POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

5 Certificações ISO: Um marco de excelência que só a **Alias Tecnologia** tem.

ÍNDICE

20 ALIAS® anos

CARTA DA PRESIDÊNCIA

Prezado(a) Leitor(a),

É com grande satisfação que apresentamos a Política de Segurança da Informação da Alias Tecnologia, documento que reafirma nosso compromisso com a proteção dos ativos de informação e com a manutenção de elevados padrões de segurança.

Esta política tem como objetivo garantir a preservação da segurança da informação, protegendo a integridade de nossa organização, de nossos colaboradores e de nossos parceiros. Ela estabelece diretrizes que orientam o caminho estratégico que devemos seguir de forma ética, responsável e inovadora.

A nossa Política de Segurança da Informação é revisada e atualizada continuamente, garantindo que permaneça relevante e eficaz diante das demandas atuais. Este documento serve como um guia de conduta e deve ser seguido por todos os colaboradores e prestadores de serviços da Alias Tecnologia em suas decisões e interações diárias.

Nosso compromisso é orientar essas ações e manter um padrão elevado de segurança da informação, baseado na valorização das pessoas e das informações, na visão integrada das atividades com foco na melhoria contínua dos resultados e na excelência dos serviços, sustentada pelo comprometimento, proatividade e atendimento de qualidade, e no fomento a relacionamentos construtivos e à confiança, fortalecendo as relações internas e externas.

A segurança da informação é uma responsabilidade coletiva. O cumprimento das diretrizes estabelecidas é essencial para garantir a integridade, a confidencialidade e a confiabilidade de nossas operações, contribuindo para a sustentabilidade e o sucesso da organização.

Seguimos confiantes de que, com o engajamento de todos, continuaremos a fortalecer nossa cultura de segurança e a consolidar os valores que sustentam nossa trajetória.

Atenciosamente,

Fernando Weigert
28/01/2026

1. OBJETIVO

Esta política estabelece as bases e diretrizes essenciais para a proteção dos ativos de informação da Alias Tecnologia. Ela define as diretrizes que orientam o tratamento seguro de dados, assegurando confidencialidade, integridade, disponibilidade e privacidade, independentemente do meio de armazenamento, processamento ou compartilhamento.

Esta política representa a premissa das regras de segurança da informação da Alias Tecnologia e fornece uma estrutura clara para:

- Garantir a proteção de informações de clientes, parceiros, fornecedores e da própria organização;
- Orientar colaboradores, gestores e prestadores de serviço sobre suas responsabilidades na segurança da informação;
- Apoiar a prevenção e mitigação de incidentes, assegurando resposta adequada a eventos de segurança;
- Cumprir requisitos legais, regulatórios e normativos aplicáveis, incluindo as normas ISO 27001 e ISO 27701;
- Promover a melhoria contínua dos processos de segurança da informação.

Esta política é um documento corporativo, disponível para consulta de todos os públicos internos e externos, reforçando o compromisso da Alias Tecnologia com a transparência, confiança e proteção das informações que gerencia.

2. ABRANGÊNCIA

Esta política deve ser seguida por todos os colaboradores, diretores, gerentes, fornecedores e prestadores de serviços da Alias Tecnologia, assim como por qualquer pessoa que tenha acesso a informações, sistemas, redes, equipamentos ou arquivos da empresa no desempenho de suas funções.

Todas as normas e diretrizes estabelecidas nesta política devem ser observadas e aplicadas de forma consistente, garantindo a proteção das informações e o uso seguro dos recursos tecnológicos da empresa.

Cada usuário é responsável por manter-se atualizado quanto ao conteúdo desta política e suas normas relacionadas, buscando orientação junto à sua liderança ou ao administrador de segurança da informação sempre que houver dúvidas sobre o manuseio, armazenamento ou descarte de informações.

3. DEFINIÇÕES

Ameaça: Qualquer fator que possa causar um incidente indesejado, gerando dano a sistemas, informações ou à organização.

Áreas críticas: Dependências da Alias ou de seus clientes que armazenam ou processam informações essenciais para os negócios, exigindo proteção reforçada.

Ativo: Qualquer recurso ou elemento que tenha valor para a organização, incluindo humanos, tecnológicos, físicos e lógicos.

Ativo de Informação: Qualquer recurso, tangível ou intangível, que armazena, processa ou transmite informações, incluindo dados, sistemas, dispositivos, pessoas ou documentos, que possua valor para a organização e cuja proteção seja essencial para garantir a continuidade, integridade, confidencialidade e disponibilidade das operações e dos negócios.

Controle: Mecanismo utilizado para gerenciar riscos, podendo ser administrativo, técnico, de gestão ou legal, incluindo políticas, procedimentos, diretrizes e práticas.

Evento de Segurança da Informação: Ocorrência observada em sistemas, serviços ou redes que indique uma possível violação da política ou falha de controles, ou situação nova que possa afetar a segurança da informação.

Gestão de Riscos: Conjunto de atividades coordenadas para identificar, avaliar e tratar riscos relacionados à segurança da informação.

Incidente de Segurança da Informação: Qualquer evento que comprometa a Confidencialidade, Integridade ou Disponibilidade (CID) das informações.

Informação: Ativo essencial para os negócios, que pode existir de forma física, eletrônica ou verbal, e deve ser protegido adequadamente conforme sua criticidade.

Informações críticas para os negócios: Informações cuja alteração, divulgação ou destruição não autorizada possa causar perdas operacionais, financeiras ou estratégicas à organização ou seus clientes, incluindo dados pessoais e estratégicos.

Política de Segurança da Informação: Documento que estabelece diretrizes corporativas para proteção de ativos de informação, prevenção de responsabilidade legal e cumprimento obrigatório por todos os usuários.

Risco: Combinação da probabilidade de ocorrência de um evento com suas consequências.

Segurança da Informação: Conjunto de medidas para proteger informações contra ameaças, garantindo a continuidade dos negócios, minimizando riscos e assegurando oportunidades de negócio, baseado nos princípios de:

a) Confidencialidade: acesso somente a pessoas autorizadas;

b) Integridade: alterações, supressões ou adições somente por pessoas autorizadas;

c) Disponibilidade: informações acessíveis às pessoas autorizadas sempre que necessário.

Vulnerabilidade: Fragilidade de um ativo que pode ser explorada por ameaças.

MAC Address: Identificador único de hardware em dispositivos de rede, usado para controle de acesso e rastreamento.

MFA (Autenticação Multifator): Mecanismo de segurança que exige múltiplas formas de verificação de identidade para acessar sistemas ou informações.

Active Directory (AD): Serviço de diretório da organização utilizado para gestão centralizada de usuários, grupos e permissões de acesso.

SharePoint: Plataforma corporativa para armazenamento, colaboração e versionamento seguro de documentos e informações.

GPOs (Group Policy Objects): Políticas de grupo aplicadas via Active Directory para controlar permissões e configurações de usuários e sistemas.

Software: Programa ou aplicativo utilizado para execução de tarefas específicas em computadores e sistemas da empresa, cuja instalação depende de autorização formal.

Firewall: Dispositivo ou software que monitora e controla o tráfego de rede, protegendo contra acessos não autorizados e ameaças externas.

Dispositivos Móveis: Equipamentos portáteis como celulares e tablets que acessam informações corporativas, devendo ser protegidos conforme política de segurança.

Wi-Fi: Rede sem fio corporativa que deve ser utilizada de forma segura, seguindo as normas de autenticação e criptografia da empresa.

VPN (Rede Privada Virtual): Conexão segura que permite acesso remoto aos recursos da organização de forma protegida.

Datacenters: Instalações físicas ou em nuvem que hospedam sistemas e informações críticas, com medidas de segurança física e lógica reforçadas.

Antivírus: Software utilizado para detectar, prevenir e remover ameaças de malware em sistemas corporativos.

DPO (Data Protection Officer / Encarregado de Proteção de Dados): Profissional responsável por orientar a empresa sobre o tratamento de dados pessoais, garantir o cumprimento da LGPD e atuar como ponto de contato entre a organização, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD).

4. NORMAS, PROCEDIMENTOS E REQUISITOS DE COMPLIANCE

- **ABNT NBR ISO 27001:2022** - Sistemas de gestão de segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos.
- **ABNT NBR ISO/IEC 27701:2019** - Técnicas de Segurança - Extensão da ABNT ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da Privacidade da informação - Requisitos e diretrizes.
- **Lei nº 13.709/2018** - Lei Geral de Proteção de Dados Pessoais (LGPD).

5. PRINCÍPIOS DE SEGURANÇA E PRIVACIDADE DA INFORMAÇÃO

A segurança e a privacidade da informação são fundamentais para proteger ativos, garantir a confiança de clientes, colaboradores e parceiros, e assegurar a continuidade dos negócios.

