Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

2024 - 2026

Empresas Públicas de Armenia ESP.

ARMENIA QUINDÍO.

25 de enero de 2024

Tabla de contenido

Tabla de Ilustraciones

Listado de Tablas

1. Introducción

Como entidad pública, Empresas Públicas de Armenia ESP, está comprometida con la seguridad y privacidad de la información, entendiendo que este compromiso, depende en gran medida de una correcta gestión del riesgo. Esta gestión se basa, en un entendimiento del contexto, así como la identificación, análisis, evaluación, monitoreo y control de los riesgos, que se asocian a las actividades que se ejecutan en los diferentes procesos, de modo que se generen esquemas de protección que permitan proteger los activos de información que hacen parte de la empresa.

Este plan de tratamiento de riesgos de Seguridad y Privacidad de la Información busca brindar herramientas a todos los funcionarios de Empresas Públicas de Armenia ESP, que permitan realizar una gestión del riesgo, eficaz, efectiva y eficiente, permitiendo realizar una identificación temprana, y un monitoreo adecuado. Además, este documento se ajusta a los lineamientos sugeridos en lo que respecta al eje temático de la estrategia en seguridad y privacidad de la información, que hace parte integral de la Política Gobierno Digital y Seguridad Digital del Ministerio de las Tecnologías de las Información y las Comunicaciones.

2. Alcance del documento

Este plan se basa en las recomendaciones y definiciones que brinda la norma ISO 27005 y el Ministerio de Tecnologías de la Información y las Comunicaciones – Mintic; y establece la metodología que se debe aplicar en la gestión de los riesgos que afecten la seguridad de la información, desde todos los procesos de Empresas Públicas de Armenia ESP, orientando la ruta que se debe recorrer, desde el momento que se identifica un riesgo, hasta su monitoreo y control.

De este modo, se busca que la gestión del riesgo sea un proceso continuo, y permita analizar lo que puede suceder y cuáles serían las posibles consecuencias, antes de decidir lo que se debería hacer y cuando hacerlo, con el fin de reducir el riesgo hasta un nivel aceptable (Icontec, 2008).

Este plan cubre la gestión de riesgos clasificados en los niveles Bajo Moderado, Muy Alto según los lineamientos en Seguridad y Privacidad de la información definidos por Empresas Públicas de Armenia ESP.

3. Objetivos

Objetivo General

Establecer los conceptos, que deben ser considerados para realizar un correcto tratamiento de los riesgos, que eventualmente pueden comprometer la seguridad de la información en Empresas Públicas de Armenia ESP, de acuerdo a un plan de gestión de la seguridad de la información y el uso de las políticas de calidad existentes, las cuales se construyen a partir de los lineamientos propuestos por la familia de normas técnicas NTC-ISO/IEC 27000, incluyendo 27005 para la gestión del riesgo en la seguridad de la información.

Objetivos Específicos

1. Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información que permita garantizar la continuidad del negocio, garantizando oportunidad en la operación y disponibilidad de los servicios y trámites bajo la competencia de Empresas Públicas de Armenia ESP.
2. Educar a los funcionarios de Empresas Públicas de Armenia ESP, desde la Alta Dirección, hasta los funcionarios operativos, respecto a la importancia que tiene la gestión del riesgo en un Sistema de Gestión de la Seguridad de la Información, y la manera como estos se tratan una vez han sido identificados y evaluados.
3. Involucrar a todas las partes interesadas, en la gestión activa de los riesgos documentados, asociados a la seguridad de la información.
4. Divulgar y promover la aplicación consciente de las políticas de la seguridad de la información, generando una cultura organizacional, enfocada a fortalecer el entendimiento, que cada funcionario aporta a que el Sistema de Gestión de la Seguridad de la Información, fomentando la responsabilidad de hacerlo cumplir, en la ejecución de las actividades de su puesto de trabajo.
5. Gestionar los riesgos en Seguridad y Privacidad de la Información que se presenten en la entidad, según los contextos propios de Empresas Públicas de Armenia ESP.
6. Cumplir con los lineamientos y directrices dados por el Mintic en cuanto al tratamiento y gestión de los riesgos de seguridad y privacidad de la información; de acuerdo con el contexto de Empresas Públicas de Armenia ESP.

4. Impacto esperado del Plan de Seguridad y Privacidad de la Información

El desarrollo del presente plan genera los siguientes impactos a la entidad y grupos de interés.

