# Plan de Seguridad y Privacidad de la Información – PSPI

## 2024-2026

Empresas Públicas de Armenia ESP.

**ARMENIA QUINDÍO.**
*22 de julio de 2024*

## 1. Tabla de contenido

## Tabla de Ilustraciones



## Listado de Tablas

## 2. Introducción

Para cumplir con el propósito de Empresas Públicas de Armenia ESP, se requiere que la entidad identifique, gestione y proteja con las mejores estrategias y tácticas los activos de valor que permitan la continuidad y mantenibilidad del negocio.

Por otro lado, el Ministerio TIC, máximo órgano de gobierno en aspectos de Tecnologías de la Información y las Comunicaciones ha definido desde su concepción un Modelo de Seguridad de Privacidad y Seguridad de la Información. Este modelo hace parte de lo establecido en la Política de Gobierno Digital y la Política de Seguridad Digital que también compone y se articula a la normatividad, guías, documentos de apoyo y formatos pensados para acompañar a las entidades públicas en una adecuada implementación de un Sistema de Gestión de Seguridad y Privacidad de la Información.

La Dirección TICs de Empresas Públicas de Armenia ESP, a través de la definición de su Plan de Seguridad y Privacidad de la Información – PSPI – EPA 2023-2025, podrá definir y adoptar los lineamientos de la Gestión de seguridad y privacidad de la Información que se establece en el gobierno de la información, desde lo definido en las Políticas de Seguridad Digital y Gobierno Digital del Estado Colombiano; desarrollar su rol estratégico al interior de la entidad en la protección de los activos de información de la entidad que deriven en espacios físicos y visuales seguros y soluciones con parámetros de seguridad reales que fortalezcan la capacidad de generar transformaciones en el Municipio de Armenia.

## 3. Alcance del documento

Este documento tiene un alcance enfocado a la actualización, mantenimiento y gobernabilidad de las estrategias, tácticas y acciones para garantizar seguridad y privacidad de la información de los activos de valor en Empresas Públicas de Armenia ESP., por medio de la operación continua del Sistema de Gestión de Seguridad y Privacidad de la Información articulado al Modelo de Madurez Digital diseñado por la entidad para la optimización y cumplimiento de las metas de negocio de la empresa en el periodo del *2024-2026.*

Inicialmente se determina la situación actual analizando las brechas y barreras para garantiza *la* seguridad y privacidad de la información, evaluando su eficacia, el grado de madurez en el que se encuentra y la incorporación de prácticas de seguridad en la ejecución de las actividades.

Este plan está proyectado a tres (3) años, y permite definir un modelo iterativo de actualización anual como mínimo, al contexto de la entidad y del sector, soportándose en los lineamientos establecidos por el Ministerio TIC en lo que respecta a las Políticas de Gobierno Digital y Seguridad Digital.

## 4. Objetivos

### Objetivo General

Establecer las actividades y el marco conceptual, sobre el cual se soporta y garantiza el aseguramiento de los activos de la información en Empresas Públicas de Armenia ESP, en el marco de la Política de Seguridad Digital del Ministerio TIC adscrito a MiPG y el estándar ISO 27001 de 2013.

### Objetivos Específicos

1. Conocer el estado actual de Empresas Públicas de Armenia ESP en el componente de Seguridad y Privacidad de la Información.
2. Fortalecer el Esquema de gobierno de TI para el Modelo Ruta de Madurez Digital de la entidad, interviniendo en Planes de acción, Políticas de seguridad y privacidad, guías, procedimientos y formatos de trabajo que brinden las capacidades necesarias para fomentar las mejores prácticas en Empresas públicas de Armenia ESP, en cuanto a la seguridad de la información.
3. Fortalecer el Sistema de Gestión de Seguridad y Privacidad de la Información tomando como referencia los parámetros, lineamientos establecidos en el Modelo de Seguridad y Privacidad de la Información definidos a nivel nacional y facilitar su inclusión en el Sistema Integrado de Gestión de Empresas Públicas de Armenia ESP.
4. Facilitar la gestión de los riesgos de seguridad y privacidad de la información, Seguridad Digital.
5. Mitigar el impacto de los incidentes de Seguridad y Privacidad de la Información y de Seguridad Digital, de forma efectiva, eficaz y eficiente.
6. Establecer condiciones de aseguramiento físico y digital que nos permita fortalecer la confidencialidad, integridad, disponibilidad, autenticidad, y privacidad de la información.
7. Definir los lineamientos necesarios para el manejo de la información, tanto física como digital, en el marco de una gestión documental basada en Seguridad y Privacidad de la Información.
8. Desarrollar acciones de Transferencias de Capacidades en la gestión de

acciones de TI para las partes interesadas, respecto a la importancia que tiene la seguridad de la información, para garantizar la continuidad del servicio.

9. Socializar y difundir el Sistema de Seguridad de la Información de Empresas Públicas de Armenia ESP.
10. 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.

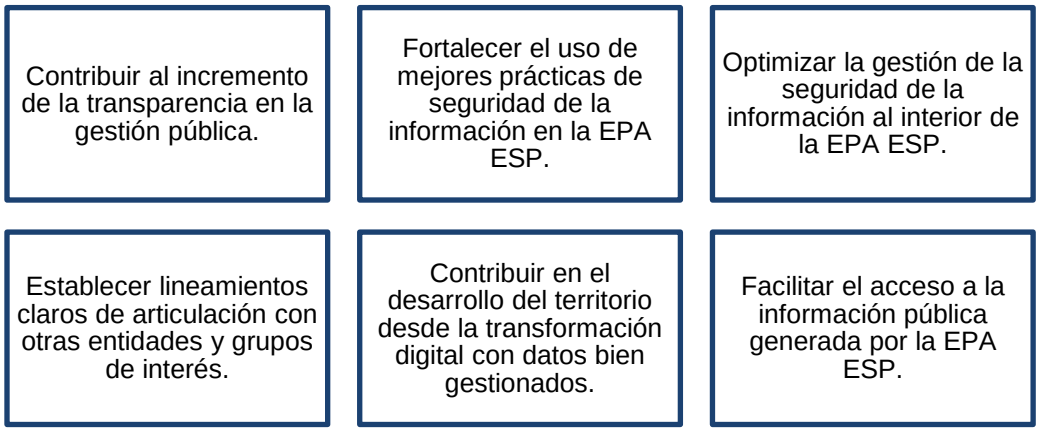


**Ilustración 1. Impactos a la Entidad y Grupos de Interés**

## 5. Marco Normativo y Documentación Técnica

Entre otras normas podemos encontrar:

## Marco Normativo

### Tabla 1. Marco Normativo de TIC Aplicable a la Entidad.

| Jerarquía de la Norma | Número Norma | Año de Expedición | Descripción de la norma |
|---|---|---|---|
| Constitución Política | Artículo 15. | 1991 | Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacer los respetar". De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. |
| Constitución Política | Articulo 20 | 1991 | Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios de comunicación masiva. Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura. |
| Ley | 23 | 1982 | Sobre derechos de autor |
| Ley | 80 | 1993 | Por la cual se expide el Estatuto General de Contratación de la Administración PÚBLICA |
| Ley | 87 | 1993 | Por la cual se dictan Normas para el ejercicio de control interno en las entidades y organismos del Estado, y demás normas que la modifiquen. |
| Ley | 128 | 2018 | Por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest. |
| Ley | 527 | 1999 | Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos. |
| Ley | 594 | 2000 | Por medio de la cual se dicta la Ley General de Archivo y se dictan otras disposiciones. |
| Ley | 603 | 2000 | Por la cual se modifica el artículo 47 de la Ley 222 de 1995, Articulo 2. Artículo 2°. Las autoridades tributarias colombianas podrán verificar el estado de cumplimiento de las normas sobre derechos de autor por parte de las sociedades para impedir que, a través de su violación, también se evadan tributos. |
| Ley | 679 | 2001 | Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución. |
| Ley | 734 | 2002 | Por medio de la cual se expide del código único disciplinario. |
| Ley | 906 | 2004 | Código de Procedimiento Penal. |

| Jerarquía de la Norma | Número Norma | Año de Expedición | Descripción de la norma |
|---|---|---|---|
| Ley | 962 | 2005 | Simplificación y Racionalización de Trámite. Atributos de seguridad en la Información electrónica de entidades públicas. |
| Ley | 1032 | 2006 | Por la cual se modifican los artículos 257, 271, 272 y 306 del Código Penal. Artículo 271. Violación a los derechos patrimoniales de autor y derechos conexos. Modificación del código Penal Colombiano Ley 599 de 2000. |
| Ley | 1150 | 2007 | Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos. |
| Ley | 1221 | 2008 | Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones. |
| Ley | 1266 | 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 | 1273 | 2009 | Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"· y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones |
| Ley | 1336 | 2009 | (Lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes.) por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes. |
| Ley | 1341 | 2009 | Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones - TIC-, se crea la agencia nacional de espectro y se dictan otras disposiciones |
| Ley | 1437 | 2011 | por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo. (Uso de medios electrónicos Procedimiento Administrativo Electrónico), Articulo 1 de la ley 1755 de 2015. |
| Ley | 1474 | 2011 | Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública. |
| Ley | 1581 | 2012 | Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales |
| Ley | 1672 | 2013 | Lineamientos para la Adopción de una política pública |

| Jerarquía de la Norma | Número Norma | Año de Expedición | Descripción de la norma |
|---|---|---|---|
| | | | de gestión integral de residuos de aparatos eléctricos y electrónicos |
| Ley | 1710 | 2012 | Por el cual se dictan disposiciones generales para la Protección de Datos Personales. |
| Ley | 1712 | 2014 | Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones. |
| Ley | 1955 | 2019 | Por el cual se expide el Plan Nacional de Desarrollo 2018- 2022. "Pacto por Colombia, Pacto por la Equidad". Incluyó el artículo 147 de Transformación Digital Pública y 148 de Gobierno Digital como política de gestión y desempeño institucional |
| Decreto | 103 | 2015 | Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones. |
| Decreto | 415 | 2016 | Por el cual se adiciona el Decreto Único reglamentario del sector de la Función Pública, Decreto 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones. |
| Decreto | 886 | 2014 | Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012. |
| Decreto | 1008 | 2018 | 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 | 1078 | 2015 | Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. |
| Decreto | 1081 | 2015 | Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República, Título 1, Disposiciones generales en materia de transparencia y del derecho de acceso a la información pública nacional |
| Decreto | 1083 | 2015 | Decreto Único Reglamentario del Sector Función Pública |
| Decreto | 1377 | 2013 | Por la cual se reglamenta la ley 1581 de 2012. |
| Decreto | 1412 | 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 |

| Jerarquía de la Norma | Número Norma | Año de Expedición | Descripción de la norma |
|---|---|---|---|
| | | | seguridad de la información certificable. Esto con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información.” |
| Decreto | 1474 | 2002 | Por el cual se promulga el "Tratado de la OMPI, Organización Mundial de la Propiedad Intelectual, sobre Derechos de Autor (WCT)", adoptado en Ginebra, el veinte (20) de diciembre de mil novecientos noventa y seis (1996). |
| Decreto | 1747 | 2000 | Por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales. |
| Decreto | 2106 | 2019 | "Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública." |
| Decreto | 2573 | 2014 | “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 | 2609 | 2012 | Por la cual se reglamenta la ley 594 de 200 y ley 1437 de 2011. |
| Decreto | 2693 | 2012 | Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Lí-nea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones. |
| Decreto | 2609 | 2012 | Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado". |
| Decreto | 2952 | 2010 | “por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008”. |
| Decreto | 4632 | 2011 | Por medio del cual se reglamenta parcialmente la Ley 1474 de 2011 en lo que se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones. |
| CONPES | 3701 | 2011 | Lineamientos de Política para Ciberseguridad y Ciberdefensa. |
| CONPES | 3854 | 2017 | Política Nacional de Seguridad Digital |
| CONPES | 3975 | 2019 | Política Nacional para la Transformación Digital e Inteligencia Artificial, del 8 de noviembre de 2019. El Consejo Nacional de Política Económica y social (CONPES) |
| Directiva | 02 | 2019 | Simplificación de la interacción digital los ciudadanos y |

| Jerarquía de la Norma | Número Norma | Año de Expedición | Descripción de la norma |
|---|---|---|---|
| Presidencial | | | el Estado. |
| Circular Externa Conjunta | 04 | 2019 | Tratamiento de datos personales en sistemas de información interoperables. |

**Fuente: Elaboración Propia**

Demás leyes, Decretos y desarrollos normativos que guían las acciones para la Gestión de Seguridad y Privacidad de la Información en Empresa Púbicas de Armenia.

