Política Interna para la Gestión de Incidentes

Empresas Públicas de Armenia ESP.

DIRECCIÓN TIC

Presentado por Ingeniero:

Cesar Iván López Bedoya
Director TIC

ARMENIA QUINDÍO.
27 de julio de 2022

Control de Cambios

Versión	Fecha	Descripción del Cambio	Realizado por	Proceso
0,1	22/07/2022	Descripción inicial del documento de Política Interna Gestión de Incidentes de la Información de Empresas Públicas de Armenia.	Moisés J. Rentería C.	Dirección TICs
0,2	29/07/2022	Descripción de los componentes iniciales de la política- Parte 1	Moisés J. Rentería C.	Dirección TICs
0,3	06/07/2022	Descripción de los componentes iniciales de la política – Parte 2	Moisés J. Rentería C.	Dirección TICs
0,4	13/07/2022	Descripción de los lineamientos de la política	Moisés J. Rentería C.	Dirección TICs
0,5	19/07/2022	Descripción de los capítulos 7, 8 y 9 de la política	Moisés J. Rentería C.	Dirección TICs
0,6	25/07/2022	Revisión del documento de Política Interna Gestión de Incidentes de la Información de Empresas Públicas de Armenia	Ana Maria Arcila	Dirección TICs
0,7	25/07/2022	Actualización del documento de Política Interna Gestión de Incidentes de la Información de Empresas Públicas de Armenia	Ana Maria Arcila Moisés J. Rentería C.	Dirección TICs

Tabla de contenido

1. Introducción

La Dirección TIC de Empresas Públicas de Armenia ESP, para cumplir con la normativa nacional de estímulo hacia la gestión de incidentes en aspectos de seguridad y privacidad de la información ha formulado la presente política interna de gestión de incidentes que tiene el fin de establecer los parámetros de comportamiento sobre la forma de gestionar los incidentes que se presenten en la entidad.

Esta política esta formulada tomando como base los siguientes documentos:

- La Guía 21 - Gestión de Incidentes del Modelo de Seguridad de la Información emitidos por Gobierno en línea programa del Ministerio de Tecnologías de la Información y las Comunicaciones.
- El punto A- 16 A16 GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN de la Norma ISO 27002:2013

Bajo este contexto de trabajo este documento describe:

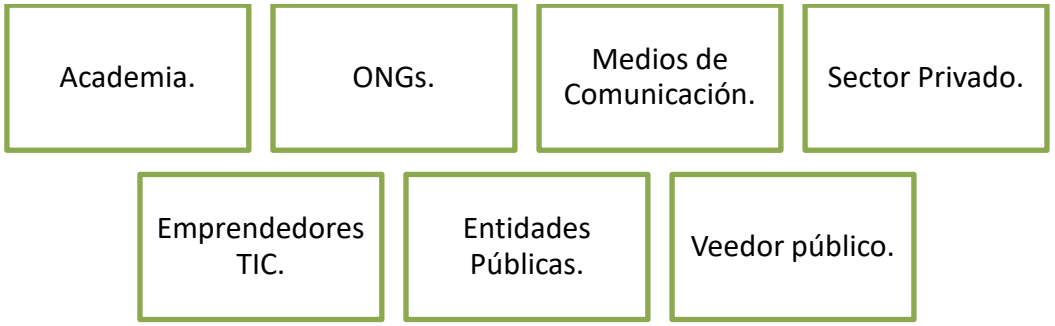
- Estructura orgánica para la toma de decisiones.
- Buenas prácticas para la gestión de incidentes.
- Lineamientos en el manejo y gestión de la política de gestión de eventos que se presenten en tecnologías de la información.
- Lineamientos para la gestión los incidentes de seguridad de la información.

El disponer de una política interna de gestión de incidentes nos permite tener un conducto regular sobre la forma en que la entidad puede actuar y comportarse sobre incidentes de TI que se presenten en la entidad que puedan poner en riesgos la integralidad de la información que la entidad maneje para la toma de decisiones.

2. Alcance

Este documento establece un alcance que contempla la descripción de lineamientos y conducto regular interno referente a la gestión de incidentes que se presenten en Empresas Públicas de Armenia y los actores externos que requieran interactuar con la entidad.

