infotec
BRASIL

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Sumário

1. RESPONSÁVEIS

Autor	Aprovador
Gerente de Infraestrutura de TI	Diretoria de Transformação Digital
	Diretoria de Governança e Sustentabilidade

2. VALIDADE

Esta política é válida por prazo indeterminado e deverá ser revisada sempre que houver alterações relevantes na legislação, nas normas aplicáveis, nos processos internos, nos riscos de segurança da informação ou nas estratégias da organização.

3. OBJETIVO

Estabelecer os princípios, responsabilidades e diretrizes gerais para a proteção das informações e dos ativos da INFOTEC BRASIL, preservando sua confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade e privacidade, em alinhamento com os objetivos do negócio e com os requisitos legais, regulatórios e contratuais aplicáveis.

Esta Política complementa as disposições do Código de Ética e das demais Políticas Corporativas da INFOTEC BRASIL, estabelecendo as diretrizes gerais para a Segurança da Informação. Os requisitos técnicos, operacionais e procedimentais necessários à sua implementação serão estabelecidos em normas, procedimentos, planos, padrões e instruções complementares.

4. ABRANGÊNCIA E APLICAÇÕES

A presente Política aplica-se a todos os representantes legais, administradores e colaboradores da INFOTEC BRASIL, em qualquer nível hierárquico, em todas as suas filiais e controladas, bem como, a terceiros, fornecedores, subcontratados, consultores, prestadores de serviços de qualquer natureza e demais pessoas físicas ou jurídicas que atuem em nome da INFOTEC BRASIL ou mantenham

relacionamento com a empresa, que tenham acesso a informações, ativos, sistemas, instalações ou ambientes sob responsabilidade da INFOTEC BRASIL.

A Política abrange informações em qualquer formato ou meio, recursos tecnológicos, instalações, processos internos, atividades realizadas remotamente, ambientes de clientes e serviços contratados ou administrados pela INFOTEC BRASIL.

Quando requisitos legais, regulatórios, contratuais ou de clientes forem mais restritivos do que esta Política, prevalecerão os requisitos mais protetivos, desde que não contrariem a legislação aplicável.

5. CONCEITOS E DEFINIÇÕES

Para fins desta Política, alguns termos devem ser entendidos da seguinte forma:

a) **Informação:** conjunto de dados, registros, documentos ou conhecimentos, independentemente do formato ou meio, que possuem valor para a organização.
b) **Segurança da Informação**: preservação da confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade das informações.
c) **Ativo:** recurso que possui valor para a INFOTEC BRASIL ou para terceiros, incluindo informações, sistemas, dispositivos, serviços, pessoas, instalações, processos e reputação.
d) **Confidencialidade**: propriedade de que a informação não seja disponibilizada ou divulgada a pessoas, entidades ou processos não autorizados.
e) **Integridade:** propriedade de exatidão, completude e proteção contra alteração indevida.
f) **Disponibilidade:** propriedade de estar acessível e utilizável quando requerida por pessoas ou processos autorizados.
g) **Proprietário da informação:** gestor da área ou do processo de negócio responsável por definir a classificação, a necessidade de acesso e os requisitos de proteção da informação.
h) **Custodiante:** área ou pessoa responsável pela administração técnica, armazenamento, proteção ou operação do ativo.
i) **Evento de segurança:** ocorrência observada que possa indicar falha, ameaça ou situação anormal.
j) **Incidente de segurança:** evento confirmado, ou conjunto de eventos, que comprometa ou

ameace a segurança das informações.

k) **Dado pessoal:** informação relacionada a pessoa natural identificada ou identificável.

l) **Risco de segurança da informação:** efeito da incerteza sobre os objetivos de segurança, resultante da combinação entre probabilidade e impacto.

6. PRINCÍPIOS, REGRAS E DIRETRIZES GERAIS

A INFOTEC BRASIL adota os seguintes princípios para a gestão da Segurança da Informação:

a) gestão baseada em riscos e proporcionalidade;

b) proteção da informação ao longo de todo o seu ciclo de vida;

c) menor privilégio, necessidade de conhecimento e segregação de funções;

d) segurança e privacidade desde a concepção e por padrão;

e) responsabilização, rastreabilidade e prestação de contas;

f) conformidade legal, regulatória, contratual e com requisitos de clientes;

g) resiliência, continuidade e capacidade de recuperação;

h) melhoria contínua baseada em riscos, incidentes, auditorias, indicadores e evolução das ameaças;

i) promoção da cultura de Segurança da Informação, da conscientização e do comportamento seguro.

