1. OBJETIVO

1.1 A Política de Segurança da Informação - PSI, visa orientar e estabelecer as diretrizes corporativas para a proteção dos ativos de informação e a gestão da sua segurança no Sistema FIEPE, estabelecendo regras e padrões para proteção dela. A PSI busca preservar as informações e seus respectivos ativos quanto à confidencialidade, integridade, disponibilidade e autenticidade.

1.2 Esta Política faz parte do trabalho de proteção de dados do Sistema FIEPE voltado ao atendimento da LGPD, desta forma, tudo o que está exposto e no momento da sua aplicação, deve ser executado à luz da referida lei, inclusive, para aplicação desta política devem ser observadas as demais políticas relacionadas.

2. ABRANGÊNCIA

2.1 As informações e diretrizes aqui estabelecidas se aplicam à informação em qualquer meio ou suporte. Deverão ser seguidas por todos os colaboradores, conselheiros e dirigentes, bem como pelos prestadores de serviço e parceiros.

2.2 Esta política dá ciência a todos os envolvidos de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados conforme previsto nas leis brasileiras.

2.3 É também obrigação de cada colaborador se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor, da Unidade de Governança e Compliance Unidade ou da Compartilhada de Tecnologia da Informação, sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

2.4 As diretrizes integrantes da estrutura deste documento devem ser divulgadas a todos os envolvidos nas atividades das entidades do Sistema FIEPE através dos meios oficiais de treinamento e divulgação interna, além de publicadas no site ou Intranet da instituição de maneira que seu conteúdo possa ser consultado a qualquer momento.

3. PROTEÇÃO À INFORMAÇÃO

3.1 É necessária a proteção das informações das entidades do Sistema FIEPE ou qualquer informação sob sua custódia para execução das atividades profissionais de cada colaborador, prestador de serviços ou cliente, sendo que:

a) Os colaboradores e prestadores de serviço devem assumir uma postura proativa no que diz respeito à proteção das informações das entidades do Sistema FIEPE e devem estar atentos às ameaças externas, bem como fraudes, roubo de informações e acesso indevido aos sistemas de informação sob responsabilidade delas, entidades do Sistema FIEPE;
b) Quaisquer informações devem ser coletadas de forma ética e legal, para propósitos específicos e devidamente informados;

c) As informações não podem ser transportadas em qualquer meio físico sem as devidas proteções e autorizações dos gestores;
d) Assuntos confidenciais devem ser tratados com os cuidado e sigilo adequados;
e) Senhas, chaves e outros recursos de caráter pessoal são considerados intransferíveis e não podem ser compartilhados e divulgados;
f) Informações de caráter pessoal não devem ser armazenadas ou arquivadas nos equipamentos ou ambiente virtuais ou físicos das entidades do Sistema FIEPE;
g) Somente softwares homologados e devidamente licenciados podem ser utilizados no ambiente computacional das entidades do Sistema FIEPE;
h) Documentos impressos e digitais contendo informações confidenciais, devem ser armazenados e protegidos. O descarte deve ser feito de acordo com o procedimento vigente e baseado na legislação pertinente;
i) Não é permitido o compartilhamento de pastas localizadas nos computadores de colaboradores e prestadores de serviço das entidades do Sistema FIEPE. Os dados que necessitam ser compartilhados devem estar alocados em servidores apropriados (em rede), atentando às permissões de acesso aplicáveis aos referidos dados;
j) Todos os dados considerados como imprescindíveis aos objetivos das entidades do Sistema FIEPE devem ser protegidos através de rotinas sistemáticas e documentadas de cópia de segurança (Backup), devendo ser submetidos à testes periódicos de recuperação;
k) Todas as estações de trabalho e servidores devem ser obrigatoriamente protegidas com a ferramenta corporativa de segurança endpoint (antivírus);
l) As informações contidas em sistema de uso interno ou externo, devem ser gerenciadas com credencias individuais, não devem ser usadas credencias padrão, como administrador ou admin, exceto em situações que exijam o uso;

4. DIRETRIZES

4.1. Quanto ao tratamento da informação:

a) Documentos imprescindíveis para as atividades dos usuários das entidades do Sistema FIEPE deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores, não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário;
b) Arquivos pessoais e/ou não pertinentes às atividades institucionais (fotos, músicas, vídeos etc.) não deverão ser copiados ou movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificados, os arquivos poderão ser excluídos definitivamente sem necessidade de comunicação prévia ao usuário, exceto caso os arquivos sejam relacionados a fins corporativos da instituição;
c) As informações deverão ser protegidas e disponibilizadas apenas para os setores/pessoas autorizados a manuseá-las;
d) Caso necessário outro setor/pessoa acessar os arquivos que não são de sua posse, se faz necessário a autorização do gestor detentor da informação.
e) O tratamento de dados aqui mencionados deve respeitar a LGPD e as políticas internas relacionadas;

f) Somente os colaboradores que estão devidamente autorizados a falar em nome das entidades do Sistema FIEPE para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, documento físico, entre outros.