La política interna aplica a todos los funcionarios, contratistas, practicantes y terceros que tengan algún vínculo con Empresa Publicas de Armenia ESP, así como diferentes entes del ecosistema de negocio como:



3. Glosario

- Accesibilidad: Garantía de acceso al usuario que lo requiera.
- Activos de Información: Elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo.
- 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.
- Acuerdo De Confidencialidad: Contrato suscrito entre las partes con el fin de compartir material confidencial o conocimiento para ciertos propósitos, pero restringiendo su uso público.
- Acuerdos De Niveles De Servicio-Ans: Documento que recoge en un lenguaje no técnico, todos los detalles de los servicios ofrecidos.
- Amenaza: Factor externo que aprovecha una debilidad en los activos de información y puede impactar en forma negativa en la organización. No existe una única clasificación de las amenazas, lo importante es considerarlas todas a la hora de su identificación.
- 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.
- Aplicativo De Gestión De Recursos Tecnológicos: Herramienta de gestión que permite registrar, administrar controlar y evaluar todas las

solicitudes y servicios de Tics atendidos por la Dirección de Tecnologías e Información.

- 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.
- Autenticidad: Aseguramiento de la identidad respecto al origen cierto de los datos o información que circula por la Red.
- Cadena de Custodia: Registro detallado del tratamiento de la evidencia, incluyendo quienes, cómo y cuándo la transportaron, almacenaron y analizaron, a fin de evitar alteraciones o modificaciones que comprometan la misma.
- Catálogo De Servicios De Ti: Es un documento no técnico que contiene la descripción de los servicios de TI ofrecidos para ser utilizado como guía para orientar y dirigir a los usuarios, incluye los niveles de servicio, recoge las condiciones de prestación de servicios, así como las responsabilidades asociadas a cada uno de estos.
- Comprensibilidad: Entendimiento e interpretación adecuada de la información por parte de un usuario.
- Confidencialidad: Acceso a los datos única y exclusivamente por personas u organizaciones autorizadas, con la intención para proteger adecuadamente la información reservada y clasificada.
- Conformidad: Cumplimiento de lineamientos y estándares vigentes
- Contención: Evitar que el incidente siga ocasionando daños.
- Control: Medida que permite garantizar la reducción del nivel de un riesgo específico o mantenerlo dentro de límites aceptables.
- Copia De Seguridad (Backup): En tecnologías de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio de recuperación en caso de su pérdida.
- CSIRT (en inglés Computer Security Incident Response Team): Equipo de Respuesta a Incidentes de Seguridad Informática.
- Disponibilidad: Garantía hacia los usuarios autorizados para tener acceso a la información en el lugar, momento y forma que sea requerida.
- Entidad: Institución u organización con la capacidad y/o facultad de definir inventarios de y conjuntos de datos e información a publicar.
- 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 a 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.

- Evento de seguridad: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad. [ISO/IEC 27000:2009]
- Firewall: Dispositivo tecnológico que tiene como función proteger la red interna de una compañía, de accesos no autorizados del interior y del exterior vía Internet.
- 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.
- 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"
- Grupo de Interés: Es un conjunto de personas, organizadas en torno a un tema de interés común, con el fin de actuar conjuntamente en el desarrollo del mismo.
- GSIT: Gestión de Servicios de Infraestructura Tecnológica.
- Hash: Función computable mediante un algoritmo, que tiene como entrada un conjunto de elementos, que suelen ser cadenas, y los convierte (mapea) en un rango de salida finito, normalmente cadenas de longitud fija.
- IDS: Software de detección de intrusos
- Impacto: Daño producido a la organización por la materialización de un riesgo sobre los activos tecnológicos, visto como diferencia en las estimaciones de los estados de seguridad obtenidas antes y después del evento.
- Incidente Mayor: Es la categoría de impacto más alta de un incidente. Un incidente mayor produce una severa interrupción del negocio.
- Incidente: Cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar una interrupción a un servicio, o una reducción de la calidad de ese servicio. Dentro de los objetivos específicos en su atención se encuentran: • Asegurar que los procedimientos y métodos estandarizados sean usados para una eficiente y pronta respuesta, análisis, documentación, gestión continua y reporte de incidentes. • Incrementar la visibilidad y comunicación de los incidentes para la organización y el grupo de soporte TI. • Alinear las actividades de gestión de incidentes y prioridades con las de la organización. • Mantener la satisfacción del usuario con la calidad de los servicios de la Dirección de Tecnologías e Información.

