Docusign Envelope ID: F4BA9157-F006-8D4B-8060-6E0D9BB8F95F

FCamara

Política de Segurança da Informação - FCamara

Docusign Envelope ID: F4BA9157-F006-8D4B-8060-6E0D9BB8F95F

Sumário

Sumário 2
1. Introdução 4
2. Objetivo 4
3. Escopo 5
4. Princípios e Diretrizes da Segurança da Informação 5
5. Diretrizes da FCamara frente a Segurança da Informação 6
6. Segurança da Informação para uso de serviços em nuvem 7
7. Diretrizes em Normas Complementares 8
7.1. Gestão de Incidentes e Riscos 9
7.2. Gerenciamento de vulnerabilidades 9
7.3. Gerenciamento de acessos 9
7.4. Gerenciamento e aquisição de *softwares* 10
7.5. Classificação de informações 10
7.6. Uso de Recursos Tecnológicos 10
7.7. Fornecedores e Parceiros 11
7.8. Privacidade e Proteção de Dados 11
7.9. Plano de Comunicação do SGSI 11
8. Papéis e Responsabilidades em S.I. 12
8.1. Comitê da Alta Gestão na Segurança da Informação 12
8.2. Departamento de Segurança Da Informação 12
8.3. Responsável Da Informação 13
8.4. Usuários Da Informação 14
9. Sanções 14
9.1. Sanções e Punições 14
9.2. Casos Omissos 15
10. Glossário 15
11. Revisões 16
12. Gestão da Política 16

Docusign Envelope ID: F4BA9157-F006-8D4B-8060-6E0D9BB8F95F

FCamara	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	Emissão 30/06/2026	Classificação INTERNO
Código PL-001		Versão V.7	Aprovado por: Vice-presidência

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.
V4	28/09/2023	Letícia	Adicionadas as Partes Interessadas em política; criação do capítulo 4 e 6 (+ derivados); incluído o item “II” em capítulo 7.3; cap. 7.1 adicionado Auditoria Interna.
V5	14/03/2025	Letícia	Adicionado capítulo 6 sobre Serviços de Nuvem; retirado comité Geral e Técnico de segurança da Informação em item 7.
V6	16/05/2025	Letícia	Índice atualizado
V7	30/06/2026	Letícia	Adicionado item 7.9

APROVAÇÃO

Elaboração	Aprovações	Aprovações
	1º Aprovador	**2º Aprovador**
Nome completo: Letícia Florêncio	**Nome completo:** Robson Santos Assinado por: ROBSON DOS SANTOS 544B8BBBC63F4BE...	**Nome completo:** Kleber Santos DocuSigned by: Kleber dos Santos DF156FCF94DC408...

Assinado por:
Nathália Bordone
62592952263044B...

Docusign Envelope ID: F4BA9157-F006-8D4B-8060-6E0D9BB8F95F

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. A FCamara tem como missão o treinamento e formação de profissionais competentes para atuarem na prestação de serviços de tecnologia.

Ainda, a Empresa 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.

Também 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 aplicáveis, com o objetivo de garantir níveis adequados de proteção a informações da organização ou sob sua responsabilidade.

A Política estabelecerá diretrizes e responsabilidades, sendo recomendável o acesso às Normas específicas ao procedimento desejado conforme destacado abaixo.

2. Objetivo

Esta política tem objetivo de:

I. Estabelecer diretrizes e normas de Segurança da Informação que permitam aos colaboradores e partes interessadas à FCamara, adotar padrões de comportamento seguro, adequados à confidencialidade, integridade e disponibilidade das informações;
II. Orientar quanto à adoção de controles e processos para atendimento dos requisitos de Segurança da Informação;
III. Resguardar as informações da FCamara, seus colaboradores e partes interessadas;
IV. Prevenir possíveis causas de incidentes;

Docusign Envelope ID: F4BA9157-F006-8D4B-8060-6E0D9BB8F95F

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 e Partes Interessadas, 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.

