POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS/ PSIPD DO SESC PR

VERSÃO 1.0

PALAVRA DO PRESIDENTE

Em meados de 2005, quando assumimos o nobre encargo da Presidência da Fecomércio PR, do Sesc PR e do Senac PR, comprometemo-nos a realizar as mudanças organizacionais necessárias para elevar estas entidades a um novo patamar no estado do Paraná. Desde então, implantamos novos programas de trabalho com o propósito de racionalizar os recursos, aperfeiçoar os controles internos, expandir e atualizar a infraestrutura e oferecer serviços de excelência à nossa clientela, razão de nossa existência.

Dentre as mudanças, destacamos a implantação do Programa de Compliance das Entidades, com a publicação de atos normativos e adoção de atitudes permanentes de postura ética, compreensão e lisura de nossa atuação, seja ela por servidores, dirigentes, licitantes, fornecedores, contratados e conveniados, e nossa clientela, sempre voltadas para a absoluta transparência e respeito à legalidade e fidelidade no cumprimento de nossas missões finalísticas.

Assim é que, agora, lançamos esta POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS das três entidades, necessária para impor condutas que salvaguardem as informações organizacionais e os dados pessoais de nossos dirigentes, empregados, fornecedores e clientes.

Os valores de retidão, justiça e integridade sempre permearam as ações institucionais da Fecomércio PR, do Sesc PR e do Senac PR, e este documento demonstra o efetivo comprometimento de suas altas administrações em agir em conformidade com a Lei e estabelecer boas práticas de gestão, permitindo, assim, o constante avanço e crescimento histórico das nossas organizações.

DARCI PIANA
Presidente

PALAVRA DO DIRETOR REGIONAL

O Sesc está constantemente comprometido com a cultura da excelência na prestação dos seus serviços nas áreas de Educação, Cultura, Saúde, Lazer e Assistência para os trabalhadores do comércio de bens, serviços e turismo e seus dependentes, de todos os municípios do Paraná.

E para que essas atividades sejam realizadas com profissionalismo, ética e eficiência, a Entidade tem feito relevantes investimentos em Tecnologia da Informação (TI) e implantando soluções tecnológicas aos seus produtos e serviços.

Essas mudanças tecnológicas impactaram na quantidade significativa de dados e documentos que são produzidos no Sesc PR, sobretudo eletronicamente, impondo o dever à Entidade de adotar métodos e controles rígidos, que garantam a correta coleta, manuseio, tratamento e proteção das valiosas informações organizacionais de que dispomos.

Além disso, o Sesc PR reconhece a importância da recente Lei Geral de Proteção de Dados Pessoais e o seu impacto social nas relações com seus clientes, servidores e fornecedores, comprometendo-se publicamente com a proteção dos direitos fundamentais de liberdade e de privacidade e livre desenvolvimento da personalidade da pessoa natural.

Por tais motivos, o Sesc PR torna pública sua Política de Segurança da Informação e Proteção de Dados (PSIPD), contendo diretrizes de condutas adequadas e seguras para todos que tratem qualquer tipo de informação organizacional, a fim de preservar os dados contra ameaças e ataques.

Este documento é fruto da criação colaborativa e participativa de servidores e dirigentes do Sesc PR, Senac PR e Fecomércio PR, em permanente apoio à alta administração.

As diretrizes do documento devem ser seguidas por todos, custodiantes de informações e clientes, no que couber, incumbindo a todos a conscientização, a responsabilidade e o comprometimento na aplicação desta PSIPD, para a efetiva salvaguarda das informações necessárias ao cumprimento de nossas nobres finalidades.

EMERSON SEXTOS
Diretor Regional

SUMÁRIO

1. INTRODUÇÃO

O propósito deste documento é estabelecer e apresentar diretrizes de condutas adequadas de Segurança da Informação e Proteção de Dados do **SERVIÇO SOCIAL DO COMÉRCIO | SESC – ADMINISTRAÇÃO REGIONAL NO ESTADO DO PARANÁ**.

A Política de Segurança da Informação e Proteção de Dados (PSIPD) atende às boas práticas de mercado, visa orientar os servidores, alunos, fornecedores e demais que se relacionem com o Sesc PR, bem como define as diretrizes, as normas e os procedimentos de segurança das informações institucionais.

2. OBJETIVO

A Política de Segurança da Informação e Proteção de Dados (PSIPD) do Sesc PR tem por objetivo instituir diretrizes estratégicas, mecanismos e controles que visam garantir atitudes adequadas para manuseio, tratamento, controle e proteção dos dados, informações, documentos e conhecimentos produzidos e armazenados, sob guarda ou transmitidos, por qualquer meio ou recurso, contra ameaças e vulnerabilidades.

Desse modo, a PSIPD busca preservar os ativos de informação, reduzir riscos de ocorrência de perdas e alterações desses, bem como de acessos indevidos a informações da Entidade e, sobretudo, preservar a imagem institucional do Sesc PR.

