ATENTO

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

POL.SI.001.V05.ESP

Política de Seguridad de la Información y Cibernética

Versión 05
08/25

#PolíticasQueNosGuían

Sumario

1. Objetivo 3
2. Contexto de la Organización 3
3. Campo de Aplicación 3
4. Referencia 4
5. Principios de Ciberseguridad 4
6. Liderazgo 6
7. Planificación 6
8. Controles de Seguridad 7
9. Concienciación y Comunicación 8
10. Evaluación del Desempeño 8
11. Mejora 8
12. Cumplimento Legal y Regulatorio 8
13. Gestión de Proveedores 9
14. Excepciones 9
15. Versión 9

1. OBJETIVO

La presente Política de Información y Ciberseguridad establece los principios y directrices de alto nivel para la protección de los recursos informáticos y tecnológicos del Grupo Atento, sirviendo como documento central del Sistema de Gestión de Seguridad de la Información y Privacidad (SGSIP). El propósito de esta política es garantizar la confidencialidad, integridad y disponibilidad de la información, así como el uso aceptable y seguro de los recursos tecnológicos, de acuerdo con las mejores prácticas, requisitos legales y regulatorios, incluyendo ABNT NBR ISO/IEC 27001, y en línea con los objetivos estratégicos del Grupo Atento.

2. CONTEXTO DE LA ORGANIZACIÓN

El Grupo Atento reconoce la importancia crítica de la seguridad de la información, la privacidad de los datos y el uso adecuado y seguro de sus recursos tecnológicos para la sostenibilidad de su negocio y la protección de los intereses de sus grupos de interés. La organización opera en un entorno dinámico, con análisis continuo de contextos internos y externos que pueden afectar y presentar cambios, así como oportunidades para el Sistema de Gestión de Seguridad de la Información y Privacidad (SGSI).

En este contexto se incluye la creciente dependencia de los sistemas de información y de las infraestructuras tecnológicas para la prestación de los servicios informáticos que soportan el negocio del Grupo Atento. El uso eficaz y responsable de estos recursos es esencial para garantizar la confidencialidad, integridad y disponibilidad de la información procesada y almacenada, así como para mitigar los riesgos asociados con el uso inapropiado o malicioso de la tecnología.

El análisis del contexto organizacional también tiene en cuenta las expectativas de los clientes, socios, organismos reguladores y otras partes interesadas en relación con la seguridad de la información, la privacidad de los datos personales y la integridad de los procesos que dependen de recursos tecnológicos confiables y utilizados de manera ética y de acuerdo con los estándares establecidos. Esta política, por tanto, abarca tanto la protección de la información como los lineamientos para el uso adecuado de los recursos tecnológicos de Grupo Atento.

3. CAMPO DE APLICACIÓN

Esta Política cubre todos los procesos y sistemas de información, equipos electrónicos e informáticos y recursos de red del Grupo Atento. Se aplica, de forma amplia y sin restricciones, a todos los recursos tecnológicos puestos a disposición o utilizados por el Grupo Atento, incluidos, entre otros, los equipos informáticos, el software, los sistemas operativos, los medios de almacenamiento, las cuentas de red nominales y de servicio, el correo electrónico, la navegación web y la transmisión de datos.
Esta política se aplica a todas las áreas del Grupo Atento, así como a todos los empleados (incluidos los permanentes y temporales), proveedores de servicios, consultores, clientes y otros socios que interactúan con los procesos, sistemas de información o recursos tecnológicos del Grupo Atento.
El objetivo de este campo de aplicación es asegurar que todas las personas y todos los activos de información y tecnología dentro del ecosistema del Grupo Atento estén sujetos a las directrices establecidas en esta Política de Información y Ciberseguridad, consolidando las responsabilidades y controles para la protección de la información y el uso adecuado de los recursos tecnológicos en un único documento normativo.

En resumen, esta política se aplica a:

- Todos los procesos del Grupo Atento.
- Todos los sistemas de información de Grupo Atento.
- Todos los recursos tecnológicos que sean propiedad, utilizados o puestos a disposición por el Grupo Atento.
- Todos los empleados del Grupo Atento.
- Todos los proveedores de servicios que acceden a la información o a los sistemas del Grupo Atento.