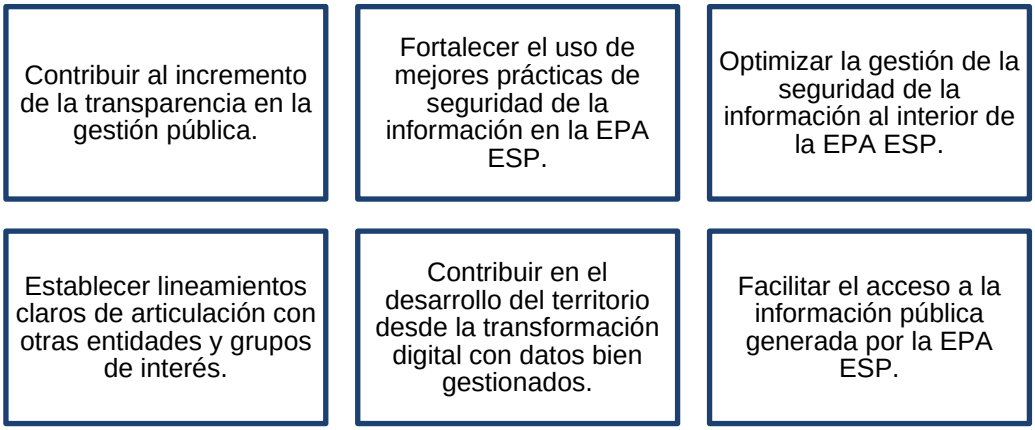

Ilustración 1. Impactos a la entidad y grupos de interés.

5. Marco Normativo y Documentación Técnica

Para consultar el Marco Normativo y Documentación Técnica aplicable a la presente política por favor remitirse al documento *Plan de Seguridad y Privacidad de la Información.*

6. Marco Referencial

A continuación, se describen los lineamientos de cumplimiento aplicables a esta gestión del riesgo para Empresas Públicas de Armenia ESP en la Política Interna Seguridad y Privacidad de la Información.

Enfoques Aplicables de la Política de Seguridad y Privacidad de la Información

Tabla 1. Enfoques Aplicables de la Política de Seguridad y Privacidad de la Información

Enfoque	Lineamientos	Referentes	Cantidad de Ítems	Procesos
Enfoque Gestión de Riesgos e Incidentes	Lineamientos sobre el mapeo y caracterización		11	Todos los procesos
	Lineamientos sobre la priorización y diagnóstico preliminar		5	
	Lineamientos sobre la resolución y recuperación		8	
	Lineamientos sobre el cierre y seguimiento de incidentes		4	

Para consultar el detalle de los lineamientos por favor dirigirse a la Política de Seguridad y Privacidad de la Información.

7. Esquemas de Gobernanza Seguridad y Privacidad de la Información

Para Empresas Públicas de Armenia ESP, es importante que la gestión del riesgo de haga de forma sistemática y comprometida por parte de la alta dirección, Sistema de Gestión Integrado, funcionarios públicos, oficiales y contratistas, los cuales, se describen a continuación de forma general:

- Alta Dirección. Por medio del Comité Institucional de Gestión y Desempeño, con funciones de comité de seguridad de la información, define el apetito del riesgo de seguridad de la información de Empresas Públicas de Armenia ESP, y responde por el fortalecimiento de las políticas *General* de seguridad *y Privacidad* de la información.

- Sistema de Gestión Integrado. Define los lineamientos de calidad, que se deben aplicar a las políticas de seguridad *y Privacidad de la información*, así como al plan de tratamiento de riesgos de seguridad *y Privacidad* de la información y *a*l plan de seguridad *y Privacidad* de la información.

- Líderes de proceso. Identifican, estiman, evalúan, valoran y monitorean los riesgos de seguridad de la información en su proceso, al menos una vez por año, y se responsabilizan de hacer cumplir la política de seguridad *y Privacidad* de la información, dentro del marco de su proceso, garantizando la interiorización del Sistema de Gestión de Seguridad de la Información, por

parte de cada uno de los funcionarios que hace parte de su proceso.

- Funcionarios públicos, oficiales y contratistas. Son responsables de ejecutar los controles sobre los riesgos establecidos en la política de seguridad *y Privacidad* de la información. Son responsables de garantizar, dentro del alcance de la ejecución de sus actividades, que se cumplan los lineamientos de seguridad.

- Gestión Control. Realiza seguimiento y control sobre la política de seguridad *y Privacidad* de la información, y sobre la idoneidad de los controles asociados a la gestión de los riesgos.

Este componente define los roles y responsabilidades para la gestión de riesgos e incidente de la Seguridad de la Información, específicamente con respecto a la protección de los activos de información.

