

# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN



**Código: MC-EC-POL-2**

<b>Elaborado por:</b> Isabella Lebolo <b>Profesional</b> <b>Cumplimiento y Datos</b> <b>Personales.</b>	<b>Revisado por:</b> Jonas Urbano <b>Subgerente de Sistemas</b>	<b>Aprobado por:</b> Javier Gonzalez <b>Subgerente de Cumplimiento, Riesgos y Sostenibilidad.</b>
---	---	---

Documento aprobado electrónicamente en el Software Kawak

DOCUMENTO

---

TRIPLE A S.A. E.S.P.

### REGISTRO DE CAMBIOS

Versión No.	Fecha	Resumen de los cambios
1	22/12/2022	Creación de la Política.

DOCUMENTO

MC-EC-POL-2 Versión: 1	DOCUMENTO POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	Página 3 de 7
---------------------------	--	---------------

## INTRODUCCIÓN

Triple A S.A. E.S.P., entidad prestadora de servicios públicos domiciliarios de Acueducto, Alcantarillado y Aseo, reconoce en la Seguridad de la Información como un conjunto de técnicas y acciones que se implementan para garantizar los niveles de seguridad de la información con sus características de confidencialidad, integridad y disponibilidad, bajo los componentes de privacidad y protección de datos personales, gestión documental y seguridad informática, entre otros. En consecuencia se compromete a gestionar los riesgos y las oportunidades en materia de seguridad de la información que inciden en su objeto social y en su entorno y de esta manera garantizar la sostenibilidad y continuidad del negocio.

Consciente de la importancia de la Seguridad de la Información, Triple A S.A.E.S.P. ha formulado esta política como marco orientador de acciones dirigidas a la gestión de riesgos y oportunidades de seguridad de la información, basado en un enfoque de precaución que conlleve a la preservación de la imagen organizacional y al fortalecimiento del relacionamiento con sus grupos de interés, con la finalidad de aportar al cumplimiento de los objetivos estratégicos y la competitividad en la compañía.

Para lo anterior, la compañía ha adoptado las mejores prácticas y estándares internacionales en materia de gestión de seguridad de la información como es la ISO 27001 además de toda la regulación aplicable.

### 1. OBJETIVO DE LA POLÍTICA

Establecer los elementos y el marco general de actuación para garantizar los niveles de seguridad de la información con sus características de confidencialidad, integridad y disponibilidad, bajo los componentes de privacidad y protección de datos personales, gestión documental y seguridad informática, entre otros, de tal manera que se eviten posibles adulteraciones, pérdidas, consultas y usos o accesos no autorizados. Este documento hace parte de la gestión de Seguridad de la Información y se complementa con los lineamientos específicos de seguridad de la información que puedan establecerse con relación a determinados procesos y proyectos.

### 2. ALCANCE

Este documento tiene alcance a toda la información gestionada por Triple A S.A. E.S.P. en los niveles estratégico, táctico y operativo de los procesos definidos en el mapa de procesos corporativo.

DOCUMENTO

MC-EC-POL-2 Versión: 1	<b>DOCUMENTO POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	Página 4 de 7
---------------------------	--	---------------

### **3. ELEMENTOS DE LA POLÍTICA**

#### **3.1 GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN**

Triple A S.A. E.S.P. ha definido la siguiente estructura organizacional con instancias, roles y responsabilidades, con el fin de asegurar un adecuado funcionamiento del Sistema de Seguridad de la Información:

##### **Gerente General**

Vela por la adopción e implementación de la Gestión de Seguridad de la Información en Triple A S.A. E.S.P. Particularmente, aprueba la Política de Seguridad de la Información Privacidad y las responsabilidades para la gestión de los riesgos relacionados con seguridad de la información. Así mismo, monitorea dichos riesgos en el contexto del direccionamiento estratégico y plantea acciones correctivas de acuerdo con el nivel tolerable que defina.

##### **Subgerencia de Cumplimiento, Riesgos y Sostenibilidad**

Asume el rol de Oficial de Seguridad de la Información. Particularmente dirige y lidera las actividades encaminadas al adecuado diseño, implementación y monitoreo del modelo de seguridad de la información de Triple A. S.A ESP, de acuerdo con los lineamientos y directrices establecidos por la organización, y la normativa aplicable. Dicha gestión será apoyada por la Jefatura de Riesgos y el área de Cumplimiento y Datos Personales según su alcance.

