

Abrangência	Sistema FIESC
Área Gestora	GETIC - Gerência Executiva de Tecnologia da Informação
Área Corresponsável	Não há
Aprovador	Mario Cezar de Aguiar

## 1. OBJETIVO

O objetivo deste documento é o de balizar o comportamento de todos os fornecedores que possuem relação com os ativos de informação do Sistema FIESC, bem como conscientizar os fornecedores sobre o correto uso dos recursos da organização.

Este documento também visa contemplar a definição de responsabilidade sobre as ações de fornecedores e ações disciplinares relacionadas.

## 2. DOCUMENTOS DE REFERÊNCIA

- CE-F00-FIESC - Código de Conduta Ética;
- Política Relacionamento com Fornecedores;
- Política de Consequências.

## 3. CONCEITOS

**Ativo:** elemento que possui valor para a organização do ponto de vista da Segurança da Informação.

**Disponibilidade:** ato de estar disponível a quem de direito quando este desejar o acesso;

**Integridade:** garantia de que a informação não foi alterada.

**Confidencialidade:** garantia de que a informação somente pode ser acessada por quem de direito.

**Fornecedor:** pessoa externa ao Sistema FIESC (não colaborador) que possui contrato de fornecimento de produtos ou serviços.

**Colaborador:** pessoas com contrato de trabalho formalmente estabelecido nas instituições que compõem o Sistema FIESC, adicionalmente no caso desta política podem incluir, estagiários, jovem aprendiz.

**Credenciais Institucionais:** Credencial para acesso a sistemas corporativos.

**VPN:** Rede Virtual Privada (*Virtual Private Network*), é uma rede de comunicações privada construída sobre uma rede de comunicações pública (como, por exemplo, a Internet). Em resumo, cria uma conexão segura e criptografada, que pode ser considerada como um túnel, entre o seu computador e um servidor operado pelo serviço VPN.

## **4. DIRETRIZES DE SEGURANÇA**

Os itens abaixo descrevem as diretrizes de segurança relacionadas com os fornecedores.

### **4.1. PROPRIEDADE INTELECTUAL**

- O fornecedor é responsável por garantir a conformidade legal de todo e qualquer sistema ou conteúdo utilizado durante a realização de seu serviço;
- O fornecedor é responsável pela propriedade intelectual do conteúdo dos equipamentos que trazer para dentro das dependências do Sistema FIESC;
- O fornecedor é responsável por garantir que os softwares por ele instalados não ferem nenhum tipo de lei de direitos autorais.

### **4.2. ACESSO À INTERNET**

- O acesso à internet realizado pelo fornecedor em qualquer uma das redes disponibilizadas pelo Sistema FIESC, somente poderá ocorrer após autorização formal e com acompanhamento de um colaborador do Sistema FIESC responsável;
- O Sistema FIESC se reserva o direito de monitorar o acesso à internet do fornecedor a fim de para garantir o uso adequado;
- O Sistema FIESC se reserva o direito de bloquear os sites que considerar inadequados para a empresa, sem prévio aviso;
- O acesso à internet realizado pelo fornecedor deverá ter como único objetivo o cumprimento de seu serviço, seja este acesso fornecido pelo Sistema FIESC ou por terceiros.

### **4.3. COMPUTAÇÃO MÓVEL**

- O Sistema FIESC reserva-se no direito de realizar auditoria nos equipamentos do fornecedor, antes de autorizar o uso na instituição;
- O fornecedor se compromete inteiramente pela segurança dos dados de seus equipamentos nas dependências do Sistema FIESC;
- O fornecedor é responsável por garantir que os equipamentos ou mídias que utiliza estão com todos os softwares atualizados, legalizados, com antivírus e livres de qualquer tipo de software que prejudique a rede interna do Sistema FIESC.

### **4.4. E-MAIL**

- O Sistema FIESC reserva-se o direito de monitorar os e-mails enviados e recebidos pelo fornecedor, quando este utilizar a plataforma de gerenciamento de e-mails fornecida pelo Sistema FIESC;
- O fornecedor assume que todos os e-mails enviados durante a execução de serviço, utilizando conta fornecida pela FIESC, são e-mails corporativos e podem ser monitorados;
- Nas dependências do Sistema FIESC o fornecedor deve ler e enviar e-mails apenas relacionados com seu trabalho;

- A qualquer tempo e de qualquer local, o fornecedor não deve encaminhar e-mails para colaboradores do Sistema FIESC cujo conteúdo não tenha relação com o trabalho.

