FCamara

# **Política de Segurança da Informação** - FCamara

# Sumário

| FCamara | POLÍTICA DE SEGURANÇA DA INFORMAÇÃO | Emissão<br>05/09/2023 | Classificação<br>INTERNO |
|---|---|---|---|
| Código<br>PL-001 | | Versão<br>V.3 | Aprovado por:<br>Arthur |

# CONTROLE DE VERSÃO

| Versão | Data | Autores | Notas da Revisão |
|---|---|---|---|
| V1 | 21/02/2022 | Letícia | Versão inicial |
| V2 | 23/03/2023 | Letícia | Adaptação da Política S.I. para constar como padrão enxuto e não como norma ou procedimento. |
| V3 | 05/09/2023 | Letícia | Alterado o papel e responsabilidade do Comitê em capítulo 5.1; adicionados demais Comitês específicos de S.I., segregando os grupos e suas peculiaridades. |

# APROVAÇÃO

| Elaboração | Aprovações | Aprovações |
|---|---|---|
| | 1º Aprovador | 2º Aprovador |
| **Nome completo:** Letícia Florêncio | **Nome completo:** Ana Raquel C. Siqueira<br>DocuSigned by:<br>Ana Raquel Calais Siqueira<br>D8673B8DEF4147F... | **Nome completo:** Arthur Lawrence<br>DocuSigned by:<br>arthur lawrence<br>B404B8C310964EF... |

# 1. Introdução

A FCAMARA é um ecossistema de tecnologia e inovação que potencializa o futuro de negócios integrando visão estratégica com execução inteligente, lado a lado com seus clientes, para proporcionar experiências transformadoras. O Grupo tem como missão o treinamento e formação de profissionais competentes para atuarem na prestação de serviços de tecnologia.

A FCAMARA entende que a informação corporativa é um bem essencial para suas atividades e para resguardar a qualidade e garantia dos produtos e processos ofertados a seus colaboradores e clientes.

A FCAMARA compreende que a manipulação de sua informação passa por diferentes meios de suporte, armazenamento e comunicação, sendo estes vulneráveis a fatores externos e internos que podem comprometer a segurança das informações corporativas.

Dessa forma, a Empresa estabelece sua Política de Segurança da Informação, como parte integrante do seu sistema de gestão corporativo, alinhada às boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção a informações da organização ou sob sua responsabilidade.

A Política estabelecerá diretrizes responsabilidades, sendo recomendável o acesso às Normas específicas ao procedimento desejado (como: Norma de Gestão de Mudanças; Norma de Classificação da Informação; Norma de Gestão de Identidade e Acessos; Norma de Uso de Recursos de Tecnologia da Informação e Comunicação; Norma de Gestão de Configuração de Segurança; Norma de Gestão de Vulnerabilidades; Norma de Gestão de Riscos...), disponíveis no Portal FCamara.

# 2. Objetivo

Esta política tem objetivo de:

**I.** Estabelecer diretrizes e normas de Segurança da Informação que permitam aos colaboradores da FCAMARA adotar padrões de comportamento seguro, adequados às metas e necessidades da Empresa;

**II.** Orientar quanto à adoção de controles e processos para atendimento dos requisitos de Segurança da Informação;

**III.** Resguardar as informações da FCAMARA, garantindo requisitos básicos de confidencialidade, integridade e disponibilidade;

IV. Prevenir possíveis causas de incidentes e responsabilidade legal da instituição e seus empregados, clientes e parceiros;
V. Minimizar os riscos de perdas financeiras, de participação no mercado, da confiança de clientes ou de qualquer outro impacto negativo no negócio da FCAMARA como resultado de falhas de segurança.

# 3. Escopo

Esta política se aplica a todos os usuários da informação da FCAMARA, incluindo qualquer indivíduo ou organização que possui (ou possuiu) qualquer tipo de conexão com a FCAMARA. Tais como: empregados, ex-empregados, prestadores de serviço, ex-prestadores de serviço, colaboradores, ex-colaboradores, que possuíram, possuem ou virão a possuir acesso às informações da FCAMARA e/ou fizeram, fazem ou farão uso de recursos computacionais compreendidos na infraestrutura da FCAMARA.

De forma específica esta política abrange todo o processo aplicado na manipulação dos sistemas corporativos, sendo eles: Financial, Fcteam e Imagine.

# 4. Diretrizes

A gestão de Segurança da Informação da FCAMARA se preocupa em garantir a gestão sistemática e efetiva de todos os aspectos relacionados à segurança da informação, provendo suporte às operações críticas do negócio e minimizando riscos identificados e seus eventuais impactos à instituição.

A Presidência, Diretoria Executiva, o Comitê de Segurança da Informação e a Equipe de IT, estão comprometidos com uma gestão efetiva de Segurança da Informação. Desta forma, adotam todas as medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização.

Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação às necessidades da empresa.

