Alupar

Política

Segurança da Informação e Segurança Cibernética

Código: HO-TIN-PL-002 | Criado em: 28/07/2017 | Última revisão: 07/2025

1. Objetivo

Este documento tem por finalidade estabelecer as diretrizes e responsabilidades sobre a proteção das informações da Alupar Investimento S.A. (“Empresa”, “Companhia”). Estas diretrizes servem como base para as normas, padrões e procedimentos que regulamentam os objetivos aqui definidos como importantes para uma boa prática da gestão da Segurança da Informação.

A Política de Segurança da Informação e Segurança Cibernética da Alupar Investimento S.A. direciona requisitos para manutenção da Integridade, disponibilidade, confidencialidade, autenticidade e privacidade das informações da Companhia e/ou sob sua custódia.

As diretrizes estabelecidas neste documento, observam e cumprem a legislação aplicável à Proteção de Dados Pessoais, em especial a Lei nº 13.709/2018 e suas alterações posteriores (“Lei Geral de Proteção de Dados Pessoais” ou “LGPD”), bem como as políticas internas de Proteção de Dados Pessoais da Companhia.

Este documento possui prazo de validade até 07/26

2. Abrangência e Aplicabilidade

Aplica-se a toda informação do ambiente de tecnologia e do ambiente convencional da Alupar Investimento S.A. e/ou empresas nas quais ela detenha participação direta ou indireta (“Empresas”), e tem como público-alvo toda estrutura de gestão e colaboradores, incluindo funcionários, estagiários, fornecedores, prestadores de serviços e parceiros de negócio, que tenham acesso em algum momento ao ambiente e às informações de propriedade das Empresas, tratadas nas redes Corporativa e Operativa.

3. Dicionário

Ameaça - Causa potencial de um incidente indesejado, que pode resultar em dano para a Companhia.

Ativo - Qualquer coisa (ativos computacionais, computadores, celulares, tablets, sistemas, aplicações, informações etc.) que tenha valor para a Companhia e precisa ser adequadamente protegido.

Ativo Intangível - Todo elemento que possui valor para a Companhia e que esteja em suporte digital ou se constitua de forma abstrata, mas registrável ou perceptível, a exemplo, mas não se limitando à dados, reputação, imagem, marca e conhecimento.

Autenticidade - Garantia de que a informação é procedente e fidedigna, sendo capaz de gerar evidências não repudiáveis da identificação de quem a criou, editou ou emitiu.

Colaborador - Membros da alta administração, funcionários, estagiários (na forma da Lei de Estágio – Lei 11.788/2008) e jovens aprendizes (na forma da Lei de Aprendizagem, Lei 10.097/2000), prestadores de serviços terceirizados e contratados da Companhia.

Confidencialidade - Princípio que está atrelado à privacidade das informações. Ou seja, garantia de que os dados da Companhia não estarão disponíveis nem serão divulgados a indivíduos, entidades ou processos sem autorização.

Disponibilidade - Propriedade de manter a informação disponível para usuários autorizados, quando estes dela necessitarem.

Incidente de Segurança - Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação levando a perda de um ou mais princípios básicos de Segurança da Informação: confidencialidade, integridade, disponibilidade e autenticidade, tais como: invasões de computador, ataques de negação de serviços, furto de informação por pessoal interno e/ ou terceiros, vazamento de dados, uso indevido de acessos privilegiados e atividades em rede não autorizadas ou ilegais.

Informação - Ativo estratégico e de alto valor para a Companhia, de sua propriedade ou sob sua responsabilidade e deve ser protegida, em conformidade com a legislação vigente, com os valores éticos e com as melhores práticas da segurança da informação.

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

Não repúdio - Garantia de que o emissor de algum dado ou informação ou o autor de alguma ação sobre a informação não possa posteriormente negar que tenha enviado o dado/informação ou que tenha alterado alguma informação.

Resposta à incidentes – Processo previamente definido que descreve como a Companhia deverá lidar com um incidente de Segurança da Informação ou Cibernético.

