1. OBJETIVO

A Política de Segurança da Informação consiste em um conjunto de diretrizes e regras que tem por objetivo possibilitar o planejamento, a implementação e o controle de ações relacionadas à Segurança da Informação, visando garantir a confidencialidade, integridade e disponibilidade das informações da cooperativa.

Normalmente, a Política de Segurança da Informação é um documento formal com as diretrizes da alta direção.

Após a publicação da Política, geralmente são desenvolvidos normativos tratando especificamente cada ponto da política.

No nosso caso, optamos por desenvolver uma Política adaptada ao que a Autoridade Nacional de Proteção de Dados sugere, que é uma Política simplificada.

A presente Política de Segurança da Informação tem como referências itens da norma ISO 27001, a Resolução CD/ANPD Nº 2, e o Guia Orientativo da ANPD “Segurança da Informação para Agentes de Tratamento de Pequeno Porte”.

Considerada pela ANPD como uma boa prática para a gestão de segurança, sua implementação evidencia boa-fé e diligência na segurança dos dados pessoais e fornece as diretrizes para que a gestão apoie a implementação de um processo estruturado de Segurança da Informação.

Deve, portanto, ser cumprida e aplicada em todas as áreas da cooperativa.

Esta Política de Segurança deve ser revisada anualmente, ou quando houver atualização relevante no contexto tecnológico e de cibersegurança da empresa.

Este documento está classificado como INTERNO, e eventual pedido de compartilhamento com terceiros deverá ser submetido previamente ao setor de Segurança da Informação da

FENCOM para ciência, análise e aprovação, devendo ser disponibilizado, em documento simplificado, digitalizado e protegido.

2. APLICAÇÃO

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

Esta política dá ciência de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados.

Todos devem se manter cientes e atualizados em relação a esta Política de Segurança da Informação e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou do setor de Segurança da Informação da FENCOM, para qualquer dúvida ou orientação sobre procedimento ou qualquer outra dúvida relacionada a Segurança da Informação.

3. DEFINIÇÕES

NA

4. DESCRIÇÃO

Divulgação

A Política de Segurança da Informação deve ser divulgada a todos os colaboradores e aos prestadores de serviços internos que tenham acesso a informações na empresa, através de uma comunicação clara, objetiva e acessível aos distintos níveis de funções.

A comunicação deve deixar claro quais as implicações consequentes nos casos de não aderência às diretrizes da Política de Segurança da Informação e das normas relacionadas ao tema de Segurança da Informação.

Ativo Informação

Considerando a LGPD, todos os dados pessoais e dados pessoais sensíveis são, por natureza, confidenciais e restritos, respectivamente.

Controles de segurança deverão ser implementados para garantir, além da segurança, todos os aspectos de privacidade.

Toda informação deve ter um proprietário (gestor da informação), que será o responsável na área de negócios por critérios de uso e concessão de acesso.

As informações e sistemas criados, modificados e/ou armazenados na cooperativa são considerados ativos pertencentes da mesma, e não podem ser copiados, reproduzidos ou enviados externamente sem prévio consentimento do responsável pela área de negócios.

As informações devem ser armazenadas em ambiente definido pela cooperativa, evitando-se o armazenamento de informações em equipamentos e computadores individuais.

Acesso à Informação

Os sistemas ou repositórios que contenham dados pessoais, devem ser acessados somente por usuários autenticados, observando-se o princípio da “necessidade de saber”.

Todo acesso deverá ser registrado e preferencialmente monitorado, para detectar possíveis tentativas de acessos indevidos ou vazamento de dados.

Compartilhamento de Dados

Os agentes externos com os quais a cooperativa compartilha dados pessoais e/ou dados sensíveis, devem comprovar adoção de medidas de segurança técnicas e administrativas aptas a proteger esses dados.

O compartilhamento de dados pessoais e/ou dados pessoais sensíveis somente poderá ocorrer obedecendo aos requisitos legais.

