VERSÃO:2

DATA DA EMISSÃO: 05/12/2023

Classificação: Interno

SINDICATO DOS TRABALHADORES DO JUDICIÁRIO FEDERAL NO ESTADO DE SÃO PAULO

SINTRAJUD

NOSSA LUTA FAZ ACONTECER!

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS

ORIENTAÇÕES GERAIS E PROCESSOS

SINTRAJUD

CNPJ nº 01.202.841/0001-44

DS DS

Sumário

Rua Antônio de Godói, n° 88 - 16° andar, Bairro Centro São Paulo SP
www.sintrajud.org.br

1. APLICABILIDADE E TRATAMENTO DE DADOS PESSOAIS

Esta Política de Segurança da Informação estabelece diretrizes claras e obrigatórias para os seus destinatários, com o propósito de garantir a compreensão e o cumprimento integral da legislação vigente relativa à proteção de dados. O destaque é dado à Lei nº 13.709/2018, também conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD). A meta é assegurar a segurança da informação por meio de diretrizes estratégicas que preservem a integridade, a segurança, a confidencialidade, a transparência, a autenticidade e a disponibilidade de dados pessoais e informações de todos os tipos.

A LGPD, em sua essência, visa resguardar os direitos fundamentais de liberdade e de privacidade do indivíduo, outorgando aos titulares de dados pessoais o exercício de direitos específicos enquanto seus dados estão sendo tratados pela instituição detentora das informações. Desse modo, os dados pessoais recebem uma proteção especial, exigindo que sejam tratados em conformidade com os princípios e disposições estabelecidos pela lei, que são:

- **Finalidade:** a realização do tratamento deve ocorrer para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- **Adequação:** a compatibilidade do tratamento deve ocorrer conforme as finalidades informadas ao titular, de acordo com o contexto do tratamento;
- **Necessidade:** o tratamento deve se limitar à realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
- **Livre acesso:** é a garantia dada aos titulares a consulta livre, de forma facilitada e gratuita, à forma e à duração do tratamento, bem como à integralidade de seus dados pessoais;
- **Qualidade dos dados:** é a garantia dada aos titulares de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

- **Transparência:** é a garantia dada aos titulares de que terão informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
- **Segurança:** trata-se da utilização de medidas técnicas e administrativas qualificadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
- **Prevenção:** compreende a adoção de medidas para prevenir a ocorrência de danos por causa do tratamento de dados pessoais;
- **Não discriminação:** sustenta que o tratamento dos dados não pode ser realizado para fins discriminatórios, ilícitos ou abusivos;
- **Responsabilização e prestação de contas:** demonstração, pelo Controlador ou pelo Operador, de todas as medidas eficazes e capazes de comprovar o cumprimento da lei e a eficácia das medidas aplicadas.

Importante mencionar que em fevereiro/2022 foi promulgada a Emenda Constitucional n.º 115, que inclui a proteção de dados pessoais entre os direitos e garantias fundamentais na Constituição da República.

2. CONCEITOS BÁSICOS

Para facilitar a compreensão e promover um entendimento claro da política delineada neste documento, apresentaremos as definições legais e conceitos que serão empregados ao longo deste instrumento. Esse esclarecimento preliminar é crucial para a efetiva compreensão e aplicação das diretrizes aqui estabelecidas, garantindo que todos os destinatários estejam alinhados em termos de terminologia e significado. Essas definições e conceitos, extraídos da legislação e do contexto regulatório, formam a base sobre a qual esta política foi construída e serão usados de maneira consistente ao longo de todo o documento. São elas:

A. Dados pessoais: informação relacionada a pessoa natural identificada ou identificável, de forma direta ou indireta. Alguns tipos de dados pessoais incluem (nome completo, RG e CPF,

Rua Antônio de Godói, n° 88 - 16° andar, Bairro Centro São Paulo SP
www.sintrajud.org.br

passaporte e carteira de habilitação, endereço, telefone, e-mail, endereço de IP, data de nascimento, localização via GPS, entre outros).

B. Dados sensíveis: relacionados aos aspectos mais íntimos de personalidade de um indivíduo, sendo qualquer informação relacionada a origem racial, étnica, opinião política, filosófica, filiação a sindicato, dados genéticos e biométricos.

C. Dados anonimizados: dados pessoais nos quais a identificação do indivíduo foi removida, tornando-os anônimos.

D. Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

E. Controlador: Pessoa natural ou jurídica, a quem competem as decisões referentes ao tratamento de dados pessoais

F. Operador: Pessoa natural ou jurídica, que realiza o tratamento de dados pessoais em nome do controlador

G. Encarregado de dados: responsável frente à ANPD e aos titulares indicados pelo controlador.

H. Tratamento de dados: qualquer operação que seja realizada com os dados pessoais (incluindo: acesso, armazenamento, arquivamento, classificação, coleta, comunicação, controle, difusão, distribuição, eliminação, extração, modificação, processamento, produção, recepção, reprodução, transferência, transmissão e utilização.

I. ANPD –Autoridade nacional de proteção de dados: é o órgão federal responsável por fiscalizar a aplicação da **Lei Geral de Proteção de Dados Pessoais**. Ela nasceu inicialmente vinculada à Presidência da República, mas hoje é uma autarquia especial, com autonomia administrativa e financeira, a qual interpreta e regula a nova lei, por meio de fiscalização e aplicação da LGPD nos casos concretos.

J. Criptografia: Criptografia: é a conversão de dados de um formato legível em um formato codificado. Os dados criptografados só podem ser lidos ou processados depois de serem descriptografados.

3. OBJETIVO

A presente Política de Segurança da Informação tem como alvo primordial os empregados da organização e objetiva demonstrar as medidas técnicas, físicas e administrativas que estão sendo

implementadas pela entidade. Estas medidas são pautadas em princípios de ética, transparência e segurança de dados, levando em conta os variados contextos de risco a que a organização está exposta.