##### **Comité de Seguridad de la Información**

Promueve la elaboración e implementación de un sistema que permita administrar los riesgos de seguridad de la información y privacidad a través de la implementación de medidas y controles transversales a los procesos de la Compañía. Este órgano debe liderar el análisis y la evaluación del sistema y los riesgos asociados a la seguridad de la información con el fin de tomar decisiones que conlleven a salvaguardar los intereses de Triple A S.A ESP por medio de la adopción de políticas, controles y medidas que permitan cumplir con lo dispuesto en la norma.

Este Comité estará conformado por representantes de las siguientes áreas que tengan potestad para la toma de decisiones:

##### **Miembros permanentes:**

- Subgerencia de Cumplimiento, Riesgos y Sostenibilidad oficiando como Oficial de Seguridad de la Información
  - Área de Cumplimiento y Datos Personales
  - Jefe de Riesgos, desempeñando la Secretaría Comité

**DOCUMENTO**

---

MC-EC-POL-2 Versión: 1	<b>DOCUMENTO POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	Página 5 de 7
---------------------------	--	---------------

- Gerencia Administrativa y Financiera
  - Coordinación Gestión documental
- Subgerencia de Sistemas

**Miembros de apoyo:**

- Gerencia Administrativa y Financiera
- Jefatura de Seguridad Física
- Subgerencia Comunicaciones
- Gerencia de Gestión humana
- Subgerencia de Auditoría Interna
- Gerencia de Asuntos Legales, Regulatorios y Secretaría General

En caso de existir algún tema relevante se llevará por parte del Oficial de Seguridad de la Información a conocimiento de la Gerencia General.

**Área de Cumplimiento y Datos Personales**

Actúa en calidad de Oficial de Protección de Datos. Lidera la implementación de las actividades para asegurar la privacidad y protección de datos personales en cumplimiento de la normativa aplicable. Adicionalmente, monitorea la administración efectiva de los riesgos relacionados con seguridad de la información y privacidad de datos que pueden afectar a la compañía.

**Subgerencia de Sistemas**

Formaliza los lineamientos para la adecuada gestión y operación de la seguridad informática, y los Recursos y Servicios Informáticos en Triple A S.A. E.S.P buscando niveles adecuados de protección y resguardo de la información para garantizar el debido control y minimizar los riesgos asociados mediante acciones tendientes a proteger de posibles riesgos de daño, pérdida y uso indebido de la información, los equipos y demás recursos informáticos de la entidad.

**Coordinación de Gestión Documental**

Lidera la implementación de las actividades y lineamientos para garantizar los niveles de seguridad de la información de la documentación física de la Compañía con sus características de confidencialidad, integridad y disponibilidad.

**Líderes de los procesos (Gerentes/Directores)**

Son responsables de la aplicación de la gestión de la seguridad de la información en los procesos a su cargo de acuerdo con las políticas y metodologías definidas para este fin. Particularmente deben identificar, medir, gestionar y monitorear los riesgos relacionados con seguridad de la información de sus procesos, incluyendo la aplicación de los controles

**DOCUMENTO**

---

MC-EC-POL-2 Versión: 1	<b>DOCUMENTO POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	Página 6 de 7
---------------------------	--	---------------

a cargo y acciones de mitigación, así como reportar los cambios en las condiciones de riesgo, los eventos materializados y los avances en los planes de acción definidos.

### **Todos los colaboradores**

Aplican la gestión de seguridad de la información en sus procesos, incluyendo la aplicación de los controles a cargo y acciones de mitigación, de acuerdo con las políticas y metodologías definidas. Particularmente deben alertar sobre los posibles riesgos o incidencias dentro del marco de seguridad de la información que puedan afectar el normal desarrollo de su trabajo y reportar los eventos de riesgo que se hayan materializado.