Risco – Possibilidade de um evento acontecer, seja ele uma Ameaça, quando negativo, ou oportunidade, quando positivo

---

Segurança Cibernética (Cyber Security) - Conjunto de meios e tecnologias empregadas na defesa dos sistemas de informação, infraestrutura, redes de computadores e/ou dispositivos pessoais, com o objetivo de prevenir danos, roubo, intrusão, alterações ou destruição da informação, ocasionados por ataques cibernéticos e que está integralmente inserido na presente Política.

Segurança da Informação - Preservação das propriedades da informação, notadamente sua confidencialidade, integridade, disponibilidade e autenticidade, permitindo o uso e o compartilhamento da informação de forma controlada, independentemente do meio de armazenamento, processamento ou transmissão que seja utilizado.

Terceiros – Qualquer pessoa física ou pessoa jurídica usada para obter e/ou reter negócios, tais como assessores, consultores, subcontratados, representantes de vendas e sócios de uma parceria; ou usada para representar as Empresas ou seus interesses perante um governo, uma entidade estatal, empresa estatal ou controlada pelo Estado; prestadores de serviço e fornecedores.

Usuário - Todo Colaborador ou Terceiro que utiliza recursos informatizados da Empresa.

Violação - Qualquer atividade que desrespeite as regras estabelecidas nos documentos normativos da Companhia.

4. Diretrizes Gerais

As diretrizes estabelecidas nesta Política têm por objetivo:

Proteger o valor e a reputação da Companhia;

Garantir a confidencialidade, integridade e disponibilidade das informações da Companhia e de informações de Terceiros por ela custodiada, contra acessos indevidos e modificações não autorizadas, assegurando ainda que as informações estarão disponíveis a todas as partes autorizadas, quando necessário;

Identificar violações de Segurança da Informação, estabelecendo ações sistemáticas de detecção, tratamento e prevenção de incidentes;

Garantir a continuidade dos negócios da Companhia, protegendo os processos críticos de interrupções inaceitáveis causadas por falhas ou desastres significativos;

Atender aos requisitos legais, regulamentares e às obrigações contratuais pertinentes à atividade da empresa;

Conscientizar, educar e treinar os Usuários na política, normas e procedimentos de Segurança da Informação para que sejam aplicadas às suas atividades diárias;

Estabelecer e melhorar continuamente o Processo de Gestão de Riscos de Segurança da Informação e Segurança Cibernética;

Garantir que os dados pessoais não sejam perdidos, roubados, utilizados indevidamente ou vazados por usuários não autorizados;

Estabelecer controles para prevenção de perda de dados, visando mitigar os riscos usuais, com o estabelecimento de mecanismos de governança e, a avaliação e melhoria contínua de todos os aspectos específicos de privacidade e proteção de dados pessoais.

5. Responsabilidades

5.1 Diretoria

- Demonstrar comprometimento na promoção de diretrizes estratégicas, desde que previamente alinhadas com o Conselho de Administração da Companhia, bem como em relação às responsabilidades, competências e apoio ao Sistema de Gestão de Segurança da Informação (SGSI), a fim de garantir a proteção dos seus Ativos tangíveis e intangíveis.

- Submeter à análise da Comissão de Segurança da Informação, toda e qualquer matéria que envolva temas estratégicos ou de assunção de riscos, no que diz respeito à Segurança da Informação.

5.2 Gerência de Segurança da Informação

- Garantir que todos os assuntos relacionados à Segurança da Informação são tratados de maneira consistente e efetiva, estabelecendo uma cultura e consciência de segurança da informação a todos os Colaboradores da companhia;
- Elaborar, custodiar, manter e divulgar esta política, assim como as demais normas pertinentes à Segurança da Informação e Segurança Cibernética, que complementam esta política;
- Analisar todas as políticas relacionadas à Segurança da Informação e Segurança Cibernética pelo menos uma vez por ano, atualizando conforme necessário para refletir as alterações nos objetivos de negócios ou no ambiente da Companhia;
- Buscar apoio e orientação, quanto aos aspectos jurídicos, relacionados aos processos de contratação e às exigências legislativas e regulatórias relacionadas à Segurança da Informação.

