POLITICA DE SEGURIDADY PRIVACIDAD DE LA INFORMACIÓN

Armenia, enero de 2023

COMITÉ COORPORATIVO

JHON FABIO SUAREZ VALERO	Gerente General.
JOHN ALEXANDER MORALES ARENAS	Secretario General.
ALBA LUCIA RODRÍGUEZ SIERRA	Jefe Oficina Control Interno de Gestión.
DARNELLY TORO JIMENEZ	Subgerente de Planeación y Mejoramiento Institucional.
FERNANDO ANDRES SALAZAR GOMEZ	Subgerente Servicios Públicos Domiciliarios.
YURANI VILLEGAS ALZATE	Subgerente de Comercialización de servicios y atención al cliente
MARIA DEL SOCORRO MEJIA Z	Subgerente Administrativa y Financiera.
JHOANA CATALINA ACEVEDO	Jefe Oficina Control Interno Disciplinario.
MARIA FERNANDA PEREZ ROJAS	Jefe de Oficina Talento Humano

TABLA DE CONTENIDO

CONTENIDO

1. PROPÓSITO

Proporcionar una serie de reglas, lineamientos y mecanismos para garantizar disponibilidad, confidencialidad e integridad los activos informáticos (computadores, redes de datos, software, procesos y funcionarios) de Empresas Públicas del Quindío EPQ S.A. ESP conectados o no a la red interna y a la información que ellos procesan o intercambien. La protección de los activos de una amplia gama de amenazas, asegura la continuidad de la operación de los servicios y funciones, minimiza los daños de la organización, maximiza la eficiencia de la administración pública y el mejoramiento continuo, propicia aumentar la confianza de la administración local ante terceros proveedores, contratistas y ciudadanos, conoce los posibles riesgos en la seguridad de la información, reduce el tiempo de respuesta a los incidentes, y provee mejores prácticas en el aseguramiento de la información. Finalmente, apoyar y controlar el cumplimiento de los requisitos legales, reglamentarios, contractuales y técnicos que haya lugar en su aplicación.

En la actualidad la información de Empresas Públicas del Quindío S.A. ESP se ha reconocido como un activo valioso, y a medida que los sistemas de información apoyan cada vez más los procesos de misión crítica se requiere contar con estrategias de alto nivel que permitan el control y administración efectiva de los datos. En nuestra institución, los sistemas y red de información enfrentan amenazas de seguridad que incluyen, entre muchas otras: el fraude por computadora, espionaje, sabotaje, vandalismo, fuego, robo e inundación. Las posibilidades de daño y pérdida de información por causa de código malicioso, mal uso o ataques de denegación de servicio se hacen cada vez más comunes.
Con la promulgación de la presente Política de Seguridad de la Información la Empresas Públicas del Quindío S.A. ESP, formaliza su compromiso con el proceso de gestión responsable de información que tiene como objetivo garantizar la integridad, confidencialidad y disponibilidad de este importante activo, teniendo como eje el cumplimiento de los objetivos misionales.

2. OBJETIVOS

Disponer de una guía sobre las políticas de seguridad informática de las EMPRESAS PÚBLICAS DEL QUINDIO S.A. (E.S.P) para orientar a los funcionarios, profesionales,

contratistas o terceros sobre la información obtenida, en especial enuncia los principios lineamientos y buenas prácticas en aspectos de seguridad y privacidad de la información, con sistemas que apoyan la gestión de la organización, servicios informáticos, equipos de cómputo, redes de datos, seguridad informática entre otros.

2.1. Objetivos Específicos

- Definir las políticas de seguridad y privacidad de la información de Empresas Públicas del Quindío.
- Establecer lineamiento para la implementación y verificación del cumplimiento de las Políticas de seguridad y privacidad de la información de la entidad.
- Definir los roles y responsabilidades para la administración de la seguridad y privacidad de la información.
- Conservar un sistema de políticas, procedimientos y estándares actualizados con el fin de mantener su vigencia y eficacia para minimizar los riesgos que puedan afectar los activos de la empresa.
- Consolidar una cultura de seguridad y privacidad de la información en funcionarios, contratistas y usuarios que hacen parte de la entidad.
- Establecer una estrategia de continuidad de los procesos de la empresa cuando se presente un incidente de seguridad de la información

3. DESCRIPCIÓN DE LA POLÍTICA

Las EMPRESAS PÚBLICAS DEL QUINDIO S.A. (E.S.P), por medio de la adaptación e implementación de los lineamientos del modelo de seguridad y privacidad de la información orientado a la gestión de sus buenas prácticas el cual conserva, administra y vigila la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información mediante la gestión de controles en la entidad. Previniendo acontecimientos cumplimiento las obligaciones reglamentarias encaminadas a la protección de los Sistemas de Gestión de Seguridad de la Información controlando el acceso, uso y manejo adecuado de los sistemas informáticos a través de políticas y programas, para mejorar las actividades de los funcionarios.

La gerencia General debe aprobar las políticas de seguridad y privacidad de la información, demostrando así su compromiso con la seguridad de la información en la Empresa EPQ SA ESP. Una vez aprobada dichas políticas, la alta dirección debe revisar periódicamente la aplicabilidad y vigencia de las siguientes políticas específicas de seguridad informática y ejecutar los ajustes necesarios sobre ellas para que sean funcional y se puede seguir exigiendo su cumplimiento por parte de todos los funcionarios y personal suministrado por terceras partes que proveen los servicios de la empresa.

4. RESPONSABILIDADES

Empresas públicas del Quindío EPQ S.A. ESP garantiza el apoyo al proceso de establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del Sistema de Gestión de la Seguridad de la Información, siendo responsabilidad de todos los funcionarios, contratistas y procesos tercerizadas la aplicación de las políticas aquí definidas.

Los jefes de dependencia, previa identificación y valoración de sus activos de información, hacen parte del grupo de responsable de Seguridad de la Información y por tanto deben seguir los lineamientos de gestión enmarcados en esta política y en los estándares, normas, guías y procedimientos recomendados por el Comité de Gestión y Desempeño Institucional y aprobados por las directivas.

- La oficina de gestión sistemas de información es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la Alcaldía. Debe ocuparse también de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros incidentes de seguridad.

- La oficina de gestión sistemas de información debe reportar al Comité de Gestión y Desempeño Institucional un informe sobre los incidentes de seguridad y estado de aplicación de la Política de Seguridad de La información.

