Política de Segurança da Informação

Versão 04

Sumário

1. OBJETIVO

Definir as diretrizes que nortearão as normas e padrões que tratam da proteção da informação, abrangendo sua geração, utilização, armazenamento, distribuição, confidencialidade, disponibilidade e integridade, em especial, mas não se limitando ao meio em que ela esteja contida.

1.1. Por princípio, a segurança da informação deve abranger aspectos básicos, destacados a seguir:

Geração/Produção: criação de bens e de serviços a partir do tratamento de dados.
Utilização: ato ou efeito do aprovitamento de dados.
Armazenamento: ação ou resultado de manter ou conservar em inventario.
Distribuição: ato ou efeito de dispor de dados.
Confidencialidade: somente pessoas devidamente autorizadas pela empresa devem ter acesso à informação.
Disponibilidade: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou demandado.
Integridade: somente alterações, supressões e adições autorizadas pela empresa devem ser realizadas nas informações.

2. RESPONSABILIDADE

Esta Política é de responsabilidade da Área de Tecnologia do CIEE-RS. Quaisquer mudanças nesta Política devem ser aprovadas pela Área de Tecnologia do CIEE-RS. A alta gestão tem o comprometimento com a melhoria contínua dos procedimentos relacionados com a segurança da informação.

3. DATA DE ENTRADA EM VIGOR

Esta Política entrará em vigor imediatamente a partir da sua publicação no site do CIEE-RS no *link* http://cieers.org.br/institucional/sobreCiee#/seguranca

4. PÚBLICO ALVO

Esta Política se aplica a todos os usuários que utilizam as informações do CIEE-RS.

5. DIRETRIZES GERAIS

A. Tratamento da Informação

A informação sob custódia do CIEE-RS, mesmo que pertencente a clientes ou fornecedores, deve ser protegida contra o acesso de pessoas não autorizadas. A geração, utilização, armazenamento, manutenção, distribuição e destruição da informação devem ser feitas de acordo com as necessidades da organização, sendo que estes processos devem estar devidamente documentados. Ao CIEE-RS reserva-se o direito de consultar e analisar informações armazenadas em suas dependências e em seus equipamentos, bem como em malotes, envelopes, arquivos físicos e eletrônicos, geradas ou recebidas com utilização de seus recursos humanos e materiais. Devem ser usados somente recursos autorizados para garantir o compartilhamento seguro da informação quando for necessário.

A informação deve ser armazenada pelo tempo determinado pela instituição ou ter o descarte adequado de documentos de acordo com seu grau de classificação ou legislação vigente, o que for maior, e recuperável quando necessário. O local de armazenamento das informações deve ser apropriado e protegido contra sinistros e acessos de pessoas não autorizadas.

A informação utilizada pela organização é um bem que tem valor. Ela deve ser protegida, cuidada e gerenciada adequadamente, utilizando-se quando necessário e aplicável ao processo de negócio, das melhores técnicas de segurança, tais como chaves de criptografia, sistemas de detecção para as invasões de rede e dispositivos, logins com senhas, duplo fator de autenticação e conformidades regulatórias, com o objetivo de garantir a sua disponibilidade, integridade, confidencialidade e legalidade, independentemente do meio de armazenamento, processamento ou transmissão que esteja sendo utilizado.

B. Acesso à Informação

O uso de redes externas de comunicação (*Internet,* redes privadas, etc.) deve ser controlado através de Servidores de *Firewalls*, Servidores de Acesso à *Internet*, Servidores de *AntiSpam*, ferramentas de Antivírus e políticas de sistemas operacionais que garantam que somente os recursos necessários estejam disponíveis para o trabalho, sem riscos para o ambiente operacional.

O acesso externo aos sistemas da organização, quando realizado pelo pessoal da área de suporte técnico ou por prestadores de serviço, deve ser controlado e restrito aos serviços necessários, mantendo trilhas de utilização e restringindo–se ao mínimo necessário.

A remessa de dados da organização, seja para atender requisitos de negócio, como para viabilizar a resolução de problemas encontrados, deve ser avaliada em função dos riscos e pela adoção de procedimentos que garantam o controle e a integridade dos dados, além da legitimidade do receptor das informações.