Relacionamento com Fornecedores e Prestadores de Serviços

Contratos para prestação de serviços, fornecimentos de sistemas, infraestrutura, processamento e/ou armazenamento de informações, devem incluir cláusulas específicas que garantam a segurança, preservação do sigilo, integridade e disponibilidade das informações e serviços acordados.

Para atender demandas e necessidades pontuais da cooperativa com suas contrapartes (empresas e pessoas externas à cooperativa), deverá ser formalizada a assinatura de um Termo de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela instituição.

Conscientização em Cibersegurança

Todos os colaboradores e terceiros internos deverão comprovar a conclusão do treinamento de conscientização em cibersegurança, quando disponibilizado, entregando o certificado de conclusão em tempo hábil a seu gestor imediato.

Se ocorrer algum incidente de segurança, que poderia ter sido evitado com a conscientização, com usuário que não concluiu o treinamento sem justificativa, o mesmo será penalizado de acordo com o determinado pela empresa.

Responsabilidades

Segurança da Informação

Em questões comumente atribuídas a um departamento interno de Segurança da Informação, a cooperativa recorre ao setor de Segurança da Informação da FENCOM, que analisa e delibera sobre os assuntos relacionados e apoia tecnicamente no entendimento e aplicação nas áreas de atuação da cooperativa.

A Segurança da Informação é responsável pelo direcionamento, acompanhamento e monitoramento das ações de cibersegurança e proteção da informação, interagindo diretamente com os gestores das áreas responsáveis pelos processos (TI e Negócios).

Atua com apoio da área de tecnologia, que executa implementação dos controles definidos pela Segurança da Informação.

Gestores

São os responsáveis pelo correto funcionamento de suas áreas e devem garantir a divulgação da Política de Segurança da Informação, o monitoramento da execução das diretrizes aprovadas, assim como das normas e procedimentos relacionados, reportando os casos de desvios de conduta por parte dos usuários.

Devem reportar todo e qualquer evento adverso (interno ou externo) gerado pelo mau uso das informações, que tenham sido identificados por um usuário sob sua responsabilidade.

Devem garantir que os equipamentos de seus setores estejam configurados de acordo com as normas, procedimentos e padrões estabelecidos.

Devem garantir acessos exclusivos dos usuários, concedidos de acordo com a necessidade para execução de suas atividades.

Devem ter postura exemplar em relação à Segurança da Informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

Usuários

São os colaboradores, terceiros, estagiários e os menores aprendizes.

Representam os principais agentes de proteção das informações da cooperativa e primeira linha de defesa contra-ataques cibernéticos.

Devem observar o cumprimento da Política de Segurança da Informação em sua totalidade, e também as normas e procedimentos relacionados.

Devem comunicar tempestivamente à Gestão e demais áreas definidas pela cooperativa, qualquer violação ou descumprimento da Política, de norma ou de procedimentos.

Controle de Acesso

Deve ser implementado um sistema de controle de acesso aplicável a todos os usuários, com níveis de permissão na proporção da necessidade de trabalhar com o sistema e de acessar dados pessoais.

O sistema de controle de acesso deve permitir a criação, aprovação, revisão e exclusão de contas dos usuários, e deve ser configurado com funcionalidades que possam detectar e não permitir o uso de senhas que não respeitem um certo nível de complexidade, definindo a quantidade mínima de caracteres, uso de caractere especial ou outros fatores que o agente de tratamento considere necessários.

Não deve ser permitido o compartilhamento de contas ou de senhas entre funcionários, visto que isso é um vetor crítico de vulnerabilidade de Segurança da Informação.

O acesso ao ambiente e/ou aos sistemas permitidos a um usuário através de seu gestor, deve levar em consideração a função que o mesmo exerce no setor, observando sempre o princípio da "Necessidade de Saber", ou seja, os usuários de um sistema terão o menor nível de acesso necessário para a realização de suas atividades.

No acesso a sistemas ou base de dados que contenham dados pessoais e dados sensíveis, deve ser obrigatoriamente utilizada a Autenticação MultiFator (MFA).

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários.