A finalidade desta Política é preservar as informações no que diz respeito à:

- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Integridade**: garantia de fidedignidade e autenticidade das Informações. Propriedade que garante a não violação das informações com intuito de protegê-las contra alteração, gravação ou exclusão indevida, acidental ou proposital.
- **Disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário.

3. REQUISITOS PARA IMPLEMENTAÇÃO DA PSIPD

- Ter o apoio da autoridade competente da Entidade para implantação desta PSIPD.
- Criar grupo de trabalho ou comitê multidisciplinar para dirimir questões relacionadas à PSIPD.
- Alinhar a PSIPD à natureza e finalidade institucionais.
- Dar plena publicidade à PSIPD, seja para o público interno (conselheiros, dirigentes, servidores) quanto ao público externo (clientes, fornecedores e demais titulares de dados).

4. ABRANGÊNCIA

A presente Política de Segurança da Informação e Proteção de Dados (PSIPD) alcança todos os processos que tratam ativos de informação do Sesc PR, digitais e analógicos, que se relacionam à Entidade e a dados dos seus titulares.

Portanto, aplica-se a todas as pessoas que trabalham no Sesc PR, sejam servidores, estagiários, dirigentes, bem como a qualquer pessoa física ou jurídica, de Direito Público ou Privado, com quem a Entidade mantém relacionamento, dentre os quais: fornecedores, prestadores de serviço, contratados e conveniados em geral e clientes.

5. REFERÊNCIAS

Esta Política foi desenvolvida tendo como suporte as seguintes normas:

- Norma ABNT NBR ISO/IEC Família 27000: Sistema de Gestão de Segurança da Informação (SGSI).
- Decreto-Lei nº 5.452, de 1º de maio de 1943: aprova a Consolidação das Leis do Trabalho (CLT).
- Lei Geral de Proteção de Dados Pessoais (LGPD): Lei nº 13.709/2018.
- Lei de Diretos Autorais: Lei nº 9.610/1998.
- Normativos próprios do Sesc PR, Decreto-Lei nº 9.853/1946 e Decreto-Lei nº 61.836/1967.

Esta Política deverá ser lida e interpretada juntamente com as seguintes normas do Sesc PR:

- Regulamento Interno de Segurança da Informação e Proteção de Dados (RISIPD).
- Código de Ética, para servidores e dirigentes.
- Código de Conduta Ética, para fornecedores e conveniados.
- Política de Privacidade.
- Política de Cookies.

6. DIRETRIZES GERAIS

6.1 Comitê de Segurança da Informação e Proteção de Dados

O **Comitê de Segurança da Informação e Proteção de Dados** é o órgão responsável pela aplicação desta Política na Entidade, autônomo em decisões de sua alçada, de caráter multiprofissional, vinculado diretamente à Direção Regional. Sua composição, organização e funcionamento estão previstos no Regimento Interno do Comitê de Segurança da Informação e Proteção de Dados.

6.2 Proteção da Informação

As diretrizes de segurança da informação e proteção de dados estabelecidas nesta PSIPD se aplicam às informações originadas em papel e em meio digital, as convertidas para papel e meio digital, faladas, armazenadas, acessadas, produzidas, utilizadas, editadas, recebidas e transmitidas pela Entidade. Essas diretrizes devem ser seguidas pelos usuários, os quais deverão atuar com responsabilidade e de acordo com o previsto nesta PSIPD.

Toda informação relacionada às operações da Entidade, gerada ou desenvolvida nas dependências da Entidade, físicas e virtuais, constitui ativo desta, independente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada.

A informação deve ser utilizada unicamente para a finalidade para a qual foi autorizada e estritamente para o propósito institucional.

É diretriz que toda informação de propriedade da Entidade deva ser protegida de riscos e ameaças, que possam comprometer a confidencialidade, a integridade, a disponibilidade ou a autenticidade destas, através de medidas técnicas e administrativas tais como: perfis de acesso, controle de senhas, troca de senhas, armários com chaves, dentre outros.

Para consolidar a proteção da informação, garantir sua disponibilidade e segurança das informações tratadas, a Entidade, por meio das respectivas áreas responsáveis pelos procedimentos, sistemas, serviços e utilização destes, deve estabelecer, cumprir e fazer cumprir os procedimentos da PSIPD, do RISIPD e demais normativos internos.

6.3 Confidencialidade de Dados e Informações

O Sesc PR obriga-se a preservar a confidencialidade dos dados cadastrais e pessoais dos servidores, clientes, fornecedores, parceiros e conveniados, e os utilizará tão e somente para propósitos legítimos e específicos, de modo adequado e conforme as necessidades institucionais, utilizando-se das medidas técnicas e administrativas para proteger tais dados, de acordo com a presente Política de Privacidade da Entidade e pela Lei Geral de Proteção da Dados (LGPD).

São consideradas informações confidenciais, para os fins desta Política, as descritas no parágrafo anterior, bem como quaisquer informações não disponíveis ao público ou reservadas, tais como dados, especificações técnicas, desenhos, manuais, esboços, modelos, amostras, materiais promocionais, projetos, estudos, documentos e outros papéis de qualquer natureza, tangíveis ou em formato eletrônico, arquivos em qualquer meio, programas e documentação de computador, comunicações por escrito, verbalmente ou de outra forma reveladas para a Entidade.

