ALCALDIA DE PEREIRA

# POLÍTICA DE GOBIERNO DIGITAL

# PROTOCOLOS Y PROCEDIMIENTOS

FORMATO PRELIMINAR AL DOCUMENTO

| | | | | | |
|---|---|---|---|---|---|
| **Título:** | **PROTOCOLOS Y PROCEDIMIENTOS** | | | | |
| **Sumario** | El presente documento surge de la aplicación del Decreto 1078 de 2015 del Ministerio de Tecnologías de la Información y las Comunicaciones MinTIC "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones" en su libro 2 de la parte 2 del título 9 capítulo 1 "Estrategia Gobierno en Línea" en su componente número cuatro "Seguridad y Privacidad de la Información" el cual establece que se deben crear documentos para la implementación del Modelo de Seguridad y Privacidad de la Información en la Alcaldía de Pereira, integrando los mismos con el Sistema de Gestión Documental de la entidad que permita gestionar adecuadamente la Seguridad y Privacidad de la Información. | | | | |
| **Palabras Claves** | Procedimientos<br>Controles | | | | |
| **Formato:** | PDF y DOC | | Lenguaje: | Español | |
| **Dependencia:** | Secretaría de Tecnologías de la Información y la Comunicación | | | | |
| **Código:** | N/A | Versión | 1.0 | Estado | En Aprobación |
| **Categoría** | Documento Técnico, Implementación de la Política de Gobierno Digital. | | | | |
| | Componente: | ARQUITECTURA T.I | | | |
| | Habilitador Transversal: | Seguridad y Privacidad de la Información | | | |
| | Lineamientos y Estándares: | Política Gobierno Digital 1008 del 14 de Junio de 2018 | | | |
| | Dominio: | Gobierno TI | | | |
| | Herramientas: | Guía 8 sobre controles | | | |
| **Asesor (es):** | Magister Carlos Mario Arteaga Pacheco<br>Contratista Prestación de Servicios Profesionales Especializados | | | | |
| **Autor (es):** | Alejandro Pineda Muñoz<br>Contratista Prestación de Servicios Profesionales | | | | |
| **Revisó:** | Diego Fernando Bonilla Ríos<br>Director de Sistemas de Información y Servicios Digitales | | | | |
| **Aprobó:** | Jaime Wainer Ruiz Rentería<br>Secretario Tecnologías de Información y Comunicaciones | | | | |

HISTÓRICO

| VERSIÓN | FECHA | CAMBIOS INTRODUCIDOS |
|---|---|---|
| 1.0 | 13/05/2019 | Emisión del documento |

# Contenido

# 1 INTRODUCCIÓN

Con este documento se pretende describir las y normas, protocolos, procedimientos, controles de seguridad de la información definidas por la Alcaldía de la Ciudad de Pereira que constituyen parte fundamental del sistema de seguridad y privacidad de la información y se convierten en la base para la aplicación adecuada de los controles en la seguridad de la información.

Para la elaboración del mismo, se toman como base regulaciones aplicables, como la norma técnica ISO 27001:2013 y las recomendaciones del estándar ISO 27002:2013, Política Gobierno Digital 1008 del 14 de Junio de 2018.

## 2 OBJETIVO

El objetivo de este documento es establecer los protocolos y procedimientos en seguridad y privacidad de la información de la Alcaldía de Pereira, con el fin de regular la gestión de la seguridad de la información al interior de la entidad.

## 3 ALCANCE

Los Servidores Públicos, contratistas, practicantes, pasantes, proveedores y terceros que cumplan funciones administrativas o que en cumplimiento de sus funciones presten servicios a cargo del municipio de Pereira deben poner en práctica las disposiciones dadas por el presente documento.

## 4 DEFINICIONES

Acuerdo de Confidencialidad: es un documento entre dos partes en este caso los funcionarios de la Alcaldía de Pereira y otras personas naturales o jurídicas donde manifiestan su voluntad de mantener la confidencialidad de la información de la institución, comprometiéndose a no divulgar o usar la información confidencial a la que tengan acceso.

Protocolo: un protocolo es un documento donde se consignan los pasos que se deben seguir para ejecutar acciones seguras dentro de los procesos de una entidad.

Medio removible: es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CD, DVD y unidades de almacenamiento USB, entre otras.

Perfiles de usuario: un perfil de un usuario es el entorno cargado por el sistema cuando un usuario inicia una sesión en un equipo

SGSI: Sistema de Gestión de Seguridad de la Información.

Control: es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye policías, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Código malicioso: es un tipo de código informático o script web dañino diseñado para crear vulnerabilidades en el sistema que permiten la generación de brechas de seguridad, robo de información y datos, así como otros perjuicios potenciales en archivos y sistemas informáticos.

Reusó o reutilización: Acción de volver a utilizar o usar los dispositivos tecnológicos, después de un uso específico.

Disco Duro: Los discos duros tienen una gran capacidad de almacenamiento de información, pero al estar alojados normalmente dentro de la computadora (discos internos), no son extraíbles fácilmente.

## 5 SIGLAS

NTC: norma técnica colombiana creada por ICONTEC.
MSPI: modelo de seguridad y privacidad de la información.

## 6 NORMATIVIDAD

Política Gobierno Digital 1008 del 14 de Junio de 2018.

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

Anexo A de ISO/IEC 27001:2013

Tratamiento de datos (Ley 1581 de 2012, art 3).

Elaboración de la política general de seguridad y privacidad de la información, guía No. 2.

Guías para construir el Sistema de Gestión de Seguridad de la Información (SGSI) para las entidades Públicas. (Ministerio de las Tecnologías de la Información y las Comunicaciones), Controles de Seguridad y Privacidad de la Información, guía No. 8.

# 7 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN

| Dominio | Norma ISO 27001:2013<br>**Soporte** |
|---|---|
| Subdominio | A.5 Políticas de la seguridad de la información |
| Etapa | **A5.1** Directrices establecidas por la dirección para la seguridad de la información |
| Objetivo de control | Brindar orientación y apoyo 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 |
| Control | A5.1.1: Políticas para la seguridad de la información<br><br>Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes. |

| Control A.5.1.1: Políticas para la seguridad de la información | |
|---|---|
| Controles relacionados: Política general de seguridad y privacidad de la información | |
| Manuales: | No aplica |
| Propósito: Definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los Servidores Públicos, contratistas, practicantes, pasantes, proveedores y terceros y partes externas pertinentes.<br><br>Lineamientos generales:<br>Los responsables y responsabilidades para la seguridad de la información son los dispuestos en la política general de seguridad y privacidad de la información.<br><br>El líder del proceso de Seguridad de la Información deberá mantener contacto con las autoridades nacionales en materia de seguridad de la información.<br><br>La Dirección de sistemas de información y servicios digitales es el responsable de elaborar las políticas, procedimientos e instructivos en materia de seguridad de la información. | |

| Procedimiento: Políticas para la seguridad de la información | | | | |
|---|---|---|---|---|
| | Actividad | Tarea | Responsable | Registros |
| 1 | Definir políticas de seguridad y privacidad de la información. | La Dirección de Sistemas de Información y Servicios Digitales será el responsable de elaborar las políticas, procedimientos e instructivos en materia de seguridad de la información. | La Dirección de Sistemas de Información y Servicios Digitales | Política general de seguridad y privacidad de la información |

| Dominio | Norma ISO 27001:2013<br>**Soporte** |
|---|---|
| Subdominio | **A.5 Políticas de la seguridad de la información** |
| Etapa | **A5.1 Directrices establecidas por la dirección para la seguridad de la información** |
| Objetivo de control | Brindar orientación y apoyo 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 |
| Control | A5.1.2: Revisión de las políticas para la seguridad de la información<br><br>Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas |

| Control A.5.1.2: Revisión de las políticas para seguridad de la información | |
|---|---|
| Controles relacionados: Política general de seguridad y privacidad de la información | |
| Manuales: | No aplica |
| Propósito: Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continúa.<br><br>Lineamientos generales:<br><br>La política general de seguridad y privacidad de la información será revisada anualmente, o antes si existiera la necesidad por un cambio normativo que obligue a su modificación. | |

| **Procedimiento: Revisión de las políticas para seguridad de la información** | | | | |
|---|---|---|---|---|
| | Actividad | Tarea | Responsable | Registros |
| 1 | Revisión de las políticas de seguridad y privacidad de la información | La Dirección de Sistemas de Información y Servicios Digitales será el responsable de la actualización de la política General de Seguridad y Privacidad de la Información, la cual será revisada anualmente, o antes si existiera la necesidad por un cambio normativo que obligue a su modificación. | La Dirección de Sistemas de Información y Servicios Digitales | Política general de seguridad y privacidad de la información |

## 8 SEGURIDAD DE LOS RECURSOS HUMANOS

| Dominio | Norma ISO 27001:2013<br>**Soporte** |
|---|---|
| Subdominio | **A.7 Seguridad en los recursos humanos** |
| Etapa | **A7.1 Antes de asumir el empleo** |
| Objetivo de control | Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran. |
| Control | **A7.1.1 Selección:**<br>Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos. |

| Control A.7.1.1: Selección (verificación de los antecedentes) | |
|---|---|
| Controles relacionados:<br><br>FUG_GR_Lista_Chequeo_Contratos_V2 1.<br><br>GR J LISTADO DE DOCUMENTOS SOPORTES VR 1.<br><br>GR Requisitos Para Toma De Posesión V1 | |
| Manuales: | Manual contratación Decr 559 de 2014 |
| Propósito:<br>Realizar la verificación de los antecedentes de todos los candidatos a un empleo.<br><br>Lineamientos generales:<br>La Dirección de Talento Humano deberá realizar los mecanismos de verificación del personal en el momento en que se postula a un cargo. Dicho mecanismo deberá incluir los aspectos legales y que dicte la Función Pública.<br><br>Las Secretarías de Despacho con los responsables de los procesos de | |

| |
|---|
| contratación de cada una de las dependencias de la Alcaldía de Pereira deben aplicar la lista de verificación que contengan los aspectos necesarios para la revisión de los antecedentes del personal a contratar por prestación de servicios.<br><br>Los documentos de verificación deberán reposar en la historia laboral o en la carpeta del contratista. |