- Consultores, clientes y otros socios que interactúan con los recursos tecnológicos, sistemas de información o procesos del Grupo Atento.

4. REFERENCIA

Esta política está integrada con el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSI) y se refiere a los siguientes documentos de alto nivel:

- ISO/IEC 27001:2022
- ISO/IEC 42001:2023
- MAN.SI.001 - Manual del sistema de gestión de seguridad de la información
- POL.LEG.012 – Política Global Privacidad
- POL.ITD.004 – Politica de uso responsable de IA
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (Reglamento General de Protección de Datos - GDPR)
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI).
- Ley 9/2014, de 9 de mayo, de Telecomunicaciones.

Otros documentos normativos, como estándares, procedimientos y políticas específicas, complementan esta política y se hace referencia a ellos en el Manual SGSIP (MAN.SI.001) y registros relacionados.

5. PRINCIPIOS DE CIBERSEGURIDAD

El Grupo Atento adopta los siguientes principios fundamentales para la gestión de la información y la ciberseguridad, que sirven como base para todas las medidas de seguridad implementadas.

- Seguridad de la Información como Proceso Integral: El conjunto de prácticas y procesos implementados para proteger los activos de información del Grupo Atento. Abarca los principios fundamentales de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, siendo la base para todas las medidas de seguridad adoptadas para mitigar riesgos y garantizar la continuidad del negocio. Este principio está intrínsecamente ligado a los objetivos de seguridad y privacidad mencionados en la sección 7 de esta política y detallados en el Manual del Sistema de Gestión de Seguridad de la Información y Privacidad (MAN.SI.001 - Manual del sistema de gestión de seguridad de la información). Consideramos la seguridad como parte de la operativa habitual, aplicándola desde el diseño inicial de los sistemas TIC y extendiéndola a lo largo de todo su ciclo de vida.
- Confidencialidad: Asegurar que la información sea accesible solo para las entidades autorizadas. Esto se logra mediante la implementación de controles de acceso (definidos en POL.SI.005 - Control de Accesos) y la protección de contraseñas (NOR.SI.011 - Norma de Gestión de Contraseñas), garantizando que solo el personal autorizado pueda acceder a datos sensibles. Un ejemplo práctico sería garantizar que los datos de clientes e información interna confidencial no sean accedidos por personas no autorizadas, permitiendo que los agentes de atención accedan únicamente a la información necesaria para su trabajo.
- Integridad: Garantizar la exactitud e integridad de la información y los métodos de procesamiento, protegiéndola contra modificaciones no autorizadas o accidentales. Esto implica asegurar que los datos

permanezcan precisos, completos y confiables a lo largo de su ciclo de vida. Medidas como el "Gerenciamiento de Vulnerabilidades" (NOR.SI.020 - Norma de Gestión de Vulnerabilidades y Aplicación de Patch) y los controles de cambio contribuyen a este principio. Ejemplo práctico: Asegurar que los registros de atención al cliente y las configuraciones de los sistemas no sean alterados de forma indebida o no autorizada.

