractuales que afecten la Entidad, además de mantenerlos actualizados.

18.1.2 Derechos de Propiedad Intelectual

La Alcaldía de Ibagué a través de la Secretaría de las TIC protegerá la propiedad intelectual propia y de terceros. El software registrado con Derechos de Autor no se podrá copiar sin previa autorización del propietario.

Todo Software instalado en los equipos de propiedad de la Alcaldía, debe ser autorizado o instalado por la Secretaría de las TIC, la cual tiene la autonomía para desinstalar o borrar software, en desarrollo de actividades de control de uso de software legal

La Secretaría de las TIC tiene la responsabilidad del control e inventario de las licencias de software y del manejo de los medios de instalación

El servidor Público asumirá la responsabilidad por el software no autorizado, instalado en el computador que tenga a cargo de propiedad de la Alcaldía.

El Personal adscrito a la Alcaldía de Ibagué de manera directa e indirecta y terceros, no harán ni usarán copias no autorizadas de software de aplicaciones de desarrollo propio o adquirido.

Bajo ninguna circunstancia se debe usar software que no esté debidamente licenciado por el editor del software. El uso o copia no autorizado de software de computadora es una violación a la ley y a la política de la Alcaldía de Ibagué, y hará que el empleado que cometa la violación esté sujeto a las acciones disciplinarias y sanciones correspondientes.

La propiedad intelectual de los programas de desarrollo propio de la Alcaldía de Ibagué, es única y exclusivamente de la Entidad, dicha propiedad abarca el desarrollo informático, su código fuente y la estructura de la base de datos.

Para el uso del software de desarrollo propio de la Alcaldía de Ibagué por terceros, es necesario suscribir un acuerdo entre las partes, para garantizar su uso apropiado y el cumplimiento de las normas de derecho de autor. En este documento se establecerán las condiciones uso, explotación, distribución, modificaciones, acceso al código fuente, cesión y las siguientes disposiciones que garanticen los derechos de autor:

- Entrega, instalación y personalización
- Extensión y límites de la licencia de uso

- Condiciones de la licencia
- Utilización del paquete informático
- Garantía y limitación de la misma
- Responsabilidad de las partes
- Efectos de la cancelación de la licencia.
- Cesión
- Capacitación en el uso de software
- Integración con otro software
- Deber del licenciatario de usar el software en debida forma.

18.1.3 Protección de Registros

Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.

En la Alcaldía de Ibagué, el archivo y retención de los documentos producidos en la ejecución de los procesos, se efectuará de conformidad con las Tablas de Retención Documental aprobadas, el procedimiento de control de registros, plan de preservación digital y disposiciones del Archivo General de la Nación.

El usuario que autoriza el uso compartido de archivos, debe delimitar a los usuarios que realmente la necesitan, controlar el tiempo en el cual estará expuesta, y asegurarse que el autorizado cuente con antivirus legal o autorizado, ya que es responsable por las acciones y el acceso a dicha información.

Los documentos que son distribuidos o compartidos con terceros, tendrán con marca de agua la clasificación de la información contenida, y su copia magnética se realizará en formato PDF de solo lectura, para impedir la modificación o eliminación accidental o intencional de los datos, y la pérdida de la confidencialidad inadvertida.

Cada funcionario se hace responsable de la administración y distribución de la información existente en su equipo de cómputo, generando las respectivas copias de seguridad y en caso de ser necesario se entregará copia de esta a la Secretaría de las TIC para salvaguardar la información.

Todo documento considerado confidencial debe ser autocontenido y no depender de la disponibilidad e integridad de fuentes externas de datos.

Los Administradores de los sistemas de información son los únicos autorizados para manipular las estructuras de los directorios y carpetas, de acuerdo con sus especificaciones

La custodia del código fuente del desarrollo propio de la Alcaldía de Ibagué, está a cargo de la Secretaría de las TIC, la cual aplicará controles lógicos y físicos que lo protejan del acceso no autorizado y salvaguarden la propiedad intelectual del mismo.

