

|                                                                                   |                                                                                                                                          |                                 |                   |                             |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|-------------------|-----------------------------|
|  | <b>EMPRESAS PÚBLICAS DEL QUINDÍO EPQ S.A E.S.P.</b><br><b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> |                                 |                   |                             |
| Código:<br>GAF-PL-02                                                              | Versión:<br>03                                                                                                                           | Fecha de emisión:<br>30/01/2024 | Página<br>1 de 23 | <b>DOCUMENTO CONTROLADO</b> |



**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

**Armenia, enero de 2024**





**EMPRESAS PÚBLICAS DEL QUINDÍO EPQ S.A E.S.P.**  
**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

Código:  
GAF-PL-02

Versión:  
03

Fecha de emisión:  
30/01/2024

Página  
2 de 23

**DOCUMENTO  
CONTROLADO**

**COMITÉ CORPORATIVO**

JHON FABIO SUAREZ VALERO

Gerente General.

JOHN ALEXANDER MORALES ARENAS

Secretario General.

ALBA LUCIA RODRÍGUEZ SIERRA

Jefe Oficina Asesora Control Interno.

DARNELLY TORO JIMENEZ

Subgerente de Planeación y  
Mejoramiento Institucional.

FERNANDO ANDRES SALAZAR GOMEZ

Subgerente Servicios Públicos  
Domiciliarios.

YURANI VILLEGAS

Subgerente de Comercialización de  
servicios y atención al cliente

MARIA DEL SOCORRO MEJIA ZULUAGA

Subgerente Administrativa y Financiera.

JHOANA CATALINA ACEVEDO

Jefe Oficina Control Interno  
Disciplinario.

ANDERSON VASQUEZ RAMIREZ

Jefe de Oficina Talento Humano



|                                                                                   |                                                                                                                                          |                                        |                          |                             |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|--------------------------|-----------------------------|
|  | <b>EMPRESAS PÚBLICAS DEL QUINDÍO EPQ S.A E.S.P.</b><br><b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> |                                        |                          |                             |
| <b>Código:</b><br>GAF-PL-02                                                       | <b>Versión:</b><br>03                                                                                                                    | <b>Fecha de emisión:</b><br>30/01/2024 | <b>Página</b><br>3 de 23 | <b>DOCUMENTO CONTROLADO</b> |

## CONTENIDO

|      |                                                  |           |
|------|--------------------------------------------------|-----------|
| 1.   | <b>PRESENTACIÓN.....</b>                         | <b>4</b>  |
| 2.   | <b>DEFINICIONES.....</b>                         | <b>4</b>  |
| 3.   | <b>MISIÓN .....</b>                              | <b>10</b> |
| 4.   | <b>VISIÓN .....</b>                              | <b>10</b> |
| 5.2. | <b>Objetivos Específicos .....</b>               | <b>11</b> |
| 6.   | <b>ALCANCE Y LIMITACIONES .....</b>              | <b>11</b> |
| 6.1. | <b>ALCANCE .....</b>                             | <b>11</b> |
| 6.2. | <b>LIMITACIONES.....</b>                         | <b>11</b> |
| 7.   | <b>RECURSOS.....</b>                             | <b>12</b> |
| 8.   | <b>RESPONSABLES.....</b>                         | <b>12</b> |
| 9.   | <b>METODOLOGÍA DE IMPLEMENTACIÓN.....</b>        | <b>13</b> |
| 10.  | <b>CRONOGRAMA DE ACTIVIDADES .....</b>           | <b>14</b> |
| 11.  | <b>MAPA DE RIESGOS DE SEGURIDAD DIGITAL.....</b> | <b>14</b> |





**EMPRESAS PÚBLICAS DEL QUINDÍO EPQ S.A E.S.P.**  
**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

Código:  
GAF-PL-02

Versión:  
03

Fecha de emisión:  
30/01/2024

Página  
4 de 23

**DOCUMENTO  
CONTROLADO**

## **1. PRESENTACIÓN**

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

El presente plan se elabora con el fin de dar a conocer cómo se realizará la implementación y socialización del componente de Gobierno Digital en el Eje Temática de la Estrategia en seguridad y privacidad de la información, el cual busca manejar de la mejor manera los datos de los usuarios de los servicios que ofrece Empresas Públicas del Quindío E.P.Q. S.A. ESP, garantizando la seguridad de la información.

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado debido a la característica propia de los sistemas digitales. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

La importancia de que las administraciones cuenten con un plan de tratamiento de riesgos de seguridad y privacidad de la información, está en aportar la evidencia necesaria de los niveles de riesgo en que se encuentran los activos mediante el nivel de madurez de la seguridad existente y sobre todo incentivar a los funcionarios a seguir las respectivas normas y procedimientos referentes a la seguridad de la información y recurso.