## Documentación Técnica

**Tabla 2. Documentación Técnica de TIC Aplicable a la Entidad.**

| Documento | Año de Expedición | Descripción |
|---|---|---|
| ISO 9000 | 2015 | Normas de gestión y garantía de calidad definidas por la ISO. |
| ISO 17799 | 2007 | Código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO transcribiendo la primera parte de 8S7799. A su vez, da lugar a ISO 27002 por cambio de nomenclatura el 1 de Julio de 2007. No es certificable. |
| ISO 19011 | 2018 | Guidelines for quality and/or environmental management systems auditing". Guía de utilidad para el desarrollo de las funciones de auditor interno para un SGSI. |
| NTC-ISO/IEC 27001- 27002: | 2013 | Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. |
| NTC ISO 17799 | 2005 | Código de práctica para la gestión de la seguridad de la información. |
| ISO lEC 27005 | 2018 | Information technology Systems- Security techniques- information security risk management. |
| NTC – ISO 19011 | 2018 | Directrices para la Auditoría de los Sistemas de Gestión. |
| Modelo Estándar de Control Interno MECI 1000 | 2009 | 2da versión "Subsistema: Control de Gestión; Componente: Actividades de Control; Elemento: Monitoreo y Revisión e Información" |
| Manual Fundamentos de Preservación Digital a Largo Plazo. | 2018 | Instrumento brinda una estructura conceptual de la preservación digital, así como elementos normativos, técnicos y metodológicos, para orientar a las entidades en la formulación de la política de gestión documental y en la definición de acciones y buenas prácticas que les permitan asumir el gran reto de la preservación digital a largo plazo. |

| Documento | Año de Expedición | Descripción |
|---|---|---|
| Guía de documentos y expedientes electrónicos | 2017 | Orientar a las entidades públicas y privadas que cumplen funciones públicas, en la producción, gestión y tratamiento de los expedientes y documentos electrónicos, desde su creación hasta la preservación a largo plazo con el fin de garantizar su autenticidad, integridad, fiabilidad y disponibilidad durante su ciclo vital. |
| Modelo de Seguridad y Privacidad | 2016 | El Modelo de Seguridad y Privacidad de la Información – MSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos. |
| Documento Maestro del Modelo de Seguridad y Privacidad de la Información | 2021 | El Modelo de Seguridad y Privacidad de la Información – MSPI define los lineamientos para la implementación de la estrategia de seguridad digital, con el objetivo de formalizar al interior de las entidades un sistema de gestión de seguridad de la información – SGSI y seguridad digital, el cual contempla su operación basado en un ciclo PHVA (Planear, Hacer, Verificar y Actuar), así como los requerimientos legales, técnicos, normativos, reglamentarios y de funcionamiento; el modelo consta de cinco (5) fases las cuales permiten que las entidades puedan gestionar y mantener adecuadamente la seguridad y privacidad de sus activos de información. |
| Guía 1 - Metodología de pruebas de efectividad | 2016 | Permite disponer de una línea base durante los análisis en el recorrido de la implementación del modelo de seguridad y privacidad, de esta manera ayudar a proteger los bienes, activos, servicios, derechos y libertades dependientes del Estado. |
| Guía 2 - Política General MSPI v1 | 2016 | El siguiente documento es un formato que puede ser utilizado como plantilla para la elaboración de la política general de seguridad y privacidad de información para las entidades públicas, como parte del Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea, según lo establecido en el Decreto 1078 de 2015. |
| Guía 3 - Procedimiento de Seguridad de la Información | 2016 | Esta guía tiene como objetivo principal, indicar los procedimientos de seguridad que pueden generarse durante el diseño y la implementación del modelo de seguridad y privacidad de la información para las entidades del estado. Dependiendo de la entidad, dichos procedimientos pueden variar o si la entidad desea puede generar más procedimientos si lo considera conveniente. |
| Guía 5 - Gestión Clasificación de Activos | 2016 | Esa guía entrega los lineamientos básicos que deben ser utilizados por los responsables de la seguridad de la información, para poner en marcha la gestión y clasificación de activos de información que son manejados por cada entidad del estado, con el fin de determinar que activos posee la entidad, de cómo deben ser utilizados, los roles y responsabilidades que tienen los funcionarios sobre los mismos y, reconociendo adicionalmente el nivel de clasificación de la información que a cada activo debe dársele. |
| Guía 6 - Gestión | 2016 | Esta guía pretende mostrar una relación de Normas Técnicas |

| Documento | Año de Expedición | Descripción |
|---|---|---|
| Documental | | Colombianas - NTC, de consulta, emitidas por el Archivo General de la Nación, sobre gestión documental del país. |
| Guía 7 - Gestión de Riesgos | 2016 | A través de esta guía se busca orientar a las Entidades a gestionar los riesgos de Seguridad de la información basado en los criterios de seguridad (Confidencialidad, Integridad, Disponibilidad) buscando la integración con la Metodología de riesgos del DAFP. Ayudar a que las Entidades logren vincular la identificación y análisis de Riesgos de la Entidad hacia los temas de la Seguridad de la Información. |
| Guía 8 - Controles de Seguridad de la Información | 2016 | Proteger la información de las entidades del Estado, los mecanismos utilizados para el procesamiento de la información, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad y confiabilidad de la información. |
| Guía 9 - Indicadores Gestión de Seguridad de la Información | 2015 | En esta guía encontrara una serie de indicadores de gestión que podrían ser utilizados al interior de su entidad para medir la efectividad, eficacia y eficiencia de la Seguridad de la Información dentro de la entidad. |
| Guía 10 - Continuidad de Negocio | 2010 | La guía expuesta en este documento es un complemento del modelo de seguridad y privacidad de la información y se constituye en un referente de la continuidad del negocio para las entidades del Estado. |
| Guía 11 - Análisis de Impacto de Negocio | 2015 | Documento guía por medio del cual las Entidades del estado puedan consultar los lineamientos de seguridad ante situaciones de emergencia a fin de mitigar el impacto producido por la interrupción de los servicios de alta criticidad que afectan sensiblemente las operaciones del negocio. |
| Guía 12 - Seguridad en la Nube | 2016 | Este documento, presenta los lineamientos y aspectos para tener en cuenta para el aseguramiento de la información en la nube – Cloud; que las Entidades del Estado deben seguir, de tal manera que se conserve la seguridad de los datos en este tipo de ambientes. |
| Guía 13 - Evidencia Digital (En actualización) | 2016 | Este documento da los lineamientos para realizar un proceso de informática forense adecuado, siendo a su vez un complemento al proceso de gestión de incidentes de seguridad de la información, ya que el enfoque de esta guía está relacionado con los eventos de seguridad de la información que pueden generar algún impacto a los activos de información. |
| Guía 14 - Plan de comunicación, sensibilización, capacitación | 2016 | Establecer lineamientos para la construcción y mantenimiento del plan de capacitación, sensibilización y comunicación de la seguridad de la información, para así, asegurar que este cubra en su totalidad los funcionarios de la Entidad, asegurando que cada uno cumpla con sus roles y responsabilidades de seguridad y privacidad de la información dentro de las entidades del Estado, |
| Guía 15 - Auditoria | 2016 | El Ministerio de las Tecnologías de la Información y las Comunicaciones, en concordancia con las actividades de la estrategia de gobierno en línea y con la implementación del modelo de seguridad y privacidad de la información, pone a disposición de |

| Documento | Año de Expedición | Descripción |
|---|---|---|
| | | las entidades, la siguiente guía, para que puedan tener una línea base durante los análisis en el recorrido de la implementación del modelo de seguridad y privacidad, de esta manera ayudar a proteger los bienes, activos, servicios, derechos y libertades dependientes del Estado. |
| Guía 16 - Evaluación de Desempeño | 2017 | Fase donde se establecen los aspectos a ser desarrollados por los responsables de la gestión de seguridad de la información en todos los niveles de la entidad, para así, evaluar y en donde sea aplicable, medir el desempeño del sistema contra la política, los objetivos y la experiencia práctica de la gestión de seguridad de la información, a la vez que se reportan los resultados a la dirección para su revisión y toma de decisiones. |
| Guía 17 - Mejora continua | 2015 | El modelo de Seguridad y Privacidad de la Información cuyo propósito es servir como guía para la mejora de los estándares de Seguridad de la Información de las Entidades, cuenta con 5 fases para la gestión de la Seguridad y Privacidad de la información de las Entidades.<br><br>La fase final del modelo corresponde a la mejora continua del proceso de gestión la cual pretende apoyar el mantenimiento y mejora del sistema. |
| Guía 18 - Lineamientos terminales de áreas financieras de entidades públicas | 2016 | En este documento encontrará los lineamientos que las entidades deben implementar para elevar el aseguramiento de los equipos o terminales móviles asignados por la entidad, donde se realizan las transacciones a financieras como los son: pago de nómina, pagos de seguridad social, pagos de contratación y transferencias de fondos, entre otros. |
| Guía 19 - Aseguramiento de protocolo IPv4_IPv6 | 2017 | Este documento, presenta los lineamientos y políticas que se requieren tener en cuenta para la seguridad del protocolo IPv6, en las distintas infraestructuras de Tecnologías de la Información y las Comunicaciones que las Entidades del Estado, teniendo en cuenta su aplicación en todo el ciclo de desarrollo que sigue el nuevo protocolo, en un ambiente controlado y seguro que permita consolidar el proceso de adopción de IPv6 con seguridad y con un nivel de impacto altamente positivo para todas las organizaciones del país. |
| Guía 20 - Transición IPv4_IPv6 | 2017 | Este documento, presenta los lineamientos técnicos que se requieren tener en cuenta para seguir el proceso de transición de IPv4 a IPv6, en las distintas organizaciones del Estado, teniendo en cuenta su aplicación para todo el ciclo de desarrollo por fases que requiere el nuevo protocolo, en un ambiente controlado y seguro que permita consolidar una adopción del protocolo IPv6 con éxito en el país. |
| Guía para la administración del riesgo y el diseño de controles en entidades públicas | 2018 | El Consejo Asesor del Gobierno nacional en materia de control interno consideró necesario unificar la metodología existente para la administración del riesgo de gestión y corrupción, con el fin de hacer más sencilla la utilización de esta herramienta gerencial para las entidades públicas y así evitar duplicidades o reprocesos. |

| Documento | Año de Expedición | Descripción |
|---|---|---|
| Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información. | 2021 | La gestión de incidentes de seguridad de la información, proceso para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.<br><br>La guía expuesta en este documento es un complemento del modelo de seguridad y privacidad de la información y se constituye en un referente de la gestión de incidentes de seguridad de la información para las entidades del Estado. |
| inventario y clasificación de activos de información e infraestructura critica cibernética nacional | 2021 | Esta guía presenta los lineamientos básicos que debe tener en cuenta para realizar una adecuada identificación, gestión y clasificación de activos de información e infraestructura critica de cada entidad. |
| Roles y Responsabilidades | 2021 | Todas las entidades deben definir internamente las responsabilidades para ejecutar las actividades específicas de seguridad de la información designando a las personas apropiadas.<br><br>El mayor aporte que genera una definición de roles es que se tendrán establecidas las tareas que realizará cada uno de los miembros del equipo del MSPI, dejando un campo muy pequeño a que se presenten imprecisiones en referencia a las responsabilidades que cada personaje tiene. |
| Indicadores de Gestión de Seguridad de la Información | 2021 | La creación de indicadores de gestión está orientada principalmente en la medición de efectividad, eficiencia y eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información, indicadores que servirán como insumo para el componente de mejora continua, permitiendo adoptar decisiones de mejora. |
| Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas | 2021 | El objetivo principal de este documento es orientar a todas las entidades públicas del orden nacional y territorial, en la implementación de la Gestión de Riesgos de Seguridad de la información, que permita incrementar la confianza de las múltiples partes interesadas en el uso del entorno digital y del aseguramiento de los activos de información en las entidades. |

## 6. Beneficios Estratégicos y tácticos

La estructuración y la puesta en marcha del PSPI cuentan con importantes beneficios estratégicos y tácticos para Empresas Públicas de Armenia ESP:

- Mapeo del estado actual de la privacidad y seguridad de la información de entidad, las brechas y barreras de seguridad, el nivel de capacidades de en uso y demandas.

- Diseño, Alistamiento y Habilitación de un Modelo de Seguridad y Privacidad de la Información en pro de la continuidad y cumplimiento del propósito de la entidad.
- Articulación con el Modelo de transferencia de Capacidades de TI para los colaboradores de la entidad.
- Identificar herramientas que apoyen en el cumplimiento de las demandas en seguridad y privacidad de la información dentro de la entidad.
- Adquirir e implementar buenas prácticas de gestión de seguridad y privacidad de la información.
- Fortalecer la Dirección TICs de la entidad para apoyar los procesos estratégicos misionales, de apoyo y de evaluación.

Este Plan de Seguridad y Privacidad será la ruta de intervención en Seguridad y Privacidad de la Información de Empresas Públicas de Armenia ESP, para garantizar una adecuado manejo y protección de los activos de valor de la entidad.

## 7. Esquemas de Gobernanza Seguridad y Privacidad de la Información

La gestión de las competencias y capacidades en Seguridad y Privacidad de la Información requiere de parte de la entidad definir un conducto regular para la toma de decisiones, así como para la asignación y seguimiento de las responsabilidad y funciones que demanda este tema de vital importancia para garantizar la protección del Know-How de la entidad descrita en los activos de información.

Se deben definir claramente todas las responsabilidades en cuanto a seguridad de la información, en especial las relacionadas con el comité de seguridad de la información (o quien haga sus veces) y del oficial de seguridad de la información.

