ATENTO

Sim, as políticas e procedimentos são nossa **responsabilidade**

POL.SI.001.V05.POR

Política de Segurança da Informação e Cibernética

Versão 05

08/25

#PolíticasQueNosOrientam

Sumário

1. OBJETIVO

A presente Política de Informação e Cibersegurança estabelece os princípios e diretrizes de alto nível para a proteção dos recursos informáticos e tecnológicos do Grupo Atento, servindo como documento central do Sistema de Gestão de Segurança da Informação e Privacidade (SGSIP). O propósito desta política é assegurar a confidencialidade, integridade e disponibilidade da informação, bem como o uso aceitável e seguro dos recursos tecnológicos, em conformidade com as melhores práticas e requisitos legais e regulatórios, incluindo a ABNT NBR ISO/IEC 27001, e em alinhamento com os objetivos estratégicos do Grupo Atento.

2. CONTEXTO DA ORGANIZAÇÃO

O Grupo Atento reconhece a importância crítica da segurança da informação, da privacidade dos dados e do uso adequado e seguro de seus recursos tecnológicos para a sustentabilidade do negócio e a proteção dos interesses de seus stakeholders. A organização opera em um ambiente dinâmico, realizando análise contínua dos contextos interno e externo, que podem impactar e gerar mudanças, bem como oportunidades para o Sistema de Gestão de Segurança da Informação e Privacidade (SGSIP).

Neste contexto, destaca-se a crescente dependência dos sistemas de informação e das infraestruturas tecnológicas para a prestação dos serviços que suportam o negócio do Grupo Atento. O uso eficaz e responsável desses recursos é essencial para garantir a confidencialidade, integridade e disponibilidade da informação processada e armazenada, além de mitigar os riscos associados ao uso inadequado ou malicioso da tecnologia.

A análise do contexto organizacional também considera as expectativas de clientes, parceiros, órgãos reguladores e demais partes interessadas em relação à segurança da informação, à privacidade de dados pessoais e à integridade dos processos que dependem de recursos tecnológicos confiáveis, utilizados de forma ética e em conformidade com os padrões estabelecidos. Esta política, portanto, abrange tanto a proteção da informação quanto as diretrizes para o uso adequado dos recursos tecnológicos do Grupo Atento.

3. CAMPO DE APLICAÇÃO

Esta Política cobre todos os processos e sistemas de informação, equipamentos eletrônicos e informáticos, bem como os recursos de rede do Grupo Atento. Aplica-se, de forma ampla e sem restrições, a todos os recursos tecnológicos disponibilizados ou utilizados pelo Grupo Atento, incluindo, entre outros: equipamentos de informática, softwares, sistemas operacionais, meios de armazenamento, contas de rede nominais e de serviço, correio eletrônico, navegação na web e transmissão de dados.

Esta Política aplica-se a todas as áreas do Grupo Atento, bem como a todos os colaboradores (permanentes ou temporários), prestadores de serviços, consultores, clientes e demais parceiros que interajam com os processos, sistemas de informação ou recursos tecnológicos do Grupo Atento.

O objetivo deste campo de aplicação é assegurar que todas as pessoas e todos os ativos de informação e tecnologia dentro do ecossistema do Grupo Atento estejam sujeitos às diretrizes estabelecidas nesta Política de Informação e Cibersegurança, consolidando em um único documento normativo as responsabilidades e controles para a proteção da informação e o uso adequado dos recursos tecnológicos.

Em resume, esta política aplica-se a:

- Todos os processos do Grupo Atento.
- Todos os sistemas de informação do Grupo Atento.
- Todos os recursos tecnológicos que sejam propriedade, utilizados ou disponibilizados pelo Grupo Atento.
- Todos os colaboradores do Grupo Atento.
- Todos os prestadores de serviços que tenham acesso à informação ou aos sistemas do Grupo Atento.