A entidade estabelece controles internos rigorosos de segurança da informação com o intuito de prevenir qualquer possibilidade de vazamento de dados. Esses controles devem ser estritamente seguidos por todos os empregados, sem exceção.

Em conformidade com a Lei 13.709/2018 (LGPD), os empregados são incumbidos de tomar todas as medidas necessárias para garantir que os dados sejam acessados e tratados de maneira adequada. Além disso, a utilização desses dados deve ser restrita apenas àqueles que realmente necessitam dessas informações para a execução de suas tarefas, principalmente no que diz respeito a dados pessoais sensíveis.

O tratamento de dados pessoais só pode ser efetuado quando o empregado tiver a certeza de que o titular dos dados deu seu consentimento explícito para tal coleta e para as subsequentes atividades de tratamento de dados. Este consentimento deve ser formalizado através da assinatura de um termo de consentimento ou com base em uma das outras hipóteses autorizadoras previstas na legislação de proteção de dados.

Ressaltamos a importância de todos os empregados se familiarizarem e cumprirem rigorosamente esta política, pois a segurança da informação é uma responsabilidade conjunta e essencial para a sustentabilidade e integridade de nossa organização.

Dessa forma, esta Política de Segurança da Informação tem como objetivos:

i. Estabelecer a Segurança da Informação como um dos itens fundamentais no planejamento estratégico da entidade;

ii. Determinar regras comportamentais e diretrizes que os empregados da entidade deverão praticar, as quais garantem a prevenção de incidentes de Segurança da Informação e violação de dados, regras de boa prática de Segurança da Informação e a Proteção de Dados Pessoais ;

iii. Nortear padrões mínimos obrigatórios para o devido uso e proteção das informações e dados pessoais criados, recebidos, armazenados, processados, transmitidos, impressos e tratados pela entidade;

iv. Propagar aspectos referente à Segurança da Informação na entidade;

v. Prover a entidade de recursos e conformidade às Leis de Segurança da Informação, nacionais e internacionais, em especial referente à LGPD (Lei

Geral de Proteção de Dados) e GDPR (General Data Protection Regulation, traduzido por Regulamento Geral de Proteção de Dados);

vi. Elaborar condições para que a entidade dê continuidade à Segurança da Informação através da adoção de diretrizes, normas ou procedimentos que asseguram e reforcem os ativos de informação da entidade objetivando a ascensão da Integridade, Confidencialidade, Autenticidade e Disponibilidade dos ativos de informação da entidade.

Também estão relacionados diretamente com a presente Política o Código de Conduta e Ética e a Política Interna de Privacidade da entidade.

4. DESTINATÁRIOS E ABRANGÊNCIA

A Política de Segurança da Informação da nossa entidade é direcionada a todos os gestores, empregados, estagiários e empregados que integram a organização, doravante chamados de usuários. Nesta condição, todos podem ter acesso a áreas, equipamentos, informações, arquivos, redes e dados que são de titularidade ou propriedade da entidade.

Esta política estabelece normas e recomendações que todos os usuários devem cumprir, em quaisquer operações ou ações que possam impactar a segurança das informações. A sua finalidade é garantir que a integridade, a confidencialidade e a disponibilidade das informações sejam mantidas, minimizando os riscos associados à sua manipulação.

Todos os destinatários desta política são encorajados a observar atentamente as regras aqui estabelecidas, pois elas desempenham um papel crucial na proteção de nossos ativos de informação. O não cumprimento destas disposições acarretará em sanções, conforme estabelecido nesta Política. Adicionalmente, caso seja aplicável, as medidas legais pertinentes poderão ser tomadas.

É essencial para a segurança e o sucesso de nossa organização que cada um de nós compreenda e respeite estas diretrizes. Juntos, podemos assegurar um ambiente de trabalho mais seguro e eficiente, onde a informação é tratada como o valioso ativo que é.

5. DIRETRIZES

5.1 Senhas

Ao longo da jornada de trabalho, diferentes senhas de acesso são requeridas para a utilização de aplicações, sistemas ou acesso a locais específicos. Estas senhas são de caráter pessoal e intransferível, e sob nenhuma circunstância devem ser compartilhadas - nem com terceiros, superiores, equipes de tecnologia ou infraestrutura. A manutenção de rotinas diárias ou quaisquer atividades não requerem a divulgação de sua senha, tornando o titular completamente responsável pelo seu sigilo e uso adequado.

Cada empregado terá acesso apenas às informações estritamente necessárias para o desempenho de suas funções, não possuindo permissões para acessar outras informações da organização.

As senhas devem ser alteradas a cada 90 (noventa) dias.

Não é permitido repetir senhas anteriores ou utilizar as mesmas senhas para diferentes aplicações ou serviços. No entanto, o usuário tem a liberdade de alterar sua senha a qualquer momento, limitado o período a 90 (noventa) dias.

Para reduzir a vulnerabilidade das senhas e a possibilidade de acesso indevido, é necessário estabelecer senhas fortes. Para isso, todas as senhas devem conter:

- No **mínimo**, **14 (quatorze) caracteres de comprimento,** e dentre estes, deve-se conter ao menos:
- 1 (um) número;
- 1 (uma) letra maiúscula
- 1 (uma) letra minúscula
- 1 caractere especial.

Na elaboração da senha, deve-se evitar o uso de:

- Nome de familiares;
- Apelidos pessoais
- Data de nascimento;
- Nome de animais de estimação;
- Palavras inclusas no dicionário;

Rua Antônio de Godói, n° 88 - 16° andar, Bairro Centro São Paulo SP
www.sintrajud.org.br

- Números de documentos pessoais;
- Evitar caracteres sequenciais (1234; abcd) ou repetidos (1111; aaaa; @@@@);
- Em nenhuma hipótese, utilizar o próprio nome ou login na senha;
- Comidas, esportes e/ou hobbies favoritos.

