FIESC
CIESC
SESI
SENAI
IEL

FIESC

Federação das Indústrias do Estado de Santa Catarina

INDÚSTRIA FORTE É DESENVOLVIMENTO

Política de Segurança da Informação para Fornecedores

Julho/2019

Florianópolis/SC

Versão 1.0

SUMÁRIO

1. ASPECTOS GERAIS

Os aspectos gerais apresentam informações sobre o documento, tais como seus objetivos, revisões, autores, entre outras informações. Seguem abaixo os tópicos relacionados com os aspectos gerais.

1.1. Objetivos

O objetivo principal 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 contempla a definição de responsabilidade sobre as ações de fornecedores e ações disciplinares relacionadas.

1.2. 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 de Operacional de Segurança da Informação.

1.3. Divulgação e Distribuição

Esta política de segurança da informação para fornecedores deve ser parte integrante do contrato de prestação de serviço de todos os fornecedores do Sistema FIESC.

No ato da assinatura do contrato de prestação de serviço o fornecedor assume total conhecimento e concordância com as diretrizes expostas neste documento.

1.4. Versão e Revisão

Esta política encontra-se na versão 1.0, aprovada em 16 de julho de 2019 pelo Comitê Operacional de Segurança da Informação.

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.

2. DIRETRIZES DE SEGURANÇA

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

2.1. Propriedade Intelectual

I. O fornecedor é responsável por garantir a conformidade legal de todo e qualquer sistema ou conteúdo utilizado durante a realização de seu serviço;

II. O fornecedor é responsável pela propriedade intelectual do conteúdo dos equipamentos que trouxer para dentro das dependências do Sistema FIESC;

III. O fornecedor é responsável por garantir que os softwares por ele instalados não ferem qualquer tipo de lei de direitos autorais.

2.2. Acesso à Internet

I. 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;

II. O Sistema FIESC se reserva o direito de monitorar o acesso à internet do fornecedor a fim de para garantir o uso adequado;

III. O Sistema FIESC se reserva o direito de bloquear os sites que considerar inadequados para a empresa, sem prévio aviso;

IV. 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.

2.3. Computação Móvel

I. O Sistema FIESC reserva-se no direito de realizar auditoria nos equipamentos do fornecedor, antes de autorizar o uso dentro da instituição;

II. O fornecedor se compromete inteiramente pela segurança dos dados de seus equipamentos dentro das dependências do Sistema FIESC;

III. 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 possa prejudicar a rede interna do Sistema FIESC.

2.4. E-Mails

I. 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;

II. 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;

III. Nas dependências do Sistema FIESC o fornecedor deve ler e enviar e-mails apenas relacionados com seu trabalho;

IV. 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;

2.5. Manuseio Lógico de Informações

I. 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;

II. O fornecedor se compromete com a total confidencialidade, integridade e disponibilidade das informações do Sistema FIESC que lhe forem concedidas;

III. A divulgação interna das informações do Sistema FIESC dentro da empresa do fornecedor deve ser formalmente informado alinhada entre as partes;

IV. O fornecedor se compromete a não transmitir informações do Sistema FIESC por canais de comunicação não seguros, que possam ocasionar vazamento destas informações;

V. 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);

VI. 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.

2.6. Armazenamento Lógico de Informações

I. 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;

II. 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;

III. O fornecedor também se compromete com a garantia de que as informações do Sistema FIESC não serão adulteradas durante o armazenamento em qualquer tipo de mídia sob sua responsabilidade.

2.7. Acesso à Rede Interna (local ou remoto)

I. O fornecedor somente poderá acessar a rede interna após autorização formal e mediante autenticação individual na rede do Sistema FIESC;

II. O acesso do fornecedor à rede interna poderá ser monitorado pelo setor de Tecnologia da Informação da FIESC quando este julgar necessário;

III. 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;

IV. Os acessos remotos de todos os fornecedores devem ser criados e autorizados pela equipe de Tecnologia da Informação da FIESC.

2.8. Uso de Senhas

I. O fornecedor não deve solicitar, aceitar ou utilizar senha de acesso dos colaboradores do Sistema FIESC em nenhum caso;

II. Toda senha utilizada pelo fornecedor deve ter sido criada especificamente para este fim e identifica-lo de modo inequívoco;

III. A FIESC é responsável por realizar a inativação da senha do fornecedor. Caso o fornecedor identifique que a credencial ainda está ativa, após finalização de contrato, este deve solicitar obrigatoriamente a sua desativação;

IV. 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;

V. O fornecedor é responsável pela segurança das senhas que lhe são entregues e deve comunicar imediatamente ao Sistema FIESC a sua perda ou vazamento.

2.9. Colaboradores do Fornecedor

I. O fornecedor deve garantir que seus colaboradores alocados para a realização de determinado serviço possuem a formação e qualificação necessária para tal;

II. O fornecedor deve informar ao Sistema FIESC o nome, formação e tempo de serviço de seus colaboradores quando for solicitado;

III. 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;

IV. 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;

V. O fornecedor deve comunicar imediatamente qualquer mudança na lista de seus colaboradores autorizados a prestar o serviço interno ao Sistema FIESC;

VI. Todos os colaboradores do fornecedor que prestam serviço ao Sistema FIESC assumem total conhecimento e concordância com o conteúdo deste documento.

2.10. Segurança Física

I. O fornecedor é responsável pela informação física concedida a ele pelo Sistema FIESC, devendo assegurar a confidencialidade, integridade e disponibilidade destas quando estiverem em seu poder;

II. O fornecedor é responsável pela devolução ao Sistema FIESC ou pelo descarte adequado das informações físicas quando estas não forem mais necessários ou ao final de seu serviço;

III. O fornecedor se compromete a acessar as dependências físicas do Sistema FIESC somente quando devidamente autorizado e acompanhado por um colaborador;

IV. O fornecedor não aceitará receber para si qualquer tipo de meio de acesso físico às dependências do Sistema FIESC (ex. senhas de alarmes, senhas de controle de acesso, chaves das portas, entre outros);

V. Para a retirada de equipamentos do Sistema FIESC, por qualquer motivo, o fornecedor deverá receber autorização formalizada por um dos colaboradores da organização, podendo esta ser por e-mail ou registro de chamado interno.

3. INCIDENTES E MEDIDAS DISCIPLINARES

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.

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.