ATENTO

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

POL.SI.002.V04.POR

Política Corporativa de Cibersegurança - Pública

Versão 04

11/24

#PolíticasQueNosOrientam

Sumário

1. OBJETIVO

O propósito desta Política é proteger os ativos de informação da organização, garantindo disponibilidade, integridade, confidencialidade, autenticidade e rastreabilidade, bem como as infraestruturas, sistemas e recursos humanos que os processam, gerenciam, transmitem e armazenam, em conformidade com os requisitos de negócios e obrigações legais e contratuais aplicáveis.

2. ÂMBITO DE APLICAÇÃO

Esta Política de Segurança da Informação aplica-se a todas as pessoas, sistemas e meios que acessam, tratam, armazenam, transmitem ou utilizam informações conhecidas, gerenciadas ou de propriedade da Atento para qualquer uma de suas atividades ao longo do ciclo de vida, incluindo criação, captura, recebimento, transmissão, visualização, classificação, retenção e eliminação.

O pessoal sujeito a esta política inclui todas as pessoas com acesso às informações mencionadas, independentemente do suporte automatizado em que estão contidas e se o indivíduo é ou não um funcionário da Atento. Portanto, aplica-se também a contratados, clientes, fornecedores ou qualquer terceiro que tenha acesso às informações ou aos sistemas da empresa.

As diretrizes contidas nesta Política serão desenvolvidas em procedimentos, instruções técnicas e guias, de acordo com o Marco Normativo de Cibersegurança.

3. DOCUMENTO DE REFERÊNCIA

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

4. TERMINOLOGIA

Termo	Definição
Ativo	Qualquer informação ou elemento que possui valor para a organização.
Análise de risco	Uso sistemático da informação para identificar fontes e estimar o risco.
Adaptabilidade	Define os eventos e sob quais critérios um sistema deve ser monitorado e revisado para controle posterior.
Autenticidade	Busca assegurar a validade da informação em tempo, forma e distribuição. Garante também a origem da informação, validando o emissor para evitar suplantação de identidade.
Confiabilidade da informação	Garante que a fonte da informação gerada seja adequada para sustentar a tomada de decisões e a execução das missões e funções.
Confidencialidade	Propriedade que determina que a informação não esteja disponível nem seja revelada a indivíduos, entidades ou processos não autorizados.
Declaração de aplicabilidade	Documento que descreve os objetivos de controle e os controles pertinentes e aplicáveis a este.
Disponibilidade	Propriedade de que a informação seja acessível e utilizável por solicitação de uma entidade.
Avaliação de risco	Processo de comparar o risco estimado contra critérios de risco dados, para determinar a importância do risco.

Termo	Definição
Evento de segurança da informação	Presença identificada de uma condição de um sistema, serviço ou rede, que indica uma possível violação da política de segurança da informação, falha das salvaguardas, ou uma situação desconhecida previamente que pode ser pertinente à segurança.
Gestão de risco	Atividades coordenadas para dirigir e controlar uma organização em relação ao risco.
Incidente de segurança da informação	Um evento ou série de eventos de segurança da informação não desejados ou inesperados, que têm uma probabilidade significativa de comprometer as operações do negócio e ameaçar a segurança da informação.
Integridade	Propriedade de salvaguardar a exatidão e o estado completo dos ativos.
Proteção à duplicação	Consiste em assegurar que uma transação seja realizada apenas uma vez, a menos que seja especificado o contrário. Impedir que uma transação seja gravada para depois reproduzi-la, com o objetivo de simular múltiplas solicitações do mesmo remetente original.
Recursos informáticos	Todos os componentes de hardware e programas (software) necessários para o bom funcionamento e otimização do trabalho com computadores e periféricos, tanto a nível individual, como coletivo ou organizacional, sem deixar de lado o bom funcionamento destes.
Risco	O efeito da incerteza sobre os objetivos.
Risco inerente	Nível de incerteza próprio de cada atividade, sem a execução de nenhum controle.
Risco residual	Nível restante de risco após o tratamento do risco.
Segurança da informação	Preservação da confidencialidade, integridade e disponibilidade da informação; pode envolver outras propriedades como autenticidade, rastreabilidade, não repúdio e confiabilidade.
Sistema de gestão da segurança da informação (SGSI)	Parte do sistema de gestão global, baseado em uma abordagem para os riscos globais de um negócio, cujo objetivo é estabelecer, implementar, operar, monitorar, revisar, manter e melhorar a segurança da informação.
Sistema de informação	Refere-se a um conjunto independente de recursos de informação organizados para a coleta, processamento, manutenção, transmissão e disseminação de informação de acordo com determinados procedimentos, tanto automatizados quanto manuais.
Tratamento do risco	Processo de seleção e implementação de ações de melhoria que permitam gerenciar o risco.
Avaliação do risco	Processo de análise e avaliação do risco.