- Información: Es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. Indicación o evento llevado al conocimiento de una persona o de un grupo. Es posible crearla, mantenerla, conservarla y transmitirla.
- Infraestructura Tecnológica: Es el conjunto de elementos de hardware (servidores, puestos de trabajo, redes, enlaces de telecomunicaciones, etcétera), software (sistemas operativos, bases de datos, lenguajes de programación, herramientas de administración, etcétera) y servicios (soporte técnico, seguros, comunicaciones, etcétera); que en conjunto dan soporte a las aplicaciones (sistemas informáticos) de una organización.
- Integridad: Condición de seguridad que garantiza que la información es actualizada, en todo su ciclo de vida, sólo por el personal y procedimientos autorizados.
- 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.
- Libros de estrategias: Procedimientos documentados que tienen como objetivo trazar la ruta de acción ante un tipo de incidente especifico.
- 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 Interna para la Gestión de Incidentes. 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.
- Log's: Registro de los sistemas de información que permite verificar las tareas o actividades realizadas por determinado usuario o sistema.
- Lote (Batch): Archivo magnético que tiene almacenada una secuencia de comandos. Al ejecutarse, reemplaza la operación de digitar los comandos de secuencia cada vez que se requiere efectuar una operación. Se utiliza para almacenar operaciones repetitivas.
- Mesa De Ayuda: Es una unidad funcional con una estructura que tiene la responsabilidad de mantener la comunicación con usuarios finales y responder de una manera oportuna, eficiente y con alta calidad a los incidentes y requerimientos de servicios de TI.
- MIPG: Modelo Integrado de Planeación y Gestión.
- MSPI: Modelo de Seguridad y Privacidad de la Información.
- NOC: Centro operativo de red.
- 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]

- Recuperación: Volver el entorno afectado a su estado natural.
- Recursos Tecnológicos: Son todos los bienes tangibles e intangibles que posee la entidad, que constituyen herramientas informáticas para el desarrollo de las labores diarias.
- Registro De Eventos: En ingles Logs. Mecanismo mediante el cual se guarda en un archivo (generalmente de texto) toda la información correspondiente a las actividades o eventos de un determinado sistema, dispositivo o equipo.
- 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.
- 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: Protección que se brinda a los activos de información mediante medidas preventivas con el fin de asegurar la continuidad del negocio y evitar la materialización de los riesgos.
- Seguridad Informática: Se encarga del aseguramiento de la infraestructura tecnológica mediante herramientas o elementos físicos, para evitar la materialización de las amenazas que se propagan por la red.
- Servicio: Es un medio para entregar valor al usuario final, facilitando los resultados que se desean en la ejecución sus funciones y estrategia de la entidad
- SGSI: Sistema de Gestión de la Seguridad de la Información.
- Sistema De Gestión De Seguridad De La Información: 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

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

la ejecución de las tareas y la toma de decisiones de los niveles estratégico, táctico y operativo.

- SOC: Los Centros de Operaciones de Seguridad se encargan de realizar un seguimiento y analizar la actividad en redes, servidores, puntos finales, bases de datos, aplicaciones, sitios web y otros sistemas, buscando actividades anómalas que puedan ser indicativas de un incidente o compromiso de seguridad.
- Spam: Se llama spam, correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming.
- TIC: Tecnologías de la Información y las Comunicaciones.
- Trazabilidad: Conjunto de medidas, acciones y procedimientos que permiten registrar, identificar y realizar seguimiento a los incidentes en cada producto desde su origen hasta su respuesta final.
- Usuario: Este concepto cobija a todos los clientes internos, servidores públicos y contratistas que utilicen la red de la entidad.
- Validación: Garantizar que la evidencia recolectada es la misma que la presentada ante las autoridades.
- VPN: Una red privada virtual -RPV- o VPN (de acuerdo con las siglas en inglés de Virtual Private Network), es una tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada.
- Vulnerabilidad: Ausencia o debilidad de un control. Condición que podría permitir que una amenaza se materialice con mayor frecuencia, mayor impacto o ambas. Una vulnerabilidad puede ser la ausencia o debilidad en los controles administrativos, técnicos y/o físicos.
- Wan: Wide Área Network o red de área amplia, es una red de computadoras que abarca varias ubicaciones físicas, proveyendo servicio a una zona, un país, incluso varios continentes. Es cualquier red que une varias redes locales (LAN).

