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

Empresas Públicas de Armenia ESP
la empresa de todos

DIRECCIÓN
TIC

Tabla de contenido

1. Justificación

Empresas Públicas de Armenia ESP, dentro de sus políticas de calidad, incluye la seguridad de la información, integrándola de manera activa en la cultura organizacional, y promoviendo la responsabilidad corporativa en tres componentes esenciales, como lo son la confidencialidad, integridad y disponibilidad de la información. Para soportar esto, el Estado Colombiano, ha desarrollado un completo marco legal y normativo, que permite a entidades como Empresas Públicas de Armenia ESP, desarrollar planes y políticas robustas, orientadas a garantizar la seguridad de la información. Entre otras normas podemos encontrar:

- Ley 1266 del 2008: *Por la cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.*

- Ley 1581 de 2012 Protección de datos personales, Artículo 4, literal g Principio de seguridad: *"La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento."*

- Ley 1581 de 2012, Artículo 17, literal d: *"Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento"*

- Ley 1712 de 2014 Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, artículo 7: "Disponibilidad de la información"
  "En virtud de los principios señalados, deberá estar a disposición del público la información a la que hace referencia la presente ley, a través de medios físicos, remotos o locales de comunicación electrónica. Los sujetos obligados deberán tener a disposición de las personas interesadas dicha información en la web, a fin de que estas puedan obtener la información, de manera directa o mediante impresiones. Asimismo, estos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que presten."

- Decreto 2573 de 2014 Estrategia Gobierno en Línea (Gobierno Digital): "Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones".

- Decreto 2573 de 2014 Estrategia Gobierno en Línea (Gobierno Digital), Artículo 5 numeral 4: *"Seguridad y privacidad de la Información. Comprende acciones*

transversales a demás componentes enunciados, a proteger la información y sistemas de información, del acceso, divulgación, interrupción o destrucción no autorizada.".

- *Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2):* *Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.*

- Decreto 1413 de 2017, artículo 2.2.17.6.6, Seguridad de la información: *"Los actores que traten información, en el marco del presente título, deberán adoptar medidas apropiadas, efectivas y verificables de seguridad que le permitan demostrar el correcto cumplimiento de las buenas prácticas consignadas en el modelo de seguridad y privacidad de la información emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones, o un sistema de gestión de seguridad de la información certificable. Esto con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información."*

- Decreto 1413 de 2007, artículo 2.2.17.6.1, Responsable y encargado del tratamiento: *"Los operadores de servicios ciudadanos digitales serán responsables del tratamiento de los datos personales que los ciudadanos le suministren directamente y encargados del tratamiento respecto de los datos que otras entidades le proporcionen."*

- Decreto 1413 de 2007, artículo 2.2.17.6.5, Privacidad por diseño y por defecto: *"Los operadores de servicios ciudadanos digitales deberán atender las buenas prácticas y principios desarrollados en el ámbito internacional en relación con la protección y tratamiento de datos personales que son adicionales a la Accountability, y que se refieren al Privacy by design (PbD) y Privacy Impact Assessment (PIA), cuyo objetivo se dirige a que la protección de la privacidad y de los datos no puede ser asegurada únicamente a través del cumplimiento de la normativa, sino que debe ser un 'modo de operar de las organizaciones, y aplicarlo a los sistemas de información, modelos, prácticas de negocio, diseño físico, infraestructura e interoperabilidad, que permita garantizar la privacidad al ciudadano y a las empresas en relación con la recolección, uso, almacenamiento, divulgación y disposición de los mensajes de datos para los servicios ciudadanos digitales gestionados por el operador"*

- Decreto 1499 de 2017, por medio del cual se modifica el Sistema de gestión y se da forma al Modelo Integrado de Planeación y Gestión, Manual Operativo, Capítulo 3.2.1.3, Seguridad de la Información: *"Una constante en la gestión de las entidades públicas debe ser implantar en todos los procesos de la entidad, políticas, controles y procedimientos con el fin de aumentar los niveles de protección y adecuada salvaguarda de la información, preservando su confidencialidad, integridad y disponibilidad, mediante la aplicación de un*

proceso de gestión del riesgo de tal manera que se brinde confianza a las partes interesadas."