Após a criação da senha, é responsabilidade do usuário memorizá-la. É estritamente proibido anotar a senha em papel físico ou usá-la para fins pessoais ou quaisquer propósitos fora do estipulado na Política de Segurança da Informação.

No caso de uma senha temporária ser fornecida, ela deve ser alterada no primeiro acesso. O Departamento de Segurança da Informação nunca solicitará sua senha para realizar qualquer procedimento ou atendimento. Fique atento a e-mails, mensagens ou chamadas suspeitas solicitando sua senha, e reporte imediatamente qualquer atividade suspeita à equipe de segurança.

Em caso de desligamento de um empregado, a entidade tomará medidas de segurança para restringir imediatamente o acesso aos sistemas, prevenindo qualquer vazamento de dados.

Como componente essencial de nossa Política de Segurança da Informação, é dever de todos os empregados utilizar o cofre de senhas, previamente homologado pela equipe de TI, em seus computadores pessoais. Esse requisito não apenas assegura a segurança das suas credenciais de acesso, mas também protege as informações críticas da nossa organização. A prática de anotar senhas em blocos de notas ou qualquer outro meio físico ou digital não seguro é estritamente proibida e coloca a integridade dos nossos sistemas e da organização como um todo em risco.

5.2 Correio eletrônico/e-mail

Com a evolução da tecnologia, o e-mail ou correio eletrônico se tornou o principal meio de comunicação corporativa, sendo indispensável no dia a dia do trabalho. Embora seja chamado de eletrônico, ele está sujeito a todas as leis e regulamentos aplicáveis aos documentos escritos.

O uso do e-mail SINTRAJUD deve ser restrito aos objetivos e finalidades da entidade, sendo proibido qualquer utilização para benefício pessoal ou fins particulares. O acesso a e-mails pessoais e sites dentro do ambiente de trabalho, utilizando o computador da entidade ou sua rede Wi-Fi, não é permitido.

É importante ressaltar que ao receber um e-mail com origem, conteúdo ou anexos suspeitos ou executáveis, é fundamental não abri-lo antes de verificar se é um e-mail válido. Essas mensagens

podem estar infectadas com vírus. Nesse caso, é recomendado entrar em contato com o Suporte Técnico de TI para obter assistência.

Evite enviar anexos muito grandes, e se necessário, consulte o Suporte Técnico de TI para orientações adequadas.

O e-mail institucional SINTRAJUD não deve ser utilizado para cadastrar-se em sites de terceiros, nem fora do horário de expediente, durante férias ou licenças legais, exceto em casos específicos de solicitação direta, por escrito e justificada pela entidade, para cumprimento de horas extras.

É importante ressaltar que qualquer e-mail enviado sob o domínio da entidade, como e-mails institucionais, não será considerado informação particular. Portanto, a entidade tem o direito de verificar, monitorar e inspecionar os e-mails dos empregados, conforme previsto em contrato de trabalho.

Quanto à ausência temporária do profissional devido a férias, licenças, etc., é necessário configurar o e-mail para enviar automaticamente uma mensagem informando o período de ausência. Além disso, em relação aos correios eletrônicos institucionais, é proibido:

- Transmitir qualquer material, vídeo, documento, imagem que possa ser considerado ofensivo, discriminatório, calunioso, fraudatório, danoso ou ilegal, que possa violar os padrões de ética profissional;
- Transmitir arquivos executáveis como anexo e extensões que possibilitem a propagação de vírus;
- Transmitir spam e promoções não relacionadas ao ambiente institucional;
- Abrir e-mails e seus arquivos anexos que tenham origem de remetentes duvidosos;
- É expressamente proibida a divulgação de informações, dados e documentos considerados sigilosos ou confidenciais dos quais a entidade seja proprietária ou de qualquer um de seus clientes, exceto quando aprovadas de maneira escrita por gerentes e/ou diretoria;
- Compartilhar o endereço de e-mail de outros profissionais sem a sua respectiva permissão.

A entidade possui ferramentas de monitoramento para controlar o acesso dos empregados. Essas ferramentas têm como objetivo bloquear o acesso a determinados sites, portas do computador,

aplicativos e recursos como o Bluetooth. Além disso, elas permitem monitorar as atividades realizadas pelos empregados, inclusive gravando as ações executadas em suas estações de trabalho. Essa ferramenta também possibilita verificar a criação de pastas e o acesso a arquivos.

É expressamente proibido que um empregado acesse o banco de dados de outro empregado sem a devida autorização.

É importante ressaltar que não devem ser enviados ou reenviados e-mails do tipo corrente, avisos de vírus, apelos para ajudar pessoas doentes ou carentes, mensagens de auto ajuda, mensagens filosóficas, piadas, paisagens, fotos, desenhos, alertas policiais, jogos, conselhos, entre outros. Além disso, é recomendado adotar o hábito de verificar a caixa de e-mails diariamente.

5.3 Credenciais de acesso

As credenciais de acesso são autorizações concedidas após o processo de credenciamento, que permitem que uma pessoa ou sistema tenha acesso a determinados recursos. Essas credenciais podem assumir formas físicas, como crachás e cartões, ou eletrônicas, como dados biométricos.

O acesso às informações deve ser controlado e restrito, levando em consideração as responsabilidades de cada usuário. Qualquer forma de acesso além do permitido requer autorização prévia do gestor da área responsável pelas informações. É fundamental garantir que todos os dispositivos de identificação utilizados pela entidade, como crachás, identificação de acesso a sistemas, certificados e assinaturas digitais, bem como a biometria, estejam devidamente vinculados a uma pessoa física. Esses dispositivos devem ser concedidos de forma pessoal, confidencial e intransferível, de acordo com a legislação brasileira e em conformidade com os documentos oficiais reconhecidos legalmente.