- La oficina de gestión sistemas de información es responsable de gestionar la implementación de la política de gestión y análisis de riesgos.

- La oficina de gestión sistemas de información es responsable de gestionar la implementación de la política y/o plan de continuidad del Negocio en armonía con las disposiciones legales y avance en otras áreas de la administración local.

- La oficina de gestión sistemas de información es responsable de la mejora continua de la política de Seguridad de la Información.

- La oficina de gestión sistemas de información es responsable de definir y reportar cuando haya lugar la aplicación las sanciones o medidas disciplinarias en el cumplimiento de la política por parte de los actores de la administración local previa investigación y soporte de la oficina de control interno.

- La oficina de gestión sistemas de información es responsable de disponer y vigilar la comunicación y aplicación de la política de seguridad de la información a todos los funcionarios y contratistas de la administración local, y ciudadanos.

- La oficina de gestión sistemas de información es responsable de brindar a la Sub Secretaria de Tecnologías y Comunicaciones los recursos necesarios para la implementación de la política de seguridad de la información.

- La oficina de gestión sistemas de información es responsable de revisar y actualizar la política de seguridad de la información al menos una vez al año y dejar documentada la acción.

- La oficina de gestión sistemas de información es responsable de un plan de acción anual de revisión y mejora donde se incluyan al menos los responsables, recursos necesarios, mecanismos de evaluación y tiempos aplicables.

5. SEGURIDAD DE LA INFORMACIÓN EN EL RECURSO HUMANO

Todo el personal de Empresas Públicas del Quindío EPQ S.A. ESP, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe debe tener asociado un perfil de uso de los recursos de información, incluyendo el hardware y software asociado. El profesional Universitario de gestión e información debe mantener un directorio completo y actualizado de tales perfiles.

La responsabilidad de custodia de cualquier archivo mantenido, usado o producido por el personal que se retira, o cambia de cargo, recae en el líder del proceso o supervisor del contrato; en todo caso el proceso de cambio en la cadena de custodia de la información debe hacer parte integral del procedimiento de terminación de la relación contractual o de cambio de cargo.

5.1. Responsabilidades del personal de Empresas Públicas del Quindío EPQ S.A ESP

Todo el personal de Empresas Públicas del Quindío EPQ S.A ESP, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y las tareas que desempeñe debe firmar un acuerdo que contenga los términos y condiciones que regulan el uso de recursos de TI y las reglas y perfiles que autorizan el uso de la información institucional.

Los procedimientos para obtener tales perfiles y las características de cada uno de ellos deben ser mantenidos y actualizados por cada dependencia, de acuerdo a los lineamientos dados por el profesional universitario de gestión e información, en cuanto a la información y la Red de Datos, en cuanto a los dispositivos hardware y los elementos software.

Empresas Públicas del Quindío EPQ S.A. ESP, debe contemplar procesos y sanciones disciplinarias para los casos en que se presente usos de información y TI que violen los términos y condiciones.

La oficina de gestión de talento humano junto a la oficina gestión sistemas de información, se encargarán de crear, actualizar, mantener y ejecutar un plan de capacitación en seguridad de la información que propenda por el crecimiento continuo de la conciencia individual y colectiva en temas de seguridad de la información.

La oficina gestión sistemas de información se encargará de tener un centro documental de acceso general con información relacionada con temas de seguridad de la información tales como responsabilidad en la administración de archivos, buenas prácticas, amenazas de seguridad, entre otros.

5.2. Responsabilidades de Usuarios Externos

Todos los usuarios externos y personal de empresas externas deben estar autorizados por un miembro del personal de Empresas Públicas del Quindío quien será responsable del control y vigilancia del uso adecuado de la información y los recursos de TI. El procedimiento para el registro de tales usuarios debe ser creado y mantenido por el profesional universitario de gestión y sistemas de información y Gestión de talento humano. Los usuarios externos deben aceptar por escrito los términos y condiciones de uso de la información y recursos de TI de EPQ.

5.3. Usuarios invitados y servicios de acceso público.

El acceso de usuarios no registrados solo debe ser permitido al sitio web de información la www.epq.gov.co. El acceso y uso a cualquier otro tipo de recurso de información y TI no es permitido a usuarios invitados o no registrados.

6. ALCANCE DE LA POLÍTICA

Los lineamientos que se describen en el presente documento aplican a todos procesos de la gestión de la información y va dirigido a directivos y funcionarios en general que se benefician con la tecnología informática de las Empresas Públicas del Quindío S.A. (E.S.P), incluyendo contratistas y terceros que laboran en las instalaciones de la EMPRESAS PÚBLICAS DEL QUINDIO S.A. E.S.P

7. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

7.1. Propósito: Proporcionar una serie de reglas, lineamientos y mecanismos para garantizar disponibilidad, confidencialidad e integridad de los recursos informáticos en relación con la organización interna para la implementación de la política de seguridad de la información en EPQ S.A. E.S.P

7.2. Descripción de la Política: La política sobre organización de la seguridad de la información cubre aspectos de roles y responsabilidades, segregación de deberes, contactos y procedimiento en caso de incidentes de seguridad de la información, así como aspectos básicos para iniciar la operación y aplicación de la política.

7.3. Responsabilidades

- Las funciones de inspección y vigilancia están a cargo de la oficina de Control Interno a través de la persona que se delegue.
- La oficina de gestión sistemas de información es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la entidad. Debe ocuparse también de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros incidentes de seguridad.

7.4. Organización Interna.

7.4.1. Seguridad de la Información Roles y Responsabilidades: Se deben definir y asignar las responsabilidades en relación con la seguridad de la información.

7.4.2. Separación de deberes: Durante la asignación de tareas se debe evaluar la posibilidad de conflicto de tareas o autorizaciones para que se asegure el uso autorizado y control de acceso en las tareas.

7.4.3. Contacto con las autoridades: Se debe mantener contacto con las autoridades locales, regionales y nacionales para la atención de incidentes de seguridad de la información. Se puede evidenciar mediante la actualización del directorio de autoridades pertinentes.

7.4.4, Contacto con grupos de interés especial: Gestionar la participación con grupos, asociaciones, o grupos especializados en la seguridad de la información.

