FUNDAÇÃO CEEE

Política de Segurança e Uso dos Recursos de Tecnologia da Informação

Fundação CEEE

Este documento descreve o que é esperado de você como usuário dos recursos de computação e comunicação em rede da Fundação CEEE, não pretendendo, ser uma lista completa de todas as atividades permitidas/proibidas, mas sim uma base para o uso ético dos serviços em tecnologia da informação disponíveis.

*Devido ao conteúdo deste documento o mesmo é classificado como **confidencial**, não estando autorizada sua divulgação ou movimentação além das dependências da Fundação CEEE, exceto com autorização expressa da Divisão de Informática.*

Sumário

1 Introdução

Este documento define as diretrizes básicas de Segurança da Informação da Fundação CEEE, visando preservar a integridade, confidencialidade e disponibilidade das informações. Descreve a conduta considerada adequada para o manuseio, controle e proteção das informações contra destruição, modificação, divulgação indevida e acessos não autorizados, sejam acidental ou intencionalmente. Fornece, também, um conjunto de normas e procedimentos e estabelece punições relativas ao tema.

2 Estrutura do documento

Com o objetivo de facilitar o manuseio e atualização deste documento, o mesmo está estruturado da seguinte forma:

- → **Diretrizes da Política de Segurança:** Informa os princípios básicos da política interna de segurança.
- → **Carta da Diretoria:** Contém a visão da Diretoria Executiva referente ao assunto segurança, bem como suas expectativas quanto à implantação da política.
- → **Normas de segurança:**
  - ✓ **Credenciais de acesso:** Descreve as necessidades e recomendações quanto ao manuseio de usuários e senhas para acesso aos recursos.
  - ✓ **Utilização do recurso internet**: Descreve o que é esperado em termos de utilização deste recurso.
  - ✓ **Utilização do sistema de correio eletrônico:** Contém as regras básicas de envio, recebimento e manuseio de mensagens dentro da organização.
  - ✓ **Estações de trabalho e demais recursos:** Contém recomendações quanto à utilização dos softwares corporativos, do uso dos computadores e demais periféricos.
- → **Sanções**: Descreve as punições previstas.
- → **Termo de compromisso:** Formaliza o entendimento, na íntegra, deste documento, por parte do usuário.

3 Diretrizes da Política

A Política de Segurança atinge todas as pessoas que, de uma forma ou de outra, trocam informações com a Fundação CEEE, tendo como diretrizes básicas:

- Somente permitir o uso de recursos homologados e autorizados pela entidade quando identificados de forma individual, protegidos, inventariados, com documentação atualizada, e estando de acordo com as cláusulas contratuais e a legislação em vigor;
- Aplicar as medidas de proteção de forma compatível com a avaliação do risco para o negócio da Fundação CEEE;
- A disponibilidade de recursos, o uso, o acesso e a proteção das informações devem preservar a continuidade e a competitividade do negócio da organização;
- Garantir a integridade das informações, sejam elas de domínio público ou privado;
- Garantir a disponibilidade dos serviços de informação oferecidos, internamente e para o público em geral;
- Garantir a manutenção e atualização da tecnologia utilizada em relação a seus dispositivos de segurança;
- Estabelecer padrões de tratamento da informação;
- Divulgar a Política com o objetivo de estimular a conscientização das pessoas em relação à segurança da informação;
- Reavaliar constantemente a segurança dos sistemas.

4 Carta da Diretoria

A tecnologia da informação é uma das principais ferramentas utilizadas pelas empresas, para garantir continuidade e competitividade no mercado; ao mesmo tempo, a inexistência de regras tornaram os sistemas informatizados uma presa fácil aos processos invasivos.

Com este cenário, nossa Entidade vem preparando-se na melhor forma tecnológica e de capacitação, para preservação dos seus interesses, onde se insere uma política de uso correto dos recursos de informática e uma postura clara do que espera de seu quadro de empregados, na proteção e segurança de suas informações.