- Disponibilidad: Garantizar que la información y los sistemas estén accesibles y utilizables para las entidades autorizadas cuando sea necesario. Esto se apoya en prácticas como NOR.SI.012 - Norma de Respaldo y Restauración de la Información y planes de continuidad de negocio para asegurar la continuidad de las operaciones en caso de incidentes. Ejemplo práctico: Mantener los sistemas de atención al cliente y las plataformas de comunicación accesibles en todo momento necesario para las operaciones del negocio.
- Autenticidad: Asegurar la veracidad y la legitimidad de una entidad, ya sea una persona, un proceso o un sistema, así como la garantía de la fuente de la que proceden los datos. Esto es fundamental para confiar en la identidad de los usuarios y en el origen de la información.
- Trazabilidad: Garantizar que las actuaciones de una entidad o persona en los sistemas y sobre la información puedan ser imputadas de manera exclusiva a dicha entidad o persona. Esto se logra a través del registro detallado de actividades y eventos, permitiendo la reconstrucción de acciones para fines de auditoría y responsabilidad.
- Privacidad (Protección de Datos Personales): Aplica las leyes, normativas o regulaciones que apliquen según el país donde se traten datos personales, incluyendo de forma prominente el Reglamento General de Protección de Datos (GDPR) y la Ley Orgánica de Protección de Datos y garantía de los derechos digitales (LOPDGDD) en España. Se garantiza la protección de los datos personales de empleados, clientes y proveedores, así como la obtención de consentimientos necesarios y la implementación de medidas de seguridad adecuadas.
- Uso Responsable de los Recursos Tecnológicos: Utilizar los recursos tecnológicos del Grupo Atento de manera ética, legal y conforme a las políticas de la empresa, tal como se establece en la "Normativa Global de Utilización Aceptable de Recursos Tecnológicos" (NOR.SI.019). Esto es fundamental para prevenir incidentes de seguridad, proteger la información y evitar el uso indebido de los activos de la empresa. Un ejemplo práctico sería utilizar los computadores y la red de Atento para fines profesionales y de acuerdo con las políticas de la empresa, evitando la descarga de software no autorizado o el acceso a sitios maliciosos (conforme detallado en la NOR.SI.019 - Norma de Utilización Aceptable de Recursos Tecnológicos).
- Control de Acceso Robusto, Incluyendo la Gestión de Contraseñas: Un aspecto fundamental de la seguridad de la información es la implementación de controles de acceso robustos para garantizar que solo usuarios, procesos o dispositivos autorizados puedan acceder a la información y a los activos de información. Esto incluye la gestión eficaz de contraseñas, las cuales deben ser robustas y gestionadas de acuerdo con la Norma de Gestión de Contraseñas (NOR.SI.011). Los requisitos detallados para la gestión del acceso lógico se encuentran definidos en la Norma de Control de Accesos (NOR.SI.005), que establece los procesos de solicitud, aprobación, concesión, revocación, modificación y revisión de cuentas de usuario.
- Determinación del Nivel de Seguridad Requerido: La organización determinará el nivel de seguridad exigido para cada sistema de información, en conformidad con los marcos regulatorios nacionales aplicables, como el establecido en el artículo 40 del Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad (ENS) en España, y los criterios generales recogidos en su Anexo I. Esta determinación se basará en la valoración del impacto en las dimensiones de seguridad (Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad), utilizando metodologías alineadas con frameworks nacionales relevantes, como la guía CCN-STIC 803 para la categorización de sistemas.
- Gobierno y Uso Responsable de Inteligencia Artificial: El Grupo Atento está comprometido con el desarrollo, la implementación y el uso responsable de sistemas de Inteligencia Artificial (IA). Para lograrlo, la organización asegura que la IA sea gestionada de manera ética, transparente y segura, con el objetivo de minimizar riesgos como sesgos, impactos no deseados en individuos y la sociedad. Esto incluye el

compromiso con la supervisión humana donde sea necesario. El Grupo Atento establecerá y mantendrá un Sistema de Gestión de IA (AIMS), alineado con los principios de la ISO/IEC 42001:2023 (Tecnología de la información — Inteligencia artificial — Sistema de gestión). Este sistema integrará la gestión de los riesgos y oportunidades específicos de la IA con el Sistema de Gestión de Seguridad de la Información (SGSI), reforzando la protección de la confidencialidad, integridad y disponibilidad de la información y garantizando la calidad de los datos utilizados en los sistemas de IA. Las directrices y procedimientos detallados para el desarrollo, la implementación y el uso responsable de la IA en Atento se encuentran definidos en POL.ITD.004. – Política de uso responsable de IA.

6. LIDERAZGO

La alta dirección del Grupo Atento demuestra su firme compromiso con la seguridad de la información y la ciberseguridad a través del establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI). Este compromiso se manifiesta en la definición de esta Política de Información y Ciberseguridad, la asignación de los recursos necesarios y la comunicación constante de la importancia crítica de la seguridad de la información a todos los empleados y partes interesadas.

