Política de Segurança da Informação

Sumário

1. Introdução

A **ALPINO INDÚSTRIA METALÚRGICA LTDA** estabelece esta Política de Segurança da Informação (PSI) como pilar central de sua governança. Ciente da importância estratégica dos dados para a sustentabilidade do negócio, a organização compromete-se com a preservação da Tríade CID (Confidencialidade, Integridade e Disponibilidade) dos ativos de informação de seus clientes, colaboradores e parceiros. Este documento formaliza a conformidade da **ALPINO** com a LGPD (Lei nº 13.709/2018) e regulamentações do setor automotivo e metalúrgico. Como controladora e operadora de dados, a empresa reconhece que controles rigorosos de segurança são salvaguardas essenciais contra fraudes, vazamentos e interrupções operacionais na cadeia de suprimentos.

Para a **ALPINO**, a Informação é um ativo indispensável que engloba desde segredos de manufatura até dados pessoais. A segurança desses ativos depende da gestão integrada entre o conteúdo informacional e seus suportes: infraestrutura de TI, sistemas de automação ind'ustrial e o capital humano. Esta PSI define as diretrizes de proteção e o comportamento esperado de todos os indivíduos vinculados à organização.

2. Objetivo

O objetivo central desta Política é estabelecer as diretrizes estratégicas que orientam a proteção do patrimônio informativo da **ALPINO** contra ameaças internas ou externas, sejam elas deliberadas ou acidentais. Através deste instrumento normativo, a organização busca consolidar uma cultura onde a segurança da informação seja intrínseca a cada processo produtivo e administrativo, garantindo a aplicação rigorosa da Tríade CID (Confidencialidade, Integridade e Disponibilidade), assegurando que o acesso aos dados seja restrito a indivíduos autorizados e que a fidedignidade dos registros seja mantida contra qualquer alteração indevida.

Além da proteção técnica, esta Política visa assegurar a continuidade operacional do negócio, minimizando os impactos de possíveis incidentes por meio de uma gestão de riscos proativa, resiliente e alinhada aos objetivos estratégicos da companhia. Ela atua como o documento de autoridade máxima (Política Mestra) que confere coesão às normas operacionais específicas, garantindo que todos os colaboradores e parceiros compreendam suas responsabilidades legais e éticas no manejo de ativos. Em última análise, busca-se não apenas o cumprimento da legislação vigente (LGPD), mas a construção de um ambiente digital confiável que sustente o crescimento e proteja a reputação da **ALPINO** perante o mercado e seus *stakeholders*.

3. Escopo

As diretrizes estabelecidas nesta Política de Segurança da Informação (PSI) aplicam-se integralmente a todas as unidades de negócio da **ALPINO**, abrangendo, sem distinção, todos os seus diretores, colaboradores efetivos, estagiários, jovens aprendizes e prestadores de serviço terceirizados. O cumprimento das normas aqui descritas é mandatório para qualquer indivíduo que possua credenciais de acesso aos sistemas corporativos, que utilize a infraestrutura tecnológica ou que manipule informações de propriedade da organização, independentemente do regime de contratação ou nível hierárquico ocupado.

No que tange ao ecossistema tecnológico e ao perímetro físico, esta política estende-se aos seguintes domínios:

- **Ativos de Informação e Suporte**: Abrange todos os dados brutos, segredos industriais, propriedade intelectual, infraestrutura de rede (LAN/WAN),

servidores físicos e virtuais, sistemas ERP, bancos de dados e, especialmente, as ferramentas de automação industrial que sustentam a operação fabril.

- **Dispositivos e Equipamentos**: Aplica-se ao uso de estações de trabalho, notebooks, dispositivos móveis (corporativos ou pessoais em regime de BYOD), meios de armazenamento removíveis e periféricos, conforme detalhado nas normas (SGSI 0005 – Política de Dispositivos Móveis) e (SGSI 0006 – Política de Gestão de Ativos).
- **Ambiente Geográfico**: As regras são válidas tanto para as atividades executadas nas dependências físicas da **ALPINO** quanto para aquelas realizadas fora do perímetro da sede, incluindo Trabalho Remoto (SGSI 0003 – Política de Trabalho Remoto), viagens de negócios e interações em ambientes de clientes ou fornecedores.
- **Terceiros e Parceiros**: Empresas parceiras, consultorias e fornecedores que, por necessidade contratual, tenham acesso ao ambiente lógico ou físico da **ALPINO**, devem aderir a estas diretrizes como condição mandatória para a manutenção de seus vínculos comerciais e contratuais.