Todos os destinatários devem observar as presentes regras e recomendações em quaisquer operações que possam impactar na segurança das informações na FCamara.

De forma específica esta política abrange todo o processo aplicado na manipulação dos sistemas corporativos declarados como essenciais ao negócio da FCamara.

4. Princípios e Diretrizes da Segurança da Informação

A Segurança da Informação, em um contexto geral, se preocupa em garantir aspectos relacionados à confidencialidade, disponibilidade e integridade da informação.

A informação pode ser criada, armazenada, processada, transmitida, usada, atualizada, descartada... E deve ser protegida em todo o seu ciclo de vida.

Dessa forma, a segurança da informação atua na preservação da confidencialidade, integridade e disponibilidade da informação da FCamara. É o meio para garantir que o negócio possa atingir seus objetivos.

- Confidencialidade: A informação da FCamara deve ser acessada apenas por pessoas ou entidades autorizadas, devendo ser protegida para a não divulgação para pessoas não autorizadas, como ex-empregados ou partes externas não autorizadas no geral;

Docusign Envelope ID: F4BA9157-F006-8D4B-8060-6E0D9BB8F95F

- Integridade: A informação da FCamara deve estar disponível de forma completa e exata;
- Disponibilidade: A propriedade da informação da FCamara de ser acessível e utilizável por partes autorizadas, garantindo que tenham acesso à informação sempre que necessário.

5. Diretrizes da FCamara frente a Segurança da Informação

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 e o Comitê da Alta Gestão de Segurança da Informação, 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.

A segurança e proteção da informação é uma responsabilidade contínua de cada usuário da informação da FCamara, em relação às informações que acessa e gerencia. Todos os usuários devem utilizar a informação da Empresa, de acordo com as determinações desta Política de Segurança da Informação.

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, quando 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, investigados, corrigidos, documentados e, quando necessário, comunicando às partes interessadas e/ou autoridades apropriadas;

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

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.

6. Segurança da Informação para uso de serviços em nuvem

A gestão de Segurança da Informação da FCamara inclui estabelecer as diretrizes corporativas para a utilização de serviços em nuvem, que devem considerar os princípios de economicidade, segurança e agilidade, de forma a facilitar as oportunidades de negócios.

O Diretor de Engenharia da FCamara deverá ser sempre consultado antes da aquisição e implementação de qualquer solução que envolva computação em nuvem na companhia, direcionado ao cliente (IaaS, PaaS ou SaaS). Se solução em nuvem direcionada à governança corporativa da FCamara (interno), o Diretor de Excelência Operacional deverá ser consultado antes da aquisição e implementação.

A utilização dos serviços de computação em nuvem no modelo de Infraestrutura como serviço deverá ser feita preferencialmente com dados armazenados em território brasileiro, com exceção a casos em que seja previsto em contrato de maneira diversa. Se o armazenamento de informações obedecer à outra jurisdição geográfica ou legal, o provedor de nuvem deverá notificar à Fcamara que, por sua vez, deverá notificar ao cliente quando aplicável.

Deverão ser utilizados somente provedores de serviço de computação em nuvem que possuam relevante reputação no mercado e plano de continuidade de negócios que

Docusign Envelope ID: F4BA9157-F006-8D4B-8060-6E0D9BB8F95F

ofereça serviço de redundância, dando preferência à: *Amazon*, *Microsoft* e *Google*. No momento da contratação deve-se observar:

- **i.** O contrato entre as Partes, devendo repassar ao Departamento Jurídico para análise minuciosa;
- **ii.** O nível de acordo de serviço para disponibilidade das informações;
- **iii.** O *backup* fornecido;
- **iv.** O retorno e fornecimento de informações necessárias (ex: arquivos de configuração, código-fonte e dados que pertencem à Fcamara);
- **v.** Quais medidas de segurança da informação o provedor de serviços gerencia (por exemplo: proteção contra *malware*; soluções de monitoramento...);
- **vi.** As medidas de segurança da informação que deverão ser gerenciados pela Fcamara residualmente;
- **vii.** O suporte e apoio dedicado em caso de incidente de segurança da informação, considerando a coleta de provas digitais;
- **viii.** Como alterar ou parar o uso de serviços em nuvem, incluindo estratégias de saída;
- **ix.** Se há notificação em caso de alterações na infraestrutura técnica que altere ou afete a oferta do serviço em nuvem;
- **x.** O uso de provedores de serviços em nuvem por pares ou outros subcontratados.