Las responsabilidades y autoridades organizacionales en materia de seguridad de la información se definen y comunican de manera clara en toda la organización, asegurando un enfoque multidisciplinario y la participación activa en la protección de los activos de información. Los detalles específicos de las funciones, responsabilidades y autoridades para la seguridad de la información, incluyendo los roles y las expectativas asociadas, se establecen en las descripciones de trabajo correspondientes y se encuentran detallados en el Manual del Sistema de Gestión de Seguridad de la Información y Privacidad (MAN.SI.001).

El liderazgo en todos los niveles de la organización es responsable de garantizar el estricto cumplimiento de esta política, así como de los estándares, procedimientos y demás documentos normativos de seguridad de la información dentro de sus respectivas áreas de especialización y responsabilidad.

7. PLANIFICACIÓN

El Grupo Atento establece, implementa y mantiene la planificación necesaria para alcanzar los objetivos de seguridad y privacidad de la información, en concordancia con esta política. Esta planificación aborda los siguientes elementos clave:

- Acciones para Abordar Riesgos y Oportunidades: El Grupo Atento, mediante su planificación estratégica y mapa de procesos, comprende los escenarios externos e internos y realiza evaluaciones periódicas del Sistema de Gestión de Seguridad de la Información y Privacidad (SGSIP). Este análisis permite identificar y evaluar periódicamente los riesgos en los activos de información y las oportunidades inherentes a los procesos que componen el SGSIP. Los detalles sobre el proceso de evaluación y tratamiento de riesgos, incluyendo la metodología utilizada y los controles implementados, se definen en documentos y procedimientos normativos específicos. Es crucial que esta planificación considere los principios de confidencialidad, integridad y disponibilidad discutidos en la sección 5 de esta política.
- Objetivos de seguridad y privacidad de la información y planificación para alcanzarlos: La alta dirección, a través de la planificación estratégica, comprende los escenarios externos e internos y las expectativas de sus partes interesadas para determinar los objetivos del SGSIP. Los objetivos de seguridad y privacidad de la información se establecen, documentan y comunican, estando alineados con los objetivos del negocio y considerando los requisitos legales y regulatorios aplicables. La planificación para alcanzar estos objetivos implica definir las acciones, responsabilidades, plazos y recursos necesarios, tal y como se detalla en el Manual del Sistema de Gestión de Seguridad de la Información y Privacidad (MAN.SI.001). Estos objetivos deben reflejar la protección de la confidencialidad, la garantía de la integridad y la disponibilidad de la información, así como el cumplimiento de los principios de privacidad.
- Planificación de Servicios: El Grupo Atento realiza la planificación de los servicios de TI que soportan el negocio, considerando la seguridad y privacidad de la información. La alta dirección analiza periódicamente el desempeño del SGSIP, considera los riesgos y oportunidades para proponer planes de acción y mejoras cuando

sea necesario, asegurando la continuidad de los servicios y el mantenimiento de un nivel adecuado de seguridad y privacidad. Los detalles sobre la planificación y el control operacional se describen en MAN.SI.001. Esta planificación debe asegurar la disponibilidad de los servicios y la integridad de la información gestionada por ellos.

Esta planificación es dinámica y se revisa y actualiza periódicamente para garantizar su eficacia y alineación con los cambios en el entorno empresarial, los requisitos legales y regulatorios, y la seguridad de la información y las amenazas cibernéticas. La claridad en los principios de seguridad, como la confidencialidad de la información sensible tratada nos servicios de TI, la integridad de los datos del negocio soportados por estos servicios, y la disponibilidad de los mismos para las operaciones, debe ser una consideración primordial en esta planificación.