Esta PSI deve ser interpretada e executada em conjunto com as normas específicas que detalham os controles operacionais e técnicos para cada domínio de segurança. O desconhecimento das regras estabelecidas não será aceito como justificativa para o seu descumprimento, uma vez que a **ALPINO** assegura a ampla divulgação deste instrumento e o fornecimento do treinamento necessário para sua correta compreensão e aplicação.

4. Definições e Termos

Termos	Definições
Ativo de Informação	Refere-se a todo e qualquer dado, conhecimento ou conteúdo informacional que possua valor estratégico para a **ALPINO**, independentemente da sua forma de armazenamento (digital ou física). Inclui segredos industriais, cadastros de clientes, projetos de engenharia e dados pessoais protegidos pela LGPD.
Ativo de Suporte	Compreende os recursos que sustentam o ciclo de vida da informação, tais como hardware (servidores, notebooks), softwares (ERP, sistemas de automação), infraestrutura de rede e os próprios recursos humanos.
BYOD (*Bring Your Own Device*)	Conceito que descreve a prática de colaboradores utilizarem os seus próprios dispositivos pessoais (smartphones, tablets ou notebooks) para aceder a recursos corporativos, como e-mails ou sistemas de gestão. O uso de BYOD na **ALPINO** exige a adesão às normas de segurança específicas e a aceitação de controlos de gestão remota por parte da equipa de TI.
Incidente de Segurança	Evento adverso que comprometa a segurança da rede ou dos sistemas de informação, resultando em violação de dados ou interrupção de serviços críticos.
LGPD	Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), que dispõe sobre o tratamento de dados pessoais com o objetivo de proteger os direitos fundamentais de liberdade e privacidade.

Tríade CID	Conceito fundamental de segurança composto por três pilares: **Confidencialidade** (garantia de que a informação só é acedida por quem de direito); **Integridade** (garantia de que a informação não foi alterada indevidamente); **Disponibilidade** (garantia de que a informação e os sistemas estão prontos para uso quando necessário).
Malware	Categoria de software (vírus, ransomware, trojans) desenvolvida para executar ações maliciosas, infiltrar-se em sistemas e causar danos ou extração ilícita de dados.
Criptografia	Mecanismo técnico de proteção que transforma dados legíveis em códigos inteligíveis, garantindo que apenas quem possui a chave de decodificação acesse o conteúdo.
Controle de Acesso	Conjunto de processos físicos e lógicos (senhas, biometria, perfis de acesso) que gerencia quem pode acessar o quê, quando e como dentro do ambiente da **ALPINO**.

5. Papéis e Responsabilidades

Diretoria Executiva:

- Atuar como o patrocinador máximo do SGSI, provendo os recursos orçamentários, humanos e tecnológicos necessários para a viabilidade das camadas de proteção. Deve assegurar que a Segurança da Informação seja tratada como um pilar estratégico de continuidade de negócio e não apenas como um suporte operacional.
- Deter a responsabilidade final sobre a aceitação de riscos residuais que possam impactar a operação ou a reputação da **ALPINO**. Validar as metas de conformidade e garantir que os objetivos do SGSI estejam alinhados às diretrizes corporativas e aos requisitos legais vigentes, incluindo a LGPD).
- Liderar pelo exemplo no cumprimento das normas e apoiar a aplicação de sanções disciplinares. Deve garantir que a Segurança da Informação seja integrada aos indicadores de desempenho da alta gestão.

Comitê de Segurança da Informação e Privacidade:

- A estrutura, as competências e o rito de atuação deste órgão são regidos pela norma (SGSI 0004 - Política do Comitê de Segurança da Informação e Privacidade). O Comitê atua como a autoridade máxima para a revisão, atualização e interpretação desta PSI e das normas específicas. Deve garantir que as políticas reflitam as mudanças nas ameaças cibernéticas e os requisitos rigorosos do setor automotivo e metalúrgico.
- Avaliar reportes de incidentes críticos, coordenando a resposta estratégica e definindo os protocolos de comunicação externa. Possui o poder de decisão sobre a interrupção de processos produtivos caso haja risco iminente de vazamento de dados ou dano sistêmico.
- Monitorar a eficácia dos controles por meio de indicadores e auditorias. É o órgão responsável por analisar violações graves, garantindo a imparcialidade no exame das ocorrências e determinando as medidas administrativas ou judiciais cabíveis.