O indivíduo associado a tais dispositivos identificadores é responsável pelo seu uso adequado perante a entidade, devendo cumprir a legislação brasileira, tanto no âmbito civil quanto no âmbito criminal. Portanto, é estritamente proibido compartilhar qualquer dispositivo de identificação pessoal com outras pessoas.

5.3.1 Identificação visual (crachá)

A utilização do crachá de identificação da entidade é mandatória, pessoal e intransferível para todos os empregados, sendo obrigatório portá-lo de maneira visível durante todo o período de permanência nas dependências da entidade. Este item é fundamental para a segurança e controle de acesso ao nosso ambiente de trabalho.

No entanto, é expressamente proibido o uso do crachá fora das instalações da entidade para evitar quaisquer potenciais riscos de segurança. O crachá deve ser removido ao sair do prédio e só deve ser usado novamente ao retornar.

Para os empregados que realizam serviços externos e precisam visitar clientes, o crachá deve ser usado nas mesmas condições, a menos que estejam saindo do local de trabalho.

Em caso de perda ou extravio do crachá, é necessário realizar um boletim de ocorrência (BO), comunicar o incidente ao departamento de Recursos Humanos e solicitar imediatamente um novo crachá.

O não cumprimento dessas regras está sujeito às sanções previstas no Capítulo 6 da Presente Política de Segurança da Informação. Pedimos a colaboração de todos para manter nosso ambiente de trabalho seguro e organizado.

5.4 Segurança do ambiente

5.4.1 Política da Mesa Limpa:

Esta política visa garantir a segurança dos dados pessoais e sensíveis. As diretrizes são:

- Documentos não poderão ser deixados na mesa ou em máquinas fotocopiadoras, exceto quando estiverem sendo manuseados por um empregado autorizado e sempre sob seu campo de visão.

- As mesas de trabalho deverão permanecer sempre organizadas, mantendo-se o mínimo possível de objetos sobre elas.

- É obrigatório guardar documentos contendo dados pessoais e sensíveis, tanto em papel quanto em mídia de armazenamento eletrônica, em cofres ou gavetas trancadas.

- A chave destes locais de armazenamento deverá ser mantida em local seguro pelo respectivo responsável, sendo proibido seu empréstimo ou entrega a terceiros, exceto por ordem judicial ou autorização expressa.

Rua Antônio de Godói, n° 88 - 16° andar, Bairro Centro São Paulo SP
www.sintrajud.org.br

5.4.2 Política da Tela Limpa:

A política de "tela limpa" é voltada para a proteção de informações exibidas em monitores. As diretrizes são:

- Ao utilizar computadores, deverá ser mantida a “área de trabalho” limpa, contendo apenas atalhos necessários e essenciais.

- Deverá ser ativado o modo “temporizador” em todos os dispositivos, para que, após **1 (um) minuto de inatividade**, o dispositivo seja bloqueado automaticamente, necessitando de senha para ser reativado.

- Todos os dispositivos deverão ser mantidos desligados quando não estiverem em uso e terem bloqueio para acesso somente por senha, token ou mecanismo de autenticação similar.

5.4.3 Outras Disposições:

- Será proibido o acesso a ambientes sem a devida autorização.

- A retirada não autorizada de arquivos físicos ou digitais que contenham dados pessoais e sensíveis é estritamente proibida.

- O transporte de documentos físicos para fora do local seguro de armazenamento deverá ser devidamente registado, com identificação clara do responsável pelo transporte.

- É estritamente proibido tirar fotografias ou vídeos de qualquer área de trabalho, de computadores, de documentos ou de qualquer outro material com dados pessoais e sensíveis. Essa proibição se aplica a todos os funcionários, visitantes, fornecedores e terceirizados.

5.5 Impressão de documentos

Os serviços de impressão devem ser utilizados exclusivamente para atividades estritamente necessárias dentro da entidade.

É recomendado priorizar o tratamento de dados no formato eletrônico sempre que possível, utilizando a impressão somente quando for necessário obter assinaturas ou carimbos físicos. Além da preocupação com a segurança da informação, é importante considerar a sustentabilidade ambiental ao utilizar esse serviço, evitando a impressão de documentos sempre que possível.

Caso seja necessário imprimir dados pessoais, é fundamental adotar medidas de segurança, incluindo a prática da "mesa limpa" conforme descrito no capítulo anterior, garantindo que dados pessoais e informações estejam acessíveis apenas a pessoas autorizadas.

As impressões devem ser realizadas dentro de cada departamento da entidade, ou na impressora mais próxima. Dessa toda forma, os empregados deverão imprimir os documentos e retirá-los imediatamente.

Qualquer documento impresso que já tenha cumprido sua finalidade deve ser adequadamente descartado, por meio de desfragmentação ou destruição adequada.

5.6 Internet

A entidade estabelece uma política de acesso à internet, autorizando o uso do recurso por meio de um "Login de Acesso" exclusivo.

O acesso à internet é restrito às necessidades de trabalho na SINTRAJUD e não deve ser utilizado para realizar tarefas de terceiros ou atividades paralelas.

Todos os acessos a sites são registrados no servidor de gerenciamento da internet, e as informações estatísticas, como locais acessados, tempo, data e horário, ficam disponíveis para a entidade.

É importante ressaltar que os sites UOL, IG, TERRA, YAHOO, FOLHA ONLINE, YOUTUBE e outros com características de portal, ou jornalismo, apenas poderão ser utilizados para fins comerciais, em setores autorizados e mesmo assim estes não poderão ser deixados abertos após o uso. Esses sites sobrecarregam a rede de comunicações da SINTRAJUD devido às constantes atualizações de informações.