7.5. Dispositivos Móviles y teletrabajo.

7.5.1. Política Para Dispositivos Móviles: Se debe implementar una política y procedimientos para el tratamiento de dispositivos móviles en Empresas Públicas del Quindío E.PQ. S.A E.S. P y sus sedes.

7.5.2. Teletrabajo: Se debe disponer la implementación de política específica para la adopción del teletrabajo y el soporte de seguridad de la información a los activos que se tenga acceso.

7.6. Alcance de la política: La política será aplicable a todos los empleados de EPQ S.A. E.S.P y de acuerdo al nivel jerárquico se aplicarán las restricciones del caso.

7.7. Propiedad de la política: La política es propiedad de EPQ S.A. ESP y la oficina de gestión de sistemas de información es el encargado de implementar las medidas para su cumplimiento.

7.8. Sanciones: En caso de incumplimiento por parte de un funcionario o servidor público, se aplican las normas vigentes relacionadas con la ley 1952 de 2019 código único disciplinario, Ley estatutaria 1581 de 17 de octubre de 2012 respecto al manejo de los datos gestionados por la administración, y el decreto reglamentario 1377 de 2013 de esta ley. Ley de delitos informáticos 1273 de 2009.

8. POLÍTICA DE SEGURIDAD DE RECURSOS HUMANOS

8.1. Propósito: Proporcionar una serie de reglas, lineamientos y mecanismos para garantizar disponibilidad, confidencialidad e integridad en la gestión de la protección de los recursos humanos para reducir el riesgo de fraude, robo, y mal uso de los activos informáticos de EPQ S.A. ESP.

8.2. Descripción y Alcance de la política La política de seguridad para gestión de los recursos humanos es aplicable a todo el personal vinculado directa o indirectamente a la entidad. Es decir, se extiende a funcionarios, contratistas, procesos tercerizados, con los cuales Empresas Públicas del Quindío S.A. ESP, tiene o presenta interacción, uso o gestión de información

Esta política debe asegurar las siguientes situaciones:

- El conocimiento de los roles y responsabilidades por parte del personal de la entidad, coherentes con las especificaciones administrativas en la gestión de manuales de funciones de la división de personal de la alcaldía.
- La aplicación de actividades capacitación y entrenamiento para el fortalecimiento del sentido de conciencia de la seguridad de la información frente a la atención y mitigación de los riesgos y amenazas.

- Equipamiento de las mejores prácticas de los servidores públicos en la aplicación de las políticas de seguridad, privacidad y gestión de datos en el desarrollo de las funciones y actividades cotidianas.

- Brindar las prácticas y controles que permitan especificar las responsabilidades de las personas y organizaciones cuando dejan o terminan la vinculación con la entidad.

8.3. Responsabilidades

- La oficina de gestión sistemas de información está encargado de elaborar y actualizar la política y los procedimientos relativos a seguridad de la información.

- El Personal de EPQ SA ESP es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la institución, en relación con la gestión de los controles sobre la protección de los recursos humanos.

8.4. Lineamientos para Antes de Asumir el Empleo:

8.4.1. Se debe verificar los antecedentes y autenticidad de los soportes documentales entregados por los aspirantes al empleo.

8.4.2. Construir el esquema de clasificación de la información a la que se va a tener acceso por parte del empleado en el marco del perfil a suplir el cual es informado por la oficina responsable de su contrato o del supervisor del mismo.

8.4.3. Definir acuerdos de responsabilidad y compromisos de acuerdo a los requerimientos de seguridad de la información, objetivos y funciones del empleo.

8.5. Lineamientos Durante la Ejecución del Empleo:

8.5.1. Responsabilidad de la Alta Dirección: Exigir a los empleados, contratistas y terceros el cumplimiento de sus responsabilidades en la seguridad de la información.

8.5.2. Toma de Conciencia, educación, y formación en seguridad de la información: Todos los empleados, contratistas y donde sea pertinente debe desarrollarse procesos de educación, toma de conciencia y actualización de las políticas y procedimientos aplicables.

8.5.3. Proceso Disciplinario: Se debe contar con un proceso formal y comunicado para emprender acciones contra los funcionarios que hayan cometido una violación a la seguridad de la Información.

8.6. Lineamientos de Terminación o Cambio de Empleo:

8.6.1. Procedimiento de terminación o cambio de responsabilidades de empleo: Se debe contar con un proceso formal y comunicado para realizar la terminación o cambio de empleo de los funcionarios.

8.6.2. Terminación o cambio de responsabilidades de empleo: Se aplica la normatividad vigente para la terminación o cambio de empleo, en cuanto a la presentación de informes y procedimientos de empalme.

8.7. Alcance de la política: La política será aplicable a todos los funcionarios, contratistas y procesos tercerizados de Empresas Públicas del Quindío EPQ S.A. ESP

8.8. Propiedad de la política: La política es propiedad de Empresas Públicas del Quindío EPQ, S.A. ESP y la oficina de gestión sistemas de información es el encargado de implementar las medidas para su seguimiento e informes de cumplimiento.

8.9. Sanciones: En caso de incumplimiento por parte de un funcionario o servidor público, se aplican las normas vigentes relacionadas con la ley 1952 de 2019 código único disciplinario, Ley estatutaria 1581 de 17 de octubre de 2012 respecto al manejo de los datos gestionados por la administración, y el decreto reglamentario 1377 de 2013 de esta ley, y la Ley de delitos informáticos 1273 de 2009.

9. POLÍTICA DE SEGURIDAD DE ACTIVOS INFORMÁTICOS

9.1. Propósito: Proporcionar una serie de reglas, lineamientos y mecanismos para garantizar disponibilidad, confidencialidad e integridad los recursos informáticos (computadores, redes de datos, software, procesos y funcionarios) en particular la gestión de los activos por parte de los funcionarios de Empresas Públicas del Quindío EPQ S.A. ESP conectados o no a la red interna y a la información que ellos poseen y manipulan.

9.2. Descripción de la Política: Este documento de política atiende aspectos de la seguridad de la información como Responsabilidad sobre los activos, Clasificación de la información, Manejo de los soportes de almacenamiento. Estos lineamientos permiten implementar acciones de control sobre el manejo de información, manejo de activos físicos y responsabilidades en el uso y propiedad.

9.3. Responsabilidades La oficina de gestión de sistemas de información es el encargado de elaborar y actualizar la política y los procedimientos relativos a seguridad de la información.