C. Sistemas Aplicativos

Sistemas e aplicativos desenvolvidos dentro da organização devem ser documentados e controlados quanto às alterações ou correções feitas, bem como seguir a metodologia “ Privacy by design”, descrita no art. 46 § 2°, em que as medidas de segurança devem ser adotadas desde capatação. Para minimizar o risco de falhas nos sistemas, deve-se fazer um planejamento e preparações prévias para garantir a disponibilidade e capacidade adequada dos recursos. Para novos sistemas os requisitos operacionais devem ser testados antes da sua aceitação e uso.

6. DIRETRIZES ESPECÍFICAS

A. Tratamento da Informação

Devem ser definidas regras claras para proteção da informação contra perda, alteração e acesso por pessoas não autorizadas, seja qual for o meio em que vier a ser armazenada (digital, correspondências, relatórios, manuscritos, etc.). Devem ser claramente definidos os usuários (empresas, áreas, pessoas etc.) das informações, os direitos que cada um tem para acessá-las e os procedimentos para protegê-las do acesso por pessoas não-autorizadas, independentemente da forma como estiver disponível. Toda informação deve ser utilizada apenas para fins profissionais, de interesse exclusivo da organização. Toda informação relevante deve ter pelo menos uma cópia reserva ou outro procedimento eficiente para pronta recuperação em caso de perda. Nenhuma informação deve ser acessada, divulgada ou disponibilizada, sob qualquer pretexto, sem a devida autorização. É proibida a transmissão a terceiros, por qualquer meio, bem como sua divulgação, reprodução, cópia, utilização ou exploração de conhecimentos, dados e informações de propriedade das Instituições, utilizáveis nas atividades das mesmas, sem a prévia e expressa autorização da Gerência responsável, e das quais os funcionários venham a tomar conhecimento durante a relação empregatícia, estendendo-se tal vedação ao período após o término do contrato de trabalho, sem prejuízo das ações de natureza penal aplicáveis ao assunto.

B. Recomendações para o tratamento da informação

A pessoa que receber indevidamente uma informação deve procurar imediatamente o remetente e alertá-lo sobre o equívoco. As informações disponíveis na Internet somente deverão ser acessadas para fins de execução das atividades de interesse exclusivo do CIEE-RS. Toda informação em papel, mídia removível ou qualquer outro meio de armazenamento deve ser destruída após o uso, ou guardada de forma a não estar disponível para pessoas não autorizadas.

Os gestores devem determinar aos usuários as regras de acesso e distribuição das informações e estão cientes que ao distribuir essas atribuições poderão estar sujeitos aos seguintes riscos:

i. *Riscos inerentes às informações:*

- Acesso por pessoas não autorizadas;
- Divulgação indevida;
- Indisponibilidade dos recursos;
- Alteração indevida.
- Erro no cadastro;
- Invasão do banco de dados;
- Descarte Indevido;

ii. *Consequências:*

- Fraudes: Possibilidades de lesarem o próprio CIEE-RS ou terceiros (clientes, fornecedores, etc.);
- Problemas legais: Possibilidades de gerar prejuízos, multas, penalidades ou embaraços às Instituições, Diretores e Funcionários do CIEE-RS, a outras pessoas físicas ou jurídicas;

- Perda de negócio: Possibilidade de não realizar receitas previstas ou gerar perdas nos negócios implantados ou em fase de implantação;
- Prejuízo de imagem do CIEE-RS: Possibilidades de prejudicar a imagem do CIEE-RS ou de seus funcionários;
- Problemas de recuperação: Possibilidades de gerar custos de recuperação de informações perdidas ou danificadas.

Para assegurar que não haja as consequências desses itens mencionados, a informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem e perda não intencional, acidentes e outras ameaças, caso ocorra tais inadequações, essa estará sujeito a penalidades da lei 13.709/2018, lei 12.965/2014 e demais leis em vigencia.

C. Segurança quanto às Pessoas

Este tópico trata da segurança quanto às pessoas e tem como finalidade reduzir os riscos de erros humanos, roubo, fraude ou uso inadequado de informações e recursos do CIEE-RS.

i. *Identificação das pessoas*

Todas pessoas com acesso aos sistemas e informações, pertencentes ou em posse do CIEE-RS, deverão ter uma única identificação (*login*). As exceções deverão ser devidamente documentadas e encaminhadas para análise para a Área de Tecnologia do CIEE-RS.

ii. *Declaração de Responsabilidade*

É um compromisso de responsabilidade direta do funcionário para com as informações, equipamentos e outras propriedades do CIEE-RS a ele confiadas, devendo ser lida e assinada quando de sua admissão.