A gestão dos serviços em nuvem será de responsabilidade da área contratante, sendo que, a nível corporativo, a responsabilidade será do Departamento de Infraestrutura Interna.

A gestão do serviço deverá manter contato próximo de suporte, para casos de problemas técnicos, dúvidas, alertas, falhas e eventuais descumprimentos contratuais.

7. Diretrizes em Normas Complementares

A FCamara utiliza de Políticas, Normas, Planos e Procedimentos complementares à esta política para disseminar conteúdo específico entre Colaboradores e Partes Interessadas, com as devidas sanções aplicáveis em caso de descumprimento.

Docusign Envelope ID: F4BA9157-F006-8D4B-8060-6E0D9BB8F95F

7.1. Gestão de Incidentes e Riscos

Caso seja observado por um Usuário, ou Parte Interessada, um possível incidente de segurança no ambiente ou que afeta à FCamara, é necessário que seja aberto chamado ao Departamento de Infraestrutura, via canal de atendimento próprio, *FreshService*. Seguindo os passos dedicados em **PR 001 - PROCEDIMENTO DE GESTÃO DE INCIDENTES**.

Quando caracterizado um risco à FCamara, a empresa seguirá com a metodologia de avaliação e tratamento de riscos de maneira contínua, que consta em **NR-001- Norma de Gestão de Riscos**, em conjunto ao **PN 002 - Plano de Continuidade de Negócios**.

7.2. Gerenciamento de vulnerabilidades

O gerenciamento de vulnerabilidades relacionados à FCamara está descrito em **NR-002-NORMA DE GESTÃO DE VULNERABILIDADE**, que se aplica aos *hardwares* e *softwares* que armazenam, processam, ou transferem dados confidenciais, considerados necessários ao negócio da Fcamara. Em norma, consta o prazo de correção de acordo com a sua classificação.

O gereciamento é realizado por ferramentas da FCamara, como IDS, Firewall, DLP e são identificados em maior abrangência durante *scan* de vulnerabilidade e/ou Pentest.

7.3. Gerenciamento de acessos

A gestão de identidade e acessos refere-se à gestão do ciclo de vida de um acesso, ou seja, ao conjunto de processos que permitem rastrear a identidade e o acesso (à instalação e aos sistemas de negócios essenciais à FCamara) dos colaboradores e Partes Interessadas.

A Norma **NR-11 - NORMA DE GESTÃO DE IDENTIDADE E ACESSOS FISICO** mencina o fluxo de controle de identidade e acesso, que é um procedimento de segurança que permite a entrada a locais de acesso restrito apenas à pessoas autorizadas e menciona o fluxo de revogação de acessos.

Os colaboradores e Partes Interessadas da FCamara são responsáveis pelos atos praticados com sua identificação, que é instransferível.

O controle de acesso lógico à rede corporativa, utiliza a tecnologia para permitir o acesso a recursos computacionais, sistemas e repositório de dados, realizando a verificação da identidade dos usuários por meio de credencias de acesso na autenticação via *Office 365,* conforme consta em **PR-005- PROCEDIMENTO ONBOARDING E OFFBOARDING** e **NR-003 - NORMA DE CONTROLE DE ACESSO LÓGICO – SISTEMAS DE NEGOCIOS.** Em complemento à Norma estão os acessos ao banco de dados das redes corporativos: Como é concedido o acesso; como é gerenciado/registrado o acesso; como é excluído, em **NR-12- NORMA DE CONTROLE DE ACESSO LÓGICO – BANCO DE DADOS**.