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

La gobernanza en Seguridad y Privacidad de la Información para la operación y cumplimientos de Empresas Públicas de Armenia ESP se describe en la siguiente estructura:

## Tabla 3. Guía Roles y Responsabilidades del Modelo de Seguridad y Privacidad de la Información.

| N° | Responsabilidad | Área/Procesos |
|---|---|---|
| 1 | Responsable de Gobierno y Gestión.<br>– Revisar y proponer al gerente general, para su aprobación, la Política de Seguridad de la Información.<br>– Supervisar la implementación de los lineamientos, procedimientos y planes asociados a la política Interna de seguridad y Privacidad de la información.<br>– Proponer estrategias y soluciones específicas para la incorporación de los controles necesarios para implementar las políticas establecidas y la debida solución de las situaciones de riesgo detectadas.<br>– Reportar al director TICs, respecto a oportunidades de mejora en materia de Seguridad de la Información, así como los incidentes relevantes y su solución.<br>– Arbitrar conflictos en materia de seguridad de la información y los riesgos asociados, y proponer soluciones. | Comité Institucional de Gestión y Desempeño |
| 2 | Responsable de Garantizar Cumplimiento.<br>– Aprobar las políticas de seguridad de la información.<br>– Evaluar el proceso de gestión de seguridad de la Información.<br>– Definir las estrategias y mecanismos de control para el tratamiento de riesgos que afecten a los activos de información.<br>– Facilitar los recursos requeridos para el sistema de gestión de seguridad de la información. | Gerencia General |
| 3 | Gestión estratégica y técnica en Seguridad y Privacidad de la Información<br>- Gestión de la Política.<br>- Gestión de Procedimientos e Instrumentos.<br>- Gestión del Plan de Seguridad y Privacidad de la Información.<br>- Garantizar el cumplimiento de los requerimientos de seguridad y privacidad de la información que demanda la presente política y demás documentos vinculantes normativos y técnicos de orden territorial y nacional.<br>- Formulación de iniciativas y planes de contingencia sobre niveles de riesgos identificados y reportados.<br>- Establecer mecanismos que permita la gestión de los incidentes reportados y la trazabilidad de estos.<br>- Establecer canales de comunicación con proveedores de TI correspondientes para la garantía de cumplimiento de la política.<br>- Socialización a los respectivos involucrados de las situaciones presentadas en gestión de incidentes.<br>- Identificar riesgos asociados a la gestión de incidentes de seguridad<br>- Contactar a las autoridades y/o grupos especializados en respuesta a incidentes para las labores de coordinación y apoyo.<br>- Monitorear el estado, nivel de aplicación de la política en la entidad.<br>- Organizar las actividades del Comité MiPG en materia de seguridad de la información. | Dirección de Tecnologías de la Información y las Comunicaciones. |

| N° | Responsabilidad | Área/Procesos |
|---|---|---|
| | - Estar en comunicación activa con los responsables de seguridad de otras entidades públicas y especialistas externos, con el fin de mantenerse actualizado acerca de las tendencias, normas y métodos de la seguridad de la Información.<br>- Apoyar a los diferentes procesos institucionales en la adopción del sistema de gestión de seguridad de la información.<br>- Mantener contacto con las autoridades en materia de ciberseguridad para conocer de primera mano indicios o alertas en materia de seguridad de la información y recibir el apoyo de grupos de respuesta ante incidentes de seguridad de la información.<br>- Mantener contacto con grupos de interés especial en materia de seguridad de la información para asegurar que la comprensión del entorno de la seguridad de la información sea actual y esté completa.<br>- Compartir e intercambiar información acerca de nuevas tecnologías, productos, amenazas o vulnerabilidades. | |
| 4 | - Garantizar el cumplimiento legal de la Política de Seguridad de la Información en la entidad.<br>- Trabajar de la mano con la Dirección TICs en la definición y gestión de los requerimientos estatuarios, reguladores y contractuales pertinentes en aspectos de seguridad y privacidad de la información.<br>- Asesorar legalmente en las acciones de Seguridad y Privacidad de la Información que se requieran en Empresas Públicas de y determinar las pautas legales que permitan cumplir con los requerimientos legales en esta materia.<br>- Asegurar que los incidentes que involucren la fuga de información sensible son manejados con base en las regulaciones aplicables.<br>- Determinar las consecuencias jurídicas que se podrán presentar sobre incumplimiento o desacato de las responsabilidades en la gestión de eventos e incidentes de TI.<br>- Orientar y asistir en acciones de adquisición de evidencia forense requerida<br>- Seguimiento y monitorio a eventos e incidentes. | Dirección Jurídica y secretaria general |
| 5 | - Fomentar la participación de los colaboradores (funcionarios y contratistas) y proveedores en las acciones de Educación, Información y Comunicación que definan.<br>- Incluir en el plan de capacitación anual temáticas asociadas a la gestión de incidentes.<br>- Garantizar cumplimientos de los lineamientos, procedimientos y planes asociados a la Seguridad y Privacidad de la Información del Talento Humano.<br>- Notificar a todo el Talento Humano que se incorpora a la entidad, sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan. | Gestión del Talento Humano |

| N° | Responsabilidad | Área/Procesos |
|---|---|---|
| | - Apoyar en la resolución de conflictos interno-asociados con violaciones u omisiones de la presente política. | |
| | - Difusión de información de carácter público a grupos de interés referente a la gestión de incidentes.<br>- Diseño de estrategias de EIC para capacitar a los colaboradores y proveedores.<br>- Difusión de material publicitario e informativo sobre las responsabilidad*es* y gestión efectiva de incidentes que se presenten. | Dirección de Comunicaciones |
| 6 | - Acompañar en la formulación y articulación de los planes de gestión de incidentes con la ruta estratégica del negocio. | Dirección de Planeación Corporativa |
| 7 | – Seguimiento al desempeño en la gestión de incidentes de TI.<br>– Realizar auditorías asociadas al cumplimiento de los establecido en esta política<br>– Reportar a los responsables el estado de cumplimiento de los lineamientos, procedimiento y uso adecuado de los instrumentos de seguridad de la información establecidos por esta política interna y los documentos de estructura y gobierno vinculantes.<br>– Recomendar acciones de mejora frente a los hallazgos y vulnerabilidades identificadas en las auditorias e informarlas al Comité MiPG. | Dirección Control de Gestión |
| | – Caracterizar y clasificar los activos de información de acuerdo con el grado de sensibilidad y criticidad de estos, documentar y mantener actualizada la clasificación.<br>– Definir los permisos de acceso para cada colaborador en su proceso teniendo en cuenta sus funciones y competencia.<br>– Informar a la Dirección TICs cuando detecte cualquier incidente de seguridad de la información, para tratarlo y corregirlo mediante la aplicación de controles.<br>– Proponer y/o implementar medidas de seguridad pertinentes para evitar vulnerabilidades e incidentes con los activos de información a su cargo.<br>– Socializar y aplicar las cláusulas de confidencialidad pertinentes para el personal y proveedores a su cargo.<br>– Apoyar y replicar la socialización de orientaciones que se presenten desde la alta dirección en materia de seguridad de la información.<br>– Ejercer liderazgo y compromiso en la aplicación de la política de Seguridad de la Información. | Procesos propietarios de activos de información |
| | – Informar a la Dirección TICs cuando detecte cualquier incidente de seguridad de la información.<br>– Sugerir controles o contramedidas para el tratamiento de incidentes que se presentes en seguridad y privacidad de la información.<br>– Documentar los aspectos de seguridad de la información aplicados dentro de su línea de gestión y su respectivo control de cambios. | Administradores de los Sistemas de Información y Plataforma de TI |

| N° | Responsabilidad | Área/Procesos |
|---|---|---|
| 8 | - Aplicar buenas prácticas en Seguridad de la Información.<br>- Asistir a los espacios de formación y capacitaciones citados.<br>- Apropiar y cumplir con los establecido en los espacios de capacitación.<br>- Conocer, divulgar, cumplir y hacer cumplir la Política Interna de Seguridad y Privacidad de la Información vigente, los procedimientos vinculantes y las normas asociadas.<br>- Hacer buen uso de los equipos de cómputo y periféricos que le sean asignados para el cumplimiento de sus funciones y responsabilidades, la relación de estos debe estar registrada en el Sistema de Inventarios de la EPA.<br>- Cumplir con los lineamientos de gestión de seguridad y privacidad de la información.<br>- Garantizar el buen manejo y custodia de la información almacenada en el equipo de cómputo y periféricos asignados.<br>- Dar el adecuado uso y cumplimiento a los activos de información mapeados en la entidad.<br>- Facilitar la revisión del equipo de cómputo, periféricos, sistemas de información y accesos asignados para el seguimiento de la adecuada gestión y uso según los establecido en la presente política<br>- Mantener en buen estado los equipos de cómputo y periféricos que le sean asignados. | Todos los procesos. |
| | – Abstenerse de acceder a espacios restringidos, manipular dispositivos e información que no estén en su rango de acceso y manipulación sin la previa autorización de manejo y gestión.<br>– Para el acceso, excepcional a recursos y activos de información es fundamental la autorización de acceso de los responsables del activo, siguiendo los parámetros establecidos en esta política.<br>– Cumplir las políticas de seguridad y privacidad de la información cuando se les autorice acceso a los activos de información institucionales.<br>– Usar únicamente las redes de acceso a invitados, la cual restringe el acceso solo a internet.<br>- Abstenerse de cualquier manipulación en los activos de información sin contar con las indicaciones y acompañamiento del responsable de la seguridad del activo de información comprometido. | Visitantes |

**Fuente: Guía Roles y Responsabilidades del Modelo de Seguridad y Privacidad de la Información. Elaborado por el MinTIC.**

## 8. Modelo Ruta de Madurez Digital

La Dirección TICs en sus acciones de integralidad ha definido para Empresas Públicas de Armenia ESP., el Modelo Ruta de Madurez Digital que contempla la integralidad de los elementos y responsabilidades en TI para cumplir con las

obligaciones de ley establecidas en la Política Gobierno Digital y Seguridad Digital.

Este Modelo Ruta de Madurez Digital describe las fases para lograr habilitación, operación, seguimiento y mejora continua en las acciones de TI que se deben realizar para llevar la entidad a ejercicios de Transformación Digital.

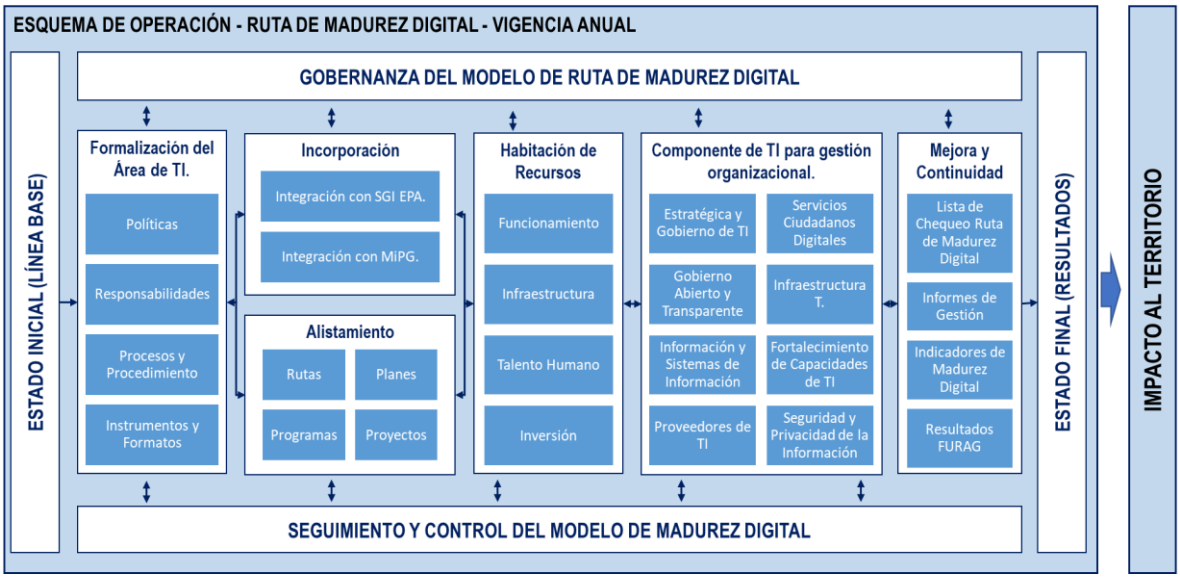


**Ilustración 2.Esquema de Operación - Ruta de Madurez Digital**

En el Modelo anterior podemos ver de manera amplia lo definido para la Madurez de TI, vemos que tiene la siguiente estructura:

- Gobernanza del Modelo Ruta de Madurez Digital: Pensado para gobernar el modelo de madurez digital y el conducto para la toma de decisiones.
- Estado Inicial (Línea Base): Los Diagnósticos pertinentes en TI, que se dividen en 2 según lo establecido desde orden nacional.
    - Diagnóstico de Gobierno Digital.
    - Diagnóstico de Seguridad Digital.
- Formalización del Área de TI: Esta fase permite la definición de los elementos de gobierno y gestión como lo son:
    - Formular políticas de gobierno en TI.
    - Establecer y asignar las responsabilidades.
    - Definir y describir los procesos y procedimientos aplicables.
    - Formular los instrumentos y formatos de trabajo pertinentes.
- Incorporación: Se encarga del acople y articulación con:
    - El Sistema de Gestión Integrado EPA ESP.
    - El Modelo Integrado de Planeación y Gestión MiPG.
- Alistamiento: Establece la formulación de los documentos de gestión y operatividad en el negocio, estos documentos son:

- Planes, que pueden ser estratégicos, de acción, de implementación, de seguimiento.
- Rutas, que están enfocadas en definir puntos clave de intervención con una continuidad para alcanzar ciertos resultados.
- Programas, se definen como un conjunto organizado, coherente e integrado de actividades, servicios o procesos, expresados en agrupaciones de proyectos que pretenden dar respuesta a una problemática definida, sin precisar un límite en el tiempo. Por ejemplo: Programa de Datos Abiertos y Colaboración.
- Proyectos, pensados para habilitar y fortalecer nuevos elementos que entreguen innovación y escalabilidad a la entidad.
- Habilitación de Recursos: Enfocado a garantizar los recursos que permitan la operación y continuidad de las acciones que se demandan en TI, acá se contempla:
- Talento Humano: Vinculación del talento humano pertinente, adecuado y calificado.
- Infraestructura: Disponibilidad de recursos físicos (muebles e inmuebles) para garantiza funcionamiento del negocio.
- Funcionamiento: Recursos económicos para garantizar funcionamiento del negocio.
- Inversión: Enfoque de habilitación para mejorar significativas que permita incorporar nuevos elementos.