D. Segurança Lógica de Computadores, Redes e Sistemas Aplicativos

Este item trata do controle de acesso aos sistemas e às informações pertencentes ou de posse do CIEE-RS. Todo sistema aplicativo define um conjunto de operações aplicáveis às informações sob seu domínio. Tipicamente estas operações são: consulta, inclusão, alteração, exclusão, liberação, entre outros. Um perfil de acesso define que operações podem ser executadas por certa classe de usuários, usando um determinado tipo de informação. As regras de acesso às informações de um sistema aplicativo devem incluir a definição dos perfis e classe de usuários, bem como os processos operacionais a serem utilizados para sua administração e controle.

i. *Normas para segurança lógica de computadores e redes:*

Os acessos aos serviços e dados devem ser controlados com base nos requisitos de cada negócio, devem estar definidos e todos os sistemas aplicativos devem estar direcionados para a implementação e manutenção desses controles.

ii. *Administração do acesso de usuários:*

Devem existir procedimentos que contemplem todas as atividades ligadas à administração de acessos, desde a criação de um usuário novo, passando pela administração de privilégios e senhas e incluindo a desativação de usuários.

iii. *Controle de acesso a computadores e redes:*

Deve ser assegurado que usuários de computadores, conectados ou não a uma rede, não comprometam a segurança de qualquer sistema ou produto. O acesso a serviços computacionais deve ocorrer sempre através de um procedimento seguro, pelo qual o usuário conecta-se a um determinado sistema ou rede, que deve ser planejado para minimizar as oportunidades de acessos não autorizados.

iv. *Normas para controle de acesso a computadores, redes e sistemas aplicativos:*

Um sistema efetivo de controle de acesso deve ser utilizado para autenticar os usuários. As principais características desse controle são:

- O acesso a computadores e redes deve ser protegido por senha;
- As senhas poderão ser alteradas pelos usuários em qualquer ambiente (operacional ou aplicativo);

- A senha é de uso exclusivo, pessoal e intransferível, sendo o compartilhamento proibido em quaisquer circunstâncias;
- As senhas não devem ser triviais e previsíveis, e devem conter para sua maior segurança letras maiusculas, minúsculas, números e caracteres especiais .

v. *Monitoramento de uso e acesso aos sistemas aplicativos:*

Todos os sistemas aplicativos deverão:

- Detectar tentativas de acesso não autorizado;
- Sempre que houver riscos que afetem o negócio devem ser realizadas auditorias para futuras investigações, registrando os dados dos acessos, tais como: identificação do usuário, localidade, identificação do terminal ou estação de rede, data e hora do acesso, identificação do aplicativo acessado e transações executadas;

E. Segurança no Acesso de Prestadores de Serviço

Este tópico visa estabelecer controles sobre recursos de processamento da informação da organização durante a execução de serviços por contratados externos. Deve ser feita uma avaliação dos riscos envolvidos para determinar as implicações de segurança e os controles necessários. É proibida a utilização de equipamentos próprios do prestador conectados à rede da organização sem a devida autorização pela área de Tecnologia da Informação que deverá avaliar a necessidade através de justificativa técnica. Se for necessário deve-se segregá-los em uma rede própria e estabelecer um *"firewall"* para controlar os acessos.

F. Segurança Física de Computadores

Este tópico destina-se aos usuários e administradores de computadores conectados ou não a uma rede. O objetivo é garantir que o CIEE-RS estabeleça, administre e utilize computadores de maneira segura, e que sejam tomadas medidas adequadas para respeitar a confidencialidade, integridade e disponibilidade das informações que são armazenadas e manipuladas através desses equipamentos.

i. *Normas para segurança física de computadores:*

Quando não estiverem sendo utilizados, devem ser trancados, com acesso restrito a pessoas autorizadas. Ao se ausentar da estação de trabalho ou quando os computadores não estiverem sendo usados, a tela deverá ser bloqueada pelo usuário responsável do equipamento.

Os dispositivos eletrônicos não ligados a uma rede, e que contenham informações importantes para os negócios da organização, devem estar instalados em uma estrutura que garanta a segurança física destes equipamentos, incluindo sistemas que mantenham fornecimento de energia elétrica e recuperação de dados. Os usuários ligados a uma rede, e que tratam com informações importantes para os negócios da empresa, devem manter estas informações armazenadas nos servidores de rede.