La gobernanza en la gestión de riesgos para garantizar la continuidad estratégica, táctica y operativa de la entidad contempla la definición de una estructura y la asignación de responsabilidades la cual se describe en la siguiente tabla:

Tabla 2. Guía Roles y Responsabilidades del Modelo de Seguridad y Privacidad de la Información.

N°	Responsabilidad	Área/Procesos
1	Responsable de Gobierno y Gestión.	Comité MiPG
2	Responsable de Garantizar Cumplimiento.	Gerencia General
3	Gestión estratégica y técnica en Seguridad y Privacidad de la Información - Gestión de la Política. - Gestión de Procedimientos e Instrumentos. - Gestión del Plan de Seguridad y Privacidad de la Información. - Seguimiento y monitoreo a eventos e incidentes. - Formulación de iniciativas y planes de contingencia sobre niveles de riesgos identificados y reportados. - Establecer mecanismos que permitan la gestión de los incidentes reportados y la trazabilidad de los mismos. - Establecer canales de comunicación con proveedores de TI correspondientes para la gestión de incidentes. - Socialización a los respectivos involucrados de las situaciones presentadas en gestión de incidentes. - Identificar riesgos asociados a la gestión de incidentes de	Dirección de Tecnologías de la Información y las Comunicaciones.

N°	Responsabilidad	Área/Procesos
	seguridad - Contactar a las autoridades y/o grupos especializados en respuesta a incidentes para las labores de coordinación y apoyo.	
4	- Aplicar buenas prácticas en Seguridad de la Información. - Asistir a los espacios de formación y capacitaciones citados. - Apropiar y cumplir con lo establecido en los espacios de capacitación. - Cumplir con los lineamientos de gestión de incidentes presentados en su área. - Dar el adecuado uso y cumplimiento a los activos de información mapeados en la entidad.	Todos los procesos.
5	- Asegurar que los incidentes que involucren la fuga de información sensible sean manejados con base en las regulaciones aplicables. - Determinar las consecuencias jurídicas que se podrán presentar sobre incumplimiento o desacato de las responsabilidades en la gestión de eventos e incidentes de TI. - Orientar y asistir en acciones de adquisición de evidencia forense requerida	Dirección Jurídica y Secretaria General
	- Incluir en el plan de capacitación anual temáticas asociadas a la gestión de incidentes. - Fomentar la participación de los colaboradores (funcionarios y contratistas) y proveedores en las acciones de Educación, Información y Comunicación que definan. - Apoyar en la resolución de conflictos interno-asociados con violaciones u omisiones de la presente política.	Gestión del Talento Humano
6	Difusión de información de carácter público a grupos de interés referente a la gestión de incidentes. - Diseño de estrategias de EIC para capacitar a los colaboradores y proveedores. - Difusión de material publicitario e informativo sobre las responsabilidades y gestión efectiva de incidentes que se presenten.	Dirección de Comunicaciones
7	Acompañar en la formulación y articulación de los planes de gestión de incidentes con la ruta estratégica del negocio.	Dirección de Planeación Corporativa
8	Seguimiento al desempeño en la gestión de incidentes de TI.	Dirección Control de Gestión

Fuente: Construido con base en Guía Roles y Responsabilidades del Modelo de Seguridad y Privacidad de la Información. Elaborado por el MinTIC.

8. Componentes de Gestión del Riesgo en Seguridad de la Información

Los siguientes, son los componentes del proceso gestión del riesgo en Seguridad de la Información, los cuales hacen parte del Sistema de Gestión de la Seguridad de la Información (Icontec, 2008), y se desarrollan más adelante en el presente documento:

Planificar	Hacer	Verificar	Actuar
Establecer contexto. Valorar el riesgo. Planificar el tratamiento del riesgo. Aceptación del riesgo.	Implementar el plan de tratamiento del riesgo.	Monitorear y revisar continuamente los riesgos	Mantener y mejorar el proceso de gestión del riesgo en la seguridad de la información

Ilustración 2. Componentes del proceso gestión del riesgo en Seguridad de la Información

9. Esquema metodológico

Para la gestión de los riesgos mapeados en Empresas Públicas de Armenia ESP se diseñó el siguiente esquema.

Ilustración 3. Riesgos mapeados en Empresas Públicas de Armenia ESP

Establecer Contexto

Como parte fundamental del Sistema de Gestión Integrado, el Sistema de Gestión de la Seguridad de la Información, requiere un reconocimiento del contexto estratégico, asociado a lo que podría eventualmente comprometer la seguridad de la información.