4. 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
Decreto	1008	2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el

Jerarquía de la Norma	Número Norma	Año de Expedición	Descripción de la norma
			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.
Resolución	500	2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital
Directiva	2	2000	Implementación de las fases de Gobierno Digital
Circular	58	2009	Cumplimiento decreto 1151 del 14 de abril del 2008 Establece los lineamientos de generales de estrategia de gobierno en línea de la república de Colombia
Manual de Gobierno Digital		2019	Implementación de la Política de Gobierno Digital – MinTIC.
Guia.21 Guía Gestión de Incidentes		2019	Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información.

Fuente: Elaboración Propia

Demás leyes, Decretos y desarrollos normativos que guían las acciones para implementar la gestión y publicación de Datos Abiertos en Empresa Púbicas de Armenia.

5. Objetivos

5.1. Objetivo General

Establecer los lineamiento y buenas prácticas que deben garantizarse en Empresas Públicas de Armenia apropiadas por todos los colaboradores (funcionario y contratistas) y proveedores, para la gestión de incidentes de seguridad y privacidad de la información.

5.2. Objetivo Especifico

En el marco de la Política Interna para la Gestión de Incidentes se plantean los siguientes objetivos específicos:

- Establecer el ecosistema de TI con los involucrados de tipo core, directo e indirecto.
- Establecer la estructura de toma de decisiones en el área del saber.
- Describir las buenas prácticas aplicables a las condiciones actuales de Empresas Públicas de Armenia para la gestión de eventos e incidentes de TI.
- Definir lineamientos de la política de Gestión de Incidentes para Empresas Públicas de Armenia.
- Definir parámetros de estrategias de EIC (Educación, Información y Comunicación) para el acceso, uso y apropiación de colaboradores (funcionarios, contratistas), proveedores y grupos de interés con la Gestión de Incidentes.

6. Componentes de la Política Interna de Gestión de Incidentes

Esta Política Interna para la Gestión de Incidentes describe las directrices, normas, lineamientos y buenas prácticas, con el propósito de gestionar la gestión de incidentes y eventos de TI que se presentes, A continuación, se describen los componentes de esta política definida:

6.1. Buenas prácticas aplicables

Teniendo en cuenta los criterios fundamentales definidos por el Ministerio TIC para la apertura de datos de calidad, a continuación, se describen los criterios aplicables de los licenciamientos de la Política Interna para la Gestión de Incidentes.

Según lo establecido en la *Guía 21 Gestión de Incidentes* del Modelo de Seguridad y Privacidad de la Información, se propone que Empresas Públicas de Armenia apropie y aplique con las siguientes buenas prácticas:

- **Aseguramiento de plataforma:** Empresas Públicas de Armenia debe ser asegurada correctamente. Se debe configurar la menor cantidad de servicios (principio de menor privilegio) con el fin de proveer únicamente aquellos servicios necesarios tanto a usuarios internos como externos. Se deben revisar configuraciones por default (usuarios, contraseñas y archivos compartidos). Cada recurso que pueda ser accedido por externos e incluso por usuarios internos debe desplegar alguna advertencia. Los servidores deben tener habilitados sus sistemas de auditoría para permitir el registro de eventos.