4.2. Quanto ao controle de acessos:

a) O controle de acesso deverá considerar e respeitar o princípio do menor privilégio para configurar as credenciais ou contas de acesso dos usuários aos ativos de informação;
b) A criação e administração de contas será realizada de acordo com procedimento específico para todo e qualquer usuário. Para o usuário que não exerce funções de administração de rede, será criada uma única conta institucional de acesso, pessoal e intransferível. Contas com perfil de administrador somente serão criadas para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação;
c) O acesso à rede corporativa deve dar-se de forma a permitir a rastreabilidade e a identificação do usuário por período mínimo a ser definido de acordo com a capacidade do serviço de armazenamento de informações;
d) As práticas de segurança deverão contemplar procedimentos de acesso físico às áreas e instalações, gestão de acessos e delimitação de perímetros de segurança;
e) Todo acesso a sala de ativos de TI deve ser acompanhado por responsável na unidade, exceto caso o acesso seja feito por colaborador interno técnico do serviço ou ação a ser executada;
f) Os acessos à sala de ativos devem ser solicitados e registrados via sistema de chamado interno.

4.3. Quanto ao correio eletrônico (e-mail):

4.3.1 O correio eletrônico é uma ferramenta disponível para todos os funcionários das entidades do Sistema FIEPE e seu uso é para fins corporativos e relacionados às atividades profissionais dos usuários;

4.3.2 É proibido aos colaboradores o uso do correio eletrônico das entidades do Sistema FIEPE para:

a) Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo e autorizado das entidades do Sistema FIEPE;
b) Enviar mensagem por correio eletrônico pelo endereço de sua unidade ou usando o nome de usuário de outra pessoa, ou endereço de correio eletrônico que não esteja autorizado a utilizar;
c) Enviar qualquer mensagem por meios eletrônicos que torne seu remetente, as entidades do Sistema FIEPE ou suas unidades, vulneráveis a ações civis ou criminais;
d) Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
e) Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários;
f) Produzir, transmitir ou divulgar mensagem que:
   i. Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses das entidades do Sistema FIEPE;
   ii. Contenha ameaças eletrônicas, como spam, mail bombing, vírus de computador;
   iii. Vise obter acesso não autorizado a outro computador, servidor ou rede;

iv. Vise interromper um serviço, servidor ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
v. Vise burlar qualquer sistema de segurança;
vi. Vise vigiar secretamente ou assediar outro usuário;
vii. Vise acessar informações confidenciais sem explícita autorização do proprietário;
viii. Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
ix. Tenha conteúdo considerado impróprio, obsceno ou ilegal;

4.4 Quanto ao acesso à internet:

4.4.1 Todas as regras corporativas sobre uso de Internet visam basicamente ao desenvolvimento de um comportamento eminentemente ético e profissional. A conexão direta e permanente da rede corporativa da instituição com a internet oferece um grande potencial de benefícios, porém, a proteção dos ativos de informação das entidades do Sistema FIEPE deverá sempre ser privilegiada, observando-se:

a) As entidades do Sistema FIEPE, em total conformidade legal, reservam-se o direito de monitorar e registrar todos os acessos à internet realizados por seus colaboradores e prestadores de serviço;
b) Os equipamentos, tecnologias e serviços fornecidos para o acesso à internet são de propriedade das entidades do Sistema FIEPE, que podem analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na internet;
c) Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada;
d) O uso de qualquer recurso para atividades ilícitas poderá acarretar em ações administrativas e penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes;
e) Como é do interesse das entidades do Sistema FIEPE que seus colaboradores estejam bem-informados, o uso de sites de notícias ou de serviços, é aceitável, desde que não comprometa a banda da rede, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio;
f) É proibida a divulgação e/ou o compartilhamento indevido de informações das entidades do Sistema FIEPE em listas de discussão externas às entidades;
g) O uso, instalação, cópia ou distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos;
h) Os colaboradores não poderão em hipótese alguma utilizar os recursos corporativos para fazer o download ou distribuição de software ou dados pirateados;
i) O download e utilização de programas de entretenimento, jogos, redes sociais ou músicas (em qualquer formato) só poderão ser realizados por usuários que tenham atividades profissionais relacionadas a essas categorias. Mediante solicitação e aprovação da área técnica responsável, o uso de jogos será passível de concessão, em regime de exceção, quando eles tiverem natureza intrínseca às atividades de uso técnico de qualquer natureza;

j) Materiais de cunho sexual são expressamente proibidos, não poderão ser acessados, expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso;
k) Os colaboradores não poderão utilizar os recursos das entidades do Sistema FIEPE para deliberadamente propagar qualquer tipo de vírus, cavalo de troia, spam ou programas de controle de outros computadores;
l) Todo colaborador deve fazer uso do sistema de comunicação instantânea interno padrão;
m) O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos;
n) Já os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos devidamente autorizados;
o) Não é permitido acesso a sites de proxy, VPN ou qualquer outro recurso que burle qualquer bloqueio ou diretriz interna das entidades do Sistema FIEPE.

