

ATENTO	Sistema Integrado de Gestión			
	PO-TEC SEG-01	Seguridad de la información	V.13	25.07.2024
Elaborado por:	José Israel Ayala - jefe de Procesos y Mejora Continua Javier Alexander Anaya Moreno - Analista de Seguridad de la Información			23.07.2024
Revisado por:	Javier Guatame – Jefe Región Sur de Seguridad de la Información			23.07.2024
Aprobado por:	Miguel José Lopez – Director País			25.07.2024

1. TABLA DE EDICIONES

N° Versión	Modificación	Fecha
V.08	Se ajusta al formato, se integran los objetivos del sistema de gestión a la política de seguridad de la información.	02/05/2019
V.09	Revisión general, ajustes de forma, reemplazo de Oficial de Seguridad de la información local por Gerente Regional de Seguridad de la Información y Director País por Regional Delivery director de acuerdo con los cambios internos de la empresa.	05/05/2020
V.10	Revisión general, ajustes de forma, reemplazo del Gerente Regional de Seguridad de la Información por CISO Región Sur de acuerdo con los cambios internos de la empresa.	17/11/2021
V.11	Revisión general, ajustes de forma, reemplazo de director País por Regional Delivery director de acuerdo con los cambios internos de la empresa.	08/12/2022
V.12	Revisión general. Se realiza ajuste de cargos para Regional Delivery director por Director País – Ajuste cambio de CISO.	07/11/2023
V.13	Se reestructura por completo la política, se incluyen los nuevos objetivos de seguridad, reemplaza el nombre comité de seguridad de la información por comité directivo. Además de la eliminación de numerales que están asociados en otras políticas, cambio de Director País	25/07/2024

2. OBJETIVO Y ALCANCE

Establecer las directrices en la organización para la gestión y fortalecimiento de la seguridad de la información.

Esta política de seguridad de la información aplica a todo el personal vinculado laboralmente con Atento Colombia S.A contratistas y terceros que tengan acceso a los recursos de información de la organización.

La información cubierta en este documento incluye la almacenada o compartida en cualquier medio: electrónico, en papel e información compartida de manera oral o visual. (Conferencias telefónicas o video conferencias).

3. REFERENCIAS

- NTC ISO/IEC 27001: 2022
- Guía GTC ISO/IEC 27002:2022

4. VOCABULARIO

N°	Concepto	Descripción
01	Amenaza	Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
02	Cifrado	Proceso de codificación de información sensible para evitar que esta llegue a personas no autorizadas.
03	Confidencialidad	Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
04	Control	Políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo aceptable.
05	Disponibilidad	Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

ATENTO	Sistema Integrado de Gestión			
	PO-TEC SEG-01	Seguridad de la información	v.13	25.07.2024

06	Encriptación	Es el proceso para volver ilegible información considerada importante. La información una vez encriptada solo puede leerse aplicándole una clave.
07	Incidente informático	Es la violación o amenaza que afectan la confidencialidad, disponibilidad, integridad como la continuidad de los servicios prestados.
08	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 impactos.
09	Vulnerabilidad	Debilidad del sistema o activo que puede usarse para causar algún daño.

5. RESPONSABILIDADES

La aprobación de la política de la seguridad de la información será realizada por el Director País, cualquier cambio, corrección o actualización, deberá ser propuesto en el comité de seguridad de la información y objeto de aprobación por parte del director País. Esta Política deberá ser divulgada a todos los usuarios de **Atento Colombia S.A.** y partes interesadas pertinentes a través de los diferentes medios de comunicación que posee.

La alta dirección debe brindar orientación y soporte para la gestión de la seguridad de la información de acuerdo con los requisitos del negocio y con la legislación aplicable.

El Comité Directivo de **Atento Colombia S.A.**, deberá establecer unas directrices claras para dar soporte a la seguridad de la información, a través de la puesta en vigencia y mantenimiento de las políticas de seguridad de toda la organización. Este comité podrá ser un grupo multidisciplinario donde participen representantes de diferentes áreas de la organización o en su defecto será la dirección país.

También, es responsabilidad del Comité Directivo identificar, actualizar y documentar todos los requisitos regulatorios y legales, e identificar los controles para cumplir estos requisitos.

Se deben identificar las leyes y regulaciones cuando se adquieran e implementen controles criptográficos, licencias, herramientas de auditoría, grabaciones de conversaciones y otros que sean regulados.