- Consultores, clientes e demais parceiros que interajam com os recursos tecnológicos, sistemas de informação ou processos do Grupo Atento.

4. REFERÊNCIAS

Esta Política está integrada ao Sistema de Gestão de Segurança e Privacidade da Informação (SGSIP) e faz referência aos seguintes documentos de alto nível:

- ISO/IEC 27001:2022
- ISO/IEC 42001:2023
- MAN.SI.001 – Manual do Sistema de Gestão de Segurança da Informação
- POL.LEG.012 – Política Global de Privacidade
- POL.ITD.004 – Política de Uso Responsável de IA
- Real Decreto 311/2022, de 3 de maio – que regulamenta o Esquema Nacional de Segurança (ENS).
- Lei Orgânica 3/2018, de 5 de dezembro – de Proteção de Dados Pessoais e Garantia dos Direitos Digitais (LOPDGDD).
- Regulamento (UE) 2016/679, de 27 de abril de 2016 – Regulamento Geral de Proteção de Dados (GDPR).
- Lei 6/2020, de 11 de novembro – reguladora de determinados aspectos dos serviços eletrônicos de confiança.
- Lei 34/2002, de 11 de julho – de Serviços da Sociedade da Informação e de Comércio Eletrônico (LSSI).
- Lei 9/2014, de 9 de maio – de Telecomunicações.

Outros documentos normativos, como normas, procedimentos e políticas específicas, complementam esta Política e encontram-se referenciados no Manual do SGSIP (MAN.SI.001) e em registros relacionados.

5. PRINCIPIOS DE CIBERSEGURIDAD

O Grupo Atento adota os seguintes princípios fundamentais para a gestão da informação e da cibersegurança, que servem como base para todas as medidas de segurança implementadas:

- Segurança da Informação como Processo Integral: Conjunto de práticas e processos implementados para proteger os ativos de informação do Grupo Atento. Abrange os princípios fundamentais de confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade, constituindo a base para todas as medidas de segurança adotadas para mitigar riscos e garantir a continuidade do negócio. Este princípio está intrinsecamente ligado aos objetivos de segurança e privacidade mencionados na seção 7 desta Política e detalhados no Manual do Sistema de Gestão de Segurança da Informação e Privacidade (MAN.SI.001 – Manual do Sistema de Gestão de Segurança da Informação). Consideramos a segurança como parte da operação habitual, aplicando-a desde a concepção inicial dos sistemas TIC e ao longo de todo o seu ciclo de vida.
- Confidencialidade: Garantir que a informação seja acessível apenas a entidades autorizadas. Isso é obtido mediante a implementação de controles de acesso (definidos na POL.SI.005 – Política de Controle de Acessos) e da proteção de senhas (NOR.SI.011 – Norma de Gestão de Senhas), assegurando que apenas o pessoal autorizado possa acessar dados sensíveis. Exemplo prático: assegurar que dados de clientes e informações internas confidenciais não sejam acessados por pessoas não autorizadas, permitindo que os agentes de atendimento acessem apenas a informação necessária ao seu trabalho.
- Integridade: Garantir a exatidão e integridade da informação e dos métodos de processamento, protegendo-os contra modificações não autorizadas ou acidentais. Isso implica assegurar que os dados permaneçam precisos, completos e confiáveis durante todo o seu ciclo de vida. Medidas como a “Gestão de Vulnerabilidades” (NOR.SI.020 – Norma de Gestão de Vulnerabilidades e Aplicação de Patches) e os controles de mudança contribuem para este princípio. Exemplo prático: assegurar que os registros de atendimento ao cliente e as configurações dos sistemas não sejam alterados de forma indevida ou não autorizada.
- Disponibilidade: Garantir que a informação e os sistemas estejam acessíveis e utilizáveis pelas entidades autorizadas sempre que necessário. Este princípio se apoia em práticas como a NOR.SI.012 – Norma de Backup e Restauração da Informação e em planos de continuidade de negócios, assegurando a continuidade das operações em caso de incidentes. Exemplo prático: manter os sistemas de atendimento ao cliente e as plataformas de comunicação acessíveis sempre que necessário para as operações da empresa.