| Procedimiento: Selección (verificación de los antecedentes) | | | | |
|---|---|---|---|---|
| | Actividad | Tarea | Responsable | Registros |
| 1 | Verificación de los soportes y antecedentes de los funcionarios de planta y contratistas. | La Dirección de Talento Humano, la Secretaría de Despacho con los responsables de los procesos de contratación deben tener los soportes en medio físicos de los antecedentes disciplinarios, fiscales y penales, la tarjeta profesional con el soporte de vigencia, así como el registro de las contravenciones o medidas correctivas de la policía. | Dirección de Talento Humano<br><br>Secretarías de Despacho con los responsa - bles de los procesos de contratación. | |
| 2 | Verificación en aplicativos web de los antecedentes de los servidores públicos y contratistas. | Se debe verificar en el aplicativo Web el estado de vigencia de:<br>La tarjeta profesional<br>los antecedentes disciplinarios, fiscales, penales.<br>El registro de las contravenciones o medidas correctivas de la policía<br><br>Esta verificación se | | |

| | | | | |
|---|---|---|---|---|
| | | debe realizar en las siguientes páginas web: antecedentes disciplinarios www.procuraduria.gov.co, antecedentes fiscales www.contraloria.gov.co, antecedentes penales https://antecedentes.policia.gov registro nacional de medidas correctivas https://srvpsi.policia.gov.co. | | |
| 3 | Anexar los documentos de verificación | Los documentos de verificación de los Servidores Públicos y los contratistas deberán reposar en la historia laboral del funcionario de planta o en la carpeta del contratista. | Dirección de Talento Humano<br><br>Secretarías de Despacho con sus responsa-bles de los procesos de contratación | GR Requisitos Para Toma De Posesion V1.<br><br>FUG_GR_Lista_Chequeo_Contratos_V2 1 GR.<br><br>GR J LISTADO DE DOCUMENTOS SOPORTES VR 1 |

| Dominio | Norma ISO 27001:2013<br>**Soporte** |
|---|---|
| Subdominio | **A.7 Seguridad en los recursos humanos** |
| Etapa | **A7.1 Antes de asumir el empleo** |
| Objetivo de control | Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran |
| Control | A.7.1.2 Términos y condiciones del empleo.<br><br>Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información |

| Control A.7.1.2: Términos y condiciones del empleo | |
|---|---|
| Controles relacionados:<br>FUG GR Minuta Contrato Prestación de Servicios_V2: clausula vigésima segunda, confidencialidad. | |
| Manuales: | N/A |
| Propósito:<br>Se debe establecer en los acuerdos contractuales con los contratistas en cuanto a las responsabilidades la seguridad y privacidad de la información.<br><br>Lineamientos generales:<br>Las Secretarías de Despacho con sus responsables en los procesos de contratación deberán definir los términos y condiciones del contrato, en los cuales se establecerá las obligaciones del contratista en materia de seguridad de la información.<br><br>La Dirección de Talento Humano y Secretarías de Despacho con los responsables de los procesos de contratación de cada dependencia deberán dar a conocer a todo el personal los términos y condiciones de empleo o contrato y especificar las responsabilidades u obligaciones en materia de la seguridad de la información y aclarar que estas se extienden más allá de los límites del trabajo o la terminación del contrato. | |

| Procedimiento: términos y condiciones del empleo | | | | |
|---|---|---|---|---|
| 1 | Actividad | Tarea | Responsable | Registros |
| 2 | Definir acuerdos contractuales | Se deben realizar acuerdos contractuales en los contratos por prestación de servicios y definir obligaciones en cuanto a la seguridad y privacidad de la información | Secretarías de Despacho con los responsa-bles de los procesos de contratación. | FUG GR Minuta Contrato Prestación de Servicios_V2: clausula vigésima segunda, confidenciali-dad |
| 3 | Establecer responsabilida-des u obligacio-nes en cuanto a la privacidad y seguridad de la información. | Se deben establecer las responsabilidades u obligaciones en cuanto a la seguridad y privacidad de la información en la posesión para el personal de planta | Dirección del Talento Humano | |

| Dominio | Norma ISO 27001:2013<br>**Soporte** |
|---|---|
| Subdominio | **A.7 Seguridad en los recursos humanos** |
| Etapa | **A7.2 Durante la ejecución del empleo** |
| Objetivo de control | Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan. |
| Control | A7.2.1<br>Responsabilidades de la dirección :<br>La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización. |

| Control A.7.2.1: Responsabilidades de la dirección | |
|---|---|
| Controles relacionados: Comunicado SAIA | |
| Manuales: | Política general de seguridad y privacidad de la información |
| Propósito:<br>Se debe exigir a todos los Servidores Públicos, contratistas, practicantes, pasantes, proveedores y terceros de la administración municipal la aplicación de la seguridad de la información de acuerdo con las políticas establecidos por la Alcaldía de Pereira<br><br>Lineamientos generales:<br>La Dirección de Talento Humano y las Secretarías de Despacho con los responsables de los procesos de contratación darán a conocer Política general de seguridad y privacidad de la información a los Servidores Públicos, contratistas, practicantes, pasantes, proveedores de la administración municipal. | |

| Procedimiento: responsabilidades de la dirección | | | | |
|---|---|---|---|---|
| | Actividad | Tarea | Responsable | Registros |
| 1 | Socializar las políticas de seguridad y | Realizar comunicación oficial a través del aplicativo SAIA dirigido | Dirección de Talento Humano | Comunicado SAIA |

| | | | | |
|---|---|---|---|---|
| | privacidad de la información. | a todas las dependencias de la administración. | Secretarías de Despacho con los responsa-bles de los procesos de contratación | |
| 2 | Promoción activa de una cultura de seguridad | Se debe socializar la política general de seguridad y privacidad de la información con una periodicidad semestral | | |

| Dominio | Norma ISO 27001:2013<br>**Soporte** |
|---|---|
| Subdominio | **A.7 Seguridad en los recursos humanos** |
| Etapa | **A7.3 Terminación y cambio de empleo** |
| Objetivo de control | Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato |
| Control | A7.3.1 Terminación o cambio de responsabilidades de empleo:<br><br>Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir |

| Control A.7.3.1: Terminación o cambio de responsabilidades de empleo | |
|---|---|
| Controles relacionados:<br>FUG_GR_Acta_de_Entrega_V1<br><br>FUG GR Minuta Contrato Prestación de Servicios_V2: clausula vigésima segunda, confidencialidad | |
| Manuales: | N/A |
| Propósito:<br>Asegurar el manejo adecuado de la información en la terminación o cambio de la vinculación laborar de los servidores públicos de la Alcaldía de Pereira<br><br>Lineamientos generales:<br>El Supervisor del contrato o a quien delegue deberá recoger y custodiar la información de la Alcaldía de Pereira de los contratistas en caso de terminación o cesión del contrato.<br><br>El jefe inmediato o a quien delegue deberá recoger y custodiar la información de la Alcaldía de Pereira en el caso de retiro, o cambio de funciones de los funcionarios de planta. | |

| Procedimiento Terminación o cambio de responsabilidades de empleo | | | | |
|---|---|---|---|---|
| | Actividad | Tarea | Responsable | Registros |
| 1 | Recoger y custodiar la información | Los Supervisores de los contratos deberán recoger y custodiar la información que entreguen los contratistas en caso de terminación o cesión del contrato.<br><br>Para el personal de planta el jefe inmediato o quien se asigne deberá recoger y custodiar la información en el caso de retiro o cambio de funciones. | Supervisores de los contratistas<br><br>Líderes de los procesos | |
| 2 | Diligenciar acta de entrega | Se debe diligenciar el acta de entrega del cargo para el caso de servidores públicos y contratistas. | Funcionario que entrega.<br><br>Funcionario que recibe. | Formato: FUG_GR_Acta_ de_Entrega_ V1 |
| 3 | Informar a la Dirección de Infraestructura Tecnológica la novedad de desvinculación para inactivar el usuario en los aplicativos. | Los Supervisores de los contratistas deben realizar solicitud por el aplicativo SAIA, informando la novedad de la terminación del contrato por parte del contratista.<br><br>Para el caso del personal de planta la Dirección de Talento Humano debe informar la desvinculación laboral de los servidores públicos por el aplicativo | Dirección de Talento Humano<br><br>Supervisores de los contratistas | Comunicado SAIA |

| | | | | |
|---|---|---|---|---|
| | | SAIA para inactivar el acceso a los diferentes aplicativos. | | |

## 9 GESTIÓN DE ACTIVOS

| Dominio | Norma ISO 27001:2013<br>**Soporte** |
|---|---|
| Subdominio | **A.8 Gestión de activos** |
| Etapa | **A.8.1 Responsabilidad por los activos** |
| Objetivo de control | Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas. |
| Control | A.8.1.1 Inventario de activos:<br>Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.<br><br>A.8.1.2 Propiedad de los activos:<br>Los activos mantenidos en el inventario deberían tener un propietario. |

| | |
|---|---|
| Control A.8.1.1: Inventario de activos<br>**A.8.1.2: Propiedad de los activos** | |
| Controles relacionados: Formato inventario de activos. | |
| Manuales: | N/A |
| Propósito:<br>Identificar los activos asociados con la información en la Alcaldía de Pereira.<br>Los activos mantenidos en el inventario deberán tener un propietario.<br><br>Lineamientos generales:<br>Los líderes de los procesos deberán mantener un inventario de sus activos de información con una periodicidad anual y serán actualizados según el evento en que se requiera.<br><br>Es responsabilidad a los líderes de los procesos de sus activos de información como la información física, archivadores, aplicaciones web, archivos físicos, los equipos de cómputo, equipos portátiles, correos electrónicos, aplicaciones. | |

Son activos de la Alcaldía de Pereira y se proporcionan para los servidores públicos, contratistas, practicantes, pasantes, proveedores y terceros que cumplan funciones administrativas o que en cumplimiento de sus funciones presten servicios a cargo del Municipio de Pereira.