G. Padrões para Instalação de Computadores

O padrão de instalação para os computadores deve atender a todas as normas estipuladas pelo CIEE-RS. A estrutura para manter a segurança física deve obedecer aos padrões de segurança geral da organização e adequar-se às seguintes especificações:

i. Sala:

- As dimensões do local devem ser suficientes para a instalação dos equipamentos;
- A disposição dos cabos lógicos e de energia deve ser adequada de forma que as pessoas possam transitar livremente;
- As entradas de ar (ventilação) dos equipamentos não devem estar obstruídas; e
- Os equipamentos devem estar em locais firmes que evitem trepidações.

ii. Refrigeração e qualidade do ar:

- Climatização deve ser conforme especificado pelo fabricante; e
- O ambiente deve estar livre de poluição por poeira, gases ou fumaça a fim de evitar que a poluição penetre nos equipamentos, possibilitando a quebra dos mesmos ou falhas de processamento.

iii. Rede elétrica:

- É recomendável que exista aterramento exclusivo para os equipamentos e que os pontos de energia sejam estabilizados;
- Para os equipamentos considerados críticos recomenda-se a instalação de UPS (*Uninterruptable Power Supply)*, fonte alternativa de alimentação de energia que é ativada automaticamente quando ocorre a queda na alimentação de energia;
- Os equipamentos devem ser instalados em uma rede elétrica seguindo os padrões recomendados pelos fabricantes; e
- As instalações elétricas devem sofrer revisões periódicas.

iv. Equipamentos Contra Incêndio:

- Devem existir equipamentos de combate a incêndios adequados para materiais eletrônicos, tais como extintores de CO2, e estes devem estar em local visível sinalizado e desobstruído, e ser de conhecimento de todos os funcionários; e
- Devem existir equipamentos de prevenção de incêndios adequados, tais como detectores de fumaça e alarme contra incêndio, devendo existir um meio eficiente de aviso a um órgão de combate a incêndio.

v. Iluminação:

- A iluminação deve ser adequada, evitando a incidência direta da luz do sol sobre os equipamentos.

H. Segurança Física dos Servidores de Rede

Este item destina-se aos usuários de sistemas operacionais com características de servidores de rede. O objetivo é garantir que o conglomerado administre e utilize os diversos sistemas operacionais de maneira segura, e que sejam tomadas medidas adequadas para garantir a confidencialidade de seus dados, a integridade e disponibilidade dos equipamentos e meios de armazenamento.

i. *Normas para segurança física dos servidores de rede:*

As mídias removíveis de armazenamento devem ter acesso controlado. Quando não estiverem sendo utilizados, devem ser trancados, com acesso restrito a pessoas autorizadas. Os servidores de arquivos devem estar instalados em uma área que garanta a segurança física destes equipamentos incluindo sistemas que mantenham fornecimento de energia elétrica e recuperação de dados.

ii. *Responsabilidades na segurança física dos servidores de rede:*

A área de tecnologia é responsável por:

- Elaborar e manter atualizado o inventário de *hardware* e *software*; e
- Garantir o controle de acesso físico aos equipamentos.

I. Padrões para Instalação dos Servidores de Rede

O padrão de instalação para servidores de rede deve atender a todas as normas estipuladas pelo CIEE-RS. A estrutura para manter a segurança física dos equipamentos de uma rede deverá adequar-se às mesmas especificações utilizadas para a instalação de computadores com as seguintes especificações adicionais:

i. Sala:

- Fechada, monitorada por câmera interna, com divisórias até o teto.

ii. Rede elétrica:

- Nos servidores, fazer uso de equipamento UPS (homologado por técnicos autorizados) com *"No Break";*
- É necessário que exista aterramento exclusivo para os equipamentos e estabilização dos pontos de energia elétrica.

iii. Equipamentos Contra Incêndio:

- No caso das salas de servidores e/ou telecomunicações deve-se considerar o uso de dispositivos automatizados de combate a incêndios, agentes extintores limpos como gases e outros recursos específicos a este tipo de ambiente.

iv. Precauções quanto à disponibilização dos meios de armazenamento:

- As manutenções mídias removíveis, realizadas no próprio local, devem ser acompanhadas pelo responsável da área.

J. Backup e Restore

Este tópico se destina aos usuários e administradores da àrea de tecnologia do CIEE-RS, visando administrar e utilizar os recursos de tecnologia de maneira segura, tomando medidas adequadas que garantam recursos alternativos de processamento na eventualidade de perda dos dados, *softwares* ou sistemas.

Para a elaboração de um plano de *backup* devem ser considerados os "*backups*" do tipo Operacional, Contingencial e Histórico.