Docusign Envelope ID: F4BA9157-F006-8D4B-8060-6E0D9BB8F95F

Devem ser implementados controles de perfil e permissões, de acordo com o cargo e função essencial à FCamara, visando a proteção dos ativos da informação da FCamara.

Todas as Normas acima citadas estão regidas em complemento à **PL-003- POLITICA DE CONTROLE DE ACESSO**, que detalha a importância de proteger ambientes físicos e lógicos contra acessos não autorizados. Os fluxos estabelecidos devem ser seguidos por todos os colaboradores e Partes Interessadas, sob pena das sanções aplicáveis.

7.4. Gerenciamento e aquisição de *softwares*

Toda aquisição, desenvolvimento e manutenção de *software* deve ter como objetivo único o atendimento e suporte dos requisitos de negócios da Fcamara. A área requisitante deve garantir a comprovação pelo fornecedor do atendimento aos requisitos de segurança da Fcamara, a serem nomeados pela área de Segurança da Informação.

Os *softwares* não poderão ser utilizados de modo contrário ao estipulado no contrato específico, na norma **NR - 005 - Norma de Aquisição Desenvolvimento e Manutenção de Software**, na orientação específica do Departamento de Infraestrutura, ou mesmo conforme a legislação vigente.

7.5. Classificação de informações

As informações de propriedade ou sob custódia da Fcamara devem ser armazenadas, transitadas ou descartadas de acordo com sua relevância e classificação atribuída (pública, restrita, interna ou confidencial), de acordo com a **NR-010 - NORMA DE CLASSIFICAÇÃO DA INFORMAÇÃO**.

O descarte de informações deve obedecer a prazos legais de retenção de informação e serem descartados de forma segura, em que não se faz possível recuperá-la, seja quando a informação estiver em meios físicos ou lógicos, em conformidade com a **NR-004 – NORMA DE USO DE RECURSOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO**.

7.6. Uso de Recursos Tecnológicos

Os colaboradores só podem acessar as informações e recursos de tecnologia da informação e comunicação corporativos, necessários e autorizados para o desenvolvimento de suas atividades profissionais, de acordo as atividades exercidas para ao Fcamara, de acordo com a **NR-004 - NORMA DE USO DE RECURSOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO**, em conjunto à **PL-006 POLÍTICA DE DISPOSITIVOS MÓVEIS**.

Todos os colaboradores da FCamara e Partes Interessadas, onde aplicável referente a uso de recursos tecnológicos, devem:

- Utilizá-los com responsabilidade, cautela, diligência e zelar pelo seu bom estado de conservação;
- Acessá-los respeitando os locais de rede, no mínimo, com senha;
- Protegê-los nas formas física e lógica contra acesso, uso indevido ou divulgação, modificação, adulteração ou destruição não autorizada das informações corporativas;
- Acessá-los por meio da identidade digital individual e respeitar os limites de acesso estabelecidos pela FCamara;
- Atentar-se aos domínios oficiais e reconhecidos pela FCamara, não abrindo arquivos de domínios não confiáveis;
- Manter a tela e mesa limpa, principalmente em sua ausência, bloqueando o acesso ao equipamento.

7.7. Fornecedores e Parceiros

Todos os colaboradores e Partes Interessadas à FCamara devem empenhar, de forma permanente, as ações e esforços para prover e exigir total segurança, sigilo, confidencialidade, disponibilidade e integridade das informações, junto aos parceiros e fornecedores, de acordo com a **PL -004 - POLÍTICA DE FORNECEDORES E PARCEIROS FCAMARA**.

Os respectivos contratos, acordos e demais documentos inerentes, devem prever a obrigação do cumprimento das políticas e normas internas da FCamara.

7.8. Privacidade e Proteção de Dados

A **PL - 005 - POLÍTICA INTERNA DE PROTEÇÃO E PRIVACIDADE DE DADOS** esclarece ao Titular quais dados são os seus dados coletados, como são coletados, qual o tratamento do dado, como é a forma de armazenamento, se há qualquer compartilhamento com Terceiros, por quanto tempo são armazenadas, dentre outras informações essenciais em relação aos dados pessoais.