O usuário que receber informações confidenciais deverá mantê-las e resguardá-las em caráter sigiloso, bem como limitar seu acesso, controlar cópias de documentos, dados e reproduções que porventura sejam extraídas da mesma, sob pena de se responsabilizar pelo seu uso indevido. Dados considerados sensíveis e de menores devem ter atenção redobrada.

Nenhum dado ou informação confidencial pode ser compartilhado com terceiros, interna ou externamente à Entidade, sem consentimento por escrito da Entidade, sob pena de aplicação das sanções previstas no item 6.5 desta Política.

6.4 Responsabilidades

É missão e responsabilidade de cada servidor, estagiário, dirigente, bem como de qualquer pessoa física ou jurídica, de Direito Público ou Privado, com quem a Entidade mantém relacionamento: fornecedores, prestadores de serviço, contratados e conveniados em geral, clientes, dentre outros, observar e seguir as políticas, padrões, procedimentos e orientações estabelecidas para o cumprimento da presente PSIPD.

É imprescindível que cada envolvido compreenda o papel da segurança da informação e proteção de dados pessoais em todas as suas atividades prestadas para a Entidade, que devem respeitar a legislação vigente e a normatização proposta por órgãos e entidades reguladoras, com relação à segurança dos dados e informações.

É também obrigação de cada usuário manter-se atualizado em relação a esta PSIPD e aos procedimentos e normas relacionadas, buscando orientação do seu gestor sempre que não estiver absolutamente seguro quanto à aquisição, uso, tratamento e/ou descarte de informações.

Para auxiliar todos os envolvidos, o Comitê de Segurança da Informação e Proteção de Dados da Entidade é responsável por gerenciar as políticas e padrões que apoiam a todos na proteção dos ativos de informação e proteção de dados, além de auxiliar na resolução de problemas relacionados ao tema e disseminação do conteúdo desta PSIPD.

6.5 Descumprimento e Sanções

As violações de segurança devem ser imediatamente informadas ao Comitê de Segurança da Informação e Proteção de Dados da Entidade, as quais serão apuradas nos termos dos normativos internos, garantida a ampla defesa e contraditório de todos os envolvidos, com vistas à adoção das medidas necessárias, inclusive a correção da falha, se houver, ou reestruturação de processos.

O descumprimento das diretrizes desta PSIPD e a violação de normas derivadas da mesma sujeitam os envolvidos, além das sanções disciplinares cabíveis, inclusive, à rescisão do contrato de trabalho, se servidor for, e à eventual responsabilização civil e criminal.

7. DIRETRIZES ESPECÍFICAS

7.1 GESTÃO DE ATIVOS

O usuário deve ter acesso apenas aos ativos necessários e indispensáveis ao seu trabalho ou atividade, respeitando as recomendações técnicas, comportamentais e de sigilo específicas aplicáveis, constantes no Regulamento Interno de Segurança da Informação e Proteção de Dados (RISIPD) da Entidade.

Como condições gerais para a gestão e o uso aceitáveis dos ativos de informação e dados dos titulares, esta PSIPD considera:

7.1.1 Acessos e Recursos de Rede

I. O acesso e o uso de todos os sistemas de informação, pastas de rede, bancos de dados e demais recursos (computadores, servidores de documentos e arquivos, impressoras, câmeras de vídeo, telefones, sistemas de videoconferência e audioconferência) devem ser restritos a pessoas expressamente autorizadas, de acordo com a necessidade para o cumprimento de suas atividades laborais e durante o exercício das mesmas nos ambientes da Entidade (físicos ou virtuais) ou externos a ela.

II. O acesso a dados, informações, sistemas, serviços e redes, seja nos ambientes da Entidade (físicos ou virtuais) ou externos a ela, via VPN, ou rede particular quando se aplicar, deve ser solicitado e/ou revogado conforme regras estabelecidas no RISIPD da Entidade.

III. Todo acesso será monitorado e se verificada a ocorrência de acessos desnecessários ou com poder excessivo, estes serão imediatamente revogados. A concessão de acesso às informações e sistemas deve ser autorizada com base na regra de mínimo acesso necessário para o desempenho da função.

IV. Acessos fornecidos sob a forma de login (usuário e senha), seja para acesso à rede corporativa, e-mail, sistemas, entre outros, sempre deverão ser realizados através de uso de senhas sigilosas. Senhas são de uso pessoal e intransferível, tendo sua divulgação e compartilhamento vedados sob qualquer hipótese, devendo ser alterada conforme as regras estabelecidas no RISIPD.

V. A área técnica responsável da Entidade poderá bloquear o login de qualquer usuário, no caso de suspeitas de vazamento de senhas ou de tentativas consecutivas de violação de acesso.

VI. Concessão e revogação de acessos para servidores, estagiários, dirigentes, bem como qualquer pessoa física ou jurídica, de Direito Público ou Privado, com quem a Entidade mantém relacionamento: fornecedores, prestadores de serviço, contratados e conveniados em geral e clientes, terão suas regras descritas no RISIPD.