É política da FCAMARA:

I. Elaborar, implantar e seguir por completo políticas, normas e procedimentos de segurança da informação, garantindo que os requisitos básicos de confidencialidade, integridade e disponibilidade da informação sejam atingidos através da adoção de controles contra ameaças provenientes de fontes tanto externas quanto internas;

**II.** Disponibilizar políticas, normas e procedimentos de segurança à todas as partes interessadas e autorizadas, tais como: Empregados, terceiros contratados e, onde pertinente, clientes e parceiros.

**III.** Disponibilizar educação e conscientização sobre as práticas adotadas pela FCAMARA de segurança da informação para Empregados, terceiros contratados e, onde pertinente, clientes.

**IV.** Atender integralmente requisitos de segurança da informação aplicáveis ou exigidos por regulamentações, leis e/ou cláusulas contratuais;

**V.** Tratar integralmente incidentes de segurança da informação, garantindo que eles sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicando às autoridades apropriadas;

**VI.** Garantir a continuidade do negócio através da adoção, implantação, teste e melhoria contínua de planos de continuidade e recuperação de desastres;

**VII.** Melhorar continuamente a Gestão de Segurança da Informação através da definição e revisão sistemática de objetivos de segurança em todos os níveis da organização.

# 5. Papéis e Responsabilidades

## 5.1 Comitê Geral de Segurança da Informação

Fica constituído o Comitê Geral de Segurança da Informação, contando com a participação dos líderes dos departamentos que possuem contato com os dados confidenciais da FCamara, bem como, aos sistemas internos essenciais ao negócio, quais sejam:

- Departamento Pessoal;
- Segurança da Informação;
- Sistemas Internos;
- Infraestrutura
- Jurídico;
- Financial Controls;
- Tesouraria;
- Contabilidade;

- FP&A;
- *People*.

É responsabilidade do Comitê:

**I.** Entender os projetos atuais e a relevância da Segurança da Informação;

**II.** Cumprir com os requisitos das políticas, normas e procedimentos internos disponibilizados no Portal FCAMARA;

**III.** Promover a divulgação da Segurança da Informação em seus Departamentos, disseminando uma cultura no ambiente FCAMARA;

**IV.** Divulgar à sua equipe o material disponível em reuniões do Comitê.

## 5.2 Comitê Técnico de Segurança da Informação

Fica constituído o Comitê Técnico de Segurança da Informação, contando com a participação de membros selecionados do Departamento de sistemas internos, infraestrutura, Imagine e segurança da informação, em conjunto à Gestão de IT.

É responsabilidade do Comitê:

**I.** Atuar em conjunto em caso de incidentes relacionados à segurança da informação, a serem convocados os membros conforme a aplicabilidade;

**II.** Realizar o mapeamento de causa raiz de cada incidente mensal, para evitar a ocorrência de evento semelhante no futuro;

**III.** Apresentar os riscos observados durante o dia a dia e possíveis melhorias;

**IV.** Cumprir com os requisitos das políticas, normas e procedimentos internos disponibilizados no Portal FCAMARA e trabalhar para que se mantenham atualizados de acordo com a realidade fática da Empresa.

## 5.3 Comitê Diretor de Segurança da Informação

Fica constituído o Comitê Diretor de Segurança da Informação, contando com a participação de pelo menos um membro da diretoria financeira da FCamara, bem como, a Gestão de IT e o Departamento de Segurança da Informação, para:

**I.** Realizar *follow up* de projetos relacionados à segurança da informação;

**II.** Apresentar preocupações com vulnerabilidades internas;

**III.** Relatar novos riscos a serem inseridos em matriz, para verificação de mitigação ou possibilidade de assumir o risco;

**IV.** Entender a necessidade de investimento financeiro em tecnologia da informação;

**V.** Apresentar planos de ação para aprovação, rejeição ou justificativa.

## 5.4 Departamento de Segurança Da Informação

É responsabilidade do Departamento de Segurança da Informação:

**I.** Conduzir a Gestão e Operação da segurança da informação, tendo como base esta política e demais resoluções dos documentos integrantes ao SGSI;

**II.** Conduzir as reuniões de Comitês relativos à Segurança da Informação;

**III.** Elaborar e apoiar na condução, propondo a necessidade de criação de políticas, normas e procedimentos;

**IV.** Identificar e avaliar as principais ameaças à segurança da informação, incluindo em matriz de risco. Bem como, propor e, quando aprovado, implantar medidas corretivas para reduzir/mitigar o risco;

**V.** Tomar as ações cabíveis para se fazer cumprir os termos desta política;

**VI.** Realizar a gestão dos incidentes de segurança da informação, para o tratamento adequado;

**VII.** Apresentar ao Comitê Diretor de S.I. os KPIs de segurança da informação, no mínimo, semestralmente.

## 5.5 Responsável Da Informação

O Responsável da Informação é o “*owner*”, criador do conteúdo.