- Resolución 2710 de 2017 (IPV6): *"Por la cual se establecen los lineamientos para la adopción del protocolo IPv6".*

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 auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (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).

- **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).

- **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).

- **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 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).

- **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.

3. Objetivos

3.1 Objetivo General

Establecer las actividades y el marco conceptual, sobre el cual se soporta el plan de seguridad, brindando los conceptos requeridos para realizar un aseguramiento de la información en Empresas Públicas de Armenia ESP, en el marco de la norma ISO 27000.

3.2 Objetivos Específicos

- Fortalecer el Sistema de Gestión de Seguridad de la Información y facilitar su inclusión en el Sistema Integrado de Gestión de Empresas Públicas de Armenia ESP.

- Impulsar la conciencia en las partes interesadas, respecto a la importancia que tiene la seguridad de la información, para garantizar la continuidad del servicio.

- Construir una plataforma, conformada por planes de acción y políticas general y específicas, que brinden las herramientas necesarias para fomentar las mejores prácticas en Empresas públicas de Armenia ESP, en cuanto a la seguridad de la información.

- Socializar y difundir el Sistema de Seguridad de la Información de Empresas Públicas de Armenia ESP.

4. Antecedentes

4.1 Estado del Arte

Por medio de una labor detallada, de levantamiento de información, se realiza el análisis de vulnerabilidades en lo que respecta a Seguridad de la Información, en cada uno de los procesos, identificando los posibles riesgos, y realizando una documentación de los mismos.

Se identifican dos tipos de vulnerabilidades, las técnicas y las administrativas. Las vulnerabilidades técnicas se refieren a los fallos de infraestructura básica, para la instalación de redes de datos y eléctricas, que por desconocimiento o faltas de controles, crean factores de riesgo que pueden llegar a comprometer la continuidad del negocio y afectar los activos de información. Las vulnerabilidades administrativas, incluyen aspectos relacionados con la operación, que podrían influir negativamente en la capacidad para prestar el servicio, tanto en condiciones normales como de emergencia interna o externa. Para ello se deben tomar en cuenta las actividades dentro de las diferentes áreas de la organización, sus interacciones, la disponibilidad de servicios básicos, y los procedimientos a seguir en caso de emergencia.

4.2 Diagnóstico de Infraestructura

Por medio de una labor detallada, de levantamiento de información, se realiza el análisis de vulnerabilidades en lo que respecta a Seguridad de la Información, en cada uno de los procesos, identificando los posibles riesgos, y realizando una documentación de los mismos.

4.3 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. E.S.P

4.4 Plan de Tratamiento de Riesgos de la Seguridad de la Información

Se construye el Plan de Tratamiento de los Riesgos de la Seguridad de la Información, donde se registran los lineamientos para la administración, de aquellos eventos que comprometan la seguridad de la información.

5. Plan de Acción

5.1 Actualización y Fortalecimiento de Políticas de Seguridad de la Información

La Dirección TIC, busca que para el año *2022, se cuenten con lo necesario para contar con un Sistema General de Seguridad de la Información; que contribuya en gran medida a la protección de los datos y definición de los procedimientos y controles que se deben llevar a cabo para mantener la seguridad y privacidad de la información; para esto se cuenta ya con las políticas de seguridad de la información y el mapa de riesgos de seguridad de la información.*

Las políticas se basan en tres elementos esenciales:

1. Lineamientos *de la Política* de Gobierno *Digital,* en lo que respecta al eje temático de Seguridad y Privacidad de la información, incluyendo las plantillas que ofrece Mintic para la construcción de políticas
2. Políticas y Objetivos de la Norma NTC-ISO/IEC 27001
3. Análisis del contexto de Empresas Públicas de Armenia ESP, entre lo que se incluyen:
    - *a.* Inventario de Activos de la Información Actualizado
    - *b.* Diagnóstico de Infraestructura TI
    - *c.* Mapa de Riesgos de Seguridad de la Información.