- **Gestión de Parches de Seguridad:** Empresas Públicas de Armenia debe contar con un programa de gestión de vulnerabilidades (Sistemas Operativos, Bases de Datos, Aplicaciones, Otro Software Instalado), este programa ayudara a los administradores en la identificación, adquisición, prueba e instalación de los parches.
- **Gestión del cambio:** La actualización de activos de información, solo se podrá realizar sobre la autorización previa de los responsables asignados en la política correspondiente.
- **Prevención de código malicioso:** Todos los equipos de la infraestructura (servidores como equipos de usuario) deben tener activo su antivirus, antimalware con las firmas actualizadas al día.
- **Seguridad en redes:** Debe existir una gestión constante sobre los elementos de seguridad. Las reglas configuradas en equipos de seguridad como firewalls deben ser revisadas continuamente. Las firmas y actualizaciones de dispositivos como IDS o IPS deben encontrarse al día. Todos los elementos de seguridad y de red deben encontrarse sincronizados y sus logs deben ser enviados a un equipo centralizado de recolección de logs para su respectivo análisis.
- **Sensibilización y entrenamiento de usuarios:** Los usuarios en Empresas Públicas de Armenia incluidos los administradores de TI deben ser sensibilizados de acuerdo a las políticas y procedimientos existentes relacionados con el uso apropiado de redes, sistemas y aplicaciones en concordancia con los estándares de seguridad de la entidad. Los encargados de los sistemas de información deben establecer las necesidades de capacitación de las personas encargadas de la protección de los datos.

Las actividades descritas anteriormente buscan prevenir la ocurrencia de incidentes de seguridad de la información que esta soportada por TI, y adicionalmente es necesario realizar una evaluación mensual.

6.2. Fases de la gestión de incidentes

Para el cumplimiento de la gestión de incidentes el modelo de seguridad y privacidad de la información establece las siguientes fases que tiene un comportamiento cíclico.

Ilustración 1 Ciclo de vida de la gestión de incidentes

Este modelo cíclico de gestión de incidentes permite conocer los parámetros para afrontar cada una de las posibles situaciones que se presenten en el momento de eventualidades que pongan en riesgos la seguridad y privacidad de la información a los actores del negocio (colaboradores, proveedores), así como activos de información.

6.3. Ecosistema de Involucrados Empresas Publicas de Armenia ESP.

Empresas Públicas describe a continuación su ecosistema de involucrados:

- **Involucrado Core:** Fundamentales en la cadena de valor de Empresa Públicas de Armenia, los necesarios para garantizar servicios.
- **Involucrado Directo:** Relevantes en el entorno de negocio, pueden ser pares, entidades que complementan servicios.
- **Involucrado Indirecto:** Involucrados en el proceso de regulación del sector, inspección, vigilancia y control.

Involucrados Core	Involucrados Directos	Involucrados Indirectos
- Consumidores (Establecimientos residenciales y Establecimientos	- Proveedores de insumos secundarios. - Entidades públicas del territorio.	- Presidencia de la República - Congreso de la república.

Involucrados Core	Involucrados Directos	Involucrados Indirectos
comerciales) - Proveedores de materiales e insumos para garantizar servicios primarios. - Colaboradores (funcionarios y contratistas) - Alcaldía de Armenia	- Entidades privadas del territorio.	- Contralorías - Procuraduría - Entidades certificadoras de calidad. - Función Publica - Ministerios

Fuente: Elaboración Propia

6.4. Estructura de toma de decisiones en el área del saber

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

N°	Responsabilidad	Área/Procesos
1	Responsable de Gobierno y Gestión.	Comité MiPG
2	Responsable de Garantizar Cumplimiento.	Gerencia General
3	Gestión estratégica y técnica en Seguridad y Privacidad de la Información - Gestión de la Política. - Gestión de Procedimientos e Instrumentos. - Gestión del Plan de Seguridad y Privacidad de la Información. - Seguimiento y monitorio a eventos e incidentes. - Formulación de iniciativas y planes de contingencia sobre niveles de riesgos identificados y reportados. - Establecer mecanismos que permita la gestión de los incidentes reportados y la trazabilidad de los mismos. - Establecer canales de comunicación con proveedore de TI correspondientes para la gestión de incidentes. - Socialización a los respectivos involucrados de las situaciones presentadas en gestión de incidentes. - Identificar riesgos asociados a la gestión de incidentes de seguridad - Contactar a las autoridades y/o grupos especializados en respuesta a incidentes para las labores de coordinación y apoyo.	Dirección de Tecnologías de la Información y las Comunicaciones.
4	- Aplicar buenas practicas en Seguridad de la Información. - Asistir a los espacios de formación y capacitaciones citados. - Apropiar y cumplir con los establecido en los espacios	Todos los procesos.