5. DESENVOLVIMENTO

A presente Política Corporativa de Cibersegurança afeta toda a organização e expressa o compromisso da Direção de aprovar e apoiar as normativas e procedimentos de segurança necessários para a gestão da segurança da informação, com base nesta Política, na normativa legal vigente e nos requisitos dos clientes.

Com esse fim, o Grupo Atento assume os seguintes Objetivos Estratégicos de Cibersegurança:

- Considerar a informação e os sistemas que a suportam como ativos estratégicos, manifestando assim sua determinação em alcançar os níveis de segurança necessários que garantam sua proteção em relação à autenticação, confidencialidade, integridade, disponibilidade e rastreabilidade;
- Instaurar um Comitê de Segurança de Cibersegurança que gerenciará todas as diretrizes que permitam preservar, resguardar e fortalecer a segurança dos ativos de informação e assim melhorar a qualidade dos serviços oferecidos aos clientes;
- Promover a implementação dos níveis de segurança apropriados que permitam proteger tanto os recursos dos sistemas de informação e a informação processada, armazenada ou transmitida por eles, quanto garantir o cumprimento da legislação vigente na matéria, velando pela confidencialidade, integridade e disponibilidade da informação; além de gerenciar os incidentes de segurança que possam afetá-la;
- Promover ações de formação e conscientização sobre Cibersegurança direcionadas a todo o pessoal e garantir a divulgação da presente Política, assim como dos documentos que a desenvolvem;
- Criar um sistema de gestão da Cibersegurança baseado em padrões internacionais e códigos de boas práticas, para identificar, quantificar, priorizar, monitorar e tratar os riscos, bem como avaliar e revisar o desenvolvimento da Política de Cibersegurança como um quadro para definição das diretrizes básicas de segurança;
- Velar pela existência dos mecanismos necessários que assegurem a continuidade das atividades críticas da Atento diante de contingências graves que afetem os sistemas de informação, permitindo a recuperação destes em um período de tempo aceitável;
- Garantir o cumprimento da legislação e regulamentações vigentes em matéria de Cibersegurança.

Todo o pessoal da Atento (Colaboradores), assim como pessoas externas (Clientes, fornecedores e stakeholders), são obrigados a conhecer, respeitar e fazer cumprir, dentro de sua área de responsabilidade, as medidas de segurança estabelecidas para a proteção da informação.

O acesso à informação e aos sistemas de informação estará condicionado à adesão a esta Política e à normativa que a desenvolve, sendo estas de cumprimento obrigatório. O não cumprimento manifesto poderá acarretar o início das medidas disciplinares apropriadas e, quando necessário, responsabilidades legais.

6. RESPONSABILIDADES

O comitê executivo deve garantir que as responsabilidades e autoridades para os papéis relevantes à segurança da informação sejam atribuídos e comunicados.

O comitê executivo deve atribuir a responsabilidade e autoridade para:

- Assegurar que o Sistema de Gestão de Segurança da Informação seja desenvolvido de acordo com os padrões internacionais mais relevantes.
- Relatar o desempenho do Sistema de Gestão de Segurança da Informação.

7. HISTÓRICO DE REVISÃO

Versão	Data	Revisor	Modificações
01	04/22	Controles Internos	Versão Inicial
02	11/22	Mauricio Baroni / Yovanni Pineda	São adicionados os pontos 1, 2, 3, 4 e 6.
03	02/24	CISO Regionais e equipe de SI	Atualização de Texto
04	11/24	CISO Regionais e equipe de SI	Atualização de Texto