Política de Segurança da Informação Advance Telecom (versão 2.0)

CODIGO: PSI-AT-Ver.2.0 **DATA:** 24/09/2025 **VERSÃO:** 2.0

1. OBJETIVO

O presente documento estabelece a Política de Segurança da Informação (PSI) da Advance Telecom, reafirmando seu compromisso com a proteção das informações de sua propriedade e sob sua responsabilidade. Esta PSI visa estabelecer diretrizes corporativas que permitam a todos os colaboradores, parceiros e clientes seguirem padrões de comportamento relacionados à segurança da informação, adequados às necessidades de negócio, proteção legal e conformidade regulatória da empresa e do indivíduo. Esta política é guiada pelos conceitos e orientações das normas ABNT NBR ISO/IEC da família 27000, Lei Geral de Proteção de Dados (LGPD) e outras regulamentações aplicáveis.

2. ESCOPO

2.1. As diretivas desta política aplicam-se a todas as informações da Advance Telecom, em qualquer formato (físico ou digital), armazenadas, processadas ou transmitidas por qualquer meio, bem como a todos os sistemas, redes, equipamentos e instalações da empresa. Abrange todos os colaboradores (funcionários, terceiros, estagiários, consultores) e quaisquer outras partes interessadas que tenham acesso ou utilizem os ativos de informação da Advance Telecom.

2.2. A segurança da informação é aqui caracterizada pela preservação da:

Confidencialidade: Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

Integridade: Garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, acidentais ou intencionais.

Disponibilidade: Garantia de que os usuários autorizados obtenham acesso às informações e ativos associados quando necessário.

3. ALÇADA DE APROVAÇÃO E GOVERNANÇA

3.1. O Comitê de Gestão de Segurança da Informação (CGSCI), representado por membros da diretoria executiva, pelo Diretor de Tecnologia da Informação, Consultor de Segurança da Informação e outros representantes designados, é responsável pela aprovação, revisão e supervisão desta política, bem como das normas e procedimentos dela derivados.

3.2. A Área de Tecnologia da Informação (TI) é responsável pela manutenção, implementação e monitoramento das políticas e controles de Segurança da Informação, atuando como ponto central para a gestão operacional do SGSI.

3.3. A atualização desta política ocorrerá anualmente ou sempre que algum fato relevante motive sua revisão antecipada, como mudanças tecnológicas, regulatórias, incidentes de segurança significativos ou alterações nos objetivos de negócio. O processo de revisão incluirá a avaliação da eficácia dos controles e a adequação da política aos riscos atuais.

4. INTRODUÇÃO

A segurança da informação é considerada um assunto relevante e prioritário na Advance Telecom, sendo pauta obrigatória nos principais comitês e subcomitês da empresa. A gestão da segurança da informação é um processo contínuo e estratégico, essencial para a proteção dos ativos da empresa e para a manutenção da confiança de seus stakeholders.

5. DIRETRIZES GERAIS

Em relação à segurança da informação, as seguintes diretrizes serão cumpridas:

- Tratar de maneira ética e sigilosa as informações de clientes, parceiros, fornecedores e colaboradores, bem como informações de caráter confidencial e restritas à empresa.
- Capacitar tecnicamente e conscientizar constantemente as pessoas acerca do trato dainformação, promovendo uma cultura de segurança.
- Melhorar de maneira contínua os processos e os procedimentos com base nos mais altos padrões de segurança, através de monitoramento, auditorias e análise de

desempenho.

- Disseminar a Política de Segurança da Informação a todos os envolvidos na operação da empresa sejam eles funcionários, terceiros ou estagiários.
- Confirmar o entendimento da Política de Segurança da Informação por parte de todos os envolvidos no início de suas contratações e anualmente, ou todas as vezes que esta seja modificada.
- Investir continuamente em tecnologia e soluções de segurança da informação.
- Estabelecer e revisar periodicamente objetivos de segurança da informação alinhados aos objetivos de negócio, monitorando seu progresso através de métricas e indicadores de desempenho (KPIs).

6. GESTÃO DE ATIVOS E CLASSIFICAÇÃO DA INFORMAÇÃO

6.1. **Inventário de Ativos:** Será mantido um inventário completo e atualizado de todos os ativos de informação da Advance Telecom, incluindo hardware, software, informações (dados), serviços e infraestrutura. Cada ativo terá um proprietário definido, que será responsável por sua proteção e classificação.

6.2. **Classificação da Informação:** Todas as informações da Advance Telecom devem ser classificadas com base em sua sensibilidade, criticidade e requisitos legais/regulatórios. A classificação determinará os controles de segurança apropriados para cada tipo de informação. As categorias de classificação incluem, mas não se limitam a:

- **Público:** Conteúdo que pode ser distribuído a qualquer pessoa interna ou externa e é de conhecimento geral, sem restrições de acesso ou uso.