18.1.3.1 Política de Preservación Digital

La Alcaldía de Ibagué, aplicará los principios que rigen la preservación digital a largo plazo e implementará estrategias, procedimientos y lineamientos técnicos que garanticen la estabilidad y persistencia de la información contenida en los diferentes medios de almacenamiento digital , gestionada por la Entidad en desarrollo de sus funciones administrativas ,constitucionales y técnicas, con el propósito de asegurar la integridad, confidencialidad y disponibilidad de la información, de conformidad con los criterios técnicos y legales establecidos por el Archivo General de la Nación y el Ministerio de las TIC. En tal sentido, la política de Preservación Digital a largo plazo será articulada con la política de Gestión Documental, la Gestión del Riesgo y la Política de Seguridad de la información.

Para garantizar la preservación digital a largo plazo, la Entidad asegurará la provisión del recurso humano, técnico, logístico y financiero que se defina en el plan de Preservación Digital.

18.1.4 Protección de los datos y privacidad de la información personal.

La Entidad aplicará lo establecido en la política de tratamiento y protección de datos personales.

18.1.5 Regulación de los controles criptográficos

Para la aplicación de mecanismos de cifrado, la Alcaldía de Ibagué debe cumplir con la normatividad establecida para el uso de medios criptográficos, limitaciones, obligatoriedad, evaluación de riesgos, cifrado legal y disposiciones del archivo General de la Nación.

17.2 Revisiones de seguridad de la información

Objetivo: Garantizar que la seguridad de la información es implementada y operada de acuerdo con las políticas y procedimientos organizacionales

18.2.1 Revisión independiente de la seguridad de la información

La auditoría interna al cumplimiento de la Seguridad de la Información en ningún caso podrá ser realizada por personal adscrito al área auditada, de tal forma que se garantice la independencia e imparcialidad de la auditoría, y será desarrollada por personal idóneo.

Le corresponde a la unidad administrativa líder del proceso Sistema Integrado de Gestión, planear y coordinar las auditorías internas al Sistema de Gestión de Seguridad de la Información.

En el proceso de evaluación de riesgos conforme a la periodicidad y metodología definida en la política de administración de riesgos, se realizará revisión al cumplimiento de los controles establecidos.

18.2.2 Cumplimiento de la política y las normas de seguridad

En la revisión por la dirección, la Alcaldía de Ibagué realizará monitoreo a la política del Sistema de Gestión de Seguridad de la Información, por lo menos una vez al año.

Los líderes de los procesos harán las revisiones en los procedimientos para establecer la aplicación de los controles de acuerdo a los requisitos, periodicidad y lineamientos indicados.

Cuando se identifiquen incumplimientos se deben establecer las causas, implementar acciones correctivas, revisar la eficacia de las acciones e identificar las debilidades del sistema.

Se deben documentar los resultados de las revisiones y las acciones correctivas implementadas.

18.2.3 Revisión del cumplimiento técnico.

Se debe revisar la configuración de los sistemas de información semestralmente de acuerdo con las reglas y políticas definidas, para identificar posibles fallos en

las actualizaciones de los sistemas, establecer medidas correctivas antes de que estos fallos se conviertan en una amenaza real para el sistema.

19. CONTROL DE CAMBIOS

VERSION	VIGENTE DESDE	OBSERVACIÓN
01	04/03/2015	PRIMERA VERSIÓN SIGAMI
02	21/09/2018	Segunda versión
03	25/04/2019	Cambio nombre del proceso
04	01/12/2020	Actualización nombre de la Secretaría, y de la política y controles de organización interna
05	26/10/2021	Cambio de nombre de proceso, inclusión en el proceso Sistema Integrado de Gestión, Actualización de todas las políticas conforme al anexo A de la ISO:27001:2013
06	24/08/2022	-Actualización política 15.1 de conformidad con los lineamientos de la resolución 746 de 2022. -Actualización 9.4.3.4 Longitud de Contraseña de usuario

Elaboró	Revisó	Aprobó
Profesional Especializado Grupo Infraestructura Tecnológica	Asesor Secretaría TIC y Administradores Sistemas de Información	Secretaria de las TIC