1. OBJETIVO

O objetivo da Política de Segurança da Informação e Cibernética ("Política") é estabelecer diretrizes, responsabilidades e princípios gerais de segurança da informação e cibernética com objetivo de manter a confidencialidade, integridade, disponibilidade, autenticidade, irretratabilidade dos ativos de informação sob gestão da Cosan S.A. ("Cosan" ou "Companhia"), observando as melhores práticas de mercado em conformidade com as regulamentações aplicáveis.

2. APLICAÇÃO E ABRANGÊNCIA

Aplica-se e abrange a todos os Colaboradores da Cosan no Brasil e no exterior, a partir da data de sua aprovação e consequente publicação.

Essa Política poderá ser aplicada a Terceiros que possuam acesso a Ativos da Companhia ou sejam Usuários na Cosan. Para melhor esclarecimento, será aplicado para esses Terceiros, o mesmo que será aplicado aos Colaboradores para fins desta Política.

3. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

A Cosan tem o compromisso de seguir os princípios básicos de segurança da informação:

Confidencialidade: Assegurar que a informação e ativos de informação sejam acessíveis somente pelos usuários autorizados, pelo período necessário;

Disponibilidade: Assegurar que a informação e ativos de informação estejam disponíveis para os usuários autorizados sempre que necessários;

Integridade: Assegurar que a informação e ativos de informação estejam completos e íntegros e que não tenham sido modificados ou destruídos de maneira não autorizada ou acidental durante seu ciclo de vida;

Autenticidade: Assegurar a veracidade da origem da informação; e

Irretratabilidade (não repúdio): Assegurar que uma ação não possa ser negada por seu autor.

3.1. DIRETRIZES GERAIS

As informações devem ser tratadas com responsabilidade, conforme os fins para os quais foram coletadas e de acordo com as leis e regulamentações vigentes, inclusive no uso de soluções externas como aplicativos de mensagens, redes sociais e ferramentas de inteligência artificial.

Deve-se promover a irretratabilidade das informações, mitigando o risco de que pessoas ou entidades neguem a autoria das ações realizadas por usuários ou processos.

Colaboradores da Cosan, conforme aplicável, devem ter ciência de que o uso dos ativos de informação, dos sistemas, ambientes e respectivas políticas de senhas podem ser monitorados pela Companhia e os respectivos registros podem detectar violações desta Política e procedimentos complementares, neste caso tais subsídios poderão servir como evidência para aplicação de medidas disciplinares, processos administrativos e/ou legais.

As tecnologias, marcas, metodologias e demais informações são propriedade intelectual da Cosan, sendo vedado o seu compartilhamento ou utilização para fins pessoais ou por terceiros, salvo mediante autorização formal. Portanto, não devem ser repassadas ou compartilhadas com terceiros, assim como utilizadas para fins pessoais, ainda que tenham sido obtidas ou desenvolvidas pelo próprio Colaborador, exceto mediante expressa autorização do *Information Owner.*

A Cosan compromete-se a aplicar medidas de segurança e proteção da informação, proporcionais ao impacto dos ativos críticos para o negócio, buscando sua atualização e aprimoramento contínuo frente às mudanças tecnológicas e regulatórias.

4. CONTROLES E PROCESSOS DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

A Cosan adota boas práticas de segurança da informação e cibernética para fortalecer a proteção dos ativos críticos de informação e apoiar na implementação e efetividade das diretrizes desta Política, bem como dos controles, processos e procedimentos estabelecidos a seguir.

4.1. UTILIZAÇÃO SEGURA DE RECURSOS DE TECNOLOGIA DA INFORMAÇÃO (“TI”)

Os Colaboradores devem utilizar os recursos de tecnologia da informação corporativos somente para fins profissionais, sendo resguardado à Cosan, o direito de controlar e monitorar sua utilização conforme legislação aplicável e interesses da Companhia.