- Autenticidade: Garantir a veracidade e a legitimidade de uma entidade — seja uma pessoa, um processo ou um sistema —, bem como a confiabilidade da fonte de onde procedem os dados. Este princípio é essencial para confiar na identidade dos usuários e na origem da informação.
- Rastreabilidade: Garantir que as ações de uma entidade ou pessoa nos sistemas e sobre a informação possam ser atribuídas exclusivamente a essa entidade ou pessoa. Isso é viabilizado por meio do registro detalhado de atividades e eventos, permitindo a reconstrução de ações para fins de auditoria e responsabilização.
- Privacidade (Proteção de Dados Pessoais): Aplicar as leis, normas e regulamentos vigentes no país onde os dados pessoais são tratados, incluindo de forma destacada o Regulamento Geral de Proteção de Dados (GDPR) e a Lei Orgânica de Proteção de Dados Pessoais e Garantia dos Direitos Digitais (LOPDGDD), na Espanha. Garante-se a proteção dos dados pessoais de empregados, clientes e fornecedores, bem como a obtenção dos consentimentos necessários e a implementação de medidas de segurança adequadas.
- Uso Responsável dos Recursos Tecnológicos: Utilizar os recursos tecnológicos do Grupo Atento de maneira ética, legal e em conformidade com as políticas da empresa, conforme estabelecido na Norma Global de Utilização Aceitável de Recursos Tecnológicos (NOR.SI.019). Este princípio é fundamental para prevenir incidentes de segurança, proteger a informação e evitar o uso indevido dos ativos da empresa. Exemplo prático: utilizar os computadores e a rede do Grupo Atento exclusivamente para fins profissionais, em conformidade com as políticas da empresa, evitando a instalação de softwares não autorizados ou o acesso a sites maliciosos (conforme detalhado na NOR.SI.019).
- Controle de Acesso Robusto, Incluindo a Gestão de Senhas: Um aspecto essencial da segurança da informação é a implementação de controles de acesso robustos para garantir que apenas usuários, processos ou dispositivos autorizados possam acessar a informação e os ativos de informação. Isso inclui a gestão eficaz de senhas, que devem ser robustas e administradas de acordo com a Norma de Gestão de Senhas (NOR.SI.011). Os requisitos detalhados para a gestão de acessos lógicos estão definidos na Norma de Controle de Acessos (NOR.SI.005), que estabelece os processos de solicitação, aprovação, concessão, revogação, modificação e revisão de contas de usuário.
- Determinação do Nível de Segurança Requerido: A organização determinará o nível de segurança exigido para cada sistema de informação, em conformidade com os marcos regulatórios nacionais aplicáveis, como o disposto no artigo 40 do Real Decreto 311/2022, que regulamenta o Esquema Nacional de Segurança (ENS) na Espanha, e os critérios gerais estabelecidos em seu Anexo I. Essa determinação será baseada na avaliação do impacto sobre as dimensões de segurança (Confidencialidade, Integridade, Disponibilidade, Autenticidade e Rastreabilidade), utilizando metodologias alinhadas com frameworks nacionais relevantes, como o guia CCN-STIC 803 para categorização de sistemas.
- Governança e Uso Responsável da Inteligência Artificial (IA): O Grupo Atento está comprometido com o desenvolvimento, a implementação e o uso responsável de sistemas de Inteligência Artificial. Para isso, a organização assegura que a IA seja gerida de forma ética, transparente e segura, com o objetivo de minimizar riscos como vieses, impactos indesejados em indivíduos e na sociedade. Isso inclui o compromisso com supervisão humana sempre que necessário. O Grupo Atento estabelecerá e manterá um Sistema de Gestão de IA (AIMS), alinhado aos princípios da ISO/IEC 42001:2023 (Tecnologia da Informação — Inteligência Artificial — Sistema de Gestão). Esse sistema integrará a gestão de riscos e oportunidades específicos da IA ao Sistema de Gestão de Segurança da Informação (SGSI), reforçando a proteção da confidencialidade, integridade e disponibilidade da informação e garantindo a qualidade dos dados utilizados nos sistemas de IA. As diretrizes e os procedimentos detalhados para o desenvolvimento, a implementação e o uso responsável de IA na Atento estão definidos na POL.ITD.004 – Política de Uso Responsável de IA.

