SISTEMA FECOMÉRCIO/SESC/SENAC RIO GRANDE DO SUL

Política de Segurança da Informação/PSI

2022

Versão 7

Sumário

APRESENTAÇÃO

Em uma economia baseada em dados e cada vez mais digital, o modo como as empresas gerenciam suas informações e seu conhecimento revela-se um fator muito importante para o sucesso dos negócios. Da mesma forma, a proteção à privacidade dos dados de clientes, colaboradores, parceiros e demais stakeholders é fundamental para a criação de um ambiente de negócios seguro, confiável e próspero. O Sistema Fecomércio/Sesc/Senac RS entende que a informação, os dados e o conhecimento são ativos de grande valor e essenciais a qualquer processo de negócio, devendo, portanto, ser gerenciados, controlados e protegidos de forma eficaz a fim de assegurar a continuidade do negócio, minimizar riscos, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

Logo, faz-se necessária a implementação de medidas e soluções de segurança da informação que se baseiem nos princípios da confidencialidade, integridade, disponibilidade e autenticidade que busquem prevenir a empresa de acessos indesejados, fraudes ou perda de informações. A Política de Segurança da Informação (PSI) é um documento que define o conjunto de normas, métodos e procedimentos, os quais devem ser comunicados a todos os funcionários. Por ser um “documento vivo”, a PSI é analisada, testada e revisada periodicamente para que reflita as práticas de gestão de segurança da informação necessárias à organização em seu contexto de tempo e espaço.

Paulo Fernando de Lucca Candia

Gerente da NTI – Fecomércio / Sesc / Senac

TERMOS E DEFINIÇÕES

NTI – Núcleo de Tecnologia da Informação.

BACKUP - Refere-se à cópia de dados de um dispositivo para o outro com o objetivo de posteriormente recuperar estes dados, caso haja algum problema. É também conhecido pelo termo “cópias de segurança”.

Disponibilidade – Garantia de que a informação deve estar disponível quando requisitada por pessoas autorizadas.

Integridade – Garantia de que a informação deve ser verdadeira, garantir que a mesma se mantenha íntegra a sua origem antes de repassá-la ou tomá-la como verdade.

Confidencialidade - Garantia de que a informação esteja acessível somente a pessoas autorizadas.

Autenticidade – Garantia que a informação recebida provém de uma fonte conhecida e se a mesma é confiável.

Correio eletrônico - Meio de comunicação baseado no envio e na recepção de mensagens via rede de computadores.

Datacenter - Ambiente projetado para concentrar os equipamentos de processamento e armazenamento de dados de uma empresa.

Dispositivos móveis - Quaisquer equipamentos eletrônicos portáteis para processamento de dados, armazenamento e comunicação, como notebooks, tablets, smartphones e consoles portáteis.

TI - Tecnologia da Informação

1. INTRODUÇÃO

Segurança da informação é o termo que descreve o conjunto de controles utilizados para a proteção das informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização.

São características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade e autenticidade, não estando está segurança restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento.

Este documento estabelece um conjunto de diretrizes que possibilitam as partes interessadas adotarem padrões de comportamento adequados com relação à utilização e preservação das informações. Foi elaborado pela NTI – Núcleo de Tecnologia da Informação com base nas melhores práticas do mercado de TI.

1.1. Objetivo

Disseminar aos usuários a regras para utilização dos recursos de Tecnologia da Informação e orientá-los a utilizar esses recursos de maneira adequada.

1.2. Abrangência

A Política de Segurança da Informação do Sistema Fecomércio/Sesc/Senac-RS aplica-se a todos os usuários, sejam eles colaboradores, prestadores de serviços, consultores, temporários e estagiários que estejam a serviço da instituição, incluindo toda a mão de obra terceirizada ou disponibilizada mediante convênios, parcerias ou quaisquer outras formas de atuação conjunta com outras empresas.

Para este documento, consideram-se recursos de Tecnologia da Informação equipamentos, instalações e recursos de informação direta ou indiretamente administrados, mantidos ou operados pelo Sistema Fecomércio/Sesc/Senac-RS.

1.3. Validade

Esta versão da Política de Segurança da Informação entra em vigor em 01/01/2022 e possui validade indefinida, podendo ser substituída por uma versão atualizada sempre que for necessário.

1.4. Divulgação

A divulgação da política deve ser clara e ampla para que todos os usuários tenham acesso e possam compreendê-la.

2. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

2.1 Classificação da informação

A Política de Segurança da Informação é aplicável a todas as informações sob gestão do Senac-RS, incluindo aquelas que são:

- Armazenadas e transmitidas por meios eletrônicos (correio eletrônico, mensagem de texto, fax e afins);
- Armazenadas em qualquer tipo de mídia (pendrive, câmeras digitais, DVD, CD e afins);
- Transmitidas em conversas formais e informais;
- Impressas ou escrita em papel.

A gestão da informação no Sistema Fecomércio/Sesc/Senac-RS prima pela transparência, tanto em âmbito interno como em âmbito externo. Entretanto, algumas informações, seja no ato de sua geração, guarda, uso, transparência ou destruição – por seu imediatismo, cunho técnico relacionado a projetos específicos e/ou provenientes dos sistemas de informação, diretórios de rede e banco de dados aos quais o usuário em geral tenha conhecimento por força das atividades profissionais – deverão ser tratadas, manuseadas, preservadas e gerenciadas adequadamente. As informações confidenciais e sigilosas só devem ser acessadas mediante solicitação de acesso de seu gestor imediato junto ao Núcleo de Tecnologia da Informação.

Todos os colaboradores têm a obrigação de cumprir, na íntegra, a Política de Segurança da Informação, servindo como exemplo de conduta em todas as situações vividas na Instituição, observando as regras estabelecidas.

2.2 REGRAS/RESPONSABILIDADES GERAIS

É de responsabilidade de todos o controle sobre a segurança das informações armazenadas nos equipamentos que estão sob seu poder, dentro da estrutura física e lógica do Sistema Fecomércio/Sesc/Senac-RS.

Os acessos realizados no ambiente informatizado através da utilização dos seus usuários e senhas de acesso, devendo sempre manter o sigilo sobre as informações e dados do Sistema Fecomércio/Sesc/Senac-RS. Usuário e senha são de uso pessoal e intransferível.

O usuário deverá solicitar permissão sempre que houver a necessidade de instalação de aplicativos ou alteração das configurações dos equipamentos do Sistema Fecomércio/Sesc/Senac-RS.

São expressamente proibidas as seguintes atividades:

- Criação, modificação, execução ou retransmissão de quaisquer instruções ou programas de computador com o intuito de obter acesso não autorizado a um recurso, equivalendo, neste caso, à tentativa de "quebra" da segurança de sistemas;
- A cópia, para utilização externa, de softwares adquiridos e/ou desenvolvidos pela instituição, a menos que formalmente autorizada e justificada pela NTI;
- A utilização de softwares não homologados pela NTI;
- A utilização dos recursos de informática dentro da estrutura física e lógica do Sistema Fecomércio/Sesc/Senac-RS para fins que não sejam relacionados à sua atividade profissional.

Qualquer incidente que possa afetar a segurança da informação deverá ser comunicado imediatamente ao Núcleo de Tecnologia da Informação do Senac-RS, através da Central de Serviços na Intranet, mesmo que haja dúvida quanto às consequências.

2.2.1 Comitê de TI

Cabe ao comitê de TI:

- Propor melhorias e aprovar as Normas de Segurança da Informação;
- Avaliar orçamentos adequados para investimentos em Segurança de informação;
- Disseminar e verificar o cumprimento das diretrizes e políticas de Segurança da informação;
- Ter conhecimento sobre incidentes de Segurança da informação;
- Efetuar reuniões periódicas.

Os membros do comitê de TI estão definidos Plano Diretor de Tecnologia da Informação.

A coordenação dos trabalhos do Comitê de TI quanto a Segurança da informação está sob responsabilidade do gestor da área de TI, cujas atribuições abrangem a convocação e a realização de outros atos de suporte às atividades desenvolvidas pelo comitê, as demais atribuições são realizadas pelo escritório de segurança da informação também vinculado a área de TI.

2.2.2 Escritório de Segurança da Informação

Cabe ao escritório de segurança da informação:

- Manter e aplicar a política em todos os dispositivos de rede;

- Prover ampla divulgação da Política e das Normas de Segurança da Informação para todos os colaboradores do Sistema Fecomércio/Sesc/Senac-RS;
- Estabelecer procedimentos e realizar a gestão dos sistemas de controle de acesso à rede, incluindo os processos de concessão, manutenção, revisão e suspensão de acessos aos usuários;
- Analisar os riscos referentes à segurança da informação e apresentar relatórios relacionados a tais riscos ao Comitê de TI, acompanhado de proposta de aperfeiçoamento quando for o caso;
- Estabelecer o mecanismo de Registro de não conformidade no Relatório de Ocorrências;
- Realizar trabalhos de análise de vulnerabilidade, com o intuito de melhorar o nível de segurança dos sistemas de informação e dos demais ambientes em que circulam as informações da empresa.

