

ATENTO

Sí, las políticas y los  
procedimientos son nuestra  
**responsabilidad**



**POL.ITD.002.V1**

Política Corporativa de  
Ciberseguridad - Pública

Versión 01

04/22



## Sumário

1.	OBJETIVO .....	3
2.	CAMPO DE APLICACIÓN .....	3
3.	DOCUMENTO DE REFERENCIA.....	3
4.	TERMINOLOGÍA.....	3
5.	DESARROLLO .....	3
6.	RESPONSABILIDADES .....	4
7.	HISTÓRICO DE REVISIÓN .....	4

**1. OBJETIVO**

N/A

**2. CAMPO DE APLICACIÓN**

N/A

**3. DOCUMENTO DE REFERENCIA**

N/A

**4. TERMINOLOGÍA**

N/A

**5. DESARROLLO**

La presente Política Corporativa de Ciberseguridad afecta a toda la organización y expresa el compromiso de la Dirección de aprobar y apoyar las normativas y procedimientos de seguridad necesarios para la gestión de la seguridad de la información, basándose en esta Política, la normativa legal vigente y los requerimientos de los clientes.

Con este fin, la Dirección asume como compromisos los siguientes Objetivos Estratégicos de Ciberseguridad:

1. Considerar la información y los sistemas que la soportan como activos estratégicos, manifestando así su determinación en alcanzar los niveles de seguridad necesarios que garanticen su protección en cuanto a la autenticación, la confidencialidad, la integridad, la disponibilidad y la trazabilidad.
2. Instaurar un Comité de Seguridad de Ciberseguridad que gestionará todas aquellas directrices que permitan preservar, resguardar y afianzar la seguridad de los activos de información y así mejorar la calidad de los servicios que se ofrecen a los clientes.
3. Promover la implantación de los niveles de seguridad apropiados que permitan proteger tanto los recursos de los sistemas de información y la información procesada, almacenada o transmitida por ellos, como asegurar el cumplimiento de la legislación vigente en la materia, velando por la confidencialidad, integridad y disponibilidad de la información; así como gestionar los incidentes de seguridad que pudiesen afectar a la misma.
4. Promover acciones de formación y concienciación sobre Ciberseguridad dirigidas a todo el personal y garantizar la difusión de la presente Política, así como de los documentos que la desarrollan.
5. Crear un sistema de gestión de la Ciberseguridad basado en estándares internacionales y códigos de buenas prácticas, para identificar, cuantificar, priorizar y tratar los riesgos, así como para evaluar y revisar el desarrollo de la Política de Ciberseguridad como marco de definición de las directrices básicas de seguridad.
6. Velar por la existencia de los mecanismos necesarios que aseguren la continuidad de las actividades críticas de Atento ante contingencias graves que afecten a los sistemas de información, permitiendo la recuperación de estos en un periodo de tiempo aceptable.
7. Garantizar el cumplimiento de la legislación y regulaciones vigente en materia de Ciberseguridad.

Todo el personal de Atento, así como el personal externo (Clientes y Colaboradores), está obligado a conocer, respetar y hacer cumplir dentro de su ámbito de responsabilidad las medidas de seguridad establecidas para la protección de la información.

El acceso a la información y a los sistemas de información estará condicionado a la adhesión a esta Política y a la normativa que la desarrolla, siendo éstas de obligado cumplimiento. Su incumplimiento manifiesto podrá acarrear el inicio de las medidas disciplinarias oportunas y, en su caso, responsabilidades legales.

## 6. RESPONSABILIDADES

N/A

## 7. HISTÓRICO DE REVISIÓN

Versión	Fecha	Revisor	Modificaciones
01	04/22	Controle Internos	Version Inicial