## **2. DEFINICIONES**

- ❖ **Acceso a la Información Pública.** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
- ❖ **Archivo.** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden



|                                                                                   |                                                                                                                                          |                                 |                   |                             |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|-------------------|-----------------------------|
|  | <b>EMPRESAS PÚBLICAS DEL QUINDÍO EPQ S.A E.S.P.</b><br><b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> |                                 |                   |                             |
| Código:<br>GAF-PL-02                                                              | Versión:<br>03                                                                                                                           | Fecha de emisión:<br>30/01/2024 | Página<br>5 de 23 | <b>DOCUMENTO CONTROLADO</b> |

para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

- ❖ **Riesgo.** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.
- ❖ **Riesgo de seguridad de la información.** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de la información.
- ❖ **Riesgo de corrupción.** Posibilidad de que por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- ❖ **Probabilidad.** Se entiende la posibilidad de ocurrencia de un riesgo. Estará asociada a la exposición del riesgo del proceso o actividad que se está analizando.
- ❖ **Causa.** Todos aquellos factores internos y externos que solos o en combinación con otros, puede producir la materialización de un riesgo.
- ❖ **Consecuencias.** Los efectos y situaciones resultantes de la materialización del riesgo que impactan en el proceso, en la entidad, sus grupos de valor y demás partes interesadas.
- ❖ **Impacto.** Las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- ❖ **Riesgo Inherente.** Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel de riesgo inherente, dentro de una escala de severidad.
- ❖ **Riesgo Residual.** El resultado de aplicar la efectividad de los controles al riesgo inherente.
- ❖ **Control.** Medida que permite reducir o mitigar un riesgo
- ❖ **Causa inmediata.** Circunstancias sobre las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.





**EMPRESAS PÚBLICAS DEL QUINDÍO EPQ S.A E.S.P.**  
**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

Código:  
GAF-PL-02

Versión:  
03

Fecha de emisión:  
30/01/2024

Página  
6 de 23

**DOCUMENTO  
CONTROLADO**

- ❖ **Causa raíz.** Causa principal o básica, corresponde a las razones por las cuales se puede presentar el riesgo.
- ❖ **Factores de Riesgo.** Son las fuentes generadoras de riesgos.
- ❖ **Confidencialidad.** Propiedad de la información que la hace no disponible ó sea divulgada a individuos, entidades o procesos no autorizados.
- ❖ **Integridad.** Propiedad de exactitud y complitud.
- ❖ **Disponibilidad.** Propiedad de ser accesible y utilizable a la demanda de una entidad.
- ❖ **Vulnerabilidad.** Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.
- ❖ **Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física y digital, recurso humano entre otros, que utiliza la organización para funcionar en el entorno digital.
- ❖ **Nivel de Riesgo:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.
- ❖ **Apetito del riesgo.** Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la alta dirección y del órgano de gobierno. El aptito del riesgo puede ser diferente para los diferentes tipos de riesgo que la entidad debe o desea gestionar.
- ❖ **Tolerancia del riesgo.** Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito del riesgo determinado por la entidad.
- ❖ **Capacidad de riesgo.** Es el máximo valor del nivel del riesgo que una entidad puede soportar y a partir del cual se considera por la alta dirección y el órgano de gobierno que no sería posible el logro de los objetivos de la entidad.
- ❖ **Auditoría.** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).



|                                                                                   |                                                                                                                                          |                                 |                   |                             |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|-------------------|-----------------------------|
|  | <b>EMPRESAS PÚBLICAS DEL QUINDÍO EPQ S.A E.S.P.</b><br><b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> |                                 |                   |                             |
| Código:<br>GAF-PL-02                                                              | Versión:<br>03                                                                                                                           | Fecha de emisión:<br>30/01/2024 | Página<br>7 de 23 | <b>DOCUMENTO CONTROLADO</b> |

- ❖ **Autorización.** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).
- ❖ **Bases de Datos Personales.** Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).
- ❖ **Ciberseguridad.** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
- ❖ **Ciberspacio.** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).
- ❖ **Datos Abiertos.** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).
- ❖ **Datos Personales.** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- ❖ **Datos Personales Públicos.** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).
- ❖ **Datos Personales Privados.** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).
- ❖ **Datos Personales Mixtos.** Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.



|                                                                                  |                                                                                                                                          |                                 |                   |                             |
|----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|-------------------|-----------------------------|
|  | <b>EMPRESAS PÚBLICAS DEL QUINDÍO EPQ S.A E.S.P.</b><br><b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> |                                 |                   |                             |
| Código:<br>GAF-PL-02                                                             | Versión:<br>03                                                                                                                           | Fecha de emisión:<br>30/01/2024 | Página<br>8 de 23 | <b>DOCUMENTO CONTROLADO</b> |