4.5 Quanto ao serviço de backup:

a) O serviço de backup deve ser automatizado por sistemas informacionais próprios;
b) A solução de backup deverá ser mantida atualizada considerando suas diversas características (atualizações de correção, novas versões, ciclo de vida, garantia, melhorias, entre outros);
c) A administração das mídias de backup deverá ser contemplada nas normas complementares sobre o serviço (política de backup), objetivando manter sua segurança e integridade;
d) Testes de restauração (restore) de backup devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, de acordo com a política de backup;
e) Para formalizar o controle de execução de backups e restores, haverá um rígido controle de execução dessas rotinas, que deverá ser auditado de acordo com a política de backup.

6. RESPONSABILIDADES

6.1 Dos colaboradores:

a) Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora das entidades do Sistema FIEPE;
b) Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar às entidades Sistema FIEPE e/ou a terceiros, em decorrência da não obediência às diretrizes e normas deste documento;
c) Cabe ao colaborador preservar a integridade e guardar sigilo das informações de que faz uso, bem como zelar e proteger os equipamentos de informática disponibilizados para a realização do seu trabalho;
d) Usar apenas as suas credenciais de acesso e protegê-las para que ninguém tenha conhecimento;
e) Utilizar os recursos e sistemas de informações somente para fins profissionais;
f) Todas as transações internas ou externas de informações devem ser feitas através de mecanismos corporativos, como o e-mail institucional;
g) Responder por todo e qualquer acesso aos recursos, bem como pelos efeitos desses acessos efetivados através de sua credencial de identificação, ou outro atributo utilizado para esse fim;

h) Comunicar ao seu superior imediato o conhecimento de qualquer irregularidade ou desvio em relação à segurança da informação.

6.2 Dos gestores:

a) Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão;
b) Capacitar os colaboradores sobre este documento para que esses assumam o dever de seguir as normas estabelecidas, bem como se comprometer a manter sigilo e confidencialidade, mesmo quando desligados, sobre todos os ativos de informações das entidades do Sistema FIEPE;
c) Atribuir aos colaboradores, na fase de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI;
d) Antes de conceder acesso às informações da instituição, exigir a assinatura do Acordo de Confidencialidade dos colaboradores e prestadores de serviços, quando pertinente;
e) Adaptar as normas, processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI;

6.3 Do Comitê Gestor de Proteção de Dados e Segurança da Informação:

a) Apoiar na implementação das ações de segurança da informação;
b) Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;
c) Propor alterações e revisar periodicamente a PSI das entidades do Sistema FIEPE, em conformidade com a legislação existente sobre o tema;
d) Apoiar na proposição de normas complementares e procedimentos internos de segurança da informação e dados pessoais, em conformidade com a legislação existente sobre os temas;
e) Subsidiar a alta gestão das entidades do Sistema FIEPE nas decisões relativas à segurança da informação.
f) Supervisionar a execução dos planos, dos projetos e das ações aprovados para viabilizar a implantação das diretrizes previstas na LGPD;
g) Prestar orientações sobre o tratamento e a proteção de dados pessoais de acordo com as diretrizes estabelecidas na LGPD e nas normas internas;
h) Promover o intercâmbio de informações sobre a proteção de dados pessoais com as Entidades Nacionais, demais Departamentos Regionais do Sistema Indústria e outros órgãos afins.

6.4 Da Alta Gestão:

a) Reforçar esta Política por meio da comunicação;
b) Liderar suas equipes para o cumprimento das diretrizes estabelecidas nesta Política;
c) Estimular a participação de suas equipes nos treinamentos sobre esta Política.

6.5 Dos fornecedores e parceiros

a) Cumprir as diretrizes desta política durante a execução dos acordos firmados com as entidades do Sistema FIEPE, mantendo a segurança das informações e ativos computacionais disponibilizados, produzidos e compartilhados no exercício de suas atividades.

7. DISPOSIÇÕES GERAIS

7.2 Dúvidas em relação a interpretação desta Política devem ser esclarecidas com o especialista de infraestrutura Unidade Compartilhada de Tecnologia da Informação ou gerente da Unidade de Governança e Compliance.

8. REFERÊNCIAS

8.1 As principais referências normativas para elaboração desta Política são:

a) Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).
b) Lei nº 12.965, de 23 de abril de 2014 – Marco Civil da Internet
c) ABNT NBR ISO/IEC 27002 – Código de Prática para Controles de Segurança da Informação