2.2.3 Núcleo Jurídico

Cabe a área de Núcleo Jurídico;

- Manter as áreas informadas sobre eventuais alterações legais e/ou regulatórias que impliquem em responsabilidade e/ou ações envolvendo a gestão da segurança da informação;
- Incluir, na análise e na elaboração de contratos, sempre que necessárias cláusulas específicas relacionadas à segurança da informação, com o objetivo de proteger os interesses da empresa.

2.2.4 Proprietário da Informação:

O proprietário da informação ou dados decorrentes de suas atividades diárias são do Sistema Fecomércio/Sesc/Senac-RS conforme contrato de trabalho firmado entre empregado e empregador.

A confidencialidade da informação está sob responsabilidade de um gerente ou diretor, responsável por solicitar concessão, revisão, manutenção e cancelamento de autorizações de acesso a determinado conjunto de informações que sejam de sua responsabilidade.

Cabe ao proprietário da informação:

- Para toda a informação sobre sua custodia elaborar uma matriz que relacione cargo e função às autorizações de acesso concedidas (perfil x função);
- Autorizar à liberação de acesso a informação sob sua responsabilidade, observando a Política e as Normas de Segura da Informação;
- Reavaliar, sempre que necessário, as liberações de acesso concedidas, solicitando o cancelamento daquelas que não são mais necessárias;
- Participar da investigação de incidentes relacionados à informação sob sua responsabilidade;
- Participar, sempre que convocado, das reuniões do Comitê de TI, prestando os esclarecimentos necessários.

2.2.5 Gerentes e Diretores

- Cumprir e fazer cumprir a Política de Segurança da Informação e suas Normas e Procedimentos;
- Assegurar que suas equipes possuem acesso e conhecimento desta Política, das Normas e Procedimentos da Segurança da Informação;
- Comunicar imediatamente eventuais casos de violação de segurança da informação à área Núcleo de Tecnologia da Informação.

2.2.6 Recursos humanos

Cabe à área de Recursos humanos:

- Colher a assinatura do Termo de Responsabilidade dos funcionários e estagiários, arquivando-o nos respectivos prontuários;
- Informar, prontamente, todos os desligamentos, afastamentos e modificação no quadro de funcionários a área de TI.

3. POLÍTICA DE GESTÃO DE ATIVOS

3.1 Utilização da estação de trabalho

Cada estação de trabalho possui códigos internos que permitem sua identificação na rede. Sendo assim, tudo que for executado na estação de trabalho será de responsabilidade do usuário do equipamento. Esse tópico visa definir as regras de utilização da estação de trabalho que abrangem o login, a manutenção de arquivos no servidor e as tentativas não autorizadas de acesso.

- É recomendado encerrar ou bloquear a sessão do sistema ao se ausentar da estação de trabalho, de modo a prevenir o acesso indevido;
- O usuário deverá desligar sua estação de trabalho no final do expediente;
- A senha de acesso à estação de trabalho é de uso pessoal e intransferível, sua divulgação é vedada sob qualquer hipótese, devendo ser alterada pelo próprio usuário a cada 42 dias ou quando da suspeita de perda do sigilo;
- A senha deve ser composta com letras, números e caractere especial, além de ter no mínimo 8 caracteres e não pode ser usada na troca as 10 últimas senhas já utilizadas.
- É recomendado fazer a manutenção do diretório pessoal, evitando acúmulo de arquivos desnecessários;
- Não será permitida a instalação de programas e qualquer alteração não prevista e autorizada pelo Núcleo de Tecnologia da Informação;
- Não será permitida a abertura de recursos tecnológicos para qualquer tipo de reparo. Caso seja necessário, o reparo deverá ser solicitado ao Núcleo de Tecnologia da Informação.

3.2 Utilização da rede

O descarte de informações consideradas críticas e confidenciais deve ser feito de modo a impossibilitar a recuperação das mesmas.

Não são permitidas as seguintes atividades:

- Transmissão ou posse de Informação que contenha material obsceno, indecente, lascivo ou outro material que explícita ou implicitamente se refira à conduta sexual;
- Transmissão ou posse de Informação, que contenha linguagem profana ou constitua apologia ao fanatismo, à prática sexual ou a quaisquer formas de discriminação;
- Transmissão ou posse de Informação que ameace a integridade física, que intimide outra pessoa ou organização;
- Transmissão de Informação que implique violação de quaisquer leis ou constitua incitamento de qualquer crime;
- Violação de direitos autorais, particularmente sobre software, dados e publicações;
- Divulgação de qualquer Informação restrita ou confidencial sem a permissão de seu proprietário ou do gestor do recurso ao qual a Informação pertence;
- Jogos direcionados ao entretenimento não poderão ser acessados, gravados ou instalados no diretório pessoal do usuário, na estação de trabalho ou em qualquer outro diretório de rede;
- Alterações das configurações de rede e inicialização das máquinas, bem como modificações que possam trazer problemas.