| Procedimiento inventario de activos y propiedad de activos. | | | | |
|---|---|---|---|---|
| | Actividad | Tarea | Responsable | Registros |
| 1 | Inventario de activos | Los líderes de los procesos y los responsables de los activos de información deberán mantener un inventario de sus activos de información con una periodicidad anual. | Líderes de los procesos.<br><br>Los responsa-bles de los activos de información | Formato inventario de activos |

| Dominio | Norma ISO 27001:2013<br>**Soporte** |
|---|---|
| Subdominio | **A.8 Gestión de activos** |
| Etapa | **A.8.1 Responsabilidad por los activos** |
| Objetivo de control | Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas. |
| Control | A.8.1.4 Devolución de activos:<br>Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo. |

| Control A.8.1.4: Devolución de activos | |
|---|---|
| Controles relacionados: FUG_GR_Acta_de_Entrega_V1 | |
| Manuales: | N/A |
| Propósito:<br>Devolver todos los activos que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.<br><br>Lineamientos generales:<br><br>Todos los servidores públicos, contratistas, practicantes, pasantes y terceros deberán devolver todos los activos de información de la Alcaldía de Pereira que se encuentren a su cargo al terminar su empleo, contrato o acuerdo. | |

| Procedimiento Devolución de activos | | | | |
|---|---|---|---|---|
| | Actividad | Tarea | Responsable | Registros |
| 1 | Devolver activos de información | Para el devolver un activo de información o documentos físicos, el | Servidores | Comunicado SAIA |

| | | | | |
|---|---|---|---|---|
| | | servidor público que termina su vinculación laboral debe clasificar la información y llevarla a gestión documental. | públicos | |
| 2 | Recoger y custodiar la información | El Supervisor del contratista deberá recoger y custodiar la información que entreguen los contratistas en caso de la terminación del contrato.<br><br>Para el caso del personal de planta el jefe inmediato o quien se asigne deberá recoger y custodiar la información del funcionario que termina su vinculación laboral con la entidad. | Supervisores de los contratistas<br><br>Líderes de los procesos | |
| 3 | Diligenciar acta de entrega | Se debe diligenciar el acta de entrega del cargo. | Funcionario Público que entrega.<br><br>Funcionario Público que recibe.<br><br>Contratistas | Formato: FUG_GR_Acta_de_Entrega_V1 |

| Dominio | Norma ISO 27001:2013<br>**Soporte** |
|---|---|
| Subdominio | **A.8 Gestión de activos** |
| Etapa | **A.8.2 Clasificación de la información** |
| Objetivo de control | Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización. |
| Control | A.8.2.1 Clasificación de la información :<br><br>La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.<br>. |

| Control A.8.2.1: Clasificación de la información | |
|---|---|
| Controles relacionados: Guía de rotulación, Formato rotulo carpeta v1. | |
| Manuales: | Ley 594 del 2000(acuerdo 042 de 2002, acuerdo 038 del 2002, acuerdo 039 de 2002) |
| Propósito:<br>La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.<br><br>La información física se debe clasificar teniendo en cuenta los principios de procedencia (áreas y asunto), orden original o cronológico.<br><br>Lineamientos generales:<br>Los que generan la información son los encargados de realizar la clasificación de la información.<br><br>Los responsables y custodios de los activos de información dentro de cada área son los encargados de monitorear periódicamente la clasificación de sus activos de información para ser archivado.<br><br>La información física de la Alcaldía de Pereira deberá tener un periodo de almacenamiento, este periodo deberá ser indicado en las tablas de retención documental y cuando se cumpla el periodo de expiración, toda la información | |

deberá ser eliminada o conservada adecuadamente según su valor.

La foliación continua de carpetas se hace para las series documentales complejas como contratos, procesos, historias laborales, esta foliación se repartirá en varias carpetas de 200 folios cada uno.

La foliación única de carpetas numeración de 1 a 200 páginas de manera independiente, se hace para las series simples como actas, decretos, acuerdo y resoluciones.

Los niveles para la clasificación de la información física se deben organizar con base en las tablas de retención documental debidamente aprobadas por el consejo departamental de archivo.

| Procedimiento clasificación de la información | | | | |
|---|---|---|---|---|
| | Actividad | Tarea | Responsable | Registros |
| 1 | Depuración documental | Se debe realizar la depuración documental, como el retiro de duplicidad de documentos, solo se debe dejar un original en la carpeta, retiro de ganchos metálicos, clips y notas. | Todos los funcionarios de la Alcaldía de Pereira | |
| 2 | Clasificación de documen-tos | Se debe clasificar los documentos por serie, sub serie, asunto, día, mes, año. | | G.E CUADRO DE CLASIFICACIÓN DOCUMENTAL |
| 3 | Conformar carpetas | Se deben conformar las carpetas de 200 folios cada una. | | |
| | Foliación de carpetas | Se debe realizar la foliación de cada una de las hojas en la parte superior derecha a lápiz | | |

| | | | | |
|---|---|---|---|---|
| | | y en sentido de orientación del documento. | | |
| 4 | Ordenación cronológica | Se debe realizar la ordenación cronológica del interior de las carpetas, para esto tener en cuenta que la fecha más antigua de la carpeta debe aparecer al abrir la carpeta, y la fecha más reciente al finalizar la carpeta. | | |
| 5 | Rotular carpetas | Se debe realizar la rotulación de la carpeta y diligenciar los siguientes campos: fondo, sección, subsección, código, serie, sub serie, nombre, número de folios, fecha inicial y fecha final. | | Formato rotulo carpeta v1 |

| Dominio | Norma ISO 27001:2013<br>**Soporte** |
|---|---|
| Subdominio | **A.8 Gestión de activos** |
| Etapa | **A.8.2 Clasificación de la información** |
| Objetivo de control | Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización. |
| Control | A.8.2.2 Etiquetado de la información:<br><br>Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización. |

| Control A.8.2.2: Etiquetado de la información | |
|---|---|
| Controles relacionados: FORMATO ROTULO CAJA MUNICIPIO, FORMATO ROTULO CARPETA, FORMATO FUID UNICO INVENTARIO DOCUMENTAL V1. | |
| Manuales: | Acuerdo 038 del 2002 responsabilidades de los servidores públicos frente a documentos y archivos e Inventarios documentales, Acuerdo 042 del 2002 criterio para organización de archivos de gestión rotulación de carpetas y cajas. |
| Propósito:<br>Dictar lineamientos para desarrollar implementar los procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la Alcaldía de Pereira.<br><br>Lineamientos generales:<br><br>Deberá aplicar la rotulación de la información para los activos de información físicos, para ello se tomarán como base, los criterios, para la rotulación de la información que ha establecido a través del documento Guía para la Rotulación de la Información.<br><br>Las Tablas de Retención Documental (TRD) deberán contener el tipo de clasificación de las series, sub series y documentos en ella contenidas. | |

Cada Propietario de la Información realizara el proceso de clasificación y rotulado de la información con fundamento en las tablas de retención documental de la entidad.

| Procedimiento etiquetado de la información | | | | |
|---|---|---|---|---|
| | Actividad | Tarea | Responsable | Registros |
| 1 | Rotulado de la información | Para marcar o rotular carpetas se debe aplicar el rotulo establecido por el municipio. | | |
| 2 | | La rotulación se hace teniendo en cuenta el contenido de la carpeta. | | Formato rotulo carpeta |
| | Rotulado de caja | La rotulación de las cajas se hace con base en el rotulo establecido por el municipio, teniendo en cuenta la cantidad de carpetas que van al interior de cada caja | | Formato rotulo caja municipio |
| | Ordenar carpetas en caja | Se debe tener en cuenta que la agrupación de las carpetas en la caja debe ser por series y el mismo año | | |
| | Inventario documental | Para realizar la transferencia documental, se debe realizar el inventario por carpetas y cajas en el formato único de inventario documental establecido por el | | Formato fuid único inventario documental v1 |

| | | | | |
|---|---|---|---|---|
| | | municipio, donde relacionamos todas las carpetas que se encuentran en el interior de cada caja. | | |

| Dominio | Norma ISO 27001:2013<br>**Soporte** |
|---|---|
| Subdominio | **A.8 Gestión de activos** |
| Etapa | **A.8.3 Manejo de medios** |
| Objetivo de control | Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios. |
| Control | A.8.3.1 Gestión de medios removibles:<br><br>Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización |

| Control A.8.3.1: Gestión de medios removibles | |
|---|---|
| Controles relacionados:<br>PDE_TICS_Registro_De_Actividades_Anexas_A_LaPrestacion_Del_SerVicio V1 | |
| Manuales: | N/A |
| Propósito:<br>Establecer lineamientos para la adecuada gestión de los medios de almacenamiento removibles como (discos duros externos, memorias flash, USB, SD,CD, DVD) que permitan asegurar la integridad, confidencialidad y disponibilidad de la información de la Alcaldía Municipal de Pereira.<br><br>Lineamientos generales:<br><br>EL uso de medios removibles será autorizado para los servidores públicos y contratistas que para el cumplimiento de sus funciones así lo requieran por lo cual se realizara la activación de los puertos de conexión del computador de manera temporal<br><br>Se encuentra restringida la conexión no autorizada de cualquier elemento de almacenamiento en los equipos de cómputo de la Alcaldía de Pereira. | |

| Procedimiento: Gestión de medios removibles | | | | |
|---|---|---|---|---|
| | Actividad | Tarea | Responsable | Registros |
| 1 | Solicitud para la utilización de medios removibles | Los Servidores Públicos, contratistas, practicantes, pasantes, proveedores y terceros que requiera la activación temporal de los puertos USB del computador, debe realizar la solicitud a la Mesa de Servicios Tecnológicos por aplicativo (MANTIS), justificando el por qué y el tiempo de activación de los puertos del computador. | Usuarios responsables de los equipos de cómputo. | Solicitud aplicativo MANTIS |
| 2 | Activar los puertos | Se realizara la activación de los puertos de conexión registrando el equipo de cómputo, el funcionario al que se le realiza el procedimiento y el tiempo de activación. | Técnico Mesa de Servicios Tecnológicos | |
| 3 | Almacenar en un lugar Seguro | Luego de realizar la copia de la información en el medio de almacenamiento debe ser guardado en un lugar seguro. | Usuarios responsables de los equipos de cómputo. | |

| | | | | |
|---|---|---|---|---|
| 4 | Bloquear los puertos USB del computador | Una vez que se cumpla el tiempo de activación de los puertos del equipo de cómputo, la Mesa Servicios Tecnológicos procederá a bloquear los puertos USB del computador. | Técnico Mesa de Servicios Tecnológicos | PDE_TICS_Registro_De_Actividades_Anexas_A_La Prestacion_Del_Servicio V1 |