Los datos privados de los empleados de **Atento Colombia S.A** deben ser protegidos de acuerdo con la legislación de cada país.

En caso de ser necesario aplicar una modificación o cambio a las políticas generales, se requiere de la revisión del Comité de Seguridad de la Información y/o del Director País de Atento Colombia S.A. para su implantación y posterior cumplimiento.

De igual forma, se designó un responsable de Seguridad de la información de **Atento Colombia S.A.**, cuya labor es denominada Oficial de Seguridad de la Información en cabeza del CISO Global de Seguridad de la Información, esta persona asegura el mantenimiento permanente de los niveles de seguridad requeridos por **Atento Colombia S.A.**, además de la seguridad de los distintos sistemas informáticos y de las redes de telecomunicaciones soportadas. En consecuencia, tendrá el compromiso de prevenir la ocurrencia de acciones inapropiadas o comportamientos ilegales de los distintos usuarios que utilizan los recursos informáticos, así como los usuarios externos que acceden a estos recursos.

Estas responsabilidades no sólo competen a la disposición de los distintos intereses que persigue **Atento Colombia S.A.**, sino también a las obligaciones legales y éticas que conciernen al buen funcionamiento y privacidad de la información de **Atento Colombia S.A.**

El Oficial de Seguridad de la Información tendrá la responsabilidad primaria de documentar, actualizar e implantar las políticas de seguridad. Además, deberá hacer evaluaciones periódicas sobre su efectividad y definir modificaciones, siempre que considere necesarias para asegurar la protección de información y los activos relacionados con ellas en Atento Colombia S.A.

	Sistema Integrado de Gestión			
	PO-TEC SEG-01	Seguridad de la información	v.13	25.07.2024

6. DESARROLLO DE LA POLITICA

6.1. Política del sistema de seguridad de la información:

El propósito de la Política de Seguridad de la Información de Atento Colombia S.A. es proteger los activos de información de todas las amenazas internas o externas bien sean intencionales o accidentales.

Atento Colombia S.A. como BTO, está comprometida con la protección de la información y los activos asociados garantizando la confidencialidad, integridad y disponibilidad, dando cumplimiento con los requisitos aplicables, promoviendo la mejora continua, generando cultura y conciencia a sus partes interesadas pertinentes sobre el sistema de gestión de seguridad de la información.

6.2 Objetivos de seguridad de la información:

- Promover una cultura sólida de seguridad de la información entre los colaboradores y las partes interesadas relevantes, fomentando prácticas seguras en el manejo de información y asegurando la adherencia a las políticas establecidas
- Identificar y gestionar proactivamente los riesgos y oportunidades que puedan influir en los procesos y afectar la seguridad de la información dentro de la organización
- Preservar la confidencialidad, integridad y disponibilidad de la información en la organización.
- Gestionar de manera proactiva la mejora continua de los procesos de seguridad de la información a través de los controles y políticas establecidas.

6.3 Violaciones a las Políticas de Seguridad de la Información

Cualquier situación que evidencie la violación a la política de seguridad de la información por parte de los empleados o terceros que tenga relación directa o indirecta en el manejo de la infraestructura tecnológica y sistemas de información de la compañía podrá resultar en un proceso que deberá ser iniciado por parte del jefe inmediato o responsable del tercero, con base a las evidencias recopiladas las cuales pueden incluir, más no estar limitadas a:

Acción de tipo disciplinario por parte del área que la organización ha dispuesto para el efecto según los lineamientos establecidos por el Código Sustantivo del Trabajo, Reglamento Interno de Trabajo, el Código de Comportamiento Empresarial Atento Colombia S.A, las Cláusulas Especiales que se establezcan con los empleados en sus Contratos Laborales y/o todo aquello que según las leyes colombianas definan como acciones disciplinarias patronales.

- Suspensión o acceso restringido a las áreas de procesamiento de la información.
- Terminación del contrato laboral o relación comercial (Basados en las disposiciones emitidas por las leyes colombianas en materia laboral y el reglamento interno de trabajo).

7. REVISION DE LA POLITICA

Cada doce meses se revisará mínimo política para asegurar la vigencia y el cumplimiento o si ocurren cambios significativos asegurando su conveniencia, adecuación y eficiencia.