4.2. CLASSIFICAÇÃO DAS INFORMAÇÕES

Os Colaboradores devem proteger adequadamente as informações, classificando-as de acordo com o seu valor, requisitos legais, relevância, sensibilidade e criticidade para a Cosan, nos termos da Norma de Classificação da Informação. Os Colaboradores devem considerar as necessidades de negócio, demandas regulatórias, compartilhamento ou restrição de acesso, os impactos no caso de utilização indevida das

informações, para que que toda informação criada seja classificada e protegida ao longo do seu ciclo de vida.

4.3. PROTEÇÃO DE DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS

A Cosan adota medidas de segurança estabelecidas nesta Política com o objetivo de proteger os dados pessoais e dados pessoais sensíveis. É responsabilidade dos Colaboradores assegurar essa proteção em todas as suas atividades. Essa conduta é fundamental para o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD).

4.4. GESTÃO DE IDENTIDADE, AUTENTICAÇÃO E ACESSOS

A Cosan adota práticas de gestão de identidade, autenticação e controle de acessos para mitigar os riscos de acessos não autorizados aos ativos críticos para o negócio. Os Colaboradores devem utilizar mecanismos de autenticação que permitam sua identificação, como a autenticação multifator (MFA).

4.5. GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO

A Cosan estabelece processo para identificar, analisar, avaliar e monitorar os riscos da Companhia inclusive aqueles relacionados aos ativos. Com base nessas análises, a área de Segurança da Informação da Cosan deve identificar os controles adequados, e testar periodicamente sua eficácia.

A gestão de riscos em Segurança da Informação obedece ao Modelo de Três linhas de Atuação, previsto no parecer do IIA de setembro de 2024, representado abaixo:

- 1ª Linha é composta pelas áreas de negócios da Companhia, incluindo suas controladas e co-controladas, responsáveis pelos riscos que gerenciam, assim como pela execução e eficácia de suas respectivas Ações Mitigatórias e de seus controles internos associados.
- 2ª Linha composta pelas estruturas que devem instrumentalizar os gestores da primeira linha para o correto gerenciamento dos riscos através da organização e estruturação dos processos, definição de metodologias, desenvolvimento de treinamentos e orientação, além de reportar as informações aos órgãos internos de governança como comitês executivos, comissões, fóruns e/ou grupos de trabalho.
- 3ª Linha é composta pela Auditoria Interna da Companhia, atuando com um olhar independente para verificar a eficácia e conformidade do modelo e reportar suas recomendações aos órgãos de governança competentes.

4.6. GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

A Cosan mantém um plano de recuperação para assegurar a continuidade das operações em casos de incidentes ou crises que impactem seus ativos críticos, bem como adota procedimentos, requisitos e mantém controles específicos para detectar, tratar e responder a incidentes de segurança da informação. Simulações periódicas contribuem para que os envolvidos estejam preparados para agir de maneira rápida e eficiente diante de situações críticas. Os incidentes relevantes devem ser controlados e reportados ao Comitê de Auditoria Estatutário.

A resposta a incidentes segue o fluxo definido na Norma de Resposta a Incidentes IT & OT, com atuação coordenada entre Segurança da Informação, DPO e demais áreas envolvidas, conforme a natureza e criticidade do incidente.

4.7. TREINAMENTO E CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO

A Cosan adota ações e iniciativas periódicas para promover, capacitar, aculturar e avaliar os Colaboradores sobre segurança da informação, reforçando as diretrizes declaradas nesta Política.

4.8. AVALIAÇÃO DE SEGURANÇA DA INFORMAÇÃO NA CONTRATAÇÃO DE SERVIÇOS

Fornecedores, a depender de critérios de elegibilidade, devem passar por avaliação de risco, que pode incluir auditoria ou avaliação remota de evidências para verificar a observância dos controles de Segurança da Informação e Privacidade, com o devido acompanhamento de correções e/ou melhorias a serem implementadas pelos fornecedores.

Os contratos com Fornecedores devem conter cláusulas contratuais mínimas de segurança da informação, especialmente sobre a necessidade de cumprimento dos normativos de segurança da informação da Cosan pelos Fornecedores e por seus subcontratados. Cabe ao gestor do contrato a responsabilidade de monitorar a aderência do terceiro a estas diretrizes, com o devido suporte consultivo do time Jurídico.

