cofan

Política de Segurança Cibernética e da Informação

Sumário

Ficha de controle da política

Título	Política de Segurança Cibernética e Segurança da Informação
Área Proprietária do Procedimento	Tecnologia da Informação
Escopo de Geografia	Brasil

Histórico de versões

Versão	Aprovado por	Data da aprovação	Resumo das alterações
1.0	Diretoria	04/06/2025	Primeira versão formal da política

Revisão e alterações

Frequência de Revisão	Anual
Próxima Revisão Prevista	04/06/2026*

**Nota:* A próxima revisão deverá ser realizada até a data indicada, salvo necessidade de revisão extraordinária decorrente de alterações regulatórias, estruturais, operacionais ou de risco relevantes.*

1. Objetivo

A Cofan reconhece a segurança cibernética e da informação como um pilar essencial na proteção de seus clientes. Esta política tem como objetivo estabelecer diretrizes claras e abrangentes para a implementação e manutenção de práticas eficazes de segurança, assegurando a confidencialidade, integridade, disponibilidade e autenticidade das informações. Além disso, busca garantir a conformidade com as regulamentações aplicáveis e fomentar uma cultura organizacional que valorize a segurança em todas as suas dimensões.

2. Aplicação

Esta política abrange todas as áreas, unidades e prestadores de serviço da Cofan que utilizam, armazenam ou processam informações da instituição. É responsabilidade de todos os colaboradores, parceiros e terceiros contratados seguir rigorosamente as diretrizes definidas neste documento.

3. Definições

Segurança da Informação: Conjunto de medidas destinadas a proteger a confidencialidade, integridade, autenticidade e disponibilidade das informações.

Confidencialidade: Assegura que as informações sejam acessadas apenas por pessoas devidamente autorizadas.

Integridade: Garante a exatidão, consistência e completude das informações ao longo de todo o seu ciclo de vida.

Disponibilidade: Assegura que as informações e os recursos de tecnologia da informação estejam acessíveis sempre que necessários.

Autenticidade: Garante que as informações são legítimas e originadas de fontes confiáveis e verificadas.

4. Princípios gerais

Princípios norteadores da Cofan em segurança da informação:

Prevenção Ativa: Identificar, antecipar e mitigar riscos cibernéticos antes que se tornem ameaças concretas.

Capacidade de Resposta e Recuperação: Fortalecer a habilidade da organização para resistir a incidentes cibernéticos e retomar suas operações com agilidade e segurança.

Adequação Regulatória: Garantir o alinhamento com as legislações vigentes e com os principais padrões e boas práticas do setor.

Cultura de Segurança: Estimular uma cultura organizacional que valorize a proteção da informação e da segurança digital em todos os níveis e áreas da empresa.

5. Responsabilidades

5.1 Diretoria

- Promover e liderar o fortalecimento da cultura de segurança cibernética em toda a organização;
- Assegurar que a política esteja em conformidade com as regulamentações aplicáveis, sendo revisada anualmente ou sempre que necessário;
- Aprovar exceções à política e garantir a adoção de medidas corretivas adequadas diante da identificação de falhas ou não conformidades.

5.2 Compliance

- Garantir que a política esteja alinhada com os regulamentos externos e as diretrizes internas da instituição;
- Elaborar e revisar anualmente o relatório de implementação do plano de ação e resposta a incidentes;
- Assegurar que todos os colaboradores, parceiros e terceiros tenham conhecimento desta política e compreendam os requisitos a ela relacionados.

5.3 Tecnologia da informação

- Implementar e manter os procedimentos e tecnologias necessários para assegurar a conformidade com esta política;

- Realizar testes periódicos de recuperação de desastres e manter atualizado o plano de continuidade de negócios;
- Monitorar continuamente o ambiente de TI para identificar e mitigar riscos.

5.4 Colaboradores, Prestadores de serviço de TI e Terceiros Contratados

- Cumprir integralmente as diretrizes desta política;
- Reportar imediatamente qualquer incidente ou ação que possa comprometer a segurança da informação.

6. Gestão de riscos e controles

6.1 Classificação da informação

- **Confidencial:** Informações que exigem proteção especial devido ao seu potencial impacto em caso de divulgação não autorizada;
- **Restrita:** Informações que, embora sensíveis, possuem impacto menor que as confidenciais;
- **Interna:** Informações destinadas exclusivamente ao uso interno, com impacto moderado em caso de divulgação não autorizada;
- **Pública:** Informações que podem ser divulgadas publicamente sem causar danos à empresa.

6.2 Segurança física e do ambiente

- Todas as informações classificadas como confidenciais devem ser armazenadas em áreas seguras, com controle de acesso apropriado;
- Medidas de segurança devem ser implementadas para proteger informações impressas ou armazenadas em mídias físicas contra vazamentos;
- Controle de Acesso e Segregação de Funções;
- Implementar políticas de acesso baseadas em papéis (RBAC) e revisar periodicamente os direitos de acesso;
- Garantir que as funções críticas sejam segregadas para minimizar o risco de erros ou fraudes.

6.3 Senhas e autenticação

- Implementar autenticação multifator (MFA) para sistemas críticos;
- Garantir que as senhas sejam únicas, complexas e alteradas regularmente, em conformidade com as melhores práticas de segurança.

6.4 Criptografia

- Utilizar criptografia de ponta a ponta para proteger dados em trânsito e em repouso;
- As chaves criptográficas devem ser gerenciadas de forma segura e revisadas periodicamente.

6.5 Prevenção e detecção de intrusão

- Monitorar continuamente o tráfego de rede para identificar e mitigar atividades maliciosas;
- Utilização de sistemas para garantir a segurança ativa do ambiente de TI.

6.6 Backup e Recuperação de dados

- Realizar backups periodicamente e testar regularmente a restauração dos dados;
- Armazenar cópias de backup em locais fisicamente separados para garantir a recuperação em caso de desastre.

7. Conscientização e treinamentos

Todos os colaboradores devem participar de programas anuais de conscientização sobre segurança cibernética, incluindo simulações de ***phishing***[i] e ***workshops***[ii] práticos.

A comunicação contínua será mantida por meio de boletins informativos, sessões de perguntas e respostas (Q&A) e uma biblioteca de recursos acessível a todos, incluindo manuais de uso, orientações de segurança da informação e boas práticas operacionais.

[i] ***Phishing:*** *fraude que visa roubar informações pessoais, confidenciais e/ou restritas.*

[ii] ***Workshops:*** *sessões interativas para desenvolvimento de habilidades e capacitação.*

8. Monitoramento e Auditoria

Realizar auditorias internas regulares para verificar a conformidade com esta política e revisar periodicamente incidentes para melhorar as práticas de segurança.

Manter um histórico de versões da política, documentando as principais mudanças realizadas.

9. Tratamento de incidentes

Incidentes de segurança devem ser documentados, analisados e comunicados aos ***stakeholders***[i] relevantes.

Desenvolver e manter um plano de resposta a incidentes para garantir que a Cofan possa responder de forma rápida e eficaz a qualquer incidente cibernético.

10. Sanções

O descumprimento desta política poderá resultar em medidas disciplinares proporcionais à gravidade da infração, incluindo advertências, suspensão, demissão e possíveis ações legais.

[i] ***Stakeholders:*** *Partes interessadas.*