Todas as informações gerenciadas pela organização devem seguir os seguintes princípios:

- **Integridade:** alterações, inclusões ou exclusões de informações devem ocorrer somente por pessoas autorizadas e de acordo com os processos estabelecidos;
- **Confidencialidade:** o acesso às informações é restrito a usuários autorizados, garantindo a proteção de dados sensíveis e estratégicos;
- **Disponibilidade:** as informações devem estar acessíveis aos usuários autorizados sempre que necessário, assegurando a continuidade das operações;
- **Transparência e confiança:** as relações internas e externas devem observar princípios de ética, responsabilidade e confiança;
- **Proteção da privacidade:** dados pessoais devem ser tratados conforme regulamentos aplicáveis, garantindo segurança, confidencialidade e conformidade com a ISO 27701 e da LGPD.

Estes princípios servem como diretrizes para todos os procedimentos, normas e controles de segurança da informação da Alias Tecnologia, orientando decisões, uso de recursos tecnológicos e responsabilidades de todos os públicos internos e externos.

6. DIRETRIZES GERAIS DE SEGURANÇA DA INFORMAÇÃO

6.1 Política de Segurança da Informação

> *"A Alias Tecnologia promove a cultura da segurança da informação em todas as suas atividades, assegurando a proteção dos dados e sistemas utilizados no registro de contratos de veículos e nas notificações extrajudiciais. Por meio da implementação de controles e processos eficazes, busca prevenir e mitigar incidentes de segurança, garantindo a*

confidencialidade, integridade, disponibilidade e privacidade das informações. A Alias Tecnologia compromete-se ainda com o cumprimento dos requisitos legais e regulatórios aplicáveis, bem como com a melhoria contínua de seus processos, fortalecendo a confiança de clientes, parceiros e colaboradores."

6.2 Objetivos da Segurança da Informação

A Alias Tecnologia estabelece os seguintes objetivos para a Política de Segurança da Informação, com foco na proteção dos seus ativos e na gestão segura das informações da organização:

- Implementar processos que previnam e mitiguem incidentes de segurança, garantindo a confidencialidade, integridade, disponibilidade e privacidade dos dados.
- Assegurar o cumprimento dos requisitos regulamentares aplicáveis ao negócio.
- Promover a melhoria contínua dos processos de segurança da informação, assegurando a evolução constante do Sistema de Gestão de Segurança da Informação.

6.3 Comitê de Segurança da Informação

O comitê de segurança da informação deve ser constituído pelos diretores e gestores de áreas com a atribuição de aprovar as diretrizes da Política de Segurança da Informação, assim como modificá-las conforme as necessidades da Alias Tecnologia.

6.4 Administrador de Segurança da Informação:

O Administrador de Segurança da Informação é designado pela alta direção como responsável pela qualidade da segurança da informação.

O Administrador de Segurança da Informação tem autonomia para cobrar, auditar e avaliar o cumprimento da Política de Segurança da Informação, bem como propor exceções, sempre com o auxílio e aprovação ou repulsa da alta direção.

É proibido omitir informações relevantes sobre incidentes de segurança, ao Administrador de Segurança da Informação, pois ele é o profissional responsável por avaliar a situação corretamente e tomar as providências adequadas.

6.5 Papéis e Responsabilidades na Segurança da Informação

6.5.1 Colaboradores e Prestadores de Serviços:

- Conhecer, compreender e cumprir todas as diretrizes da Política de Segurança da Informação;
- Zelar continuamente pela proteção das informações da organização ou de seus clientes contra acesso, modificação, destruição ou divulgação não autorizada;
- Assegurar que os recursos (computacionais ou não) colocados à sua disposição sejam

utilizados apenas para as finalidades oficiais da organização;

- Garantir que os sistemas e informações sob sua responsabilidade estejam adequadamente protegidos;
- Garantir a continuidade do processamento das informações críticas para os negócios da organização;
- Cumprir as leis e normas que regulamentam os aspectos de propriedade intelectual;
- Atender às leis que regulamentam as atividades da organização e seu mercado de atuação;
- Participar de treinamentos e campanhas de conscientização sobre segurança da informação e privacidade de dados;
- Comunicar imediatamente ao Administrador de Segurança da Informação qualquer descumprimento da Política de Segurança da Informação;
- Buscar orientação com o gestor ou com o Administrador de Segurança da Informação em caso de dúvidas sobre a interpretação da política ou procedimentos de segurança;
- Não compartilhar dados da empresa em e-mails pessoais ou com pessoas externas à organização;
- Utilizar senhas fortes, exclusivas para os acessos corporativos, e não compartilhar as senhas com terceiros;
- Estar atento a sites não seguros ou suspeitos e reportar qualquer irregularidade ao Administrador de Segurança da Informação;
- Solicitar autorização sempre que houver necessidade de utilizar softwares não aprovados pela empresa;
- Solicitar o download ou instalação de aplicativos nos equipamentos corporativos; nunca instalar aplicativos por conta própria;
- Não utilizar redes sociais nos equipamentos da empresa para fins pessoais;
- Não conectar dispositivos pessoais ou mídias externas (pen drives, HDs, cartões de memória) sem autorização e verificação da área de segurança;
- Não deixar estações de trabalho, laptops ou dispositivos móveis desprotegidos ou desbloqueados em locais públicos ou compartilhados;
- Bloquear a estação de trabalho ao se ausentar, mesmo que por curtos períodos;
- Não acessar redes Wi-Fi públicas ou não seguras com equipamentos corporativos sem

utilizar mecanismos de segurança fornecidos pela empresa;

- Não modificar configurações de segurança dos sistemas, antivírus ou firewalls corporativos;
- Não remover ou danificar etiquetas, selos ou mecanismos de rastreio de equipamentos ou documentos da empresa;
- Não encaminhar ou responder e-mails suspeitos (phishing) e reportar qualquer tentativa de fraude ao Administrador de Segurança da Informação;
- Não acessar ou armazenar conteúdo impróprio, ilegal ou que possa comprometer a imagem da empresa;
- Utilizar crachá de identificação de forma visível nas dependências da empresa;
- Assinar o Termo de Responsabilidade, declarando estar ciente da Política e das Normas de Segurança da Informação, comprometendo-se com seu integral cumprimento;
- Não conectar, parear ou tentar utilizar qualquer dispositivo Bluetooth nos equipamentos corporativos, salvo quando houver autorização formal.

6.5.2 Departamento de Infraestrutura e Suporte Técnico

- Propor ajustes, melhorias e atualizações na estrutura normativa de segurança da informação, submetendo-os à aprovação da diretoria e conselho de administração, quando necessário;
- Elaborar e redigir normas e procedimentos de segurança da informação, garantindo clareza e consistência, e submetê-los à aprovação da diretoria e conselho de administração, quando necessário;
- Requisitar informações às áreas da organização, por meio de suas diretorias, gerências ou supervisões, para verificar o cumprimento da Política, Normas e Procedimentos de Segurança da Informação;
- Receber, documentar, analisar e tratar casos de violação da Política, Normas ou Procedimentos de Segurança da Informação;
- Estabelecer mecanismos de registro e monitoramento de eventos e incidentes de segurança da informação, bem como de não conformidades com as diretrizes vigentes;
- Notificar a Diretoria e demais responsáveis sobre casos de violação da Política, Normas ou Procedimentos;
- Receber sugestões e demandas dos gestores da informação para a implantação de novas normas e procedimentos de segurança da informação;

- Propor e acompanhar projetos e iniciativas voltados à melhoria contínua da segurança da informação;
- Realizar a gestão sistemática dos ativos de informação, garantindo integridade, confidencialidade e disponibilidade;
- Gerir e validar planos de continuidade de negócios, em conjunto com as áreas envolvidas, garantindo testes e revisões periódicas;
- Conduzir a gestão de riscos relacionados à segurança da informação, identificando, avaliando e mitigando potenciais ameaças;
- Apoiar o núcleo interno de desenvolvimento na implementação de controles de segurança da informação em sistemas, aplicativos e infraestrutura tecnológica;
- Definir, implementar e gerenciar um sistema de controle de acesso para todos os ativos de informação da Alias Tecnologia, não importando sua localização física;
- Prover o controle e a autenticação das conexões externas dos usuários e viabilizar a segurança da informação quando for necessária a utilização de computação móvel e demais recursos de trabalho remoto;
- Assegurar que o uso de programas ou ferramentas especiais não comprometa os controles de segurança dos sistemas e aplicações;
- Criar contas de serviço observando-se a premissa do menor privilégio possível, os requisitos do negócio, e o resultado da análise de risco.

6.5.3 Departamento de Desenvolvimento e Produtos

- Garantir que os princípios de *Privacy by Design* sejam integrados a todos os projetos, produtos e sistemas desde a fase de concepção e planejamento, considerando a proteção de dados pessoais como requisito essencial.
- Elaborar, manter e atualizar documentos e registros que comprovem a aplicação do *Privacy by Design* em produtos, sistemas e funcionalidades;
- Garantir que coleta, armazenamento, processamento e compartilhamento de dados pessoais estejam alinhados política de segurança de informação, à LGPD e demais normas de privacidade aplicáveis;
- Avaliar e implementar medidas adequadas de segurança e privacidade, incluindo anonimização, pseudonimização, criptografia e controle de acesso, com o objetivo de minimizar riscos à privacidade;
- Integrar revisões periódicas de conformidade e impacto à privacidade no ciclo de desenvolvimento, garantindo que atualizações ou novas funcionalidades mantenham a

proteção de dados pessoais;

- Trabalhar em conjunto com o Administrador de Segurança da Informação, o Encarregado pelo Tratamento de Dados (DPO) e o departamento jurídico para validar decisões e soluções relacionadas à privacidade e à proteção de dados;
- Comunicar imediatamente ao Administrador de Segurança da Informação e ao DPO qualquer risco, vulnerabilidade ou incidente de privacidade identificado durante o desenvolvimento ou operação de sistemas.