Neste contexto, adicionamos em nossas instruções Normativas, a adoção de um conjunto de regramentos que denominamos ***Política de Segurança e Uso dos Recursos de Tecnologia da Informação***, como uma das peças fundamentais de nosso Planejamento Estratégico de Tecnologia da Informação-PETI, que valoriza e preserva os objetivos expostos, definindo responsabilidades no uso das ferramentas, sem cerceamento, mas no estrito limite da ética e dos costumes.

A busca constante de padrões mais elevados e segurança deve ser um compromisso mútuo e de todos os usuários, porque, mesmo de forma inadvertida, cada um poderá transformar-se em porta de *entradas* indevidas; por isto, contamos com o apoio de todos para observação das recomendações técnicas constantes do documento.

Para ser uma empresa com a Visão: "**Ter o reconhecimento como empresa referência de Previdência Privada no Estado do Rio Grande do Sul e conquistar 4500 novos participantes até o ano de 2010",** é necessário estabelecer os mais elevados padrões de segurança, com o mesmo compromisso mútuo e disposição, que definimos nossa Visão de Empresa. Por isso, investimos no engajamento de todos os colaboradores, para continuar fazendo da FUNDAÇÃO CEEE uma empresa referência frente aos novos desafios do mercado.

A DIRETORIA DA FUNDAÇÃO CEEE DEFINE QUE:

1. Na data de divulgação desta política entram em vigor as Normas de Segurança da Informação, estabelecidas para a Fundação CEEE.
2. As Diretorias e Gerências devem divulgar as Normas de Segurança da Informação.
3. As ações executadas com uma determinada senha e identificação de acesso serão de responsabilidade do seu portador, devendo o mesmo manter a confidencialidade destes dados, pois são sua identificação formal junto aos sistemas da Fundação CEEE.
4. As Normas de Segurança da Informação passam a integrar o conjunto de Normas da Fundação CEEE, ficando todo e qualquer empregado obrigado a conhecê-las e cumprí-las.
5. Através de Resolução de Diretoria Executiva, reserva-se o direito de alterar os termos e condições mencionados nesta política a qualquer momento, da forma que melhor entender, devidamente divulgada.
6. Reserva-se o direito de recorrer a todas as ações judiciais cabíveis e em compensação por qualquer violação desses termos e condições.
7. Avaliará constantemente os procedimentos de segurança e privacidade disponibilizados aos colaboradores com o intuito de garantir a integridade das informações prestadas.

Porto Alegre, 04 de outubro de 2005.

Diretoria Executiva

5 Normas

As normas estabelecem os pilares para a implementação de procedimentos que irão concretizar as Diretrizes aqui estabelecidas. As mesmas estão divididas em quatro itens para facilitar seu manuseio e entendimento.

As normas definidas neste documento estão em conformidade com a norma brasileira NBR ISO/IEC-17799, que especifica aspectos de um programa eficaz de proteção da informação, apropriado às necessidades da Fundação CEEE. A Proteção na NBR ISO/IEC-17799 tem por base assegurar a integridade, a disponibilidade e a confiabilidade dos recursos incorporados da informação.

5.1 Credenciais de acesso

As credenciais de acesso (ou senhas) fornecem um meio de validação da identidade. Estabelecem os direitos de acesso para os recursos ou serviços de processamento da informação aos quais o empregado tem direito. As normas e recomendações, abaixo descritas, devem ser seguidas na criação e manutenção de senhas, conforme segue:

a) Alterar senhas temporárias no primeiro acesso à rede de informações;

b) Manter a confidencialidade das senhas, não compartilhando credenciais (senhas) individuais, que são de uso pessoal, sigiloso e intransferível;

c) Evitar o registro das senhas em papel,

d) Evitar o uso da opção "gravar senha automaticamente" quando do acesso à intranet ou internet;

e) Alterar a senha sempre que existir qualquer indicação de possível comprometimento do sistema ou da própria senha;

f) Usar senha de qualidade, com um tamanho mínimo de 8 (oito) caracteres, que sejam:

1) Fáceis de lembrar;

2) Não baseadas em formas que outras pessoas possam facilmente adivinhar ou obter a partir de informações pessoais, por exemplo: nome, nome da esposa, filhos, números telefônicos, datas de nascimento, placa de veículos, nome de ruas, etc.;

3) É recomendado que a senha contenha, pelo menos, dois (2) caracteres numéricos, um (1) caracter especial e cinco (5) caracteres alfabéticos, evitando o uso de caracteres idênticos consecutivos ou de grupos de caracteres somente numéricos ou alfabéticos.