5.3 Comissão de Segurança da Informação

- Garantir que todos os assuntos relacionados à Segurança da Informação e Segurança Cibernética são tratados de maneira consistente e efetiva, estabelecendo uma cultura e consciência de Segurança da Informação e Segurança Cibernética a todos os Colaboradores da companhia;
- Avaliar e aprovar todas as políticas de segurança pelo menos uma vez por ano, atualizando conforme necessário para refletir as alterações nos objetivos de negócios ou no ambiente da Companhia;
- Avaliar, acompanhar e deliberar quanto aos temas relacionados à Segurança da Informação e Segurança Cibernética considerando a estratégia de riscos da companhia;
- Submeter para análise do Comitê de Governança, Comitê de Auditoria e posterior deliberação do Conselho de Administração toda e qualquer matéria que envolva temas estratégicos ou de assunção de riscos, no que diz respeito à Segurança da Informação e Segurança Cibernética.
- Garantir a responsabilização dos Colaboradores e/ou Terceiros que não observarem as políticas e procedimentos internos das Empresas, relativos à Segurança da Informação e Segurança Cibernética.

5.4 Gerência de Tecnologia da Informação

- Definir e implementar os procedimentos para configuração segura do ambiente tecnológico da Companhia;
- Manter registros de todas as violações de segurança ocorridas nos ambientes e sistemas da Companhia, contendo detalhes suficientes para que possam ser usados em ações disciplinares e/ou de revisão das políticas e procedimentos;
- Monitorar e analisar os alertas e as informações de segurança, distribuindo-os para as equipes apropriadas para o tratamento, conforme requisitos e procedimentos definidos na Norma de Tratamento e Resposta a Incidentes;

- Administrar as contas dos Usuários, incluindo adições, exclusões e modificações, avaliando continuamente o gerenciamento da autenticação aos componentes do sistema;
- Garantir que os Colaboradores tenham acesso somente às informações e recursos previamente autorizados;
- Executar avaliação periódica sobre as contas dos Usuários e controles de acesso que assegurem sua validade e exatidão;
- Implementar, administrar e monitorar controles de tecnologia e de segurança que apoiam, comprovam e evidenciem a aplicação desta Política;

5.5. Gestão de Pessoas

- Conduzir o programa de conscientização e realizar os treinamentos periódicos com o apoio da área de Segurança da Informação;
- Garantir a disponibilidade dos documentos de Segurança da Informação a todos os Colaboradores da Companhia;
- Garantir, no processo de admissão, a orientação dos Colaboradores quanto ao tema de Segurança da Informação e Segurança Cibernética.

5.6 Gestores

- Gerenciar e assegurar o cumprimento desta Política e demais documentos complementares pelos seus Colaboradores;
- Assegurar que os contratos e serviços sob sua responsabilidade estejam aderentes à esta Política e demais documentos complementares;

- Avaliar criteriosamente antes de aprovar solicitações de acesso às informações e recursos da Companhia, sistemas ou aplicações específicas para seus Colaboradores, de forma que não comprometa a segurança das informações da empresa com liberação de permissões que vão além das necessidades das atividades de trabalho exercidas (Princípio do Privilégio Mínimo – acessos e autorizações mínimas necessárias para execução das atribuições);
- Informar à área de Gestão de Pessoas e a Gerência de Segurança da Informação sobre eventuais trocas dos direitos de acessos, transferências e mudanças de funções dos Colaboradores sob sua responsabilidade;
- Garantir o conhecimento desta Política e suas normas complementares por parte de seus Terceiros.

5.7 Colaboradores

- Proteger as informações da Empresa, de acordo com suas classificações e sensibilidade, sendo que na ausência do rótulo ou classificação, não é permitido revelar qualquer informação de propriedade ou sob a responsabilidade da Companhia sem a prévia e formal autorização da área de “Segurança da Informação”;
- Conhecer e seguir todas as políticas e procedimentos operacionais de segurança da Companhia que são pertinentes às suas funções e atividades;
- Conhecer suas responsabilidades a respeito da Segurança da Informação e Segurança Cibernética, atuando de forma segura, ética e legal na utilização dos recursos e dados da Companhia, primando pela preservação da confidencialidade, integridade e disponibilidade das informações da empresa;
- Responder pelos danos causados em decorrência da não observância das regras de proteção da informação e dos recursos computacionais da rede corporativa, nos termos previstos nesta Política;
- Participar do programa de conscientização e treinamentos em Segurança da Informação e Segurança Cibernética corporativa;