O download de programas e atualizações de software deve ser realizado exclusivamente pela equipe técnica de TI.

Fica explicitamente proibido o download de filmes, músicas e outros materiais **não relacionados ao trabalho**, assim como o acesso a sites inapropriados, de relacionamento ou bate-papo.

5.7 Aparelhos eletrônicos pessoais e institucionais

Rua Antônio de Godói, n° 88 - 16° andar, Bairro Centro São Paulo SP
www.sintrajud.org.br

5.1 Dispositivos e aparelhos eletrônicos pessoais e corporativos

A entidade busca facilitar a mobilidade e o fluxo de informações entre seus funcionários, permitindo o uso de dispositivos portáteis, como notebooks, smartphones e pendrives, de acordo com as normas da ISO 27001, 27002 e 27701 para a gestão da segurança da informação e privacidade.

Restrição no Uso de Dispositivos Pessoais para Recebimento de documentos com dados pessoais e sensíveis de titulares que se relacionam com o SINTRAJUD, incluindo clientes e outros empregados:

É imperativo que os funcionários não recebam arquivos contendo informações confidenciais e dados pessoais e sensíveis em seus dispositivos pessoais, incluindo celulares. Esta medida visa proteger a confidencialidade e integridade dos dados pessoais, sensíveis e outros confidenciais e está alinhada com as melhores práticas de segurança da informação.

Gestão de Informações em Dispositivos Corporativos:

Em relação aos dispositivos móveis corporativos, é crucial seguir um plano de temporalidade para o armazenamento de informações, conforme as normas ISO 27001, 27002 e 27701. Todos os dados relevantes devem ser classificados e mantidos pelo período determinado pelas políticas de retenção de dados da entidade. Após este período, os dados devem ser avaliados e, caso não sejam mais necessários ou exigidos para retenção, descartados de forma segura e responsável.

É expressamente proibido o uso de dispositivos móveis corporativos para o armazenamento, download ou processamento de dados pessoais para fins não profissionais. Isso inclui, mas não se limita a, imagens, vídeos ou documentos pessoais do funcionário, bem como de seus familiares ou contatos pessoais. Esta proibição visa preservar a integridade e a finalidade profissional dos dispositivos fornecidos pela entidade, garantindo a segurança da informação e a privacidade pessoal. Qualquer exceção a esta regra precisa ser expressamente aprovada pela gerência, justificada por uma necessidade de negócio clara e em conformidade com as políticas internas de segurança da informação e as leis de proteção de dados aplicáveis.

Não é permitido emprestar a terceiros os equipamentos portáteis institucionais ou fornecidos pela entidade em qualquer circunstância.

Uso do WhatsApp Business em Celulares Corporativos:

Para melhorar a comunicação e a gestão de informações em dispositivos móveis fornecidos pela entidade, recomenda-se a instalação do WhatsApp Business. Esta versão do aplicativo foi projetada para entidades, oferecendo recursos adicionais para organizar, automatizar e responder rapidamente às mensagens.

Em caso de rescisão do contrato de trabalho, os equipamentos corporativos e quaisquer dados neles armazenados devem ser devolvidos no prazo estipulado, e o funcionário deve assegurar o descarte seguro de informações corporativas armazenadas em dispositivos pessoais.

Política de Bring Your Own Device (BYOD):

A política de BYOD da entidade reconhece a utilidade de dispositivos pessoais no ambiente de trabalho. No entanto, é fundamental que os funcionários que optarem por utilizar seus próprios dispositivos no trabalho assinem a política de BYOD. Esta política define regras claras sobre o uso, segurança, privacidade e responsabilidades associadas aos dispositivos pessoais.

O uso de dispositivos, seja pessoal ou corporativo, deve ser feito de maneira responsável e sempre em conformidade com a política de segurança da informação da entidade. co

A entidade se compromete a oferecer o suporte técnico necessário e a assegurar o cumprimento de todas as diretrizes para promover um ambiente de trabalho seguro e eficiente.

5.8 Home Office

É estritamente proibido o uso de equipamentos particulares não autorizados pelo responsável pela TI para conexões remotas ao ambiente da entidade.

No caso de dispositivos habilitados e autorizados para acesso remoto, é obrigatório que eles sejam configurados pelo departamento de TI com mecanismos de segurança, como criptografia, antivírus, ferramentas para acesso seguro à VPN (Rede Privada Virtual) e firewall pessoal, a fim de garantir a confidencialidade e a integridade das informações da entidade.

Os serviços remotos devem ser interrompidos automaticamente após 5 minutos de inatividade. No entanto, é responsabilidade do empregado ou parceiro encerrar sua sessão imediatamente quando não estiver utilizando os recursos.

É estritamente proibido realizar tratamento de dados em meios físicos, como impressão de documentos, no home office, exceto em casos excepcionais devido ao cargo ocupado ou com autorização do superior hierárquico. Nessas situações, os dados devem ser imediatamente descartados de forma segura, como picotagem ou fragmentação, após o uso.

Em nenhuma circunstância, membros da mesma família poderão ter acesso a dispositivos utilizados para o trabalho e que contenham dados e informações pessoais de titulares, em posse da entidade, bem como informações confidenciais da entidade.

Os dispositivos fornecidos em comodato, destinados ao uso exclusivo do empregado, devem receber os mesmos cuidados aplicados ao trabalho presencial, inclusive em relação aos prazos de repouso.

O não cumprimento deste capítulo pode resultar em sanções disciplinares, desde advertências

até demissões por justa causa, levando-se em consideração a gravidade da infração cometida pelo empregado.