Para esto, es importante que cada proceso considere los siguientes elementos:

- Identificar los funcionarios, que, por sus responsabilidades, pueden tener mayor responsabilidad en el aseguramiento de la información, garantizando, dentro de su alcance, la confidencialidad, disponibilidad e integridad de la misma.
- Establecer los factores tanto internos como externos, que afectan la seguridad de la información en el proceso, y plasmarlo en la matriz Identificación de Amenazas y Vulnerabilidades de Seguridad de la Información por proceso.

Identificación de los Riesgos

Es la etapa que permite conocer los eventos potenciales, estén o no bajo el control de Empresas públicas de Armenia ESP, que pueden llegar a generar una pérdida de información. Para esto, es importante que cada proceso considere los siguientes elementos:

- Identificar los activos de acuerdo con el alcance establecido (Icontec, 2008), y realizar el respectivo registro en el documento Inventario de Activos de Información - Etapa de Planificación - Buenas Prácticas SGSI DTIC-D-003.
- Identificar las amenazas asociadas y sus orígenes según el activo de información identificado y registrarlas en documento Inventario de Activos de Información - Etapa de Planificación - Buenas Prácticas SGSI DTIC-D-003
- Identificar los controles existentes, de modo que no exista una duplicidad, realizando una validación de suficiencia de cobertura de los mismos, en los riesgos en los cuales se están aplicando.
- Realizar un análisis de vulnerabilidades para cada uno de los procesos y registrarlo en el formato DTIC-R-008
- Identificar las consecuencias de la materialización de cada riesgo, y registrarla en el formato DTIC-R-008

Análisis del Riesgo

El análisis del riesgo se puede realizar con diferentes grados de detalle dependiendo de la criticidad de los activos, la amplitud de las vulnerabilidades conocidas y los

incidentes anteriores que implicaron a la organización (Icontec, 2008).

Para el caso de Empresas Públicas de Armenia ESP, el análisis de riesgo asociado a la Seguridad de la Información se plantea en las siguientes etapas:

Calificación del Riesgo

La calificación del riesgo se basa en el resultado del producto entre la probabilidad y el impacto. Para obtener estos valores, se deben tener en cuenta las siguientes escalas:

Tabla 3. Calificación de probabilidad

Calificación de Probabilidad		
Probabilidad	**Valor**	**Descripción**
Casi cierto	5	Se espera que el evento se presente la mayoría de las veces
Probable	4	El evento probablemente se presenta la mayoría de las veces
Moderado	3	El evento podría ocurrir en algún momento
Improbable	2	El evento difícilmente podría ocurrir en algún momento
Raro	1	El evento podría ocurrir en un momento de forma excepcional

Tabla 4. Escala para calificar el impacto del riesgo

Escala para calificar el impacto del riesgo								
Tipos de efecto o impacto		**Valor**	**Estratégico**	**Operativo**	**Financieros**	**Cumplimiento**	**Tecnología**	**Imagen**
BAJO	El evento, de presentarse genera un impacto menor.	5	Afecta las metas del proceso	Genera correcciones a procedimientos del SGI	Genera pérdida financiera que afecta la operación	Genera investigaciones	Afecta la operación del proceso.	Compromete la imagen de Empresas Públicas de Armenia ESP.
MODERADO	El evento, de presentarse genera un impacto moderado.	10	Afecta las metas de varios procesos	Genera cambios en los procesos.	Genera pérdida financiera que afecta la operación del servicio	Genera interrupciones en la prestación de servicios.	Afecta las operaciones	Compromete la Imagen de Empresas públicas de Armenia ESP.
MUY ALTO	El evento, de presentarse genera un impacto alto y consecuencias desastrosas para Empresas Públicas de Armenia ESP	25	Afecta las metas de toda la Empresa y de la Administración Municipal.	Empresas Públicas de Armenia ESP se paraliza completamente.	Genera pérdida financiera en la administración municipal.	Implica cierre de Empresas Públicas de Armenia ESP.	Afecta a la Ciudad de Armenia	Compromete la imagen de la ciudad de Armenia ESP.

Evaluación del Riesgo

Tabla 5. Evaluación del Riesgo

Prioridad	Valor	Zona de Riesgo		
Alta	**3**	15 Zona de Riesgo Moderada Evitar el Riesgo	30 Zona de Riesgo Importante Evitar el riesgo Reducir el Riesgo Compartir o Transferir	60 Zona de Riesgo Inaceptable Evitar el riesgo Reducir el Riesgo Compartir o Transferir
Media	**2**	10 Zona de Riesgo Tolerable. Reducir el riesgo. Asumir el riesgo.	20 Zona de Riesgo Moderado Reducir el riesgo Compartir o Transferir	40 Zona de Riesgo Importante Evitar el riesgo Reducir el Riesgo Compartir o Transferir
Baja	**1**	5 Zona de Riesgo Aceptable Asumir el riesgo.	10 Zona de Riesgo Tolerable Reducir el riesgo Compartir o Transferir	20 Zona de Riesgo Moderado Reducir el riesgo Compartir o Transferir
	Impacto	**Leve**	**Moderado**	**Catastrófico**
	Valor	**5**	**10**	**20**