6.1. RESPONSABILIDADES

a) **Alta Direção:** patrocinar a Segurança da Informação, aprovar esta Política, assegurar a disponibilização de recursos compatíveis com os riscos identificados e deliberar sobre temas estratégicos relacionados à Segurança da Informação.

b) **Diretoria de Transformação Digital:** exercer a governança da Segurança da Informação e do tratamento das informações da INFOTEC BRASIL, coordenando a implementação desta Política, coordenando a implementação desta Política, acompanhando riscos, indicadores, incidentes, exceções, requisitos de privacidade, continuidade dos negócios e a conformidade com esta Política, submetendo, quando necessário, temas relevantes ao Comitê de Riscos e ao Comitê de

Compliance e Integridade.

c) **Gerência de Infraestrutura de TI:** implementar, operar, monitorar e manter os controles técnicos e operacionais relacionados à Segurança da Informação e ao tratamento das informações da INFOTEC BRASIL, abrangendo infraestrutura, identidades, acessos, redes, dispositivos, sistemas, monitoramento, continuidade dos serviços e resposta a incidentes tecnológicos.

d) **Transformação Digital e áreas de desenvolvimento:** incorporar requisitos de segurança e privacidade no ciclo de vida de soluções, integrações, automações e mudanças tecnológicas.

e) **Sistema de Gestão Integrada (SGI):** apoiar a gestão de de riscos, a realização de auditorias, o tratamento de não conformidades, o monitoramento de indicadores e melhoria contínua relacionados à Segurança da Informação.

f) **Jurídico:** prestar orientação quanto às obrigações legais, regulatórias e contratuais relacionadas à Segurança da Informação, à Proteção de Dados, à privacidade e às demais normas aplicáveis, apoiando a avaliação de riscos jurídicos e a tomada de decisões.

g) **Gente e Cultura**: apoiar a aplicação dos controles de Segurança da Informação nos processos de admissão, movimentação, afastamento e desligamento, bem como nas ações de treinamento, , conscientização, formalização de termos e aplicação de medidas disciplinares.

h) **Gestores:** proteger as informações e processos sob sua responsabilidade, aprovar e revisar as necessidades de acesso, identificar e comunicar riscos relacionados à Segurança da Informação e assegurar o cumprimento desta Política por suas equipes.

i) **Usuários e terceiros:** cumprir esta Política e os documentos complementares, proteger suas credenciais e os ativos sob sua responsabilidade, comunicar prontamente eventos ou incidentes de segurança e colaborar com ações autorizadas de prevenção, apuração, contenção e e correção.

7. DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

As diretrizes abaixo estabelecem os requisitos corporativos mínimos. Regras técnicas, prazos, critérios, fluxos operacionais e controles específicos deverão ser mantidos em normas, procedimentos, padrões e planos complementares.

7.1. CLASSIFICAÇÃO DA INFORMAÇÃO

Todas as informações tratadas pela INFOTEC BRASIL, sejam adquiridas, recebidas ou geradas internamente, são consideradas ativos da organização ou de terceiros e devem ser protegidas conforme sua sensibilidade, criticidade, finalidade e requisitos legais ou contratuais.

As informações devem ser classificadas e tratadas de acordo com critérios corporativos, sendo adotados controles proporcionais para acesso, armazenamento, compartilhamento, transmissão, retenção e descarte.

A classificação e os requisitos de tratamento serão detalhados em norma específica.

7.2. CONTROLE DE ACESSOS

O acesso às informações, sistemas, serviços e ambientes deve observar os princípios do menor privilégio, necessidade de conhecimento, segregação de funções e rastreabilidade.

Os acessos devem ser concedidos, alterados, revisados e revogados por processo formal, com aprovação compatível com o risco e a criticidade das informações.

Contas privilegiadas, administrativas, de serviço ou compartilhadas, quando excepcionalmente necessárias, devem ser submetidas a controles reforçados, monitoramento e gestão segura de credenciais.

7.3. SEGURANÇA DE REDES

As redes de dados da INFOTEC BRASIL devem ser protegidas contra acesso ou uso indevido, alteração não autorizada, indisponibilidade e interrupções não planejadas.

A arquitetura de rede deve considerar segmentação, controle de tráfego, proteção de conexões, monitoramento, registro de eventos e revisão periódica dos acessos e serviços expostos.

7.4. USO DE RECURSOS DE TI

Os recursos tecnológicos corporativos destinam-se prioritariamente às atividades profissionais e devem ser utilizados de forma ética, responsável, segura e em conformidade com as leis, contratos e normas internas.

É vedado o uso dos recursos para fins ilegais, ofensivos, discriminatórios, fraudulentos ou que comprometam a segurança, a continuidade, a reputação ou a imagem da INFOTEC BRASIL e de seus clientes.

Somente soluções, dispositivos, aplicações e serviços previamente autorizados poderão processar ou armazenar informações corporativas.