TI é responsável por:

- Atua como a única autoridade competente para a instalação, configuração e manutenção de qualquer ativo de software ou hardware, sendo terminantemente proibido o procedimento de instalação por usuários comuns. A equipe deve garantir o bloqueio técnico de privilégios de administrador em todas as estações de trabalho, realizando a validação prévia de segurança e compatibilidade de cada aplicação antes de sua disponibilização.
- Deter a autoridade máxima para a aprovação final técnica de segurança, validando se a implementação de novos ativos ou tecnologias está em conformidade com as diretrizes de risco da **ALPINO**. É o único responsável por analisar, documentar e conceder aprovação formal para qualquer exceção a esta política, devendo revisar essas concessões anualmente para garantir a segurança contínua do ecossistema.
- Extrair mensalmente relatórios de status e realizar conciliações trimestrais físicas e lógicas em ativos críticos para detectar dispositivos não autorizados. Deve garantir a aplicação rigorosa de correções de segurança (patches), a conformidade das licenças de uso e coordenar o descarte seguro de ativos, emitindo certificados de eliminação definitiva de dados.

Gestores da área:

- Definir formalmente a classificação de Confidencialidade, Integridade e Disponibilidade (CID) dos ativos sob sua gestão. Atuam como os "Proprietários da Informação", determinando quem possui a necessidade de negócio para acessar cada recurso.
- Assegurar que os ativos sejam utilizados exclusivamente para finalidades profissionais, monitorando o comportamento de sua equipe em relação ao uso de recursos tecnológicos. Devem revisar semestralmente se os privilégios de acesso de seus subordinados permanecem alinhados às funções desempenhadas.
- Notificar imediatamente os departamentos de TI e RH sobre qualquer movimentação de pessoal (promoções, transferências ou desligamentos) para garantir a revogação ou ajuste imediato dos acessos, mitigando riscos de acesso indevido por contas órfãs.

Todos os colaboradores da ALPINO:

- Manter a integridade física dos equipamentos recebidos e garantir o sigilo absoluto de suas senhas, chaves de acesso e duplo fator de autenticação (MFA). É expressamente proibido o compartilhamento de credenciais ou o uso de recursos para fins pessoais que comprometam a segurança da rede.
- Informar imediatamente à TI sobre qualquer falha, perda de dispositivos móveis, suspeita de *phishing* ou comportamentos anômalos nos sistemas. Ocultar ou retardar o reporte de um incidente é considerado descumprimento desta política e passível de sanção.
- No encerramento do vínculo, devolver todos os ativos em perfeitas condições e colaborar com os protocolos de remoção de dados corporativos em dispositivos BYOD. O colaborador reconhece que sua responsabilidade de sigilo sobre os segredos industriais da **ALPINO** permanece mesmo após o fim do contrato.

6. Diretrizes Gerais de Segurança

6.1 Controle de Acesso e Identidade Digital

- O acesso aos ativos de informação da **ALPINO** é regido estritamente pelo princípio do privilégio mínimo, garantindo que cada colaborador ou terceiro possua apenas as permissões essenciais para o desempenho de suas funções contratuais sob os preceitos de "*Need to Know*" (necessidade de conhecer) e "*Least Privilege*" (menor privilégio). Os procedimentos operacionais para solicitação, concessão, alteração e revogação de privilégios estão detalhados na norma (SGSI 0008 - Política de Gestão de Acessos), sendo a concessão um processo formal via sistema de chamados, condicionado à aprovação do gestor e validação técnica da TI. É terminantemente proibida a criação de perfis baseados em "similaridade" ou permissões genéricas; cada acesso deve ser justificado por necessidade de negócio e revisado obrigatoriamente em casos de mudança de cargo ou departamento.
- O acesso aos ativos de informação da **ALPINO** é regido estritamente pelo princípio do privilégio mínimo, garantindo que cada colaborador ou terceiro possua apenas as permissões essenciais para o desempenho de suas funções contratuais. Os procedimentos operacionais para solicitação, concessão, alteração e revogação de privilégios estão detalhados na norma (SGSI 0008 - Política de Gestão de Acessos). A concessão de credenciais é um processo formal, obrigatório e documentado via sistema de chamados, condicionado à aprovação expressa do gestor da área e à validação técnica da equipe de TI. É terminantemente proibida a criação de perfis de acesso baseados em "similaridade" ou a manutenção de permissões genéricas; cada acesso deve ser justificado por uma necessidade clara de negócio e revisado obrigatoriamente caso haja mudança nas atribuições ou no departamento do colaborador.
- A identidade digital é pessoal, intransferível e sua proteção é de responsabilidade exclusiva e indelegável do titular. Devem ser utilizadas senhas de alta complexidade conforme os requisitos técnicos da norma (SGSI 0001 – Política de Gerenciamento de Senhas), sendo mandatória a ativação de Autenticação Multifator (MFA) em todos os sistemas críticos, acessos remotos (VPN), e-mail corporativo e, sem exceção, em contas com privilégios administrativos. O compartilhamento de credenciais, o uso de senhas óbvias ou a anotação de chaves de acesso em locais inseguros são classificados como violações gravíssimas, uma vez que comprometem a rastreabilidade das ações e a integridade do ambiente tecnológico da **ALPINO**.
- A manutenção da base de usuários ocorre por meio de um processo rigoroso de recertificação de acessos. A TI e os Gestores de Área devem realizar revisões formais periódicas para as contas dos usuários, garantindo a higienização das permissões e assegurando que nenhum colaborador mantenha acessos obsoletos. Em casos de desligamento ou suspensão de contrato, a revogação das credenciais deve ocorrer de forma imediata (em tempo real), visando eliminar o risco de "contas órfãs" que representam vetores críticos de intrusão no ambiente corporativo e industrial.
- Para contas de terceiros e prestadores de serviço, a **ALPINO** aplica adicionalmente a política de validade pré-determinada, onde o acesso é