- ❖ **Datos Personales Sensibles.** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).
- ❖ **Declaración de aplicabilidad.** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).
- ❖ **Derecho a la Intimidad.** derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).
- ❖ **Encargado del Tratamiento de Datos.** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3).
- ❖ **Gestión de incidentes de seguridad de la información.** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- ❖ **Información Pública Clasificada.** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).
- ❖ **Información Pública Reservada.** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de



|                                                                                   |                                                                                                                                          |                                 |                   |                             |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|-------------------|-----------------------------|
|  | <b>EMPRESAS PÚBLICAS DEL QUINDÍO EPQ S.A E.S.P.</b><br><b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> |                                 |                   |                             |
| Código:<br>GAF-PL-02                                                              | Versión:<br>03                                                                                                                           | Fecha de emisión:<br>30/01/2024 | Página<br>9 de 23 | <b>DOCUMENTO CONTROLADO</b> |

acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

- ❖ **Plan de continuidad del negocio.** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
- ❖ **Plan de tratamiento de riesgos.** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).
- ❖ **Privacidad.** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.
- ❖ **Responsabilidad Demostrada.** Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.
- ❖ **Responsable del Tratamiento de Datos.** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).
- ❖ **Seguridad de la información** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- ❖ **Sistema de Gestión de Seguridad de la Información SGSI.** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
- ❖ **Titulares de la información.** Personas naturales cuyos datos personales sean



|                                                                                  |                                                                                                                                          |                                 |                    |                             |
|----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|--------------------|-----------------------------|
|  | <b>EMPRESAS PÚBLICAS DEL QUINDÍO EPQ S.A E.S.P.</b><br><b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> |                                 |                    |                             |
| Código:<br>GAF-PL-02                                                             | Versión:<br>03                                                                                                                           | Fecha de emisión:<br>30/01/2024 | Página<br>10 de 23 | <b>DOCUMENTO CONTROLADO</b> |

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

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

### 3. MISIÓN

Empresas Públicas del Quindío, E.P.Q S.A. E.S.P, es una empresa que existe para contribuir a la vida y al bienestar de la comunidad de la región donde ejerce su actividad, a través de la prestación de servicios públicos domiciliarios de Acueducto, Alcantarillado y Gas que cumplen altos estándares de calidad,

Continuidad, cantidad y cobertura, labores ejercidas con responsabilidad social y ambiental, dando aplicación a la normatividad vigente y a los principios de neutralidad, solidaridad, distribución, simplicidad y transparencia.

### 4. VISIÓN

En los próximos cuatro años, Empresas Públicas del Quindío, E.P.Q. S.A E.S.P, continuara siendo una empresa sostenible y sólida financieramente, que será reconocida en la región por el cumplimiento exitoso e innovador de su propuesta de valor relacionada con la prestación de servicios públicos domiciliarios de Acueducto, Alcantarillado y Gas que satisfacen plenamente a la comunidad beneficiaria, logrados a través de trabajadores competentes y de gran calidad humana que ven soportada su labor en procesos estandarizados y eficaces y en una infraestructura física y tecnológica que evoluciona continuamente ante los cambios del entorno y ante las necesidades y expectativas de sus clientes.

### 5. OBJETIVOS

#### 5.1. Objetivo General



|                                                                                   |                                                                                                                                          |                                 |                    |                             |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|--------------------|-----------------------------|
|  | <b>EMPRESAS PÚBLICAS DEL QUINDÍO EPQ S.A E.S.P.</b><br><b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> |                                 |                    |                             |
| Código:<br>GAF-PL-02                                                              | Versión:<br>03                                                                                                                           | Fecha de emisión:<br>30/01/2024 | Página<br>11 de 23 | <b>DOCUMENTO CONTROLADO</b> |

Controlar y minimizar los riesgos asociados a los procesos tecnológicos existentes, en Empresas Públicas del Quindío E.P.Q. S.A. E.S.P, con el fin de salvaguardar los activos de información, el manejo de medios, control de acceso, gestión de usuarios, confidencialidad y disponibilidad de la información.

## 5.2. Objetivos Específicos

- ❖ Realizar el mapa de riesgos de seguridad de la información de Empresas públicas del Quindío E.P.Q.S.A. E.S.P, con el fin de evitar la materialización de los riesgos de seguridad de la información.
- ❖ Aplicar las metodologías del DAPF e ISO respectivamente en seguridad y riesgo de la información, para Empresas Públicas del Quindío E.P.Q S.A E.S.P.

## 6. ALCANCE Y LIMITACIONES

### 6.1. ALCANCE

El alcance del presente plan, aplica para todos los funcionarios, contratistas, procesos tercerizados, población general de la oficina central y los municipios donde se presta el servicio de acueducto, alcantarillado y gas, por parte de Empresas Públicas del Quindío E.P.Q S.A. E.S.P.