6. LIDERANÇA

A alta direção do Grupo Atento demonstra seu firme compromisso com a segurança da informação e a cibersegurança por meio do estabelecimento, implementação, manutenção e melhoria contínua do Sistema de Gestão de Segurança da Informação (SGSI). Esse compromisso se manifesta na definição desta Política de Informação e Cibersegurança, na alocação dos recursos necessários e na comunicação constante da importância crítica da segurança da informação a todos os colaboradores e partes interessadas.

As responsabilidades e autoridades organizacionais em matéria de segurança da informação são definidas e comunicadas de forma clara em toda a organização, assegurando uma abordagem multidisciplinar e a participação

ativa na proteção dos ativos de informação. Os detalhes específicos das funções, responsabilidades e autoridades relacionadas à segurança da informação — incluindo papéis e expectativas associadas — encontram-se estabelecidos nas descrições de cargos correspondentes e detalhados no Manual do Sistema de Gestão de Segurança da Informação e Privacidade (MAN.SI.001).

A liderança, em todos os níveis da organização, é responsável por garantir o estrito cumprimento desta Política, bem como dos padrões, procedimentos e demais documentos normativos de segurança da informação dentro de suas respectivas áreas de especialização e responsabilidade.

7. PLANEJAMENTO

O Grupo Atento estabelece, implementa e mantém o planejamento necessário para alcançar os objetivos de segurança e privacidade da informação, em conformidade com esta Política. Esse planejamento abrange os seguintes elementos-chave:

- Ações para tratar riscos e oportunidades: O Grupo Atento, por meio de seu planejamento estratégico e mapa de processos, compreende os cenários internos e externos e realiza avaliações periódicas do Sistema de Gestão de Segurança da Informação e Privacidade (SGSIP). Essa análise permite identificar e avaliar periodicamente os riscos nos ativos de informação e as oportunidades inerentes aos processos que compõem o SGSIP. Os detalhes sobre o processo de avaliação e tratamento de riscos, incluindo a metodologia utilizada e os controles implementados, estão definidos em documentos normativos específicos. É essencial que esse planejamento considere os princípios de confidencialidade, integridade e disponibilidade discutidos na seção 5 desta Política.
- Objetivos de segurança e privacidade da informação e planejamento para alcançá-los: A alta direção, por meio do planejamento estratégico, considera os cenários internos e externos e as expectativas de suas partes interessadas para determinar os objetivos do SGSIP. Esses objetivos são estabelecidos, documentados e comunicados, estando alinhados com os objetivos do negócio e considerando os requisitos legais e regulatórios aplicáveis. O planejamento para alcançar esses objetivos implica definir ações, responsabilidades, prazos e recursos necessários, conforme detalhado no Manual do Sistema de Gestão de Segurança da Informação e Privacidade (MAN.SI.001). Esses objetivos devem refletir a proteção da confidencialidade, a garantia da integridade e a disponibilidade da informação, bem como o cumprimento dos princípios de privacidade.
- Planejamento de serviços: O Grupo Atento realiza o planejamento dos serviços de TI que suportam o negócio, considerando a segurança e a privacidade da informação. A alta direção analisa periodicamente o desempenho do SGSIP, considera riscos e oportunidades e propõe planos de ação e melhorias quando necessário, assegurando a continuidade dos serviços e a manutenção de um nível adequado de segurança e privacidade. Os detalhes sobre o planejamento e o controle operacional estão descritos no MAN.SI.001. Esse planejamento deve garantir a disponibilidade dos serviços e a integridade da informação gerida por eles.