4) Recomenda-se que a senha contenha caracteres no mínimo de três (3) classes das quatro (4) listadas abaixo:

- Letras minúsculas : a,b,c,d.....z
- Letras maiúsculas : A,B,C,D...Z
- Números : 0,1,2,3,...9
- Caracteres especiais : #,$,&,%

Exemplos de senhas fortes:

MFT10anos (Minha Filha Tem 10 anos)

Cafe+Leitepra2 (Café mais leite prá dois)

1Ondacom10pes (Uma onda com 10 pés)

1$Vale3Reais (Um dólar vale 3 reais)

g) Alterar a senha conforme o sistema de Gerenciamento de Senhas, (contas privilegiadas devem ser alteradas com maior freqüência do que as senhas normais. ex. Administradores de rede e banco de dados) evitar a reutilização de senhas antigas;

h) A descoberta da senha pessoal por outras pessoas, usuários ou não, deve ser imediatamente comunicada à gerência de segurança e a senha deve ser rapidamente trocada;

i) O sistema permitirá no máximo três (3) tentativas de acesso ao sistema sem sucesso, por erro no fornecimento da senha. Após a terceira tentativa a conta do usuário será automaticamente bloqueada e a ocorrência será registrada no log de segurança;

j) A senha terá validade de 120 dias e o usuário terá que alterar sua senha sempre que o sistema de Gerenciamento de Senhas informá-lo que a senha atual expirou;

k) Não incluir senhas em processos automáticos de acesso ao sistema, por exemplo, armazenadas em macros ou teclas de função;

A norma de senhas, descrita acima, está em conformidade com a RFC 1244

(Request For Comments) – Item 4.3 Password Management Procedures, página 57. (http://www.ietf.org/rfc.html)

5.2 Utilização do recurso Internet

A Internet é um recurso poderoso que dá aos usuários acesso a uma variada gama de conteúdos e informações de domínio público. Atualmente, nesta mesma proporção, existem riscos associados, como por exemplo, os riscos de segurança. Com o objetivo de minimizar tais riscos e otimizar a utilização desse recurso ressalta-se que:

a) A utilização da Internet é um privilégio e não um direito, ou seja, poderá ser recusado a qualquer momento devido ao comportamento abusivo;

b) A Fundação CEEE possui softwares e sistemas implementados que monitoram e gravam todos os usos da Internet através da rede e das estações de trabalho da entidade;

c) É expressamente proibida a utilização da Internet para fins ilegais ou atividades consideradas ilegais;

d) Sendo do interesse da entidade que os seus empregados estejam bem informados, o uso de sites de notícias ou de serviços de notícias é aceitável, desde que o seu uso não comprometa o bom funcionamento da banda da rede, nem prejudique o bom andamento dos trabalhos individuais e/ou coletivos da organização;

e) Os empregados poderão utilizar a internet para atividades não relacionadas ao negócio durante o horário de almoço, ou fora do expediente, desde que dentro das regras de uso definidas nesta política, com a devida ciência de sua gerência;

f) Sites que hospedam qualquer tipo de material impróprio não poderão ser acessados, como por exemplo:

1) Pornografia;
2) Erotismo, book de mulheres ou de homens;
3) Sites que contenham material racista, terrorista, discriminatórios, jogos on-line, jogos off-line e hackers;
4) Sites de violência, ilegais ou de drogas
5) Sites que ofereçam conteúdos que afetam a banda de navegação, como áudio e vídeo
6) Outros sites poderão ter o acesso negado, caso haja a necessidade para tal.