- **Somente Interno:** Conteúdo produzido pela Advance Telecom para conhecimento exclusivo de seus colaboradores, terceiros e fornecedores, com acesso restrito ao ambiente interno da empresa.

- **Confidencial:** Conteúdo sensível e de acesso restrito apenas a pessoas com necessidade de conhecer, cuja divulgação não autorizada poderia causar danos significativos à empresa ou a terceiros. Inclui dados pessoais sensíveis, informações financeiras estratégicas, segredos comerciais, etc.

6.3. **Rotulagem da Informação:** As informações devem ser rotuladas de acordo com sua classificação, tanto em formato digital quanto físico, para facilitar o

manuseio adequado e a aplicação dos controles de segurança correspondentes.

6.4. **Uso Aceitável de Ativos:** Serão definidas regras claras para o uso aceitável de todas as informações e outros ativos associados, garantindo que sejam utilizadosapenas para fins de negócio autorizados e em conformidade com as políticas internas e regulamentações.

7. CONTROLE DE ACESSO E AUTENTICAÇÃO

7.1. **Princípio do Menor Privilégio e Necessidade de Conhecer (Need to Know):** O acesso a informações, sistemas e recursos será concedido estritamente com base no princípio do menor privilégio e na necessidade de conhecer. Os usuários terão acesso apenas aos recursos essenciais para o desempenho de suas funções.

7.2. **Autenticação de Usuários:** O acesso ao ambiente de informações ocorrerá através de autenticação do usuário, que deverá ser pessoal e intransferível. As senhas deverão satisfazer os seguintes requisitos de complexidade:

- Não conter partes significativas do nome da conta do usuário ou o nome todo.
- Ter pelo menos 8 caracteres de comprimento (recomendado).
- Conter caracteres de três das quatro categorias a seguir: caracteres maiúsculos (A-Z), caracteres minúsculos (a-z), números (0-9) e caracteres especiais (ex.: !, $, #, %).
- Expirar a cada 90 dias (exceto para contas de sistema ou serviço com gestão de acesso privilegiado específica).
- Serem bloqueadas após 5 tentativas sem sucesso.
- Desbloquear através de ação do administrador do sistema.
- Não repetir as últimas 10 senhas utilizadas.
- Armazenar as senhas de forma criptografada.
- Trocar obrigatoriamente a senha inicial.

7.3. **Autenticação Multifator (MFA):** A autenticação multifator será obrigatória para acessos remotos, acessos privilegiados a sistemas críticos e para sistemas que armazenam ou processam informações confidenciais.

7.4. **Gestão de Acessos Privilegiados:** A gestão de acessos privilegiados (contas de

administradores, contas de serviço) será realizada de forma rigorosa, com senhas complexas e rotativas, monitoramento contínuo do uso dessas contas e revisão frequente dos privilégios concedidos.

7.5. **Segregação de Funções (SoD):** Serão identificados e gerenciados acessos considerados tóxicos que, se combinados, podem gerar conflitos de interesse. Caso o acesso seja necessário, a aprovação da área responsável deverá ser documentada e controles compensatórios implementados.

7.6. **Revisão de Acessos:** Todos os acessos concedidos serão revisados periodicamente, e obrigatoriamente no caso de mudança de função de um colaborador, para garantir que os privilégios de acesso estejam sempre alinhados às responsabilidades atuais.

7.7. **Registro de Autorizações:** As autorizações de acesso aos sistemas e informações serão devidamente registradas e documentadas.

8. SEGURANÇA FÍSICA E AMBIENTAL

8.1. **Controle de Acesso Físico:** O acesso a todas as áreas onde serão processadas ou armazenadas informações pertinentes à operação da empresa será restrito por controles físicos apropriados e proporcionais à criticidade dos equipamentos e informações. Listas de acesso serão mantidas e revisadas regularmente.

8.2. **Proteção de Áreas Seguras:** Escritórios, salas e instalações que contenham ativos de informação críticos serão protegidos contra acesso não autorizado, danos e interferências. Isso inclui o uso de crachás, biometria, câmeras de vigilância e registro de visitantes.

8.3. **Mesa Limpa e Tela Limpa:** Todos os colaboradores devem aderir à política de mesa limpa (não deixar documentos confidenciais expostos) e tela limpa (bloquear a estação de trabalho ao se ausentar) para proteger informações contra acesso visual não autorizado.

8.4. **Proteção contra Ameaças Físicas e Ambientais:** Serão implementadas medidas para proteger os ativos de informação contra ameaças físicas e ambientais, como incêndios, inundações, falhas de energia e desastres naturais.