### 6.2. LIMITACIONES



|                                                                                  |                                                                                                                                          |                                 |                    |                             |
|----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------|--------------------|-----------------------------|
|  | <b>EMPRESAS PÚBLICAS DEL QUINDÍO EPQ S.A E.S.P.</b><br><b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> |                                 |                    |                             |
| Código:<br>GAF-PL-02                                                             | Versión:<br>03                                                                                                                           | Fecha de emisión:<br>30/01/2024 | Página<br>12 de 23 | <b>DOCUMENTO CONTROLADO</b> |

Las soluciones de seguridad informáticas requieren el uso de equipos tecnológicos que presentan un elevado costo tanto es su hardware como en su software para su adecuado funcionamiento siendo el factor económico una de las principales limitaciones.

## 7. RECURSOS

Empresas Públicas del Quindío E.P.Q S.A E.S.P, en el marco de la gestión de riesgos de seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, dispone de los siguientes recursos que se listan a continuación.

| RECURSOS    | VARIABLE                                                                                                                                                                                                                                                                                                                                     |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Humanos     | La Oficina de Gestión y Servicios de la Información a través de seguridad de la información es responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Entidad en lo concerniente a la seguridad y privacidad de la información lo cual contribuye a la mejora continua. |
| Técnicos    | Guía de Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 5 - Diciembre de 2020 del DAFP.                                                                                                                                                 |
| Logísticos  | Gestión de recursos para realizar socializaciones transferencia de conocimientos y seguimiento a la gestión de riesgos.                                                                                                                                                                                                                      |
| Financieros | Recursos para la adquisición de conocimiento, recursos humanos, técnicos para los controles producto de la gestión de riesgos.                                                                                                                                                                                                               |

## 8. RESPONSABLES

- ❖ El Comité de gestión y desempeño institucional es el encargado de elaborar y actualizar la política y los procedimientos relativos a seguridad de la información.



|                                                                                   |                                                                                                                                          |                                        |                           |                             |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|---------------------------|-----------------------------|
|  | <b>EMPRESAS PÚBLICAS DEL QUINDÍO EPQ S.A E.S.P.</b><br><b>PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b> |                                        |                           |                             |
| <b>Código:</b><br>GAF-PL-02                                                       | <b>Versión:</b><br>03                                                                                                                    | <b>Fecha de emisión:</b><br>30/01/2024 | <b>Página</b><br>13 de 23 | <b>DOCUMENTO CONTROLADO</b> |

- ❖ Las demás dependencias de Empresas Públicas del Quindío E.P.Q S.A E.S.P, son los responsables de implementar y velar por el cumplimiento 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.

## 9. METODOLOGÍA DE IMPLEMENTACIÓN

Para llevar a cabo la implementación del Modelo de Seguridad y Privacidad de la Información Empresas Públicas del Quindío E.P.Q. S.A E.S.P, se toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar) y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, a través de los decretos emitidos.

De acuerdo con esto, se definen las siguientes fases de implementación del MSPI:

- Fase 1 – Planear: Consiste en definir el alcance del SGSI, sus objetivos permiten identificar los riesgos de la información.
- Fase 2 – Hacer: Se establecen planes de tratamiento de los riesgos identificados y se aplica controles de mitigación.
- Fase 3 – Verificar: Se evalúa la eficacia del sistema mediante el análisis de indicadores, realización de auditorías y revisión de la dirección.
- Fase 4 – Actuar: Se toman acciones tanto preventivas como correctivas y aplicación de las mejoras identificadas.

Fuente: Modelo de Seguridad y Privacidad de la Información emitida por MinTIC





**EMPRESAS PÚBLICAS DEL QUINDÍO EPQ S.A E.S.P.**  
**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

Código:  
GAF-PL-02

Versión:  
03

Fecha de emisión:  
30/01/2024

Página  
14 de 23

**DOCUMENTO  
CONTROLADO**

## 10. CRONOGRAMA DE ACTIVIDADES

Se describe el cronograma con sus respectivas actividades y tiempos.

| Actividad                                                                                  | Enero |   |   |   | Mayo |   |   |   | Junio |   |   |   | Septiembre |   |   |   | Diciembre |   |   |   |
|--------------------------------------------------------------------------------------------|-------|---|---|---|------|---|---|---|-------|---|---|---|------------|---|---|---|-----------|---|---|---|
|                                                                                            | 1     | 2 | 3 | 4 | 1    | 2 | 3 | 4 | 1     | 2 | 3 | 4 | 1          | 2 | 3 | 4 | 1         | 2 | 3 | 4 |
| Realizar diagnóstico de la entidad para actualizar los riesgos                             |       |   |   |   |      |   |   |   |       |   |   |   |            |   |   |   |           |   |   |   |
| Actualización de los riesgos de sistemas de información                                    |       |   |   |   |      |   |   |   |       |   |   |   |            |   |   |   |           |   |   |   |
| Aplicación y control de los riesgos de seguridad informática                               |       |   |   |   |      |   |   |   |       |   |   |   |            |   |   |   |           |   |   |   |
| Realizar procesos de capacitaciones en seguridad informática a funcionarios y contratistas |       |   |   |   |      |   |   |   |       |   |   |   |            |   |   |   |           |   |   |   |
| Realizar capacitación en la realización de Back ups tanto a funcionarios como contratistas |       |   |   |   |      |   |   |   |       |   |   |   |            |   |   |   |           |   |   |   |