7.1.2 Correio Eletrônico (e-mail) e Sistemas de Mensageria e de Correspondências

I. A Entidade fornecerá, a seu critério exclusivo, o acesso às plataformas digitais e correio eletrônico (e-mail) ao servidor, com o respectivo domínio, em sua admissão através de perfis de acessos previamente definidos, baseados em cargos e funções.

II. Por quaisquer meios de correio eletrônico, e-mail, mensageria e correspondência, o usuário é responsável pelas informações recebidas, enviadas e compartilhadas, bem como pela sua guarda, confidencialidade e publicidade.

III. As plataformas de colaboração, correio eletrônico e mensageria disponibilizadas pela Entidade deverão ser utilizadas para fins corporativos e relacionados às atividades do servidor, enquanto se mantiver o vínculo empregatício. A utilização desses serviços para fins pessoais fica limitada ao contido no Código de Ética da Entidade.

IV. As mensagens de correio eletrônico sempre deverão incluir assinatura conforme o padrão estabelecido pela Entidade.

V. É obrigatória a manutenção da caixa de e-mails pelo respectivo usuário, evitando acúmulo de e-mails e arquivos desnecessários.

VI. O uso dos recursos de correio eletrônico, bem como o conteúdo das mensagens poderão ser vistoriados por amostragem, estando a Entidade autorizada a ler, copiar, e/ou bloquear mensagens que violem as normas estabelecidas nesta PSIPD, no RISIPD, Código de Ética, e os interesses da Entidade.

VII. É importante verificar o uso da ferramenta para que o envio de mensagens não seja caracterizado como SPAM, lixo eletrônico ou malware, abstendo-se de:

- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação.
- Produzir, transmitir ou divulgar mensagem que não estejam de acordo com o Código de Ética da Entidade e/ou com a legislação vigente.
- Enviar mensagens contendo material protegido por direitos autorais sem a permissão do detentor dos direitos.
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas na legislação vigente ou ato normativo interno.

7.1.3 Internet (Rede Mundial)

I. Qualquer informação que for acessada, transmitida, recebida ou produzida na internet estará sujeita a divulgação e auditoria. Portanto, a Entidade reserva-se o direito de monitorar e registrar todos os acessos à internet.

II. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da Entidade, que analisará e, se necessário, bloqueará qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em unidade de armazenamento de dados local, na estação de trabalho, ou em áreas privadas da rede, visando assegurar o cumprimento desta PSIPD.

III. É proibido o acesso a sites da internet ou quaisquer arquivos digitais, bem como sua produção e propagação, que desrespeitem o Código de Ética da Entidade, possuam conteúdo ilegal, pornográfico, preconceituoso, racista, bem como objetos, fatos, imagens, conceitos, opiniões e outros que possam disseminar o ódio e a violência e influenciar atitudes alheias aos interesses da Entidade, expondo pessoas físicas ou jurídicas, produtos, marcas ou assemelhados à exposição pública, calúnia, injúria e/ou difamação.

7.1.4 Dispositivos de Acesso (Computadores, Notebooks, Smartphones e ou dispositivos similares), Móveis e Mídias Removíveis

I. A Entidade, na qualidade de proprietária dos dispositivos fornecidos aos usuários, reserva-se o direito de inspecioná-los a qualquer tempo, sendo de incumbência da área técnica responsável da Entidade realizar o controle e supervisão do uso dos mesmos dispositivos.

II. O usuário do dispositivo mantido pela Entidade e utilizado para fins corporativos é responsável por sua conservação, segurança, bloqueio de acesso por meio de senhas e/ou outros recursos, cópia de segurança dos dados, e notificação do seu gestor imediato e área técnica responsável e de infraestrutura e patrimônio da Entidade em caso de extravio, furto, roubo ou danos.

III. Não é permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área técnica responsável da Entidade.

IV. Os dispositivos móveis devem ser controlados e supervisionados pela área técnica responsável da Entidade, sendo ao usuário confiado o responsável e correto uso, guarda e segurança do mesmo.

V. O uso de mídias removíveis (cartões de memória, disquetes, pen drive, pen USB e similares) não é recomendado, pois trata-se de uma das maiores fontes de ameaças a vulnerabilidades, tanto no sentido de injetar ataques cibernéticos na Rede Corporativa, bem como fontes de vazamento de informações. Contudo, caso seja imprescindível a utilização das mesmas, atuar com toda a cautela possível e, quando estas não forem mais necessárias, deverão ser descartadas de forma segura e protegida.

7.1.5 Computação em Nuvem

O uso das "plataformas de nuvem" para transmissão e armazenamento de informações só poderá ocorrer nas plataformas formalmente contratadas pela Entidade e disponibilizadas pela área técnica responsável.

7.1.6 Redes e Mídias Sociais

I. O uso das redes e mídias sociais institucionais, por parte dos servidores, deve ser regido pelas determinações contidas nesta PSIPD, no Manual de Mídias Sociais e por outras normativas a ela complementares.