9. SEGURANÇA DE OPERAÇÕES

9.1. **Uso de Equipamentos**: As estações de trabalho deverão estar sempre bloqueadas quando não estiverem sendo utilizadas, com bloqueio automático após um determinado período de inatividade, a ser estabelecido pela Área de Tecnologia da Informação. Todo e qualquer equipamento utilizado nas dependências da empresa deverá ser de conhecimento e consentimento da Área de Tecnologia da Informação.

9.2. **Uso do Correio Eletrônico e Mensagens Instantâneas**: São instrumentos de comunicação interna e externa para a realização apenas dos negócios da empresa. As mensagens devem ser escritas em linguagem profissional, não devendo comprometer a imagem e nem os princípios éticos da empresa. Somente softwares autorizados podem ser utilizados para troca de mensagens instantâneas que contenham informações internas ou sigilosas. As informações devem ser gravadas e mantidas pelo tempo definido na legislação e políticas de retenção.

9.3. **Uso da Internet**: O acesso à Internet será autorizado para os usuários que necessitarem exclusivamente para o desempenho de suas atividades profissionais. É vedada a instalação de programas provenientes da Internet nos computadores da empresa, sem expressa anuência da Área de Tecnologia da Informação. É vedada a visualização, transferência (downloads e/ou uploads), cópia ou qualquer outro tipo de acesso a sites de conteúdo inadequado ou ilegal, conforme diretrizes da empresa.

9.4. **Instalação e Utilização de Softwares**:

- Somente software homologado e autorizado pela Área de Tecnologia da Informação poderá ser instalado e utilizado.
- É proibido o uso de softwares ilegais ou em não conformidade com a licença de uso do software.

A Área de Tecnologia da Informação deverá estabelecer as diretrizes de controle, homologação e instalação de software, garantindo que todos os softwares estejam atualizados e com patches de segurança aplicados.

9.5. **Acesso Remoto**: O acesso remoto aos recursos computacionais deve ser

realizado adotando mecanismos de segurança robustos, como Redes Privadas Virtuais (VPNs) com criptografia forte e autenticação multifator, para evitar ameaças à integridade e sigilo do serviço. Dispositivos utilizados para acesso remoto devem estar protegidos com software de segurança atualizado.

9.6. **Cópias de Segurança (Backup)**: Os dados críticos da empresa serão copiados regularmente para local diferente de sua origem, com armazenamento seguro (preferencialmente em nuvem com fornecedor qualificado pela TI). Será definida uma política de retenção de mídias virtuais de cópia de segurança de acordo com o tipo de informação armazenada e a legislação vigente. Informações consideradas confidenciais serão armazenadas de modo criptografado.

Testes de restauração das cópias de segurança serão realizados periodicamente (no mínimo a cada 120 dias por amostragem) para garantir sua integridade e disponibilidade.

9.7. **Trilhas de Auditoria e Monitoramento**: Sistemas e rede corporativa devem manter trilhas de auditoria detalhadas, registrando login e logout dos usuários, bem como as ações executadas (inclusão, exclusão e alteração) nos sistemas utilizados na empresa. Os logs serão protegidos contra adulteração, retidos por um período definido e revisados periodicamente para identificar atividades suspeitas ou não autorizadas.

9.8. **Gestão de Vulnerabilidades e Testes de Invasão**: Serão realizadas varreduras de vulnerabilidades regulares e testes de invasão periódicos (Penetration Tests) por empresas especializadas em sistemas acessíveis via internet e sistemas críticos internos, para identificar e remediar proativamente as vulnerabilidades de segurança. Os resultados desses testes serão documentados e um plano de remediação será estabelecido e acompanhado.

10. SEGURANÇA NO DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

10.1. **Segurança no Ciclo de Vida do Desenvolvimento (SDLC)**: A segurança

será integrada em todas as fases do ciclo de vida do desenvolvimento de software, desde a concepção e design até a implementação, testes, implantação e manutenção. Isso inclui a definição de requisitos de segurança, design seguro, codificação segura e testes de segurança (incluindo testes de aceitação).

10.2. **Ambiente de Homologação**: Todas as alterações em sistemas de informação deverão ser homologadas pelos usuários em ambiente segregado do ambiente de produção. O ambiente de homologação não deverá conter dados de produção, exceto quando com anuência do proprietário do sistema e por tempo determinado, com os dados devidamente mascarados ou anonimizados e o uso registrado.

