Sistema de Gestión de Seguridad de la Información
Empresas Públicas de Armenia E.S.P.

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, 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 Gobierno Digital.

2. Glosario

- **Activo**

En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

- **Amenazas**

Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

- **Análisis de Riesgo**

Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- **Auditoría**

Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

- **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).

- **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).

- **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.

- **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).

- **Estimación del Riesgo**

Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo. (ISO/IEC 27005)

- **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).

- **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)

- **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 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).

- **Probabilidad**

Es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo. (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).

- **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)

- **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).

- **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).

- **Vulnerabilidad**

Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

3. Objetivos

3.1 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.

3.2 Objetivos Específicos

- 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

- Involucrar a todas las partes interesadas, en la gestión activa de los riesgos documentados, asociados a la seguridad de la información.

- 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.

- 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 al contexto de Empresas Públicas de Armenia ESP.

4. Alcance

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).

5. Roles y responsabilidades

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 de seguridad de la información.

- Sistema de Gestión Integrado. Define los lineamientos de calidad, que se deben aplicar a las políticas de seguridad general y específicas, así como al plan de tratamiento de los riesgos de seguridad de la información y el plan de seguridad 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 las políticas de seguridad de la información, general y específicas, 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 las políticas de seguridad 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 las políticas de seguridad de la información, y sobre la idoneidad de los controles asociados a la gestión de los riesgos.

6. 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:

6.1 Planificar

- Establecer contexto
- Valorar el riesgo
- Planificar el tratamiento del riesgo
- Aceptación del riesgo

6.2 Hacer

- Implementar el plan de tratamiento del riesgo

6.3 Verificar

- Monitorear y revisar continuamente los riesgos

6.4 Actuar

- Mantener y mejorar el proceso de gestión del riesgo en la seguridad de la información

7. Despliegue de Plan de tratamiento de Riesgos de Seguridad de la Información

7.1 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.

7.2 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 al alcance establecido (Icontec, 2008), y realizar el respectivo registro en el documento Inventario de Activos de Información - Etapa de Planificación - Buenas Practicas 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 Practicas 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

7.3 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:

7.3.1 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:

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 1 Calificación de probabilidad

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 compromete la prestación del servicio	Genera interrupciones en la prestación del servicio	Afecta la operación de varios procesos proceso	Compromete la imagen de Empresas Públicas de Armenia ESP y sus funcionarios
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

Tabla 2 Calificación de impacto

7.3.2 Evaluación del Riesgo

Probabilidad	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 Evitar el Riesgo 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 Evitar el Riesgo Reducir el Riesgo Compartir o Transferir
	Impacto	Leve	Moderado	Catastrófico
	Valor	5	10	20

Tabla 3 Evaluación del Riesgo

7.4 Valoración del Riesgo

7.4.1 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.

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 evitan la materialización del riesgo
Asignables	tienen responsables definidos para su ejecución

Tabla 4 Identificación de Controles

7.4.2 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.

7.4.3 Ejecución de la Valoración del Riesgo

Criterios	Valoración del Riesgo
No existen controles	Se mantiene el resultado de la evaluación antes de controles
Existen pero no son efectivos	Se mantiene el resultado de la evaluación antes de controles
Los controles existente 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 efectivos y son documentados	Pasa a escala inferior, según criterio de los responsables