- Componentes de TI para gestión organizacional: estos componentes representan la*s* acciones táctico-operativas que se deben hacer para la gobernanza en TI para la EPA ESP.
  - Estrategia y Gobierno de TI.
  - Servicios Ciudadanos Digitales.
  - Gobierno Abierto y Transparente.
  - Infraestructura de TI.
  - Información y Sistemas de Información.
  - Fortalecimiento de Capacidades de TI.
  - Seguridad y Privacidad de la Información.
- Mejora y Continuidad del Negocio: Esta fase contempla las acciones de mejoramiento continuo que se identifique, se compone de:
  - Lista de chequeo ruta de madurez.
  - Informes de gestión.
  - Indicadores de madurez digital.
  - Resultados del FURAG.
- Estado Final (Resultados): Definir el nivel de madurez que se ha logrado en la EPA con las estrategias, tácticas y operaciones establecidas en la vigencia.
- Seguimiento y Control del Modelo de Madurez: Analiza constantemente las

mejoras que se requieren en la estructura y articulación del modelo.

A continuación, se presenta el Modelo Ruta de Madurez para la perspectiva de seguridad y privacidad de la información.

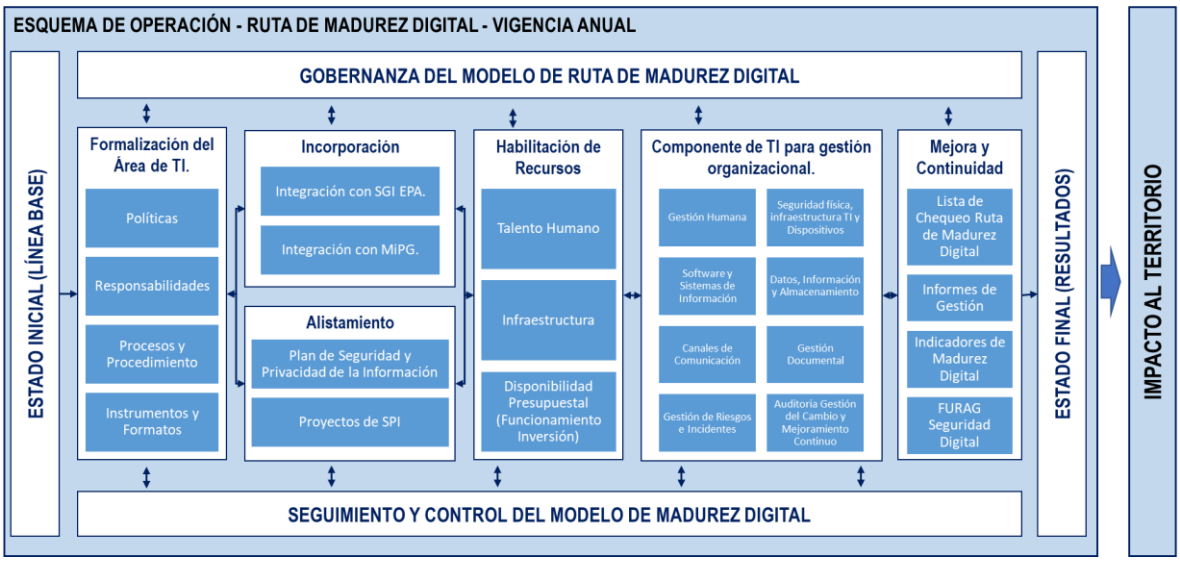


**Ilustración 3. Modelo Ruta de Madurez para la perspectiva de seguridad y privacidad de la información.**

## 9. Situación Actual

### Estado del Arte

Desde su creación en el 2016 la Dirección TIC ha trabajado para dar cumplimiento a los parámetros establecidos desde el Ministerio TIC con sus dos políticas Gobierno Digital y Seguridad Digital.

En esos temas Empresas Públicas de Armenia ha trabajado desde sus capacidades para apropiar las competencias y habilitades que se requieren para dar cumplimiento, así como en generar la vinculación pertinente con proveedores de TI para una implementación adecuada y pertinente.

Siendo consecuentes con ellos a continuación se reportan los proyectos asociados a Seguridad y Privacidad de la Información que se han trabajado:

**Tabla 4. Proyectos asociados a Seguridad y Privacidad de la Información**

| Gobierno Digital (Decreto 1008 de 2018) | | |
|---|---|---|
| Habilitadores Transversales | Año | Asignación presupuestal |
| SEGURIDAD Y PRIVACIDAD | 2016 | $ 16.322.250,00 |
| | 2017 | $ 153.772.486,00 |
| | 2018 | $ 79.654.421,00 |
| | 2019 | $ 77.892.060,00 |
| | 2020 | $ 30.892.400,00 |
| | 2021 | $ 214.279.927,00 |

Proyectos Vinculados acciones de Seguridad y Privacidad de la Información.

**Tabla 5. Proyectos Vinculados acciones de Seguridad y Privacidad de la Información.**

| **Habilitadores Transversales:** | | Seguridad y privacidad | |
|---|---|---|---|
| **Fecha de Ejecución** | **Tipo de Contrato** | **No Contrato** | **Objetivo Contractual** |
| 2016 | Clausulado simplificado | 161-2016 | Prestación de Servicios Profesionales Especializado de apoyo y acompañamiento a la Dirección TIC de Empresas Públicas de Armenia ESP en la gestión del Datacenter y los equipos servidores alojados en él. |
| 2017 | Clausulado simplificado | 006-2017 | Prestación de Servicios Profesionales Especializados de Apoyo y Acompañamiento a la Dirección TIC de Empresas Públicas de Armenia ESP. en la gestión del Datacenter y los Equipos Servidores Alojados en él. |
| 2017 | Clausulado simplificado | 183-2017 | Prestación de Servicios Profesionales Especializados de Apoyo y Acompañamiento a la Dirección TIC de Empresas Públicas de Armenia ESP. en la gestión del Datacenter y los Equipos Servidores Alojados en él. |
| 2017 | Clausulado Simplificado | 107-2017 | Compra venta de 200 licencias Antivirus, para los equipos de cómputo de las diferentes sedes de la EPA-ESP. |
| 2017 | Compraventa | 008-2017 | Adquisición de firewall activo-pasivo, con su respectiva licencia |
| 2017 | Clausulado simplificado | 186-2017 | Diseño e implementación del sistema de gestión de seguridad de la información para Empresas Públicas de Armenia ESP. |
| 2017 | Clausulado simplificado | 348-2017 | Endurecimiento de servicios, sistema operativo de servidor ORION e instalación de certificado de seguridad de FIREWALL SOPHOS para exposición de |

| **Habilitadores Transversales:** | | Seguridad y privacidad | |
|---|---|---|---|
| **Fecha de Ejecución** | **Tipo de Contrato** | **No Contrato** | **Objetivo Contractual** |
| | | | componente de trámites y servicios de Empresas Públicas de Armenia. |
| 2018 | Clausulado Simplificado | 207-2018 | Prestación de Servicios Profesionales Especializados de Apoyo y Acompañamiento a la Dirección TIC de Empresas Públicas de Armenia ESP. en la gestión del Datacenter y los Equipos Servidores Alojados en él. |
| 2018 | Clausulado Simplificado | 009-2018 | Prestación de servicios profesionales especializado de apoyo y acompañamiento a la dirección tic de Empresas Públicas De Armenia ESP en la gestión del datacenter y los equipos servidores alojados en él |
| 2018 | Prestación de Servicios | 012-2018 | Prestación de servicios profesionales especializados en la preparación del plan de trabajo, preparación de requisitos y generación de documentación para la implementación de la norma ISO 27000 en la dirección tic de empresas públicas de armenia esp. |
| 2019 | Clausulado simplificado | 009-2019 | Prestación de servicios profesionales especializado de apoyo y acompañamiento a la dirección tic de Empresas Públicas De Armenia ESP en la gestión del datacenter y los equipos servidores alojados en él. |
| 2019 | Clausulado simplificado | 196-2019 | Prestación de servicios profesionales especializados de apoyo y acompañamiento dirección tic de Empresas Públicas De Armenia ESP., en la gestión del datacenter y los equipos servidores alojados en él |
| 2019 | Clausulado simplificado | 032-2019 | Compra de 200 licencias antivirus para los equipos de cómputo de las diferentes sedes de la EPA-ESP. |
| 2019 | Clausulado Simplificado | 405-2019 | Prestación de servicios profesionales especializados de apoyo y acompañamiento dirección tic de Empresas Públicas De Armenia ESP., en la gestión del datacenter y los equipos servidores alojados en él |
| 2019 | Clausulado simplificado | 206-2019 | Compra de cámaras como apoyo para la seguridad de las sedes, Aseo, Abedules, Corbones y CAM de Empresas Públicas De Armenia ESP |
| 2020 | Clausulado Simplificado | 297-2020 | Adquisición de la licencia para el firewall de la entidad |
| 2021 | Compraventa | 151-2021 | Renovación de 300 licencias antivirus, para los equipos de cómputo de las diferentes sedes de la epa esp. |
| 2021 | Compraventa | 019-2021 | Compra e instalación de cámaras de seguridad y sistemas y sistema de control de acceso en diferentes áreas de empresas públicas de armenia esp. |
| 2021 | Clausulado Simplificado | 329-2021 | Renovación del Uso de la Licencia del FIREWALL PA-820 de Empresas Públicas de Armenia ESP |

**Diagnóstico de Seguridad y Privacidad de la Información, Política de Seguridad Digital.**

La realización de este diagnóstico contó con la capacitación por parte del Ministerio TIC enfocado a socializar la actualización de la hoja de ruta para el diagnóstico de Seguridad Digital, esta capacitación se realizó vía Microsoft Teams el día 10 de febrero de 2022.


**Ilustración 4. Modelo de Seguridad y Privacidad de la Información (MSPI)**

Posterior a la capacitación se nos compartió información sobre los nuevos instrumentos para trabajar.

1. Presentación MSPI.
2. Resolución 500 de 2021.
3. Anexo 1.
4. Instrumento evaluación MSPI.
5. Instrumento Inventario y Clasificación de Activos de Información.
6. Instrumento Identificación de riesgos.
7. Grabación socialización.

Con dicha información procedemos a hacer el proceso de recuperación de la información asociada a las etapas que propone el diagnóstico en cuestión. Actualmente nos encontramos en la etapa de identificación del nivel de madurez y análisis de la documentación recuperada. A continuación, mostramos el instrumento de trabajo usado para el diagnóstico.

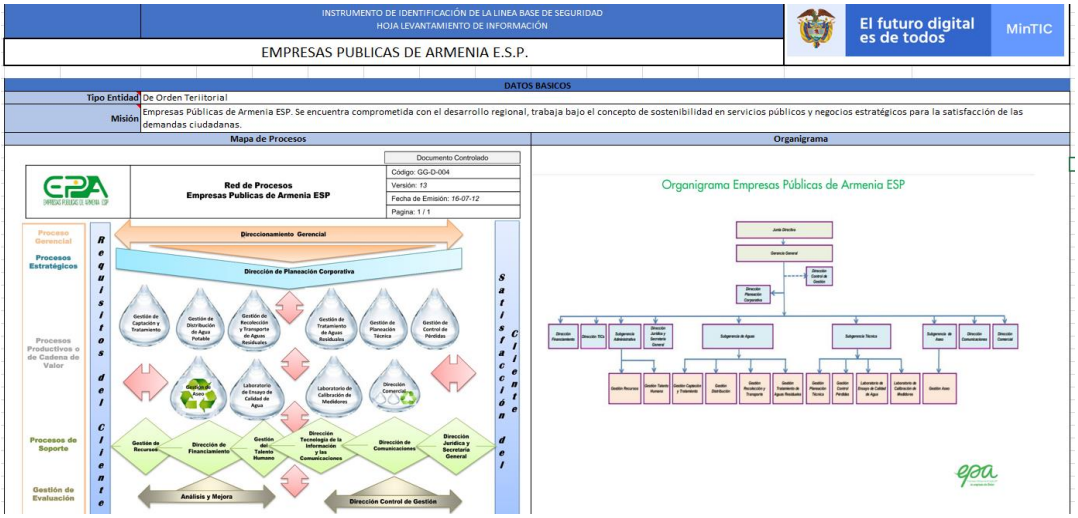


**Ilustración 5. El instrumento de trabajo usado para el diagnóstico.**

## *Valoración del nivel de madurez*

La siguiente tabla muestra los niveles de madurez del modelo de seguridad y privacidad definidos por el Ministerio TIC.

**Tabla 6. Nivel De Madurez Modelo Seguridad Y Privacidad De La Información**

| | **NIVEL DE CUMPLIMIENTO** |
|---|---|
| **Inicial** | INTERMEDIO |
| **Repetible** | CRÍTICO |
| **Definido** | CRÍTICO |
| **Administrado** | CRÍTICO |
| **Optimizado** | CRÍTICO |

## Resultado del Diagnóstico *Vigencia 2022*

*El resultado del diagnóstico deja a la Entidad en un puntaje medio-bajo sobre la implementación en Seguridad de la información.*

Bajo los lineamientos *Nivel De Madurez Modelo Seguridad Y Privacidad De La Información* se procede a entregar los resultados del autodiagnóstico los cuales se entregan a continuación en la tabla de Evaluación De Efectividad De Controles - ISO 27001:2013 Anexo A.

**Tabla 7. Evaluación Efectiva de Controles**

| No. | Evaluación de Efectividad de controles | | | |
|---|---|---|---|---|
| | **Dominio** | **Calificación Actual** | **Calificación objetivo** | **Evaluación de efectividad de control** |
| A.5 | Políticas de seguridad de la información | 0 | 100 | **INEXISTENTE** |
| A.6 | Organización de la seguridad de la información | 0 | 100 | **INEXISTENTE** |
| A.7 | Seguridad de los recursos humanos | 39 | 100 | **REPETIBLE** |
| A.8 | Gestión de activos | 29 | 100 | **REPETIBLE** |
| A.9 | Control de acceso | 20 | 100 | **INICIAL** |
| A.10 | Criptografía | 10 | 100 | **INICIAL** |
| A.11 | Seguridad física y del entorno | 32 | 100 | **REPETIBLE** |
| A.12 | Seguridad de las operaciones | 39 | 100 | **REPETIBLE** |
| A.13 | Seguridad de las comunicaciones | 43 | 100 | **EFECTIVO** |
| A.14 | Adquisición, desarrollo y mantenimiento de sistemas | 0 | 100 | **INEXISTENTE** |
| A.15 | Relaciones con los proveedores | 30 | 100 | **REPETIBLE** |
| A.16 | Gestión de incidentes de seguridad de la información | 9 | 100 | **INICIAL** |
| A.17 | Aspectos de seguridad de la información de la gestión de la continuidad del negocio | 60 | 100 | **EFECTIVO** |
| A.18 | Cumplimiento | 48,5 | 100 | **EFECTIVO** |
| **PROMEDIO EVALUACIÓN DE CONTROLES** | | **26** | **100** | **REPETIBLE** |

**Tabla 8. AVANCE PHVA**

| AVANCE PHVA | | |
|---|---|---|
| **COMPONENTE** | **% de Avance Actual Entidad** | **% Avance Esperado** |
| Planificación | 9% | 40% |
| Implementación | 8% | 20% |
| Evaluación de desempeño | 20% | 20% |
| Mejora continua | 20% | 20% |
| **TOTAL** | **57%** | **100%** |

Para conocer el detalle del instrumento por favor ver el documento **Autodiagnóstico Seguridad Digital Vigencia 2022**

**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.

## 10. Situación Deseada (Análisis Cómo Será)

Empresas Públicas de Armenia ESP desde el componente de Seguridad y Privacidad de la Información presente alcanzar los siguientes resultados en su operación.


**Ilustración 6. Resultados en su operación.**

Para lograr lo anteriormente descrito se formulan las siguientes iniciativas:

**Iniciativas para implementación del Modelo de Seguridad y Privacidad de la Información**

A continuación, se presenta el plan para fortalecer la implementación del modelo de seguridad y privacidad para Empresas Públicas de Armenia ESP:

**Tabla 9. Plan para fortalecer la implementación del modelo de seguridad y privacidad para Empresas Públicas de Armenia ESP:**

| PLAN TÁCTICO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023-2025 | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Seguridad Digital** | | | | **Acciones Clave** | | | | | **Metas de Cumplimiento** | **Indicadores de Cumplimiento** | | | | | |
| **Tópico** | **Componente de TI** | **Proyectos/ Iniciativas** | **Sub-Componentes** | **Actividades Clave** | **Evidencia** | **Periodicidad de seguimiento** | **Proceso Responsable** | **Estado de cumplimiento 2022** | **Nombre Meta** | **Nombre del indicador** | **Línea Base 2022** | **Meta 2023** | **Meta 2024** | **Meta 2025** | **Total, a 2025** |
| Arquitectura TI | Estrategia de TI | Gobernabilidad del Modelo de Seguridad y Privacidad de la Información para la continuidad de la EPA ESP. | Planeación de SPI | Revisar Política de Seguridad Digital vigente. | Reporte de actualización | Anual | Dirección TICs. | **100%** | Plan de Seguridad y Privacidad de la Información cumplido al 100% para diciembre de 2025 | Porcentaje de cumplimiento del Plan de Seguridad y Privacidad de la Información. | **43%** | **100 %** | **100 %** | **100 %** | **100 %** |
| | | | | Realizar actualización del Diagnóstico de Seguridad Digital. | Diagnóstico de Seguridad Digital | Anual | Dirección TICs. | **100%** | | | | | | | |
| | | | | Formular Plan de acción de Seguridad y Privacidad de la Información para cada vigencia | Plan de Acción de Seguridad y Privacidad de la Información | Anual | Dirección TICs. | ***100%*** | | | | | | | |

## PLAN TÁCTICO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023-2025

| Seguridad Digital | | | | Acciones Clave | | | | | Metas de Cumplimiento | Indicadores de Cumplimiento | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Tópico** | **Componente de TI** | **Proyectos/ Iniciativas** | **Sub-Componentes** | **Actividades Clave** | **Evidencia** | **Periodicidad de seguimiento** | **Proceso Responsable** | **Estado de cumplimiento 2022** | **Nombre Meta** | **Nombre del indicador** | **Línea Base 2022** | **Meta 2023** | **Meta 2024** | **Meta 2025** | **Total, a 2025** |
| | | | Indicadores de SPI | Formular los indicadores de Seguridad y Privacidad de la Información. | Ficha de Indicadores de SPI. | Anual | Dirección TICs. | **0%** | | | | | | | |
| | | | | Realizar seguimiento al desempeño de los indicadores. | Reporte de Seguimiento de Indicadores. | Anual | Dirección TICs. | **0%** | | | | | | | |
| | | | *Comité Institucional de Gestión y Desempeño CIGD* | Realizar comités de Seguridad Digital y Seguridad y Privacidad de la Información. | Presentación de Comité | Anual | Dirección TICs. | ***100%*** | | | | | | | |
| | | | | Realizar reportes sobre decisiones en Seguridad Digital y Privacidad de la Información. | Informes de Comité | Anual | Dirección TICs. | ***100%*** | | | | | | | |
| | Gobierno de TI | | Esquema de Gobierno de TI. | Realizar revisión y seguimiento a la Política de Seguridad y Privacidad de la Información. | Reporte del estado del Esquema de Gobierno de TI en Seguridad y | Anual | Dirección TICs. | **1** | Esquema de Gobierno de TI en SPI Actualizado. | Cantidad de actualizaciones del Esquema de Gobierno de TI en SPI | **0,50** | **1** | **1** | **1** | **1** |

| PLAN TÁCTICO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023-2025 | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Seguridad Digital** | | | | **Acciones Clave** | | | | | **Metas de Cumplimiento** | **Indicadores de Cumplimiento** | | | | | |
| **Tópico** | **Componente de TI** | **Proyectos/ Iniciativas** | **Sub-Componentes** | **Actividades Clave** | **Evidencia** | **Periodicidad de seguimiento** | **Proceso Responsable** | **Estado de cumplimiento 2022** | **Nombre Meta** | **Nombre del indicador** | **Línea Base 2022** | **Meta 2023** | **Meta 2024** | **Meta 2025** | **Total, a 2025** |
| | | | | Realizar seguimiento a los roles y responsabilidades de seguridad y privacidad de la información. | Privacidad de la Información. | *Anual* | Dirección TICs. | **0** | | | | | | | |
| | | | | Realizar revisión y seguimiento a los Procedimientos en Seguridad y Privacidad de la Información. | | Anual | Dirección TICs. | **0** | | | | | | | |
| | | | | Mantener actualizado el listado maestro de documentos de TI en el habilitador de Seguridad y Privacidad de la Información. | Listado Maestro de Documento de TI | Anual | Dirección TICs. | **1** | | | | | | | |
| | | | Seguimiento Requisitos Legales. | Formular la Matriz de verificación de Requisitos Legales de Seguridad de la Información. | Matriz de verificación de Requisitos Legales de | Anual | Dirección TICs. | **1** | Listado Maestro de Documentos Actualizados y en | Cantidad de actualizaciones del Listado Maestro de | **1** | **2** | **2** | **2** | **6** |

## PLAN TÁCTICO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023-2025

| Seguridad Digital | | | | Acciones Clave | | | | | Metas de Cumplimiento | Indicadores de Cumplimiento | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Tópico** | **Componente de TI** | **Proyectos/ Iniciativas** | **Sub-Componentes** | **Actividades Clave** | **Evidencia** | **Periodicidad de seguimiento** | **Proceso Responsable** | **Estado de cumplimiento 2022** | **Nombre Meta** | **Nombre del indicador** | **Línea Base 2022** | **Meta 2023** | **Meta 2024** | **Meta 2025** | **Total, a 2025** |
| | | | | Realizar seguimiento a la Matriz de verificación de Requisitos Legales de Seguridad de la Información. | Seguridad de la Información. | Anual | Dirección TICs. | **1** | Vigencia Normativa y Técnica. | Documentos de la Dirección TICs | | | | | |
| | Gestión de Proveedores de TI | Fortalecimiento de la gestión y seguimiento de los proveedores de TI en las acciones de continuidad y transformación digital. | Proveedores de TI. | Definir criterios de selección de proveedores. | Criterios de selección de Proveedores. | Anual | Dirección TICs. | **0%** | Modelo de Proveedores de TI habilitado y en operación al 100% | Porcentaje de habilitación del Modelo de Proveedores de TI en EPA ESP. | **33%** | **100 %** | **100 %** | **100 %** | **100 %** |
| | | | | Explorar y vincular proveedores de TI para cumplir las demandas y necesidades de la entidad. | Banco de Proveedores de TI | Anual | Dirección TICs. | **0%** | | | | | | | |
| | | | | Realizar contratación de los proveedores de TI para las diferentes asignaciones requeridas en la entidad. | - Banco de Proveedores seleccionados y vinculados con contratación.<br>- Contratos Celebrados. | A necesidad | Dirección TICs. | **100%** | | | | | | | |

## PLAN TÁCTICO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023-2025

| Seguridad Digital | | | | Acciones Clave | | | | | Metas de Cumplimiento | Indicadores de Cumplimiento | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Tópico** | **Componente de TI** | **Proyectos/ Iniciativas** | **Sub-Componentes** | **Actividades Clave** | **Evidencia** | **Periodicidad de seguimiento** | **Proceso Responsable** | **Estado de cumplimiento 2022** | **Nombre Meta** | **Nombre del indicador** | **Línea Base 2022** | **Meta 2023** | **Meta 2024** | **Meta 2025** | **Total, a 2025** |
| | | | | Realizar capacitación inicial y kick-off a los proveedores de TI contratados. | Acta de inicio y capacitación. | A necesidad | Dirección TICs. | **0%** | | | | | | | |
| | | | | Seguimiento y evaluación al desempeño de los proveedores con las responsabilidades asignadas. | Acta de seguimiento de proveedores de TI. | A necesidad | Dirección TICs. | **100%** | | | | | | | |
| | | | | Solicitar a los proveedores retroalimentación sobre el gobierno en las acciones de TI. | Instrumento de retroalimentación de proveedores de TI. | A necesidad | Dirección TICs. | **0%** | | | | | | | |
| *Seguridad y* | Gestión Humana | Sensibilización, Transferencia y Apropiación de competencias y buenos hábitos en Seguridad y Privacidad de la Información. | Gestión del Cambio y Cultura en Seguridad y Privacidad de la Información. | Formular Modelo de Transferencia de Capacidades de TI vinculando el componente de Seguridad y Privacidad de la Información. | Modelo de Transferencia de Capacidades de TI con componentes de Seguridad y Privacidad de la Información. | Anual | Dirección TICs. | **100%** | Personal de la EPA ESP capacitado y con apropiación de buenas prácticas en SPI. | Porcentaje de cobertura de áreas y procesos de EPA ESP capacitados. | **33%** | **18%** | **19%** | **30%** | **100 %** |

## PLAN TÁCTICO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023-2025

| Seguridad Digital | | | | Acciones Clave | | | | | Metas de Cumplimiento | Indicadores de Cumplimiento | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Tópico** | **Componente de TI** | **Proyectos/ Iniciativas** | **Sub-Componentes** | **Actividades Clave** | **Evidencia** | **Periodicidad de seguimiento** | **Proceso Responsable** | **Estado de cumplimiento 2022** | **Nombre Meta** | **Nombre del indicador** | **Línea Base 2022** | **Meta 2023** | **Meta 2024** | **Meta 2025** | **Total, a 2025** |
| | | | | Realizar acciones de transferencia de capacidades según la agenda de capacitación establecida. | Reporte de Transferencias de TI. | A necesidad | Dirección TICs. | **0%** | | | | | | | |
| | | | | Medir el desempeño y resultado del modelo de transferencia en el personal de la entidad. | Informe de medición. | A necesidad | Dirección TICs. | **0%** | | | | | | | |
| | Seguridad física, infraestructura TI y Dispositivos | Gestión de Activos y Recursos Tecnológicos. | Activos de Tecnologías de Información. | Consolidación y Agrupación de Activos de Tecnologías de Información y de las Comunicaciones. | Banco de Inventario de Activos y Recursos de Tecnologías de Información | Anual | Dirección TICs. | **0%** | Inventario de Activos de Tecnologías de Información consolidado y con capacidad de gestión. | Porcentaje de avance en la consolidación del Inventario de Activos de Tecnologías de Información consolidado y con capacidad de gestión. | **0%** | **30%** | **40%** | **30%** | **100 %** |
| | | | | Actualización de riesgos sobre activos de tecnologías de información y comunicaciones, desde el enfoque de Seguridad y Privacidad de la Información. | | Anual | Dirección TICs. | ***0%*** | | | | | | | |

## PLAN TÁCTICO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023-2025

| Seguridad Digital | | | | Acciones Clave | | | | | Metas de Cumplimiento | Indicadores de Cumplimiento | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Tópico | Componente de TI | Proyectos/ Iniciativas | Sub-Componentes | Actividades Clave | Evidencia | Periodicidad de seguimiento | Proceso Responsable | Estado de cumplimiento 2022 | Nombre Meta | Nombre del indicador | Línea Base 2022 | Meta 2023 | Meta 2024 | Meta 2025 | Total, a 2025 |
| | Software y Sistemas de Información | Gestión de Software y Sistemas de Información | Metodología de Software | Definir una metodología de software que permita determina los parámetros para la construcción de software a la medida. | Marco Metodológico de desarrollo de software. | Anual | Dirección TICs. | **0%** | Metodología de Desarrollo de Software definida y publicada. | Porcentaje de avance en el diseño de la metodología de software | **0%** | **0%** | **100 %** | **0%** | **100 %** |
| | | | | Definir los lineamientos mínimos de calidad para la compra de soluciones digitales (software y/o Sistemas de información) de terceros bajo esquemas de ITO. | | Anual | Dirección TICs. | **0%** | | | | | | | |
| | | | Despliegue y Operatividad de Software y Sistemas de Información | Establecer condiciones y lineamientos de integración entre los diferentes software y sistemas de información. | Condiciones y lineamientos de integración de software. | Anual | Dirección TICs. | **0%** | Arquitectura de Integración de los Software y Sistemas de Información definid y en operación. | Porcentaje de avance en la formulación de la Arquitectura de Integración de los Software y Sistemas de Información | **0%** | **67%** | **16%** | **17%** | **100 %** |
| | | | | Formular una ruta transicional para la articulación integral de los diferentes Sistemas | Ruta transicional para la articulación integral | Anual | Dirección TICs. | **0%** | | | | | | | |

| PLAN TÁCTICO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023-2025 | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Seguridad Digital** | | | | **Acciones Clave** | | | | | **Metas de Cumplimiento** | **Indicadores de Cumplimiento** | | | | | |
| **Tópico** | **Componente de TI** | **Proyectos/ Iniciativas** | **Sub-Componentes** | **Actividades Clave** | **Evidencia** | **Periodicidad de seguimiento** | **Proceso Responsable** | **Estado de cumplimiento 2022** | **Nombre Meta** | **Nombre del indicador** | **Línea Base 2022** | **Meta 2023** | **Meta 2024** | **Meta 2025** | **Total, a 2025** |
| | | | | de Información y/o Software. | | | | | | | | | | | |
| | | | | Ejecutar la ruta transicional para la articulación entre los diferentes sistemas de información y/o software implementados en la entidad. | | Anual | Dirección TICs. | **0%** | | | | | | | |
| | | | Mejoras de Software y Sistemas de Información | Seguimiento al desempeño y cumplimiento de las demandas de la entidad por los sistemas de información y el software en operación. | Bitácora de seguimiento al desempeño de software | A necesidad | Dirección TICs. | **0** | Banco de Necesidades de Transformación en operación | Cantidad de necesidades de transformación registradas en el banco. | **0** | **50** | **75** | **50** | **175** |

## PLAN TÁCTICO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023-2025

| Seguridad Digital | | | | Acciones Clave | | | | | Metas de Cumplimiento | Indicadores de Cumplimiento | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Tópico** | **Componente de TI** | **Proyectos/ Iniciativas** | **Sub-Componentes** | **Actividades Clave** | **Evidencia** | **Periodicidad de seguimiento** | **Proceso Responsable** | **Estado de cumplimiento 2022** | **Nombre Meta** | **Nombre del indicador** | **Línea Base 2022** | **Meta 2023** | **Meta 2024** | **Meta 2025** | **Total, a 2025** |
| | | | | Mantener comunicación activa y dinámica con los proveedores de TI que nos lleva a la implementación de mejoras sobre el desempeño esperado del software. | Acta de reunión | A necesidad | Dirección TICs. | ***0*** | | | | | | | |
| | Datos, Información y Almacenamiento | Gestión y Madurez de los activos de información de Empresas Públicas de Armenia ESP. | Activos de Información | Establecer lineamientos para el levantamiento de activos de información | Documentación Actualizada en SGI. | Anual | Dirección TICs. | **0%** | Activos de Información formalizados, clasificados y categorizados según sus niveles de confidencialidad. | Porcentaje de avance en la formalización, clasificación y categorización d los activos de información de la EPA ESP. | **6%** | **94%** | **0%** | **0%** | **100 %** |
| | | | | Mapeo de Activos de Información | Inventario de Activos de Información actualizado. | Anual | Todos los Procesos | **25%** | | | | | | | |
| | | | | Aprobación de categorías de Activos de Información | Memorando de aceptación. | Anual | Dirección Jurídica y Secretaria General | **0%** | | | | | | | |

## PLAN TÁCTICO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023-2025

| Seguridad Digital | | | | Acciones Clave | | | | | Metas de Cumplimiento | Indicadores de Cumplimiento | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Tópico** | **Componente de TI** | **Proyectos/ Iniciativas** | **Sub-Componentes** | **Actividades Clave** | **Evidencia** | **Periodicidad de seguimiento** | **Proceso Responsable** | **Estado de cumplimiento 2022** | **Nombre Meta** | **Nombre del indicador** | **Línea Base 2022** | **Meta 2023** | **Meta 2024** | **Meta 2025** | **Total, a 2025** |
| | | | | Publicación en Portal Web según Ley 1712 | Enlace de publicación | Anual | Dirección de Comunicaciones | **0%** | | | | | | | |
| | | | Gestión de Datos Personales | Recolectar bases de datos personales de acuerdos con los estándares normativos. | Memorando de solicitud enviado. | A necesidad | Proceso que aplique según trámites y servicios | **1** | Datos Personal con integridad y seguridad reportados en la SIC. | Cantidad de actualizaciones de Datos Personales en la SIC | **0** | **1** | **1** | **1** | **1** |
| | | | | Realizar revisión de las bases de datos. | Formatos y listados asistencia. | Semestral | Proceso que aplique según trámites y servicios | ***0*** | | | | | | | |
| | | | | Registro y actualización de bases de datos ante la SIC. | Certificado del registro de BD que expide la SIC | Anual | Dirección TICs. | **0** | | | | | | | |
| | Canales de Comunicación | Gestión y mantenibilidad de los canales digitales de la EPA ESP. | Portal WEB: www.epa.gov.co | Establecer parámetros y niveles mínimos de seguridad sobre la información y operaciones del portal Web. | Guía de parámetros de seguridad web. | Anual | Dirección TICs. | **0%** | Portal Web habilitado, accesible, fácil de usar y disponible para los usuarios y grupos de interés de la EPA ESP. | Porcentaje de cumplimiento de los parámetros de accesibilidad, usabilidad y | **25%** | **100 %** | **100 %** | **100 %** | **100 %** |

| PLAN TÁCTICO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023-2025 | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Seguridad Digital** | | | | **Acciones Clave** | | | | | **Metas de Cumplimiento** | **Indicadores de Cumplimiento** | | | | | |
| **Tópico** | **Componente de TI** | **Proyectos/ Iniciativas** | **Sub-Componentes** | **Actividades Clave** | **Evidencia** | **Periodicidad de seguimiento** | **Proceso Responsable** | **Estado de cumplimiento 2022** | **Nombre Meta** | **Nombre del indicador** | **Línea Base 2022** | **Meta 2023** | **Meta 2024** | **Meta 2025** | **Total, a 2025** |
| | | | | Revisar y establecer la necesidad de reformular los Términos de Uso y condiciones del Portal Web epa.gov.co según los lineamientos establecidos en la normatividad nacional y las políticas Gobierno Digital y Seguridad Digital. | Términos de Uso y Condiciones de Uso del Portal Web www.epa.gov.co | Anual | Dirección TICs. | **0%** | | transparencia según la Ley 1712 de 2014. | | | | | |
| | | | | Verificar la actualización y versión vigente en la Web la Política de Privacidad y Protección de Datos | Política de Privacidad y Protección de Datos vigente publicada. | A necesidad | Dirección de Comunicaciones | ***100%*** | | | | | | | |
| | | | | Realizar verificaciones y validación de los niveles de seguridad del código y protocolo de comunicación del portal web. | Reportes de verificaciones y validación de los niveles de seguridad. | Anual | Dirección TICs. | ***0%*** | | | | | | | |

**PLAN TÁCTICO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023-2025**

| Seguridad Digital | | | | Acciones Clave | | | | | Metas de Cumplimiento | Indicadores de Cumplimiento | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Tópico | Componente de TI | Proyectos/ Iniciativas | Sub-Componentes | Actividades Clave | Evidencia | Periodicidad de seguimiento | Proceso Responsable | Estado de cumplimiento 2022 | Nombre Meta | Nombre del indicador | Línea Base 2022 | Meta 2023 | Meta 2024 | Meta 2025 | Total, a 2025 |
| | | | Portal WEB: www.intraepa.gov.co | Establecer parámetros y niveles mínimos de seguridad sobre la información y operaciones del portal Web. | Guía de parámetros de seguridad web. | Anual | Dirección TICs. | **0%** | Portal IntraEPA habilitado con mejoras en SPI según Banco de Necesidades de Transformación definidas. | Porcentaje de implementación de mejoras en SPI al Portal IntraEPA | **0%** | **100 %** | **100 %** | **100 %** | **100 %** |
| | | | | Revisar y establecer la necesidad de reformular los Términos de Uso y condiciones del Portal Web epa.gov.co según los lineamientos establecidos en la normatividad nacional y las políticas Gobierno Digital y Seguridad Digital. | Términos de Uso y Condiciones de Uso del Portal Web www.intraepa.gov.co | Anual | Dirección TICs. | **0%** | | | | | | | |
| | | | | Realizar verificaciones y validación de los niveles de seguridad del código y protocolo de | Reportes de verificaciones y validación de los niveles de seguridad. | Anual | Dirección TICs. | ***0%*** | | | | | | | |

## PLAN TÁCTICO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023-2025

| Seguridad Digital | | | | Acciones Clave | | | | | Metas de Cumplimiento | Indicadores de Cumplimiento | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Tópico** | **Componente de TI** | **Proyectos/ Iniciativas** | **Sub-Componentes** | **Actividades Clave** | **Evidencia** | **Periodicidad de seguimiento** | **Proceso Responsable** | **Estado de cumplimiento 2022** | **Nombre Meta** | **Nombre del indicador** | **Línea Base 2022** | **Meta 2023** | **Meta 2024** | **Meta 2025** | **Total, a 2025** |
| | | | | comunicación del portal web. | | | | | | | | | | | |
| | | | | Realizar seguimiento a los tipos de usuarios, sus privilegios, y tiempo de privilegios. | Bitácora de Usuarios y privilegios de acceso. | A necesidad | Dirección TICs. | ***0%*** | | | | | | | |
| | Gestión de Riesgos e Incidentes | Continuidad Operativa del Negocio desde la gestión del riego y la recuperación eficiente ante desastres e incidentes de seguridad. | Gestión del Riesgo | Actualización de lineamientos de riesgos en SPI | Reporte de actualización | Anual | Dirección TICs. | **0%** | Riesgos de TI gestionados y bajo seguimiento rutinario. | Porcentaje de eventos de riesgos mitigados y en control. | **63%** | **100 %** | **100 %** | **100 %** | **100 %** |
| | | | | Socialización de lineamientos de Gestión de Riesgos de Seguridad y privacidad de la Información. | Registro de asistencia. | A necesidad | Dirección TICs. | **0%** | | | | | | | |
| | | | | Identificación de Riesgos de Seguridad y Privacidad de la Información | Mapa de Riesgos EPA actualizada. | Anual | Dirección TICs. | **100%** | | | | | | | |

## PLAN TÁCTICO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023-2025

| Seguridad Digital | | | | Acciones Clave | | | | | Metas de Cumplimiento | Indicadores de Cumplimiento | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Tópico | Componente de TI | Proyectos/ Iniciativas | Sub-Componentes | Actividades Clave | Evidencia | Periodicidad de seguimiento | Proceso Responsable | Estado de cumplimiento 2022 | Nombre Meta | Nombre del indicador | Línea Base 2022 | Meta 2023 | Meta 2024 | Meta 2025 | Total, a 2025 |
| | | | | Aprobación de Riesgos Identificados | Memorando de aprobación. | Anual | Dirección TICs. | **100%** | | | | | | | |
| | | | | Publicación mapas de riesgos de los proceso. | Mapa de Riesgos EPA publicado en SGI. | Anual | Dirección de Planeación Corporativa | **100%** | | | | | | | |
| | | | | Seguimiento a los riesgos en Seguridad y Privacidad de la Información | Seguimiento al mapa de riesgo. | Trimestral | Dirección TICs. | **100%** | | | | | | | |
| | | | | Acciones de mejoramiento a riesgos residuales. | | Anual | Dirección TICs. | ***100%*** | | | | | | | |
| | | | | Realizar medición, presentación y reporte de indicadores | Reporte de indicadores. | Trimestral | Dirección TICs. | ***0%*** | | | | | | | |
| | | | Vulnerabilidades | Establecer lineamientos para la ejecución de pruebas de vulnerabilidades. | Lineamientos de Ejecución de Pruebas de Vulnerabilidad. | Anual | Dirección TICs. | ***0*** | Reducción del nivel de vulnerabilidad identificadas en Software, Sistemas de | Cantidad de pruebas de vulnerabilidad realizadas | ***0*** | ***1*** | ***1*** | ***1*** | ***3*** |

## PLAN TÁCTICO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023-2025

| Seguridad Digital | | | | Acciones Clave | | | | | Metas de Cumplimiento | Indicadores de Cumplimiento | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Tópico** | **Componente de TI** | **Proyectos/ Iniciativas** | **Sub-Componentes** | **Actividades Clave** | **Evidencia** | **Periodicidad de seguimiento** | **Proceso Responsable** | **Estado de cumplimiento 2022** | **Nombre Meta** | **Nombre del indicador** | **Línea Base 2022** | **Meta 2023** | **Meta 2024** | **Meta 2025** | **Total, a 2025** |
| | | | | Vincular y seleccionar proveedores en la ejecución de pruebas de vulnerabilidades. | Banco de Proveedores seleccionados y vinculados con contratación. | A necesidad | Dirección TICs. | ***0*** | Información y Servicios Tecnológicos. | | | | | | |
| | | | | Realizar pruebas de vulnerabilidades según parámetros establecidos. | Reporte de Pruebas de Vulnerabilidades. | A necesidad | Dirección TICs. | **0** | | | | | | | |
| | | | | Ejecutar plan de contingencia sobre vulnerabilidades encontradas. | Seguimiento al Plan de Contingencia sobre vulnerabilidades. | A necesidad | Dirección TICs. | **0** | | | | | | | |
| | | | Gestión de Incidentes | Formular procedimiento de gestión de incidentes de seguridad de la información. | Procedimiento actualizado. | Anual | Dirección TICs. | **0%** | Incidentes de TI resueltos y bajo control. | Porcentaje de incidentes resueltos | **25%** | **100 %** | **100 %** | **100 %** | **100 %** |
| | | | | Realizar revisiones de seguridad de la información. | Bitácora de revisiones de incidentes. | Trimestral | Dirección TICs. | **100%** | | | | | | | |

## PLAN TÁCTICO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023-2025

| Seguridad Digital | | | | Acciones Clave | | | | | Metas de Cumplimiento | Indicadores de Cumplimiento | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Tópico** | **Componente de TI** | **Proyectos/ Iniciativas** | **Sub-Componentes** | **Actividades Clave** | **Evidencia** | **Periodicidad de seguimiento** | **Proceso Responsable** | **Estado de cumplimiento 2022** | **Nombre Meta** | **Nombre del indicador** | **Línea Base 2022** | **Meta 2023** | **Meta 2024** | **Meta 2025** | **Total, a 2025** |
| | | | | Realizar reporte de eventos en seguridad en la información | Reporte de eventos de seguridad. | Trimestral | Dirección TICs. | **0%** | | | | | | | |
| | | | | Realizar reporte de incidentes de seguridad en la información mitigados. | Reporte de incidentes de seguridad. | Trimestral | Dirección TICs. | **0%** | | | | | | | |
| | Auditoria Gestión del Cambio y Mejoramiento Continuo | Verificación y Control del desempeño del Modelo de Seguridad y Privacidad de la Información. | Auditorías Internas y Externas | Realizar auditorías internas para verificación del cumplimiento de seguridad y privacidad de la información. | Plan de Auditorías Internas. | Anual | Dirección Control de Gestión | **100%** | Niveles óptimos de cumplimiento de los lineamientos y planes en SPI. | Hallazgos de SPI inferiores al 20% sobre la cantidad de ítem auditados | **9** | **1,80** | **0,90** | **0,00** | **0%** |
| | | | | Participar en auditorías externas en seguridad digital según los establezcan las entidades de Inspección, Vigilancia y Control. | Plan de Auditorías Externas. | Anual | Dirección Control de Gestión | **100%** | | | | | | | |

## PLAN TÁCTICO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023-2025

| Seguridad Digital | | | | Acciones Clave | | | | | Metas de Cumplimiento | Indicadores de Cumplimiento | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Tópico | Componente de TI | Proyectos/ Iniciativas | Sub-Componentes | Actividades Clave | Evidencia | Periodicidad de seguimiento | Proceso Responsable | Estado de cumplimiento 2022 | Nombre Meta | Nombre del indicador | Línea Base 2022 | Meta 2023 | Meta 2024 | Meta 2025 | Total, a 2025 |
| | | | Continuidad del Negocio | Realizar reporte del Impacto de las acciones en Seguridad y Privacidad de la Información. | Reporte de acciones en Seguridad y Privacidad de la Información. | Anual | Dirección TICs. | **0** | Parámetros de continuidad del negocio aprobados. | Plan de Continuidad de Negocio Aprobado | **0** | **1** | **1** | **1** | **3** |
| | | | | Realizar valoración de riesgos de interrupción | Documento Valoración de Riesgos de interrupción para el plan de continuidad. | Anual | Dirección TICs. | ***0*** | | | | | | | |
| | | | | Formular estrategias de continuidad pertinentes. | Documento Estrategias de Continuidad | Anual | Dirección TICs. | ***0*** | | | | | | | |
| | | | | Formular el plan de continuidad de la operación. | Documentación del Plan de continuidad de la Operación | Anual | Dirección TICs. | **0** | | | | | | | |
| | | | Oportunidades de Mejora | Realizar reporte de estado de acciones correctivas identificadas | Informe del estado actual de Acciones Correctivas y | Anual | Dirección Control de Gestión | **100%** | Acciones Correctivas con ruta de resolución definidas. | Acciones correctivas de SPI inferiores al 20% sobre la | **12** | **2,40** | **1,20** | **0,00** | **0%** |

| PLAN TÁCTICO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023-2025 | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Seguridad Digital** | | | | **Acciones Clave** | | | | | **Metas de Cumplimiento** | **Indicadores de Cumplimiento** | | | | | |
| **Tópico** | **Componente de TI** | **Proyectos/ Iniciativas** | **Sub-Componentes** | **Actividades Clave** | **Evidencia** | **Periodicidad de seguimiento** | **Proceso Responsable** | **Estado de cumplimiento 2022** | **Nombre Meta** | **Nombre del indicador** | **Línea Base 2022** | **Meta 2023** | **Meta 2024** | **Meta 2025** | **Total, a 2025** |
| | | | | y oportunidades de mejora. | Oportunidades de Mejora. | | | | | cantidad de ítems auditados. | | | | | |
| | | | | Realizar seguimiento al estado de las acciones de mejora. | Reporte de reunión. | Anual | Dirección Control de Gestión | **100%** | | | | | | | |

Cronograma de Intervención
A continuación, se describen los tiempos de operación de cada actividad para las vigencias anuales del tiempo del presente plan:

**Tabla 10. Cronograma de Intervención del Presente Plan**

| Seguridad Digital | | | | Cronograma Vigencia 2022-2025 | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Tópico** | **Componente de TI** | **Proyectos/ Iniciativas** | **Sub-Componentes** | **ENE** | **FEB** | **MAR** | **ABR** | **MAY** | **JUN** | **JUL** | **AGO.** | **SEP** | **OCT** | **NOV** | **DIC** |
| Arquitectura TI | Estrategia de TI | Gobernabilidad del Modelo de Seguridad y Privacidad de la Información para la continuidad de la EPA ESP. | Planeación de SPI | | | | | | | | | | | | |
| | | | Indicadores de SPI | | | | | | | | | | | | |
| | | | Comités MiPG. | | | | | | | | | | | | |
| | Gobierno de TI | | Esquema de Gobierno de TI. | | | | | | | | | | | | |
| | | | Seguimiento Requisitos Legales. | | | | | | | | | | | | |
| | Gestión de Proveedores de TI | Fortalecimiento de la gestión y seguimiento de los proveedores de TI en las acciones de continuidad y transformación digital. | Proveedores de TI. | | | | | | | | | | | | |
| Seguridad y Privacidad de la Información | Gestión Humana | Sensibilización, Transferencia y Apropiación de competencias y buenos hábitos en Seguridad y | Gestión del Cambio y Cultura en Seguridad y Privacidad de la Información. | | | | | | | | | | | | |

| **Seguridad Digital** | | | | **Cronograma Vigencia 2022-2025** | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Tópico** | **Componente de TI** | **Proyectos/ Iniciativas** | **Sub-Componentes** | **ENE** | **FEB** | **MAR** | **ABR** | **MAY** | **JUN** | **JUL** | **AGO.** | **SEP** | **OCT** | **NOV** | **DIC** |
| | | Privacidad de la Información. | | | | | | | | | | | | | |
| | Seguridad física, infraestructura TI y Dispositivos | Gestión de Activos y Recursos Tecnológicos. | Activos de Tecnologías de Información. | | | | | | | | | | | | |
| | Software y Sistemas de Información | Gestión de Software y Sistemas de Información | Metodología de Software | | | | | | | | | | | | |
| | | | Despliegue y Operatividad de Software y Sistemas de Información | | | | | | | | | | | | |
| | | | Mejoras de Software y Sistemas de Información | | | | | | | | | | | | |
| | Datos, Información y Almacenamiento | Gestión y Madurez de los activos de información de Empresas Públicas de Armenia ESP. | Activos de Información | | | | | | | | | | | | |
| | | | Gestión de Datos Personales | | | | | | | | | | | | |
| | Canales de Comunicación | Gestión y mantenibilidad de los | Portal WEB: www.epa.gov.co | | | | | | | | | | | | |

| **Seguridad Digital** | | | | **Cronograma Vigencia 2022-2025** | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Tópico** | **Componente de TI** | **Proyectos/ Iniciativas** | **Sub-Componentes** | **ENE** | **FEB** | **MAR** | **ABR** | **MAY** | **JUN** | **JUL** | **AGO.** | **SEP** | **OCT** | **NOV** | **DIC** |
| | | canales digitales de la EPA ESP. | Portal WEB: www.intraepa.gov.co | | | | | | | | | | | | |
| | | | Redes Sociales | | | | | | | | | | | | |
| | Gestión de Riesgos e Incidentes | Continuidad Operativa del Negocio desde la gestión de los riegos y la recuperación eficiente ante desastres e incidentes de seguridad. | Gestión del Riesgo | | | | | | | | | | | | |
| | | | Vulnerabilidades | | | | | | | | | | | | |
| | | | Gestión de Incidentes | | | | | | | | | | | | |
| | Auditoria Gestión del Cambio y Mejoramiento Continuo | Verificación y Control del desempeño del Modelo de Seguridad y Privacidad de la Información. | Auditorías Internas y Externas | | | | | | | | | | | | |
| | | | Continuidad del Negocio | | | | | | | | | | | | |
| | | | Oportunidades de Mejora | | | | | | | | | | | | |

## 11. Parámetros de estrategias de EIC (Educación, Información y Comunicación)

Empresas Públicas de Armenia ESP establece:

- Para estrategias de EIC a los grupos de interés e involucrados externos esto estará bajo la responsabilidad de Dirección de Comunicaciones, quien deberá formular estrategias y tácticas que permitan la socialización de los enfoques y lineamientos para resguardar la seguridad y privacidad de la información a los activos de información de Empresas Públicas de Armenia ESP.
- Para fines específicos de Educación la Gestión de Talento Humano con el apoyo de Dirección TIC, diseñará planes de capacitación y entrenamiento para los funcionarios y contratistas de la Empresas Públicas de Armenia ESP según las necesidades de formación para cumplir con los lineamientos nacionales establecidos en la Política de Gobierno Digital y Política de Seguridad Digital de Empresas Públicas de Armenia ESP de Tecnologías de la Información y las Comunicaciones.
- Ambas asignaciones contarán con la participación y acompañamiento de la Dirección TICs para lograr asertividad y pertenencia en la información divulgada.