## 11. MAPA DE RIESGOS DE SEGURIDAD DIGITAL.

| Nº | Nombre del Riesgo | Actividad | Tipo | Amenaza | Vulnerabilidad | Probabilidad | Impacto | Riesgo Residual | Opción de Manejo | Actividades de Control | Soporte | Responsable | Tiempo | Indicador |
|----|-------------------|-----------|------|---------|----------------|--------------|---------|-----------------|------------------|------------------------|---------|-------------|--------|-----------|
|----|-------------------|-----------|------|---------|----------------|--------------|---------|-----------------|------------------|------------------------|---------|-------------|--------|-----------|





**EMPRESAS PÚBLICAS DEL QUINDÍO EPQ S.A E.S.P.**  
**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

Código:  
GAF-PL-02

Versión:  
03

Fecha de emisión:  
30/01/2024

Página  
15 de 23

**DOCUMENTO  
CONTROLADO**

|   |                        |                         |                               |                                                                                                          |                                                                                                                                                                                                                        |         |       |         |                   |                                                                                             |                                                         |                                                                                                                             |                                    |                                                                                      |             |                    |
|---|------------------------|-------------------------|-------------------------------|----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|-------|---------|-------------------|---------------------------------------------------------------------------------------------|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------|--------------------------------------------------------------------------------------|-------------|--------------------|
| 1 | Perdida de información | Sistemas de información | Seguridad informática/digital | Borrado manual voluntario o involuntario, ataque de virus, daño electrónico en el sistema de información | Sistema de información sin contraseña, sin antivirus actualizado, desatención del funcionario, error al teclear un comando, mala instalación eléctrica, equipo desactualizado, equipo que supero los años de vida útil | Posible | Mayor | Extremo | Reducir el riesgo | Uso de contraseñas en los sistemas de información, cambio de las contraseñas periódicamente | Instalar antivirus corporativos y tenerlos actualizados | Revisar tiempo de vida del equipo y hacer cambios de estos, actualizar el sistema eléctrico y adecuar protecciones al mismo | Archivos digitales, archivo físico | Funcionario de cada sistema de información y Oficina Gestión Sistemas de Información | Todo el año | Numero de informes |
|---|------------------------|-------------------------|-------------------------------|----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|-------|---------|-------------------|---------------------------------------------------------------------------------------------|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------|--------------------------------------------------------------------------------------|-------------|--------------------|



**EMPRESAS PÚBLICAS DEL QUINDÍO EPQ S.A E.S.P.**  
**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

Código:  
GAF-PL-02

Versión:  
03

Fecha de emisión:  
30/01/2024

Página  
16 de 23

**DOCUMENTO  
CONTROLADO**

|   |                                                   |                                                                                   |                               |                                                                             |                                                                                                                                                                                                                                                                         |         |       |         |                   |                                                                                                                        |                                                          |                                                                                                          |                                                                           |                                                                                      |                                              |
|---|---------------------------------------------------|-----------------------------------------------------------------------------------|-------------------------------|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|-------|---------|-------------------|------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------------------------------------|
| 2 | Perdida de integridad en los documentos digitales | Sistemas de información, correos electrónicos, discos duros de backup, servidores | Seguridad informática/digital | Borrado manual voluntario o involuntario, ataque de virus, daño electrónico | Sistema de información con contraseña sin cambiar en periodos altos de tiempo, contraseñas de nivel bajo de seguridad, sin antivirus actualizado, desatención del funcionario, error al teclear un comando, bajo conocimiento del sistema informático, mala instalación | Posible | Mayor | Extremo | Reducir el riesgo | Cambio periódico de las contraseñas de los sistemas de información, generar contraseñas con niveles de seguridad alto, | Instalar antivirus corporativos y tenerlos actualizados, | Capacitar a los funcionarios en temas diversos sobre los sistemas de información y seguridad informática | Archivo digital, backup de bases de datos respaldada en diversos sistemas | Funcionario de cada sistema de información y Oficina Gestión Sistemas de Información | Numero de informes, capacitaciones recibidas |
|---|---------------------------------------------------|-----------------------------------------------------------------------------------|-------------------------------|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|-------|---------|-------------------|------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------|----------------------------------------------|