g) Jogos, sejam eles de azar ou não, são expressamente proibidos via Internet;

h) Nenhum empregado pode utilizar os recursos da entidade para deliberadamente propagar qualquer tipo de vírus, worms, ou programas

de controle de outros computadores (Cavalos de tróia, ex: Back Oriffice, Netbus, etc.);

i) É expressamente proibido executar ou baixar (Downloads) arquivos com extensões consideradas inadequadas (mp3 e arquivos de sons, exe, dat, sys, bat) e outros tipos de arquivos executáveis;

j) É expressamente proibido ouvir rádio ou assistir vídeos via Internet.

k) NUNCA registrar identificação relativa a contas bancárias que pertençam à Fundação CEEE em nenhum site da Internet;

l) A transferência (Downloads) de programas de entretenimento, jogos, filmes e softwares protegidos por direitos autorais, não pode ser efetuada através da conexão Internet da entidade. Da mesma forma, o uso de jogos contra oponentes na Internet é proibido;

m) A Fundação CEEE não se responsabilizará por nenhuma transação feita via Internet, seja ela financeira ou não, iniciadas de dentro de sua rede corporativa. A responsabilidade é inteira do Site que está sendo acessado;

n) O acesso aos sites de conversação online, como por exemplo, chat, é proibido;

o) O MSN Messenger é a ferramenta de conversação que poderá ser utilizada dentro do ambiente da Fundação CEEE, observando que o uso deverá ser moderado, com conversações objetivas, e priorizando os casos que tenham relação com a atividade da organização. Arquivos anexos não devem ser transferidos por representarem riscos à segurança;

p) Qualquer outra ferramenta de conversação, como AOL Messenger, ICQ, etc, não tem seu uso nem instalação autorizado;

q) Acesso aos sites de comunidades virtuais, por exemplo, ORKUT é proibido;

r) Todos os conteúdos (sites e tipos de arquivos) que tiverem relação com a atividade da entidade serão liberados;

s) Os empregados que divulgarem informações confidenciais da entidade (ex.: em grupos de discussão ou bate-papo), não importando se a divulgação foi deliberada ou inadvertida, poderão sofrer as penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei;

t) Para efetuar a navegação na Internet não poderá ser utilizada nenhuma outra conexão a não ser aquela cedida pela Fundação CEEE;

u) A entidade instalou uma série de softwares e hardwares para proteger a rede interna e garantir a integridade dos dados e programas, incluindo um Firewall*, que é a primeira, mas não a única barreira entre a rede interna e a Internet. Qualquer tentativa de alteração dos parâmetros do Firewall, por qualquer empregado, sem ser devidamente credenciado e autorizado para tal, resultará nas penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei;

*Firewall - Sistema que filtra os acessos feitos da empresa para a internet e da internet para a empresa, controla o acesso e é responsável por interligar, de forma segura, a rede de informações da Fundação CEEE com a rede Internet, garantindo o controle, verificação e o log (auditoria) dos pacotes que passam entre elas. Seu nome foi originado das paredes corta-fogo, existentes para impedir a passagem do fogo em prédios.

5.3 Utilização do sistema de correio eletrônico corporativo

O serviço de Correio Eletrônico, implementado na organização, permite a troca de mensagens eletrônicas para maior agilidade aos processos e auxílio ao desenvolvimento das tarefas dos empregados.

Da utilização do Correio Eletrônico:

a) A Divisão de Informática deve promover junto aos seus usuários o incentivo ao uso do serviço de correio eletrônico no desempenho de suas atividades funcionais, objetivando a racionalização do trabalho e o aumento da produtividade por meio da facilitação da troca de informações e do intercâmbio de idéias;

b) O usuário deve eliminar periodicamente as mensagens contidas nas caixas postais;

c) Não é permitido o acesso de terceiros ao correio eletrônico através de sua senha;

d) O usuário deve estar alerta em relação a qualquer resposta a um e-mail que se supõe não ter enviado;

e) O usuário deve estar alerta para mensagens que, apesar de virem do endereço de alguém conhecido, tenham um conteúdo discrepante com a personalidade da pessoa que você acredita que o enviou;

f) Cabe à Divisão de Recursos Humanos comunicar à Divisão de Informática o desligamento de empregados, terceirizados, temporários e estagiários para a exclusão definitiva da caixa postal em, no máximo, dez (10) dias após o desligamento;