3.3 Utilização do correio eletrônico

O correio eletrônico é instrumento essencial para comunicação corporativa e seu uso requer o estabelecimento de regras que garantam a segurança e efetividade das informações por ele vinculadas. Quaisquer comunicações não corporativas que sobrecarreguem o tráfego na rede e/ou possam causar prejuízos à instituição ou constrangimento a terceiros serão tratados.

As mensagens de correio eletrônico deverão sempre conter a assinatura do remetente com o formato padronizado pelo Núcleo de Marketing, a qual deverá ser divulgada a todos os usuários junto com as instruções para configurá-la.

3.4 Utilização de dispositivos móveis

Para estabelecer as regras de dispositivos móveis, serão considerados quanto a seu proprietário:

3.4.1 Pertencentes ao Sistema Fecomércio/Sesc/Senac-RS

- Será de responsabilidade do Núcleo de Tecnologia da Informação a configuração desses equipamentos para que estejam aptos a interagir com os demais dispositivos fixos pertencentes à rede Sistema Fecomércio/Sesc/Senac-RS. Deverão ser seguidos os mesmos critérios relativos à segurança da informação adotados para os equipamentos fixos (desktop);
- Cabe ao colaborador, usuário do dispositivo móvel, seguir os mesmos padrões de segurança adotados para os usuários de dispositivos fixos;
- Além dos procedimentos de segurança usuais para todos os equipamentos, o usuário de equipamento móvel deverá utilizar todos os meios disponíveis no equipamento destinados à proteção dos dados nele contidos, como senhas de acesso, travamentos de hardware ou outros recursos;
- No caso de conexão a uma rede externa por motivo de viagem, compete ao colaborador, além da manutenção da configuração original por meio de backup e/ou de ponto de restauração, o cuidado especial com as redes externas eventualmente utilizadas, de forma a não expor conteúdo corporativo que viole a confidencialidade;
- Preferencialmente conectar sempre os dispositivos a redes seguras privadas, protegidas por senha, evitar a utilização de redes públicas abertas.
- Os técnicos do Núcleo de Tecnologia da Informação poderão realizar, a qualquer tempo, inspeção para verificar os aspectos relativos à configuração e à segurança dos equipamentos.

3.4.2 Pertencentes a usuários e visitantes

Os usuários e visitantes poderão utilizar seus equipamentos portáteis nas dependências do Condomínio Fecomércio, escolas/unidades, com as seguintes ressalvas:

- O equipamento poderá se conectar à rede WiFi (Fecomércio - Visitantes), exclusivamente para navegação da internet, onde serão considerados todos os itens de segurança e restrições de acesso à internet contidos neste documento;
- A conexão de equipamento particular do usuário à rede do Sistema Fecomércio/Sesc/Senac-RS, só será possível após análise e autorização do Núcleo de Tecnologia da Informação, ressalvados todos os itens de segurança estabelecidos neste documento.

3.5 Acesso à internet

Conforme Política de rede sem fio, não são permitidas as seguintes atividades:

- Download de arquivos de músicas, filmes, jogos e outros que não tenham relação direta com a função desempenhada e as necessidades da instituição;
- Acesso a sites com conteúdo impróprio;
- Utilização de softwares de compartilhamento de arquivos, gerenciadores de downloads (bloqueados) ou de mensagens instantâneas (exceto o de uso corporativo ou liberado pelo gestor imediato);
- Utilização de sites de serviços de vídeo e/ou música on-line;
- Utilização de sites de serviços de jogos ou de entretenimento;
- Utilização de sites de serviços de relacionamento pessoal.

Todos os acessos a sites ficam registrados no servidor de internet e são monitorados mensalmente, sendo que a qualquer momento podem ser auditados com emissão de relatórios por usuário e/ou por equipamento, conforme solicitação. Salientamos que esta é uma ferramenta de aprendizado e trabalho, portanto passível de auditoria.

A liberação de acesso a sites de relacionamento pessoal, mensagens instantâneas ou entretenimento para ensinamento em cursos promovidos pelas unidades, deverá ser feita mediante autorização do gestor através de registro de serviço na Central de Serviços do NTI na intranet com antecedência de 48 horas antes da realização do primeiro acesso ao site. O gestor estará ciente dos riscos inerentes a esta liberação como internet mais lenta, riscos de entrada de vírus e acesso indireto a conteúdos maliciosos.