Valoración del Riesgo

Identificación de Controles

Los controles, son aquellas acciones que se ejecutan con el objetivo de prevenir la materialización de un riesgo, o en su defecto para minimizar el impacto de un riesgo que se ha materializado. Basado en esto, se debe considerar, que un control de cumplir con ciertas características, más aún cuando estamos tratando riesgos de seguridad de la información.

A continuación, se detallan las características principales que deben considerarse, para la identificación de los controles, que se deben ajustar a las posibles causas y

consecuencias de la materialización de un riesgo.

Tabla 6. características principales para la identificación de los controles

Característica	Descripción
Objetivos	No dependen del criterio de quien lo define y/o ejecute, sino de los resultados que se esperan obtener
Pertinentes	Están directamente orientados a atacar las causas o consecuencias del riesgo
Realizables	Se deben definir controles que la entidad o el proceso esté en capacidad de llevar a cabo
Medibles	Permiten el establecimiento de indicadores para verificar el cumplimiento de su aplicación y/o efectividad
Periódicos	Tienen frecuencia de aplicación en el tiempo
Efectivos	Eliminan o mitigan las causas o consecuencias y eviten la materialización del riesgo
Asignables	Tienen responsables definidos para su ejecución

Evaluación de los Controles

Permite determinar, si los controles realmente permiten disminuir el riesgo o sus impactos, y debe aplicarse a cada uno de los controles identificados.

Ejecución de la Valoración del Riesgo

Tabla 7. Ejecución de la Valoración de Riesgo

Criterios	Valoración del riesgo
No existen controles.	Se mantiene el resultado de la evaluación antes de los controles.
Existen, pero no son efectivos.	Se mantiene el resultado de la evaluación antes de los controles.
Los controles existen son efectivos, pero no están documentados	Cambia el resultado inferior de la evaluación antes de controles (El desplazamiento queda a criterio de los responsables)
Los controles son efecto y son documentados.	Pasa a escala inferior, según criterio de los responsables.

Formulación de documentos de gestión de riesgos

Esta etapa se enfoca en la formulación y aprobación de los documentos primarios para la gestión de riesgos los cuales son:

- **Mapa de Riesgos:** Herramienta de análisis esencial que permite identificar zonas de mayor o menor riesgo frente a diferentes peligros, como factor clave a la hora de determinar las áreas a intervenir con determinada inversión en infraestructura.
- **Plan de Acción de Riesgos Vigencia Anual:** Describe las acciones de intervención necesarias para gestionar los riesgos mapeados.
- **Matriz de Contexto:** Documento que describe de forma amplia los riesgos y oportunidades de mapeados por el proceso TICs.

La aprobación de estos documentos se va por medio de valoración de los profesionales técnicos y el Director de TICs, para posteriormente socializar con el Director de Planeación Corporativa, con la aprobación de las partes se procede a publicarse en el Sistema de Gestión Integrado con el versionamiento pertinente.

10. Acciones Clave para la Gestión de Riesgos

Las acciones clave para la Gestión de Riesgos establecidas para la vigencia *2024-2026* están definidas de manera integral en el componente Gestión de Riesgos e Incidentes del Plan de Seguridad y Privacidad de la Información. A continuación, se describen las acciones establecidas.

Tópico	Seguridad y Privacidad de la Información
Componente de TI	Gestión de Riesgos e Incidentes
Proyectos/Iniciativas	Continuidad Operativa del Negocio desde la gestión de los riesgos y la recuperación eficiente ante desastres e incidentes de seguridad.