6.5.4 Administrador de Segurança da Informação

- Gerenciar a implementação da Política de Segurança da Informação, assegurando que seus princípios, diretrizes e controles sejam aplicados em toda a organização;
- Avaliar e autorizar acessos a informações e recursos considerados sensíveis, garantindo que apenas pessoas devidamente autorizadas tenham permissão de uso;
- Realizar a análise de riscos e vulnerabilidades, propondo medidas preventivas e corretivas que reduzam a probabilidade de incidentes de segurança;
- Estabelecer e monitorar controles técnicos, físicos e administrativos que garantam a confidencialidade, a integridade, a disponibilidade e a privacidade das informações;
- Supervisionar o cumprimento das normas internas de segurança por todos os colaboradores, prestadores e parceiros, adotando medidas cabíveis em caso de não conformidade;
- Acompanhar e registrar incidentes de segurança da informação, promovendo a apuração, resposta e tratamento adequado, em conjunto com as áreas envolvidas;
- Manter atualizados os planos de contingência e de continuidade de negócios, garantindo sua efetividade e testes periódicos;
- Promover ações de conscientização e treinamento contínuo sobre segurança da informação para todos os níveis da organização;
- Avaliar periodicamente a eficácia dos controles implantados e recomendar melhorias;
- Atuar em conjunto com o setor jurídico e de compliance na adequação às legislações vigentes, incluindo a Lei Geral de Proteção de Dados (LGPD) e outras normas aplicáveis;
- Gerenciar o ciclo de vida dos ativos de informação, incluindo classificação, armazenamento, acesso e descarte seguro;
- Autorizar e monitorar o uso de dispositivos e mídias removíveis, assegurando que não representem risco à segurança dos dados corporativos;

- Participar ativamente das auditorias internas e externas, garantindo a integridade das evidências e o cumprimento dos requisitos normativos;
- Reportar periodicamente os indicadores, resultados e incidentes relacionadas à segurança da informação;
- Propor e liderar iniciativas de melhoria contínua dos processos e controles de segurança, alinhando-os aos objetivos estratégicos da organização;
- Avaliar, aprovar ou reprovar solicitações de exceção para uso de Bluetooth, com base em critérios de risco, necessidade operacional e conformidade normativa.

6.5.5 Gerências e Superintendências

- Garantir o cumprimento e a aplicação da Política, das Normas e dos Procedimentos de Segurança da Informação em suas respectivas áreas;
- Assegurar que todos os colaboradores sob sua gestão tenham acesso, compreendam e sigam corretamente as diretrizes de Segurança da Informação;
- Apoiar o núcleo de segurança da informação na elaboração e atualização de normas e procedimentos específicos de suas áreas, quando solicitado;
- Comunicar imediatamente ao núcleo de segurança da informação quaisquer incidentes, suspeitas ou violações relacionadas à Política de Segurança da Informação;
- Promover a conscientização contínua de suas equipes sobre boas práticas de segurança da informação;
- Assegurar que novos processos, sistemas ou projetos sob sua responsabilidade considerem, desde a fase de planejamento, os requisitos de segurança da informação;
- Garantir que acessos, permissões e credenciais sejam revisados periodicamente, conforme a necessidade de cada função;
- Colaborar com auditorias e inspeções internas relacionadas à segurança da informação, fornecendo as evidências e informações solicitadas.

6.5.6 Assessoria Jurídica

- Manter as áreas da organização informadas sobre alterações legais, regulatórias ou normativas que impliquem responsabilidades, riscos ou ações relacionadas à Política de Segurança da Informação;
- Incluir cláusulas específicas de segurança da informação, confidencialidade e proteção de dados pessoais na análise e elaboração de contratos, visando resguardar os interesses da organização;

- Avaliar, quando solicitado, a Política, as Normas e os Procedimentos de Segurança da Informação, garantindo conformidade com a legislação vigente;
- Acompanhar incidentes de segurança que possuam impacto jurídico, orientando sobre as medidas legais cabíveis e sobre a preservação de evidências;
- Orientar as áreas competentes quanto à coleta, guarda e preservação de provas eletrônicas, assegurando sua validade para uso judicial ou administrativo, quando necessário;
- Revisar periodicamente os documentos jurídicos, políticas e contratos relacionados à tecnologia e à segurança da informação, propondo adequações de acordo com as atualizações legais e regulatórias;
- Apoiar a aplicação de medidas disciplinares relacionadas a violações de segurança da informação, assegurando conformidade com os aspectos legais e trabalhistas;
- Garantir a conformidade das normas e procedimentos internos com o ordenamento jurídico brasileiro, abrangendo legislações sobre proteção de dados, anticorrupção, direito civil e digital, bem como outras normas legais que impactem a atuação institucional;
- Assessorar a organização quanto a novos projetos de lei, regulamentações ou demandas judiciais que possam impactar o negócio e o uso de tecnologias da informação;

6.5.7 Departamento de Recursos Humanos

- Garantir que todos os empregados, estagiários, aprendizes e prestadores de serviços participem da integração na organização, incluindo a realização obrigatória da avaliação online no ambiente de treinamento interno;
- Divulgar a Política de Segurança da Informação, Normas e Procedimentos da organização durante a integração, assegurando que todos compreendam suas responsabilidades;
- Criar mecanismos para comunicar, de forma antecipada e organizada, ao canal técnico apropriado, qualquer alteração no quadro funcional da organização, incluindo admissões, desligamentos e mudanças de função;
- Manter registros atualizados da participação nos treinamentos de integração e reciclagem, assegurando a rastreabilidade e comprovação de ciência;
- Apoiar o departamento técnico e ao administrador de segurança na identificação de necessidades de treinamento contínuo em Segurança da Informação;
- Revisar periodicamente os processos de integração e treinamentos, propondo melhorias que aumentem a eficácia da divulgação da Política de Segurança da Informação.

6.5.8 Conselho de Administração

- Aprovar a Política de Segurança da Informação e suas revisões, garantindo alinhamento

aos objetivos estratégicos da Organização;

- Aprovar a estrutura do departamento técnico de segurança da informação.
- Nomear o Administrador de Segurança da Informação;
- Promover a cultura de segurança da informação no nível estratégico, incentivando o comprometimento da liderança.
- Deliberar sobre incidentes críticos ou exceções que possam impactar a organização.

6.5.9 Comitê de Segurança da Informação

- Propor ajustes, aprimoramentos e modificações desta Política;
- Propor melhorias e aprovar as Normas de Segurança da Informação;
- Definir a classificação das informações pertencentes e/ou custodiadas pela organização com base na política de classificação da informação;
- Analisar casos de violação desta Política e das Normas de Segurança da Informação;
- Realizar reuniões para aprovar e propor adequações voltadas à melhoria da segurança da informação da Alias Tecnologia;
- Conduzir ações de conscientização e educação dos usuários sobre princípios e procedimentos de segurança da informação;
- Monitorar o plano de tratamento de riscos e revisar a matriz de riscos periodicamente;
- Revisar relatórios de auditoria interna e externa relacionados à segurança da informação, privacidade e compliance;
- Emitir recomendações para o Conselho de Administração sobre decisões críticas de segurança, continuidade e resposta a incidentes;
- Realizar reuniões mensais, podendo ocorrer em maior frequência ou de forma extraordinária quando necessário, sempre registradas em ata. Conforme a demanda, representantes de outras áreas da Alias Tecnologia ou convidados externos poderão participar das reuniões.

7. DIRETRIZES ESPECÍFICAS DE SEGURANÇA DA INFORMAÇÃO

7.1 Gestão e Governança

A empresa determina que a segurança da informação deve estar integrada a todas as atividades e processos, garantindo a proteção de dados, sistemas e operações essenciais. Todas as práticas de segurança devem estar alinhadas aos objetivos estratégicos da organização e à

legislação vigente. Políticas e controles devem ser revisados sempre que ocorrerem mudanças significativas no ambiente, nos processos ou na tecnologia utilizada.

7.1.1 Auditoria e Monitoramento

Todos os ativos de informação sob responsabilidade da organização estão sujeitos a auditorias, que podem ocorrer em diferentes formatos:

- **Auditorias internas e externas**, previamente agendadas, voltadas a verificar o cumprimento das normas ISO 27001, ISO 27701 e das políticas internas da organização, conduzidas por equipes independentes da gestão operacional.
- **Auditorias conduzidas pelo Administrador de Segurança da Informação**, em datas e horários determinados, com aprovação da Diretoria de TI, podendo ocorrer sem aviso prévio ou a pedido de gestores ou da direção da empresa, com foco em monitoramento e controle de conformidade operacional;

Durante todas as auditorias, devem ser resguardados os direitos de privacidade de informações pessoais, desde que não estejam misturadas com dados sob responsabilidade da Alias Tecnologia ou de seus clientes.