g) É permitida ao usuário a participação em Listas de Discussão com assuntos relacionados exclusivamente ao interesse do trabalho, tanto profissionais quanto educativos;

h) O acesso aos provedores de e-mail pessoais está autorizado, desde que observado o uso moderado, que não comprometa a produtividade da entidade nem gere riscos à segurança interna da rede;

i) O empregado pode utilizar o correio eletrônico da entidade com fins não profissionais, tanto de uma maneira interna como externa, desde que de forma não abusiva e com a condição de que não interfira em suas atividades profissionais (uso social do e-mail);

j) Convém que a confirmação de recebimento seja utilizada para mensagens consideradas importantes pelo usuário, como envio de documentos, envio de senhas, etc.;

k) O usuário deve notificar à Divisão de Informática sobre quaisquer fatos ou ocorrências suspeitas com seu e-mail ou mensagens de origem desconhecida;

l) A criação de novas caixas postais ocorrerá quando da admissão de um novo colaborador, devidamente comunicada pela DRH, ou via solicitação da chefia imediata ou superior;

m) As mensagens enviadas e recebidas pelo usuário, inclusive quanto ao seu conteúdo, estarão sujeitas à monitoramento eletrônico, garantido o princípio da confidencialidade.

Ficam vedados as seguintes formas de utilização:

a) Qualquer uso com propósitos ilegais;

b) Transmissão de tipos ou quantidades de dados que comprometam os serviços e/ou equipamentos na rede da Fundação CEEE;

c) O repasse de correntes e formas similares de comunicação; quaisquer mensagens não solicitadas (*spam*) e mensagens em massa, comercial ou não, e grande quantidade de mensagens idênticas ao mesmo destinatário;

d) O uso do e-mail quando a Divisão de Informática informar aos usuários que a entidade passa por problemas de segurança emergenciais, como por exemplo: vírus, manutenções preventivas, etc.;

e) Transmissão ou divulgação de ameaças, pornografia, material racista, material político-partidário, material ofensivo ou qualquer outro que viole a legislação em vigor no país ou quaisquer outras normas internas da Fundação CEEE;

f) Difamação de qualquer pessoa, empregado (a) ou não da Fundação CEEE;

g) Fica estritamente proibido abrir anexos com extensões EXE, VBS, BAT, COM ou outros anexos com códigos executáveis. No caso de recebimento, entrar em contato com a Divisão de Informática para devidas providências;

h) De forma alguma poderá ser configurado outro SMTP*(Servidor de mensagens) que não seja o de uso corporativo da Fundação CEEE dentro da organização;

Por ser um recurso da Fundação CEEE, o correio eletrônico poderá ser auditado no caso de motivos justificáveis. Para tanto, será necessária autorização por escrito por parte do superior imediato.

A inobservância dos dispositivos acima, implicará ao empregado a aplicação de sanções definidas nesta política.

*SMTP – Simple Mail Transfer Protocol – Protocolo de entrega de e-mails baseado na arquitetura de rede em que todas as máquinas estão ligadas.

5.4 Estações de trabalho e demais recursos

Para que os usuários e prestadores de serviço tenham uma boa segurança na manipulação das informações da Fundação CEEE, é necessário observar alguns procedimentos para a proteção de equipamentos não monitorados e de domínio da entidade, bem como definir as responsabilidades para implementação de tais proteções.

Para que a estação de trabalho tenha uma segurança adequada devem ser observados os seguintes procedimentos:

a) Ao ausentar-se temporariamente o empregado deve encerrar as sessões ativas, bloqueando sua estação de trabalho;

b) Não são permitidas modificações nas configurações do Sistema Operacional, exemplo: configuração de rede, configuração do navegador etc. Este tipo de operação deve ser executada apenas por pessoal autorizado pela Divisão de Informática;

c) Toda e qualquer instalação deverá ser previamente autorizada pela Divisão de Informática, não podendo ser instalado qualquer tipo de aplicativo como jogos, softwares de bancos, utilitários, etc.;

d) Informações de propriedade da Fundação CEEE devem ser copiadas (backup periódico) para a área de segurança da rede;