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

Fuente: Elaboración Propia

6.5. Manejo de incidentes

6.5.1. Recursos de Comunicación

Según lo establece la Guía 21 de Gestión de Incidentes del Modelo de Seguridad y Privacidad de la Información, en esa sección se pretende describir los elementos necesarios para la comunicación del equipo de atención de incidentes dentro de la entidad.

- Información de Contacto: Se debe tener una lista de información de contacto de cada una de las personas que conforman el grupo de gestión de incidentes o quienes realicen sus funciones.

- Información de Escalamiento: Se debe contar con información de contacto para el escalamiento de incidentes según la estructura de la entidad.
    .1. Información de los administradores de la plataforma tecnológica (Servicios, Servidores)
    .2. Contacto con el área de recursos humanos o quien realice sus funciones (por si se realizan acciones disciplinarias).
    .3. Contacto con áreas interesadas o grupos de interés (CCP - Policía Nacional, Fiscalía, entre otras)
- Política de Comunicación: La entidad debe tener una política de comunicación de los incidentes de seguridad para definir que incidente puede ser comunicado a los medios y cual no.

6.5.2. Recursos para el análisis de incidentes

Empresas Públicas de Armenia ESP. debe considerar los siguientes elementos al momento de realizar un análisis de incidentes.

- Listado de los puertos conocidos y de los puertos utilizados para realizar un ataque.
- Diagrama de red para tener la ubicación rápida de los recursos existentes.
- Una Línea – Base de Información de: Servidores (Nombre, IP, Aplicaciones, Parches, Usuarios Configurados, responsable de cambios).

Esta información siempre debe estar actualizada para conocer el funcionamiento normal del mismo y realizar una identificación más acertada de un incidente.

• Se debe disponer de un análisis del comportamiento de red estándar, teniendo en cuenta puertos utilizados por los protocolos de red, horarios de utilización, direcciones IP con que generan un mayor tráfico, direcciones IP que reciben mayor número de peticiones.

6.5.3. Recursos Para La Mitigación Y Remediación

En este punto se consideran los elementos básicos para la contención de un posible incidente, Backup de Información, imágenes de servidores, y cualquier información base que pueda recuperar el funcionamiento normal del sistema.

6.5.4. Estado de un incidente

- *Registrado:* Incidente caracterizado con una identificación, categoría y

prioridad.

- *En ejecución:* Incidente asignado y con acciones claras en operación.
- *Anulado:* Incidentes duplicado, registrado por error.
- *Solucionado:* Incidente resuelto con acciones de seguimiento para verificar estado.
- *Suspendido:* Incidente que es pausado en su resolución, deberá tener una causa justificada.
- *Cerrado:* Estado del incidente que cuenta con un informe y se registra en la bitácora.

6.6. Lineamientos

A continuación, se describen los lineamientos de cumplimiento para la política interna de gestión de incidencias sobre infraestructura TI y servicios TI de Empresas Públicas de Armenia ESP.

6.6.1. Sobre la mapeo y caracterización:

- Identificar a la Dirección TICs como primer y único punto de contacto para reporte de incidencias.
- El reporte de cualquier incidencia se realizará únicamente por los siguientes medios de comunicación:
  - Mesa de Ayuda – Dirección TICs, accediendo al sitio web www.intraepa.gov.co
  - Correo electrónico: atic@epa.gov.co
  - Extensión: 1512-1513
- Cada proceso es responsable de notificar a la dirección TICs las incidencias identificadas en los servicios de TI.
- Empresas Públicas de Armenia ESP., desde el proceso de Dirección TICs deberá garantizar canales y vehículos de comunicación que permitan efectividad y eficiencia en la identificación y registro de las incidencias.
- Toda incidencia identificada deberá ser registradas y categorizada bajo las tipologías definidas en la presente Política Interna de Seguridad y Privacidad de la Información.
- El reporte de cinco (5) o más incidente del mismo tipo dará pie para que se declare como un incidente masivo.
- Si un incidente es catalogado como masivo, su gestión deberá seguir el siguiente conducto regular:
  - La Dirección TICs deberá notificar a la gerencia general.
  - La Dirección TICs bajo autorización de la gerencia general, deberá notificar a todos los procesos la incidencia masiva presentada.