#### **4.5. MANUSEIO LÓGICO DE INFORMAÇÕES**

- O fornecedor se compromete a apenas receber informações do Sistema FIESC que tenham relação direta com seu serviço e após consentimento e autorização formal do proprietário da informação;
- O fornecedor se compromete com a total confidencialidade, integridade e disponibilidade das informações do Sistema FIESC que lhe forem concedidas;
- A divulgação interna das informações do Sistema FIESC na empresa do fornecedor deve ser informado formalmente alinhada entre as partes;
- O fornecedor se compromete a não transmitir informações do Sistema FIESC por canais de comunicação não seguros, que possam ocasionar vazamento destas informações;
- O fornecedor se compromete com o descarte adequado e seguro das informações do Sistema FIESC ao final do serviço ou quando elas não forem mais utilizadas (o que ocorrer primeiro);
- O Sistema FIESC se reserva no direito de realizar auditorias de segurança da informação em seus fornecedores, quando as informações fornecidas forem de classificação RESTRITA ou CONFIDENCIAL.

#### **4.6. ARMAZENAMENTO LÓGICO DE INFORMAÇÕES**

- O armazenamento de informações do Sistema FIESC pelo fornecedor deve ser realizado de modo seguro, ou seja, com controle de acesso restrito aos envolvidos com o serviço dentro da empresa e com criptografia quando a informação for confidencial;
- Caso o fornecedor esteja com uma mídia em trânsito contendo informações do Sistema FIESC, este é responsável por garantir que a perda ou roubo desta mídia não implique no acesso a estas informações;
- O fornecedor também se compromete com a garantia de que as informações do Sistema FIESC não serão alteradas durante o armazenamento em qualquer tipo de mídia sob sua responsabilidade;
- Todo e qualquer dado armazenado pelo fornecedor deverá ser excluído de maneira irreversível após o término do contrato ou quando os dados não forem mais necessários para a prestação de serviços. Para dados eletrônicos, os fornecedores devem seguir práticas reconhecidas de exclusão segura, incluindo a destruição física de mídias.

#### **4.7. ACESSO À REDE INTERNA (LOCAL OU REMOTO)**

- O fornecedor somente poderá acessar a rede interna após autorização formal e mediante autenticação individual na rede do Sistema FIESC;
- O acesso do fornecedor à rede interna poderá ser monitorado pelo setor de Tecnologia da Informação da FIESC quando este julgar necessário;

- O Sistema FIESC se reserva no direito de liberar o acesso local ou remoto a sua rede interna, somente após a autorização formal e com o devido acompanhamento por um colaborador;
- Os canais de acesso aos ambientes do Sistema FIESC podem seguir regras para garantir a sua confidencialidade, integridade e disponibilidade, desta forma, estes acessos podem ser realizados utilizando MFA (Múltiplo Fator de Autenticação) ou tecnologias seguras, tais como gestão de acesso, criptografia ou VPNs (*Virtual Private Network*);
- Os acessos remotos de todos os fornecedores devem ser criados e autorizados pela equipe de Tecnologia da Informação da FIESC.

#### **4.8. USO DE SENHAS**

- O fornecedor não deve solicitar, aceitar ou utilizar senha de acesso dos colaboradores do Sistema FIESC em nenhum caso;
- Toda senha utilizada pelo fornecedor deve ter sido criada especificamente para este fim e identificá-lo de modo inequívoco;
- A FIESC é responsável por realizar a inativação da senha do fornecedor. Caso o fornecedor identifique que a credencial continua ativa, após finalização de contrato, este deve solicitar obrigatoriamente a sua desativação;
- O fornecedor não deve compartilhar senhas utilizadas para acesso a sistemas da FIESC entre seus colaboradores, ou seja, cada credencial e senha deve identificar um único colaborador do fornecedor;
- O fornecedor é responsável pela segurança das senhas que lhe são entregues e deve comunicar imediatamente ao Sistema FIESC a sua perda ou vazamento.

#### **4.9. COLABORADORES DO FORNECEDOR**

- O fornecedor deve garantir que seus colaboradores alocados para a realização de determinado serviço possuem a formação e qualificação necessária para tal;
- O fornecedor deve informar ao Sistema FIESC o nome, formação e tempo de serviço de seus colaboradores quando for solicitado;
- O Sistema FIESC reserva-se no direito de estabelecer requisitos de qualificação, formação e tempo de serviço, para autorizar o acesso de colaboradores do fornecedor a suas informações, sistemas ou dependências físicas;
- O fornecedor é responsável por comunicar imediatamente ao Sistema FIESC o desligamento de seus colaboradores, quando estes estejam prestando algum serviço interno ou possuam credenciais de acesso aos sistemas da FIESC;
- O fornecedor deve comunicar imediatamente qualquer mudança na lista de seus colaboradores autorizados a prestar o serviço interno ao Sistema FIESC;
- Todos os colaboradores do fornecedor que prestam serviço ao Sistema FIESC assumem total conhecimento e concordância com o conteúdo deste documento, ficando sob a responsabilidade da empresa fornecedora a divulgação entre seus funcionários.

