POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

CONTROLE DE REVISÕES DESTE DOCUMENTO

ITEM	EMISSÃO / REVISÃO	DATA
00	Emissão deste documento	25/10/2024
01	Revisão de Layout e aprovação	25/10/2024

SUMÁRIO

1. OBJETIVO

A presente política é adotada pela liderança do SITRANS, referida neste documento como “Sindicato”

O Sindicato estabelece a Política de Segurança da Informação como parte integrante do seu sistema de gestão corporativo, alinhada às boas práticas do mercado, à normas internacionalmente aceitas e a legislação brasileira pertinente, com o objetivo de garantir níveis adequados de proteção a informações e dados pessoais operados pelo Sindicato, de seus clientes e colaboradores sob sua responsabilidade.

2. POLÍTICA

Esta política se aplica a todos os colaboradores, fornecedores e parceiros do Sindicato, que possuem acesso às informações e dados pessoais do Sindicato e/ou fazem uso de recursos computacionais compreendidos na infraestrutura interna.

3. PRINCÍPIOS

A Segurança da Informação e Cibernética baseia-se em 03 (três) princípios fundamentais:

- Confidencialidade: Garantir que apenas pessoas devidamente autorizadas tenham acesso às informações e aos Ativos de Informação, limitando esse acesso apenas ao necessário para o desempenho de suas funções.
- Integridade: Garantir a veracidade e integridade das informações, bem como os métodos de execução física ou lógica, garantindo a proteção contra alterações indevidas, sejam elas intencionais ou acidentais, tanto durante o armazenamento quanto na transmissão dos dados.
- Disponibilidade: Garantir que os usuários autorizados tenham acesso às informações e aos Ativos de Informação correspondentes sempre que necessário, de forma oportuna e eficiente, para o desempenho de suas atividades.

4. RESPONSABILIDADE DOS PROFISSIONAIS

4.1. É dever de todos os indivíduos que trabalham, prestam serviços e fazem uso dos Sistemas do Sindicato, conhecer, entender e aderir às informações contidas nesta Política. O Sindicato promoverá treinamento e conscientização contínua sobre as diretrizes e normas estabelecidas na Política de Segurança da Informação. É responsabilidade de cada usuário manter-se informado sobre atualizações e mudanças na referida Política.

4.2. Todo profissional deve participar dos Programas de Treinamento e Conscientização de Segurança da Informação;

4.3. Todo profissional deve estar ciente de suas responsabilidades quanto à manutenção do CID (confidencialidade, integridade e disponibilidade) dos ativos de TI da empresa, garantindo que uma "nota" de confiabilidade de cada ativo permaneça alta;

4.4. É dever de todos os profissionais garantir que a segurança das informações esteja incluída no planejamento de todas as tarefas e projetos, garantindo que a proteção de dados e ativos esteja presente em cada etapa do processo;

4.5. Todos os usuários devem garantir que as informações relacionadas ao Sindicato permaneçam fora do alcance de pessoas não autorizadas, mantendo o local de trabalho limpo e organizado, e assegurando que as informações sejam em formato físico ou digital, devidamente armazenadas e protegidas;

4.6. Os usuários não devem discutir detalhes técnicos sobre os sistemas ou mecanismos de segurança utilizados pelo Sindicato com pessoas não autorizadas, mesmo que sejam de sua confiança.

5. DIRETRIZES

5.1. O Sindicato adota um pilar de Segurança da Informação, adequado à sua natureza, porte, complexidade, estrutura, perfil de risco e modelo de atuação. Esse pilar tem como principal função garantir o gerenciamento eficaz do Risco de Segurança da Informação e Cibernético. As diretrizes corporativas estabelecem os fundamentos sobre os quais os principais processos e controles de Segurança da Informação e Cibernética devem ser baseados, garantindo a conformidade e a proteção contra ameaças digitais e riscos operacionais

5.1.1. **Conscientização em Segurança da Informação**: Os princípios e diretrizes de Segurança da Informação devem ser amplamente disseminados por meio de programas de conscientização e capacitação voltados para profissionais e terceiros do Sindicato. Além disso, dicas de segurança e prevenção à fraudes podem ser disponibilizadas tanto no site institucional quanto nas redes sociais, promovendo um ambiente de proteção contínua e engajamento em boas práticas de segurança digital.

