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

POL.SI.002.V04.ESP

Política Corporativa de Ciberseguridad - Pública

Versión 04

11/24

#PolíticasQueNosGuían

Sumario

1. OBJETIVO

El propósito de esta Política es proteger los activos de información de la organización, asegurando sus dimensiones de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad, así como las infraestructuras, sistemas y recursos humanos que la procesan, gestionan, transmiten y almacenan, siempre de acuerdo con los requerimientos del negocio y las obligaciones legales y contractuales aplicables.

2. CAMPO DE APLICACIÓN

La presente Política de Seguridad de la Información es de aplicación a todas las personas, sistemas y medios que accedan, traten, almacenen, transmitan o utilicen la información conocida, gestionada o propiedad de Atento para cualquiera de sus actividades del ciclo de vida, creación, captura, recepción, transmisión, visualización, clasificación, retención y eliminación.

El personal sujeto a esta política incluye a todas las personas con acceso a la información descrita, independientemente del soporte automatizado o no en el que se encuentre esta y de si el individuo es empleado o no de Atento, por lo tanto, también aplica a los contratistas, clientes, proveedores o cualquier tercero que tenga acceso a la información o los sistemas de la empresa.

Las directrices recogidas en la presente Política serán desarrolladas en procedimientos, instrucciones técnicas y guías, de acuerdo con el Marco Normativo de Ciberseguridad.

3. DOCUMENTO DE REFERENCIA

- *ISO/IEC 27001:2022*
- *ISO/IEC 27000:2018*
- *ISO/IEC 27701:2019*

4. TERMINOLOGÍA

Término	Definición
Activo	Cualquier información o elemento que tiene valor para la organización
Análisis de riesgo	Uso sistemático de la información para identificar fuentes y para estimar el riesgo.
Adaptabilidad	Define los eventos y bajo qué criterios un sistema debe poder ser monitoreado y revisado para su control posterior
Autenticidad	Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando al emisor para evitar suplantación de identidad.
Confiabilidad de la información	Garantiza que la fuente de la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
Confidencialidad	Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
Declaración de aplicabilidad	Documento que describe los objetivos de control y los controles pertinentes y aplicables para el mismo.
Disponibilidad	Propiedad de que la información sea accesible y utilizable por solicitud de una entidad.
Evaluación del riesgo	Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

Término	Definición
Evento de seguridad de la información	Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información, la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.
Gestión del riesgo	Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.
Incidente de seguridad de la información	Un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
Integridad	Propiedad de salvaguardar la exactitud y estado completo de los activos.
Protección a la duplicación	Consiste en asegurar que una transacción solo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
Recursos informáticos	Todos aquellos componentes de hardware y programas (software) que son necesarios para el buen funcionamiento y la optimización del trabajo con computadores y periféricos, tanto a nivel Individual, como colectivo u organizativo, sin dejar de lado el buen funcionamiento de estos.
Riesgo	El efecto de la incertidumbre sobre los objetivos.
Riesgo inherente	Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.
Riesgo residual	Nivel restante de riesgo después del tratamiento del riesgo.
Seguridad de la información	Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.
Sistema de gestión de la seguridad de la información SGSI	Parte del sistema de gestión global, basado en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.
Sistema de información	Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales que se realicen.
Tratamiento del riesgo	Proceso de selección e implementación de acciones de mejora que permita gestionar el riesgo.
Valoración del riesgo	Proceso de análisis y evaluación del riesgo

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, Grupo Atento asume como compromisos los siguientes Objetivos Estratégicos de Ciberseguridad:

- 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;
- 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;
- 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;
- 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;
- Crear un sistema de gestión de la Ciberseguridad basado en estándares internacionales y códigos de buenas prácticas, para identificar, cuantificar, priorizar, monitorear 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;
- 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;
- Garantizar el cumplimiento de la legislación y regulaciones vigente en materia de Ciberseguridad.

Todo el personal de Atento (Colaboradores), así como personas externas (Clientes, proveedores y stakeholders), están obligados 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

El comité ejecutivo debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información sean asignados y comunicados.

El comité ejecutivo debe asignar la responsabilidad y autoridad para:

- Asegurarse de que el Sistema de Gestión de Seguridad de la Información se desarrolle conforme a los estándares internacionales más relevantes.
- Informar sobre el desempeño del Sistema de Gestión de Seguridad de la Información.

7. HISTÓRICO DE REVISIÓN

Versión	Fecha	Revisor	Modificaciones
01	04/22	Controles Internos	Versión Inicial
02	11/22	Mauricio Baroni / Yovanni Pineda	Se añaden los puntos 1,2,3, 4, y 6
03	02/24	CISO Regionales e equipo de SI	Actualización de Texto
04	11/24	CISO Regionales e equipo de SI	Actualización de Texto