Esse planejamento é dinâmico e é revisto e atualizado periodicamente para garantir sua eficácia e alinhamento com as mudanças no ambiente empresarial, nos requisitos legais e regulatórios e nas ameaças à segurança da informação e cibernética. A clareza dos princípios de segurança — como a confidencialidade da informação sensível tratada nos serviços de TI, a integridade dos dados do negócio suportados por esses serviços e a disponibilidade para as operações — deve ser uma consideração primordial nesse planejamento.

8. CONTROLES DE SEGURANÇA

O Grupo Atento implementa e mantém controles de Segurança da Informação e Cibersegurança para garantir a confidencialidade, integridade e disponibilidade da informação, em conformidade com os princípios estabelecidos nesta Política e com as leis e regulações aplicáveis. O Grupo Atento está comprometido com a implementação de controles que abrangem, entre outras, as seguintes áreas:

- Controles de acesso: assegurar que o acesso à informação e aos ativos de informação esteja autorizado e restrito a usuários, processos ou dispositivos autorizados. Os detalhes estão definidos em documentos normativos específicos, como a POL.SI.005 – Política de Controle de Acesso e a NOR.SI.011 – Norma de Gestão de Senhas, conforme referenciado no Manual SGSIP (MAN.SI.001).

- Gestão de vulnerabilidades: identificar, analisar e tratar vulnerabilidades de segurança em sistemas e aplicações. Os procedimentos estão definidos na NOR.SI.020 – Norma de Gestão de Vulnerabilidades e Aplicação de Patches e no Manual SGSIP (MAN.SI.001).
- Proteção contra malware: implementar medidas para proteger os sistemas contra software malicioso. A NOR.SI.018 – Norma Global de Prevenção de Vírus e Malware detalha as medidas de proteção.
- Segurança de rede: proteger a infraestrutura de rede contra acessos não autorizados e ameaças. A NOR.SI.016 – Norma de Gestão de Firewalls e a NOR.SI.063 – Norma de Filtro de Conteúdo estabelecem os requisitos aplicáveis.
- Criptografia: utilizar criptografia para proteger a confidencialidade e integridade da informação em trânsito e em repouso. A NOR.SI.023 – Norma para o Uso de Criptografia define as diretrizes.
- Backup e restauração: realizar cópias de segurança periódicas e testar a restauração para garantir a disponibilidade da informação em caso de incidentes. A NOR.SI.012 – Norma de Backup e Restauração da Informação detalha os procedimentos.
- Classificação da informação: classificar a informação de acordo com seu nível de sensibilidade e implementar controles adequados. A NOR.SI.036 – Norma de Classificação da Informação define os critérios.
- Gestão de incidentes de segurança e privacidade: estabelecer processos para identificar, analisar, responder e recuperar-se de incidentes. A NOR.SI.009 – Norma de Gestão de Incidentes de Segurança da Informação e Cibernéticos detalha os processos.
- Conscientização em segurança da informação e privacidade: promover programas de conscientização e capacitação dos colaboradores sobre riscos e responsabilidades. Os detalhes estão descritos na seção 9.3 do Manual SGSIP (MAN.SI.001).
- Segurança física e ambiental: implementar controles para proteger as instalações físicas e o ambiente de TI. Essas práticas estão definidas em documentos normativos internos.
- Proteção de dados pessoais: implementar medidas para garantir a proteção e privacidade dos dados pessoais em conformidade com as regulamentações aplicáveis.
- Segurança da informação proprietária: definir regras de segurança para dispositivos móveis e equipamentos que se conectem à rede interna.
- Uso aceitável e inaceitável: estabelecer condições de uso aceitável e atividades proibidas, incluindo violações de direitos autorais, compartilhamento inseguro de arquivos e introdução de código malicioso na rede.
- Governança e uso responsável de Inteligência Artificial: o Grupo Atento compromete-se com o desenvolvimento, implementação e uso responsável da IA, de forma ética, transparente e segura, com mitigação de riscos como vieses e impactos sociais indesejados. Inclui a supervisão humana quando necessária. O Grupo Atento estabelecerá e manterá um Sistema de Gestão de IA (AIMS) alinhado à ISO/IEC 42001:2023, integrando riscos e oportunidades específicos da IA ao SGSI.