## 12. Glosario

- **Accesibilidad:** Garantía de acceso al usuario que lo requiera.
- **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.
- **Actualidad:** Vigencia de la información.
- **Acuerdos de servicio:** se deben generar reglas para la prestación de los servicios para las diferentes tareas que surjan en las diferentes etapas para definir los tiempos de respuesta entre las dos partes.
- **Administración de incidentes de seguridad:** Procedimientos, estrategias y herramientas de control, enfocados a una correcta evaluación de las amenazas existentes, en este caso hacia toda la infraestructura de TI, se basa en un análisis continuo y mejorado del desempeño de todos los activos y recursos gerenciales que tiene la entidad. Su objetivo principal es atender y orientar las acciones inmediatas para solucionar cualquier situación que cause una interrupción de los diferentes servicios que presta la entidad, de manera rápida y eficaz. No se limita a la solución de problemas específicos sino a buscar las causas que determinaron el incidente limitando el marco de acción de futuras ocurrencias, su enfoque se base en tres pilares fundamentales: o Detectar cualquier alteración en los servicios TI. o Registrar y clasificar estas alteraciones. o Asignar el personal encargado de restaurar el servicio.
- **Administrador:** Toda persona responsable por la operación día a día de un sistema de cómputo o red de cómputo.
- **Alcance:** Ámbito de la organización que queda sometido al Sistema de Gestión de Seguridad de la Información - SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la organización.
- **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 riesgos**: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- **Aplicación:** Una aplicación es cualquier programa, o grupo de programas, que está diseñado para el usuario final. El software de aplicaciones (también llamado programas de usuario final) incluye elementos como programas de bases de datos, procesadores de texto, navegadores web y hojas de cálculo.
- **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.
- **Auditoria:** Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del Sistema de Gestión de Seguridad de la Información - SGSI de una organización.
- **Autenticación:** Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.
- **Autenticidad:** Proceso mediante el cual se tiene un alto grado de certeza de la correcta identificación de personas, equipos, interfaces, datos y procesos.
- **Automatización:** Ejecución automática de ciertas tareas con el fin de agilizar el desarrollo de los procesos.
- **Autorización:** Proceso de dar privilegios a los usuarios.
- **Buzón:** espacio de almacenamiento de información reservado en un servidor de correo electrónico con fines de almacenar correos, contactos, calendario, entre otros**.**
- **Calidad:** se deben definir requisitos con los que se pueda evaluar la calidad, tales como reconocimiento de marca y tiempo en el mercado.
- **Canal de comunicación:** medio utilizado para la transmisión de información, por ejemplo: el cableado, fibra óptica y la atmósfera.
- **Características de la Información:** las principales características desde enfoque de seguridad de información son: confidencialidad, disponibilidad e integridad.
- **Centro de cómputo:** espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización

llamado también data center por su término anglosajón.

- **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.
- **Compatibilidad:** el sistema a adquirir debe ser compatible con la tecnología e infraestructura que tiene la entidad.
- **Comprensibilidad:** Entendimiento e interpretación adecuada de la información por parte de un usuario.
- **Compromiso de la Dirección:** Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI - **Sistema de Gestión de la Seguridad de la Información**.
- **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
- **Conjunto de Datos:** la serie de datos estructurados, vinculados entre sí y agrupados dentro de una misma unidad temática y física, de forma que puedan ser procesados apropiadamente para obtener información.
- **Consistencia:** Datos coherentes y libres de contradicción.
- **Contención:** Evitar que el incidente siga ocasionando daños.
- **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 Social:** Es el derecho y el deber de los ciudadanos a participar de manera individual o a través de sus organizaciones, redes sociales e instituciones, en la vigilancia de la gestión pública y sus resultados.
- **Control**: Toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas y que pueden ser de carácter administrativo, técnico o legal. En la entidad se aplica por medio de la declaración de aplicabilidad.
- **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.
- **Correo electrónico:** servicio de red que permite a los usuarios enviar y recibir mensajes (también denominados mensajes electrónicos o cartas digitales) mediante redes de comunicación electrónica.
- **Credibilidad:** Información veraz y confiable para los usuarios.
- **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.
- **Custodio de activo de información:** individuo, cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de cumplir y velar por el cumplimiento de los controles que el responsable del activo de información haya definido, con base en los controles de seguridad disponibles en la entidad.
- **Custodio:** Ente, área, proceso o persona encargada de preservar y

resguardar la información entregada y que generalmente son de propiedad de otro proceso o área.

- **DAFP:** Departamento Administrativo de la Función Pública
- **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.
- **Derechos de autor:** Entendida en este contexto como Propiedad Industrial, hace referencia a la protección de los intereses de los creadores al ofrecerles ventajas en relación con sus creaciones. La entidad nacional delegada para la administración de la Propiedad Industrial en Colombia es la Superintendencia de Industria y Comercio a través de la Delegatura para la Propiedad Industrial. Esta entidad cuenta con la Oficina de Servicio al Consumidor y Apoyo Empresarial, OSCAE, quien administra y coordina las actividades de divulgación y formación en temas de Propiedad Industrial. La Oficina tiene entre sus funciones diseñar y promover los mecanismos y herramientas para la divulgación, promoción y fomento de las funciones, trámites y servicios institucionales.
- **Día Cero:** Vulnerabilidad de software que el fabricante desconoce y para la que, por lo tanto, no existen parches o actualizaciones de seguridad. Si los cibercriminales descubren un Día Cero, ejecutan un exploit para atacar los sistemas afectados.
- **Dirección IP:** Cada nodo en una red TCP/IP requiere de una dirección numérica que identifica una red y un anfitrión local o nodo de la red, esta dirección se compone de cuatro números separados por puntos, por ejemplo, 10.2.1.250
- **Directiva o directriz:** Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.
- **Directiva:** Según [ISO IEC 13335-1: 2004): una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.
- **Eficiencia:** Capacidad para realizar análisis y descargas de los datos con unos niveles de desempeño y tiempos esperados.
- **Encriptación**: Proceso que permite volver ilegible la información que se considera importante. Una vez la información esta encriptada solo puede accederse aplicando una clave.
- **Equipo de cómputo**: Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o

bien compilando y correlacionando otros tipos de información.

- **Erradicación:** Eliminar la causa del incidente y todo rastro de los daños.
- **Escalamiento:** El primer nivel de resolución es la mesa de servicios, cuando no sea capaz de resolver en primera instancia, debe recurrir a especialistas o algún superior que tome las decisiones que se escapen de su responsabilidad, es decir escalonar el servicio. Existe un tercer nivel de escalonamiento a expertos para temas muy especializados
- **Especialista:** Usuario a quien se le designan los casos de acuerdo con la clasificación estipulada en el árbol de incidentes o de petición de servicio.
- **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.
- **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.
- **Exactitud:** Datos diligenciados correctamente.
- **Excepciones (Seguridad de información):** Casos especiales que no cumplen una política, procedimiento o regla.
- **Formato Libre:** Formato de archivo que se puede crear y manipular mediante cualquier software libre, sin restricciones legales
- **Formato propietario:** Son formatos de archivo que requieren herramientas que no son públicas
- **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:** (inglés: Information security incident management). Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información
- **Gestión de Incidentes:** Es el conjunto de todas las acciones, medidas, mecanismos, recomendaciones, tanto proactivos, como reactivos, tendientes a evitar y eventualmente responder de manera eficaz y eficiente a incidentes de seguridad que afecten activos de una Entidad. Minimizando su impacto en el negocio y la probabilidad que se repita.

- **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.
- **Gestión documental:** Son las actividades administrativas y técnicas que propenden por la planificación, manejo y organización de la información producida y recibida por las entidades desde que se produce o recibe hasta su disposición final.
- **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"
- **Impacto:** el costo para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.
- **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.
- **Información:** Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen. Constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras, es decir puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.
- **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.

- **Infraestructura:** Es el conjunto de recursos tecnológicos, hardware y software que permite la optimización de los procesos que soportan los servicios ofrecidos a nuestros clientes.
- **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)
- **ISO 27001:** ISO 27001 es una norma emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.
- **LAN:** Local área network o red de área local, es la interconexión de una o varias computadoras y periféricos.
- **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.
- **Lineamiento:** Es una directriz o norma obligatoria para efecto de esta política que debe ser implementada por la entidad para el desarrollo de la política de Datos Abiertos. Los lineamientos pueden ser a través de estándares, guías, recomendaciones o buenas prácticas.
- **Llamadas De Servicio:** Requerimiento que no interrumpe o disminuye la calidad del servicio, como: solicitud de préstamo, asignación y traslado de equipos de cómputo o video, configuración de telefonía, entre otros.
- **Mantenimiento, actualizaciones y soporte:** se deben definir los tiempos o momentos para aplicar el mantenimiento, definir de qué manera se realizarán las actualizaciones, cada cuánto y cómo se realizarán. Además, se debe identificar el alcance del soporte que se realice.
- **Medios de almacenamiento extraíbles:** Medios para guardar y portar

información de forma electrónica tales como disquetes, CD's, DVD's, discos ZIP, discos ópticos, discos duros externos, memoria digital USB, etc.

- **Mesa de Ayuda de Tecnología:** es el único Centro de Atención al Usuario en donde la DIRECCIÓN TICS presta servicios con la posibilidad de gestionar la atención de requerimientos relacionados con los servicios TICs.
- **Metadato:** Los metadatos son "datos sobre datos" - es decir, los datos que describen los aspectos básicos de un conjunto de datos, por ejemplo, cuando se creó el conjunto de datos, cuál es la agencia responsable de la base de datos, el formato de los datos, etc.
- **MIPG:** Modelo Integrado de Planeación y Gestión.
- **MSPI:** Es el Modelo de Seguridad y Privacidad de la Información definido por el Ministerio de Tecnologías de la Información – MINTIC.
- **Navegar por la red**: Es la acción de visitar páginas en la World Wide Web por medio de una aplicación llamada explorador y que contiene documentos de hipertexto interconectados y accesibles vía Internet.
- **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.
- **Participación Ciudadana:** Es la intervención de los ciudadanos en los asuntos de carácter público que le son de su interés o en donde pueden decidir. El propósito de la Participación Ciudadana es permitir que las entidades públicas garanticen la incidencia efectiva de los ciudadanos y sus organizaciones en los procesos de planeación, ejecución, evaluación - incluyendo la rendición de cuentas- de su gestión, a través de diversos espacios, mecanismos, canales y prácticas de participación.
- **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]

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

- **Requerimiento:** Son solicitudes estándar asociadas a los servicios de TI para las cuales existe una aprobación predefinida y un impacto controlado. Dentro de los objetivos específicos en su atención se encuentran: • Aconsejar a los usuarios sobre el uso adecuado de los servicios de tecnología dispuestos para su utilización. • Proveer información a los usuarios sobre la disponibilidad de los servicios y los procedimientos requeridos para obtenerlos. • Otorgar y entregar los componentes de las peticiones de servicio estándar.
- **Responsable de activo de información:** identifica a un individuo, un cargo, proceso o grupo de trabajo designado encargado de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados, quien puede designar custodios del activo de información y autorizar a los usuarios para el acceso al activo de información.
- **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 consideraciones. (ISO Guía 73:2002).
- **Riesgo:** Probabilidad o posibilidad de que una amenaza aprovechando la vulnerabilidad o vulnerabilidades de un sistema, equipo o cualquier otro tipo de activo, se concrete, causando daños, perjuicios o pérdidas a la organización propietaria del mismo.
- **Seguridad de la información:** Según [ISO IEC 27002:2005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.
- **Seguridad:** Medida tomada para reducir el riesgo
- **Sistema De Gestión De Seguridad De La Información - SGSI:** Parte del sistema de gestión general de una organización, basada en un enfoque hacia los riesgos globales del negocio, cuyos fines son establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.
- **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:** Propiedad que garantiza que las acciones de una entidad se pueden rastrear únicamente hasta dicha entidad.
- **Unidad de Conservación:** Medio utilizado para archivar la documentación.
- **Unidades de almacenamiento:** Dispositivos que se usan para guardar y localizar la información de forma ordenada para acceder a ella cuando se necesario. Pueden ser internos como el disco duro o externos como memorias USB, unidades de CD, unidades de DVD, unidades de Blu-ray (BD), tarjetas de memoria SD.
- **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.

## 13. 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

## 14. 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.