configurado para expirar automaticamente ao fim do período contratual estabelecido. Qualquer necessidade de extensão do prazo exige uma nova solicitação formal, análise de risco pela TI e aprovação do gestor responsável, garantindo que o acesso externo seja mantido apenas pelo tempo estritamente necessário para o cumprimento das obrigações contratuais.

6.2 Proteção de Ativos e Estações de Trabalho

- Os ativos de suporte, incluindo notebooks, smartphones, tablets e coletores de dados, são ferramentas de propriedade exclusiva da **ALPINO**, destinadas estritamente para a execução de atividades profissionais e objetivos de negócio. O usuário detém a responsabilidade como guardião legal e fiel depositário do ativo (SGSI 0006 – Política de Gestão de Ativos), devendo zelar pela sua integridade física contra quedas, derramamento de líquidos, furtos ou acessos por terceiros, inclusive familiares. É terminantemente proibida qualquer modificação nas configurações de hardware ou a desativação manual de agentes de proteção cibernética (como Antivírus, EDR e Firewalls locais) instalados pela TI, sendo qualquer tentativa de *bypass* desses controles tratada como um incidente de segurança grave.
- É mandatório o bloqueio imediato da sessão na estação de trabalho (atalho Windows+L ou equivalente) sempre que o colaborador se ausentar de sua mesa, independentemente do tempo de afastamento, visando impedir o acesso indevido por indivíduos não autorizados ou a visualização de dados confidenciais. Complementarmente, a **ALPINO** adota a política de "Mesa e Tela Limpa", na qual é vedado deixar documentos impressos com dados sensíveis, mídias removíveis (pendrives, HDs externos) ou anotações físicas contendo credenciais expostos no ambiente de trabalho durante ou após o expediente. Ao término da jornada, o colaborador deve garantir que todos os ativos e documentos físicos de nível III ou IV (Confidencial/Restrito) sejam armazenados em gavetas ou armários com chave, mantendo a organização e a segurança visual do perímetro.
- O uso de ativos móveis corporativos ou dispositivos pessoais no modelo BYOD (SGSI 0005 – Política de Dispositivos Móveis) fora do perímetro físico da **ALPINO** exige a aplicação de criptografia total de disco e o uso obrigatório de túneis seguros via VPN para o tráfego de qualquer dado institucional. Em cenários de perda, roubo ou furto de ativos móveis, o usuário deve notificar a equipe de TI em um prazo máximo de 1 (uma) hora para que os protocolos de contenção sejam executados, visando mitigar o risco de vazamento de segredos industriais. Ao aceitar o uso de recursos tecnológicos móveis, o colaborador declara ciência e autoriza a capacidade de "limpeza remota" (*remote wipe*) pela TI, procedimento que elimina todos os dados do dispositivo para preservar o sigilo da organização em caso de comprometimento físico do ativo.

6.3 Resiliência e Gestão de Ameaças

- A **ALPINO** mantém um ciclo contínuo de identificação, análise e correção de falhas em toda a sua infraestrutura, conforme as normas (SGSI 0010 – Política de Vulnerabilidade e Malware) e (SGSI 0014 – Política de Gestão de Patchs). A

equipe de TI é a autoridade responsável por coordenar e aplicar atualizações críticas de sistemas operacionais, *firmwares* e aplicações em janelas de manutenção previamente homologadas, garantindo que o ambiente corporativo e industrial esteja protegido contra *exploits* e vulnerabilidades conhecidas (CVEs). Este processo de "*patch management*" prioriza ativos que processam dados de nível III e IV, assegurando a proteção da rede sem comprometer a continuidade da linha de produção ou causar indisponibilidade nos sistemas de gestão.