| Dominio | Norma ISO 27001:2013<br>**Soporte** |
|---|---|
| Subdominio | **A.8 Gestión de activos** |
| Etapa | **A.8.3 Manejo de medios** |
| Objetivo de control | Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios. |
| Control | A.8.3.2 Disposición de los medios:<br><br>Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales. |

| Control A.8.3.2: Disposición de los medios | |
|---|---|
| Controles relacionados:<br>PDE_TICS_Formato_De_Certificación_Para_Concepto_Técnico_De_Equipos_De_Computación_Y_Accesorios V1 | |
| Manuales: | N/A |
| Propósito:<br>Disponer en forma segura de los medios de almacenamiento o equipos cuando estos ya no se requieran, utilizando procedimientos formales<br><br>Lineamientos generales:<br><br>Los equipos que tengan medios de almacenamiento, que requieran ser dados de baja, deberán contar con un acta de borrado seguro. | |

| Procedimiento: Disposición de los medios (equipos con medios de almacenamiento) | | | | |
|---|---|---|---|---|
| | Actividad | Tarea | Responsable | Registros |
| 1 | Realizar solicitud para dar de baja el equipo o medio de almacena-miento | Los Servidores Públicos deben realizar la solicitud a la Mesa de Servicios Tecnológicos (plataforma MANTIS), también se puede | Servidores Públicos | Plataforma MANTIS |

| | | | | |
|---|---|---|---|---|
| | | hacer por llamada telefónica o correo electrónico, solicitando el concepto técnico del equipo cuando se requiera dar de baja. | | |
| 2 | Revisar la solicitud | La coordinadora de la Mesa de Servicios Tecnológicos recibe la solitud, según como se realizó la solicitud lo registra en la plataforma MANTIS y la direcciona al técnico de soporte | Coordinadora de la Mesa de Servicios Tecnológicos. | |
| 3 | Atender la solicitud | El técnico de soporte revisa el equipo y realiza el concepto técnico. | Técnico de la Mesa de Servicios Tecnológicos. | PDE_TICS_Formato_De_Certificación_Para_Concepto_Técnico_De_Equipos_De_Computación_Y_Accesorios V1 |
| 4 | Realizar borrado seguro de medios de almacenamiento | Para el caso que el equipo se requiera dar de baja, se debe realizar el borrado seguro del medio de almacenamiento del equipo, para esto se debe diligenciar un formato de borrado seguro de equipos, el cual debe ir firmado por el Director de Infraestructura Tecnológica. | Técnico de la Mesa de Servicios Tecnológicos. | |

| Dominio | Norma ISO 27001:2013<br>**Soporte** |
|---|---|
| Subdominio | **A.8 Gestión de activos** |
| Etapa | **A.8.3 Manejo de medios** |
| Objetivo de control | Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios. |
| Control | A.8.3.3 Transferencia de medios físicos:<br><br>Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte. |

| Control A.8.3.3: Transferencia de medios físicos | |
|---|---|
| Controles relacionados: Comunicado SAIA, PDE_Transferencia_De_ Medios_Fisicos V1 | |
| Manuales: | N/A |
| Propósito:<br>Los medios de almacenamiento como discos duros, equipos de cómputo, que contienen información, se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.<br><br>Lineamientos generales:<br><br>Los Servidores Públicos, contratistas, practicantes, pasantes, proveedores y terceros que realicen procesos de intercambio de información al interior y exterior de la Alcaldía de Pereira son responsables del uso adecuado de la información.<br><br>La transferencia de información al interior de la Alcaldía de Pereira se realizará a través de los medios oficiales de comunicación.<br><br>Cuando se requiera transportar los medios, discos duros, equipos de cómputo con su medio de almacenamiento de la alcaldía de Pereira a otras entidades se debe tener en cuenta su contenido, se debe proteger el contenido de cualquier daño físico, ambiental o de otra naturaleza que pueda ocurrir durante el transporte.<br><br>En el caso de información confidencial, se debe etiquetar cómo tal y especificar claramente el destinatario. | |

Cualquier violación a la seguridad establecida debe ser informada de inmediato cómo incidente de Seguridad de la Información.

El transporte de los medios de almacenamiento de la entidad debe darse de acuerdo a la clasificación de la información contenida en éstos, para ello se deben utilizar servicios de mensajería confiables, las técnicas de embalaje y llevar un registro correspondiente a los medios de almacenamiento transportados.

| Procedimiento: Transferencia de medios físicos | | | | |
|---|---|---|---|---|
| | Actividad | Tarea | Responsable | Registros |
| 1 | Transferencia de medios físicos de información en el interior de la Alcaldía de Pereira. | La transferencia de medios físicos de información al interior de la Alcaldía de Pereira se realizará a través de un comunicado SAIA, indicando el medio que se va a transferir, el contenido de lo que se va a transferir y la clasificación de la información, los datos de la persona que va a transferir la información de una dependencia a otra | Funcionarios de la adminis-tración | Comunicado SAIA |
| | Transportar un medio de almacenamiento con información de la Alcaldía de Pereira a otra entidad. | Al transportar un medio o equipo de cómputo con su medio de almacenamiento de la alcaldía de Pereira a otra entidad externa, se debe tener en cuenta el contenido del medio de almacenamiento, la | | PDE_Transfer encia_De_ Medios_Fisico s V1 |

| | | | | |
|---|---|---|---|---|
| | | protección y los responsables del transporte. | | |

## 10 CONTROL DE ACCESO

| Dominio | Norma ISO 27001:2013 |
|---|---|
| Subdominio | **A.9 Control de acceso** |
| Etapa | **A.9.1 Requisitos del negocio para control de acceso** |
| Objetivo de control | Limitar el acceso a información y a instalaciones de procesamiento de información |
| Control | A.9.1.2 Uso de los servicios de red:<br><br>Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente. |

| Control A.9.1.2: Uso de los servicios de red | |
|---|---|
| Controles relacionados:<br>Comunicado SAIA “Solicitud para la creación y renovación de perfiles” | |
| Manuales: | Políticas sobre el uso de los servicios de red |
| Propósito:<br>Establecer permisos de acceso de los usuarios a la red y a los servicios de red para lo que hayan sido autorizados.<br><br>Lineamientos generales:<br><br>La Dirección de Infraestructura Tecnológica suministrará a los usuarios los permisos respectivas para el acceso a la red y sistemas de información a los que hayan sido autorizados; los permisos de acceso son de uso personal e intransferible.<br><br>Los Servidores Públicos, contratistas, practicantes, pasantes, proveedores y terceros que tengan acceso a los servicios de la red, deberán ser específicamente los autorizados para su uso.<br><br>Los equipos de cómputo de usuarios que se conecten a las redes de datos de la Alcaldía de Pereira, únicamente podrán realizar las tareas para las que fueron autorizados o que son competencia de su cargo. | |

| Procedimiento: Uso de los servicios de red | | | | |
|---|---|---|---|---|
| | Actividad | Tarea | Responsable | Registros |
| 1 | Realizar la solicitud para la creación de usuarios para el acceso a la red | Para solicitar el acceso a los servicios de la red, se debe realizar la solicitud por el aplicativo SAIA, ingresando por la parte de formato, se selecciona "solicitud para la creación y la renovación de perfiles"<br><br>Se debe seleccionar si el acceso a la red es a un punto de red o a la red WIFI, también se debe seleccionar si el acceso es por PC de escritorio o mediante portátil. | Servidores Públicos y Contratistas | Comunicado SAIA(Solicitud para la creación y renovación de perfiles) |
| 2 | Se recepciona la solicitud. | La Dirección de Infraestructura Tecnológica recibe la solicitud y activa los diferentes permisos de acceso a la red. | Dirección de Infraestructura Tecnológica | |
| 3 | Dar respuesta a la solicitud de activación de los servicios de red | Por comunicado SAIA se da la respuesta a la solicitud indicando la red y la clave de conexión para el punto de red. | Dirección de Infraestructura Tecnológica | Comunicado SAIA(Solicitud para la creación y renovación de perfiles) |
| 4 | Para el caso de la red WIFI | Para activar la red WIFI, el funcionario que realizo la solicitud para acceder a la red, debe llevar el computador portátil a la Dirección de | Dirección de Infraestructura Tecnológica | |

| | | | | |
|---|---|---|---|---|
| | | Infraestructura Tecnológica para que le ingresen la clave de activación a la red WIFI. | | |

| Dominio | Norma ISO 27001:2013 |
|---|---|
| Subdominio | **A.9 Control de acceso** |
| Etapa | **A.9.2 Gestión de acceso de usuarios** |
| Objetivo de control | Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado y sistemas y servicios. |
| Control | **A.9.2.1 Registro y cancelación del registro de usuarios:** Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.<br>**A.9.2.2 Suministro de acceso de usuarios:** Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.<br>**A.9.2.3 Gestión de derechos de acceso privilegiado:** Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.<br><br>**A.9.2.4 Gestión de información de autenticación secreta de usuarios:** La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal. |

| | |
|---|---|
| Controles A.9.2.1: Registro y cancelación del registro de usuarios.<br>A.9.2.2: Suministro de acceso de usuarios.<br>A.9.2.3: Gestión de derechos de acceso privilegiado.<br>A.9.2.4: Gestión de información de autenticación secreta de usuarios | |
| Controles relacionados:<br>Comunicado SAIA “Solicitud para la creación y renovación de perfiles de usuarios”, Políticas sobre el uso de los servicios de red | |
| Manuales: | N/A |
| Propósito:<br>Asignar o cancelar los privilegios de acceso para todo tipo de usuarios para los sistemas de información de la Alcaldía de Pereira.<br><br>Restringir y controlar la asignación y uso de derechos de acceso privilegiado. | |

La asignación de información de autenticación secreta y uso de contraseñas se debe realizar mediante un proceso confidencial.

Lineamientos generales:
Se deberá deshabilitar los permisos de acceso a la información a los funcionarios que no tengan ningún vínculo laboral.

En caso de terminación del contrato el sistema automáticamente bloqueara el perfil para salvaguardar la información, y no será habilitado bajo ninguna circunstancia hasta que no exista renovación o un contrato nuevo.

El acceso a la información es otorgado sólo a los Servidores Públicos, contratistas, practicantes, pasantes, proveedores y terceros o usuarios autorizados, teniendo en cuenta las funciones relacionadas con su cargo o alcances del contrato. El acceso a los sistemas de información es restringido y con los privilegios por un tiempo limitado.

Servidores Públicos, contratistas, practicantes o usuarios sólo podrán acceder a los sistemas de información sobre los cuales están autorizados, no podrán acceder a otros sistemas sobre los cuales no tienen permisos.

Los Servidores Públicos, contratistas, practicantes, pasantes, deberán cumplir con los lineamientos para la creación y uso de contraseñas no se otorgara permisos de acceso a los sistemas de información a los usuarios que no realicen el proceso formal de solicitud para la creación de usuarios.

Todos Servidores Públicos, contratistas, practicantes, pasantes, terceros y usuarios que tienen acceso a los sistemas de información deben mantener de forma confidencial las contraseñas con el fin de conservar la seguridad y privacidad de la información.

Solo se deberá otorgar los privilegios de acceso a los diferentes sistemas de información con permisos especiales a los funcionarios como administradores de recursos tecnológicos, servicios de red y sistemas de información únicamente a aquellos colaboradores que cumplan dichas funciones.

Cada dependencia debe reportar inmediatamente las modificaciones ocurridas con los contratistas (terminación o renovación del contrato) a la Dirección de Infraestructura Tecnológica.

La información de la contraseña para la autenticación de a los diferentes

| |
|---|
| sistemas de información se deberá suministrar a los usuarios de manera segura.<br><br>La información secreta de las contraseñas para la autenticación a los diferentes sistemas de información se deberá suministrar para un único usuario. |

| | | | | |
|---|---|---|---|---|
| | Procedimiento:<br>Registro y cancelación del registro de usuarios.<br>Suministro de acceso de usuarios.<br>Gestión de derechos de acceso privilegiado.<br>Gestión de información de autenticación secreta de usuarios. | | | |
| | Actividad | Tarea | Responsable | Registros |
| 1 | Realizar la solicitud para la creación de usuarios para el acceso a los sistemas de información | Servidores Públicos, contratistas, practicantes, pasantes, que requieran una cuenta de usuario deben realizar la solicitud por el aplicativo SAIA, se debe ingresar a la parte de formatos y se selecciona “solicitud para la creación y la renovación de perfiles”, indicar si es funcionario o contratista con el número de contrato, fecha de inicio y terminación del mismo.<br><br>Indicar si el acceso a la red es a un punto de red o a la red WIFI, también se debe seleccionar si es por PC de escritorio o mediante portátil.<br><br>Para solicitar el | Servidores Públicos, contratistas, practicantes, pasantes. | Comunicado SAIA(Solicitud para la creación y renovación de perfiles) |

| | | | | |
|---|---|---|---|---|
| | | usuario para el ingreso a los diferentes aplicativos se debe enviar el oficio SAIA debidamente autorizado por los líderes de los Procesos.<br><br>La autorización para los privilegios de acceso se debe realizar de acuerdo a las funciones de la labor a desempeñar | | |
| 2 | Activar los diferentes perfiles y asignar usuarios y contraseñas | La Dirección de Infraestructura Tecnológica activa los perfiles en los diferentes aplicativos, da respuesta por comunicado SAIA, indicando el usuario y contraseña para el aplicativo para el cual se realizó la solicitud para el permiso de acceso | Dirección de Infraestructura Tecnológica | Comunicado SAIA |
| 3 | Informar la terminación de la vinculación laboral para el personal de planta. | La Dirección de Talento Humano debe informar a la Dirección de Infraestructura Tecnológica cuando un funcionario termine su vinculación laboral en la alcaldía de Pereira para que se inactiven los permisos de acceso. | Dirección de Talento Humano | Comunicado SAIA |

| | | | | |
|---|---|---|---|---|
| 4 | Reportar la terminación del contrato. | El supervisores de los contratistas deben reportar inmediata-mente las modificaciones ocurridas con los contratistas (terminación o renovación del contrato) a la Dirección de Infraestructura Tecnológica. | Supervisores de los contratistas | Comunicado SAIA |
| 5 | Inactivar usuario | Se recibe la solicitud y se inactiva el usuario de los funcionarios que terminan su vinculación laboral con la Alcaldía de Pereira, se da respuesta indicando el cumplimiento de la solicitud | Dirección de Infraestructura Tecnológica. | Comunicado SAIA |

| Dominio | Norma ISO 27001:2013<br>**Soporte** |
|---|---|
| Subdominio | **A.9 Control de acceso** |
| Etapa | **A.9.2 Gestión de acceso de usuarios** |
| Objetivo de control | Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios. |
| Control | A.9.2.5 Revisión de los derechos de acceso de usuarios:<br>Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares. |

| Control A.9.2.5: Revisión de los derechos de acceso de usuarios | |
|---|---|
| Controles relacionados:<br>Reporte por comunicado SAIA | |
| Manuales: | N/A |
| Propósito:<br>Los administradores de los sistemas de información deberán revisar los derechos de acceso de los usuarios a intervalos regulares.<br><br>Lineamientos generales:<br><br>La Dirección de Infraestructura Tecnológica deberá realizar un informe del uso de los sistemas de información que utilizan los Servidores Públicos y Contratistas de la Alcaldía de Pereira con el fin de identificar los usuarios que no están operando el sistema asignado.<br><br>Los administradores de los sistemas de información deben inactivar los usuarios que no estén ingresando a los diferentes aplicativos. | |

| Procedimiento: Revisión de los derechos de acceso de usuarios | | | | |
|---|---|---|---|---|
| | Actividad | Tarea | Responsable | Registros |
| 1 | Revisar los derechos de acceso a los sistemas de información | Los administradores de los diferentes aplicativos deben revisar los derechos de acceso de los usuarios en los aplicativos que se les ha dado permisos de acceso, por lo menos dos veces al año | Dirección de Infraestructura Tecnológica(administradores de los sistemas de información) | |
| 2 | Generar reportes de uso de los sistemas de información | Los administradores de los sistemas de información deberán generar reportes de uso de cada una de los sistemas de información con el fin de identificar la periodicidad de ingreso de cada uno de los usuarios. | | |
| 3 | Informar a las dependencias los usuarios que no ingresan a los diferentes sistemas de información. | Los administradores de los sistemas de información deben informar por comunicado SAIA a los líderes de los procesos donde operan los aplicativos, indicando los usuarios que no están usando los sistemas de información para que puedan ser inactivados en el sistema. | Dirección de Infraestructura Tecnológica(administradores de aplicativos) | Comunicado SAIA |

| | | | | |
|---|---|---|---|---|
| 4 | Respuesta informando los usuarios que no operan aplicativos. | Los líderes de los procesos deben dar la respuesta a la Dirección de Infraestructura Tecnológica, por comunicado SAIA, indicando los usuarios que se deben inactivar en los diferentes sistemas de información. | Líderes de los procesos | Comunicado SAIA |
| 5 | Inactivar los usuarios en los sistemas de información. | Los administradores de los sistemas de información proceden a inactivar los usuarios que no presentan historial de uso y que fueron informados por los líderes de los procesos de las diferentes dependencias. | Dirección de Infraestructura Tecnológica(administradores de aplicativos) | Comunicado SAIA |

| Dominio | Norma ISO 27001:2013<br>**Soporte** |
|---|---|
| Subdominio | **A.9 Control de acceso** |
| Etapa | **A.9.2 Gestión de acceso de usuarios** |
| Objetivo de control | Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios. |
| Control | A.9.2.6 Retiro o ajustes de los derechos de acceso:<br>Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios. |

| Control A.9.2.6: Retiro o ajustes de los derechos de acceso | |
|---|---|
| Controles relacionados:<br>Comunicado SAIA. | |
| Manuales: | N/A |
| Propósito:<br>Los derechos de acceso a la información de todos usuarios de los sistemas de información se deberían retirar al terminar su empleo, contrato o se deberían ajustar cuando se hagan cambios.<br><br>Lineamientos generales:<br>El retiro o ajuste para el acceso a los diferentes Sistemas de información se deberá hacer inmediatamente se tenga conocimiento de la solicitud.<br><br>Es obligación de la Dirección de Talento Humano y de los supervisores de los contratistas dar a conocer a la Dirección de Infraestructura Tecnológica el retiro, cambio o cualquier novedad que se presente con los funcionarios de la Alcaldía de Pereira. | |

| Procedimiento: Retiro o ajuste de los derechos de acceso | | | | |
|---|---|---|---|---|
| | Actividad | Tarea | Responsable | Registros |
| 1 | Informar el retiro, | Se debe realizar la solicitud por | Dirección de Talento | Comunicado SAIA |

| | | | | |
|---|---|---|---|---|
| | suspensión o cualquier novedad administrativa que se presente con los Servidores Públicos y contratistas. | comunicado SAIA informando la novedad de la desvinculación laboral o término del contrato (personal de planta o contratistas), se solicitara inactivar el acceso a los diferentes aplicativos. | Humano<br><br>Líderes de los Procesos.<br><br>Supervisores de los contratistas | |
| 2 | Realizar inactivación del usuario | La Dirección de Infraestructura Tecnológica recibe la solicitud por comunicado SAIA y realiza la inactivación de los diferentes perfiles de acceso a los aplicativos y redes. | Dirección de Infraestructura Tecnológica | |
| 3 | Informar la novedad | La dirección de Infraestructura Tecnológica debe informar al funcionario que realizo la solicitud el retiro o ajuste de los derechos de acceso a los diferentes aplicativos del personal que termino su vinculación laboral o requirió algún cambio. | Dirección de Infraestructura Tecnológica | Comunicado SAIA |

| Dominio | Norma ISO 27001:2013<br>**Soporte** |
|---|---|
| Subdominio | **A.9 Control de acceso** |
| Etapa | **A.9.3 Responsabilidades de los usuarios**<br>**A.9.4 Control de acceso a sistemas y aplicaciones** |
| Objetivo de control | -Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.<br>-Evitar el acceso no autorizado a sistemas y aplicaciones. |
| Control | A.9.3.1 Uso de la información de autenticación secreta:<br>Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.<br>A.9.4.3 Sistemas de gestión de contraseñas:<br>Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas. |

