POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA SEGURANÇA DA INFORMAÇÃO

1. Atribuições

A Política de Segurança Cibernética e da Informação tem como objetivo atender a resolução nº 4.658 do Banco Central do Brasil, considerando os princípios estabelecidos pelo parágrafo primeiro do Artigo Segundo da referida norma, e estabelecer os princípios, conceitos, valores e práticas que devem ser adotados pelos administradores, empregados, prestadores de serviços ou outros colaboradores da C.E.C.M.E.A.P. da CEEE e Eletricitários do Rio Grande do Sul-CRECE, inscrita no CNPJ/MF sob nº 92.825.397/0001-79 com sede a Avenida Princesa Isabel, nº 636/707-708-Bairro Santana-Porto Alegre-RS-CEP 90.620-000 na sua atuação interna e com o mercado.

A CRECE incorpora em seus valores corporativos a convicção de que o exercício de suas atividades e a expansão de seus negócios devem se basear em princípios éticos, os quais devem ser compartilhados por todos os seus operadores. Na constante busca do seu desenvolvimento e da satisfação dos associados, a CRECE prima pela transparência e cumprimento da legislação aplicável às atividades de administração e gestão de recursos de terceiros.

A publicação desta Política representa o compromisso de todos os que trabalham na CRECE com os valores e as práticas fundamentadas na integridade, confiança e lealdade. Portanto, a constante busca do desenvolvimento da CRECE e a defesa dos interesses dos associados estarão sempre pautadas nas diretrizes aqui expostas.

A Diretoria Executiva é responsável pela implementação de um sistema de supervisão que demonstre que os controles de segurança da informação estejam sendo devidamente executados e alinhados com os níveis adotados pela CRECE, tendo em vista a natureza e a baixa complexidade de produtos e serviços.

A Diretoria Executiva está apta a detectar eventuais desvios de conduta que possam colocar em risco: Associados/Investidores, colaboradores e a CRECE.

2. Importância da Segurança da Informação

Os pilares da segurança da informação nos dão subsídios para proteger as informações da CRECE. Portanto, quando mencionamos "segurança da informação" estamos falando de proteções voltadas às informações impressas, verbais e sistêmicas, bem como nos controles de acesso, vigilância, contingência de desastres naturais, contratações, cláusulas e demais questões que juntas formam uma proteção adequada para qualquer empresa.

O que é Política de Segurança da Informação?

Política de Segurança é um conjunto de diretrizes que definem formalmente as regras, os direitos e deveres de todos os colaboradores, visando à proteção adequada dos que compartilham a informação. Ela também define as atribuições de cada um dos colaboradores, em relação à segurança dos recursos com os quais trabalham, além disso, deve prever o que pode ser feito e o que será considerado inaceitável.

A informação é só o que está nos sistemas?

Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para a organização ou pessoa. Além do que, está armazenado nos computadores a informação, também impressa em relatórios, documentos, arquivos físicos, ou até mesmo repassada através de conversas nos ambientes interno e externo.

Por isso, todo cuidado é pouco na hora de imprimir relatórios, jogar papéis no lixo, deixar documentos em cima da mesa, conversar sobre a empresa em locais públicos ou com pessoas estranhas ao nosso meio.

3. Princípios da Segurança da Informação

Os princípios básicos da segurança da informação são: confidencialidade, integridade, disponibilidade e acesso controlado. Outras características são: irrefutabilidade, autenticação e o controle de acesso. Os benefícios são evidentes ao reduzir os riscos com vazamentos, fraudes, erros, uso indevido, sabotagens, roubo de informações e diversos outros problemas que possam comprometer esses princípios básicos.

– **Confidencialidade:** Proteção da informação compartilhada contra acessos não autorizados. A Ameaça à segurança acontece quando há uma quebra de sigilo de uma determinada informação, permitindo que sejam expostos, voluntaria ou involuntariamente, dados restritos, e que deveriam ser acessíveis apenas por um determinado grupo de usuários.

– **Integridade:** Garantia da veracidade da informação, pois a mesma não deve ser alterada enquanto está sendo transferida ou armazenada.

A Ameaça à segurança acontece quando uma determinada informação fica exposta ao manuseio por uma pessoa não autorizada, que efetue alterações não aprovadas e sem o controle do proprietário (corporativo ou privado) da informação.

– **Disponibilidade:** Prevenção contra as interrupções das operações da CRECE como um todo. Os métodos para garantir a disponibilidade incluem um controle físico e técnico das funções dos sistemas de dados, assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópias de segurança.

– **Acesso controlado:** O acesso dos usuários à informação é restrito e controlado, significando que só as pessoas que devem ter acesso a uma determinada informação, tenham esse acesso.

A Ameaça à segurança acontece quando há, por culpa ou dolo, quebra da confidencialidade das senhas de acesso à rede, motivo pelo qual abaixo são elencadas as regras

às quais a CRECE deve observar:

Regras do uso dos Recursos de Tecnologia

Regras para o Uso do Computador

a. Propriedade do computador;

b. Disponibilização e uso;

c. Programas utilizados no computador;

d. Verificação dos equipamentos e acessos;

e. Responsabilidades do usuário;

f. Outras proteções;

g. Compromisso.

Regras para o uso da Internet

a. Responsabilidade e forma de uso;

b. Uso de serviço de mensagem instantânea;

c. Uso de serviço de rádio, TV, download de vídeos, filmes e músicas;

d. Bloqueio de endereços de Internet;

e. Uso de Correio Eletrônico particular.

Regras para o Uso do Correio Eletrônico (E-mail)

a. Endereço eletrônico do usuário;

b. Criação, manutenção e exclusão do endereço de correio eletrônico;

c. Endereço eletrônico de programas ou de comunicação corporativa;

d. Acesso à distância;

e. Propriedades do endereço;

f. **Responsabilidades e forma de uso;**

g. **Cópias de segurança.**

Regras para o uso de Telefone

a. **Número do telefone do usuário;**

b. **Propriedades do número do telefone;**

c. **Responsabilidades e forma de uso**

Linhas Gerais de Comportamento Seguro

No ambiente externo, será melhor ficar atento

Cuidado com o lixo que você produz

Gestão de mudanças

Revisões de acesso

Dúvidas

Quaisquer dúvidas relacionadas com a presente política devem ser esclarecidas com a Diretoria Executiva da CRECE.

Porto Alegre, 06 de abril de 2020.

Antônio Carlos Oleques da Rocha
Presidente

Paulo Roberto Gonçalves Fernandes
Vice-Presidente