5.9 Backup e prevenção de perda de dados

O processo de backup, que consiste na criação de cópias digitais de segurança de dados pessoais e informações, será realizado de forma automatizada por meio de programas de computador, também conhecidos como "robôs". Essas cópias serão armazenadas externamente, em uma entidade especializada em segurança digital e prevenção de perda de dados, preferencialmente com certificações ISO 27001, 27002 e 27701.

Essa entidade contratada deverá atender a critérios mínimos, como a localidade remota para armazenamento dos backups, garantindo assim a proteção dos dados em caso de problemas na instalação principal. Além disso, a entidade deve fornecer um nível apropriado de proteção física e ambiental em suas instalações, garantindo a integridade dos dados.

A redundância de armazenamento e proteção também é um requisito importante, garantindo a segurança das cópias de backup. A entidade contratada deve cumprir um Acordo de Nível de Serviço (SLA) que garanta uma disponibilidade mínima de 99,8% dos dados e um tempo máximo de restauração (período de restore) de até 12 horas.

Essas medidas garantem a segurança e a integridade dos dados pessoais e informações da entidade, permitindo a recuperação dos mesmos em caso de perda ou falha nos sistemas principais. O *backup* será protegido pelo processo de encriptação e realizado de forma periódica, observando as rotinas, frequência e períodos de retenção abaixo:

5.10 Gestão de incidentes e violação de dados

Na eventualidade de ocorrência de um incidente da segurança da informação, incluídas as hipóteses de incidente de vazamento de dados ou violação de dados, deverão ser documentados os procedimentos necessários por meio de abertura de chamado técnico via sistema, acompanhamento para neutralização ou mitigação e resultado final, devendo ser mantido registro escrito de todo o procedimento via chamado técnico, resguardando o máximo de evidências digitais.

De toda forma, ao ser identificado um vazamento de dados o empregado deverá

imediatamente desconectar da internet e permanecer com a máquina ligada e entrar em contato o mais rápido possível com a TI.

A equipe de segurança deverá imediatamente contatar a DPO (Encarregada pelo Tratamento de Dados Pessoais), nomeada, quando se tratar de incidente envolvendo dados pessoais, para as providências cabíveis, incluindo as comunicações, assim como o gestor de TI para adoção dos procedimentos técnicos.

O relatório de incidente da segurança da informação, a ser registrado via chamado técnico específico, deverá conter as informações e detalhes do incidente, podendo ser atualizado conforme evolução da situação, devendo conter o seguinte. Origem, data, horário (GMT) e local (IP TCP, UDP, etc);

1. Titulares envolvidos
2. Classificação da natureza do incidente e listagem de serviços e sistemas alvos do ataque (ex. código malicioso, vírus, trojan, spyware, phishing por e-mail, engenharia social, tentativa de exploração de vulnerabilidades e acesso remoto, comprometimento de senha, uso de identidade falso, dentre outros);
3. Descrição detalhada do incidente e classificação de grau de criticidade (Alto, Moderado, Baixo);
4. Se houve comprometimento de dados, exposição, transferência, sequestro, categoria e natureza dos dados envolvidos, com listagem completa dos titulares afetados na hipótese de dados pessoais;
5. Logs, Códigos de erro, imagens, registros de sistema e demais evidências digitais.
6. Status do Incidente, observando os seguintes estágios: 1. Detecção do Incidente, 2. Contenção/Mitigação; 3. Erradicação; 4. Recuperação da normalidade do sistema; 5. Avaliação e Registro Final de Evidências.
7. Procedimentos adotados para corrigir eventuais falhas detectadas ou aprimorar a proteção.

O Encarregado de Proteção de Dados (DPO), em casos de vazamento ou violação de dados pessoais, deverá tomar as medidas legais necessárias para notificar a Agência Nacional de Proteção de Dados dentro do prazo máximo de 2(dois) dias úteis, ou outro prazo que venha a ser determinado pela Autoridade Nacional de Proteção de Dados. Além disso, dependendo do caso, os titulares de dados pessoais afetados também devem ser notificados, conforme previsto no artigo 48 da Lei Geral

de Proteção de Dados.

No caso de suspeita fundamentada, com fortes indícios de que um empregado esteja voluntariamente, conscientemente e intencionalmente envolvido em um esquema ilícito de aliciamento de pessoas para sequestro, transferência, violação ou concessão de acesso não autorizado a terceiros, a entidade deve tomar medidas preventivas, como interromper o acesso do empregado ao sistema, suspender suas atividades laborais e iniciar um processo de sindicância.

Se for comprovado e constatado que o empregado agiu de forma intencional e direta em uma operação ilícita que resulte em violação de dados ou ofereça um risco concreto de violação, o empregado sofrerá a sanção disciplinar de justa causa direta, conforme previsto na Consolidação das Leis do Trabalho (CLT) e na Política de Segurança da Informação da entidade. Além disso, o empregado poderá ser responsabilizado por eventuais prejuízos causados à entidade decorrentes da concretização do incidente de segurança ou violação de dados, nos termos previstos no contrato de trabalho ou no seu aditivo contratual.

No caso de envolvimento do empregado na violação de dados, mesmo que por negligência, de acordo com o disposto no parágrafo primeiro do artigo 462 da CLT e os termos do contrato de trabalho, poderão ser aplicadas sanções disciplinares, que podem variar desde advertências até a aplicação de justa causa direta, dependendo da gravidade da falta cometida.

5.11 Descarte de dados

De acordo com a norma ISO 27002, é estabelecido que as informações menos críticas devem possuir menos controles, enquanto as informações mais sensíveis devem ter um maior nível de controle. Isso inclui todos os tipos de dados pessoais, os quais devem ser fragmentados de forma a impossibilitar qualquer visualização por terceiros não autorizados.