É atribuído ao Responsável da Informação:

**I.** Gerenciar as informações geradas, ou sob a responsabilidade da sua área de negócio, durante todo o seu ciclo de vida, incluindo a criação,

classificação, manuseio e descarte, conforme as normas estabelecidas pela FCAMARA;

**II.** Identificar, classificar e rotular as informações geradas ou sob a responsabilidade da sua área de negócio conforme normas, critérios e procedimentos adotados pela FCAMARA;

**III.** Periodicamente revisar as informações geradas ou sob a responsabilidade da sua área de negócio, ajustando a classificação e rotulagem delas, conforme necessário;

**IV.** Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade;

**V.** Solicitar a concessão ou revogação de acesso à informação ou sistemas de informação de acordo com os procedimentos adotados pela FCAMARA.

### 5.6 Usuários Da Informação

Usuário da Informação é quem a consome.

É responsabilidade dos Usuários da Informação:

**I.** Ler, compreender e cumprir integralmente os termos da Política de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;

**II.** Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política de Segurança da Informação, suas normas e procedimentos ao Departamento de Segurança da Informação;

**III.** Comunicar ao Departamento de Segurança da Informação qualquer evento que viole esta Política ou coloque/possa vir a colocar em risco a segurança das informações ou dos recursos computacionais da FCAMARA;

**IV.** Assinar o Termo de Entrega, Uso ou Responsabilidade da FCAMARA, formalizando a ciência e o aceite integral das disposições da Política de Segurança da Informação, bem como, para as demais normas e procedimentos de segurança, assumindo total responsabilidade pelo seu cumprimento;

**V.** Responder pela inobservância da Política de Segurança da Informação, normas e procedimentos de segurança, conforme definido no item sanções.

# 6. Sanções

## 6.1 Sanções e Punições

As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como, demais normas e procedimentos de segurança, serão passíveis de penalidades que incluem advertência verbal, advertência por escrito, suspensão não remunerada e a demissão por justa causa, tratando-se de empregado. Prestadores de serviço, parceiros e clientes, responderão pelos danos que vierem a dar causa, em conjunto de eventuais perdas e danos sofridas pela Empresa e Terceiros envolvidos, e/ou ainda, aplicação de multa, quando previsto em contrato.

A aplicação de sanções e punições será realizada conforme a análise do Comitê Gestor de Segurança da Informação e/ou do Departamento Jurídico, devendo-se considerar:

- **a.** A gravidade da infração;
- **b.** O efeito alcançado;
- **c.** A recorrência;
- **d.** As hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, em caso de Empregados.

Podendo o CGSI, no uso do poder disciplinar que lhe é atribuído, aplicar a pena que entender cabível quando tipificada a falta grave.

### 6.2 Casos Omissos

Os casos omissos serão avaliados pelo Comitê Gestor de Segurança da Informação para posterior deliberação.

As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui rol enumerativo, sendo obrigação do Usuário da Informação adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção às informações da Empresa e Terceiros.

## 7. Glossário

**Ameaça:** Causa potencial de um incidente, que pode vir a prejudicar a FCAMARA;

**Ativo:** Tudo aquilo que possui valor para a FCAMARA;

**Ativo de informação:** Patrimônio intangível da FCAMARA, constituído por suas informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro, mercadológico, de recursos humanos, legal natureza, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas a FCAMARA por parceiros, clientes, empregados e terceiros, em formato escrito, verbal, físico ou digitalizado, armazenada, trafegada ou transitando pela infraestrutura computacional da FCAMARA ou por infraestrutura externa contratada pela organização, além dos documentos em suporte físico, ou mídia eletrônica transitados dentro e fora de sua estrutura física.

**Confidencialidade:** Propriedade dos ativos da informação da FCAMARA, de não serem disponibilizados ou divulgados para indivíduos, processos ou entidades não autorizadas.

**Controle:** Medida de segurança adotada pela FCAMARA para o tratamento de um risco específico.

**Disponibilidade:** Propriedade dos ativos da informação da FCAMARA, de serem acessíveis e utilizáveis sob demanda, por partes autorizadas.

**Empresa**: A Fcamara e/ou seus fornecedores e clientes, conforme o caso.

**Responsável da Informação:** Usuário da informação, criador ou modificador, ao qual foi atribuída responsabilidade sob um ou mais ativos de informação criados, adquiridos, manipulados ou colocados sob a responsabilidade de sua área de atuação.

**Incidente de segurança da informação:** Um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações da FCAMARA.

**Integridade:** Propriedade dos ativos da informação da FCAMARA, de serem exatos e completos.

**Risco de segurança da informação:** Efeito da incerteza sobre os objetivos de segurança da informação da FCAMARA.

**Segurança da informação:** A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações da FCAMARA.
**Usuário da informação:** Colaboradores, sejam Empregados, Terceiros, Prestadores de Serviço (pontual ou recorrente), assim como quaisquer outros indivíduos ou organizações devidamente autorizadas a utilizar manipular qualquer ativo de informação da FCAMARA para o desempenho de suas atividades profissionais.

**Vulnerabilidade:** Causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as operações ou ameaçar as informações da FCAMARA.

# 8. Revisões

Esta política é revisada com periodicidade anual ou conforme a alteração dos procedimentos internos, o que ocorrer primeiro.

# 9. Gestão da Política

A Política de Segurança da Informação é aprovada pela Gestão de IT, em conjunto com a Diretoria da FCAMARA.