Os detalhes específicos para a implementação e gestão desses controles encontram-se descritos em políticas, normas e procedimentos complementares, que fazem parte do SGSIP do Grupo Atento, conforme detalhado no Manual SGSIP (MAN.SI.001).

9. CONSCIENTIZAÇAO E COMUNICAÇÃO

O Grupo Atento promove programas periódicos de conscientização para garantir que todos os colaboradores, terceiros e demais partes interessadas conheçam esta Política de Segurança da Informação e suas responsabilidades. A comunicação da Política e de informações relevantes é realizada por meio de diversos canais.

10. AVALIAÇÃO DE DESEMPENHO

O desempenho do SGSI é monitorado, medido, analisado e avaliado continuamente. Isso inclui o acompanhamento dos objetivos de segurança da informação, a análise de incidentes, os resultados das auditorias internas e a revisão crítica pela alta direção.

Auditorias internas são realizadas periodicamente para verificar o cumprimento dos requisitos do SGSI e desta Política. Os resultados são reportados para ações corretivas e melhorias.

A alta direção conduz revisões críticas do SGSI em intervalos planejados, assegurando sua pertinência, suficiência e eficácia contínuas.

11. MELHORIA

O Grupo Atento está comprometido com a melhoria contínua da adequação, suficiência e eficácia do SGSI. Não conformidades são tratadas com ações corretivas para eliminar suas causas e evitar recorrências. Oportunidades de melhoria são constantemente avaliadas.

12. CONFORMIDADE E SANSÕES

O descumprimento dos requisitos estabelecidos nesta Política, bem como de quaisquer normas, procedimentos ou diretrizes operacionais dela derivados, resultará na aplicação de medidas disciplinares. O Grupo Atento considera a segurança da informação como prioridade fundamental, e qualquer violação das políticas e normas aqui estabelecidas expõe a empresa a riscos significativos.

As medidas disciplinares poderão incluir a rescisão do contrato de trabalho, sem prejuízo de outras ações trabalhistas ou legais aplicáveis. Qualquer violação intencional desta Política ou infração cometida com o propósito, intenção ou efeito de fraude será considerada um fator agravante e poderá resultar na rescisão imediata do vínculo empregatício.

Além das consequências trabalhistas, violações desta Política podem resultar em medidas cíveis e/ou criminais conforme legislação aplicável. A aplicação de ações corretivas não é exclusiva, e o Grupo Atento poderá exercer todos os direitos legais disponíveis, sem prejuízo das decisões relacionadas ao vínculo de trabalho.

A aplicação destas medidas será realizada de acordo com as diretrizes estabelecidas no PRO.SI.002 – Procedimento de Sanções de Segurança da Informação do Grupo Atento, garantindo um processo justo, transparente e consistente em todas as operações globais.

13. GESTÃO DE FORNECEDORES

Os fornecedores e prestadores de serviços devem cumprir os requisitos de segurança da informação do Grupo Atento, definidos nesta Política e em outros documentos relevantes. Acordos de confidencialidade são estabelecidos quando necessário.

14. EXCEÇÕES

Todas e quaisquer exceções a esta Política devem ser revisadas, avaliadas e aprovadas pela área de Segurança da Informação, com autorização final do CISO Global e do CIO.

15. VERSÃO

Versão	Data	Revisor	Modificações
01	08/25	CISO GLOBAL	Criação