Colaboradores que utilizem dispositivos com rede sem fio ou cabeada concordam em fornecer o *MAC ADDRESS* desses equipamentos, quando solicitado, garantindo que não sejam utilizados de forma indevida.

A área de Segurança da Informação poderá realizar monitoramento e controles proativos para detectar atividades anômalas ou violações da política, mantendo a confidencialidade das informações obtidas.

As informações levantadas em auditorias ou monitoramento podem servir como indícios ou evidências em processos administrativos ou legais, reforçando a governança e a responsabilidade na proteção dos ativos de informação da organização.

7.1.2 Abordagem de Riscos e Oportunidade

A empresa adota uma abordagem sistemática para identificação, avaliação e tratamento de riscos e oportunidades relacionados à segurança da informação.

Os investimentos em segurança da informação devem ser realizados com base em análises formais de risco, priorizando a proteção de informações críticas, sistemas estratégicos e dados sensíveis. As decisões de alocação de recursos devem considerar o impacto potencial de incidentes, o valor dos ativos envolvidos e o custo-benefício das medidas de mitigação, assegurando que os recursos sejam aplicados de forma eficiente, consistente com os princípios de governança e a gestão de riscos da empresa.

Os projetos estratégicos conduzidos pela Alias Tecnologia devem incorporar a avaliação de riscos desde sua fase de planejamento até a implementação e operação. Essa análise deve contemplar

os riscos relacionados à confidencialidade, integridade e disponibilidade da informação, bem como impactos financeiros, operacionais e de imagem. As áreas envolvidas devem assegurar que os controles de segurança sejam adequadamente dimensionados e aplicados, prevenindo vulnerabilidades e garantindo a continuidade e confiabilidade dos resultados dos projetos.

7.2 Proteção dos Ativos de Informação

Toda informação gerada, manipulada ou armazenada pela Alias Tecnologia é considerada ativo de informação e deve ser protegida conforme sua classificação e criticidade.

- O uso e a coleta de informações devem se limitar ao estritamente necessário para desempenhar as atividades da empresa, incluindo o registro de contratos e o acompanhamento de processos relacionados.
- As informações disponibilizadas pela organização têm finalidade única de suportar atividades corporativas, sendo proibido seu uso para qualquer outro propósito, por colaboradores e prestadores de serviços.
- Todos os colaboradores e prestadores de serviços são responsáveis por proteger as informações a que têm acesso, assegurando confidencialidade, integridade e uso correto.
- A proteção das informações deve estar presente em todas as atividades e processos, garantindo que decisões e ações sejam avaliadas quanto a impacto, criticidade e risco à segurança da informação.

7.3 Controle de Acesso

Na Alias Tecnologia, o acesso a sistemas, informações e recursos tecnológicos é concedido de forma controlada e de acordo com o princípio do menor privilégio, ou seja, cada colaborador tem acesso apenas ao que é necessário para o desempenho de suas atividades.

Todos os acessos devem ser feitos por meio de credenciais individuais e intransferíveis, sendo expressamente proibido o compartilhamento de senhas, tokens, certificados digitais ou qualquer outro tipo de credencial de autenticação.

O uso dos recursos tecnológicos da empresa está condicionado à assinatura do Termo de Responsabilidade e Confidencialidade, documento que formaliza o compromisso do colaborador com o uso ético e seguro das informações e sistemas da Alias Tecnologia.

A criação, alteração ou bloqueio de contas de acesso deve respeitar os critérios de autorização definidos pela organização, incluindo o credenciamento prévio dos usuários.

O bloqueio ou exclusão de acessos deve ocorrer sempre que houver término de vínculo, encerramento de contratos ou identificação de acessos indevidos, assegurando que apenas usuários autorizados permaneçam com permissões ativas.

Todos os acessos devem ser revisados, passíveis de monitoramento e auditoria, e qualquer

violação ou uso indevido deve ser imediatamente comunicado à área de Segurança da Informação.

7.4 Controles Específicos

A Alias Tecnologia estabelece que todos os ativos de informação devem ser protegidos por controles específicos e monitoramento contínuo, garantindo a confidencialidade, integridade e disponibilidade das informações. Segue abaixo os principais controles adotados:

7.4.1 Controle e Gestão de Incidentes de Segurança da Informação

Todos os colaboradores e prestadores de serviço devem comunicar imediatamente qualquer incidente ou suspeita de incidente de segurança da informação ao departamento de Segurança da Informação, utilizando os canais oficiais definidos pela Alias Tecnologia.

A gestão dos incidentes deve assegurar o registro, análise, tratamento e acompanhamento de todos os eventos, garantindo que sejam avaliados de forma adequada e que as ações corretivas e preventivas sejam implementadas rapidamente para evitar recorrências.

Os incidentes devem ser classificados conforme seu nível de impacto e criticidade, permitindo a priorização das respostas e a comunicação adequada às partes interessadas.

O processo de gestão deve garantir a rastreabilidade de todas as etapas, desde a identificação até o encerramento do incidente, preservando evidências e mantendo a confidencialidade das informações envolvidas.

Cabe à área de Segurança da Informação coordenar as atividades de investigação, propor melhorias nos controles e promover ações de conscientização voltadas à prevenção de novos incidentes.

Todos os registros devem ser analisados periodicamente, visando à melhoria contínua dos processos de segurança e à redução dos riscos organizacionais.

7.4.2 Monitoramento de Sistemas

Os sistemas da organização devem registrar todas as ações realizadas, garantindo a rastreamento completo e confiável das atividades. Isso permite identificar a origem de qualquer ação ou evento, fortalecendo a responsabilidade e a integridade das operações.

7.4.3 Monitoramento da Rede de Colaboradores

Os dispositivos corporativos conectados à rede da empresa devem ser monitorados quanto ao uso da internet e demais recursos de rede. Todos os acessos e atividades devem ser registrados, garantindo rastreamento completo e análise de segurança sempre que necessário.

7.4.4 Monitoramento de Segurança da Informação

A segurança da informação deve ser monitorada diariamente, incluindo a análise de logs e

indicadores críticos, de forma a detectar e prevenir incidentes. Entre os pontos de atenção estão:

- Disponibilidade dos sistemas;
- Monitoramento de sistemas de segurança desenvolvidos internamente;
- Análise de logs de servidores web e de banco de dados;
- Verificação de registros do web firewall;
- Testes periódicos das regras de segurança;
- Garantia da integridade e disponibilidade dos backups.

7.5 Proteção Física e Lógica

Para reforçar a proteção da Alias Tecnologia, esta política estabelece regras claras para o controle de acesso físico às suas instalações, garantindo a segurança dos ativos de informação e a proteção dos colaboradores.

Além disso, a organização implementa controles de proteção lógica voltados à segurança do ambiente digital, assegurando que apenas usuários devidamente autorizados tenham acesso aos sistemas, redes e informações corporativas.

7.5.1 Acesso a áreas sensíveis (estoque de dispositivos e equipamentos):

- O acesso a essas áreas é restrito e deve ser autorizado exclusivamente pelo Administrador de Segurança da Informação. Somente o departamento de Infraestrutura e segurança da informação está autorizado a entrar nessas dependências, garantindo que dispositivos e equipamentos críticos estejam protegidos contra acesso não autorizado, roubo ou dano.
- Nos CPDs e na sala de processamento e armazenamento de documentos, as barreiras físicas devem ser estendidas do piso ao teto, garantindo proteção contra acesso não autorizado, propagação de fogo e contaminação ambiental.
- Áreas críticas ou sensíveis (como salas de servidores, armazenamento de documentos e equipamentos) devem estar localizadas em ambientes de acesso restrito, com perímetro de segurança definido, mantendo barreiras de segurança e controles de entrada apropriados em volta dessas áreas.

7.5.2 Acesso ao escritório e demais dependências:

- O ingresso de colaboradores e prestadores de serviço deve ser realizado mediante uso obrigatório da credencial de acesso (crachá) em local visível e autorização prévia, com registro biométrico.
- Visitantes devem ser previamente anunciados à recepção e autorizados por um responsável antes de adentrar as dependências da empresa, devendo portar crachá de

visitante durante toda a permanência. Fica vedado a entrada de visitantes, fornecedores ou prestadores de serviço que não foram previamente identificados e autorizados a entrar no ambiente.

- Colaboradores devem abordar qualquer pessoa não identificada, desacompanhada ou sem crachá visível, encaminhando-a à recepção para verificação e registro de acesso.
- O acesso para as dependências do escritório da Alias Tecnologia deve ser protegido contra o acesso não autorizado, com mecanismo de controle, barras, alarmes, fechaduras etc.
- O controle e a auditoria dos acessos físicos devem ser mantidos em registros seguros e revisados periodicamente, assegurando que somente pessoal autorizado possua acesso às áreas críticas.
- Falhas ou vulnerabilidades observadas nos controles de acesso físico devem ser imediatamente comunicadas ao Administrador de Segurança da Informação para tratamento adequado.
- A área de recepção deve manter mecanismos eficazes de controle e registro de entrada e saída, garantindo que o acesso à empresa ocorra apenas mediante autorização formal e identificação válida.