**EMPRESAS PÚBLICAS DEL QUINDÍO EPQ S.A E.S.P.**  
**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

Código:  
GAF-PL-02

Versión:  
03

Fecha de emisión:  
30/01/2024

Página  
17 de 23

**DOCUMENTO  
CONTROLADO**

|   |                                                         |                                                           |                               |                                            |                                                                                                                                                                      |         |       |         |                   |                                                                                                                        |                                                                 |                                                                                              |                                                                           |                                                                                      |              |                                              |
|---|---------------------------------------------------------|-----------------------------------------------------------|-------------------------------|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|-------|---------|-------------------|------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------|--------------|----------------------------------------------|
|   |                                                         |                                                           |                               |                                            | ón eléctrica , equipo desactualizado, equipo que supero los años de vida útil                                                                                        |         |       |         |                   |                                                                                                                        |                                                                 |                                                                                              |                                                                           |                                                                                      |              |                                              |
| 3 | Perdida de confidencialidad en los documentos digitales | Sistemas de información, sistema de backup de información | Seguridad informática/digital | Robo, alteración y difusión de información | Sistema de información con contraseña sin cambiar en periodos altos de tiempo, contraseñas de nivel bajo de seguridad, desatención o préstamo por parte del funciona | Posible | Mayor | Extremo | Reducir el riesgo | Cambio periódico de las contraseñas de los sistemas de información, generar contraseñas con niveles de seguridad alto, | Resguardar la información por parte del funcionario responsable | Capacitar a los funcionarios en temas diversos sobre los sistemas de información y seguridad | Archivo digital, backup de bases de datos respaldada en diversos sistemas | Funcionario de cada sistema de información y Oficina Gestión Sistemas de Información | To do el año | Numero de informes, capacitaciones recibidas |





**EMPRESAS PÚBLICAS DEL QUINDÍO EPQ S.A E.S.P.**  
**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

Código:  
GAF-PL-02

Versión:  
03

Fecha de emisión:  
30/01/2024

Página  
18 de 23

**DOCUMENTO  
CONTROLADO**

|   |                                                                                        |                                                                                             |                                                   |                                                                                                                                                                                                                   | rio del<br>sistema<br>de<br>informac<br>ión o del<br>backup                                                                                                                                                                                                                        |             |           |             |                                 |                                                                            | ad<br>info<br>rmá<br>tica                                                                                                                                                              |                                                                                                                                                                                                               |                                                                                               |                                                                                                                                      |                       |                                                       |
|---|----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|-----------|-------------|---------------------------------|----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|-----------------------|-------------------------------------------------------|
| 4 | Desco<br>nexió<br>n a<br>base<br>de<br>datos<br>de<br>plataf<br>ormas<br>digital<br>es | Siste<br>mas<br>de<br>infor<br>maci<br>ón,<br>swich<br>es,<br>route<br>rs<br>servi<br>dores | Segur<br>idad<br>infor<br>mática<br>a/digi<br>tal | Daño<br>extern<br>o del<br>ISP<br>(Intern<br>et<br>service<br>provid<br>er),<br>Ataque<br>DDoS<br>o DOS<br>(deneg<br>ación<br>de<br>servici<br>os<br>distrib<br>uidos o<br>Deneg<br>ación<br>de<br>servici<br>os) | Ausenci<br>a de<br>contrato<br>de<br>conectivi<br>dad<br>Fallas en<br>los<br>dispositi<br>vos,<br>Caída de<br>los<br>canales<br>de<br>datos,<br>ataque<br>hacker,<br>daño en<br>las<br>bases<br>de datos<br>de los<br>software<br>, virus o<br>mal<br>funciona<br>miento<br>de los | Posi<br>ble | May<br>or | Extre<br>mo | Red<br>ucir<br>el<br>ries<br>go | Revisar<br>conexi<br>ones y<br>equipo<br>s con<br>person<br>al del<br>ISP. | Instala<br>ción y<br>configu<br>ración<br>de<br>Firewal<br>l<br>electró<br>nico o<br>en softwa<br>re e<br>instala<br>ción de<br>antivir<br>us<br>corpor<br>ativo y<br>actuali<br>zado. | Hac<br>er<br>man<br>teni<br>mie<br>nto<br>prev<br>enti<br>vo y<br>corr<br>ecti<br>vo<br>con<br>el<br>pers<br>onal<br>técn<br>ico<br>de<br>los<br>servi<br>dor<br>es,<br>soft<br>war<br>e y<br>bas<br>es<br>de | Back<br>up de<br>bases<br>de<br>datos<br>respa<br>ldada<br>en<br>diver<br>sos<br>siste<br>mas | Funcio<br>nario<br>de<br>cada<br>sistem<br>a de<br>inform<br>ación y<br>Oficina<br>Gestió<br>n<br>Sistem<br>as de<br>Inform<br>ación | To<br>do<br>el<br>año | Nu<br>mer<br>o de<br>info<br>rme<br>s<br>técni<br>cos |