II. A gestão dos perfis institucionais da Entidade nas redes sociais deve ser realizada por servidores competentes e/ou por terceirizados contratados para tal, devidamente autorizados, identificados e instruídos de forma a preservar a imagem institucional, sendo vedado aos demais servidores a criação de perfis em nome da Entidade.

III. Quanto ao conteúdo das publicações nas redes e mídias sociais, fica vedado divulgar informações sigilosas e internas da Entidade ou da vida pessoal e profissional de qualquer pessoa física sem a devida autorização; difamar pessoas ou divulgar assuntos que venham prejudicar a imagem da Entidade ou de terceiros; discriminar e compartilhar temas que venham prejudicar pessoas ou grupos de pessoas, por qualquer motivo.

IV. A Entidade detém legalmente a propriedade intelectual e os direitos autorais de suas obras e criações, composta sobretudo por bens imateriais, tais como marcas, obras intelectuais, nomes empresariais, fotografias e obras audiovisuais, as quais somente podem ser divulgadas nas redes e mídias sociais ou em quaisquer outros meios, para fins profissionais, sendo vedado o uso para fins particulares.

7.1.7 Dados e Informações

I. A Entidade preservará a confidencialidade dos dados cadastrais e pessoais dos seus titulares e os utilizará tão somente para propósitos legítimos e específicos, de modo adequado e conforme as necessidades institucionais, utilizando-se das medidas técnicas e administrativas aptas a proteger tais dados pessoais.

II. A Entidade decidirá sobre o compartilhamento ou restrição de acesso aos dados e informações, sob sua gestão, bem como adotará meios de monitoramento do uso dos seus dados.

III. Cabe ao usuário da informação tratar as informações que estejam sob seus cuidados com zelo e de acordo com os princípios desta PSIPD e jamais, sob qualquer fundamento, tentar acessar informações e dados sem autorização para fazê-lo e sem correlação com suas funções laborais.

IV. Cabe ao usuário da informação documental proceder a guarda dos documentos que estejam sob seus cuidados em locais seguros durante o expediente, enquanto estiver manuseando e ao final do dia de trabalho.

V. Cabe à Entidade adotar e manter Inventário de Dados e/ou Ativos de Informações, bem como os normativos internos relacionados.

VI. Cabe à Entidade estabelecer condições para transferência segura de informações a partes externas, prevendo responsabilidades aos usuários que exercerem atividades de tratamento de dados pessoais, observando os seguintes processos:

- Controle e notificação de transmissões de dados pessoais.
- Procedimentos para assegurar a rastreabilidade dos eventos e o não repúdio.
- Normas para identificação de portadores.
- Notificação e registro de incidentes de segurança da informação, como perda de dados.
- Utilização de um sistema acordado de identificação para informações críticas e sensíveis, garantindo que a informação esteja devidamente protegida.

7.1.8 Guarda de Informações Digitais (Backup) e Documentação Física

I. Rotinas sistemáticas de backup e guarda de informações devem ser realizadas por servidores da área técnica responsável da Entidade.

II. Cópias dos dados de produção, backup local e backup off-site devem ser produzidas, aplicando-se as melhores práticas de mercado com relação à segurança e proteção de dados.

III. Documentos imprescindíveis para as atividades da Entidade deverão ser salvos em drives de rede corporativa, viabilizando a produção de backup e guarda da informação.

IV. Documentações Físicas devem ser guardadas/arquivadas de forma segura, quer seja em ambiente interno ou externo, de acordo com os prazos previstos em lei para guarda e arquivamento de referidos documentos.

V. As cópias de segurança devem ser armazenadas em uma localidade remota, a uma distância suficiente para escapar dos danos de um eventual desastre ocorrido no local principal, bem como as mídias de backup devem ser regularmente testadas para garantir que elas são confiáveis no caso do uso emergencial.

7.1.9 Instalação de Programas (Softwares)

I. Os softwares instalados e utilizados nos equipamentos da Entidade e externos devem ser legalmente adquiridos e/ou autorizados pela área técnica responsável, mesmo que supostamente de livre uso, como aqueles usualmente classificados como “freeware”, “shareware”, “demoware”, sendo todos utilizados somente dentro do seu período de validade de licenciamento.

II. A área técnica responsável deverá realizar a gestão dos softwares instalados nas estações de trabalho e servidores da Entidade, mantendo o devido registro das licenças disponíveis.

III. O processo de homologação de software deve avaliar, sobretudo, o impacto da utilização deste na segurança da informação da Entidade e o suporte para o mesmo.

IV. É vedado efetuar réplicas dos softwares adquiridos pela Entidade, bem como promover esta prática com outros programas.

V. É vedado utilizar softwares que, por algum motivo, descaracterizem os propósitos da Entidade ou danifiquem de alguma forma o ambiente instalado.

VI. A área técnica responsável poderá remover programa de computador instalado em estação de trabalho que não se enquadre nos critérios estabelecidos nessa norma.

VII. O usuário deverá manter a configuração do equipamento disponibilizada pela Entidade, seguindo os devidos controles de segurança exigidos por esta PSIPD, pelas normas específicas da Entidade, assumindo a responsabilidade como custodiante de informações.