El profesional universitario de gestión de sistemas de información es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la institución. Debe ocuparse también de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros incidentes de seguridad.

9.4. Lineamientos Responsabilidad sobre los activos:

- El funcionario que recibe formalmente el activo es responsable de operación, manejo y traslado.
- El funcionario es responsable de notificar o hacer que notifique oportunamente a las dependencias encargadas de atender los fallos o incidentes de seguridad sobre los activos a cargo.
- El funcionario es responsable de acuerdo a la normatividad vigente del inventario de activos e información que reposan en los activos o se deleguen en su uso y aprovechamiento.
- La propiedad del activo informático es del funcionario a quién mediante documento de entrega de Almacén se registre como usuario responsable.
- Se entiende como uso aceptable de los equipos, aquellas prácticas que no ocasionen daños o mal funcionamiento de los activos. Entre ellas se puede mencionar:
    - Desconectar los equipos cuando se vayan a usar.
    - No Ingerir alimentos cerca de los activos informáticos.
    - Proteger los activos informáticos de riesgos de lluvia, golpes o sustancias peligrosas.

- Evitar Exponer los activos a posibles hurtos. o Entregar, prestar o ceder los activos sin ningún registro o documento de autorización.
- Permitir a terceros la utilización de los equipos o activos informáticos sin la debida autorización.

- Utilizar los activos para actividades diferentes a las funciones o actividades contratadas.
- Solicitar los mantenimientos preventivos con oportunidad y periodicidad.
- Facilitar el acceso a activos de información sin la debida autorización.
- Los activos informáticos deben devolverse a almacén de manera formal y evitar reasignar de manera arbitraria y sin previa autorización del jefe inmediato, responsable del activo o directiva de almacén.

9.5. Lineamientos Clasificación de La información:

- El funcionario es responsable de administrar los datos e información del activo informático de acuerdo al soporte de la oficina de gestión sistemas de información, de manera, que se especifique expresamente los datos institucionales y los datos personales.

- Realizar copias de seguridad de los datos e información personales e institucionales periódicamente o adelantar estos con el personal autorizado de la oficina de gestión sistemas de información.

- Cuando se haya adelantado el proceso de inducción y entrenamiento a los funcionarios de Empresas Públicas del Quindío EPQ S.A. ESP en términos de las políticas de seguridad y gestión de tecnología por parte de la oficina de gestión de sistemas de información, cada funcionario debe firmar el acuerdo de confidencialidad y responsabilidad.

- Los activos informáticos físicos o documentos se deben seguir los lineamientos de etiquetado y manipulación de acuerdo a la normatividad local y nacional de archivo.

9.6. Lineamientos Manejo de los soportes de almacenamiento:

- El funcionario es responsable del manejo, protección de los soportes de información. Se entiende por soportes los medios físicos o electrónicos para el almacenamiento de datos e información que le hayan delegado o asignado.
- Evitar sacar de las instalaciones de la administración los medios o soportes de información sin previa autorización o registro en las bitácoras de vigilancia.
- La eliminación de soportes físicos o electrónicos debe realizarse en las siguientes etapas: Revisión y diagnóstico, devolución a almacén y disposición final.

10.7. Alcance de la política: La política será aplicable a todos los funcionarios de Empresas Públicas del Quindío S.A. ESP sin distinción de la forma de vinculación. Se entiende como funcionario a la persona vinculada a EPQ mediante cualquier tipo o forma, en este sentido, se aplica a funcionarios de carrera administrativa, libre nombramiento, contratistas, pasantes, practicantes entre otros.

10.8. Propiedad de la política: La política es propiedad de EPQ S.A. ESP y la oficina de gestión sistemas de información es la encargada de implementar las medidas para su cumplimiento.

10.9. Sanciones: En caso de incumplimiento por parte de un funcionario o servidor público, se aplican las normas vigentes relacionadas con la ley 1952 de 2019 código único disciplinario, Ley estatutaria 1581 de 17 de octubre de 2012 respecto al manejo de los datos gestionados por la administración, y el decreto reglamentario 1377 de 2013 de esta ley. Ley de delitos informáticos 1273 de 2009.

10.POLÍTICA DE SEGURIDAD DE CONTROL DE ACCESO

10.1. Propósito: Proporcionar una serie de reglas, lineamientos y mecanismos para garantizar disponibilidad, confidencialidad e integridad en relación con las directivas de control de acceso a los recursos informáticos (computadores, redes de datos, software, procesos y funcionarios) de EPQ S.A. ESP conectados o no a la red interna y a la información que ellos poseen y manipulan.

10.2. Descripción de la Política:

La información y los equipos de cómputo como recursos necesarios y fundamentales para el desarrollo normal de las actividades institucionales y misionales de EPQ S.A. ESP requieren un marco que permita preservar y restringir de acuerdo a su importancia, por ello, es necesario establecer un conjunto de acciones para proteger los sistemas informáticos muchas clases de amenazas y riesgos tales como fraude, sabotaje, espionaje industrial, extorsión, violación de la privacidad, intrusos, hackers, interrupción de servicio, accidentes y desastres naturales.

El presente documento emplea medidas para salvaguardar la información física y lógica, las reglas de uso de la red, uso de las estaciones de trabajo y restricciones de acceso.
Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos, dentro de las cuales podría incluirse un informe al Gerente de Empresas Públicas del Quindío S.A. ESP, que muestre el estado de la información sensible y calificada de acuerdo a su grado de importancia y un análisis de las mejoras obtenidas para preservarla.

Es importante proporcionar capacitaciones al personal tanto interno como externo para que se maneje apropiadamente los recursos informáticos de EPQ. La violación de dichas políticas puede acarrear medidas disciplinarias, legales e incluso el despido o terminación del contrato.

10.3. Responsabilidades

- La oficina de gestión de sistemas de información está encargada de elaborar y actualizar la política y los procedimientos relativos a seguridad en informática y telecomunicaciones.

- La oficina de gestión de sistemas de información, y oficina de talento humano, son responsables de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la institución.

- La oficina de gestión de sistemas de información debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros incidentes de seguridad.

10.4. Lineamientos de Control de Acceso.

10.4.1. **Política de Control de Acceso:** Se debe establecer, documentar y revisar una política de control de acceso con base en la normatividad vigente, aspectos administrativos y operacionales, y requerimientos de seguridad de la información.