Medidas técnicas, físicas e administrativas devem ser adotadas para eliminar os dados pessoais assim que sua finalidade for alcançada, em conformidade com as diretrizes estabelecidas pela Lei Geral de Proteção de Dados (LGPD). A entidade deverá implementar procedimentos adequados de descarte em computadores, e-mails, mídias e outros meios físicos, e todos os empregados devem cumprir essas medidas de segurança, realizando o descarte no momento apropriado e da maneira correta.

Em alinhamento com as normas ABNT NBR ISO/IEC 27701:2019 e ABNT NBR ISO/IEC 27002:2022, os empregados da entidade devem tomar as medidas necessárias para garantir que os

dados sejam descartados adequadamente após atingirem sua finalidade, especialmente quando se tratarem de dados pessoais sensíveis. Essas diretrizes se aplicam a todas as operações, pessoas e processos que fazem parte do sistema de informações da entidade, incluindo empregados, membros do conselho, diretores, fornecedores, clientes e terceiros que tenham acesso aos dados tratados pela entidade.

O empregado não deve descartar qualquer mídia de forma independente, sendo necessário comunicar e entregar ao setor de TI, ou equivalente, para que o descarte seja realizado de acordo com procedimentos seguros. Os dados físicos devem ser sempre picotados ou fragmentados antes do descarte.

É importante ressaltar que todos os dispositivos que contenham mídias de armazenamento de dados devem ser analisados antes do descarte, garantindo que todas as informações sensíveis tenham sido removidas de forma segura.

Quando dispositivos defeituosos contiverem informações sensíveis e/ou dados pessoais, é necessário realizar uma avaliação de risco para determinar se é mais adequado destruí-los fisicamente ou consertá-los.

O não cumprimento das normas estabelecidas nesta política de segurança da informação poderá resultar em sanções disciplinares, conforme previsto no artigo 482 da Consolidação das Leis do Trabalho (CLT).

5.12 Dos ativos

Os ativos da organização devem ser usados exclusivamente dentro da Entidade, e é de responsabilidade de todos os empregados zelarem por eles.

6. SANÇÕES DISCIPLINARES PELO DESCUMPRIMENTO DA PRESENTE POLÍTICA

Baseado em todos os tópicos expostos anteriormente, salienta-se que todas as ações, princípios, objetivos e diretrizes da presente Política de Segurança da Informação aplicam-se aos trabalhadores com vínculo empregatício, aos empregadores, gestores e sócios da entidade. Portanto, todas as ações tomadas contrárias à presente Política de Segurança da Informação serão de responsabilidade do respectivo profissional.

Rua Antônio de Godói, n° 88 - 16° andar, Bairro Centro São Paulo SP
www.sintrajud.org.br

Por outro lado, é importante salientar que, se o descumprimento ocorrer devido a uma falha ou erro da entidade, o funcionário não será submetido a sanções disciplinares. Neste cenário, a empresa assumirá a responsabilidade por quaisquer lapsos que levem ao não cumprimento da política e tomará as medidas necessárias para corrigir a situação, garantindo que tais incidentes não se repitam no futuro.

Com o objetivo de assegurar-se a segurança da informação, poderá ser estabelecido ao infrator das boas práticas presentes nesta política de segurança da informação, as seguintes sanções:

- **Advertência verbal:** nos casos considerados como falta leve, haverá uma advertência verbal ao infrator, relembrando-o sobre as boas práticas da Política de Segurança da Informação;
- **Advertência Escrita:** nos casos considerados como falta média. Haverá uma advertência escrita ao infrator, neste caso o infrator receberá uma cópia sobre a Política de Segurança da Informação e será exigida a sua releitura;
- **Suspensão Disciplinar:** nos casos considerados como falta grave. O infrator estará sujeito à suspensão disciplinar, mediante notificação por escrito, devendo assinar o documento na presença de uma testemunha. O período de suspensão será proporcional aos danos causados por tal falta, não podendo ser superior a 30 dias. Em seu retorno, o profissional deverá realizar um curso de reciclagem relacionado às condutas de segurança da informação, aplicadas pela equipe responsável, reler a presente política e realizar prova com aproveitamento mínimo de 70%.
- **Justa Causa:** nos casos considerados como falta gravíssima, haverá a rescisão contratual direta, ou na reincidência de condutas mais leves, como exposto no Contrato de Trabalho ou no Termo Aditivo ao Contrato de Trabalho, além do direito de regresso ao responsável pela falta, nos termos do contrato de trabalho.

Nos casos de recebimento de uma advertência escrita, suspensão disciplinar ou rescisão contratual, é disponibilizado o direito de revisão da sanção em relação ao Comitê de Segurança da Informação.

7. PROGRAMA DE CONSCIENTIZAÇÃO, EDUCAÇÃO E TREINAMENTO EM SEGURANÇA DA INFORMAÇÃO

O programa de conscientização, educação e treinamento para os empregados, tem o intuito de explicar para os empregados o porquê da segurança da informação.

É importante que todos os empregados entendam o objetivo da segurança da informação e os impactos positivos e negativos para a entidade.

Este programa de conscientização ocorrerá da seguinte forma:

Treinamento (Admissão): todos os empregados iniciantes, deverão realizar os treinamentos iniciais, bem como receber, ler e assinar todas as políticas internas da organização. Nenhum empregado iniciará suas atividades, sem antes realizar e ter ciência de todas as políticas internas e externas, bem como sanções pelo descumprimento.

Treinamento: Os treinamentos de capacitação inicial ocorrerão nos setores individualizados ou em conjunto conforme cronograma anexado à presente Política de Privacidade e Segurança da Informação voltada para os empregados.

Reciclagem: Os treinamentos de capacitação serão periódicos.

Processo de adequação: Treinamento dedicado aos empregados que agiram ou estiveram envolvidos em condutas não éticas, formados por sessões de conscientização e advertência.