8. CONTROLES DE SEGURIDAD

El Grupo Atento implementa y mantiene controles de Seguridad de la Información y Ciberseguridad para garantizar la confidencialidad, integridad y disponibilidad de la información, de acuerdo con los principios establecidos en esta política y con las leyes y regulaciones aplicables. El Grupo Atento está comprometido con la implementación de controles de seguridad que aborden, entre otras, las siguientes áreas:

- Controles de acceso: Asegúrese de que el acceso a la información y a los activos de información esté autorizado y restringido a los usuarios, procesos o dispositivos autorizados. Los detalles sobre los controles de acceso se definen en documentos normativos específicos, como POL. SI.005 - Control de Acceso - propuesto y NOR.SI.011 - Norma de Gestión de Contraseñas, según se referencia en el Manual SGSIP (MAN.SI.001).
- Gestión de vulnerabilidades: identifique, analice y aborde las vulnerabilidades de seguridad en sistemas y aplicaciones. Los procedimientos para la gestión de vulnerabilidades se detallan en NOR. SI.020.V01.ESP - Norma de Gestión de Vulnerabilidad y Aplicación de Patch e no Manual do SGSIP (MAN.SI.001).
- Protección contra malware: implemente medidas para proteger los sistemas del software malicioso. NOR. SI.018.V01.ESP - El Estándar Global de Prevención de Antivirus y Malware detalla las medidas de protección contra malware.
- Seguridad de red: Proteja la infraestructura de red contra accesos no autorizados y amenazas. NOR.SI.016.V01.ESP - Norma de Gestión de Firewalls y NOR.SI.063 - Norma de Filtro de Contenido Estándar establecen los requisitos para la seguridad de la red.
- Cifrado: Utilizar la criptografía para proteger la confidencialidad e integridad de la información en tránsito y en reposo. NOR.SI.023 - Normativa para el Uso de Criptografía define las pautas para el uso de la criptografía.
- Copia de seguridad y restauración: Realice copias de seguridad periódicas y pruebe la capacidad de restauración para garantizar la disponibilidad de la información en caso de incidentes. NOR.SI.012 - Norma de Respaldo y Restauración de la Información detalla los procedimientos de copia de seguridad y restauración.
- Clasificación de la información: Clasifique la información de acuerdo con su nivel de sensibilidad e implemente controles de seguridad adecuados para cada nivel. NOR.SI.036 - Norma de Clasificación de la Información establece los criterios para clasificar la información.
- Gestión de incidentes de seguridad y privacidad de la información: establezca procesos para identificar, analizar, responder y recuperarse de incidentes de seguridad y privacidad. NOR.SI.009 - Norma de Gestión de Incidentes de Seguridad de la Información y Cibernéticos detalla los procesos de gestión de incidentes.
- Concientización sobre la seguridad de la información y la privacidad: Promover la concientización y capacitación de los empleados sobre los riesgos de seguridad y privacidad de la información y sus responsabilidades. Los detalles sobre la concienciación se tratan en la sección 9.3 del Manual SGSIP (MAN.SI.001).
- Seguridad física y ambiental: Implementar controles para proteger las instalaciones físicas y el entorno de TI. Las prácticas de seguridad física se definen en documentos normativos internos.
- Protección de Datos Personales: Implementar medidas para garantizar la protección y privacidad de los datos personales en cumplimiento de las regulaciones aplicables.

- Seguridad e información propietaria: Defina reglas de seguridad para dispositivos móviles y informáticos que se conectan a la red interna.
- Uso aceptable e inaceptable: Establecer condiciones de uso aceptable y actividades prohibidas, como infracciones de derechos de autor, intercambio inseguro de archivos e introducción de código malicioso en la red.
- Gobierno y Uso Responsable de Inteligencia Artificial: El Grupo Atento está comprometido con el desarrollo, la implementación y el uso responsable de sistemas de Inteligencia Artificial (IA). Para lograrlo, la organización asegura que la IA sea gestionada de manera ética, transparente y segura, con el objetivo de minimizar riesgos como sesgos, impactos no deseados en individuos y la sociedad. Esto incluye el compromiso con la supervisión humana donde sea necesario.
- El Grupo Atento establecerá y mantendrá un Sistema de Gestión de IA (AIMS), alineado con los principios de la ISO/IEC 42001:2023 (Tecnología de la información — Inteligencia artificial — Sistema de gestión). Este sistema integrará la gestión de los riesgos y oportunidades específicos de la IA con el Sistema de Gestión de Seguridad de la Información (SGSI), reforzando la protección de la confidencialidad, integridad y disponibilidad de la información y garantizando la calidad de los datos utilizados en los sistemas de IA. Las directrices y procedimientos detallados para el desarrollo, la implementación y el uso responsable de la IA en Atento se encuentran definidos.