10.4.2. **Acceso a redes y servicios de red**: Sólo está permitido el acceso a los

recursos de red a los usuarios que efectivamente se les haya autorizado.

10.5. Lineamientos de Gestión de Usuarios.

10.5.1. **Registro y Cancelación de Usuarios**: Debe existir un procedimiento formal de registro y cancelación de derechos de acceso a los usuarios.

10.5.2. **Suministro de acceso de usuarios**: Debe existir un procedimiento formal para el suministro de derechos de acceso a todos los sistemas y servicios a los usuarios.

10.5.3. **Gestión de Derechos de Acceso Privilegiado**: Debe existir controles para restringir, conceder y controlarla asignación y uso con acceso privilegiado.

10.5.4. **Revisión de los Derechos de Acceso de los usuarios**: Se delega a los propietarios de los activos la revisión de los derechos de acceso de los usuarios de manera periódica.

10.5.5. **Cancelación o Ajuste de los derechos de acceso**: Los derechos de acceso de empleados, contratistas, y terceros deben cancelarse a la información, instalaciones, y servicios al momento de terminar el empleo, finalización del contrato o acuerdo, y se deben ajustar los cambios.

10.6. Lineamientos de Responsabilidades de Usuarios.

10.6.1. **Uso de información secreta o sensible**: Se debe exigir a los usuarios que cumplan con las prácticas reglamentadas por la ley en el uso y gestión de información de autenticación secreta.

10.7. Lineamientos de Control de Acceso a Sistemas y aplicaciones.

10.7.1. **Restricción de Acceso a la Información**: Se debe aplicar la política de control de acceso a las funciones e información de los sistemas de aplicaciones.

10.7.2. **Procedimiento de Conexión Segura**: De acuerdo a la política de control de Acceso se requiere la aplicación de procesos de conexión segura.

10.7.3. Sistema de Gestión de Contraseñas: Los sistemas de Gestión de Contraseñas deben ser interactivos y asegurar contraseñas de calidad.

10.7.4. Uso de Programas utilitarios privilegiados: Se debe restringir y controlar el uso de programas utilitarios que puedan tener la capacidad de anular los controles de los sistemas y aplicaciones.

10.7.5. Control de Acceso a Códigos Fuente de Programas: Se debe restringir el acceso a códigos fuente de programas.

10.8. Alcance de la política: La política será aplicable a todos los empleados de EPQ S.A. ESP y de acuerdo al nivel jerárquico se aplicarán las restricciones del caso.

10.9. Propiedad de la política: La política es propiedad de Empresas Públicas del Quindío S.A. ESP

10.10. Sanciones: En caso de incumplimiento por parte de un funcionario o servidor público, se aplican las normas vigentes relacionadas con la ley 1952 de 2019 código único disciplinario, Ley estatutaria 1581 de 17 de octubre de 2012 respecto al manejo de los datos gestionados por la administración, y el decreto reglamentario 1377 de 2013 de esta ley. Ley de delitos informáticos 1273 de 2009.

11. POLÍTICA DE SEGURIDAD FISICA Y AMBIENTAL

11.1. Propósito: Proporcionar una serie de reglas, lineamientos y mecanismos para garantizar disponibilidad, confidencialidad e integridad los recursos informáticos relacionados con la seguridad física y ambiental de Empresas Públicas del Quindío EPQ S.A. ESP.

11.2. Descripción de la Política:

Esta política ofrece los aspectos para proteger los activos de las amenazas alrededor de los espacios físicos, condiciones de trabajo o actividad y la ejecución de las funciones de la

organización. Cubre temas como la gestión de áreas seguras, controles y seguridad física, gestión de equipos y maquinaria, y entorno de trabajo de los empleados, contratistas y terceros.

Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos, dentro de las cuales podría incluirse un informe al gerente que muestre el estado de la información sensible y calificada de acuerdo a su grado de importancia y un análisis de las mejoras obtenidas para preservarla.
Es importante proporcionar capacitaciones al personal tanto interno como externo para que se maneje apropiadamente los recursos informáticos de EPQ. La violación de dichas políticas puede acarrear medidas disciplinarias, legales e incluso el despido o terminación de contrato.

11.3. Responsabilidades

- La oficina de gestión sistemas de información es el encargado de elaborar y actualizar la política y los procedimientos relativos a seguridad de la información.
- La oficina de talento humano, la oficina de gestión sistemas de información y demás dependencias son los responsables de implementar y velar por el cumplimento de las políticas, normas, pautas y procedimientos de seguridad a lo largo de toda la institución, en relación con la gestión de los controles sobre la protección de los recursos y la gestión de la seguridad física.

11.4. Lineamientos sobre áreas seguras.

11.4.1. **Perímetro de Seguridad Física**: Se debe especificar formalmente el perímetro de áreas seguras o que contengan información confidencial, crítica, e instalaciones de manejo de información.

11.4.2. **Controles físicos de Entrada**: la administración debe especificar controles de acceso físico de acuerdo a las condiciones del entorno y clasificación de la información, y asegurar que solo se permita el acceso a personal autorizado.

11.4.3. **Seguridad en oficinas, salones e instalaciones**: Se debe especificar el diseño de controles en el acceso a oficinas, salones e instalaciones.

11.4.4. Protección contra amenazas externas y ambientales: Se debe especificar controles que permitan la protección contra desastres naturales, ataques maliciosos o accidentes de acuerdo al diseño de control de acceso físico.

11.4.5. Trabajo en áreas seguras: Se debe implementar las medidas que especifiquen los mecanismos de protección de las áreas y personas.

11.4.6. Áreas de despacho y carga: Especificar, señalizar y controlar el acceso a áreas de despacho y carga, áreas donde se pueda dar acceso no autorizado de personas. Estos lugares deben ser bien definidos y permitir el aislamiento de las zonas de protección de la información.

11.5. Lineamientos sobre equipos.

11.5.1. Ubicación y protección de los equipos: Los equipos o activos informáticos deben ubicarse y protegerse de riesgos de amenazas ambientales, y posibilidades de acceso no autorizado.

11.5.2. Servicios públicos de soporte: Los equipos deben disponer de mecanismos de protección de fallas de potencia u otros tipos de interrupciones.