4.9. MONITORAMENTO E DETECÇÃO DE AMEAÇAS

A área de Segurança da Informação deve prevenir e detectar acessos não autorizados e tentativas de intrusão aos ativos críticos da Cosan.

4.10. GESTÃO DE VULNERABILIDADES

A área de Segurança da Informação deve realizar testes de detecção de vulnerabilidades em sistemas e ambientes críticos da Cosan por meio de análises periódicas.

4.11. PROTEÇÃO CONTRA *SOFTWARES* MALICIOSOS

A área de Segurança da Informação deve proteger os ativos de informação da Cosan contra *softwares* maliciosos.

4.12. RASTREABILIDADE E DETECÇÃO

A área de Segurança da Informação deve adotar medidas de rastreamento e monitoramento das atividades em ambientes tecnológicos relevantes.

4.13. BACKUP

A Cosan deve manter cópias de segurança (*backup*) das informações críticas, atualizadas e testadas regularmente.

4.14. SEGURANÇA NO CICLO DE VIDA E NA AQUISIÇÃO DE SISTEMAS E *SOFTWARES*

A Cosan deve integrar práticas de desenvolvimento seguro desde a concepção até a manutenção de sistemas.

A Cosan também deve assegurar que a aquisição de *softwares* respeite os direitos autorais e os termos de licença, permitindo apenas *softwares* legalmente autorizados em suas estações de trabalho e servidores.

4.15. CONFORMIDADE E AVALIAÇÃO DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

A Cosan deve avaliar periodicamente a conformidade com esta Política por auditorias internas e/ou externas, seguindo metodologias e critérios definidos com o objetivo de avaliar a eficácia dos controles de segurança implementados, identificar desvios, vulnerabilidades e oportunidades de melhoria.

5. PAPÉIS E RESPONSABILIDADES

A segurança da informação é responsabilidade de todos os Colaboradores da Cosan, com papéis específicos definidos.

5.1. DIRETORIA

Aprovar esta Política, assim como qualquer alteração e atualização.

5.2. ÁREA DE SEGURANÇA DA INFORMAÇÃO

Revisar esta Política de Segurança da Informação e submetê-la a aprovação, conforme procedimento de gestão de documentos internos e externos.

Implementar, manter, monitorar, promover a melhoria contínua dos controles, processos e procedimentos de segurança da informação e cibernética da Cosan, e disseminar e incentivar as boas práticas sobre o tema aos Colaboradores.

Avaliar os riscos reportados pelas áreas de negócio e garantir seu devido tratamento, conforme a criticidade identificada.

5.3. *INFORMATION OWNER*

Garantir que os dados estejam classificados, protegidos e utilizados, nos termos da Norma de Classificação da Informação.

Definir o controle de acesso seguindo o princípio do menor privilégio.

Apoiar a coordenação das ações de segurança da informação e cibernética relacionadas aos dados sob sua responsabilidade em conjunto com o S*ystem* O*wner*.

54. *SYSTEM OWNER*

Atuar junto as áreas técnicas e área de segurança da informação para garantir que os sistemas estejam em conformidade com os requisitos de proteção da informação definidos pela Cosan;

Estabelecer a implementação e manutenção dos controles, processos e procedimentos de segurança da informação e cibernética nos sistemas sob sua responsabilidade.

5.5. GESTOR DA ÁREA DE NEGÓCIO

Gerenciar o cumprimento desta Política e demais documentos complementares pelos seus liderados;

Reportar os riscos de segurança da informação, bem como dúvidas sobre a Política e procedimentos relacionadas à área de Segurança da Informação da Cosan.

Analisar resultados de auditorias e definir prazos de execução das ações preventivas e corretivas devidas.

5.6. COLABORADORES

Proteger as informações da Cosan sob sua responsabilidade, assegurando a aplicação dos princípios básicos de segurança da informação definidos nesta Política.

Cumprir e orientar os Fornecedores contratados a seguirem as diretrizes estabelecidas nesta Política e nos procedimentos internos complementares.

Zelar pelo tratamento adequado dos dados sob titularidade da Cosan e/ou de terceiros que lhes forem confiados, respondendo legalmente por quaisquer ações realizadas durante todo o seu ciclo de vida.