### **Subgerencia de Auditoría Interna**

Evaluá la eficiencia y eficacia del Sistema de Seguridad de la Información, genera recomendaciones para su mejoramiento, realiza seguimiento a la efectividad de las acciones adoptadas para gestionar los riesgos y evalúa el funcionamiento de los controles clave. Adicionalmente, contribuye con la identificación de nuevos riesgos relacionados con seguridad de la información y privacidad durante el desarrollo de sus actividades de auditoría.

## **3.2 DECLARACIONES**

Triple A S.A. E.S.P adquiere, retiene y produce información para la administración del negocio y el cumplimiento de los requisitos legales, por lo que la calidad de la información es de suma importancia para la compañía.

En Triple A S.A. E.S.P se administran los sistemas de información con el fin de preservar la confidencialidad, disponibilidad e integridad de la información a la que tenemos acceso, desde la ejecución de las funciones asociadas a los cargos, asegurando su veracidad, a partir de la responsabilidad de contar con información clara y detallada que permita reflejar la realidad de todas las operaciones, así como de los registros comerciales y financieros que esta conlleva.

En Triple A S.A. E.S.P se debe proteger la información que se considere como confidencial y/o privilegiada acorde a las consideraciones de cada uno de los líderes de área; así mismo, deben guardar confidencialidad frente a procesos de negociación, contractuales, relaciones comerciales y operacionales, entre otros. La información confidencial incluye información que no ha sido divulgada al público, que brinda a Triple A S.A. E.S.P una ventaja y que podría causar daños en caso de que llegase a ser divulgada en forma inadecuada, recordando que la obligación de guardar la confidencialidad continúa, aun si ya no se labora en la compañía.

Como consecuencia de lo anterior, Triple A S.A. E.S.P adopta los siguientes compromisos:

**DOCUMENTO**

---

MC-EC-POL-2 Versión: 1	<b>DOCUMENTO POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN</b>	Página 7 de 7
---------------------------	--	---------------

- Respetar las leyes de privacidad y de protección de datos personales vigentes y aplicables, así como las políticas de privacidad de la información y cualquier otra directriz emitida por la empresa en esta materia.
- Se prohíbe revelar información de carácter no pública a terceros, incluidos familiares, amigos y compañeros de trabajo; excepto cuando se requiera por ley, por fines comerciales o por razones laborales.
- Adoptar las medidas de seguridad física, tecnológica y/o administrativa que sean necesarias para impedir la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de los datos, para garantizar los atributos de integridad, autenticidad y confiabilidad de los mismos.
- Abstenerse de usar o acceder a información confidencial o propiedad intelectual de clientes, competencia, socios comerciales o colaboradores sin su consentimiento por escrito para obtener una ventaja desleal.
- Garantizar la legitimidad en todos los documentos, evitando la falsificación, destrucción y alteración de los mismos, entendiendo que cualquier acción en este sentido se entenderá como la constitución de un fraude.
- Recopilar información de terceros necesaria, pertinente y no excesiva para la finalidad de selección, evaluación y ejecución de la relación contractual o comercial a que haya lugar conforme a la legislación vigente.
- Los colaboradores se responsabilizan por no divulgar información confidencial o estratégica, ya sea de la compañía, proveedores, consultores, contratistas o clientes, a la que tengan acceso por ocasión de su cargo. En caso de que un colaborador esté autorizado para entregar información y/o mantener correspondencia con terceros, debe ser responsable de que tal información sea veraz.
- Limitar el acceso a la información confidencial exclusivamente a aquellos colaboradores que necesiten conocer dicha información para desempeñar sus funciones.
- No usar la información confidencial para beneficio personal o para favorecer a terceros.
- Garantizar la veracidad de la información que sea remitida tanto interna como externamente.

#### **4. RESPONSABLES DE CONTROL Y APROBACIÓN**

Es responsabilidad de la administración, en cabeza de la Subgerencia de Cumplimiento, Riesgos y Sostenibilidad, la revisión periódica de la Política de Seguridad de la Información y la solicitud de ajustes correspondientes al Comité de Seguridad de la Información, para que éste dentro de sus atribuciones recomiende las aprobaciones de competencia de la Gerencia General, siendo esta última, la única instancia de aprobación de esta política.

La presente política rige a partir de la fecha de su expedición.

**DOCUMENTO**

---