**EMPRESAS PÚBLICAS DEL QUINDÍO EPQ S.A E.S.P.**  
**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

Código:  
GAF-PL-02

Versión:  
03

Fecha de emisión:  
30/01/2024

Página  
19 de 23

**DOCUMENTO  
CONTROLADO**

|   |                                                                   |                                                                                                                                   |                                              |                                                                                         |                                                                                                                                                                                                                                                                     |             |           |                     |                                 |                                                                                                                                                                                       |                                                                                                                                                                    |                                                                                                                                                                       |                                                                                               |                                                                                                                                      |                       |                                                                                           |
|---|-------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|-----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|-----------|---------------------|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|-----------------------|-------------------------------------------------------------------------------------------|
|   |                                                                   |                                                                                                                                   |                                              |                                                                                         | servidor<br>es.                                                                                                                                                                                                                                                     |             |           |                     |                                 |                                                                                                                                                                                       |                                                                                                                                                                    | dat<br>os.                                                                                                                                                            |                                                                                               |                                                                                                                                      |                       |                                                                                           |
| 5 | Daño<br>parcial<br>o<br>total<br>de<br>plataf<br>ormas<br>físicas | Siste<br>mas<br>de<br>infor<br>maci<br>ón,<br>servi<br>dores<br>, siste<br>mas<br>de<br>respa<br>ldo<br>de<br>infor<br>maci<br>ón | Segur<br>idad<br>infor<br>mática/digi<br>tal | Hacker<br>, virus,<br>mal<br>manej<br>o de<br>los<br>sistem<br>as de<br>inform<br>ación | Abrir<br>archivos<br>adjuntos<br>enviado<br>s desde<br>direccio<br>nes de<br>correo<br>electróni<br>co<br>sospech<br>osas. Descarg<br>ar en los<br>equipos<br>software<br>descono<br>cidos, intentan<br>do el<br>robo de<br>informac<br>ión y<br>acceso<br>inapropi | Posi<br>ble | May<br>or | catas<br>breñe<br>o | Red<br>ucir<br>el<br>ries<br>go | Instala<br>ción<br>softwa<br>re anti-<br>Hackin<br>g, que<br>analiza<br>rá el<br>equipo<br>en<br>busca<br>de<br>cualqui<br>er<br>softwa<br>re<br>malicio<br>so y lo<br>elimina<br>rá. | Capacit<br>ar a<br>los<br>funcion<br>arios<br>en<br>temas<br>diverso<br>s sobre<br>los<br>sistem<br>as de<br>inform<br>ación y<br>segurid<br>ad<br>inform<br>ática | Revi<br>sar<br>peri<br>ódic<br>ame<br>nte<br>el<br>esta<br>do de<br>las<br>red<br>es<br>par<br>a<br>evit<br>ar<br>con<br>exio<br>nes<br>no<br>aut<br>oriz<br>ada<br>s | Back<br>up de<br>bases<br>de<br>datos<br>respa<br>ldada<br>en<br>diver<br>sos<br>siste<br>mas | Funcio<br>nario<br>de<br>cada<br>sistem<br>a de<br>inform<br>ación y<br>Oficina<br>Gestió<br>n<br>Sistem<br>as de<br>Inform<br>ación | To<br>do<br>el<br>año | Nu<br>mer<br>o de<br>info<br>rme<br>s,<br>cap<br>acit<br>acio<br>nes<br>reci<br>bida<br>s |





**EMPRESAS PÚBLICAS DEL QUINDÍO EPQ S.A E.S.P.**  
**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

Código:  
GAF-PL-02

Versión:  
03

Fecha de emisión:  
30/01/2024

Página  
20 de 23

**DOCUMENTO  
CONTROLADO**

|   |                         |                                                       |                               |                                                                   |                                                                                                                                                                                            |         |       |         |                   |                                                    |                                                                 |                                                                                                 |                                                           |                                         |              |                             |
|---|-------------------------|-------------------------------------------------------|-------------------------------|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|-------|---------|-------------------|----------------------------------------------------|-----------------------------------------------------------------|-------------------------------------------------------------------------------------------------|-----------------------------------------------------------|-----------------------------------------|--------------|-----------------------------|
|   |                         |                                                       |                               |                                                                   | ado al sistema.                                                                                                                                                                            |         |       |         |                   |                                                    |                                                                 |                                                                                                 |                                                           |                                         |              |                             |
| 6 | Perdida de conectividad | Sistemas de información, switches, routers servidores | Seguridad informática/digital | Posible caída de la red de transmisión de datos interna y externa | Ausencia de contrato de conectividad<br>Fallas en los dispositivos y redes internas, Caída de los canales de datos, daño en las bases de datos de los software, virus o mal funcionamiento | Posible | Mayor | Extremo | Reducir el riesgo | Revisar conexiones y equipos con personal del ISP. | Revisar periódicamente el cableado estructurado, puntos de red. | Hacer mantenimiento preventivo y correctivo por parte del proveedor a los servidores y bases de | Back up de bases de datos respaldada en diversos sistemas | Oficina Gestión Sistemas de Información | To do el año | Número de informes técnicos |