- Como pilar de estabilidade, qualquer alteração significativa na infraestrutura, sistemas ou rede de automação (OT) deve seguir rigorosamente os fluxos de aprovação e execução estabelecidos na (SGSI 0011 – Política de Gestão de Mudanças). Isso implica que modificações de hardware, software ou configurações críticas devem ser previamente documentadas, avaliadas quanto aos riscos de segurança e aprovadas pela autoridade competente antes da implementação em ambiente produtivo. Mudanças em sistemas que suportam dados Restritos ou Confidenciais exigem um plano de contingência (*rollback*) para garantir a restauração imediata do estado anterior em caso de falha, minimizando impactos operacionais e garantindo a rastreabilidade exigida por auditorias externas.
- Para garantir a resiliência frente a desastres naturais, falhas de hardware ou ataques cibernéticos destrutivos, todos os dados críticos são protegidos por rotinas de *backup* automatizadas com redundância geográfica, conforme a norma (SGSI 0002 – Política de Backup e Restore de Dados). A organização adota a estratégia de *backups* imutáveis e tecnicamente segregados da rede de produção (*Air Gap*), o que impede a propagação de *malwares* e assegura a fidedignidade dos dados. Testes de integridade e restauração (*Restore*) devem ser executados e documentados pela TI semestralmente, validando a recuperação total dos ativos dentro dos padrões de conformidade.
- Qualquer anomalia sistêmica, suspeita de infecção ou tentativa de *phishing* deve ser reportada imediatamente à TI pelos canais oficiais, seguindo a norma (SGSI 0007 – Política de Norma de Resposta a Incidente de Segurança da Informação). A **ALPINO** mantém Planos de Continuidade de Negócios (PCN) e de Recuperação de Desastres (DRP) estruturados para restabelecer serviços essenciais, como faturamento e automação industrial, dentro dos prazos de RTO (*Recovery Time Objective*) definidos pela diretoria. Este gerenciamento visa minimizar impactos financeiros e reputacionais, garantindo uma capacidade de resposta rápida para isolar ameaças e retomar as operações em um estado seguro e auditável.

6.4 Criptografia e Segurança nas Comunicações

- A **ALPINO** estabelece o uso obrigatório de criptografia de nível industrial para assegurar a confidencialidade e a integridade de todos os dados armazenados em seus ativos. Conforme a norma (SGSI 0009 – Política de Criptografia), todos os dispositivos portáteis, incluindo notebooks, tablets e smartphones, devem possuir criptografia de disco total (*Full Disk Encryption*) ativa e configurada pela TI antes da entrega ao usuário. A seleção de algoritmos deve priorizar padrões reconhecidos internacionalmente e homologados por órgãos de segurança,

como o AES-256, sendo terminantemente vedada a utilização de métodos de cifragem obsoletos, vulneráveis ou "proprietários" que não tenham passado pela validação técnica e análise de risco da equipe de Segurança da Informação.

- Toda e qualquer transmissão de dados classificados como Confidenciais (Nível III) ou Restritos (Nível IV) através de redes públicas ou externas deve ser realizada, obrigatoriamente, por meio de canais seguros, utilizando protocolos de comunicação criptografados como HTTPS/TLS 1.2 (ou superior) e VPN corporativa. É expressamente proibido o tráfego de segredos industriais, projetos de engenharia ou dados pessoais sensíveis em canais de comunicação abertos, e-mails sem proteção ou aplicativos de mensagens que não possuam criptografia de ponta-a-ponta homologada. Esta diretriz visa mitigar riscos de interceptação por terceiros mal-intencionados, ataques do tipo (*Man-in-the-Middle*) e garantir a autenticidade das pontas de comunicação durante o intercâmbio de informações estratégicas da **ALPINO**.
- As chaves de criptografia, chaves mestras e certificados digitais são considerados ativos de alta criticidade e devem ser gerenciados e armazenados exclusivamente pela TI em infraestruturas seguras ou cofres de senhas homologados. O ciclo de vida dessas chaves, incluindo geração, custódia, rotação e revogação, deve seguir protocolos rígidos para impedir o acesso de pessoal não autorizado ou a exposição de segredos em ambientes de desenvolvimento. A perda, o extravio ou o compartilhamento indevido de uma chave de criptografia é tratado como um incidente de segurança gravíssimo, uma vez que o comprometimento de uma única credencial mestre pode invalidar toda a camada de proteção do ecossistema de dados, resultando em danos catastróficos à propriedade intelectual da organização.