Backup Operacional: é a cópia das informações estratégicas que fazem parte do quotidiano do usuário e que são importantes para garantir a continuidade de suas tarefas. Destina-se à recuperação instantânea.

Backup Contingencial: é a cópia das informações sensíveis, softwares e sistemas vitais à continuidade dos negócios da organização e deve ser guardado em local externo ou em ambiente de *cloud computing*. Este tipo de Backup destina-se a permitir a recuperação em situações catastróficas.

Backup Histórico: é a cópia das informações determinadas por exigência legal ou normas internas e deve ser guardado em local externo ou em ambiente de *cloud computing.*

Em casos de Cloud terceirizado devem ser adotadas medidas que estejam em confomidade com o art. 11 da lei 12.965/2014 - Marco Civil da Internet, bem como toda forma de proteção descrita na lei 13.709/2018 - LGPD.

i. *Normas para Backup/Restore:*

A elaboração do plano de *Backup/Restore* deverá levar em consideração os aspectos abaixo:

- Os períodos de atualização dos dados; e
- Particularidades de cada área de negócios da organização;

As informações consideradas imprescindíveis devem estar presentes nas rotinas de *backups* operacional e contingencial, levando-se em consideração a periodicidade de atualização dos dados.

As informações devem estar sujeitas às rotinas de *backups* operacional e contingencial conforme critério definido pelo usuário. As cópias de *backup* devem estar guardadas em local apropriado e seguro, e protegidas contra o acesso por pessoas não autorizadas. Deve-se manter uma cópia do plano de *Backup/Restore* juntamente com o *backup* contingencial. Devem ser mantidas, no mínimo, as duas últimas versões dos *backups* operacional e contingencial. Para os *backups* históricos, a quantidade de versões será determinada por exigência legal ou norma interna.

ii. *Plano de Backup/Restore - Conteúdo:*

***Abrangência**:* Relação dos arquivos e diretórios a serem copiados no processo de *backup*.

***Periodicidade**:* Intervalo de tempo após o qual o sistema é submetido à rotina de *backup*.

Retenção: Prazo pelo qual os *backups* devem ser mantidos.

Procedimentos: Descrição dos procedimentos de *backup*.

Quantidade de cópias: Número de cópias de *backup*, locais e meios de armazenamento.

Identificação dos meios de armazenamento: Os meios de armazenamento devem estar devidamente identificados(físicos ou em ambiente cloud).

Registro do uso das cópias de backup: A manipulação dos meios de armazenamento deve ser registrada e controlada.

K. Responsabilidades quanto ao *Backup/Restore*

É de responsabilidade da Àrea de Tecnologia elaborar, manter e documentar o plano de *backups* e garantir a execução de seus procedimentos.

L. Pirataria

Este item se destina a todos os usuários e administradores de servidores de redes ou computadores, inclusive portáteis, conectados ou não a rede do CIEE-RS e tem como objetivo garantir que sejam tomadas medidas adequadas para coibir a pirataria de *softwares ou violação de qualquer propriedade intelectual* dentro das instalações do CIEE-RS.

Normas contra pirataria:

A quantidade de licenças de *softwares* não pode ser inferior à quantidade de softwares instalados, mesmo que para fins de testes ou treinamentos, a não ser que esta situação esteja coberta contratualmente. Não é permitido duplicar *software* de propriedade da organização a não ser com a finalidade de cópia de segurança e mesmo assim, somente por pessoas autorizadas. Uma licença de uso de *software* da organização só pode ser instalada em computadores da organização, a não ser que, contratualmente pelo detentor dos direitos autorais esteja autorizado de outra forma. Não é permitido executar ou instalar qualquer *software* (inclusive *software* livre e de domínio público), telas de "*screen saver*", “papéis de parede” etc., que não estejam autorizados pela área de tecnologia do CIEE-RS. É proibida a utilização e reprodução não autorizada de manuais, livros, revistas, periódicos protegidos por direitos autorais.

i. *Responsabilidades quanto à pirataria:*

É da responsabilidade da área de tecnologia do CIEE-RS:

- Verificar se o *software* a ser instalado é original, conferindo o mesmo com as devidas licenças de uso;
- Se a instalação foi autorizada pelo Responsável Administrativo da Unidade, verificar se o *software* foi previamente homologado pela área de tecnologia; e
- Implementar mecanismos que dificultem a pirataria através de qualquer meio.