3.6 Acesso aos sistemas informatizados

Este tópico visa definir as regras de utilização dos sistemas informatizados que abrangem seu acesso e uso.

- Os sistemas informatizados devem ser acessados somente por necessidade de serviço ou por determinação expressa do superior hierárquico, realizando as tarefas e operações em estrita observância aos procedimentos, às normas e disposições contidas na legislação;

- As senhas de acesso aos sistemas informatizados deverão ser mantidas em caráter confidencial e intransferível;
- Os usuários serão responsáveis pelos acessos realizados com o login que lhes forem atribuídos. No caso de empresas terceiras, essa responsabilidade será do gestor da área contratante, isto é, que utiliza os serviços contratados. É de responsabilidade do usuário cuidar da integridade, confidencialidade e disponibilidade dos dados, informações e sistemas aos quais tem acesso, devendo comunicar por escrito, ao gestor imediato, quaisquer indícios ou possibilidades de irregularidades, de desvios ou falhas identificadas, sendo proibida a exploração de falhas ou vulnerabilidade porventura existentes nos sistemas;
- Não é permitido o acesso aos sistemas com fins escusos ou imotivados.

3.7 Acesso ao Data Center

O acesso ao Data Center Site A localizado no Condomínio da Fecomercio e ao data center Site B localizado na Avenida Alberto bins,665, é restrito aos técnicos do Núcleo de Tecnologia da Informação ou de pessoas acompanhadas por estes.

As unidades e faculdades que possuírem um rack central, o acesso à sala é restrito aos diretores, técnicos do Núcleo de Tecnologia da Informação, Facilitador de TI ou de pessoas acompanhadas por estes.

3.8 Senhas

O usuário não deve divulgar suas senhas, já que servem como assinatura eletrônica, responsabilizando dessa maneira seu usuário pelas atividades desenvolvidas quando conectado na rede/servidor. Em caso de suspeita da perda de sigilo, as senhas devem ser trocadas imediatamente, na ocorrência de (5) cinco erros consecutivos, os acessos serão temporariamente bloqueados.

Não devem ser adotados para senhas: datas, nomes próprios, palavras do vocabulário e siglas. As mesmas devem ser compostas de uma combinação alfanumérica optando entre caracteres especiais ou letras maiúsculas e minúsculas, tendo no mínimo 8 (oito) caracteres.

As senhas devem ser trocadas a cada 42 dias, sem repetição das últimas cinco.

3.9 Backup

Conforme estabelecido na Política de Backups, os backups dos servidores do Datacenter são de responsabilidade do Núcleo de Tecnologia da Informação.

O backup das informações contidas nas estações de trabalho é de responsabilidade de cada usuário, o Núcleo de Tecnologia da Informação recomenda que nenhuma informação deixe de estar no servidor de dados, mesmo se estiver sendo alterado.

Os backups deverão ser objeto de testes periódicos com a simulação de restauração de dados em ambiente teste e, caso sejam detectados quaisquer defeitos, deverão ser imediatamente identificados e solucionados.

No servidor de dados, o procedimento de cópia será realizado de forma automática em horários pré-determinados.

4. PENALIDADES

O não atendimento aos requisitos previstos nesta Política de Segurança da Informação será considerado violação às regras internas do Sistema Fecomércio/Sesc/Senac-RS.

Toda violação ou desvio caracteriza infração funcional. O infrator ou facilitador, seja por ação ou omissão, estará sujeito a medidas administrativas e legais cabíveis.

5. MONITORIA E AUDITORIA DO AMBIENTE

O Núcleo de Tecnologia da Informação dispõe de recursos que poderão registrar e controlar a utilização dos sistemas e serviços disponibilizados, incluindo acesso à internet, visando garantir a disponibilidade e segurança das informações institucionais.

6. CONSIDERAÇÕES FINAIS

Este documento deverá ser amplamente divulgado a todos os usuários e será obrigatório o aceite do mesmo no primeiro acesso à intranet da instituição.

É importante que todos estejam cientes de que os ambientes, sistemas, computadores e rede da instituição poderão ser monitorados e gravados, conforme previsto nas leis brasileiras.

Em caso de dúvida quanto ao uso e/ou descarte de informações, deverá ser obtida a orientação necessária com o Núcleo de Tecnologia da Informação, através da Central de Serviços na Intranet.

7. REFERÊNCIAS

SENAC. DN. **Política de Segurança da Informação do Departamento Nacional do Senac**, de outubro de 2013. Rio de Janeiro, 2013.