11.5.3. Seguridad del cableado: Se debe implementar mecanismos de protección de las redes de cableado de energía y telecomunicaciones, que portan datos o brindan el servicio a sistemas y servicios de la entidad. Estos deben protegerse de interceptaciones, interferencias o daños.

11.5.4. Mantenimiento de Equipos: Deben existir programas de mantenimiento regular para asegurar su disponibilidad e integridad.

11.5.5. Retiro de Activos: Los equipos, información o software no deben retirar de su sitio sin autorización previa.

11.5.6. Seguridad de equipos y activos fuera del predio: Se debe especificar procedimientos y controles a los activos fuera de los predios de la entidad, teniendo en cuenta los posibles riesgos.

11.5.7. Disposición segura y reutilización: Durante la disposición final se deben revisar si estos conservan dispositivos de almacenamiento para asegurar que datos,

software o licencias sean retirados o sobre escritos de forma segura antes de su disposición o reusó.

11.5.8. Equipos sin supervisión de los usuarios: Los usuarios deben asegurarse que los equipos sin supervisión han sido asegurados de forma apropiada.

11.5.9. Política de escritorio limpio y pantalla limpia: Se debe adoptar una política de escritorio libre de papeles, dispositivos de almacenamiento removibles en los puestos de trabajo, y una política de pantalla limpia que no refleje información en las instalaciones de procesamiento de información.

11.6. Sanciones: En caso de incumplimiento por parte de un funcionario o servidor público, se aplican las normas vigentes relacionadas con la ley 1952 de 2019 código único disciplinario, Ley estatutaria 1581 de 17 de octubre de 2012 respecto al manejo de los datos gestionados por la administración, y el decreto reglamentario 1377 de 2013 de esta ley. Ley de delitos informáticos 1273 de 2009.

12. POLÍTICA DE SEGURIDAD OPERACIONAL

12.1. Propósito: Proporcionar una serie de reglas, lineamientos y mecanismos para garantizar disponibilidad, confidencialidad e integridad los recursos informáticos relacionados con la operación, documentación, copias de respaldo y registros de Empresas Públicas del Quindío E.P.Q. S.A. ESP.

12.2. Descripción de la Política:

La gestión de procedimientos, responsabilidades, copias de respaldo, control de cambios, registros y documentación son temas que permiten la protección y continuidad de los negocios. Mediante esta política se fundamenta las prácticas para asegurar la operación y procesos de Empresas Públicas del Quindío EPQ S.A ESP

Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos, dentro de las cuales podría incluirse un informe al gerente que muestre el estado de la información sensible y calificada de acuerdo a su grado de importancia y un análisis de las mejoras obtenidas para preservarla.

Es importante proporcionar capacitaciones al personal tanto interno como externo para que se maneje apropiadamente los recursos informáticos de EPQ. La violación de dichas políticas puede acarrear medidas disciplinarias e incluso el despido.

12.3. Responsabilidades

- La oficina de gestión de sistemas de información es la encargada de elaborar y actualizar la política y los procedimientos relativos a seguridad de la información.
- La oficina de gestión de sistemas de información, la oficina de talento humano y demás dependencias son los responsables de implantar y velar por el cumplimento de las políticas, normas, pautas y procedimientos de seguridad a lo largo de toda la institución, en relación con la gestión de los controles sobre la protección de los recursos y activos señalados en esta política.

12.4. Procedimientos Operacionales y Responsabilidades.

12.4.1. **Procedimientos de Operación Documentadas**: Los procedimientos deben estar documentados y publicados para todos los usuarios. En particular, para la entidad se deben documentar y disponer los procedimientos de acuerdo a los lineamientos del modelo integrado de planeación y gestión y el SUIT. De igual manera, los procedimientos operativos de áreas de planeación y sistemas deben estar documentados y publicados.

12.4.2. **Gestión de Cambios**: Se deben documentar y controlar los cambios en procesos y procedimientos, instalaciones, y sistemas de información.

12.4.3. **Gestión de Capacidad**: Se debe implementar mecanismos que permitan realizar seguimiento a los recursos, cambios y ajustes, proyección de capacidad futura, desempeño y aseguramiento.

12.4.4. **Separación de ambientes de desarrollo, ensayo y operación**: Se debe especificar y separar los entornos de desarrollo y ensayo, y operación. Se debe asegurar para evitar accesos no autorizados.

12.4.5. **Protección contra códigos maliciosos**: Se deben implementar controles de detección, prevención y recuperación. Se debe promover la conciencia apropiada entre los usuarios.

12.5. Copias de Respaldo.

12.5.1. Copias de Respaldo de La información: Se deben hacer copias de la información, software e imágenes de sistemas periódicamente y de acuerdo al procedimiento o política de copias de seguridad.

12.6. Registro y seguimiento.

12.6.1. Registros de Eventos: Se deben elaborar, conservar y revisar los registros de eventos acerca de actividades de usuarios, fallas del sistema, excepciones, y eventos de seguridad.

12.6.2. Protección de la Información de registro: Se deben incorporar mecanismos de protección de los registros de eventos.

12.6.3. Registros del administrador y operador: Se debe aplicar los procedimientos de registro, conservación y revisión en las bitácoras de roles administrador y operador.

12.6.4. Sincronización de relojes: Se deben implementar mecanismos de sincronización de reloj entre los diferentes activos que prestan servicios, con referencia a una fuente de tiempo.

12.7. Control de Software Operacional.

12.7.1. Instalación de software en sistemas operativos: Se debe disponer de procedimientos sobre la instalación de software en sistemas operativos.

12.8. Gestión de Vulnerabilidades técnicas

12.8.1. Gestión de vulnerabilidades: Se debe recolectar con oportunidad información sobre las vulnerabilidades de los sistemas en producción, evaluar el nivel de exposición y plantear acciones o medidas apropiadas.

12.8.2. Restricciones sobre la instalación de software: Se debe formalizar la instalación de software por parte de los usuarios mediante la documentación y registro de procedimientos.

12.9. Consideraciones sobre auditorías de sistemas de información:

12.9.1. Controles sobre auditorías de sistemas de información: Se debe plantear los requisitos y actividades a ejecutar en las auditorías a los sistemas en operación, de manera que armonicen con los procesos de negocio.

12.10. Alcance de la política: La política será aplicable a todos los empleados de Empresas Públicas del Quindío.E.P.Q. S.A ESP.