7.5.3 Proteção Física de Equipamentos

- Todos os equipamentos de processamento, armazenamento ou transporte de informações devem ser protegidos contra furto, incêndio, água, vibração, poeira, radiação eletromagnética, interferências externas e quaisquer outros riscos ambientais.
- A localização e disposição dos equipamentos devem ser planejadas para reduzir riscos ambientais, minimizar oportunidades de acesso não autorizado e proteger os recursos de apoio, como suprimento de energia e infraestrutura de cabeamento.
- Equipamentos que manuseiam informações sensíveis devem ser posicionados e isolados de forma a reduzir o risco de olhares indiscretos e garantir o nível adequado de proteção física.
- É proibido comer, beber ou fumar nas instalações de armazenamento de informações ou em suas proximidades.
- Condições ambientais que possam afetar a operação segura dos equipamentos devem ser monitoradas constantemente, considerando impactos de acidentes internos ou externos, incluindo incêndios em prédios vizinhos, vazamentos de água ou explosões em áreas próximas.
- A identificação de equipamentos que processam ou armazenam informações sensíveis não deve constar em listas de pessoal, listas telefônicas internas ou qualquer local acessível ao público.

- O descarte de equipamentos eletrônicos deve garantir a eliminação completa das informações, seguindo os procedimentos internos da Alias Tecnologia e a legislação ambiental vigente.

7.5.4 Proteção de Informações

- Colaboradores e prestadores de serviços devem se atentar as diretrizes de mesa limpa e tela limpa, descritas nesta política no item 7.18.
- Equipamentos críticos devem ser posicionados em locais restritos e não acessíveis ao público.
- Não deve haver divulgação de detalhes da arquitetura da rede em acessos externos.
- Sistemas de detecção de intrusos devem ser instalados conforme padrões profissionais e testados regularmente para cobrir todas as portas externas.
- Alarmes devem permanecer armados permanentemente nas áreas não ocupadas.
- Equipamentos administrados pela organização devem estar fisicamente separados de equipamentos administrados por terceiros.
- Materiais perigosos ou combustíveis devem ser armazenados de forma segura e a distância adequada de áreas críticas.
- Suprimentos em grande volume devem ser armazenados em áreas seguras e requisitados apenas conforme a necessidade de uso
- Equipamentos e mídias de backup devem ser posicionados a uma distância segura para evitar danos em caso de acidentes no site principal.

7.5.5 Monitoramento por Câmeras de Segurança

O monitoramento das instalações da Alias Tecnologia por meio de câmeras de segurança tem como objetivo proteger os ativos físicos e as informações da empresa, devendo ser realizado de forma abrangente e respeitando a privacidade. Desta forma, as seguintes diretrizes devem ser seguidas:

- As instalações devem ser monitoradas por câmeras de vigilância em pontos estratégicos, tanto internos quanto externos. Os sistemas de monitoramento devem estar operacionais 24 horas por dia, 7 dias por semana.
- O sistema de monitoramento deve preservar a privacidade das áreas de uso individual, como estações de trabalho.
- Deve cobrir todas as áreas de circulação, entradas e saídas.

- Deve abranger todas as áreas de acesso restrito, internas e externas.
- Deve permitir a captura de imagens detalhadas e resumidas para análise conforme necessário.
- As imagens devem ser armazenadas por, no mínimo, três meses.
- Os locais monitorados devem ser sinalizados de forma visível, informando que há monitoramento em funcionamento.

Observações:

Qualquer exceção a essas diretrizes deve ser tratada de forma pontual e rápida, utilizando ligações telefônicas, videoconferência ou outros meios, sem comprometer os prazos de segurança previstos.

7.6 Gestão de Senhas e Credenciais

- Todas as senhas utilizadas para acesso a sistemas, dispositivos, redes e informações corporativas da Alias Tecnologia devem ser criadas, armazenadas e utilizadas de forma a garantir a confidencialidade e a integridade das credenciais.
- As senhas devem atender aos padrões de complexidade definidos pela organização, incluindo combinações de letras maiúsculas e minúsculas (Aa), números (0–9) e símbolos especiais (#@), com no mínimo 11 caracteres.
- Para arquivos comprimidos que exigem senha, a complexidade deve seguir o mesmo padrão, sendo exigido mínimo de 12 caracteres.
- É proibida a utilização de informações pessoais como CPF, datas de nascimento, números de telefone, nomes próprios ou outras combinações que possam ser facilmente identificadas.
- As senhas não devem conter sequências previsíveis ou caracteres repetidos em série (ex.: “111”, “abc”, “123”).
- Toda senha é pessoal, intransferível e de uso exclusivo do colaborador. É vedado o compartilhamento de credenciais sob qualquer circunstância.
- As senhas devem ser alteradas a cada 45 dias, ou conforme parametrização específica de cada sistema, respeitando eventuais exceções para ambientes web que adotem políticas diferenciadas.
- A criação e alteração de senhas devem ser realizadas apenas em equipamentos corporativos e dentro do ambiente controlado da Alias Tecnologia.
- Em caso de suspeita de comprometimento de senha, o colaborador deve realizar a troca imediata e comunicar a área de Segurança da Informação para análise e registro do

incidente.

- Sempre que possível, deve ser utilizada a autenticação multifator (MFA), que exige mais de uma forma de verificação da identidade do usuário como medida adicional de segurança.
- O descumprimento desta diretriz constitui violação às normas de segurança da informação e poderá acarretar medidas disciplinares conforme as políticas internas da organização.
- A redefinição de senhas em Active Directory e Sistemas Especiais de Servidores deve ser realizada exclusivamente pelo departamento de T.I., por colaboradores com perfil de "Administrador de T.I". Todas as solicitações devem ser formalizadas por meio de chamados registrados, garantindo controle, rastreabilidade e conformidade do processo.
- Os resets de senha das contas de e-mail corporativas devem ser realizados exclusivamente pelo departamento de T.I., por colaboradores com acesso do perfil de "Administrador de T.I". A execução deve ocorrer conforme a necessidade e somente após a devida confirmação da identidade do solicitante.
- Os administradores responsáveis pelos resets de senha devem seguir boas práticas, garantindo que os resets sejam realizados apenas quando a identidade do solicitante for devidamente confirmada, evitando alterações indevidas.

7.7 Criptografias e Chaves Criptográficas

As diretrizes a seguir têm como objetivo estabelecer os princípios para uso, proteção e gestão de mecanismos criptográficos na Alias Tecnologia.

- **Uso adequado da criptografia:** A criptografia deve ser utilizada para proteger a confidencialidade, integridade e autenticidade das informações em trânsito e em repouso, de acordo com o nível de classificação da informação. Apenas algoritmos e protocolos criptográficos reconhecidos por órgãos internacionais (como ISO) devem ser empregados.
- **Gestão de chaves criptográficas:** O ciclo de vida das chaves (geração, distribuição, uso, armazenamento, rotação e descarte) deve seguir práticas seguras e documentadas.

  Chaves criptográficas devem possuir tamanhos e prazos de validade adequados à sensibilidade da informação protegida.

  O compartilhamento de chaves deve ocorrer exclusivamente por canais seguros e autorizados, conforme as diretrizes de controle de acesso.
- **Responsabilidade e controle de acesso:** O acesso às chaves criptográficas é restrito a pessoal autorizado e deve ser controlado por meio de autenticação e segregação de funções.

  Cada área é responsável por garantir que os controles definidos nesta política sejam aplicados aos sistemas sob sua gestão.

- **Revisão e atualização:** Os algoritmos e certificados utilizados deverão ser periodicamente revisados para garantir que não existam vulnerabilidades conhecidas.

  Chaves comprometidas ou suspeitas de exposição devem ser imediatamente revogadas e substituídas.

- **Conformidade e auditoria:** Todos os processos de criptografia devem atender às normas ABNT NBR ISO/IEC 27001 e 27002, bem como à LGPD e demais legislações aplicáveis.

  Logs e evidências de uso de chaves e certificados devem ser mantidos para auditoria e rastreabilidade.

7.8 Classificação e Tratamento da Informação

Todas as informações devem ser classificadas de acordo com seu nível de criticidade e confidencialidade, assegurando que o acesso, o uso e o armazenamento sejam compatíveis com o grau de sensibilidade de cada dado.

Os documentos produzidos ou compartilhados pelos colaboradores da Alias Tecnologia devem seguir a seguinte classificação:

- **Pessoal (Classificação 1):** Somente podem ser conhecidos e acessados pela própria pessoa como por exemplo sua própria senha pessoal.
- **Seletiva (Classificação 2):** Somente podem ser conhecidos e acessados pelo superior imediato da pessoa que emitiu o documento e pela pessoa para quem foi compartilhada a informação.
- **Setorial (Classificação 3):** Podem ser conhecidos e acessados pelas pessoas do próprio setor, pela direção ou pelas pessoas dos setores a quem é emitido o documento.
- **Interna (Classificação 4):** Podem ser conhecidos e acessados por todos da empresa.
- **Pública (Classificação 5):** Podem ser conhecidos e acessados publicamente.