Los detalles específicos para la implementación y gestión de estos controles se definen en políticas, normativas y procedimientos complementarios, que forman parte del Sistema de Gestión de la Seguridad de la Información y la Privacidad (SGSIP) del Grupo Atento, tal y como se detalla en el Manual SGSIP (MAN.SI.001).

9. CONCIENCIACIÓN Y COMUNICACIÓN

El Grupo Atento promueve programas periódicos de concienciación para garantizar que todos los empleados, terceros y otros grupos de interés conozcan la política de seguridad de la información y sus responsabilidades. La comunicación de la política y la información relevante sobre seguridad de la información se lleva a cabo a través de diversos canales.

10. EVALUACIÓN DEL DESEMPEÑO

El desempeño del SGSI se monitorea, mide, analiza y evalúa continuamente. Esto incluye el seguimiento de los objetivos de seguridad de la información, el análisis de incidentes, los resultados de las auditorías internas y el análisis crítico por parte de la alta dirección.

Periódicamente se realizan auditorías internas para verificar el cumplimiento de los requisitos de la SGSI y de la presente política. Los resultados se informan para acciones correctivas y mejoras.

El personal directivo superior lleva a cabo exámenes críticos del sistema de gestión de la información a intervalos planificados para garantizar su pertinencia, suficiencia y eficacia continuas.

11. MEJORA

El Grupo Atento está comprometido con la mejora continua de la adecuación, suficiencia y eficacia del SGSI. Las no conformidades se abordan con acciones correctivas para eliminar sus causas y evitar que se repitan. Las oportunidades de mejora se evalúan constantemente.

12. CUMPLIMENTO Y SANCIONES

El incumplimiento de los requisitos establecidos en esta Política, así como de cualquiera de las normas, procedimientos o directrices operativas derivadas de ella, dará lugar a la aplicación de medidas disciplinarias. El Grupo Atento considera la seguridad de la información como una prioridad fundamental, y cualquier violación de las políticas y normativas aquí establecidas expone a la empresa a riesgos sustanciales.

Las medidas disciplinarias podrán incluir la terminación del contrato, sin perjuicio de otras acciones laborales o legales que correspondan. Toda violación intencional de esta Política o cualquier infracción cometida con el propósito, intención o efecto de cometer fraude se considerará un factor agravante y podrá resultar en la terminación inmediata del empleo.

Además de las consecuencias relacionadas con el empleo, las infracciones de esta Política pueden dar lugar a que Atento busque recursos penales y/o civiles en virtud de las leyes y reglamentos aplicables. La imposición de acciones correctivas no es un recurso exclusivo, y Atento puede ejercer todos los derechos y recursos legales sin perjuicio de las decisiones relacionadas con el empleo.

La aplicación de estas medidas se realizará conforme a los lineamientos y la metodología establecida en el PRO.SI.002 - Procedimiento de Sanciones de Seguridad de la Información del Grupo Atento, garantizando un proceso justo, transparente y coherente en todas las operaciones globales.

13. GESTIÓN DE PROVEEDORES

Los proveedores y prestadores de servicios deben cumplir con las premisas de seguridad de la información del Grupo Atento, definidas en esta política y en otros documentos relevantes. Se establecen acuerdos de confidencialidad cuando es necesario.

14. EXCEPCIONES

Todas y cada una de las excepciones a esta política deben ser revisadas, evaluadas y aprobadas por el área de Seguridad de la Información, con la autorización final del CISO Global y CIO.

15. VERSIÓN

Versión	Fecha	Reviso	Modificaciones
01	08/25	CISO GLOBAL	Creación