7.5. SEGURANÇA NA NUVEM

O uso de serviços em nuvem deve ser previamente avaliado e aprovado pelas áreas responsáveis, considerando riscos, requisitos legais, contratuais, de privacidade, continuidade e segurança.

A responsabilidade pela proteção das informações deve ser definida conforme o modelo de responsabilidade compartilhada entre a INFOTEC BRASIL, o provedor, clientes e terceiros envolvidos.

Devem existir mecanismos adequados de identidade e acesso, registro de eventos, auditoria, backup, recuperação, continuidade, portabilidade e encerramento seguro do serviço.

As informações devem ser armazenadas e processadas em conformidade com a legislação aplicável e com os requisitos contratuais.

7.6. USO DE INTELIGÊNCIA ARTIFICIAL

A utilização de soluções baseadas em inteligência artificial deve observar transparência, finalidade legítima, supervisão humana, proteção das informações, respeito à propriedade intelectual e avaliação dos riscos associados.

Dados pessoais, informações confidenciais ou restritas e informações de clientes somente poderão ser processados por soluções de IA após avaliação e autorização compatíveis com o risco, a finalidade e os requisitos legais ou contratuais.

Os resultados produzidos por IA devem ser revisados antes de sua utilização em decisões, comunicações, códigos, contratos, avaliações ou entregas profissionais.

Soluções de IA com potencial de afetar direitos, pessoas, serviços críticos ou decisões relevantes devem possuir mecanismos de explicabilidade, auditabilidade, prevenção de vieses e intervenção humana.

7.7. TREINAMENTO E CONSCIENTIZAÇÃO

Todos os usuários devem receber orientação e participar de treinamentos periódicos sobre Segurança da Informação, proteção de dados pessoais, prevenção a incidentes e riscos relacionados ao uso de tecnologias, serviços em nuvem e inteligência artificial.

As ações de conscientização devem ser proporcionais ao perfil de risco e às responsabilidades de cada função, sendo sua participação e eficácia monitoradas.

7.8. GESTÃO DE INCIDENTES

Eventos e incidentes de segurança devem ser prontamente comunicados pelos canais corporativos definidos e tratados por processo formal.

O processo deve contemplar registro, classificação, análise, contenção, preservação de evidências, erradicação, recuperação, comunicação, encerramento e lições aprendidas.

Incidentes envolvendo dados pessoais, clientes, serviços críticos, provedores de nuvem ou uso indevido de ferramentas de IA devem envolver as áreas competentes e observar as obrigações legais,

regulatórias e contratuais aplicáveis.

Somente pessoas autorizadas poderão realizar comunicações externas sobre incidentes.

7.9. SEGURANÇA FÍSICA E AMBIENTAL

Instalações, ambientes críticos, áreas técnicas, equipamentos e mídias devem ser protegidos contra acesso não autorizado, danos, interferências, desastres e interrupções.

Os controles físicos e ambientais devem ser proporcionais à criticidade dos ativos e aos riscos existentes, incluindo controle de acesso, proteção de visitantes, energia, climatização, incêndio, armazenamento e descarte seguro.

7.10. GESTÃO DE TERCEIROS

Terceiros que tenham acesso a informações, sistemas, ativos, instalações ou processos da INFOTEC BRASIL devem assumir compromissos de confidencialidade e cumprir requisitos de segurança compatíveis com os riscos envolvidos.

A avaliação de riscos de terceiros deve ocorrer antes da contratação ou do início do acesso e ser revisada conforme a criticidade, mudanças relevantes, incidentes ou exigências contratuais.

Os contratos devem estabelecer responsabilidades sobre acesso, proteção das informações, dados pessoais, incidentes, continuidade, subcontratação, auditoria, devolução e eliminação de dados e encerramento do serviço.

7.11. PROTEÇÃO DE DADOS PESSOAIS

O tratamento de dados pessoais deve observar a legislação aplicável e os princípios de finalidade, adequação, necessidade, transparência, segurança, prevenção, não discriminação e responsabilização.

A INFOTEC BRASIL deve manter governança própria de privacidade, incluindo definição dos papéis de tratamento, atendimento aos direitos dos titulares, gestão de incidentes, retenção, compartilhamento, contratação de operadores e avaliação de riscos.

As regras detalhadas para proteção de dados pessoais serão estabelecidas em Política de Privacidade e Proteção de Dados e em procedimentos complementares.

7.12. ANÁLISE DE RISCOS

A INFOTEC BRASIL deve manter processo formal para identificar, analisar, avaliar e tratar riscos de Segurança da Informação, considerando ameaças, vulnerabilidades, probabilidade, impacto e controles existentes.

Os riscos devem possuir proprietário, plano de tratamento, prazo e forma de acompanhamento. A aceitação de riscos residuais deve respeitar critérios e alçadas formalmente definidos.