Para garantir a identificação correta, toda informação classificada deve conter no cabeçalho a indicação de sua classificação, por exemplo: *"Classificação: 5 – Pública"* ou *"Confidencialidade 5 – Pública"*.

7.9 Classificação da Informação em E-mails

Toda comunicação por e-mail deve apresentar a classificação da informação logo acima da assinatura do remetente, garantindo a identificação adequada do nível de confidencialidade da mensagem.

7.10 Troca de Informações

Na Alias Tecnologia, a troca de informações deve seguir rigorosamente a classificação estabelecida no item 7.8 desta Política, garantindo que cada dado seja compartilhado de forma

segura e responsável.

Classificação	Tipo	Diretriz para Troca de Informação
1	Pessoal	Informações pessoais não devem ser compartilhadas. Exceções só poderão ocorrer com autorização formal do Administrador de Segurança da Informação ou, na ausência deste, do gestor responsável. A comunicação da autorização deve ser registrada e informada posteriormente ao Administrador de Segurança.
2	Seletiva	**Troca verbal:** deve ocorrer apenas entre os profissionais autorizados, em ambiente reservado e sem a presença de terceiros. Caso haja anotações, estas devem ser digitalizadas em arquivo protegido por senha e o material físico deve ser descartado adequadamente. **Troca em documento físico:** permitir acesso apenas às pessoas previamente definidas. **Troca em meio eletrônico:** criptografar os arquivos e proteger com senha, conforme instruções do procedimento interno de Gestão de Senhas. A senha de acesso deve ser enviada por canal diferente do utilizado para o envio do arquivo. **Exceções:** somente mediante autorização formal (e-mail) do Administrador de Segurança da Informação ou, em sua ausência, do Superintendente de Infraestrutura e Segurança da Informação.
3	Setorial	A troca de informações deve ser feita exclusivamente por meio do sistema de e-mail corporativo da Alias Tecnologia (Office 365) ou outra ferramenta interna aprovada pela área de Segurança da Informação.
4	Interna	As informações podem ser trocadas por e-mail corporativo, em reuniões internas, em documentos eletrônicos ou outros meios oficiais de comunicação da Alias Tecnologia, desde que o acesso permaneça restrito somente a colaboradores da Alias Tecnologia.
5	Pública	A troca de informações é livre, podendo ser compartilhada publicamente, desde que o conteúdo esteja classificado como de acesso público.

As orientações abaixo definem os cuidados que devem ser adotados conforme o tipo de classificação da informação:

7.11 Uso Correto dos Ativos

Os ativos de informação da Alias Tecnologia, tais como, equipamentos, sistemas, redes, e-mails e documentos, devem ser utilizados exclusivamente para atividades profissionais e em conformidade com as políticas internas da empresa.

É proibida a instalação de softwares não autorizados, o acesso a conteúdos ilícitos, inadequados ou que possam comprometer a segurança da informação.

Dispositivos móveis corporativos devem possuir bloqueio por senha e, sempre que aplicável, criptografia, garantindo a proteção das informações armazenadas e o uso seguro dos recursos tecnológicos da Alias Tecnologia.

É vedado o uso de dispositivos de armazenamento externo, como pen drives, HDs portáteis ou qualquer equipamento USB pessoal, a fim de evitar riscos de contaminação, vazamento ou perda de dados corporativos. Em casos excepcionais, o uso de dispositivos de armazenamento deve ser previamente solicitado e autorizado pelo Administrador de Segurança da Informação.

Apenas o departamento de Segurança da Informação tem permissão para usar dispositivos de armazenamento removível. Esse uso é restrito a atividades administrativas, como instalação de programas, transferência de arquivos e formatações, garantindo a continuidade das operações da Alias Tecnologia.

7.12 Uso de Arquivos Compartilhados na Rede

- **Criação e armazenamento de arquivos:** Os arquivos devem ser criados inicialmente na área de trabalho local e, após concluídos, armazenados nos diretórios de rede designados. Os nomes dos arquivos devem ser objetivos, breves e sem o uso de acentos, caracteres especiais ou símbolos, prevenindo falhas de indexação, lentidão de acesso e eventuais falhas nos processos de backup e restauração.
- **Acesso e manipulação:** O acesso simultâneo a um mesmo arquivo na rede deve ser evitado, pois pode gerar conflitos durante o processo de backup, resultando em corrupção de dados, perda parcial de informações ou comprometimento do servidor.
- **Edição e exclusão:** É permitido editar ou excluir apenas arquivos de autoria própria. Em caso de necessidade de alteração em arquivos de terceiros, o colaborador deve consultar seu superior imediato antes de proceder, assegurando a responsabilidade e a rastreabilidade das ações.
- **Uso dos diretórios de rede:** Os diretórios de rede destinam-se exclusivamente ao armazenamento de informações relacionadas às atividades corporativas. É

expressamente proibido o armazenamento de arquivos pessoais ou sem vínculo com as operações da empresa, a fim de evitar degradação de desempenho, falhas de backup e riscos à segurança da informação.

7.13 Uso do Sharepoint

A Alias Tecnologia adota o SharePoint como plataforma oficial para armazenamento, colaboração e gestão de documentos corporativos. O uso seguro e adequado dessa ferramenta é essencial para preservar a confidencialidade, integridade e disponibilidade das informações.

Para tanto, todos os colaboradores e prestadores de serviços devem-se atentar as seguintes diretrizes:

- **Criação de Arquivos:** Os arquivos devem ser criados e armazenados nas pastas e bibliotecas adequadas, conforme a estrutura de diretórios definida pela empresa. Devem ser utilizados nomes claros, objetivos e descritivos, evitando o uso de caracteres especiais, símbolos ou abreviações que dificultem a busca e identificação dos documentos.

- **Acesso a Arquivos:** O acesso às bibliotecas, pastas e arquivos deve respeitar os níveis de permissão concedidos. É vedado tentar acessar, compartilhar ou modificar documentos fora do escopo de autorização do usuário. O acesso deve ser realizado preferencialmente por meio de links compartilhados de forma controlada ou diretamente pelo ambiente corporativo da Alias Tecnologia.

- **Edição e Exclusão de Arquivos:** As edições devem ser realizadas de forma responsável, respeitando as versões anteriores e evitando sobrescritas desnecessárias. Qualquer alteração, exclusão ou revisão de documento deve ser previamente comunicada ao Núcleo do SGI, que será responsável por formalizar a solicitação de mudança e garantir o controle das versões. É proibida a exclusão de arquivos sem autorização do responsável pela pasta, área e do próprio Núcleo do SGI.

- **Organização e Uso de Diretório:** Os documentos devem permanecer organizados nas pastas e subpastas designadas, mantendo a hierarquia de diretórios estabelecida para facilitar o versionamento, a localização e o compartilhamento. Não é permitido armazenar arquivos pessoais, temporários ou sem relação direta com as atividades corporativas.

- **Compartilhamento e Permissões:** O compartilhamento de arquivos ou pastas deve ser restrito a usuários autorizados e, sempre que possível, limitado a grupos internos. É proibido o compartilhamento público ou com domínios externos sem a devida autorização da área de Segurança da Informação ou da Diretoria responsável.

7.14 Gestão de Ativos

7.14.1 Orientações de Uso dos Ativos

- Todos os ativos físicos, lógicos e informacionais da Alias Tecnologia devem ser identificados, registrados e protegidos conforme seu valor, criticidade e relevância para o negócio.
- O uso dos ativos é restrito às finalidades corporativas, sendo proibido qualquer uso pessoal ou não autorizado.
- Cada ativo deve ter um responsável designado, garantindo sua guarda, integridade e utilização adequada.
- A equipe de Tecnologia da Informação é responsável por controlar, registrar e monitorar os ativos de tecnologia, assegurando sua rastreabilidade, inventário atualizado e conservação.
- Todos os colaboradores que recebam equipamentos ou dispositivos corporativos devem assinar o Termo de Responsabilidade pelo Uso de Equipamentos, formalizando a posse e o compromisso com sua correta utilização e devolução.
- Os ativos devem ser armazenados em locais adequados, garantindo sua conservação e segurança física, com controle de acesso restrito às áreas de estoque e infraestrutura.
- Os ativos relacionados à informação devem possuir identificação física ou lógica (etiqueta, código ou registro) que permita sua rastreabilidade.
- Equipamentos de baixo valor ou bens de consumo, como teclados, mouses, headsets, cabos e periféricos similares, não necessitam de código individual, mas devem ser utilizados exclusivamente em atividades corporativas.
- Movimentações, substituições, manutenções e descartes de ativos devem ser controlados e registrados, garantindo rastreabilidade e conformidade com as normas internas.
- Ativos de informação devem ser classificados conforme o nível de confidencialidade, de acordo com as diretrizes de Classificação da Informação.
- Qualquer extravio, dano, perda ou uso indevido de ativo deve ser comunicado imediatamente à área de Segurança da Informação e à Diretoria de TI para análise e providências cabíveis.
- A Alias Tecnologia manterá processos contínuos de revisão, atualização e aprimoramento da gestão de ativos, garantindo conformidade, eficiência e proteção dos recursos tecnológicos e informacionais.

7.14.2 Aquisição de Ativos

A aquisição de novos ativos deve estar alinhada à estratégia organizacional, à matriz de riscos e à criticidade das funções que o ativo irá desempenhar.

- A seleção e compra devem considerar indicadores e critérios que assegurem:

  a) Facilidade de manutenção e suporte técnico;

  b) Confiabilidade operacional, garantindo desempenho adequado às funções requeridas, dentro de prazos e contextos específicos;

  c) Sustentação logística e operacional eficiente, com estratégias de manutenção e operação baseadas em confiabilidade e disponibilidade.

- Todos os ativos adquiridos devem atender aos requisitos de segurança da informação e conformidade técnica definidos pela organização antes de sua incorporação ao ambiente corporativo.

7.14.3 Operação e Manutenção de Ativos

- Todos os ativos devem ser operados e mantidos garantindo disponibilidade, continuidade, eficiência de custos e conformidade regulatória.
- É obrigatório seguir os planos e estratégias de operação e manutenção, respeitando os padrões técnicos e de segurança definidos pela Alias Tecnologia.
- A organização deve promover a melhoria contínua dos processos, incorporando inovações, novas tecnologias e boas práticas, assegurando eficiência e proteção dos ativos.
- Deve ser mantida uma visão integrada dos ativos, favorecendo o compartilhamento eficiente de recursos e informações entre áreas.
- As informações sobre os ativos devem ser registradas e gerenciadas de forma estruturada, permitindo análises precisas e decisões fundamentadas.
- É responsabilidade da organização controlar de forma proativa os custos de operação e manutenção, considerando criticidade, risco, retorno e alinhamento à estratégia.
- O acesso a ativos durante manutenção deve ser restrito a pessoal autorizado, com registro formal de todas as intervenções.
- Revisões e manutenções devem garantir a continuidade dos serviços e a segurança da informação, incluindo testes de recuperação, backups e redundâncias quando aplicável.

7.15 Backup e Armazenamento de Informações

Todas as informações corporativas da Alias Tecnologia devem ser protegidas por backup que garantam a preservação e a disponibilidade dos dados, abrangendo sistemas internos, documentos e informações armazenadas em nuvem.

Os backups devem contemplar sistemas críticos, incluindo registros de contratos, arquivos no Active Directory e documentos no SharePoint, assegurando versionamento e possibilidade de

recuperação de versões anteriores.

É proibido armazenar arquivos com informações sensíveis em computadores locais fora da rede corporativa, visto que esses dados não estão incluídos nos backups regulares.

A efetividade dos backups deve ser testada anualmente, pelo departamento de segurança da informação, com o objetivo de garantir a conformidade no processo.

Os procedimentos de backup devem assegurar a integridade, a segurança e a disponibilidade das informações, permitindo restauração confiável e protegendo os dados contra acesso não autorizado, falhas ou perdas físicas.

7.16 Uso da Internet

O uso da Internet corporativa é exclusivo para realizar atividades relacionadas às funções e objetivos da empresa, incluindo pesquisa de informações, execução de tarefas e desenvolvimento profissional. O acesso a redes sociais deve ocorrer apenas pelos departamentos que as utilizam para fins corporativos.

É proibido o uso da Internet para atividades pessoais, incluindo, mas não se limitando a consultas bancárias, compras online, redes sociais pessoais, entretenimento ou qualquer outro fim que não estejam diretamente relacionados ao trabalho.

O acesso a sites que possam comprometer a segurança ou a integridade da empresa é estritamente proibido. Isso inclui, entre outros: conteúdos impróprios, pornográficos, violentos, discriminatórios, racistas, difamatórios, falsos ou que violem leis e regulamentos aplicáveis.

Todos os colaboradores devem utilizar os recursos de rede com responsabilidade, seguindo as diretrizes de segurança da informação e evitando qualquer comportamento que possa expor a empresa a riscos ou prejuízos.

7.17 Uso da Impressora

O uso das impressoras é restrito as necessidades profissionais e atividades diretamente relacionadas às operações. A utilização de impressoras para fins pessoais não é permitida, visando preservar os recursos e manter o foco na eficiência e eficácia.

Colaboradores e prestadores de serviço devem utilizar as impressoras de maneira responsável, garantindo que todos os documentos impressos estejam em conformidade com as necessidades e objetivos da empresa.

As impressoras devem permanecer protegidas por bloqueios de teclas, senhas ou outros mecanismos de controle quando não estiverem em uso, prevenindo acessos não autorizados, especialmente fora do horário normal de expediente.

Documentos contendo informações sensíveis ou confidenciais devem ser retirados imediatamente após a impressão, evitando exposição ou acesso indevido.

7.18 Mesa e Tela Limpa

Todos os colaboradores, prestadores de serviços e visitantes que utilizam ou têm acesso às áreas de trabalho da Alias Tecnologia devem seguir as práticas de mesa limpa e tela limpa a fim de garantir a proteção das informações corporativas.

7.18.1 Mesa Limpa

- As áreas de trabalho devem permanecer organizadas e sem exposição de informações sensíveis.
- Ao se ausentar, mesmo que por pouco tempo, documentos, pen drives, anotações e outros materiais confidenciais devem ser guardados em locais seguros, como gavetas ou armários trancados.
- No final do expediente, a mesa deve estar limpa e sem materiais confidenciais à vista.
- Informações sensíveis não devem ser anotadas em post-its ou deixadas expostas sobre mesas, monitores ou murais.
- Não deve haver exposição de documentos ou mídias contendo informações classificadas em qualquer grau de sigilo, que possam ser danificadas, furtadas ou destruídas em caso de catástrofes, como incêndios, inundações ou explosões.
- Documentos e mídias de computador devem ser armazenados em armários ou estantes apropriadas e trancadas, ou em outras formas de mobília de segurança, quando não estiverem em uso, especialmente fora do horário de expediente.
- Informações empresariais sensíveis ou críticas devem ser trancadas em cofres ou arquivos à prova de fogo quando não estiverem em uso, principalmente quando não houver ninguém no escritório.

7.18.2 Tela Limpa

- Computadores e dispositivos corporativos devem ser configurados para bloquear automaticamente a tela após um curto período de inatividade.
- Sempre que se afastar da estação de trabalho, o colaborador e prestador de serviço deve bloquear a tela do dispositivo utilizado.
- Ao término do expediente, o usuário deve finalizar e bloquear o acesso a todos os sistemas e dispositivos sob sua responsabilidade.

7.18.3 Conscientização e Cumprimento

- O cumprimento desta diretriz faz parte das boas práticas de segurança da informação.
- O tema deve reforçado em processos de integração, treinamentos e campanhas internas.

- A equipe de Segurança da Informação poderá realizar verificações para garantir a conformidade e orientar as áreas em caso de ajustes necessários.
- Violações a esta diretriz devem ser reportadas imediatamente ao gerente ou supervisor direto do colaborador, para que sejam tomadas as ações corretivas cabíveis.

7.19 Permissão para Instalação de Softwares

Todas as instalações de softwares nos equipamentos corporativos da Alias Tecnologia devem ocorrer exclusivamente mediante autorização formal do departamento de Infraestrutura e Segurança da Informação, por meio de solicitação registrada no sistema de chamado corporativo.

É expressamente proibida a instalação de programas não licenciados, piratas, de uso pessoal ou sem relevância para as atividades corporativas, bem como de quaisquer aplicativos que possam comprometer a integridade, a disponibilidade ou a confidencialidade das informações.

O ambiente tecnológico da organização é protegido por políticas de controle de acesso implementadas via Active Directory, que, por meio de GPOs (Group Policy Objects), restringem privilégios administrativos e asseguram que:

- A instalação e desinstalação de programas não autorizados sejam bloqueadas;
- O acesso a processos críticos do sistema operacional seja restrito;
- Somente softwares homologados pela área responsável sejam utilizados.

A Alias Tecnologia adota, ainda, mecanismos de proteção em camadas, por meio de Firewall e WebFilter, destinados a prevenir o acesso a sites e conteúdos potencialmente maliciosos, evitando a instalação de códigos maliciosos, adwares ou outros softwares não permitidos.

Essas diretrizes têm como objetivo preservar a integridade, a disponibilidade e a segurança dos recursos tecnológicos e das informações corporativas da organização.

7.20 Uso de Dispositivos de Bluetooth

O uso de tecnologia Bluetooth nos ativos de informação corporativos é restrito e não autorizado, considerando os riscos associados à segurança da informação, como acesso não autorizado, interceptação de dados e introdução de dispositivos não confiáveis no ambiente corporativo.