#### **4.10. SEGURANÇA FÍSICA**

- O fornecedor deve garantir que seus colaboradores alocados para a realização de determinado serviço possuem a formação e qualificação necessária para tal;
- O fornecedor deve informar ao Sistema FIESC o nome, formação e tempo de serviço de seus colaboradores quando for solicitado;
- O Sistema FIESC reserva-se no direito de estabelecer requisitos de qualificação, formação e tempo de serviço, para autorizar o acesso de colaboradores do fornecedor a suas informações, sistemas ou dependências físicas;
- O fornecedor é responsável por comunicar imediatamente ao Sistema FIESC o desligamento de seus colaboradores, quando estes estejam prestando algum serviço interno ou possuam credenciais de acesso aos sistemas da FIESC;
- O fornecedor deve comunicar imediatamente qualquer mudança na lista de seus colaboradores autorizados a prestar o serviço interno ao Sistema FIESC;
- Todos os colaboradores do fornecedor que prestam serviço ao Sistema FIESC assumem total conhecimento e concordância com o conteúdo deste documento, ficando sob a responsabilidade da empresa fornecedora a divulgação entre seus funcionários.

#### **4.11. GESTÃO DE RISCOS DE FORNECEDORES**

- O Sistema FIESC se reserva no direito de realizar a gestão de riscos de fornecedores, baseado principalmente no tipo de serviço oferecido, tipos de dados trafegados e quaisquer outros parâmetros que julgue necessário;
- Os fornecedores do Sistema FIESC podem receber a qualquer momento questionários de auditoria ou visitas para homologação e gestão de risco de seus fornecedores;
- Em toda nova contratação, o Sistema FIESC poderá realizar uma avaliação de riscos de segurança dos novos fornecedores. Este fator pode ser decisivo para a contratação.

### **5. AUTORES E REVISÃO**

A Política de Segurança da Informação para Fornecedores do Sistema FIESC, bem como a sua revisão e manutenção, são de autoria do Comitê Operacional de Segurança da Informação.

Dúvidas sobre a aplicação desta política ou sugestões de alteração e melhoria podem ser encaminhadas para os membros do Comitê Operacional de Segurança da Informação.

### **6. INCIDENTES E MEDIDAS DISCIPLINARES**

Por padrão, os fornecedores devem notificar imediatamente a organização em caso de qualquer incidente de segurança envolvendo os ativos ou dados do Sistema FIESC. A organização e o fornecedor devem seguir um plano de resposta a incidentes colaborativo, a fim de resolver os incidentes da maneira mais rápida e assertiva possível.

Qualquer violação das diretrizes constantes nesta política constitui-se em incidentes de segurança da informação e será devidamente registrado e analisado pelo Comitê de Segurança da Informação da FIESC, em consonância com a Política de Consequências. Após análise do Comitê de Segurança, serão deliberadas medidas disciplinares ao fornecedor, que podem incluir:

- Advertência formal ou informal;
- Cancelamento do contrato de prestação de serviço;
- Multas previstas em contrato;
- Ações judiciais ou abertura de boletim de ocorrência.

## 6.1. INTEGRANTES DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO

Os integrantes do Comitê estão descritos no Anexo III da PO-F00, disponível na [Base do Conhecimento](#).

## 7. ANEXOS

- Não há.

## 8. QUADRO DE REVISÃO

Este documento deve ser revisado, e uma nova versão deve ser elaborada, homologada, divulgada e distribuída nos seguintes casos:

Alteração significativa em um ativo de informação coberto por esta política;

- Criação de novos ativos de informação relevantes a esta política;
- A cada 12 meses a partir da homologação desta política.

Versão	Data	Redator	Descrição das mudanças
03	22/01/2025	Comitê Operacional de Segurança da Informação	Inclusão do item 4.11 GESTÃO DE RISCOS DE FORNECEDORES; Atualização do item 6. INCIDENTES E MEDIDAS DISCIPLINARES; Revisão dos demais itens da política.
02	22/05/2023	Comitê Operacional de Segurança da Informação	Item 2 - Documentos de Referência; Item 6 - Incidentes e Medidas Disciplinares.