**EMPRESAS PÚBLICAS DEL QUINDÍO EPQ S.A E.S.P.**  
**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

Código:  
GAF-PL-02

Versión:  
03

Fecha de emisión:  
30/01/2024

Página  
21 de 23

**DOCUMENTO  
CONTROLADO**

|   |                                  |                         |                               |                                                                               | de los<br>servidor<br>es.                                                                                                                                                   |         |       |         |                   |                                                                                             | dat<br>os                                                |                                                                                               |                                     |                                            |             |                    |
|---|----------------------------------|-------------------------|-------------------------------|-------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|-------|---------|-------------------|---------------------------------------------------------------------------------------------|----------------------------------------------------------|-----------------------------------------------------------------------------------------------|-------------------------------------|--------------------------------------------|-------------|--------------------|
| 7 | pérdida o robo de la información | Sistemas de información | Seguridad informática/digital | Borrado manual o voluntario o involuntario, ataque de virus, daño electrónico | Sistema de información sin antivirus actualizado, desatención del funcionario, error al teclear un comando, equipo desactualizado, equipo que supero los años de vida útil, | Posible | Mayor | Extremo | Reducir el riesgo | Uso de contraseñas en los sistemas de información, cambio de las contraseñas periódicamente | Instalar antivirus corporativos y tenerlos actualizados, | Realizar periódicamente copias de seguridad de la información almacenada en los dispositivos. | Archivos digitales, archivo físico, | Funcionario de cada sistema de información | Todo el año | Numero de informes |





**EMPRESAS PÚBLICAS DEL QUINDÍO EPQ S.A E.S.P.**  
**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

Código:  
GAF-PL-02

Versión:  
03

Fecha de emisión:  
30/01/2024

Página  
22 de 23

**DOCUMENTO  
CONTROLADO**

|   |                                             |                                                                         |                               |                                                                                                                                                     |                                                                                                                                                                                                       |         |       |         |                   |                                                                                                          |                                                                                                                       |                                                                 |                                                                           |                                                                                      |             |                                              |
|---|---------------------------------------------|-------------------------------------------------------------------------|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|-------|---------|-------------------|----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------|-------------|----------------------------------------------|
| 8 | correos electrónicos de extraña procedencia | Sistemas de información, correos electrónicos, discos duros, servidores | Seguridad informática/digital | Las técnicas persuasivas de ingeniería social, que utilizan mucho los ciberatacantes para vencer a las personas de que abran los archivos adjuntos. | Recibir correos de un remitente desconocido genera desconfianza, muchos de los correos electrónicos peligrosos, contienen archivos ejecutables. Estos poseen extensiones del tipo .exe, .com, o .bat. | Posible | Mayor | Extremo | Reducir el riesgo | Capacitar a los funcionarios en temas diversos sobre los sistemas de información y seguridad informática | Instalación y configuración de Firewall electrónico en software e instalación de antivirus corporativo y actualizado. | Resguardar la información por parte del funcionario responsable | Archivo digital, backup de bases de datos respaldada en diversos sistemas | Funcionario de cada sistema de información y Oficina Gestión Sistemas de Información | Todo el año | Número de informes, capacitaciones recibidas |
|---|---------------------------------------------|-------------------------------------------------------------------------|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|-------|---------|-------------------|----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------|-------------|----------------------------------------------|





**EMPRESAS PÚBLICAS DEL QUINDÍO EPQ S.A E.S.P.**  
**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**

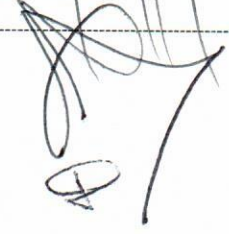
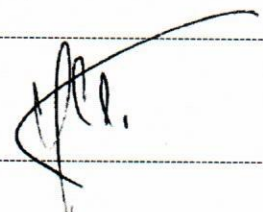
Código:  
GAF-PL-02

Versión:  
03

Fecha de emisión:  
30/01/2024

Página  
23 de 23

**DOCUMENTO  
CONTROLADO**

|                                                                                                                                                                             |                                                                                      |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Elaborado por: Jhon Freddy Montoya Ovalle<br>Profesional Universitaria Sistemas                                                                                             |   |
| Revisado por:<br>María del Socoro Mejía Zuluaga<br>Subgerente Administrativa y Financiera<br>Darnelly Toro Jiménez<br>Subgerente de Planeación y Mejoramiento Institucional |   |
| Aprobado por: Jhon Fabio Suarez Valero<br>Gerente General                                                                                                                   |  |

**CONTROL DE CAMBIOS**

| Fecha      | Versión | Descripción del cambio                                                                                                                                          |
|------------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 31/01/2022 | 01      | Se inicia el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.                                                                        |
| 30/01/2023 | 02      | Actualización del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.                                                                   |
| 30/01/2023 | 03      | Actualización vigencia 2024 Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.<br>Cambio de Código: GSI-P-01-PL-02 A Código: GAF-PL-02 |