e) Nenhum componente físico da estação de trabalho poderá ser retirado ou acrescentado sem a presença e permissão formal de um técnico da Divisão de Informática;

f) Não é permitido submeter a estação de trabalho a qualquer dano físico ou lógico;

g) Não é permitida a prática de jogos em horário de trabalho;

h) Não deixar qualquer tipo de material que contenha magnetismo (como imãs) sobre os equipamentos de informática ou da estação de trabalho;

i) Não alimentar-se próximo aos equipamentos de TI;

j) Recomenda-se cautela quanto ao uso dos dispositivos de entrada e saída, como CDs, pen Drives, dvds, disquetes, etc.;

k) Toda e qualquer operação executada com a identificação do usuário será de responsabilidade do mesmo.

6 Sanções

Esta Política de Segurança faz parte das regras internas de conduta da Fundação CEEE. Assim, seus empregados ficam sujeitos às punições já definidas em lei, e de acordo com as formas de contratação existentes.

No caso dos prestadores de serviços contratados, as punições são estabelecidas pelo próprio contrato e, no caso de contratação direta, a forma é definida pela CLT, podendo variar entre mera advertência, suspensão disciplinar ou despedida por justa causa, sem prejuízo de responsabilização civil e penal, inclusive reparação de danos, tanto morais quanto materiais.

No caso de desrespeito às normas da Política de Segurança o infrator ficará sujeito à aplicação das normas referidas no artigo 482, alíneas a, b, c, e, g, h e/ou l da CLT:

a) ato de improbidade; como, por exemplo, furtar programa desenvolvido pela empresa ou desviar recursos para conta corrente do autor do delito;

b) incontinência de conduta; como, por exemplo, divulgar no site da empresa ou enviar a outros empregados fotos de natureza sexual; ou mau procedimento - envio de *spams* (mensagens não solicitadas);

c) negociação habitual por conta própria ou alheia sem permissão do empregador, e quando constituir ato de concorrência à empresa para a qual trabalha o empregado, ou for prejudicial ao serviço; como, por exemplo, quando o empregado se utilizar dos produtos da empresa, bem como de seu site para venda de produtos de outra empresa;

e) desídia no desempenho das respectivas funções; como, por exemplo, no caso do empregado permanecer horas navegando na internet e prejudicando seus serviços além do prejuízo material para empresa;

g) violação de segredo da empresa; como, por exemplo, quando o empregado utilizar os meios eletrônicos para violar documentos secretos que não podem ser divulgados sob pena de causar prejuízos ao empregador;

h) ato de indisciplina; como, por exemplo, quando o empregado utilizar recursos de informática para fins pessoais mesmo sabendo que existe no regulamento da empresa norma que o proíbe;

l) prática constante de jogos de azar; como, por exemplo, jogo de cartas disponível em programa de computador e praticado em horário de expediente pelo empregado.

7 Termo de compromisso

Eu, , declaro que tomei ciência e que recebi, nesta data, da Fundação CEEE de Seguridade Social a Política de Segurança da Informação, com suas respectivas normas de utilização, referentes a Credenciais de Acesso, Utilização do Recurso Internet, Utilização do Sistema de Correio Eletrônico Corporativo e Estações de Trabalho e demais Recursos, da qual tomei pleno conhecimento, comprometendo-me a observar rigorosa e integralmente as normas ali estabelecidas.

Declaro, também, estar plenamente ciente de que, caso venha a violar qualquer dos itens da norma acima mencionada, estarei sujeito a medidas de ordem disciplinar, previstas internamente com base no artigo 482 e seus incisos da C.L.T.(Consolidação das Leis do Trabalho).

Porto Alegre, de de 2005.

assinatura empregado.

Nome do empregado:

Registro nº:

APROVAÇÃO		
Nome	**Função**	**Rubrica**
Dalmiro Schaf Lopes	Presidente	
Ivan Giordani	Diretor Financeiro	
Lilian Arenhart da Veiga Lima	Diretora de Seguridade	
Manuel Valente	Diretor Administrativo	

CONTROLE DE ALTERAÇÕES	
Data	**Histórico**
01/11/2005	Emissão do Documento