Treinamento de Implementação: Os empregados, receberão treinamento de capacitação decorrente da adequação/implementação da LGPD. Após os treinamentos, os empregados serão submetidos a uma avaliação do treinamento. Caso o empregado não atinja a pontuação necessária, ele, passará por um novo treinamento de capacitação.

Material de Apoio: Durante os treinamentos, serão distribuídos materiais de apoio com as principais dúvidas e respostas, juntamente com uma cópia da presente Política de Privacidade em Segurança da Informação.

Os treinamentos serão realizados pelo Comitê de Proteção de Dados Pessoais ou pela DPO (Encarregada de Proteção de Dados Pessoais).

8. FISCALIZAÇÃO E EFETIVIDADE

A conformidade com as diretrizes estabelecidas nesta política será monitorada pelo Comitê de Proteção de Dados Pessoais, responsável por manter relatórios mensais contendo registros de apontamentos e sugestões de melhorias.

Em caso de identificação de uma não conformidade, seja por meio do Canal de Notificação, Comitê de Proteção de Dados ou qualquer outra fonte, medidas corretivas e reparadoras devem ser adotadas imediatamente, no prazo máximo de 5 dias úteis a partir do registro da ocorrência. Essas medidas têm o objetivo de corrigir a não conformidade e evitar que ocorram danos adicionais.

Rua Antônio de Godói, n° 88 - 16° andar, Bairro Centro São Paulo SP
www.sintrajud.org.br

O tratamento das não conformidades deve ser realizado de forma eficiente e eficaz, considerando a gravidade da situação e os impactos potenciais na segurança da informação. Além disso, é importante documentar todas as ações tomadas durante o processo de tratamento, a fim de manter um registro claro e transparente das medidas adotadas.

O Comitê de Proteção de Dados será responsável por supervisionar o cumprimento das medidas coercitivas e reparadoras, garantindo que sejam implementadas de acordo com as melhores práticas e com as exigências legais e regulatórias aplicáveis. Dessa forma, busca-se garantir a efetividade da política de segurança da informação e proteção de dados na entidade.

9. CONFIDENCIALIDADE E PRIVACIDADE

A proteção da privacidade e confidencialidade das informações dos empregados é uma prioridade fundamental para a Entidade. Por esse motivo, são estabelecidos controles e processos internos para garantir a manutenção do sigilo dos dados pessoais dos titulares.

É importante ressaltar que o uso ou divulgação não autorizada de informações confidenciais é considerado crime e está sujeito a sanções civis e penais. Portanto, é dever de cada usuário notificar imediatamente as áreas de TI, Compliance e Segurança da Informação caso tomem conhecimento de qualquer utilização inadequada de recursos fornecidos pela Entidade.

Qualquer desconformidade em relação a esta política, que seja do conhecimento do empregado, deve ser prontamente reportada para o e-mail dpo@sintrajud.org.br. A entidade valoriza a transparência e incentiva os empregados a compartilharem informações sobre possíveis violações ou problemas de segurança.

Ao ingressarem na organização, todos os empregados recebem um termo de confidencialidade e não divulgação de informações. Esse termo é assinado pelo empregado e armazenado junto com sua ficha cadastral. Além disso, o empregado recebe uma cópia do termo para sua referência e conhecimento.

Essas medidas visam reforçar o compromisso da Entidade com a proteção dos dados pessoais e a garantia da confidencialidade das informações dos empregados. O cumprimento dessas diretrizes é essencial para a preservação da segurança e privacidade de todos os envolvidos.

Rua Antônio de Godói, n° 88 - 16° andar, Bairro Centro São Paulo SP
www.sintrajud.org.br

10. DISPOSIÇÕES FINAIS

Esta Política tem o objetivo de estabelecer diretrizes e orientações relacionadas à segurança da informação na entidade. No entanto, é importante ressaltar que esta política não abrange todas as possíveis questões éticas que podem surgir no ambiente da entidade. Caso ocorram condutas que violem o bom senso, a ética e a moral, poderão ser aplicadas medidas coercitivas, mesmo que não estejam expressamente mencionadas nesta política.

A presente Política entra em vigor imediatamente após sua divulgação e não possui previsão para término. No entanto, será revisada anualmente ou em períodos menores, caso ocorram alterações legais ou edições de novas normas administrativas relevantes, como as Resoluções da Autoridade Nacional de Proteção de Dados (ANPD).

Quando ocorrerem alterações nesta política, a entidade comunicará os empregados por meio de canais internos, garantindo que todos estejam cientes das atualizações e das normas vigentes.

Com o intuito de assegurar a conformidade com as diretrizes estabelecidas nesta Política, serão realizados treinamentos e auditorias periódicas. Essas ações têm o objetivo de avaliar o cumprimento das normas da Política de Segurança da Informação (PSI), identificar possíveis usos incorretos, condutas incompatíveis, diagnosticar e corrigir problemas, além de promover treinamentos e conscientização para aprimorar constantemente as boas práticas relacionadas à segurança da informação.

É importante ressaltar que este documento foi elaborado com base na LGPD (Lei Geral de Proteção de Dados), GDPR (General Data Protection Regulation) e nas normas ISO 27001, 27002 e 27701, garantindo uma abordagem alinhada com as melhores práticas e padrões internacionais de segurança da informação.

11. LEI E FORO APLICÁVEIS

A Política de Privacidade, bem como a coleta, tratamento ou transmissão de Dados do Titular, serão regidos pelo disposto na LGPD.

Quaisquer litígios decorrentes da validade, interpretação, ou execução da presente Política de Privacidade, ou que estejam relacionados com a coleta, tratamento ou transmissão de Dados do titular serão dirimidos nesta cidade, local de prestação de serviços, nos termos do artigo 651 da CLT.

A presente política foi aprovada em de junho de 2023.

DocuSigned by:
5878691DF6764D1...

DPO DIRETORIA