M. Utilização Segura de *Hardware* e *Software*

Todos os equipamentos portáteis (*notebooks, laptops, netbooks, ultrabooks, tablets e smartphones*) que tenham capacidade de armazenamento de dados, devem ser protegidos conforme especificação do CIEE-RS. Quando estes equipamentos contiverem informações que não possam ser de conhecimento público, as mesmas devem ter seu acesso protegido por senha. É expressamente vedada a aquisição, reprodução, utilização e cessão de cópias não autorizadas de *"softwares"* ou de quaisquer programas e produtos, mesmo aqueles desenvolvidos pelas áreas técnicas do CIEE-RS ou desenvolvidos por terceiros para o próprio CIEE-RS

N. Acesso à *Internet*

A *Internet* abrange vários aspectos e serviços *(websites* de serviços governamentais, prestadores de serviço e outros) que devem ser disponibilizados de forma restrita ou controlados conforme as necessidades de negócio.

A restrição a *websites* não relativos aos negócios da organização deve ser implementada, garantindo o uso efetivo da rede de *Internet*. O usuário deve verificar a Política de Cookies e Privacidade em websites que acessar nas máquinas e equipamentos da empresa antes de concordar. O acesso à *Internet* deve ser rastreado a fim de permitir o monitoramento do uso indevido da tecnologia (Nome do usuário e endereço acessado são informações obrigatórias no rastreamento). A área de tecnologia deve bloquear o acesso aos *websites* que possam denegrir a imagem da organização (por exemplo: pornografia, pedofilia, racismo etc.) e que não têm relação com os objetivos de negócio da organização (*Webmail*, jogos etc.). Deve também comunicar o endereço eletrônico desses *websites* à área de segurança da informação do CIEE-RS, que deverá realizar seu imediato bloqueio. O acesso à *Internet* deve ser feito através de "Servidores de Acesso" protegidos por sistemas de *Firewall*. Quando for necessário o acesso utilizando uma segunda conexão através de *modem* ou rede *wi-fi*, a configuração da máquina deve garantir o isolamento da rede normal de serviço da empresa, evitando assim que uma contaminação seja propagada. Os requisitos de segurança destas máquinas em particular devem ser respeitados (antivírus e *firewall* local). Casos específicos como esses devem ser aprovados pelos responsáveis da área de segurança da informação do CIEE-RS.

O. Acesso ao Correio Eletrônico

O CIEE-RS disponibiliza aos seus funcionários a tecnologia necessária a fim de facilitar a comunicação interna, comunicação com clientes, fornecedores e outras organizações que tenham relação com a mesma.

É de responsabilidade do usuário a utilização da tecnologia de forma adequada, prudente, e de modo compatível com as leis e princípios aplicáveis aos negócios. As mensagens de correio eletrônico devem ser rastreadas, a fim de permitir o monitoramento para identificar o uso indevido da tecnologia. Por consequência, devem ser observadas as orientações descritas, inclusive, em políticas internas já formalizadas e contrato de trabalho.

As mensagens de correio eletrônico são instrumentos de comunicação interna e externa para a realização do negócio da organização. Elas devem ser escritas em linguagem profissional e que não comprometa a imagem da organização, não conflite com a legislação vigente e nem aos princípios éticos da organização. Mensagens fora dessas características não devem ser enviadas e quem o fizer poderá responder, proporcionalmente, ao impacto que isso poderá causar a outra pessoa ou organização. O conteúdo do correio eletrônico de cada usuário pode ser acessado pela organização quando em situações que ponham em risco a sua imagem e o seu negócio. Este acesso será feito a critério da organização, mediante comunicação ao superior imediato do usuário, á àrea de tecnologia e deve ser registrado formalmente. O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço. Mensagens recebidas não coerentes com essa política devem ser eliminadas.

P. Conscientização de Segurança da Informação

A conscientização da segurança da informação do CIEE-RS passa por todos os seus colaboradores conhecerem e compreenderem esta politica.

Para isso, as diretrizes básicas são:

- Elaboração de um processo de treinamento continuado contemplando todos os níveis funcionais do CIEE-RS;
- Divulgação de diversos materiais e alertas referente a Segurança da Informação para funcionários, colaboradores, prestadores de serviços e clientes;
- Criação de procedimentos de aferição do nível de conhecimento dos usuários em geral;
- Organização de eventos que tenham o intuito de fortalecer a conscientização sobre diversos aspectos de segurança em geral;
- Revisão periódica adequando as ações às novas necessidades, evitando torná-lo repetitivo.

Esta Política de Segurança da Informação foi atualizada pela última vez em agosto de 2022.