6. PENALIDADES

As violações a esta Política estarão sujeitas às sanções disciplinares previstas na Política de Medidas Disciplinares e no Código de Conduta, sem prejuízo da Cosan adotar medidas administrativas, civis e penais cabíveis conforme o caso.

Terceiros estarão sujeitos às sanções contratuais, incluindo a imediata rescisão contratual e penalidades, sem prejuízo do ingresso pela Cosan com as ações judiciais e outras providências legais cabíveis.

7. TERMOS E DEFINIÇÕES

Ativo: elementos tangíveis, como equipamentos e infraestrutura, quanto intangíveis, como dados, informações e conhecimento;

ACN (Ativos críticos do negócio): são os ativos que garantem o funcionamento do negócio e são

fundados nos pilares básicos da segurança, quais sejam, a disponibilidade, integridade e confidencialidade. O não cumprimento de tais pilares, mesmo que momentaneamente, podem causar

impactos à reputação e/ou ao faturamento da companhia e por este motivo devem possuir um suporte

prioritário;

Colaborador(es): empregados, estagiários, menores aprendizes e administradores da Cosan;

Dados Pessoais: quaisquer informações que possam identificar ou tornar identificável uma pessoa natural;

Dados Pessoais Sensíveis: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Fornecedores: empresas fornecedoras, parceiras e prestadoras de serviços a terceiros que celebraram uma proposta comercial ou contrato de fornecimento, parceria e/ou prestação de serviços com a Cosan, bem como seus representantes. Ressalvadas situações pontuais, será aplicada aos Fornecedores, as mesmas responsabilidades atribuídas aos Colaboradores por essa Política;

Information Owner: função responsável por um conjunto específico de dados dentro da organização.

MFA (Multi-Factor Authentication): é um processo no qual os usuários são solicitados, durante o processo de entrada, a fornecer uma forma adicional de identificação, como um código no celular ou uma verificação de impressão digital.

Princípio do Menor privilégio: é um princípio na governança de identidade que envolve a atribuição de usuários e grupos apenas no nível mínimo de acesso e as permissões necessárias para executar suas funções.

System Owner: função responsável pelo sistema de informação que armazena, processa ou transmite os dados.

Terceiros: contratados, subcontratados, terceiros desde possuam acesso aos Ativos da Companhia e/ou sejam Usuários.

Usuário: qualquer indivíduo, processo, dispositivo ou mecanismo que acesse, use ou manipule uma informação ou ativo de informação.

9. HISTÓRICO DE REVISÃO E APROVAÇÃO

ETAPA	ÁREA	NOME	CARGO	DATA	
Elaboração/Alteração	Segurança da Informação	Eliana Fagundes	Analista de SI SR	29/05/2025	Versão 04
Revisão	Controles Internos	Christian Rodrigues	Analista de CI SR	12/06/2025	
Revisão	RI & ESG	Paula Macedo	Coordenadora de RI & ESG	17/06/2025	
Revisão	Jurídico	Laís Sumida	Coordenadora Compliance	25/06/2025	
Revisão	Jurídico Societário	Jefferson Molero	Coordenador Societário	30/06/2025	
Revisão	Controles Internos	Priscilla Ferreira	Gerente Controles Internos	02/07/2025	
Revisão	Gestão de Riscos	Jorge Manoel	Gerente Gestão de Riscos	03/07/2025	
Revisão	Segurança da Informação	Thaís Diniz	Especialista em Privacidade	16/07/2025	
Revisão/Aprovação	Segurança da Informação	Eunice Silva	Gerente de Proteção de Dados	16/07/2025	
Aprovação Executiva	Diretoria Executiva			17/07/2025	

10. REFERÊNCIAS

Procedimento de Elaboração e aprovação de documentos internos e externos;

Procedimento do Programa de *Vendor Risk Management*;

Procedimento de Classificação da Informação;

Política de Medidas Disciplinares;

Código de Conduta;

Procedimento de Gestão de Riscos em Segurança da Informação;

Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709/2018.