Tabla 8. Acciones Clave para la Gestión de Riesgos

Tópico	Componente de TI	Sub-Componentes	Actividades Clave	Evidencia	Periodicidad de seguimiento
Seguridad y Privacidad de la Información	Gestión de Riesgos e Incidentes	Gestión del Riesgo	Actualización de lineamientos de riesgos	Reporte de actualización	Anual
			Socialización de lineamientos de Gestión de Riesgos de Seguridad y privacidad de la Información.	Registro de asistencia.	A necesidad
			Identificación de Riesgos de Seguridad y Privacidad de la Información	Mapa de Riesgos EPA actualizado.	Anual
			Aprobación de Riesgos Identificados	Memorando de aprobación.	Anual
			Publicación mapas de riesgos de los procesos.	Mapa de Riesgos EPA publicado en SGI.	Anual
			Seguimiento a los riesgos en Seguridad y Privacidad de la Información	Seguimiento al mapa de riesgo.	Anual
			Acciones de mejoramiento a riesgos residuales.		Anual
			Realizar medición, presentación y reporte de indicadores	Reporte de indicadores.	Anual
		Vulnerabilidades	Establecer lineamientos para la ejecución de pruebas de vulnerabilidades.	Lineamientos de Ejecución de Pruebas de Vulnerabilidad.	Anual
			Vincular y seleccionar proveedores en la ejecución de pruebas de vulnerabilidades.	Banco de Proveedores seleccionados y vinculados con contratación.	A necesidad
			Realizar pruebas de vulnerabilidades según parámetros establecidos.	Reporte de Pruebas de Vulnerabilidades.	A necesidad
			Ejecutar plan de contingencia sobre vulnerabilidades encontradas.	Seguimiento al Plan de Contingencia sobre vulnerabilidades.	A necesidad
		Gestión de Incidentes	Formular procedimiento de gestión de incidentes de seguridad de la información.	Procedimiento actualizado.	Anual
			Realizar revisiones de seguridad de la información.	Bitácora de revisiones de incidentes.	Trimestral
			Realizar reporte de eventos en seguridad en la información	Reporte de eventos de seguridad.	Trimestral
			Realizar reporte de incidentes de seguridad en la información mitigados.	Reporte de incidentes de seguridad.	Trimestral

11. Oportunidad de Mejora

Empresas Públicas de Armenia ESP deberá de manera transversal a todas las etapas de gestión identificar oportunidades de mejora para fortalecer las dinámicas de gestión de riesgos. Por lo anterior la oportunidad deberá entenderse como la consecuencia positiva frente al resultado del tratamiento del Riesgo.

12. Recursos Clave

Empresas Públicas de Armenia ESP, contempla los siguientes recursos para garantizar operatividad en la gestión de los riesgos identificados.

Tabla 9. Recursos para garantizar operatividad en la gestión de los riesgos identificados.

Recursos	Variable
Físicos:	● Equipos de cómputo. ● Espacio de cómputo.
Humanos	● Personal vinculado de la Dirección TICs. ● Proveedores de TI con las competencias suficientes y certificadas para acompañar el proceso.
Intelectuales:	● Política de Seguridad y Privacidad de la Información. ● Plan de Seguridad y Privacidad de la Información. ● Procedimiento de Seguridad y Privacidad de Información. ● Matriz de Riesgos de Empresa Publicas de Armenia ESP. ● Mapa de Contexto.
Financieros	● Recursos para la adquisición de conocimiento, recursos humanos, técnicos, y desarrollo de auditorías externas.

13. Presupuesto

La estimación y asignación del presupuesto para el plan de tratamiento de riesgos de Seguridad y Privacidad de la Información en Empresas Públicas de Armenia EPS, corresponderá al responsable de gestión del riesgo, quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos y del plan de tratamiento.

14. Glosario

- **Acceso:** Es la capacidad de disponer de una información que ya existe dentro de un sistema informático (fichero, memoria, etc.) y que es posible acceder a ésta, continuando una secuencia fija y predeterminada de operaciones como también a partir de una clave, independientemente de las anteriores operaciones.
- **Acción correctiva:** Remediación de los requisitos o acciones que dieron origen al establecimiento de no una conformidad, de tal forma que no se vuelva a presentar.
- **Acción preventiva:** Disposición de operaciones que buscan de forma preliminar, que no se presente en su ejecución, desarrollo e implementación una no conformidad.
- **Activo de Información:** recurso o elemento que contiene información con valor para la organización debido a su utilización en algún proceso o que tiene relación directa o indirecta con las funciones de la entidad: software, hardware, personas (roles), físicos (instalaciones, áreas de almacenamiento de expedientes, centros de procesamiento de datos), intangibles (imagen y reputación).
- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- **Activos Tecnológicos:** Recursos del sistema de información o relacionados con éste, necesarios para que la entidad funcione correctamente y alcance los objetivos propuestos por su Dirección. Se pueden estructurar en las siguientes categorías: Software, Hardware, Servicios, Datos, Personal, Proveedores, instalaciones físicas, Comunicaciones, Equipamiento auxiliar.
- **Alteración:** Es un tipo de delito informático mediante el cual se puede realizar fraude introduciendo, cambiando o borrando datos informáticos o la interferencia de sistemas informáticos.
- **Amenaza:** Según [ISO IEC 13335-1:2004): causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.
- **Análisis De Brecha (Gap):** El GAP Análisis es un estudio preliminar que permite conocer la manera en la que se desempeña una empresa en materia de seguridad de la información, con relación a las mejores prácticas reconocidas en la industria, para esto se utilizan criterios establecidos en normas o estándares. El análisis establece las diferencias entre el desempeño actual y el deseado. Este análisis se puede aplicar a cualquier estándar certificable, lo normal es que se lleve a cabo para nuevos esquemas de certificación.

- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- **Árbol De Incidentes:** Es un listado de la estructura jerárquica de los tipos de incidentes, los cuales podrán ser seleccionados para categorizar la problemática reportada por el usuario.
- **Auditor:** Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.
- **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).
- **Ciberespacio:** Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701, Tomado de la Academia de la lengua española).
- **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).
- **Claves, contraseña o password:** forma de autentificación que utiliza información secreta o confidencial para controlar el acceso hacia algún recurso.
- **Código malicioso:** Programas potencialmente peligrosos diseñados para dañar los sistemas y los datos, o modificarlos para que funcionen de manera incorrecta.
- **Computación en la nube (Cloud Computing):** Es un término utilizado para describir servicios proporcionados a través de una red por una colección de servidores remotos. Esta "nube" abstracta de computadoras proporciona una gran capacidad de almacenamiento distribuido y de procesamiento a la que se puede acceder desde cualquier dispositivo conectado a Internet que ejecute un navegador web.
- **Confiabilidad:** Se puede definir como la capacidad de un producto de realizar su función de la manera prevista, De otra forma, la confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.
- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. [NTC 5411-1:2006].
- **Conformidad:** Cumplimiento de lineamientos y estándares vigentes
- **Continuidad de negocio:** (inglés: Business Continuity). Incluye la planificación para asegurar la continuidad de las funciones críticas de un negocio en la eventualidad de una falla o desastre. Este tipo de planificación

abarca aspectos claves de la operación tales como personal, facilidades, comunicaciones, y cambio de controles. Un plan de continuidad de negocio es inclusive de un Plan de Recuperación de Desastre para la recuperación de infraestructura tecnológica.

- **Continuidad del servicio TI:** Procedimientos de continuidad adecuados y justificables en términos de costos para cumplir con los objetivos propuestos en el renglón de continuidad en la organización. Esto incluye el diseño de planes de recuperación y medidas de reducción de riesgo.
- **Control de Acceso**: Es el que se ejecuta con el fin de que un usuario sea identificado y autenticado de manera exitosa para que le sea permitido el acceso al sistema.
- **Control informático:** las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo reduciendo la probabilidad o impacto del evento.
- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Copia de seguridad (Backup):** Es el proceso de respaldo de archivos o bases de datos físicos o virtuales a un sitio secundario para la preservación en caso de falla del equipo u otra catástrofe. El proceso de copia de seguridad de datos es fundamental para un plan de recuperación de desastres (DR) exitoso.
- **Criticidad:** Medida del impacto que tendría la organización debido a una falla de un sistema y que éste no funcione como es requerido.
- **Cuenta de usuario:** Es una colección de información que indica al sistema operativo los archivos y carpetas a los que puede tener acceso un determinado usuario del equipo, los cambios que puede realizar en él y sus preferencias personales, como el fondo de escritorio o el protector de pantalla.
- **Dato:** Descripción de hechos, situaciones, sucesos o valores, representados mediante símbolos físicos o electrónicos.
- **Datos Abiertos:** 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 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.
- **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).

- **Encriptación**: Proceso que permite volver ilegible la información que se considera importante. Una vez la información esta encriptada solo puede accederse aplicando una clave.
- **Estándar:** Es un conjunto de características y requisitos que se toman como referencia o modelo y son de uso repetitivo y uniforme. Para que sea un estándar debe haber sido construido a través de consenso y refleja la experiencia y las mejores prácticas en un área en particular.
- **Estimación del Riesgo:** Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo. (ISO/IEC 27005).
- **Evaluación de riesgos:** Según [ISO/IEC Guía 73:20022], es el proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.
- **Evento:** Según [ISO IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.
- **Garantía:** se deben tener en cuenta los plazos de vigencia de la garantía ofrecidos y los requeridos para el proceso de implementación, adaptación, pruebas, y puesta en funcionamiento.
- **Gestión de claves:** (inglés: Key management). Controles referidos a la gestión de claves criptográficas.
- **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).
- **Gestión de riesgos:** Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.
- **Gobierno Abierto:** Doctrina política que sostiene que los temas de Gobierno y administración pública deben ser abiertos a todos los niveles posibles en cuanto a transparencia.
- **Gobierno Digital:** Es la política pública liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones -Ministerio TIC, que tiene como objetivo “Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital”