7.1.10 Antivírus

I. Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente de forma automática pela área técnica responsável.

II. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar imediatamente a área técnica responsável.

III. O usuário não pode, em hipótese alguma, desabilitar o programa de antivírus instalado no computador.

IV. Todo arquivo proveniente do ambiente externo (internet, e-mail, pen drive etc.) deverá ser verificado pelo antivírus, antes de ser aberto.

V. É proibida a instalação de outros sistemas de antivírus, que não sejam os fornecidos pela área técnica responsável.

7.1.11 Datacenter

I. O ambiente do Datacenter é de acesso restrito, visto que abriga equipamentos computacionais e guarda de dados pessoais e institucionais, em funcionamento ininterrupto.

II. Situações emergenciais que venham a ocorrer no extra-horário, fins de semana e feriados deverão ser comunicados à área técnica responsável imediatamente.

III. O Datacenter deve contar com proteção física contra perturbações da ordem pública, desastres naturais ou causados pelo homem. Os equipamentos devem ser protegidos contra falta e oscilações de energia elétrica e outras interrupções.

IV. Todo acesso físico ao ambiente do Data Center deve ser controlado e monitorado.

V. Somente será permitido acesso de pessoas externas ao ambiente do Datacenter por ocasião de manutenções preventivas ou corretivas, desde que acompanhadas por servidor da área técnica responsável.

7.1.12 Dispositivos de Impressão, Cópia e Digitalização

I. Todos os ativos de informação devem ser devidamente guardados, especialmente documentos em papel ou mídias removíveis da Entidade. Documentos não devem ser abandonados após a sua cópia, impressão ou utilização. Ao usar uma impressora coletiva, o usuário deverá recolher o documento impresso imediatamente.

II. As impressoras e seus respectivos suprimentos são de uso exclusivo para as atividades da Entidade.

III. Os usuários devem recolher imediatamente suas impressões, sejam elas corretas ou impressões com falhas. No caso de impressões com falhas, deverão ser descartadas de forma adequada.

IV. Impressões com falhas contendo informações sigilosas devem ser inutilizadas, tornando-as ilegíveis.

7.2 GESTÃO DE OUTROS RECURSOS DE INFORMAÇÃO

7.2.1 Estação de Trabalho

I. Nenhuma informação confidencial deve ser deixada à vista, seja em papel ou em quaisquer dispositivos, eletrônicos ou não, devendo ser adequadamente armazenada em local provido com chaves/fechaduras.

II. No caso dos computadores, notebooks ou similares, os mesmos devem ficar bloqueados, mesmo quando o usuário se ausentar por curto período de tempo, assim como os dispositivos móveis, quando necessário, devem ser guardados em local provido com chaves/fechaduras.

III. Os usuários devem devolver todos os ativos de informação da organização que estejam em sua posse, após o encerramento de suas atividades, do respectivo contrato ou acordo.

IV. No caso de baixas patrimoniais ou uso do próprio equipamento pessoal pelo servidor, deverão ser adotados procedimentos para assegurar que toda a informação relevante seja transferida para a organização e que seja apagada de forma segura do equipamento.

7.2.2 Controle de Acesso Físico

I. Todos os servidores da Entidade que transitem por ambientes administrativos do Sesc PR devem possuir identificação pessoal visível por crachás e registrados em sistema de controle de acessos.

7.2.3 Serviços Postais e de Envelopes Vai e Vem

I. Os serviços de correspondências, malote e PAC da Entidade estão disponíveis aos servidores, estagiários, dirigentes e prestadores de serviços, na proporção das respectivas autorizações pessoais de uso e deverão atender, exclusivamente, às finalidades e aos objetivos da Entidade, respeitando as medidas técnicas para proteger os dados pessoais.

II. As regras específicas sobre o tema estão disponíveis em normativo interno específico.

7.2.4 Plano de Continuidade de Negócio

I. A Entidade se compromete a elaborar e manter Plano de Continuidade do Negócio, que consiste no desenvolvimento de ações preventivas e de recuperação, através de estratégias e procedimentos, a serem adotados quando houver problemas que comprometam o andamento normal dos processos e a prestação dos serviços, a fim de minimizar possíveis riscos.

II. Cabe ao Comitê de Segurança da Informação e demais áreas de negócio da entidade dar subsídio técnicos à Alta Administração do Sesc PR, a quem compete a responsabilidade pelas tomadas de decisões estratégicas para a execução do Plano de Continuidade de Negócio, destinando orçamento necessário para elaboração, implementação, divulgação, treinamento, testes e manutenção do mesmo, bem como designando uma equipe específica para o PCN.

7.2.5 Riscos de Segurança da Informação

I. O Sesc PR compromete-se a adotar e manter processo contínuo de Gestão de Riscos de Segurança da Informação, conforme metodologia contida no Plano de Governança de Riscos, ou documento correspondente que venha a substituí-lo.