5.1.2. **Declaração de Responsabilidade**: Todos os profissionais e terceiros contratados diretamente pelo Sindicato devem conhecer e comprometer-se a seguir a Política de Segurança da Informação.

5.1.3. **Gestão de Ativos da Informação**: Todos os ativos de informação do Sindicato devem ser identificados, inventariados e catalogados pelo departamento de TI. A Segurança da Informação deve proteger esses ativos contra acessos indevidos, implementando controles físicos e lógicos adequados.

5.1.4. **Utilização de Recursos da Informação**: Apenas equipamentos autorizados pelo time de Tecnologia da Informação e Segurança da Informação do Sindicato, podem ser conectados à rede corporativa. A conexão de dispositivos pessoais não autorizados é proibida. Todos os equipamentos devem ter proteção contra softwares maliciosos devidamente instalada e configurada.

5.1.5. **Segurança Física**: Os controles e processos de segurança física devem prevenir o acesso não autorizado, danos e interferências nos ativos de informação.

5.1.6. **Criptografia e Confidencialidade**: A criptografia deve ser utilizada, sempre que possível, para proteger dados sensíveis ou críticos, tanto no armazenamento quanto na transmissão, dependendo da confidencialidade das informações.

5.1.7. **Gestão de Riscos**: Os riscos devem ser identificados e avaliados por meio de um processo estruturado que analisa vulnerabilidades, ameaças e impactos nos ativos de informação, visando implementar controles adequados de proteção.

5.1.8. **Teste de Segurança**: Para identificar e reduzir vulnerabilidades, devem ser realizados testes de segurança periodicamente, com varreduras de vulnerabilidades.

5.1.9. **Cópias de Segurança (Backup)**: Deve-se garantir a integridade e confiabilidade da restauração de dados em sistemas e servidores, assegurando a confidencialidade, integridade e disponibilidade das informações.

5.1.10. **Segurança na Gestão de Fornecedores**: Os fornecedores devem ser classificados e gerenciados conforme sua relevância, garantindo a conformidade com os controles de segurança e regulatórios. Serviços que envolvem o processamento de dados do Sindicato devem seguir rigorosos controles de segurança.

5.1.11. **Aquisição de Bens e Serviços**: A contratação de sistemas ou serviços deve contemplar a análise de requisitos de segurança, incluindo a prova de conceitos e a formalização da coleta de evidências. O setor de Segurança da Informação sinalizará e manterá registro quando verificar a contratação de serviços que não atendam às regulamentações e políticas de segurança estabelecidas.

5.1.12. **Controles e Incidentes de Segurança**: Fornecedores que manuseiam dados sensíveis devem implementar controles para prevenir e tratar incidentes de segurança, e qualquer incidente relevante deve ser comunicado ao setor de Segurança da Informação e ao DPO do Sindicato.

5.1.15. **Proteção de Perímetro**: Ferramentas e controles devem ser implementados para proteger a infraestrutura contra ataques externos, incluindo bloqueios contra softwares maliciosos e invasões, bem como o controle de segmentação da rede para mitigar acessos não autorizados.

5.1.16. **Registro e Monitoramento**: Todos os eventos lógicos de sistemas e serviços devem ser registrados e monitorados conforme as diretrizes estabelecidas.

5.1.17. **Gestão de Incidentes**: Devem ser realizadas ações de prevenção, identificação, resposta e registro de incidentes que comprometam a confidencialidade, integridade ou disponibilidade dos ativos de informação. Quando na ocorrência ou mera suspeita de um Incidente, é necessário reportar

à Comissão de Lei Geral de Proteção de Dados e ao Encarregado de Dados Pessoais, que atuará em conformidade com o Plano de Resposta à Incidentes;

5.1.19. **Ciclo de Vida de Acesso**: Criar processo de provisionamento e desprovisionamento de acesso dos colaboradores, onde a TI seja comunicada de imediato, assim que o colaborador for admitido ou desligado da empresa.

6. TRANSFERÊNCIA E COMPARTILHAMENTO DE DADOS PESSOAIS COM TERCEIROS

6.1. O Sindicato, como controlador de dados pessoais, está comprometido em cumprir as regras e diretrizes estabelecidas pela Lei Geral de Proteção de Dados (LGPD) ao realizar transferências e compartilhamentos de dados pessoais com terceiros. Abaixo, apresentamos as diretrizes que o Sindicato adota para garantir a proteção adequada dos dados pessoais:

6.1.1. **Base Legal para Transferência e Compartilhamento** - O Sindicato assegura que todas as transferências e compartilhamentos de dados pessoais com terceiros sejam baseados em uma das bases legais previstas na LGPD. Isso inclui obter o consentimento do titular dos dados, cumprir com obrigações legais e regulatórias, proteger a vida ou a integridade física, exercer direitos em processos judiciais ou legítimos interesses do controlador ou de terceiros.

6.1.2. **Informação ao Titular** - Antes de realizar a transferência ou compartilhamento de dados pessoais, o Sindicato fornece informações claras e transparentes aos titulares dos dados. Essas informações incluem os detalhes sobre as finalidades da transferência, as categorias de dados envolvidos, a identificação dos terceiros envolvidos e as medidas de segurança adotadas para proteger os dados pessoais.

6.1.3. **Contrato ou Instrumento Similar -** O Sindicato estabelece contratos ou instrumentos similares com os terceiros receptores dos dados pessoais. Esses contratos contêm cláusulas que garantem a proteção adequada dos dados pessoais transferidos. As cláusulas incluem medidas de segurança, confidencialidade, especificação das finalidades do tratamento, prazo de retenção dos dados, entre outros aspectos necessários para assegurar a conformidade com a LGPD.

6.1.4. **Responsabilidade Solidária –** O Sindicato reconhece sua responsabilidade solidária pelos danos causados em caso de violação dos dados pessoais pelos terceiros com os quais ocorreu a transferência ou compartilhamento. Assim, a empresa realiza uma avaliação criteriosa dos terceiros antes de compartilhar os dados e implementa medidas para garantir que eles cumpram as obrigações legais de proteção de dados.

6.1.5. **Transferências Internacionais -** No caso de transferências de dados pessoais para países fora do Brasil, o Sindicato verifica se esses países oferecem um nível adequado de proteção de dados pessoais. Caso contrário, a empresa adota medidas adicionais, como a utilização de cláusulas contratuais padrão, regras corporativas globais, selos, certificados ou códigos de conduta para garantir a proteção adequada dos dados pessoais transferidos.

7. RISCOS DE PRIVACIDADE

7.1. A gestão de riscos de privacidade refere-se a um conjunto de práticas e processos adotados por organizações para identificar, avaliar e mitigar os riscos associados à privacidade dos dados pessoais que são coletados, armazenados, processados e compartilhados. Com o crescente volume de informações pessoais sendo gerenciadas pelas empresas e a preocupação crescente com a proteção dos dados dos indivíduos, a gestão de riscos de privacidade tornou-se uma área essencial nas práticas de governança corporativa. A gestão de riscos de privacidade envolve várias etapas, incluindo a identificação e classificação dos dados pessoais coletados, a análise dos riscos associados à sua manipulação, o desenvolvimento de medidas de segurança e controle, e o monitoramento contínuo para garantir a conformidade com as leis e regulamentos de privacidade aplicáveis. No âmbito da gestão de riscos de privacidade, algumas das principais atividades incluem:

7.1.1. Avaliação de riscos: Identificar e avaliar os riscos associados à privacidade dos dados pessoais. Isso envolve examinar as informações coletadas, como são processadas e compartilhadas, e identificar possíveis vulnerabilidades e ameaças.

7.1.2. Mapeamento de dados: Realizar um inventário dos dados pessoais coletados e armazenados pelo Sindicato, incluindo sua origem, finalidade, localização e fluxo dentro da empresa. Esse mapeamento é essencial para

entender quais informações estão sujeitas a riscos e para tomar medidas adequadas de proteção.

7.1.3. Análise de impacto na privacidade (AIPD): Realizar uma análise detalhada dos possíveis impactos que as atividades de processamento de dados podem ter sobre a privacidade das pessoas. Isso envolve identificar os riscos associados, avaliar sua gravidade e probabilidade de ocorrência, e determinar as medidas de mitigação adequadas.

7.1.4. Implementação de medidas de segurança: Desenvolver e implementar medidas de segurança técnicas e organizacionais para proteger os dados pessoais. Isso pode incluir a adoção de criptografia, o estabelecimento de restrições de acesso, a implementação de políticas de segurança de TI, a realização de testes de penetração, entre outras práticas.

7.1.5. Políticas e procedimentos: Estabelecer políticas e procedimentos claros relacionados à privacidade dos dados pessoais. Isso envolve definir diretrizes para a coleta, armazenamento, processamento e compartilhamento de informações pessoais, bem como instruções sobre como lidar com solicitações de acesso, correção ou exclusão de dados.

7.1.6. Monitoramento e conformidade: Realizar monitoramento contínuo das práticas de privacidade e segurança para garantir que estejam alinhadas com as leis e regulamentos aplicáveis. Isso inclui auditorias internas, revisões periódicas, avaliações de conformidade e ações corretivas quando necessário.

7.1.7. Treinamento e conscientização: Fornecer treinamento regular aos funcionários sobre as políticas e práticas de privacidade, incluindo a importância da proteção dos dados pessoais e as melhores práticas de segurança. A conscientização dos colaboradores é fundamental para garantir a conformidade e minimizar os riscos.

7.1.8. Resposta a incidentes: Estabelecer planos de resposta a incidentes de privacidade para lidar com violações de dados, vazamentos ou acessos não autorizados. Isso envolve a definição de processos para investigação, notificação adequada às autoridades competentes e às partes afetadas, e ações para mitigar os impactos do incidente.

8. ACESSO AOS SISTEMAS

8.1. Todas as solicitações de concessão de acesso devem ser encaminhadas ao time de Suporte, via e-mail ou por meio do formulário de chamado técnico.

8.2. Todas as solicitações de acesso precisam ser aprovadas pelo responsável pelo perfil solicitado, garantindo que o acesso concedido seja o mínimo necessário para atender às exigências do negócio e às funções do solicitante, sem comprometer os princípios de segregação de funções.

8.3. Antes de obter acesso aos sistemas de informação do Sindicato, terceiros, prestadores de serviços ou parceiros comerciais devem receber e conhecer as definições previstas nesta Política.

8.4. Os IDs fornecidos a terceiros, prestadores de serviços ou parceiros comerciais terão uma data de expiração máxima de 90 dias. Esse prazo pode ser reduzido conforme a duração do contrato ou estendido mediante solicitação formal.

8.5. As lideranças devem informar imediatamente ao time de suporte sobre quaisquer mudanças de função ou desligamento de usuários, para que as ações adequadas sejam tomadas em relação ao acesso.

8.6. Os IDs de usuários serão bloqueados após 60 dias de inatividade e removidos após 90 dias, salvo se o usuário solicitar a reativação da conta, comprovando sua identidade e demonstrando que seu vínculo com a empresa permanece inalterado durante o período de inatividade.

9. SENHAS

9.1. Todo usuário deve estar ciente de que seu ID de usuário e senha não devem ser compartilhados. Qualquer infração ou anormalidade no sistema será atribuída ao proprietário da credencial em uso.

9.2. O uso de senhas com pelo menos dez (10) caracteres é obrigatório.

9.3. Após cinco (5) tentativas incorretas de acesso ao sistema, a senha será bloqueada e só poderá ser reativada após trinta (30) minutos de espera.

9.4. Os usuários devem verificar a notificação sobre a última utilização do sistema no início de cada sessão (quando disponível) e notificar o superior em caso de suspeita de uso indevido de suas credenciais por terceiros.

9.5. Todas as senhas têm validade de cento e vinte (120) dias e, após esse prazo, o usuário será obrigado a alterá-las, sendo proibido repetir a última senha usada.

9.6. É proibido escrever ou armazenar senhas de forma desprotegida ou deixá-las próximas aos dispositivos que protegem. As senhas devem ter o mesmo nível de proteção que as informações que elas protegem.

9.7. As senhas devem ser alteradas imediatamente ao menor sinal de comprometimento do sistema ou da própria senha.

10. USO DE SOFTWARE

10.1. Qualquer software, independentemente de sua condição comercial, deve ser homologado e instalado exclusivamente pelo time de Suporte do Sindicato.

10.3. Todo o desenvolvimento ou compra de softwares deve ser avaliado pelo setor de TI.

10.4. Softwares comerciais estão sujeitos à legislação de direitos autorais e devem ser utilizados conforme a licença comercial obtida.

10.5. A utilização de ferramentas shareware sem a aquisição de licença após o período gratuito é proibida, pois pode acarretar sanções legais.

10.6. Cópias não autorizadas de software da empresa são proibidas para uso pessoal ou para terceiros.

10.7. Cada profissional deve notificar o setor de TI em caso de anomalias ou dúvidas relacionadas ao uso de software.

11. USO DA INTERNET

11.1. Os profissionais do Sindicato devem seguir as políticas de segurança da informação ao trabalhar remotamente, garantindo o uso de conexões seguras e criptografadas.

11.2. O Sindicato não se responsabiliza por ações ou transações feitas na internet pelos profissionais. O uso impróprio da internet pode violar legislações vigentes, e o Sindicato poderá ser obrigado a fornecer evidências para ações judiciais.

11.3. A divulgação de informações corporativas na internet é proibida sem autorização explícita do Sindicato, seja via mensagens, upload de arquivos ou publicações.

11.4. Ao expressar opiniões pessoais na internet, os profissionais não devem se posicionar em nome do Sindicato em listas de discussão ou outros canais, a menos que explicitamente autorizados.

11.5. O acesso a sites de conteúdo pornográfico, criminoso ou de violência explícita, bem como o uso do e-mail corporativo para disseminar tais conteúdos, será considerado ofensivo e passível de consequências disciplinares.

11.6. Cada usuário deve manter sua conta de e-mail individual, não compartilhando ou utilizando-a em listas de discussão. É proibido enviar e-mails que aparentem ter sido enviados por outro usuário.

11.7. O envio de mensagens de corrente ou sobre alertas de vírus não autorizadas pelos recursos do Sindicato é proibido.

11.8. Os usuários não devem acessar links contidos em e-mails de origem duvidosa e devem ser cautelosos com mensagens de remetentes externos.

11.9. Comunicados gerais por e-mail devem ser enviados pelos times de Comunicação do Sindicato.

11.10. Os equipamentos e meios de comunicação eletrônica do Sindicato estão sujeitos a monitoramento, e os profissionais declaram-se cientes de que esses recursos podem ser inspecionados a qualquer momento.

12. USO DE ESTAÇÕES DE TRABALHO E DISPOSITIVOS MÓVEIS

12.1. A conexão de equipamentos pessoais deve ser precedida pela aprovação formal do setor de TI.

12.2. A troca de dados entre dispositivos móveis e computadores do Sindicato é proibida, exceto quando o recurso móvel foi cedido pela organização.

12.3. Dispositivos com tecnologia wireless só podem ser usados nas instalações do Sindicato se estiverem configurados de acordo com os padrões de segurança da empresa.

12.4. Os profissionais devem assinar o Termo de Cessão de Uso de Bens Móveis tão logo haja o recebimento do equipamento cedido pelo Sindicato.

12.5. A perda ou roubo de equipamentos móveis deve ser imediatamente comunicado ao setor de TI e à Segurança da Informação.

12.6. Todas as estações de trabalho devem utilizar proteção de tela com senha, sendo bloqueadas após 5 minutos de inatividade.

12.7. Os usuários não estão autorizados a desativar o software antivírus e devem reportar suspeitas de vírus ao time de suporte imediatamente.

12.8. Alterar, transferir ou remover equipamentos sem autorização é considerado falta grave.

12.9. A inclusão ou exclusão de hardware/software nas estações de trabalho só pode ser feita pelo time de suporte.

O Uso de dispositivos pessoais nas atividades corporativas remotas deverá ser informado à liderança. Este dispositivo deverá ser previamente averiguado pelo time de TI, que verificará se o sistema operacional está atualizado e se o mesmo possui ferramentas de antivírus, antispywares, entre outros. Após esta verificação, o dispositivo poderá ser considerado como apto, tendo, assim, acessos às ferramentas corporativas

13. HISTÓRICO DAS ALTERAÇÕES

Data	Revisão	Histórico
xx/xx/xx	01	Aprovação inicial

14. ANEXOS

ANEXO I - Formulário de Comunicação de Incidente de Segurança com Dados Pessoais

ANEXO II - Plano de Resposta a Incidentes