- **Identificación del riesgo:** Proceso para encontrar, enumerar y caracterizar los elementos de riesgo. (ISO/IEC 27005).
- **Impacto:** Cambio adverso en el nivel de los objetivos del negocio logrados. (ISO/IEC 27005).
- **Incidente:** Según [ISO IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Información Pública:** Agrupación ordenada de datos públicos, que permite otorgarle a los datos una utilidad y uso en determinado contexto, y que se genera a partir del desarrollo de actividades para el funcionamiento del Estado, es decir de los registros periódicos de las actividades misionales de las entidades, o como consecuencia del ejercicio de funciones de rutina en el Estado.
- **Infraestructura de procesamiento de información:** Cualquier sistema de procesamiento de información, servicio, plataforma tecnológica, o instalación física que los contenga.
- **Infraestructura tecnológica:** elementos de hardware, software y comunicaciones que soportan la operación de los diferentes servicios de la entidad, entre los cuales se encuentran: equipos de trabajo, equipos portátiles, impresoras, escáner, videocámaras, wifi, sistemas operacionales, herramientas ofimáticas e internet entre otros.
- **Intranet:** Es un servidor Web seguro, interno y exclusivo, que le da a los empleados y al personal de una institución o compañía la posibilidad de compartir información sin que se exponga a la comunidad Web en general.
- **Inventario de activos: L**ista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del Sistema de gestión de seguridad de la información, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos. (ISO 27000.es, 2012)
- **Legalidad:** El principio de legalidad o Primacía de la ley es un principio fundamental del Derecho público conforme al cual todo ejercicio del poder público debería estar sometido a la voluntad de la ley de su jurisdicción y no a la voluntad de las personas (ej. el Estado sometido a la constitución o al imperio de la ley). Por esta razón se dice que el principio de legalidad establece la seguridad jurídica, Seguridad de Información, Seguridad informática y garantía de la información.
- **No conformidad grave:** Ausencia o fallo de uno o varios requerimientos de la ISO 27001 que, basada en evidencias objetivas, permita dudar seriamente de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo inaceptable.

- **No conformidad:** Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.
- **Parte interesada (Stakeholder):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- **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 riesgo:** 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 De La Información:** Derecho que tienen todos los titulares de la información, en relación con la información que involucre datos personales y la información clasificada que éstos 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, la correlativa obligación de proteger dicha información en observancia del marco legal vigente.[1]
- **Probabilidad:** Es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo. (ISO/IEC 27005)
- **Riesgo en la seguridad de la información:** Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización. (ISO/IEC 27005)
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **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

[1] 1 modelo de Seguridad y Privacidad de la Información.

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).

- **Sistema De Información:** Conjunto de datos, aplicaciones y equipos que de manera conjunta proveen a la empresa la información necesaria para la ejecución de las tareas y la toma de decisiones de los niveles estratégico, táctico y operativo.
- **Sistema operativo:** Programa de computador que organiza y gestiona todas las actividades que sobre él se ejecutan. Algunos sistemas operativos son Windows, Unix y Linux.
- **Software:** Información organizada en forma de sistemas operativos, utilidades, programas y aplicaciones que permiten que los computadores funcionen. Consiste en instrucciones y códigos cuidadosamente organizados escritos por programadores en cualquiera de los diferentes lenguajes de programación especiales. El software se divide comúnmente en dos categorías principales: Software del sistema: controla las funciones básicas (e invisibles para el usuario) de un computador y generalmente viene preinstalado con la máquina.
- **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).
- **Usuarios:** personas que, directa o indirectamente, tengan algún tipo de relación con la Entidad y/o que tengan acceso a los recursos tecnológicos de la Entidad, por ejemplo: servidores, contratistas, terceros, proveedores, entre otros.
- **Valoración de riesgos:** Según [ISO IEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.
- **Vulnerabilidad:** Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISOI/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

15. Declaración de Aplicabilidad

Se relacionan los controles establecidos en el estándar NTC-ISO-IEC 27001 que presentan oportunidades de mejora en Empresas Públicas de Armenia S.A. ESP

16. Declaración de publicación

La publicación del Plan de Seguridad y Privacidad de la Información de Empresas Públicas de Armenia ESP. se realizará en:

1. El Sitio Web www.epa.gov.co una vez sea aprobada.
2. El Sistema de Gestión Integrado disponible en la Intranet. https://intraepa.gov.co/

El presente plan rige a partir de su publicación.