| | |
|---|---|
| Control A.9.3.1: Uso de la información de autenticación secreta.<br>A.9.4.3: Sistema de gestión de contraseñas. | |
| Controles relacionados: Forzar en los sistemas de información el cambio inicial de contraseñas, comunicado SAIA. | |
| Manuales: | N/A |
| Propósito:<br><br>Exigir a los Servidores Públicos, contratistas, practicantes, pasantes, que cumplan funciones en la Alcaldía de Pereira, el uso de información de autenticación secreta (contraseñas).<br><br>Lineamientos generales:<br><br>Se debe mantener los datos de acceso (contraseñas) en secreto.<br>Las contraseñas deben ser fáciles de recordar y difíciles de adivinar.<br>Las contraseñas no estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento.<br>Los Servidores Públicos, contratistas, practicantes, pasantes de la Alcaldía de Pereira son responsables del uso y manejo de las contraseñas de acceso a los sistemas de información que se le asignen, las contraseñas se deben cambiar obligatoriamente cada 6 meses o cuando lo indique la Dirección de Infraestructura Tecnológica. | |

| Procedimiento: Uso de la información de autenticación. Sistema de gestión de contraseñas. | | | | |
|---|---|---|---|---|
| | Actividad | Tarea | Responsable | Registros |
| 1 | Forzar el cambio periódico de contraseñas al ingreso de los sistemas de información | Los administradores de los sistemas de información deben programar el cambio de contraseñas cada 6 meses, el cual debe estar aprobado por el Director de Infraestructura Tecnológica. | Administradores de los sistemas de información | |
| 2 | Informar del cambio de contraseñas para el ingreso de los diferentes sistemas de información | Director de Infraestructura Tecnológica debe informar el cambio de contraseñas a los funcionarios de la Alcaldía de Pereira por el aplicativo SAIA. | | Comunicado SAIA |
| 3 | Forzar el cambio inicial de contraseñas para usuarios nuevos | Los administradores de los sistemas de información deben garantizar que en primer ingreso de los usuarios nuevos, sea obligatorio el cambio de contraseña. | | |
| 3 | Forzar el bloqueo del sistemas después de 3 (tres) intentos de ingreso no exitosos a los diferentes sistemas de información | Los administradores de los sistemas de información deben asegurar que después del tercer intento de ingreso no exitoso a los diferentes aplicativos el sistema se debe bloquear automáticamente. | | |

| Dominio | Norma ISO 27001:2013<br>**Soporte** |
|---|---|
| Subdominio | **A.9 Control de acceso** |
| Etapa | **A.9.4 Control de acceso a sistemas y aplicaciones** |
| Objetivo de control | Evitar el acceso no autorizado a sistemas y aplicaciones |
| Control | A.9.4.1 Restricción de acceso a la información:<br>El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso. |

| Control A.9.4.1: Restricción de acceso a la información | |
|---|---|
| Controles relacionados:<br>Comunicado SAIA “Solicitud para la creación y renovación de usuarios” | |
| Manuales: | N/A |
| Propósito:<br><br>Garantizar el acceso de forma segura a los sistemas de información de acuerdo a las funciones del cargo que se desempeña.<br><br>Lineamientos generales:<br><br>Establecer diferentes perfiles en la asignación de accesos a los sistemas de información de la Alcaldía de Pereira. | |

| Procedimiento: Restricción de acceso a la información | | | | |
|---|---|---|---|---|
| | Actividad | Tarea | Responsable | Registros |
| 1 | Realizar la solicitud para el acceso a los sistemas de información o diferentes aplicativos. | La solicitud para una cuenta de usuario se debe realizar por el aplicativo SAIA ingresando a la parte de formatos, se selecciona “solicitud para la creación y la | Funcionarios de la administración | Comunicado SAIA(Solicitud para la creación y renovación de perfiles) |

| | | | | |
|---|---|---|---|---|
| | | renovación de perfiles", indicar si es funcionario o contratista con el número de contrato, fecha de inicio y terminación del mismo.<br><br>Para solicitar un usuario para el ingreso a los diferentes aplicativos, se debe enviar un comunicado SAIA debidamente autorizado por el líder del proceso, la autorización para los privilegios de acceso se debe realizar de acuerdo a las funciones de la labor a desempeñar | | |
| 2 | Activar los diferentes perfiles y asignar usuarios y contraseñas | Se activan los perfiles y se da respuesta por el aplicativo SAIA, indicando el usuario y contraseña para el aplicativo para el cual se realizó la solicitud para el permiso de acceso | Dirección de Infraestructura Tecnológica | Comunicado SAIA |

| Dominio | Norma ISO 27001:2013 |
|---|---|
| Subdominio | **A.9 Control de acceso** |
| Etapa | **A.9.4 Control de acceso a sistemas y aplicaciones** |
| Objetivo de control | Evitar el acceso no autorizado a sistemas y aplicaciones |
| Control | A.9.4.2 Procedimiento de ingreso seguro a los aplicativos: El acceso a los sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro. |

| Control A.9.4.2: Procedimiento de ingreso seguro a los aplicativos | |
|---|---|
| Controles relacionados: Bloqueo automático de sección después de 5 minutos de inactividad en el equipo de cómputo. | |
| Manuales: | N/A |
| Propósito:<br>Controlar mediante un ingreso seguro, el acceso a sistemas y aplicaciones.<br><br>Lineamientos generales:<br><br>El acceso a los sistemas o aplicaciones deberá estar protegido, mediante un inicio seguro de sesión. | |

| Procedimiento: Procedimiento de ingreso seguro a los aplicativos | | | | |
|---|---|---|---|---|
| | Actividad | Tarea | Responsable | Registros |
| 1 | Después de cinco (5) minutos de inactividad del sistema, se deberá bloquear la sesión. | Los administradores de los sistemas de información deben garantizar que después de 5 minutos de inactividad del sistema o aplicación se deberá bloquear la sesión | Administradores de los sistemas de información | |
| 2 | Limitar el número de intentos fallidos de conexión | Los administradores de los sistemas de información deben asegurar que después | Administradores de los sistemas de información | |

| | | | | |
|---|---|---|---|---|
| | auditando los intentos no exitosos hasta un máximo de (3) intentos. | del 3 intento de ingreso no exitoso a los diferentes aplicativos el sistema se debe bloquear | | |
| 3 | No suministrar mensajes de ayuda, durante el proceso de autenticación. | Los administradores de los sistemas de información deben garantizar que durante el proceso de autenticación de los usuarios en los aplicativos, no muestre mensajes de ayuda. | Administradores de los sistemas de información | |

| Dominio | Norma ISO 27001:2013<br>**Soporte** |
|---|---|
| Subdominio | **A.9 Control de acceso** |
| Etapa | **A.9.4 Control de acceso a sistemas y aplicaciones** |
| Objetivo de control | Evitar el acceso no autorizado a sistemas y aplicaciones |
| Control | A.9.4.4 Uso de programas utilitarios y privilegiados:<br>Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones. |

| Control A.9.4.4: Uso de programas utilitarios y privilegiados | |
|---|---|
| Controles relacionados:<br>Verificación por el aplicativo OCS.<br>PDE_TICS_Registro_De_Actividades_Anexas_A_La_Prestación_Del_Servicio | |
| Manuales: | N/A |
| Propósito:<br>Restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema o las aplicaciones.<br><br>Lineamientos generales:<br><br>Deshabilitar los programas utilitarios privilegiados de la plataforma tecnológica<br><br>Mantener actualizado un listado de programas utilitarios privilegiados de la plataforma tecnológica<br><br>Verificar que los usuarios de la plataforma tecnológica y los sistemas de información, no tengan instalados en sus equipos de cómputo programas utilitarios que permitan evadir controles de seguridad y privacidad de la información. | |

| 9.8.1 Procedimiento: Uso de programas utilitarios y privilegiados | | | | |
|---|---|---|---|---|
| | Actividad | Tarea | Responsable | Registros |
| 1 | Configurar el conjunto mínimo requerido de funcionalidades | La Mesa de Servicios Tecnológicos debe configurar el conjunto mínimo requerido de funcionalidades o | Mesa de servicios tecnológicos | |

| | | | | |
|---|---|---|---|---|
| | o programas utilitarios. | programas utilitarios que se deben instalar en cada estación de trabajo en las dependencias de la Alcaldía de Pereira | | |
| 2 | Verificación periódica del software no licenciado. | Se debe realizar la verificación trimestral por el aplicativo OCS para el control de software instalado y no licenciado en los equipos de cómputo. | Mesa de Servicios Tecnológicos | Aplicativo OCS |
| 3 | Eliminación de software no licenciado | Realizar la eliminación de software no licenciado aprobado por el municipio y llenar registro de actividades anexas a la prestación del servicio | Mesa de Servicios Tecnológicos | PDE_TICS_Registro_De_Actividades_Anexas_A_La_Prestación_Del_Servicio |

| Dominio | Norma ISO 27001:2013<br>**Soporte** |
|---|---|
| Subdominio | **A.9 Control de acceso** |
| Etapa | **A.9.4 Control de acceso a sistemas y aplicaciones** |
| Objetivo de control | Evitar el acceso no autorizado a sistemas y aplicaciones |
| Control | A.9.4.5 Control de acceso a códigos fuentes de programas.<br>Se debería restringir el acceso a los códigos fuente de los programas. |

| Control A.9.4.5: Control de acceso a códigos fuentes de programas. | |
|---|---|
| Controles relacionados: PDE_TICS_Inventario_De_Software | |
| Manuales: | N/A |
| Propósito:<br>Restringir el acceso a los códigos fuente de los programas.<br><br>Lineamientos generales:<br>Las librerías de los sistemas de información no deberán estar contenidas en el ambiente de las bases de datos.<br><br>El acceso al código fuente de los programas debe ser limitado, solo pueden ingresar los ingenieros desarrolladores o ingenieros de soporte autorizados por la Dirección de Infraestructura Tecnológica. | |

| Procedimiento: Control de acceso a códigos fuentes de programas. | | | | |
|---|---|---|---|---|
| | Actividad | Tarea | Responsable | Registros |
| 1 | Limitar el acceso a los códigos fuentes de los aplicativos | Se debe restringir el acceso a los códigos fuentes de los programas, solo puede acceder al código fuente los ingenieros desarrolladores o ingenieros de soporte autorizados por la Dirección de Infraestructura | Dirección de Infraestructura Tecnológica | |

| | | | | |
|---|---|---|---|---|
| | | Tecnológica. | | |
| 2 | Llevar un registro actualizado de todos los programas en uso. | La Dirección de Infraestructura Tecnológica debe llevar el registro actualizado de todos los aplicativos en uso licenciados, indicando nombre del programa, versión, última actualización | Dirección de Infraestructura Tecnológica | PDE_TICS_Inventario_De_Software |