Para dados tratados de Partes Interessadas, deve ser observada a Política de proteção de dados externa, disponível no site oficial FCamara.

7.9. Plano de Comunicação do SGSI

O **Plano de Comunicação do SGSI (PN-003)** estabelece as diretrizes para a comunicação de assuntos relacionados à Segurança da Informação, privacidade, proteção de dados, continuidade de negócios, incidentes de segurança e compliance. O documento define quem pode realizar comunicações internas e externas, quais informações devem ser comunicadas, para quem, por quais canais e em quais situações, garantindo que as comunicações sejam seguras, rastreáveis, tempestivas e alinhadas aos requisitos da ISO 27001, LGPD e demais obrigações regulatórias e contratuais. A responsabilidade pela coordenação dessas comunicações é centralizada na área de Segurança da Informação, DPO e, quando necessário, no Departamento Jurídico.

Docusign Envelope ID: F4BA9157-F006-8D4B-8060-6E0D9BB8F95F

Além disso, o plano define os fluxos de comunicação para incidentes críticos, vazamentos de dados, crises cibernéticas, problemas técnicos, gestão de mudanças e comunicação com clientes, fornecedores, autoridades regulatórias e outras partes interessadas.

Também estabelece os canais oficiais de comunicação (como teams, e-mail corporativo e ITSM), os responsáveis por cada tipo de comunicação e as regras para gestão de crises, determinando que somente a Alta Direção ou representantes formalmente autorizados podem se manifestar em nome da organização durante situações críticas.

8. Papéis e Responsabilidades em S.I.

8.1. Comitê da Alta Gestão na Segurança da Informação

Fica constituído o Comitê da Alta Gestão de Segurança da Informação, contando com a participação de pelo menos um membro da Diretoria e/ou Vice-presidência 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. Estabelecer processos permanentes de conscientização e sensibilização em Segurança da Informação;

III. Apresentar preocupações com vulnerabilidades internas;

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

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

VI. Apresentar planos de ação para aprovação, rejeição ou justificativa;

VII. Agir de acordo com a **PL-007 - POLITICA DA ALTA DIRETORIA**.

8.2. Departamento de Segurança Da Informação

É responsabilidade do Departamento de Segurança da Informação:

Docusign Envelope ID: F4BA9157-F006-8D4B-8060-6E0D9BB8F95F

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 da Alta Gestão de S.I. os KPIs de segurança da informação, no mínimo, semestralmente;

VIII. Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade.

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

Docusign Envelope ID: F4BA9157-F006-8D4B-8060-6E0D9BB8F95F

8.4. 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.

9. Sanções

9.1. 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.

Partes Interessadas 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 da Alta Gestão 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.

Docusign Envelope ID: F4BA9157-F006-8D4B-8060-6E0D9BB8F95F

9.2. Casos Omissos

Os casos omissos serão avaliados pelo Comitê da Alta Gestão de S.I. 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.

10. 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 partes interessadas, 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.

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

Empresa: A FCamara e/ou seus clientes, Partes Interessadas, 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.

Risco de segurança da informação: Efeito da incerteza sobre os objetivos de segurança da informação da FCamara, que envolvam possível quebra de confidencialidade, integridade e/ou disponibilidade.

Usuário da informação: Colaboradores, sejam Empregados, Terceiros, Prestadores de Serviço (pontual ou recorrente), assim como quaisquer outros indivíduos ou organizações devidamente autorizadas, denominados como Partes Interessadas, a

Docusign Envelope ID: F4BA9157-F006-8D4B-8060-6E0D9BB8F95F

utilizar manipular qualquer ativo de informação da FCamara para o desempenho de suas atividades.

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

11. Revisões

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

12. Gestão da Política

A Política de Segurança da Informação é aprovada pelo Comitê da Alta Gestão de Segurança da Informação