6.5 Monitoramento, Auditoria e Ética Digital

- A **ALPINO** reserva-se o direito de monitorar e auditar o uso de todos os ativos tecnológicos e recursos de comunicação fornecidos aos seus colaboradores, incluindo tráfego de internet, e-mails corporativos, logs de sistemas e arquivos armazenados em rede. Este monitoramento é realizado com o objetivo estrito de garantir a segurança dos ativos de informação, prevenir incidentes cibernéticos e assegurar a conformidade com a LGPD, não gerando para o usuário qualquer expectativa de privacidade no uso de ferramentas de propriedade da organização. O uso das ferramentas para fins pessoais deve ser mínimo e nunca deve comprometer a integridade dos sistemas ou infringir as regras de conduta estabelecidas.
- Todas as ações realizadas em sistemas de gestão (ERP), bancos de dados e infraestrutura de rede são devidamente registradas em logs de auditoria conforme a norma (SGSI 0013 – Política de Gestão de Logs). Estes logs devem ser protegidos contra alteração ou exclusão não autorizada, garantindo sua integridade, e mantidos pelo período mínimo definido pela organização e requisitos legais aplicáveis. A **ALPINO** realiza auditorias periódicas, baseadas na norma (SGSI 0015 – Política de Escopo de Auditorias), para validar se os registros estão sendo gerados corretamente e se há sinais de comportamentos anômalos. Qualquer tentativa de burlar, apagar ou modificar esses registros de

auditoria será tratada como uma infração gravíssima, passível de sanções disciplinares e legais imediatas.

- O acesso aos recursos tecnológicos da **ALPINO** deve ser pautado pela ética, legalidade e profissionalismo, sendo vedada a utilização dos ativos para a prática de assédio, disseminação de notícias falsas (*fake news*), acesso a conteúdo pornográfico ou atividades político-partidárias. O colaborador é responsável direto por qualquer conteúdo transmitido ou armazenado sob sua credencial, devendo zelar pela imagem institucional da organização em todos os pontos de interação digital, inclusive em redes sociais quando houver menção à empresa. O descumprimento destas diretrizes éticas compromete a confiança depositada no profissional e aciona automaticamente os protocolos de investigação do Comitê de Segurança da Informação.

6.6 Gestão de Pessoas e Segurança

- A segurança da informação na **ALPINO** inicia-se antes da concessão de qualquer acesso físico ou lógico e estende-se para além do término do vínculo contratual. O processo de recrutamento e seleção para funções que lidem com dados de nível III (Confidencial) e IV (Restrito) deve incluir verificações de antecedentes e referências profissionais, assegurando que o candidato possua a integridade necessária para o manejo de segredos industriais e propriedade intelectual da organização. Todo novo colaborador deve passar obrigatoriamente por um treinamento de integração focado em segurança, onde será instruído sobre as diretrizes desta PSI e deverá assinar formalmente o Termo de Ciência e Responsabilidade antes do início de suas atividades.
- Durante a vigência do contrato, a **ALPINO** promoverá ações contínuas de conscientização e educação digital, visando manter a equipe atualizada sobre as novas ameaças cibernéticas, técnicas de engenharia social e procedimentos internos de proteção. É responsabilidade do departamento de Recursos Humanos, em conjunto com os Gestores de Área, garantir que qualquer alteração nas responsabilidades do colaborador (como promoções ou transferências de setor) seja acompanhada da revisão imediata de seus privilégios de acesso, aplicando o princípio do "menor privilégio" para evitar que o acúmulo de permissões desnecessárias gere vulnerabilidades ao ecossistema de dados.
- No encerramento do vínculo, seja por iniciativa da empresa ou do colaborador, deve-se executar o protocolo formal de desligamento (*offboarding*) de segurança. Este procedimento inclui a revogação imediata de todas as credenciais de acesso aos sistemas, e-mails, VPNs e portarias físicas, além da devolução obrigatória de todos os ativos de suporte (notebooks, smartphones, tokens e cartões de acesso) em perfeito estado de conservação. O colaborador será expressamente advertido, em sua entrevista de desligamento, de que as obrigações de sigilo e confidencialidade sobre os ativos de informação da **ALPINO** permanecem juridicamente válidas e exigíveis, sujeitando o infrator às sanções civis e criminais cabíveis em caso de vazamento de informações estratégicas após a sua saída.

6.7 Desenvolvimento Seguro e Gestão de Softwares

- A **ALPINO** estabelece que a segurança deve ser integrada em todas as fases do ciclo de vida de um software ou sistema, desde a sua concepção até o seu descarte, seguindo as diretrizes da norma (SGSI 0012 – Política de Desenvolvimento de Sistemas). Para garantir a integridade operacional, os ambientes de desenvolvimento, homologação e produção devem permanecer segregados lógica e administrativamente, evitando acessos indevidos ou alterações não autorizadas em sistemas produtivos. Esta norma visa assegurar que códigos-fonte e arquiteturas sejam protegidos contra vulnerabilidades críticas, como injeções de código malicioso ou falhas de autenticação.
- No caso de softwares adquiridos de terceiros ou desenvolvidos sob demanda por parceiros externos, a equipe de TI deve realizar uma validação técnica prévia para assegurar que o produto atende aos requisitos mínimos de segurança da organização. É expressamente proibida a utilização de softwares não licenciados ou a realização de alterações em sistemas críticos sem a devida homologação em ambiente de testes. O armazenamento de códigos-fonte e a gestão de bibliotecas devem ocorrer em repositórios seguros, com acesso restrito e trilhas de auditoria para prevenir o vazamento de propriedade intelectual e segredos industriais da **ALPINO**.

6.8 Segurança Física e Ambiental

- A **ALPINO** estabelece que áreas críticas, como salas de servidores (Data Centers), hubs de infraestrutura de rede e arquivos físicos contendo documentos confidenciais, devem possuir perímetros de segurança definidos com controles de acesso restritos e monitoramento constante por CFTV. O acesso a estas áreas é limitado exclusivamente a pessoal autorizado e deve ser formalmente registrado em trilhas de auditoria (físicas ou digitais), garantindo a proteção dos ativos de hardware contra danos, interferências, sabotagens ou acessos indevidos.
- Os ambientes que abrigam infraestrutura tecnológica devem ser dotados de controles ambientais adequados, incluindo sistemas de climatização de precisão e mecanismos de proteção contra incêndio e falhas elétricas (nobreaks), visando garantir a disponibilidade e a integridade física dos equipamentos. É responsabilidade da TI e da Manutenção assegurar que estes locais estejam protegidos contra ameaças externas e desastres naturais que possam comprometer a continuidade do negócio.
- A entrada de visitantes, prestadores de serviço ou terceiros nas dependências da organização deve ser rigorosamente controlada, identificada e documentada na recepção. É obrigatório o acompanhamento por um colaborador responsável durante toda a permanência em áreas de manipulação de dados ou infraestrutura crítica. A circulação de pessoas não autorizadas em áreas restritas é tratada como um incidente de segurança, devendo ser reportada imediatamente a equipe de TI.

7. Classificação da Informação

A **ALPINO** adota quatro níveis de classificação para garantir que cada dado receba o nível de proteção adequado ao seu valor e risco.

- **Público**: Informações classificadas como públicas são aquelas cujo acesso é livre tanto para colaboradores internos quanto para o público externo, não exigindo controles de confidencialidade. A divulgação dessas informações não acarreta prejuízos financeiros, operacionais ou danos à reputação da **ALPINO**, sendo utilizadas para fortalecer a transparência e a marca.
- **Interno**: As informações de nível Interno são destinadas exclusivamente ao uso dos colaboradores e parceiros autorizados da **ALPINO** para a execução de suas rotinas de trabalho e processos administrativos. Embora sua divulgação externa não seja autorizada, o impacto de um eventual vazamento é considerado baixo, afetando apenas a organização interna sem comprometer segredos estratégicos. Estão inseridos nesta categoria os manuais de treinamento, listas de ramais internos, circulares administrativas, comunicados de RH e as versões vigentes das políticas e normas internas do SGSI.
- **Confidencial**: Este nível abrange dados sensíveis que exigem proteção rigorosa, pois o acesso por pessoas não autorizadas pode causar prejuízos financeiros significativos, sanções legais ou danos operacionais. O acesso é restrito a grupos específicos de usuários que possuem a "necessidade de saber" para o desempenho de suas funções críticas. Exemplos incluem dados pessoais protegidos pela LGPD, contratos com fornecedores, tabelas de preços, informações de faturamento e dados de saúde dos colaboradores. O manuseio desses dados deve, obrigatoriamente, ser realizado em sistemas protegidos por MFA e criptografia, conforme diretrizes das normas de apoio.
- **Restrito**: O nível Restrito representa o grau máximo de sigilo da **ALPINO**, protegendo ativos de informação que constituem o diferencial competitivo e a propriedade intelectual da organização. O vazamento ou comprometimento destas informações causaria danos catastróficos, irreversíveis e ameaçaria a continuidade do negócio. Esta classificação é aplicada a segredos industriais, fórmulas metalúrgicas exclusivas, projetos de engenharia de novos produtos, planos estratégicos da diretoria e credenciais de administração de infraestrutura crítica. Informações deste nível devem ser armazenadas em ambientes isolados, com logs de acesso monitorados em tempo real e descarte físico via destruição definitiva.