- La Dirección TICs deberá activar el *Procedimiento de Gestión de Incidentes de Seguridad y Privacidad de la Información.*
- La Dirección TICs deberá notificar bajo el carácter de "emergencia" a los proveedores directamente vinculados al incidente masivo.

- La Dirección TIC deberá apoyar a los procesos en la definición de un lenguaje de modelado que permita el mapeo y relacionamiento de los datos. Esto puede ser un Modelo Entidad-Relación, un diagrama de datos, un modelo de arquitectura de datos.
- Los incidentes que en su identificación den origen a cambios en los ítems de configuración del servicio de TI serán atendido por medio de una *Solicitud de Cambios* descrito en el *Procedimiento de Gestión de Incidentes de Seguridad y Privacidad de la Información.*
- Los incidentes de TI asociados a Seguridad de Información serán gestionados mediante el *Procedimiento de Gestión de Incidentes de Seguridad y Privacidad de la Información.*
- La Dirección TICs deberá registrar en una bitácora todos los incidentes reportados con sus respectivos estados resolutivos.

6.6.2. Sobre la priorización y diagnóstico preliminar:

- La Dirección TICs será la encargada de diagnosticar y priorizar las incidencias reportadas por los procesos y de establecer la forma de darle resolución.
- La Dirección TICs deberá establecer, por medio propio o con el apoyo de proveedores si lo requiere, el origen del incidente.
- La Dirección TICs asignará y notificará a quien, por competencia y responsabilidad, deba trabajar en resolver el incidente presentado.
- La Dirección TICs deberá escalar cada incidente, dado el caso de cada incidente, al especialista responsable de garantizar la solución tecnológica afectada. Si el incidente es asignado a un proveedor, se deberá hacer efectiva aplicando lo que establece la Política Interna de Gestión de Proveedores.
- La Dirección TICs, deberá mantener informados a los involucrados el estado del incidente, teniendo en cuenta parámetros de tiempos para cada actualización del reporte, los niveles de escalamiento para comunicación y conocimiento son:

Nivel	Tiempo de atención	Acciones	Área a informar	Propósito
0	De 0-60 minutos de transcurrido el incidente.	El delegado de TI notificará vía telefónica el resumen del incidente y el tiempo de atención	Proceso directamente implicado en el incidente.	Que las áreas implicadas conozcan cómo actuar ante posible

		estimado.		incidente y exista una comunicación asertiva hacia terceros.
1	De 61-100 minutos de transcurrido el incidente.	El delegado de TI notificará vía correo electrónico con resumen del incidente y el tiempo estimado según clasificación del incidente. Con recomendaciones de conducta sobre la situación.	Proceso directamente implicado en el incidente, Proceso jurídico y secretaria general.	Que las áreas de implicadas sepan como actuar sobre el incidente reportado.
2	De 101-179 minutos de transcurrido el incidente.	El Director TICs notificará vía circular a los directores implicados con resumen del incidente y el tiempo estimado de resolución según reportes del proveedor del servicio.	Proceso directamente implicado en el incidente, Proceso jurídico y secretaria general. Gerencia General	Preparar acciones de contingencia sobre procesos vitales de Empresas Publicas de Armenia.
3	De 180 minutos en adelante de transcurrido el incidente.	Luego de tres (3) horas de detención de la operación, el incidente se convierte en problema y se efectúan las actividades del procedimiento de gestión e problemas, el director TICs comunicará al gerente general y demás procesos la situación y posible tiempo de atención del problema para la generación de planes de contingencia.	Nivel directivo de todas las áreas de la entidad, todas los procesos y comunicación al ciudadano.	Gestionar el protocolo de contingencia ante la operación.