A análise de riscos deve ser revisada periodicamente e diante de mudanças relevantes, incidentes, novos serviços, fornecedores, contratos ou requisitos legais.

7.13. CONTINUIDADE DOS NEGÓCIOS

Planos de continuidade, resposta a crises e recuperação devem ser mantidos para processos, informações, sistemas e serviços críticos, considerando pessoas, instalações, fornecedores e dependências tecnológicas.

Os planos devem ser atualizados e testados periodicamente, com objetivos de recuperação definidos conforme os impactos ao negócio.

Os cenários de continuidade devem considerar, quando pertinentes, falhas em serviços de terceiros, ambientes em nuvem, incidentes cibernéticos, indisponibilidade de sistemas e dependências de soluções baseadas em IA.

7.14. CONFORMIDADE COM LEIS E CONTRATOS

A INFOTEC BRASIL deve identificar, cumprir e manter conformidade com leis, regulamentações, normas, obrigações contratuais e requisitos de clientes aplicáveis à Segurança da Informação, proteção de dados pessoais e continuidade dos negócios.

O cumprimento desta Política e dos controles relacionados deve ser monitorado por meio de

indicadores, avaliações, auditorias, registros e tratamento de não conformidades.

7.15. EXCEÇÕES

Exceções a esta Política ou aos documentos complementares devem ser formalmente solicitadas, justificadas, avaliadas quanto ao risco, possuir responsável, controles compensatórios, prazo de validade e aprovação conforme a alçada definida.

Exceções não serão permanentes por padrão. Exceções vencidas ou descumpridas deverão ser tratadas como não conformidades.

8. COMUNICAÇÃO E PROCEDIMENTO PADRÃO

Qualquer pessoa que tenha conhecimento ou suspeita de prática incompatível com esta Política deverá comunicar o fato. Caso sejam identificados indícios, reais ou potenciais, de algum ato ilícito ou em desconformidade com os princípios e diretrizes desta política ou com os valores éticos e de integridade da INFOTEC BRASIL praticados por qualquer colaborador, o Comitê de Compliance e Integridade deverá ser informado imediatamente, por meio do Canal de Ética disponível em:
https://contatoseguro.com.br/infotecbrasil
O referido canal possui garantia de respeito ao anonimato, caso o denunciante deseje preservar sua identidade e, ainda, os normativos da INFOTEC BRASIL proíbem a realização de qualquer medida em represária na hipótese de identificação.

9. INVESTIGAÇÕES E SANÇÕES

Todos os incidentes reportados com indícios ou suspeitas de violação desta Política serão investigados de forma imediata, independente e adequada pelo Comitê de Compliance e Integridade da INFOTEC BRASIL.
Caso, após a apuração, seja comprovada qualquer conduta incompatível com as diretrizes desta Política, serão adotadas medidas corretivas proporcionais e exemplares, levando-se em consideração a gravidade, reincidência, impacto e a legislação aplicável.

As violações desta Política constituem infração às normas internas da INFOTEC BRASIL e poderão ensejar medidas disciplinares, contratuais ou legais, observado o devido processo interno, a proporcionalidade, a gravidade da conduta e a legislação aplicável.

Qualquer pessoa que atue em nome da INFOTEC BRASIL — incluindo administradores, colaboradores, terceiros ou parceiros — estará sujeita às sanções disciplinares e legais previstas no Código de Conduta Ética, conforme abaixo:

a) Advertência por escrito;
b) Suspensão temporária;
c) Demissão sem justa causa (pessoa física);
d) Demissão por justa causa (pessoa física);
e) Rescisão de contratos e exclusão do fornecedor, parceiro ou terceiro (pessoa jurídica);
f) Adoção de medidas judiciais cabíveis, inclusive para reparação de danos.

10. DISPOSIÇÕES GERAIS

9.1. A INFOTEC BRASIL promoverá monitoramento periódico da efetividade desta Política, utilizando indicadores, incidentes, testes, avaliações internas, resultados de treinamentos, manifestações recebidas pelo Canal de Ética e demais mecanismos de governança, visando sua melhoria contínua.

9.2. A INFOTEC BRASIL promoverá treinamentos periódicos sobre Segurança da Informação, Segurança Cibernética, Proteção de Dados Pessoais, prevenção a incidentes, uso seguro dos recursos tecnológicos e demais temas relacionados a esta Política, podendo estabelecer programas obrigatórios conforme o nível de risco ou a natureza das atividades desempenhadas.

11. REFERÊNCIAS

a) Código de Ética da INFOTEC BRASIL;

b) Código de Conduta da INFOTEC BRASIL;

c) Política de Proteção de Dados e Confidencialidade da INFOTEC BRASIL;

d) Política do Sistema de Gestão Integrada da INFOTEC BRASIL;

e) ABNT NBR ISO/IEC 27001:2022 – Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos.