RESOLUÇÃO N.º 93/2023
14 de dezembro de 2023

SESCOOP/PR
Serviço Nacional de Aprendizagem do Cooperativismo no Estado do Paraná

DISPÕE SOBRE A APROVAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS DO SESCOOP/PR E CONSOLIDA SEU TEXTO.

O Conselho Administrativo do Serviço Nacional de Aprendizagem do Cooperativismo – SESCOOP PARANÁ, em conformidade com as atribuições conferidas pelo artigo 8º. incisos I e XVIII do seu Regimento Interno:

RESOLVEU

Art. 1º - Aprovar e instituir a Política de Segurança da Informação e Proteção de Dados do Sescoop/PR, em conformidade com o texto do Anexo Único desta Resolução, como parte integrante do seu sistema de gestão institucional, compatível com os requisitos da legislação brasileira, além de boas práticas e normas internacionalmente aceitas sobre os temas relacionados à privacidade de dados pessoais.

Art. 2º - Esta Resolução entra em vigor na data de sua assinatura, revogando disposições em contrário.

Curitiba, 14 de dezembro de 2023.

(assinado eletronicamente)
JOSÉ ROBERTO RICKEN
Presidente do Sescoop/PR

SUMÁRIO

1 INTRODUÇÃO

O propósito desta Política de Segurança da Informação e Proteção de Dados (PSIPD) é estabelecer e apresentar diretrizes de condutas adequadas da Segurança da Informação e Proteção de Dados do Serviço Nacional de Aprendizagem do Cooperativismo do Estado do Paraná (Sescoop/PR).

Este documento cumpre com as boas práticas de mercado, propõe-se a orientar os conselheiros, diretores, empregados, estagiários, prestadores de serviços e público beneficiário do Sescoop/PR e demais que se relacionem com o ele, bem como define as diretrizes, as normas e os procedimentos de segurança das informações institucionais.

Esta PSIPD institui 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 Sescoop/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.

2 ABRANGÊNCIA

A presente Política de Segurança da Informação e Proteção de Dados (PSIPD) se aplica a conselheiros, diretores, empregados, estagiários, prestadores de serviços e público beneficiário do Sescoop/PR. Seu alcance abrange todos os processos que tratam ativos de informação do Sescoop/PR, digitais e analógicos, que se relacionam à Entidade e a dados dos seus titulares.

3 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; e
- Normativos próprios do Sescoop/PR, Decreto-Lei nº 8.621/1946 e Decreto-Lei nº 61.843/1967.

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

- Resolução Sescoop/PR que normatiza o uso das informações, equipamentos e estruturas de ti, e procedimentos no ambiente da tecnologia da informação; e
- Resolução Sescoop/PR que institui o Código de Ética e Conduta.

4 DIRETRIZES GERAIS

4.1 Comitê de segurança da informação e resposta à incidentes

O Comitê de Segurança da Informação e Resposta à Incidentes (CSIRI) é o órgão responsável pela aplicação desta Política na Entidade, possui caráter multiprofissional e é vinculado diretamente à Superintendência. Sua composição, organização e funcionamento estão previstos no Regimento Interno do CSIRI.

Para auxiliar a todos os envolvidos, o CSIRI da Entidade é responsável por, sem limitação, 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, sanar dúvidas e receber sugestões para melhoria desta PSIPD.

4.2 Proteção da Informação

As diretrizes de segurança da informação e proteção de dados estabelecidas nesta PSIPD se aplicam às informações que, mas não se limitando, forem geradas em meio físico e em meio digital, convertidas para meio físico 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 em conformidade com o previsto nesta PSIPD.

Toda informação relacionada às operações da Entidade, gerada ou desenvolvida nas dependências da Entidade, físicas e digitais, constitui ativo desta, independente da forma apresentada ou da unidade de registro, qualquer que seja o suporte ou formato.

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

É diretriz que toda informação de propriedade da Entidade deve ser protegida de riscos e ameaças, que possam comprometer a confidencialidade, a integridade, a disponibilidade ou a autenticidade destas, por meio 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 e demais normativos internos.

4.3 Confidencialidade de Dados e Informações

O Sescoop/PR obriga-se a preservar a confidencialidade dos dados cadastrais e pessoais dos conselheiros, diretores, empregados, estagiários, prestadores de serviços e público beneficiário, 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 PSIPD e pela Lei Geral de Proteção da Dados (LGPD).

Para fins desta política a informação será classificada como:

(a) CONFIDENCIAL: Informação sigilosa a qual o acesso é restrito a usuários autorizados; São informações de acesso restrito a um empregado ou grupo de empregados. Sua revelação

pode violar a privacidade de indivíduos, violar acordos de confidencialidade, dentre outros. Exemplos:

- Exames admissionais e demissionários;
- Processos judiciais;
- Dados pessoais de, mas não se limitando, empregados, clientes, prestadores de serviços.

(b) RESTRITA: Informações de acesso restrito a um empregado ou grupo de empregados que obrigatoriamente contam como destinatários dela, em geral, associadas ao interesse estratégico da empresa e restritas ao Conselho de Administração, Superintende, Gerentes e empregados cujas funções requeiram conhecê-las. Exemplos:

- Atas de reunião do Conselho de Administração;
- Ata de reunião do Conselho Fiscal;
- Ata de reunião do Comitê de Gestão;
- Projetos de investimentos Estratégicos;
- Planejamento Estratégico;
- Indicadores, estudos e estatísticas dos projetos de novos negócios;
- Relatórios de Auditorias Internas e Externas.

(c) INTERNA: Informações disponíveis aos empregados para a execução de suas tarefas rotineiras, não se destinando, portanto, ao uso do público externo. Exemplos:

- Comunicados, Memorandos, Padrões e Procedimentos internos;
- E-mails e lista telefônica internos;
- Avisos e campanhas internas.

(d) PÚBLICA: Informação que pode ser acessada pelos usuários da organização e o público em geral. São informações explicitamente aprovadas por seu responsável para consulta irrestrita e cuja divulgação externa não compromete o negócio e que, por isso, não necessitam de proteção efetiva ou tratamento específico. Exemplos:

- Atas de Assembleias;
- Estatuto Social;
- Código de Ética e Conduta;
- Termos de privacidade.

Cabe ao usuário verificar o nível de acesso da informação (confidencial, restrita, interna ou pública) e se possui autorização para acessá-la. A tentativa ou o acesso à informação para a qual não possui autorização, poderá acarretar a rescisão do contrato de trabalho por justa causa e a adoção de medidas judiciais cabíveis.

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 dessas informações, 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 4.5 desta Política.

A forma de tratamento da informação de acordo com a sua classificação e a sua rotulagem será tratada na Norma de Classificação da Informação.

4.4 Responsabilidade

É missão e responsabilidade dos conselheiros, diretores, empregados, estagiários, prestadores de serviços e público beneficiário do Sescoop/PR 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 se manter atualizado em relação a esta PSIPD e aos procedimentos e normas relacionadas, buscando orientação do seu gestor sempre que não estiver absolutamente seguro quanto, mas não se limitando, à aquisição, uso, tratamento e/ou descarte de informações.

4.5 Descumprimento e sanções

As violações, ou tentativas de violações de segurança devem ser imediatamente informadas ao Comitê de Segurança da Informação e Resposta a Incidentes 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 dela sujeitam os envolvidos, além das sanções disciplinares, quando cabível, à rescisão do contrato celebrado com a Entidade e à eventual responsabilização civil e criminal.

5 DIRETRIZES ESPECÍFICAS

5.1 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 nesta PSIPD.

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

5.1.1 Senhas de acesso à rede interna

I. No primeiro acesso, o usuário receberá uma senha temporária que deverá ser alterada no primeiro uso, conforme padrão determinado pela coordenação de tecnologia da informação.
II. O usuário se declara ciente que o login e a senha são de uso pessoal, intransferível e deve ser mantido sob absoluta confidencialidade; o descumprimento desta obrigação acarretará a aplicação das sanções de cunho administrativo e das medidas judiciais cabíveis.
III. Caso a senha do usuário tenha sido revelada por terceiros mal-intencionados, tenha sido esquecida ou bloqueada, deve ser aberto um chamado na área de TI por meio do seguinte canal: ticket.ti@sistemaocepar.coop.br.

IV. É proibido usar como próprio o login e senha de outro usuário ou ceder a outrem, para que dele se utilize, documento dessa natureza, próprio ou de terceiros.

5.1.2 Acessos e Recursos de rede

I. O acesso e o uso de, mas não se limitando, 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 áudio conferência) de propriedade da Entidade devem ser restritos às pessoas expressamente autorizadas, de acordo com a necessidade para o cumprimento de suas atividades laborais e durante o exercício delas 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.

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 por meio de uso de senhas sigilosas. Senhas são de uso pessoal e intransferível, tendo sua divulgação e compartilhamento vedados sob qualquer hipótese.

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 empregados, estagiários, dirigentes, bem como qualquer pessoa física ou jurídica, de Direito Público ou Privado, com quem a Entidade mantém relacionamento: fornecedores, prestadores de serviço e clientes, terão suas regras descritas no Resolução Sescoop/PR n° 37/2011.

VII. Arquivos pessoais e/ou não pertinentes ao negócio da Organização como, mas não se limitando, fotos, músicas, vídeos, não deverão ser copiados, movidos para a rede da Organização, pois podem sobrecarregar o armazenamento nos servidores e/ou rede. Caso identificada a existência desses arquivos, eles serão excluídos definitivamente, sem aviso prévio.

5.1.3 Correio eletrônico e sistemas de mensageria e correspondência

I. A Entidade fornecerá, a seu critério exclusivo, o acesso às plataformas digitais e correio eletrônico (e-mail) ao empregado, com o respectivo domínio, em sua admissão por meio 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 empregado, enquanto se mantiver o vínculo empregatício. A utilização desses serviços para fins pessoais fica limitada ao contido no Código de Ética e Conduta da Entidade.
IV. O usuário deverá utilizar a assinatura padrão da 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 os interesses da Entidade, bem como suas normas estabelecidas nesta PSIPD, no Códigos de Ética e Conduta e demais regulamentos.
VII. É necessário 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.

5.1.4 Internet (Rede Mundial)

I. Qualquer informação que 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. O usuário se declara ciente de que não existirá expectativa de privacidade no uso de, sem limitação, qualquer equipamento, tecnologia e/ou serviço de propriedade da Entidade.

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 e (ou) compartilhamento a sites da internet ou quaisquer arquivos digitais, bem como sua produção e propagação, que desrespeitem os Códigos de Ética e Conduta da Entidade, possuam material protegido por direitos autorais sem a permissão do detentor dos direitos, 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.

5.1.5 Dispositivos de acessos (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.

III. Em caso de furto, roubo ou extravio de qualquer dispositivo, o usuário interno deverá lavrar um boletim de ocorrência na autoridade competente e entregar uma cópia do boletim de ocorrência para a gerência administrativa que, ato contínuo, remeterá o documento para o gestor de TI para as providências cabíveis.

IV. 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.
V. O usuário se declara ciente de que no caso de extinção, interrupção ou suspensão do contrato mantido com a organização, o dispositivo móvel deverá ser devolvido imediatamente, todas as informações e dados de qualquer natureza neles contidos poderão ser excluídos.
VI. O usuário interno se declara ciente de que o dispositivo móvel estará sujeito a monitoramento e auditoria; logo, em relação ao dispositivo da organização não há expectativa de privacidade.
VII. O uso de mídias removíveis (cartões de memória, pen drive, demais dispositivos USB e similares) não é recomendado, pois se trata de uma das maiores fontes de ameaças, aumentando a probabilidade de ataques cibernéticos na Rede Corporativa e vazamento de informações. Caso haja a necessidade de cópia de dados para equipamentos particulares ou externos o CSRI ou TI devem ser consultados.

5.1.6 Computação em nuvem

I. O uso das “plataformas de nuvem” para transmissão e armazenamento de informações só poderá ocorrer naquelas formalmente contratadas pela Entidade e disponibilizadas pela área técnica responsável, exceto serviços e ferramentas avaliadas e autorizadas pelo CSIRI Ou TI.

5.1.7 Redes e mídias sociais

I. O uso das redes e mídias sociais institucionais, por parte dos empregados e estagiários, deve ser regido pelas determinações contidas nesta PSIPD e por outras normativas a ela complementares.
II. A gestão dos perfis institucionais da Entidade nas redes sociais deve ser realizada por empregados designados e/ou por terceirizados designados para tal, devidamente autorizados, identificados e instruídos de forma a preservar a imagem institucional, sendo vedado aos demais empregados a criação de perfis não oficiais em nome da Entidade.

III. Quanto ao conteúdo das publicações nas redes e mídias sociais, fica vedado divulgar informações confidenciais, restritas 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.

V. As redes corporativas devem ser utilizadas conforme os objetivos pelos quais foram projetadas. Por exemplo, a rede interna é exclusiva para execução das atividades profissionais, rede visitantes é exclusiva para o público que visitante, rede de fornecedores é exclusiva para fornecedores.

5.1.8 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, específicos e legais, 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 ou contratuais.

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. Quando autorizada e necessária a transferência de informação classificada como confidencial e (ou) interna, bem como a relativa a dados pessoais, devem ser protegidas quando forem transferidas para usuários externos.

VII. É proibido ao usuário deixar informações confidenciais, internas e dados pessoais armazenados sem limitação de controle de acesso.

VIII. 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; e
- Utilização de processo de identificação de informações críticas e sensíveis, garantindo que a informação esteja devidamente protegida.

5.1.9 Guarda de informações digitais (backup) e documentação física

I. Rotinas sistemáticas de backup e guarda de informações devem ser realizadas por empregados 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 unidades 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 arquiva mento 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.

VI. As necessidades especiais de backup devem ser solicitadas à área de T.I. por meio de processo interno.

VII. O login e senha do backup, quando aplicável, deve ser armazenado em local seguro e de fácil acesso ao gestor responsável. É vedado a armazenar, arquivar o login e senha no mesmo servidor no qual é mantida cópia de segurança e/ou no servidor principal.

5.1.10 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. Os colaboradores da Organização não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e autorização área de T.I.

IV. O usuário deverá salvar todos os documentos necessários para as atividades da Organização na rede interna, especificamente nos locais designados que pertencem as estratégias de backup. Os referidos arquivos, se gravados apenas localmente nos dispositivos não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no sistema operacional ou ataque por códigos maliciosos.

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

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

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

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

IX. 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.

5.1.11 Controles criptográficos

I. Cabe a organização adquirir e fornecer as aplicações adequadas para criptografar as informações de sua propriedade e dados pessoais.
II. Na troca de informações com usuários externos, a Entidade deve instalar em seu servidor e utilizar certificado digital emitido, preferencialmente, pela Infraestrutura de Chaves Públicas Brasileira [ICP-Brasil]. O uso de certificados não emitidos pela ICP-Brasil é válido desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.
III. Toda a informação classificada como confidencial e dados pessoais sensíveis que for produzida, armazenada e/ou transmitida, em parte ou totalmente, por qualquer meio eletrônico, deve ser protegida com recurso criptográfico.
IV. A transmissão eletrônica de dados pessoais, dados pessoais sensíveis e os dados classificados como críticos deve ser realizada com a utilização de recurso criptográfico.
V. As informações e dados pessoais transportadas em mídias removíveis e dispositivos móveis devem ser criptografadas;
VI. Todos os usuários devem utilizar apenas o recurso criptográfico definido pela Entidade.

5.1.12 Antivírus

I. Os sistemas e computadores devem ter proteções ativas e atualizadas permanentemente, sendo responsabilidade da área técnica o monitoramento.
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.

5.1.13 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 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 DataCenter 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 empregado da área técnica responsável ou por empregado designado por ela.

5.1.14 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.

5.2 Gestão de outros recursos de informação

5.2.1 Estação de trabalho

I. Nenhuma informação confidencial ou contendo dados pessoais e dados pessoais sensíveis 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. Computadores, notebooks ou similares devem ficar bloqueados, mesmo quando o usuário se ausentar por curto período, assim como os dispositivos móveis, quando necessário, devem ser guardados em local provido com chaves/fechaduras.

III. Se precisar se ausentar de sua mesa o usuário deve efetuar o procedimento de bloqueio de tela com o “Ctrl+alt+delete” ou “botão iniciar do Windows + L.

IV. A estação de trabalho deverá ser bloqueada automaticamente após 10 minutos de inatividade.

V. Em caso impossibilidade de abrir um chamado deve-se entrar e contato por telefone e posteriormente realizar o procedimento de abertura de ticket.

VI. 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, inclusive quando forem somente informações que estão em sua posse

VII. No caso de baixas patrimoniais 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.

VIII. Equipamentos pessoais de qualquer natureza não devem ser conectado à rede corporativa sem prévia autorização da área técnica.

5.2.2 Controle de acesso físico

I. Perímetros de segurança física devem incluir controles de segurança necessários para impedir o acesso físico não autorizado às dependências da Organização como, por exemplo, portas de entradas seguras; recepção com controle de acessos; sistema de monitoramento por circuito fechado de televisão.

II. Todos os empregados da Entidade que transitem por ambientes internos do Sescoop/PR devem possuir identificação pessoal visível por crachás e registrados em sistema de controle de acessos.

III. Os recursos de controle de acesso físico devem ser associados ao respectivo empregado, o qual tem a responsabilidade de mantê-los sob sua guarda. O usuário jamais poderá utilizar, como próprio, os recursos de outro usuário, bem como poderá ceder o seu para outrem.

IV. O usuário deve estar atento às políticas de mesa limpa e tela sempre bloqueada quando não utilizada em função dos riscos associados ao acesso de terceiros às dependências da Entidade.

5.2.3 Serviços postais

Os serviços de correspondências, malote e PAC da Entidade estão disponíveis aos empregados, estagiários e dirigentes 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.

5.2.4 Plano de continuidade de negócio

A Entidade se compromete a elaborar e manter Plano de Continuidade do Negócio (PCN). Cabe ao Comitê de Segurança da Informação e demais áreas de negócio da entidade dar subsídio técnicos à Alta Administração do Sescoop/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, bem como designando uma equipe específica para o PCN.

5.2.5 Riscos de segurança da informação

I. O Sescoop/PR compromete-se a adotar e manter processo contínuo de Gestão de Riscos de Segurança da Informação, conforme metodologia contida na Política de Gestão de Riscos, ou documento correspondente que venha a substituí-lo.
II. Os processos de segurança da informação deverão ser revistos periodicamente pelo CSIRI 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 ao CSIRI e grupos de trabalho específicos a criação e atualização do Plano de Resposta a Incidentes.

6 REVISÃO

As regras contidas nessa Política serão revisadas no mínimo com periodicidade anual ou em menos tempo conforme o entendimento do CSIRI do Sescoop/PR.

7 DISPOSIÇÕES FINAIS

I. As diretrizes estabelecidas nessa Política e nas demais normas e procedimentos que a complementam não se esgotam em razão da contínua evolução tecnológica, da legislação vigente e constante surgimento de novas ameaças e requisitos.
II. Qualquer exceção à aplicação das disposições estabelecidas nesta Política deverá ser documentada e aprovada pelo CSIRI.
III. Em caso de dúvidas sobre as diretrizes descritas ou não nessa Política, o colaborador deverá procurar esclarecimento através do e-mail dpo.sescoop@sistemaocepar.coop.br.
IV. Esta Política entra em vigor na data de sua publicação.

8 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 Entidade.
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 fotografiado ambiente na linha do tempo. Backup local: armazenado nas instalações da Entidade. Backup off-site: armazenado em instalações externas à Entidade, como pororganizações terceiras em ambiente físico e/ou em nuvem.
CLT	Consolidação das Leis do Trabalho.
COMITÊ DE SEGURANÇA DA INFORMAÇÃO E RESPOSTA À INCIDENTES (CSIRI)	Grupo multifuncional que tem como finalidade estabelecer políticas e diretrizes para a segurança da informação no âmbito da Entidade, além de auxiliar na resolução de problemas relacionados ao tema e divulgação do conteúdo dessas políticas e diretrizes.
Controles criptográficos	O uso de controles criptográficos tem o propósito de garantir a segurança da informação quando ela for transmitida pela internet e/ou armazenada nos dispositivos da Organização ou não. O recurso dificulta que a informação seja, mas não se limitando, interpretada, visualizada, aberta em caso de interceptação.
COOKIES	Arquivos de texto baixados em seu dispositivo quando você visita um site. Sãoúteis 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	Ferramentas que permitem o envio e o recebimento de mensagens, documentos digitais incluindo sons/voz, imagens e afins.
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 empregado 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 organizadae 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 váriosconteúdos 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 asegurança das informações.
Plano de Continuidade de Negócio. (PCN)	Consiste no desenvolvimento de ações preventivas e de recuperação a serem adotadas quando houver problemas que comprometam o andamento normal dos processos e a prestação dos serviços, a fim de minimizar possíveis riscos.
REDE CORPORATIVA	Sistema de transmissão de dados e informações entre equipamentos de uma mesma corporação, tais como computadores e similares, servidores dedocumentos 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 digital-mente 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.

SEGURANÇA DA INFORMAÇÃO	Esforços contínuos para a proteção da 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 determinadonúmero 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 dastratativas em questão.
USUÁRIO(S)	Empregados, 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 deCompromisso, 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.

VERSÕES DO DOCUMENTO

Versão	Última Atualização	Elaborado Por	Revisado Por
1.0	06/12/2023	CSIRI	Gerente de Integridade – José Ronkoski

24 páginas - Datas e horários baseados em Brasília, Brasil
Sincronizado com o NTP.br e Observatório Nacional (ON)
Certificado de assinaturas gerado em 18 de December de 2023, 09:32:01

RESOLUÇÃO 93 2023 - Dispõe sobre a Aprovação da Política de Segurança da Informação do Sesc

Código do documento 38637b44-430b-47c6-a839-8f2f0ad1c808

Assinaturas

José Roberto Ricken
jose.ricken@sistemaocepar.coop.br
Assinou

Eventos do documento

15 Dec 2023, 15:36:19
Documento 38637b44-430b-47c6-a839-8f2f0ad1c808 **criado** por THAINE GABRIELI CZELUSNIAK (0d0cc849-1515-4bf5-bf84-e0b767a293c9). Email:thaine.gabrieli@sistemaocepar.coop.br. - DATE_ATOM: 2023-12-15T15:36:19-03:00

15 Dec 2023, 15:37:12
Assinaturas **iniciadas** por THAINE GABRIELI CZELUSNIAK (0d0cc849-1515-4bf5-bf84-e0b767a293c9). Email: thaine.gabrieli@sistemaocepar.coop.br. - DATE_ATOM: 2023-12-15T15:37:12-03:00

15 Dec 2023, 16:11:27
JOSÉ ROBERTO RICKEN **Assinou** (3c078489-360a-4999-a93e-6202864c8f8a) - Email: jose.ricken@sistemaocepar.coop.br - IP: 177.220.186.153 (153.186.220.177.dynamic.copel.net porta: 10404) - Documento de identificação informado: 206.913.009-68 - DATE_ATOM: 2023-12-15T16:11:27-03:00

Hash do documento original
(SHA256):5573104808b4f70739c2c502d68c6a97ee794db1c613fe9ea614cad3a2f0c70d
(SHA512):8289d1706770e7525c34d8efcd3d54877ac2f351be574a475206e2f4fd6a15274e59be1105f0760acadf2091e512c350383c6090061ef96f5a9d3f9576fb126f

Esse log pertence **única** e **exclusivamente** aos documentos de HASH acima

Esse documento está assinado e certificado pela D4Sign