5.2 Plan de Divulgación de Políticas de Seguridad de la Información

La Dirección TIC, ha venido socializando las políticas de seguridad de la información a través de la Intranet. Se deberá continuar con dicha socialización y concientización; construyendo mensajes asertivos y que lleguen de forma clara y directa; para un mayor entendimiento y cumplimiento de dichas políticas.

5.3 Actualización de Activos de Información

La Dirección TIC, cuenta con un inventario de los activos de información detallado de todos los equipos de cómputo de Empresas Públicas de Armenia; lo que permitió la identificación y registro en el mapa de riesgos de seguridad de la información; de vulnerabilidades, amenazas, riesgos y controles a aplicar; en el caso de que uno de estos activos se vea afectado por un fallo en el Sistema de Seguridad de la Información.

5.4 Actualización y Seguimiento del Mapa de Riesgos de Seguridad de la Información

Una vez identificado y documentado el inventario de activos, se ha construido el mapa de riesgos de seguridad de la información, toda vez, que se tiene como *uno de los* objetivos, lograr la certificación en la norma ISO 27000 para *el* proceso *de Dirección Comercial.*

5.5 Fortalecimiento de Infraestructura TI

Se han venido ejecutando proyectos para la actualización de la infraestructura, se cambiaron a puntos de datos que se soportan por cableado de tecnología de frontera, en este caso categoría 7ª, que incluye características como, Certificable RETIE, blindaje anti espionaje y convergencia de tecnología entre otros. Además, esta actualización tecnológica, incluye el reemplazo del Switch core y los switchs de borde, en capa 3, los cuales permiten realizar de forma inteligente la segmentación de la red de datos, brindando capas adicionales de protección de los datos que se transmiten en la intranet.

Incluyendo procesos de corrección de ubicación de cableado y patch cord visibles y sin canalizaciones, mejorando desde lo estético, pasando por lo tecnológico y finalizando en seguridad de la información.

Entre los proyectos se incluye la compra de equipos y periféricos para la actualización de la plataforma tecnológica. Y se espera dentro de este plan continuar beneficiando en los proyectos a todos los funcionarios de Empresas Públicas de Armenia.

5.6 Alistamiento ISO 27000 Proceso Comercial

Empresas Públicas de Armenia ESP, por medio de la Dirección TIC, construye un plan y un cronograma, para realizar el alistamiento del proceso de Dirección Comercial, para lograr la certificación en la norma ISO 27000. Para esto, se realizó, todo un trabajo de levantamiento de información, entendimiento del contexto y reuniones de partes interesadas, identificando los riesgos y construyendo un marco de trabajo, sobre el cual la Dirección Comercial, fortalece su proceso a través de la adopción de las políticas de Seguridad de la Información.

5.7 Plan de Auditorías internas ISO 27000

Teniendo en cuenta que se realiza el alistamiento del proceso de Dirección Comercial, en lo que respecta a ISO 27000, se plantea un plan de auditoría a partir del mes de Julio de la presente vigencia, con el fin de evaluar lo siguiente:

1. Entendimiento y conocimiento general del Sistema de Gestión de Seguridad de la Información.
2. Conocimiento de las políticas de seguridad que aplican al puesto de trabajo.
3. Identificación y aplicación de controles, según la matriz de riesgos identificado.
4. Conciencia de la Seguridad y Privacidad de la Información.

5.8 Cronograma

N°	Acciones Clave	*Año 2022*										
		Feb	Mar	Abril	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic
1	Actualización y *Fortalecimiento de* Políticas de Seguridad de la Información											
2	*Plan de Divulgación de Políticas de Seguridad de la Información*											
3	Actualización del Inventario de Activos de Información											
4	Seguimiento Mapa de Riesgos de Seguridad de la Información											
5	Actualización Infraestructura TI											
6	Alistamiento y ejecución de Auditoria del Sistema de Seguridad de la Información ISO 27000											
7	Seguimiento y/o actualización de Políticas de Seguridad Perimetral											