10.3. **Chaves de Criptografia e Certificados Digitais**: A gestão de chaves de criptografia e certificados digitais será realizada de forma segura, incluindo a guarda, registro, renovação, revogação e inutilização, com processos documentados. Serão utilizados algoritmos de criptografia fortes e, para chaves críticas, módulos de segurança de hardware (HSMs) serão considerados.

11. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

11.1. **Processo de Gestão de Incidentes**: Será estabelecido e mantido um processo formal de gestão de incidentes de segurança da informação, cobrindo as fases de detecção, análise, contenção, erradicação, recuperação e lições aprendidas. Todos os incidentes de segurança serão registrados, investigados e documentados.

11.2. **Comunicação de Incidentes**: Incidentes de segurança da informação serão comunicados internamente às partes interessadas relevantes e, quando aplicável (ex: vazamento de dados pessoais), externamente às autoridades competentes e aos titulares dos dados, conforme exigido pela LGPD e outras regulamentações.

11.3. **Processo Disciplinar:** Violações a esta política podem gerar advertência e até demissão, conforme a gravidade e o impacto do incidente. O processo disciplinar será justo, transparente e em conformidade com a legislação trabalhista.

12. CONSCIENTIZAÇÃO, EDUCAÇÃO E TREINAMENTO

12.1. **Programa de Conscientização**: Será mantido um programa contínuo de conscientização, educação e treinamento em segurança da informação para todos os colaboradores. O programa abordará tópicos como phishing, engenharia social, uso seguro da internet, proteção de dados pessoais, uso de senhas fortes e as responsabilidades individuais de segurança.

12.2. **Treinamento Específico**: Treinamentos específicos serão fornecidos para colaboradores com responsabilidades de segurança da informação ou que lidam com informações sensíveis, como desenvolvedores, administradores de sistema e equipes de atendimento ao cliente.

13. CONFORMIDADE LEGAL E REGULAMENTAR

13.1. **Requisitos Legais e Contratuais**: A Advance Telecom identificará e cumprirá todos os requisitos legais, estatutários, regulatórios e contratuais aplicáveis à segurança da informação, incluindo a Lei Geral de Proteção de Dados (LGPD).

13.2. **Proteção de Dados Pessoais**: Serão implementadas medidas técnicas e organizacionais apropriadas para proteger dados pessoais, garantindo a privacidade e os direitos dos titulares dos dados, em conformidade com a LGPD.

13.3. **Revisão de Conformidade**: A conformidade com os requisitos legais, regulamentares e contratuais será revisada periodicamente para garantir a adequação contínua da política e dos controles de segurança da informação.

14. GESTÃO DE RELACIONAMENTO COM FORNECEDORES

14.1. **Segurança da Informação em Relacionamentos com Fornecedores:** Serão estabelecidos requisitos de segurança da informação para fornecedores e parceiros que tenham acesso aos ativos de informação da Advance Telecom ou que prestem serviços que impactem a segurança da informação. Isso inclui a realização de avaliações de segurança de fornecedores e a inclusão de cláusulas

contratuais de segurança.

14.2. **Segurança para Uso de Serviços em Nuvem:** A utilização de serviços em nuvem será avaliada quanto aos riscos de segurança da informação, e controles apropriados serão implementados para garantir a proteção dos dados e sistemas hospedados em ambientes de nuvem.

15. DESLIGAMENTO DE COLABORADORES E DESCARTE DE ATIVOS

15.1. **Desligamento de Colaboradores:** Em caso de desligamento de colaboradores, o acesso ao ambiente de informações deverá ser bloqueado de imediato. Serão realizados procedimentos para a devolução de ativos da empresa, a revisão de acessos concedidos e a garantia de transferência de conhecimento relevante.

15.2. **Descarte Seguro de Material Impresso:** Estará à disposição dos colaboradores trituradores de papel ou equipamento similar, para o descarte de material sensível. Todo material impresso com dados internos ou confidenciais deve ser descartado apenas após utilização de triturador de papel.

15.3. **Descarte Seguro de Mídias Físicas e Equipamentos de TI:** Todos os equipamentos de TI que forem descartados, que contenham discos rígidos ou removíveis, deverão ter suas mídias destruídas de modo a não permitir a recuperação dos dados contidos. Os equipamentos deverão seguir padrões de descarte que evitem impacto ao meio ambiente e sejam ambientalmente responsáveis.

16. RESUMO DA REVISÃO

Esta política será revisada anualmente ou sempre que houver mudanças significativas no ambiente de negócios, tecnologia, riscos ou requisitos regulatórios. As revisões serão submetidas à aprovação do CGSCI e da Diretoria.

Revisor	Data	Versão	Descrição
José Lourenço e Débora Silva	24/09/2025	2.0	Versão inicial com base nas sugestões de melhoria e alinhamento ISO 27000