6.6.3. Sobre la resolución y recuperación:

- Empresas Públicas de Armenia ESP., deberá identificar las causas del incidente para proceder a la debida solución.
- Empresas Públicas de Armenia ESP., desde el proceso Dirección TIC, implementar una estrategia que permita la toma de decisiones oportuna con el fin de evitar la propagación de incidentes ya así disminuir los daños a los recursos de TI y la perdida de la confidencialidad, integridad y disponibilidad de la información.
- Empresas Públicas de Armenia ESP., desde el proceso Dirección TIC, definir e implementar acciones contención que permita la oportuna detección de incidentes y evitar propagación a niveles masivo que afecten la integridad de la información.
- Empresas Públicas de Armenia ESP., desde el proceso Dirección TIC,

realizar una erradicación y eliminación de cualquier rastro dejado por el incidente.

- Empresas Públicas de Armenia ESP., deberá realizar pruebas después de garantizar la erradicación completa del incidente.
- Empresas Públicas de Armenia ESP., desde el proceso Dirección TIC, restablecer la funcionalidad de los sistemas afectados, y realizar un fortalecimiento del sistema que permita prevenir incidentes similares en el futuro.
- Empresas Públicas de Armenia ESP., desde el proceso Dirección TIC, definir una ruta de continuidad del servicio suficientemente probado en los diferentes escenarios, como apoyo en la restauración de los servicios, sistemas y aplicativos.
- Empresas Públicas de Armenia ESP., deberá revisar procesos, procedimientos, lineamientos, entre otros, con el fin de determinar modificaciones para prevenir futuros incidentes.

6.6.4. Sobre el cierre y seguimiento:

- Cuando el incidente haya sido resuelto se registrará en la bitácora de incidentes establecida por la Entidad.
- Los procesos o áreas afectadas deberán aplicar encuesta y/o cuestionario de satisfacción para verificar el estado del servicio y el desempeño y acompañamiento en la resolución del incidente.
- Si el incidente es catalogado como masivo, el proveedor de servicios de TI deberá entregar un informe sobre la gestión del incidente y las recomendaciones pertinente para evitar nuevos eventos. Este informe será reportado en el seguimiento que se realiza desde el calendario establecido por Empresas Públicas de Armenia ESP.
- La Dirección TICs deberá consolidar anualmente la información registrada en la bitácora y generar un reporte sobre las incidencias e incidencias masivas presentadas en Empresas Públicas de Armenia con su respetivo reporte resolutivo. Este informe deberá dar respuesta a las siguientes métricas:
    - Número total de incidencias.
    - Número y/o porcentaje de incidencias graves.
    - El número y/o porcentaje de incidencias asignadas de manera incorrecta.
    - El porcentaje de incidencias gestionadas en el plazo acordado.
    - Lecciones aprendidas y acciones de mejora para la siguiente vigencia.

Instrumentos para la Gestión de Incidentes
Empresas Públicas de Armenia ESP., ha diseñado un Modelo de Madurez para dar cumplimiento a las Políticas Nacionales de Gobierno Digital y Seguridad y Privacidad de la Información y específicamente en la gestión de incidentes. A continuación, se muestran los documentos para la gestión de incidentes:

- Política Interna para la Gestión de Incidentes.
- Plan de Seguridad y Privacidad de la Información.
- Procedimiento de Gestión de Incidentes de Seguridad y Privacidad de la Información.
- Plataforma Mesa de Ayuda -Intraepa.

7. 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 el acceso, apropiación y uso del conjunto de datos para los propósitos pertinentes de cada involucrado.
- Para fines específicos de Educación la Gestión de Talento Humano con el apoyo de Dirección TICs, 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 del Ministerio de Tecnologías de la Información y las Comunicaciones.

8. Declaración de publicación

La publicación de la *Política Interna de Gestión de Incidentes Empresas Públicas de Armenia*. se realizará en la Intranet de la entidad, sitio web www.intraepa.gov.co una vez sea aprobada. La presente política rige a partir de su publicación.

Elaboró: Moisés Jhónatan Rentería Campaña – Contratista, Dirección TIC.
Revisó: Ana María Arcila – Profesional Universitario, Dirección TIC.
Aprobó: Cesar Iván López Bedoya – Director TIC.