## 11 SEGURIDAD FÍSICA Y DEL ENTORNO

| Dominio | Norma ISO 27001:2013<br>**Soporte** |
|---|---|
| Subdominio | **A.11 Seguridad física y del entorno** |
| Etapa | **A.11.1 Áreas seguras** |
| Objetivo de control | 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. |
| Control | A.11.1.2 Controles físicos de entrada:<br>Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado |

| Control A.11.1.2: Controles físicos de entrada | |
|---|---|
| Controles relacionados: Minuta para el ingreso al data center | |
| Manuales: | Control de ingreso físico al data center |
| Propósito:<br>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.<br><br>Lineamientos generales:<br><br>Los colaboradores o terceras partes que dispongan de acceso al centro de datos, deberán ser específicamente los autorizados para su uso por la Dirección de infraestructura tecnológica.<br><br>Se deberá otorgar los privilegios para la administración de recursos tecnológicos, servicios de red y sistemas de información únicamente a aquellos colaboradores que cumplan dichas funciones.<br><br>Se deberá restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deberá permitir el acceso a los colaboradores autorizados por la Dirección de infraestructura tecnológica.<br><br>El retiro de los privilegios al centro de datos y conexiones remotas se deberá | |

hacer inmediatamente se termine el contrato o su vínculo laboral.

El perímetro de las áreas que contienen la información y sus instalaciones de procesamiento sensible o crítico deberán estar protegidos de accesos no permitidos.

Las puertas y ventanas deberán permanecer cerradas con llave cuando no hay supervisión o están desocupadas.

La Dirección de infraestructura tecnológica será responsable, de administrar el ingreso y salida del personal del centro de datos.

La Dirección de infraestructura tecnológica será responsable de llevar el control de ingreso y salida de personal de los centros de datos de la Alcaldía de Pereira.

La Dirección de infraestructura tecnológica autorizara el ingreso a personal ajeno a la Alcaldía de Pereira a los centros de datos para fines laborales, este deberá estar acompañado por quien sea autorizado, este se hará responsable de la estadía del personal ajeno a la Alcaldía de Pereira durante el tiempo que permanezca en las instalaciones.

La Dirección de infraestructura tecnológica, las secretarias administrativas deberán autorizar cambios, modificaciones y/o reparaciones por parte de personal externo o que no pertenezcan a la Alcaldía de Pereira.

Todo el personal que ingrese al Data-center o centros de datos deberá portar identificación visible y presentarla en la puerta de acceso antes de su ingreso.

La Dirección de infraestructura tecnológica deberá controlar que los centros de datos permanezcan siempre con las puertas de acceso cerradas y con controles de seguridad para el acceso a personal no autorizado.

La Dirección de infraestructura tecnológica deberá implementar y administrar los circuitos cerrados de televisión (CCTV) para los centros de cableado y Data-center, esto con el fin de tener un monitoreo permanente de los mismos.

La Dirección de Información y Tecnología deberá mantener libre de objetos o elementos que no sean propios del Data-center.

No se debe consumir líquidos y fumar en cercanías de las instalaciones de procesamiento de información.

| Procedimiento: Control de acceso centro de datos | | | | |
|---|---|---|---|---|
| | Actividad | Tarea | Responsable | Registros |
| 1 | Solicitud de ingreso | El funcionario o persona externa que va a ingresar al cuarto de datos debe realizar la solicitud al Director de Infraestructura Tecnológica, la solicitud se debe realizar por comunicado SAIA o correo electrónico. | Funcionarios públicos | Oficio SAIA, Correo electrónico |
| 2 | Dar respuesta a la solicitud | El Director de Infraestructura Tecnológica da respuesta indicando el día y hora para el ingreso al data-center | Director de Infraestructura Tecnológica | Oficio SAIA o correo electrónico |
| 3 | Identificación para el ingreso | El funcionario que va ingresar debe mostrar el carnet de identificación o la autorización para el ingreso al data center | Persona encargada de llevar el control y el registro | Minuta para ingreso al data-center |
| 4 | Registro en el libro de ingreso | La persona encargada debe registrar en la minuta la fecha, hora de ingreso, hora de salida, nombre, cedula, cargo, actividad a realizar del funcionario o la persona que va a ingresar a realizar | Persona encargada de llevar el control y el registro. | Minuta para ingreso al data-center |

| | | | | |
|---|---|---|---|---|
| | | alguna actividad | | |
| 5 | Solicitud de llaves | El director de infraestructura tecnología debe entregar las llaves al personal para el ingreso | Director operativo de infraestructura tecnológica | Minuta para ingreso al data-center |
| 6 | Registro salida del cuarto de datos | El funcionario debe firmar con fecha y hora de salida del data-center | Persona encargada de llevar el control y el registro. | Minuta para ingreso al data-center |

| Dominio | Norma ISO 27001:2013<br>**Soporte** |
|---|---|
| Subdominio | **A.11 Seguridad física y del entorno** |
| Etapa | **A.11.2 Equipos** |
| Objetivo de control | Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización. |
| Control | A.11.2.1 Ubicación y protección de equipos:<br>Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado. |

| Control A.11.2.1: Ubicación y protección de equipos | |
|---|---|
| Controles relacionados: Controles contra incendio, control de temperatura. | |
| Manuales: | N/A |
| Propósito:<br><br>Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno.<br><br>Lineamientos generales:<br><br>No se debe comer, fumar y consumir líquidos en cercanías de los equipos de procesamiento de información.<br><br>Se debe disponer de controles contra incendio, humo e interferencia del suministro eléctrico.<br><br>El centro de datos de la Alcaldía de Pereira, debe contar con un control de temperatura determinado por el aire acondicionado. | |

| Procedimiento: Ubicación y protección de equipos | | | | |
|---|---|---|---|---|
| | Actividad | Tarea | Responsable | Registros |
| 1 | Disponer de controles contra incendio, humo e interferencia del suministro eléctrico | La Gestión de recursos Administrativos debe garantizar la disponibilidad de sensores de humo, controles en caso de incendio y la interferencia del suministro eléctrico en los cuartos de datos y de red. | Gestión de Recursos Administrativos<br><br>Dirección de Infraestructura Tecnológica | N/A |
| 2 | Control de temperatura | El cuarto de los servidores y de red, debe existir un control de temperatura determinado por el aire acondicionado. | Gestión de Recursos Administrativos<br><br>Dirección de Infraestructura Tecnológica | N/A |

| Dominio | Norma ISO 27001:2013<br>**Soporte** |
|---|---|
| Subdominio | **A.11 Seguridad física y del entorno** |
| Etapa | **A.11.2 Equipos** |
| Objetivo de control | Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización. |
| Control | A.11.2.2 Servicios de suministro:<br>Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. |

| Control A.11.2.2: Servicios de suministro | |
|---|---|
| Controles relacionados: | |
| Manuales: | N/A |
| Propósito:<br><br>Proteger los equipos contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.<br><br>Lineamientos generales:<br><br>Todos los Servidores Públicos, contratistas, practicantes, pasantes de la Alcaldía de Pereira deben usar la red de energía regulada, en los puestos de trabajo solo se deberán conectar CPU, portátiles, los otros equipos y elementos deberán conectarse a la red no regulada.<br><br>Se debe garantizar el flujo adecuado de energía por interrupciones causados por fallas de las empresas de energía. | |

| Procedimiento: Servicios de suministro | | | | |
|---|---|---|---|---|
| | Actividad | Tarea | Responsable | Registros |
| 1 | Inspeccionar regularmente el adecuado | Dirección de Infraestructura | Servicios Generales | |

| | | | | |
|---|---|---|---|---|
| | funcionamiento la red de energía regulada y no regulada. | Tecnológica deberá inspeccionar regularmente la red de energía regulada.<br><br>La dependencia de Servicios Generales deberá inspeccionar regularmente la red de energía no regulada para asegurar el funcionamiento apropiado | Dirección de Infraestructura Tecnológica | |
| 2 | Garantizar el flujo adecuado de energía. | La dependencia de Servicios Generales debe garantizar el flujo adecuado de energía suministrado por la planta eléctrica causado por fallas en el servicio de la red de energía externa | Servicios Generales | |
| 3 | Verificar el uso de la red de energía regulada y no en los puestos de trabajo | Verificar periódicamente que las CPU estén conectadas en la red regulada. | Dirección de Infraestructura Tecnológica<br><br>Servicios generales | |

| Dominio | Norma ISO 27001:2013<br>**Soporte** |
|---|---|
| Subdominio | **A.11 Seguridad física y del entorno** |
| Etapa | **A.11.2 Equipos** |
| Objetivo de control | Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización. |
| Control | A.11.2.3 Seguridad del cableado:<br>El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño. |

| Control A.11.2.3: Seguridad del cableado | |
|---|---|
| Controles relacionados: | |
| Manuales: | N/A |
| Propósito:<br><br>El cableado de potencia y de telecomunicaciones que soportan datos o servicios de información debería estar protegido contra interceptación, interferencia o daño.<br><br>Lineamientos generales:<br><br>Realizar revisiones periódicas del cableado que transporta datos y energía para garantizar su adecuado funcionamiento.<br><br>El cableado que transporta datos y energía este protegido contra la interferencia o daños por canaletas. | |

| 10.3.1 Procedimiento: Seguridad del cableado | | | | |
|---|---|---|---|---|
| | Actividad | Tarea | Responsable | Registros |
| | Garantizar que el cableado que transporta datos y energía | La oficina de Servicios Generales y la Dirección de Infraestructura | Servicios Generales<br><br>Dirección de | |