8. Sanções e Penalidades

8.1 Enquadramento e Graduação de Faltas

- O descumprimento de qualquer diretriz estabelecida nesta Política de Segurança da Informação ou em suas normas específicas constitui infração disciplinar passível de punição imediata. As violações serão analisadas e classificadas pelo Comitê de Segurança da Informação e Privacidade em níveis de gravidade: leve, média ou grave. Para esta gradação, serão considerados critérios objetivos como a reincidência do colaborador em falhas de segurança, a existência de dolo (intenção) ou culpa (negligência/imprudência), e a magnitude do dano real ou potencial causado aos ativos tecnológicos, aos segredos industriais ou à reputação da **ALPINO** perante seus clientes e parceiros de mercado.

8.2 Medidas Disciplinares Aplicáveis

- A **ALPINO** reserva-se o direito de aplicar sanções disciplinares proporcionais à gravidade da infração cometida, agindo estritamente fundamentada na Consolidação das Leis do Trabalho (CLT) e em seu Regulamento Interno de Conduta. As medidas punitivas seguem uma escala pedagógica e punitiva que inclui: advertência verbal (para casos leves e iniciais), advertência escrita formal, suspensão temporária das atividades e das gratificações, até a rescisão do contrato de trabalho por justa causa em casos de violações graves ou reincidentes. No caso de prestadores de serviço, consultores e terceiros, qualquer descumprimento das normas de segurança acarretará a rescisão imediata do vínculo comercial, sem prejuízo da aplicação de multas contratuais e vedações de futuras parcerias com a organização.

8.3 Responsabilização Civil e Criminal

- Independentemente das sanções administrativas aplicadas internamente, o infrator poderá ser responsabilizado nas esferas civil e criminal caso sua conduta resulte em prejuízos financeiros diretos, violação de segredos industriais protegidos por lei ou infrações graves à Lei Geral de Proteção de Dados (LGPD). A **ALPINO** cooperará plenamente com as autoridades policiais e judiciais em investigações de crimes cibernéticos, fraudes ou vazamentos de dados que comprometam direitos de terceiros ou o patrimônio intelectual da empresa. A organização manterá a custódia de todas as evidências digitais e logs de auditoria necessários para servir como prova em processos judiciais, garantindo que a impunidade não comprometa a integridade do seu Sistema de Gestão de Segurança da Informação (SGSI).

9. Disposições Finais

9.1 Vigência e Revisão Periódica

- Esta Política de Segurança da Informação (PSI) entra em vigor imediatamente na data de sua publicação oficial, revogando e substituindo integralmente todas as disposições, normas ou comunicados anteriores que tratem de diretrizes de segurança. O documento deverá passar por um processo de revisão crítica anualmente ou sempre que houver mudanças substanciais na infraestrutura tecnológica, alterações no modelo de negócio da **ALPINO** ou atualizações em requisitos legais e normativos internacionais. Tais atualizações incluem a conformidade com a ISO/IEC 27001, o referencial VDA ISA (TISAX) para o setor automotivo e a Lei Geral de Proteção de Dados (LGPD), garantindo que a governança da informação permaneça alinhada às melhores práticas globais de proteção cibernética.

9.2 Divulgação e Ciência Obrigatória

- A ciência e o aceite integral desta PSI e normativos complementares constituem requisitos obrigatórios para todos os colaboradores, estagiários, consultores e parceiros estratégicos da **ALPINO**. A adesão formal será realizada mediante a assinatura do Termo de Ciência e Responsabilidade, podendo ocorrer de forma física ou eletrônica através do sistema **Apps Alpino**, integrando o dossiê de conformidade do indivíduo. A organização promoverá campanhas periódicas de aculturamento e treinamentos de reciclagem para assegurar o entendimento das regras, reforçando que o desconhecimento das diretrizes estabelecidas não

poderá ser utilizado, sob nenhuma hipótese, como justificativa para o seu descumprimento ou para a mitigação de sanções disciplinares.

9.3 Casos Omissos e Exceções

- Situações não previstas explicitamente nesta Política ou dúvidas relacionadas à interpretação técnica e normativa de seus termos deverão ser submetidas à análise do Gestor de TI e, dependendo da criticidade, ao Comitê de Segurança da Informação. Nenhuma exceção às regras de segurança será permitida sem que haja uma análise de risco prévia documentada, que identifique controles compensatórios e tenha a aprovação formal e por escrito das autoridades designadas no Bloco 5. Todas as exceções aprovadas deverão possuir um caráter temporário e ser registradas em um inventário específico de riscos aceitos, sendo reavaliadas semestralmente para garantir que não se tornem vulnerabilidades permanentes no ambiente tecnológico da **ALPINO**.

REVISÃO	ALTERAÇÃO	
00	Edição inicial	
Há necessidade de treinamento?	Quais áreas/ setores/ cargos devem participar?	
Sim	Todos os colaboradores Alpino	
Elaborado por:	Verificado por:	Aprovado por:
Maikon Santos e Nycolas Leme	Maikon Santos	Fabio Alonso