12.11. Propiedad de la política: La política es propiedad de Empresas Públicas del Quindío EPQ S.A. ESP y es la oficina gestión sistemas de información el encargado de implementar las medidas para su cumplimiento.

12.12. Sanciones: En caso de incumplimiento por parte de un funcionario o servidor público, se aplican las normas vigentes relacionadas con la ley 1952 de 2019 código único disciplinario, Ley estatutaria 1581 de 17 de octubre de 2012 respecto al manejo de los datos gestionados por la administración, y el decreto reglamentario 1377 de 2013 de esta ley. Ley de delitos informáticos 1273 de 2009.

13. POLÍTICA DE SEGURIDAD EN TELECOMUNICACIONES

13.1. Propósito: Proporcionar una serie de reglas, lineamientos y mecanismos para garantizar disponibilidad, confidencialidad e integridad los recursos informáticos basados en comunicaciones por redes de datos o telemáticas de Empresas Públicas del Quindío.

13.2. Descripción de la Política: En esta política se abordan las consideraciones sobre gestión de la seguridad en las redes y sistemas de telecomunicación, de igual manera, en los escenarios que permitan el intercambio o transferencia de datos con otras entidades.

Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos, dentro de las cuales podría incluirse un informe al gerente que muestre el estado de la información sensible y calificada de acuerdo a su grado de importancia y un análisis de las mejoras obtenidas para preservarla.

Es importante proporcionar capacitaciones al personal tanto interno como externo para que se maneje apropiadamente los recursos informáticos de Empresas Públicas del Quindío EPQ. La violación de dichas políticas puede acarrear medidas disciplinarias e incluso el despido.

13.3. Responsabilidades

- La oficina de gestión de sistemas de información es encargada de elaborar y actualizar la política y los procedimientos relativos a seguridad de la información.
- La oficina de gestión de sistemas de información es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la institución, en relación con la gestión de los controles sobre la protección de los recursos humanos.

13.4. Gestión de seguridad de redes.

13.4.1. **Controles de redes**: Se debe implementar mecanismos para gestionar y controlar las redes de datos para proteger los sistemas de información y aplicaciones.

13.4.2. **Seguridad de los servicios de red**: se deben identificar mecanismos de seguridad, niveles de servicio, y requisitos de los servicios de red. Incluir estas características en los acuerdos de nivel de servicio, ya sea que se provean internamente o por terceros.

13.4.3. **Separación de las Redes**: Se deben implementar mecanismos que permitan la separación en grupos de usuarios, servicios de información y sistemas de información.

13.5. Transferencia de información.

13.5.1. **Políticas y procedimientos de transferencia de información**: Se debe especificar políticas y/o procedimientos formales para el intercambio de información que protejan el uso de todo tipo de comunicaciones.

13.5.2. **Acuerdo sobre transferencia de información**: Los acuerdos para transferencia de información debe tratar sobre la transmisión segura de datos dentro de la organización y con otras entidades.

13.5.3. **Mensajes electrónicos**: Se deben especificar mecanismos para la protección de los servicios de mensajería.

13.5.4. Acuerdos de confidencialidad o no divulgación: Se deben especificar, documentar, revisar y actualizarlos acuerdos de confidencialidad que disponga la organización.

13.6. Alcance de la política: La política será aplicable a todos los empleados de Empresas Públicas del Quindío.

13.7. Propiedad de la política: La política es propiedad de EPQ y es oficina de gestión sistemas de información el encargado de implementar las medidas para su cumplimiento.

13.8. Sanciones: En caso de incumplimiento por parte de un funcionario o servidor público, se aplican las normas vigentes relacionadas con la ley 1952 de 2019 código único disciplinario, Ley estatutaria 1581 de 17 de octubre de 2012 respecto al manejo de los datos gestionados por la administración, y el decreto reglamentario 1377 de 2013 de esta ley. Ley de delitos informáticos 1273 de 2009.

14. POLÍTICA DE SEGURIDAD EN ADQUICISÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

14.1. Propósito: Proporcionar una serie de reglas, lineamientos y mecanismos para garantizar disponibilidad, confidencialidad e integridad los recursos informáticos relacionados con la adquisición y desarrollo de sistemas de información de Empresas Públicas del Quindío EPQ.

14.2. Descripción de la Política:

Para la protección de los sistemas de información se incorporan actividades en los escenarios de adquisición, desarrollo y mantenimiento de los sistemas de información.

Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos, dentro de las cuales podría incluirse un informe al gerente que muestre el estado de la información sensible y calificada de acuerdo a su grado de importancia y un análisis de las mejoras obtenidas para preservarla.

Es importante proporcionar capacitaciones al personal tanto interno como externo para que se maneje apropiadamente los recursos informáticos de Empresas Públicas del Quindío EPQ. La violación de dichas políticas puede acarrear medidas disciplinarias e incluso el despido.

14.3. Responsabilidades

- La oficina de gestión sistemas de información es el encargado de elaborar y actualizar la política y los procedimientos relativos a seguridad de la información.
- La oficina de gestión sistemas de información es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la institución, en relación con la gestión de los controles sobre la protección de los recursos humanos.

14.4. Adquisición, desarrollo y mantenimiento de sistemas de información.

14.4.1. **Análisis y especificación de Requisitos de seguridad de los sistemas de información**: en todos los proyectos de sistemas nuevos o mejoras se deben incluir requerimientos de seguridad de la información.

14.4.2. **Seguridad de servicios de las aplicaciones en redes públicas**: Se deben incluir requerimientos que cubran la atención a posibles fraudes, divulgación, modificación o disputas contractuales en aplicaciones sobre redes públicas.

14.4.3. **Protección de Transacciones de servicios de aplicaciones**: Se deben proteger los servicios transaccionales sobre situaciones de transmisión incompleta, enrutamiento errado, alteración no autorizada de mensajes, divulgación, duplicación o reproducción no autorizados.

14.5. Seguridad en los procesos de desarrollo.

14.5.1. **Política de Desarrollo Seguro**: Se debe especificar los aspectos, reglas y lineamientos en los proyectos de desarrollo de software dentro de la organización.

14.5.2. **Procedimiento de Control de Cambios**: Se debe formalizar, documentar y publicar el procedimiento de gestión de cambios de acuerdo al ciclo de vida de desarrollo de software.