| | | | | |
|---|---|---|---|---|
| | este protegido. | Tecnológica deben garantizar que el cableado que transporta datos y energía este protegido contra la interferencia o daños. | Infraestructura Tecnológica | |
| | Verificación del cableado que transporta datos y energía. | La oficina de Servicios Generales y la Dirección de Infraestructura Tecnológica deben verificar que los cables de comunicaciones y datos estén separados de los cables de energía eléctrica para evitar interferencia y que estén protegidos por canaletas. | Servicios Generales<br><br>Dirección de Infraestructura Tecnológica | |

| Dominio | Norma ISO 27001:2013<br>**Soporte** |
|---|---|
| Subdominio | **A.11 Seguridad física y del entorno** |
| Etapa | **A.11.2 Equipos** |
| Objetivo de control | Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización. |
| Control | A.11.2.4 Mantenimiento de equipos:<br>Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.<br>. |

| Control A.11.2.4: Mantenimiento de equipos | |
|---|---|
| Controles relacionados:<br>PDE_TICS_Cronograma_De_Actividades_Mesa_De_Ayuda.<br>PDE_TICS_Mantenimientos_Preventivos_Y_Correctivos_De_Hardware_Y_Software_v1 | |
| Manuales: | N/A |
| Propósito:<br><br>Los equipos se deberían mantener correctamente para asegurar su disponibilidad, integridad y buen funcionamiento.<br><br>Lineamientos generales:<br><br>La Dirección de Infraestructura Tecnológica deberá elaborar el cronograma de mantenimiento preventivo de los equipos de la Alcaldía de Pereira.<br><br>Solo los técnicos de mantenimiento pueden realizar el soporte técnico de los equipos y reparaciones.<br><br>Para las actividades de mantenimiento preventivo, se debe informar a los funcionarios de administración municipal con anterioridad al día en que se va a realizar el mantenimiento del equipo de cómputo. | |

| Procedimiento: Mantenimiento de equipos | | | | |
|---|---|---|---|---|
| | Actividad | Tarea | Responsable | Registros |
| 1 | Elaborar Cronograma de mantenimiento | Se debe elaborar el cronograma de ejecución y mantenimiento preventivo de la infraestructura tecnológica | Coordinación Mesa de Servicios Tecnológicos. | PDE_TICS_Cronograma_De_Actividades_Mesa_De_Ayuda |
| 2 | Informar el mantenimiento a realizar | Para las actividades de mantenimiento preventivo el coordinador de la mesa de servicios tecnológicos, debe informar a los funcionarios de administración municipal con anterioridad al día en que se va a realizar el mantenimiento del equipo de cómputo | Coordinación Mesa de Servicios Tecnológicos | |
| 3 | Realizar inventario de Hardware y Software. | Se debe realizar el inventario de Hardware y Software del Equipo, realizar mantenimiento, instalación, movimientos adiciones y cambios del Software que se requieran. | Personal Técnico Mesa de Servicios Tecnológicos. | PDE_TICS_Mantenimientos_Preventivos_Y_Correctivos_De_Hardware_Y_Software_v1 |

| Dominio | Norma ISO 27001:2013<br>**Soporte** |
|---|---|
| Subdominio | **A.11 Seguridad física y del entorno** |
| Etapa | **A.11.2 Equipos** |
| Objetivo de control | Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización. |
| Control | A.11.2.5 Retiro de activos:<br>Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.<br>. |

| 10.5 Control A.11.2.5: Retiro de activos | |
|---|---|
| Controles relacionados: FUG GR Salida de elementos - equipos V1 | |
| Manuales: | N/A |
| Propósito:<br>Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.<br><br>Lineamientos generales:<br><br>Se deberán registrar los equipos de cómputo que salgan o ingresen de la Alcaldía de Pereira. | |

| Procedimiento: Retiro de activos | | | | |
|---|---|---|---|---|
| | Actividad | Tarea | Responsable | Registros |
| 1 | Solicitud para el retiro de equipos en préstamo solo para actividades propias de la entidad | En caso que el equipo dependa de la Secretaria de las TIC, para retirar un equipo fuera de las dependencias de la Alcaldía se debe realizar la solicitud por el aplicativo Mantis indicando el equipo | Funcionarios de la administración | Solicitud aplicativo MANTIS |

| | | | | |
|---|---|---|---|---|
| | | que se requiere sacar. | | |
| 2 | Respuesta informando la disponibilidad del equipo | Se da respuesta por el aplicativo MANTIS al funcionario que realizo la solicitud indicando la disponibilidad del equipo, el cual procede a recoger el equipo y a firmar el libro de préstamos de equipos.<br><br>También debe diligenciar el formato "salida de elementos y/o equipos", el cual debe estar firmado por el líder del proceso al que pertenece el funcionario solicitante | Dirección de Infraestructura Tecnológica | Respuesta aplicativo MANTIS<br><br>Libro prestamos de equipos |
| 3 | Retiro de equipos de la entidad | Para retirar el equipo de la entidad se debe presentar el formato “salida de elementos y/o equipos" en la portería, los guardas de seguridad quedan con este formato, el cual se verificara de nuevo en el ingreso a la Alcaldía de Pereira. | Funcionarios de la administración<br><br>Guardas de seguridad | FUG GR Salida de elementos - equipos V1 |

| Dominio | Norma ISO 27001:2013<br>**Soporte** |
|---|---|
| Subdominio | **A.11 Seguridad física y del entorno** |
| Etapa | **A.11.2 Equipos** |
| Objetivo de control | Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización. |
| Control | A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones:<br>Se deberían 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. |

| 10.6 Control A.11.2.6: Seguridad de equipos y activos fuera de las instalaciones | |
|---|---|
| Controles relacionados: Póliza de riesgos | |
| Manuales: | N/A |
| Propósito:<br><br>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.<br><br>Lineamientos generales:<br><br>Los equipos de procesamiento de información que se autorizan para trasladarse o mantenerse fuera de las instalaciones se protegen mediante pólizas de seguros. | |

| 10.6.1 Procedimiento: Seguridad de equipos y activos fuera de las instalaciones | | | | |
|---|---|---|---|---|
| | Actividad | Tarea | Responsable | Registros |
| 1 | Disponer de pólizas de seguros para | La Administración de Bienes y Recursos Físicos debe | La Administración de Bienes y | Póliza de riesgos. |

| | | | | |
|---|---|---|---|---|
| | los equipos de procesamiento. | garantizar que los equipos que se autorizan para trasladarse fuera de las instalaciones este protegido mediante pólizas de seguros. | Recursos Físicos | |

| Dominio | Norma ISO 27001:2013<br>**Soporte** |
|---|---|
| Subdominio | **A.11 Seguridad física y del entorno** |
| Etapa | **A.11.2 Equipos** |
| Objetivo de control | Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización. |
| Control | A.11.2.7 Disposición segura o reutilización de equipos:<br><br>Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización. |

| 10.7 Control A.11.2.7: Disposición segura o reutilización de equipos | |
|---|---|
| Controles relacionados:<br>PDE_TICS_Formato_De_Certificación_Para_Concepto_Técnico_De_Equipos_De_Computación_Y_Accesorios. | |
| Manuales: | N/A |
| Propósito:<br>Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado en forma segura antes de su disposición o reutilización.<br><br>Lineamientos generales:<br><br>Se debe tener actualizado el inventario de licencias.<br><br>Garantizar que los medios de almacenamiento que contengan cualquier dato sensible o software con licencia, se han eliminado de forma segura antes de su disposición final o reutilización. | |

| 10.7.1 Procedimiento: Disposición segura o reutilización de equipos. | | | | |
|---|---|---|---|---|
| | Actividad | Tarea | Responsable | Registros |
| 1 | Realizar borrado seguro. | La Mesa de Servicios Tecnológicos debe | Mesa de Servicios | |

| | | | | |
|---|---|---|---|---|
| | | garantizar que los medios de almacenamiento de los equipos que estén para dar de baja o estén para reutilización, se debe realizar el borrado seguro. | Tecnológicos. | |
| 2 | Diligenciar formato de borrado seguro | La Mesa de Servicios Tecnológicos debe registrar en el formato de borrado seguro la realización del procedimiento de borrado del medio de almacenamiento. | | PDE_TICS_Formato_De_Certificación_Para_Concepto_Técnico_De_Equipos_De_Computación_Y_Accesorios |

| Dominio | Norma ISO 27001:2013<br>**Soporte** |
|---|---|
| Subdominio | **A.11 Seguridad física y del entorno** |
| Etapa | **A.11.2 Equipos** |
| Objetivo de control | Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización. |
| Control | A.11.2.8 Equipos de usuarios desatendidos:<br><br>Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada. |

| 10.8 Control A.11.2.8: Equipos de usuarios desatendidos | |
|---|---|
| Controles relacionados: Procedimiento equipos de usuarios desatendidos. | |
| Manuales: | N/A |
| Propósito:<br>Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.<br><br>Lineamientos generales:<br>Los funcionarios de la Alcaldía de Pereira no deben dejar encendidos los equipos de cómputo en horas no laborables.<br><br>Los funcionarios de la Alcaldía de Pereira deben bloquear sus estaciones de trabajo en el momento de abandonar su puesto de trabajo.<br><br>Los funcionarios de la Alcaldía de Pereira deberán bloquear la pantalla del computador a su cargo cuando se ausenten de su puesto de trabajo. | |

| 10.8.1 Procedimiento: Equipos de usuarios desatendidos | | | | |
|---|---|---|---|---|
| | Actividad | Tarea | Responsable | Registros |
| 1 | Configurar protector de pantalla. | La Mesa de Servicios Tecnológicos debe garantizar que los | La Mesa de Servicios Tecnológicos | |

| | | | | |
|---|---|---|---|---|
| | | computadores tengan configurado el protector de pantalla con un tiempo máximo de cinco (5) minutos para que se active cuando el equipo no esté en uso y bloquee el acceso con contraseña. | | |
| 2 | Bloquear estaciones de trabajo | Los funcionarios de la Alcaldía de Pereira deben bloquear sus estaciones de trabajo en el momento de abandonar su puesto de trabajo | Usuarios de los equipos de cómputo. | |
| 3 | Apagar los equipos de cómputo en horas no laborales. | Los funcionarios de la Alcaldía de Pereira no deben dejar encendidos los equipos de cómputo en horas no laborables. | Usuarios de los equipos de cómputo | |