Portanto, quando do afastamento, férias ou movimentação de qualquer usuário, o Recursos Humanos deverá, imediatamente, comunicar tal fato a Tecnologia da Informação que bloqueará os acessos.

Atenção especial nos casos de desligamentos, onde o setor de TI deverá ser antecipadamente comunicado.

A mesma conduta se aplica aos usuários cujo contrato de prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

Uso de Senhas

Ao realizar o primeiro acesso ao ambiente ou a sistemas, o usuário deverá trocar imediatamente a sua senha provisória.

As senhas devem ter no mínimo 8 (oito) caracteres alfanuméricos, utilizando caracteres especiais, números e variação entre maiúsculo e minúsculo sempre que possível.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

As senhas não devem ser anotadas em papel ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento.

Para garantir um melhor gerenciamento das senhas de acessos, todos deverão utilizar aplicativo de Cofre de Senhas, onde deverão ficar armazenadas as senhas relacionadas as atividades corporativas.

Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo com regularidade, principalmente, no caso de suspeita de que terceiros obtiveram acesso indevido ao seu login/senha.

A periodicidade máxima para troca das senhas deve ser de 120 (cento e vinte dias) dias, não podendo ser repetidas as 5 (três) últimas senhas.

As senhas padrão disponibilizadas pelos fornecedores de software ou hardware adquiridos, devem ser alteradas por outras com requisitos mais seguros, tendo em vista que geralmente os atacantes utilizam estas senhas padronizadas (default) para tentativas de conexão e realizar os seus ataques.

Cópias de Segurança

Os dados de sustentação dos negócios da cooperativa devem ser protegidos contra perdas através de cópias de segurança (backup), que devem ser automatizados e executados regularmente de forma completa, sendo armazenado em locais seguros e distintos dos dispositivos de armazenamento principais.

Os backups não devem ser sincronizados online (em tempo real), para evitar a perda de dados em casos de infecções por códigos maliciosos que sequestram os dados (ransomware).

Todos os backups (local e nuvem) devem ser configurados com agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas “janelas de backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

Arquivos pessoais e/ou não pertinentes ao negócio da cooperativa (fotos, músicas, vídeos, etc.), não deverão ser copiados/movidos para os drives de rede/nuvem, pois podem sobrecarregar o armazenamento nos servidores, o que impacta na execução do backup.

Para o backup dos documentos imprescindíveis para as atividades dos colaboradores da instituição, estes deverão ser salvos em drives de rede ou no local disponibilizado na nuvem.

Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:, pasta Documentos, etc), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Uso de E-mail

O e-mail corporativo só deve ser utilizado para fins relacionados às atividades do usuário dentro da instituição, e o processo que envolva envio de dados pessoais e/ou dados pessoais sensíveis devem ser validados criteriosamente pelo responsável da área de negócios.

O e-mail corporativo deve ser integrado ao antivírus, e contar com filtros e proteção AntiSpam. Fica proibido aos colaboradores o uso do correio eletrônico da cooperativa com o propósito de:

- enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas ao uso legítimo da instituição;
- enviar e-mail por endereço que não esteja autorizado a utilizar;
- divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação.

Atualização de Softwares

Os sistemas e aplicativos devem ser mantidos em suas últimas versões, e todas as correções de segurança disponíveis lançadas pelo desenvolvedor do sistema operacional e aplicativos devem ser imediatamente instaladas.

Um sistema de gerenciamento de atualizações automatizado, que demonstre visibilidade do status dos ativos deve ser implantado para garantir a atualização de todos os softwares utilizados.

Os sistemas e computadores devem ter versões do sistema operacional ativadas e atualizadas permanentemente.

MEDIDAS DE SEGURANÇA

Uso de Antivírus

Todos os computadores, notebook, servidores e smartphones corporativos devem utilizar softwares antivírus ou antimalwares corporativos, que detectam, impeçam e atuem na remoção de programas maliciosos, como vírus.

Os antivírus devem ser mantidos funcionando ativamente e atualizados, realizando varreduras periódicas nos dispositivos, inclusive nos e-mails, e não devem ser desativados ou alterados pelos usuários.