II. Os processos de segurança da informação deverão ser revistos periodicamente pelo Comitê de Segurança da Informação e Proteção de Dados da Entidade, com a participação da área técnica responsável, a fim de aperfeiçoar e agir proativamente contra riscos advindos de novas tecnologias e ameaças, objetivando a constante elaboração de planos de ação apropriados para a proteção dos seus ativos de informação.

III. Caberá aos Comitês Técnico de Riscos e Estratégico de Riscos, a criação e atualização do Plano de Tratamento de Riscos, com a participação do Comitê de Segurança da Informação e Proteção de Dados e de grupos de trabalho específicos.

8. REVISÃO

O Comitê de Segurança da Informação e Proteção de Dados do Sesc PR deverá, de ofício, avaliar a necessidade de se revisar esta política, ao menos uma vez por ano, expressando seu entendimento e sugestões no relatório de prestação de contas anual à Direção Regional.

9. TERMO DE CIÊNCIA

O Termo de Aceite à PSIPD, parte integrante da RISIPD, deve ser assinado por todos os empregados e estagiários, devendo passar a constar, inclusive, como documento do processo de admissão ou de adaptação.

Os usuários devem entender os riscos associados ao aceite da PSIPD do Sesc PR e cumprir rigorosamente o que está previsto neste documento.

Nos contratos em que se fizer necessário a concessão de acesso a ativos de informação do Sesc PR, o Aceite à PSIPD do Sesc PR será condição imprescindível para que o tal acesso seja concedido, o que será instrumentalizado por intermédio de Termo de Aceite à PSIPD, contendo cláusula de Confidencialidade das informações.

10. GLOSSÁRIO E LISTA DE SIGLAS

Os principais termos e siglas citados nesta Política incluem:

ÁREA TÉCNICA RESPONSÁVEL	Equipe e/ou setor, gerência, assessoria, coordenadoria, departamento ou divisão responsável pela gestão dos ativos de TI dentro da organização.
ATIVO	Qualquer recurso físico ou digital que tenha valor para a Entidade.
ATIVOS DE INFORMAÇÃO	Podem ser tangíveis ou intangíveis. Ativos tangíveis são ativos físicos, como documentos em papel, servidores, discos rígidos, laptops, profissionais qualificados, dentre outros. Já os ativos intangíveis, são os ativos não físicos, como dados armazenados em computadores e banco de dados, arquivos de dados, informações pessoais, arquivos de áudio, imagens e vídeos digitalizados, dentre outros.
BACKUP	Cópia de segurança, na qual são armazenados dados e informações importantes isoladamente do ambiente de produção, para recuperação futura no caso de algum problema, necessidade ou sinistro. É uma fotografia do ambiente na linha do tempo. *Backup local: armazenado nas instalações da Entidade. *Backup off-site: armazenado em instalações externas à Entidade, como por organizações terceiras em ambiente físico e/ou em nuvem.
CLT	Consolidação das Leis do Trabalho.

COMITÊ DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS	Grupo multifuncional, responsável por gerenciar as políticas e padrões que apoiam a todos na proteção dos ativos de informação na Entidade, além de auxiliar na resolução de problemas relacionados ao tema e divulgação do conteúdo dessas políticas e padrões.
COOKIES	Arquivos de texto baixados em seu dispositivo quando você visita um site. São úteis para gravar algumas preferências de acesso e para oferecer um serviço mais eficiente quando ocorrer um acesso posterior pelo titular.
CORREIO ELETRÔNICO, E-MAIL, SISTEMAS DE MENSAGERIA	Plataformas digitais que permitem compor, enviar, receber e gerenciar mensagens por meio de sistemas eletrônicos de comunicação.
DATACENTER	Ambiente no qual estão instalados servidores, equipamentos de rede como roteadores e switches, e equipamentos de armazenamento de dados.
DEMOWARE	Versão de demonstração ou de teste, de determinado software.
DISPOSITIVOS DE IMPRESSÃO, CÓPIA, DIGITALIZAÇÃO E GRAVAÇÃO	Equipamentos contendo softwares que permitem reproduzir de forma idêntica, documentos físicos e/ou digitais, incluindo sons/voz, imagens e afins quando se aplica.
DISPOSITIVOS MÓVEIS	Quaisquer equipamentos eletrônicos portáteis para processamento de dados, armazenamento e comunicação, tais como: notebooks, tablets, smartphones, consoles portáteis, câmeras fotográficas e similares.
ESTAÇÃO DE TRABALHO	Local destinado ao servidor para a execução de suas atividades laborais e contempla, além de todos os mobiliários, os equipamentos e materiais de expediente necessários para a execução das atividades de forma organizada e segura.
FREEWARE	Software distribuído gratuitamente aos usuários.
INTERNET (REDE MUNDIAL)	Várias redes de computadores interligados que utilizam um conjunto de protocolos próprios de comunicação, com o propósito de servir progressivamente o mundo inteiro, permitindo que usuários tenham acesso a vários conteúdos e informações, de outras redes corporativas e ou instituições, sendo estes conteúdos públicos, autênticos ou não.
MALWARE	Software malicioso projetado para se infiltrar em dispositivos sem o conhecimento do usuário, causando danos ao sistema ou comprometendo a segurança das informações.
PCN	Plano de Continuidade de Negócio.
PSIPD	Política de Segurança da Informação e Proteção de Dados.
REDE CORPORATIVA	Sistema de transmissão de dados e informações entre equipamentos de uma mesma corporação, tais como computadores e similares, servidores de documentos e arquivos, impressoras, câmeras de vídeo, telefones, sistemas de videoconferência, webconferência e audioconferência, podendo ou não possuir acesso à internet.

REDES E MÍDIAS SOCIAIS	Ecossistema composto por pessoas e/ou instituições que se conectam digitalmente por diferentes tipos de interesses, formando ou fortalecendo relações, e que compartilham valores, objetivos comuns e conteúdo de diferentes formatos, buscando uma identidade entre as partes, sendo as mídias sociais as plataformas onde esse compartilhamento ocorre.
RISIPD	Regulamento Interno de Segurança da Informação e Proteção de Dados.
SEGURANÇA DA INFORMAÇÃO	Esforços contínuos para a proteção dos ativos de informação, em todo o seu ciclo de vida.
SHAREWARE	Software comercial distribuído gratuitamente aos usuários, seja em um formato limitado ou como uma avaliação, que expira após um determinado número de dias.
SPAM OU LIXO ELETRÔNICO	E-mails não solicitados e/ou que podem conter malware.
TITULAR DE DADOS	Pessoa natural a quem se referem os dados pessoais que são objeto das tratativas em questão.
USUÁRIO(S)	Servidores, terceirizados, consultores, auditores, conselheiros, estagiários e visitantes que obtiveram autorização do responsável pela área interessada, de acesso e, quando pertinente, de tratamento dos ativos de informações, formalizada por meio de assinatura de um Termo de Compromisso, Sigilo e Confidencialidade.
VPN	"Virtual Private Network" (Rede Virtual Privada, em tradução livre). Trata-se de um mecanismo capaz de delimitar a comunicação entre celulares, computadores e outros aparelhos que têm acesso restrito à rede em questão, mediante uso das credenciais necessárias.

COMISSÃO ESPECIAL

REPRESENTANTES DO SENAC
Odacir Antonio Zanatta
Rogério Vosnika

REPRESENTANTES DO SESC
Zildo Costa
Paulo Salesbram

REPRESENTANTE DA FECOMÉRCIO
Luiz Sérgio Wozniaki

EQUIPE TÉCNICA

REPRESENTANTES DO SENAC
Ana Carolina Greef
Luciana Pickler
Roberto Ferrarini
Rodrigo Sepulcri Rosalem

REPRESENTANTES DO SESC
Anderson Sanchez
Joil Cezar Baptistel
Tadeu Litwin

REPRESENTANTES DA FECOMÉRCIO
Alessandra Soares Barreto
Eduardo Luiz Gabardo Martins
Fabiane Castro Schleuner

COMPOSIÇÃO DO CONSELHO REGIONAL SESC PR (2018-2022)

PRESIDENTE
Darci Piana

DIRETOR REGIONAL
Emerson Sextos

TITULARES	SUPLENTES
REPRESENTANTES DAS ATIVIDADES DE COMÉRCIO DE BENS, SERVIÇOS E TURISMO	
Eduardo Rubens de Andrade	Gelcio Miguel Schibelbein
Félix Archanjo Bordin	Beloir João Rotta
Abrão José Melhem	Emerson Alcides Veronese
Sigismundo Mazurek	Nelcir Antônio Ferro
Paulo César Nauiack	Ademar Bayer
Everton Calamucci	Paulo Salesbram
Ari Faria Bittencourt	Aída Santos Assunção
Zildo Costa	José Marioli Simão
Carlos Rodrigues do Nascimento	Ottílio Monaco
Luís Antônio Langer	José Carlos Strassi
REPRESENTANTES DAS ATIVIDADES DO SETOR DE ESTABELECIMENTOS DE SERVIÇOS DE SAÚDE	
Benno Kreisel	Marina Abe
Rangel da Silva	Mauricio Duarte Barcos
REPRESENTANTES DAS FEDERAÇÕES NACIONAIS	
Fábio Eduardo Araújo Teixeira	Jerfferson Simões
REPRESENTANTES DO MINISTÉRIO DA ECONOMIA / SECRETARIA DO TRABALHO E EMPREGO	
Paulo Alberto Kroneis	Luiz Fernando Favaro Busnardo
REPRESENTANTES DO INSTITUTO NACIONAL DO SEGURO SOCIAL	
Aldebrando Lins de Albuquerque	Antonio Marcos Ribeiro
REPRESENTANTES DAS CENTRAIS SINDICAIS	
Roni Anderson Barbosa	Juceli Pacifico
Ariosvaldo Rocha	Denilson Pestana da Costa
Flávio Bonifácio Pinto	Remi Stelmach
REPRESENTANTES DO CONSELHO REGIONAL, JUNTO AO CONSELHO NACIONAL	
Darci Piana	Sigismundo Mazurek
Ari Faria Bittencourt	Paulo César Nauiack
João Inácio Kreuz	Everton Calamucci


Sesc