14.5.3. **Revisión técnica de aplicaciones después de cambios en la plataforma de operación**: Cuando se debe cambios en la plataforma tecnológica

de operación se debe revisar la operación de las aplicaciones y servicios.

14.5.4. Principios de construcción de software seguro: Se deben especificar, documentar, mantener los requerimientos de software que hagan la producción de software seguro en la organización y se deben aplicar en todos los trabajos de implementación.

14.5.5. Ambiente de desarrollo seguro: Se debe implementar mecanismos de aseguramiento de los entornos de desarrollo en todo el ciclo de vida del software.

14.5.5.1. Desarrollos contratados externamente: Se debe supervisar y monitorizar los desarrollos contratados externamente.

Pruebas de seguridad de sistemas: Durante el desarrollo se deben ejecutar pruebas de la seguridad de los sistemas.

14.5.5.2. Pruebas de aceptación de los sistemas: para los sistemas nuevos, actualización o nuevas versiones se deben adelantar pruebas de aceptación en relación con el modelo de negocio y los criterios especificados.

15. POLÍTICA DE SEGURIDAD EN RELACIONES CON PROVEEDORES

15.1. Propósito: Proporcionar una serie de reglas, lineamientos y mecanismos para garantizar disponibilidad, confidencialidad e integridad los recursos informáticos en relación con los temas de relación con los proveedores de Empresas Públicas del Quindío EPQ

15.2. Descripción de la Política:

Esta política plantea aspectos a considerar frente a la protección de los activos de información que pueden ser accedidos por terceros o proveedores. Cubre temas como los acuerdos, composición y prestación de los servicios y gestión de las relaciones con proveedores.

Cuando ocurra un incidente grave que refleje alguna debilidad en los sistemas informáticos, se deberán tomar las acciones correctivas rápidamente para así reducir los riesgos, dentro de las cuales podría incluirse un informe al gerente que muestre el estado de la información sensible y calificada de acuerdo a su grado de importancia y un análisis de las mejoras obtenidas para preservarla.
Es importante proporcionar capacitaciones al personal tanto interno como externo para que se maneje apropiadamente los recursos informáticos de Empresas Públicas del Quindío

EPQ. La violación de dichas políticas puede acarrear medidas disciplinarias e incluso el despido.

15.3. Responsabilidades

- La oficina de gestión de sistemas de información es el encargado de elaborar y actualizar la política y los procedimientos relativos a seguridad de la información.
- La oficina de gestión de sistemas de información es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la institución, en relación con la gestión de los controles sobre la protección de los recursos.

15.4. Seguridad de la Información en las relaciones con los proveedores.

15.4.1. Política de seguridad de la información en relaciones con los proveedores: se debe especificar y documentar los lineamientos, riesgos y aspectos a definir en los acuerdos de acceso a la información con los proveedores.

15.4.2. Tratamiento de la seguridad de la información dentro de los acuerdos con proveedores: Dentro de los acuerdos se deben especificar los requisitos de seguridad de la información con el proveedor teniendo en cuenta elementos como el acceso, proceso, almacenar, comunicar o suministrar componentes de infraestructura de TI.

15.5. Gestión de la prestación de servicios de proveedores.

15.5.1. Seguimiento y revisión de los servicios de proveedores: Se deben programar con periodicidad el seguimiento, revisión y auditoría de los servicios prestados.

15.5.2. Gestión de Cambios a los servicios de los proveedores: Se deben establecer mecanismos que apoyen la gestión de cambios de los servicios, que incluyan aspectos como mantenimiento, mejora de políticas, procedimientos, y controles de seguridad. Teniendo en cuenta variables como los procesos de negocio, criticidad y reevaluación de riesgos.

15.6. Alcance de la política: La política será aplicable a todos los empleados de Empresas Públicas del Quindío EPQ y de acuerdo al nivel jerárquico se aplicarán las restricciones del caso.

15.7. Propiedad de la política: La política es propiedad de Empresas Públicas del Quindío y es la oficina de gestión de sistemas información la encargada de implementar las medidas para su cumplimiento.

15.8. Sanciones: En caso de incumplimiento por parte de un funcionario o servidor público, se aplican las normas vigentes relacionadas con la ley 1952 de 2019 código único disciplinario, Ley estatutaria 1581 de 17 de octubre de 2012 respecto al manejo de los datos gestionados por la administración, y el decreto reglamentario 1377 de 2013 de esta ley. Ley de delitos informáticos 1273 de 2009.

16. CRONOGRAMA DE ACTIVIDADES

Estrategia	Objetivo	Nombre del Indicador	Formula	Meta	Fecha de cumplimiento	Responsable
Política de seguridad y privacidad de la información	Establecer lineamiento para la implementación y verificación del cumplimiento de las Políticas de seguridad y privacidad de la información de la entidad.	Implementación de medidas de seguridad de la información en Empresas Públicas del Quindío S.A. ESP	Actividades realizadas	100%	31 de diciembre de 2023	Profesional Universitario en sistemas de información
		Adoptar el plan de activos de la información de Empresas Públicas del Quindío EPQ S.A. ESP	Adopción	1	31 de diciembre de 2023	Profesional Universitario en sistemas de información

		Implementación de la política de seguridad operacional	Actividades realizadas	100%	31 de diciembre de 2023	Profesional Universitario en sistemas de información
		Implementación de la política de seguridad y adquisición , desarrollo y mantenimiento de sistemas de información	Actividades realizadas	100%	31 de diciembre de 2023	Profesional Universitario en sistemas de información

JHON FABIO SUÁREZ VALERO
Gerente General
Empresas Públicas del Quindío

Proyectó y Revisó: Jhon Freddy Montoya Ovalle – P.u Subgerencia Administrativa y Financiera
Revisó: Martha Liliana Gómez Fajardo – P.U Subgerencia de Planeación Corporativa
Aprobó:
Maria del Socorro Mejia Z - Subgerente administrativa y Financiera
Darnelly Toro Jiménez - Subgerente de Planeación Y Mejoramiento Institucional

CONTROL DE CAMBIOS

Fecha	Versión	Descripción del cambio
31/01/2022	01	Se inicia Política De Seguridad Y Privacidad De La Información en normalización del Documento.
30/01/2023	02	Actualización de integrantes Comité Coorporativo y adjunto de Cronograma de Actividades punto 16.