Uso da Internet

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet.

É proibida a divulgação e/ou o compartilhamento indevido de informações em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

Os colaboradores não poderão sob qualquer hipótese utilizar os recursos da cooperativa para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

Utilização dos Recursos

Os equipamentos disponibilizados aos colaboradores são de propriedade da cooperativa, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações e diretrizes constantes nesta Política de Segurança da Informação.

É proibido todo e qualquer procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o prévio conhecimento e o acompanhamento de um técnico da Tecnologia da Informação, ou de quem este determinar.

Se for permitido ao colaborador e o mesmo desejar utilizar seu próprio dispositivo para execução de seu trabalho, o mesmo deverá estar ciente de que esse dispositivo deverá

estar equiparado aos dispositivos corporativos com relação a proteções de segurança, visando proteger os dados nele presentes.

Todo usuário deve bloquear a estação de trabalho antes de se ausentar.

O colaborador deverá manter a configuração do equipamento disponibilizado pela cooperativa, respeitando as regras de segurança exigidas por esta Política de Segurança da Informação e pelas demais normas específicas da instituição, assumindo a responsabilidade como custo diante de informações.

É proibido utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

Todo colaborador deverá utilizar senhas de bloqueio automático para os dispositivos em uso e, no caso de “desktop” (computador de mesa), quando das súbitas ausências de suas estações de trabalho.

O espaço de trabalho do colaborador deve seguir a “Política de Mesa Limpa”, não deixando exposto nesse espaço documentos que contenham dados pessoais, senhas anotadas etc.

Da mesma forma, deve ser evitado deixar documentos abandonados na impressora, e não devem ser utilizados como rascunho documentos que contenham dados pessoais.

Dispositivos Móveis

Preferencialmente, devem ser utilizados somente notebooks e celulares corporativos, configurados com a autenticação multifator para o acessá-los.

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela cooperativa, notificar imediatamente seu gestor direto e a Gerência de Tecnologia da Informação, e procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

Os dispositivos móveis corporativos, devem contar com funcionalidades que permitam apagar remotamente os dados pessoais armazenados, nos casos de perda ou roubo, para prevenir vazamento de dados pessoais.

DISPOSIÇÕES FINAIS

A Segurança da Informação deve ser entendida como parte fundamental da cultura interna da cooperativa, dessa forma, o não cumprimento dos requisitos previstos nesta Política de Segurança da Informação acarretará violação às regras internas da instituição e sujeitará o usuário a medidas administrativas de acordo com os procedimentos vigentes na empresa.

Em casos de dúvidas ou esclarecimentos sobre o conteúdo desta Política, ou sobre a aplicação da mesma em relação a algum assunto específico, o colaborador deverá entrar em contato a qualquer momento com o gestor da sua área ou com o setor de Segurança da Informação da FENCOM.

Todos os colaboradores deverão ser instruídos e orientados sobre os procedimentos de segurança, bem como do uso correto dos ativos de informação, a fim de reduzir possíveis riscos.

Devem ser instituídos controles apropriados em todos os dispositivos e sistemas da cooperativa para reduzir os riscos dos seus ativos de informação, como por exemplo, nas estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico, nos sistemas desenvolvidos pela cooperativa ou por terceiros.

Demandas relacionadas à Lei Geral de Proteção de Dados Pessoais (LGPD), possuem um canal próprio de comunicação:

E-mail do DPO responsável pelas cooperativas: dpo@fencom.coop.br.

5. INDICADORES

NA

6. REFERÊNCIAS

Não se aplica

7. REGISTROS

NA

8. HISTÓRICO DAS ALTERAÇÕES

VERSÃO	ITEM	NATUREZA DAS ALTERAÇÕES
01	Todos os itens e Cabeçalho	. Descrição de todos os itens . Inserção de dados de elaboração e nº da versão da POI
02	Rodapé	. Atualização para versão correta do rodapé

9. ANEXOS

NA