Dessa forma, fica estabelecido que:

- É vedada a conexão de dispositivos Bluetooth (tais como fones de ouvido, teclados, mouses, celulares, smartwatches ou quaisquer outros dispositivos similares) aos equipamentos corporativos;
- O bloqueio da funcionalidade Bluetooth é realizado por meio de controles técnicos, incluindo regras de GPO (Group Policy Object), como medida preventiva de segurança;

- Qualquer tentativa de contorno, desativação ou violação dos controles de bloqueio configura descumprimento da Política de Segurança da Informação e estará sujeita às sanções previstas nas normas internas da organização;

- Exceções, por motivo operacional ou técnico, deverão ser formalmente solicitadas via sistema de chamados, avaliadas pelo Administrador de Segurança da Informação e autorizadas, com registro e aplicação de controles adequados.

7.21 Uso de Dispositivos Móveis

- Os dispositivos móveis pessoais não podem ser conectados em nenhuma hipótese a Wi-fi da rede de colaboradores.

- Os dispositivos móveis da organização devem possuir adesivo de identificação para reconhecer sua propriedade como sendo da Alias Tecnologia.

- Smartphones e tablets corporativos só poderão ser conectados na rede de visitantes.

- Os dispositivos fornecidos pela empresa são destinados exclusivamente às atividades profissionais, sendo proibido o uso pessoal que possa comprometer a segurança das informações.

- O colaborador é responsável pela guarda e uso correto do equipamento, devendo comunicar imediatamente qualquer perda, roubo, dano ou uso indevido à equipe de TI.

- Todos os dispositivos devem possuir senha de acesso, bloqueio automático e, quando aplicável, autenticação multifator (MFA).

- É proibido armazenar informações sensíveis localmente em dispositivos móveis. Todos os dados devem ser mantidos apenas em ambientes corporativos seguros (como SharePoint ou rede interna).

- O acesso remoto deve ocorrer apenas por conexões seguras, como VPN. É proibido o uso de redes públicas ou não seguras.

- Não é permitido instalar aplicativos, softwares ou extensões sem autorização da equipe de TI.

- Os notebooks devem permanecer atualizados, com antivírus ativo e configurações de segurança definidas pela empresa.

- Os equipamentos estão sujeitos a auditoria e controle remoto para garantir conformidade com as políticas de segurança.

- Em caso de desligamento, substituição ou manutenção, o colaborador deve devolver o dispositivo à área de TI para exclusão segura dos dados corporativos.

7.22 Descarte de Ativos, Arquivos, Documentos e Mídias

O descarte de ativos, documentos, mídias e equipamentos deve ser realizado de forma segura, responsável e em conformidade com as diretrizes desta política e com a legislação vigente.

Todos os colaboradores e prestadores de serviço da Alias Tecnologia devem assegurar que informações corporativas, especialmente as classificadas como sigilosas, sejam devidamente eliminadas, impedindo qualquer possibilidade de recuperação ou uso indevido.

Os ativos e equipamentos que contenham dados devem ter seus registros completamente apagados antes do descarte ou reutilização, garantindo a proteção das informações armazenadas. Documentos impressos e mídias físicas devem ser destruídos de modo a inviabilizar sua leitura ou reconstrução.

O descarte deve ser conduzido de maneira ambientalmente responsável e sob a gestão do departamento de segurança da informação, respeitando os prazos legais de retenção e os controles patrimoniais da empresa.

7.23 Uso de Sistemas em Nuvem ou Terceirização de Infraestrutura e Servidores

O acesso à administração dos sistemas em nuvem privada deve ser restrito exclusivamente ao departamento de Segurança da Informação e Infraestrutura. Todo acesso administrativo deve ser realizado por meio de conexão segura, utilizando OpenVPN.

Os provedores de nuvem privada devem garantir sistemas de backup confiáveis, preferencialmente utilizando ferramentas como o Veeam, assegurando a recuperação das máquinas virtuais (VMs) quando necessário.

Os datacenters que hospedam os serviços em nuvem devem possuir certificação ISO 27001 válida, garantindo a proteção das informações. Caso a certificação esteja vencida, o datacenter tem até seis meses para apresentar uma nova certificação.

7.24 Continuidade de Negócio

A Alias Tecnologia estabelece que a continuidade de negócios deve ser garantida para todos os processos e sistemas críticos da organização, assegurando operação ininterrupta mesmo diante de falhas, incidentes ou desastres.

O Plano de Continuidade de Negócios (PCN), conforme descrito no PR-119 Procedimento para Continuidade de Negócio, deve ser mantido atualizado, testado e revisado de forma sistemática, assegurando que os colaboradores conheçam suas responsabilidades e procedimentos.

Devem ser realizados exercícios que incluam treinamento da equipe, simulações de interrupções nos sistemas e na matriz, acionamento de redundâncias e restauração completa das funcionalidades críticas.

Todos os testes e revisões devem ser documentados e analisados para promover a melhoria contínua do PCN, garantindo que a Alias Tecnologia mantenha resiliência operacional, proteção de seus ativos de informação e atendimento seguro às necessidades dos clientes e partes

interessadas.

7.25 Uso Correto de Inteligencia Artificial

O uso de recursos de Inteligência Artificial (IA) na Alias Tecnologia deve ocorrer de forma ética, responsável e em conformidade com a PO-11 Política de Governança da Inteligência Artificial, documento que estabelece as diretrizes específicas para sua aplicação.

Toda utilização de ferramentas ou modelos de IA deve priorizar a proteção das informações corporativas, a privacidade dos dados e a integridade dos processos organizacionais, sendo vedado o uso para fins pessoais ou que comprometam a segurança e a confidencialidade das informações da empresa.

8. VIOLAÇÕES E SANÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

São consideradas violações à Política de Segurança da Informação todas as ações, omissões ou comportamentos que possam comprometer a confidencialidade, integridade, disponibilidade ou privacidade das informações da Alias Tecnologia, incluindo, mas não se limitando a:

- Uso indevido ou divulgação não autorizada de informações internas, dados de clientes, documentos corporativos ou segredos comerciais.
- Acesso, cópia, modificação, exclusão ou compartilhamento de dados e arquivos sem a devida autorização.
- Utilização inadequada de recursos tecnológicos (como computadores, redes, e-mails, sistemas e softwares) para fins pessoais, ilícitos, antiéticos ou em desacordo com as políticas da empresa.
- Armazenamento de informações sensíveis fora dos locais autorizados, como computadores pessoais, mídias removíveis ou serviços de nuvem não corporativos.
- Negligência na proteção das credenciais de acesso, incluindo compartilhamento de senhas, uso de senhas fracas ou falha em realizar o bloqueio de tela ao se ausentar do posto de trabalho.
- Tentativas de burlar mecanismos de segurança, como antivírus, firewall, bloqueios de acesso, criptografia ou controle de dispositivos.
- Não comunicação imediata de incidentes de segurança, suspeitas de violação ou descumprimentos das normas ao Administrador de Segurança da Informação.
- Obstrução ou falta de colaboração em auditorias, investigações ou ações corretivas relacionadas à segurança da informação.
- Instalação, utilização ou acesso a aplicações, sistemas, ferramentas ou serviços web sem

a prévia aprovação do Departamento de Segurança da Informação, incluindo softwares gratuitos, extensões de navegador ou soluções em nuvem não homologadas pela empresa.

Toda e qualquer violação será tratada com seriedade, independentemente da intenção, podendo ser considerada falta grave conforme a gravidade do impacto causado.

O não cumprimento das diretrizes e normas estabelecidas nesta Política de Segurança da Informação poderá resultar em medidas disciplinares e legais, aplicáveis a colaboradores, prestadores de serviço, estagiários ou terceiros vinculados à Alias Tecnologia.

As sanções poderão incluir, conforme a gravidade da ocorrência:

- Advertência verbal ou escrita;
- Suspensão das atividades;
- Rescisão contratual por justa causa;
- Responsabilização civil e/ou criminal, conforme a legislação vigente;
- Outras medidas cabíveis conforme descritas no **MA-02 Manual de Recursos Humanos.**

Além das penalidades, poderão ser adotadas ações corretivas e preventivas, como reavaliação de acessos, reforço de controles, treinamentos adicionais e revisão de procedimentos internos.

9. CONTROLE DAS REVISÕES

Revisão	Data	Histórico das Alterações
00	05/12/2024	Emissão inicial do documento.
01	10/02/2025	Alteração item 6.1 alteração de periodicidade do comitê, 6.27 adições dos contatos das autoridades
02	21/03/2025	Inclusão do item 6.2.1 Objetivos da Política de Segurança da Informação.
03	04/12/2025	Revisão completa da Política de Segurança da Informação, com aprimoramento da comunicação e alinhamento ao negócio da Alias Tecnologia. Incluído o item 5 – Princípios de Segurança e Privacidade da Informação, incluído e atualizado os conteúdos no item 6 – Diretrizes Gerais de Segurança da Informação, além da inclusão e revisão de conteúdos no item 7 – Diretrizes Específicas de Segurança da Informação.
04	28/01/2026	Inclusão de diretrizes referentes às regras de uso de dispositivos Bluetooth no item 7.20.

ALIAS®
20 anos

www.aliasnet.com.br

Alias Tecnologia

contato@aliasnet.com.br

0800 068 6868

(41) 99811-2794