- Zelar por toda e qualquer informação armazenada na rede corporativa contra alteração, destruição, divulgação, cópia e acesso não autorizados;
- Zelar pela devida utilização dos recursos de hardware e pela sua conservação para uso nas atividades profissionais suas e de seus colegas;
- Guardar sigilo das informações confidenciais, mantendo-as em caráter restrito;
- Manter em caráter confidencial e intransferível a senha de acesso aos recursos computacionais da organização;
- Reportar formalmente ao seu Gestor quaisquer eventos relativos à violação ou possibilidade de violação desta política ou atividades suspeitas,
- Atender às recomendações pertinentes, constantes nas normas e procedimentos de segurança da informação da Empresa.

6. Adesão

A adesão à presente Política implica estrita observância às regras contidas nela e na legislação vigente, sob pena de aplicação de sanções disciplinares. A adesão dos Colaboradores a esta Política será formalmente confirmada por meio da assinatura de **"Termo de Adesão à Política de Segurança da Informação e Segurança Cibernética";**

Os Colaboradores serão comunicados sempre que alterações realizadas nessa Política forem consideradas como relevantes e/ou importarem obrigações adicionais. Desta forma, os Colaboradores deverão reiterar a sua adesão à Política e às Normas de Segurança da Informação e Segurança Cibernética.

7. Sansões Disciplinares

Qualquer atividade que desrespeite as diretrizes estabelecidas nesta Política será considerada como uma violação e tratada pela área de Segurança da Informação, a fim de apurar as responsabilidades dos envolvidos, visando aplicação de medidas disciplinares e/ou sanções cabíveis previstas em cláusulas contratuais e na legislação vigente pelas áreas responsáveis.

A tentativa de burlar as diretrizes e controles estabelecidos, quando constatada, será tratada como uma violação.

8. Referências

- Termo de Responsabilidade
- Código de Ética, Conduta & Compliance
- Política de Privacidade
- Normas Complementares de Segurança da Informação
- Norma ABNT NBR ISO/IEC 27001:2013
- Norma ABNT NBR ISO/IEC 27002:2013

9. Fundamentos Regulatórios

- Lei n°9.609/98 (Lei de Software)
- Lei n°9.610/98 (Lei de Direitos Autorais)
- A Lei nº 13.709/2018, a LGPD;
- A Lei nº 12.965/2014, o Marco Civil da Internet;
- A Lei nº 12.527/2011, a Lei de Acesso à Informação;
- Os regulamentos e normas publicados pela ANPD (Autoridade Nacional de Proteção de Dados).
- Constituição da República Federativa do Brasil, de 05 de outubro de 1988;
- Lei Federal 8159, de 08 de janeiro de 1991 (Dispõe sobre a Política Nacional de Arquivos Públicos e Privados);
- Lei Federal 9279, de 14 de maio de 1996 (Dispõe sobre Marcas e Patentes);
- Lei Federal 3129, de 14 de outubro de 1982 (Regula a Concessão de Patentes aos autores de invenção ou descoberta industrial);
- Lei Federal 10406, de 10 de janeiro de 2002 (Institui o Código Civil);
- Decreto-Lei 2848, de 7 de dezembro de 1940 (Institui o Código Penal);
- Lei Federal 9983, de 14 de julho de 2000 (Altera o Decreto-Lei 2.848, de 7 de dezembro de 1940 - Código Penal e dá outras providências);
- Decreto nº 9637, de 26 de dezembro de 2018 - Política Nacional de Segurança da Informação.

10. Histórico de Revisão

Nº da Revisão	Data da Publicação	Descrição da revisão	Aprovador (Nome/Função)
01	07/2017	Criação do documento	-
02	02/2023	Revisão com base no Projeto de SI e atualização com a ISO 27001	Conselho de Administração Alupar
03	07/2025	Revisão periódica	Conselho de Administração Alupar

Esta Política poderá ser alterada a qualquer momento, sem prévio aviso.