CEM PRIVACIDADE

100 situações comuns que desafiam a privacidade e a proteção de dados

Categoria do Risco: Comportamental / Humano	
Situação/Conduta	**Impacto à Privacidade do Titular**
Compartilhar número de celular de colegas em grupos	Exposição de dado pessoal identificável; invasão de privacidade. O compartilhamento deve ser consentido pelo titular e direcionado, em particular, à pessoa por ele autorizada
Utilizar o modo viva voz em chamadas, sem informar ao interlocutor	Exposição da privacidade e quebra de confiança
Publicar fotos de colegas em confraternizações e eventos internos da unidade, não oficiais, sem seu consentimento	Violação do direito de imagem e privacidade
Publicar dados pessoais de terceiros em rede social privada	Exposição indevida de dado pessoal, risco de fraude financeira (golpes) e invasão de privacidade
Repassar informações de saúde de colega em grupo de trabalho	Violação de dado sensível; risco de discriminação
Expor dados pessoais ou situações particulares de magistrados/servidores/estagiários/público interno em geral	Exposição da privacidade
Compartilhar e/ou divulgar opinião política, convicção religiosa ou dado referente à vida sexual, dado genético ou biométrico de colega na unidade, em grupos ou reuniões de trabalho	Exposição de dados sensíveis, risco de discriminação e violação da privacidade
Repassar prints de telas com dados pessoais do usuários, sem base legal de tratamento	Vazamento de informações confidenciais ou sigilosas

Conversar sobre casos sigilosos (de saúde, disciplinar ou processual) em áreas comuns, sem as cautelas recomendadas à segurança da informação	Violação de dever funcional e do sigilo judicial
Deixar computador desbloqueado em ambiente compartilhado de trabalho	Risco de acesso indevido a dados pessoais e corporativos
Permitir que terceiros usem computador logado em nome de usuário interno	Acesso indevido a sistemas internos e e-mails.
Usar nuvem pessoal para armazenar dados institucionais	Transferência não autorizada para ambiente externo
Manter acessos de ex-usuário ativo a sistemas corporativos	Acesso indevido prolongado a dados corporativos
Solicitar dados pessoais em excesso e/ou sem justificativa	Coleta excessiva; violação dos princípios da necessidade e adequação
Compartilhar dados pessoais com setores não envolvidos na atividade	Tratamento sem base legal adequada
Reutilizar dados pessoal para finalidade diversa da informada ao titular na coleta original	Desvio de finalidade; uso indevido de dados
Utilizar os campos "Para" e "CC" para enviar e-mail com utilização de lista de transmissão em massa (ao invés do campo adequado: CCo)	Risco de exposição de dados e privacidade (possibilita que o receptor do e-mail, ao clicar apenas em responder a todos, envie resposta a todos os contatos da lista)

Categoria do Risco: Comportamental / Legal

Situação/Conduta	Impacto à Privacidade do Titular
Publicar dados pessoais de servidores afastados para tratamento de saúde	Exposição de dados sensíveis, risco de discriminação e violação à privacidade
Exigir biometria para franquear o acesso ou condicionar o atendimento público à pessoa já devidamente identificada, por documento oficial válido	Coleta excessiva; violação dos princípios da necessidade e adequação *Biometria é dado sensível
Manter visível número de conta bancária em execução em ambiente público	Risco de fraude e violação de sigilo bancário
Incluir dados pessoais de menores em publicações processuais abertas, sem anonimização/pseudonimização	Violação de privacidade e direitos da criança e do adolescente
Divulgar contracheque com dados pessoais de dependente menor e descontos/consignados	Exposição de dados financeiros e familiares

Divulgar ficha funcional de servidor em processo disciplinar público	Exposição indevida de dados profissionais e pessoais
Responder e-mail sem acautelar pela retransmissão do conteúdo a todos os contatos da lista de transmissão em massa	Impacta a privacidade do titular
Exposição indevida de dados, com violação de sigilo e potencial dano moral ao titular. Violação direta de segredo de justiça, com impacto institucional e sanções. A publicidade indevida amplia o alcance do dano e dificulta a remediação. Impacta a privacidade do titular e a confiança na instituição	Armazenamento indevido de dados, com risco de incidente de segurança e responsabilização do controlador frente ao titular
Gravar reuniões por iniciativa própria, sem o consentimento dos participantes ou sem base legal	Violação do direito de imagem e voz. Impacta a privacidade do titular e a confiança na instituição
Acessar sistemas institucionais através de aplicativo móvel sem senha (celular e notebook), com risco de furto do aparelho ou acesso indevido por terceiros	Exposição indevida da instituição, com risco de incidente de segurança da informação e cibernética
Não comunicar o Tribunal* sobre o furto de aparelhos particulares contendo registro de senhas, logins e documentos institucionais *Notebook: chamado à TIC, celular: Secretaria Administrativa, sem prejuízo de informar a Secretaria de Segurança Institucional)	Exposição indevida da instituição, com risco de incidente de segurança da informação e cibernética
Não substituir senha de acesso à conta de usuário, em caso de suspeita de violação	Exposição indevida da instituição, com risco de incidente de segurança da informação e cibernética
Não comunicar imediatamente a área de TI sobre o recebimento de mensagens com vírus, spam ou qualquer outro tipo de conteúdo inadequado	Exposição indevida da instituição, com risco de incidente de segurança da informação e cibernética
Enviar ou armazenar mensagens com informações sensíveis, inclusive senhas e/ou dados pessoais de outrem, para pessoas ou organizações não autorizadas	Exposição indevida de dados pessoais, com violação de sigilo e potencial dano moral ao titular. Impacta a privacidade do titular e a confiança na instituição
Enviar ou armazenar material obsceno, ilegal, comercial, político-partidário, de interesse estritamente pessoal, de propaganda, de entretenimento, bem como mensagens do tipo corrente, spam, e hoax (mensagens enganosas)	Mau uso do correio eletrônico. Impacto na credibilidade e imagem da instituição
Enviar ou armazenar propositalmente mensagens contendo vírus ou qualquer forma de rotinas de programação prejudiciais às estações de trabalho e ao sistema de e-mail	Mau uso do correio eletrônico. Exposição indevida da instituição, com risco de incidente de segurança da informação e cibernética

Enviar ou armazenar mensagens contendo fotos, músicas, vídeos, animações, ou qualquer mídia que não seja de interesse específico da instituição ou que possua proteção de direito autoral sem a devida autorização	Violação de direitos autorais e potencial dano moral ao titular. Impacta a proteção de dados e a confiança na instituição
Forjar a identidade de outra pessoa ou fazer falsa declaração de sua identidade	Prejuízo à rastreabilidade e violação da segurança da informação. Impacta a privacidade do titular e a confiança na instituição
Suprimir, modificar ou substituir a identidade do remetente ou do destinatário de uma mensagem de e-mail institucional	Prejuízo à rastreabilidade e violação da segurança da informação. Impacta a privacidade do titular e a confiança na instituição
Acessar de forma não autorizada as caixas postais de terceiros	Acesso indevido a dados pessoais, com violação de sigilo e potencial dano moral ao titular. Impacta a privacidade do titular e a confiança na instituição
Não comunicar qualquer acesso ou autorização concedida indevidamente, para a imediata correção das permissões e acessos aos recursos de TIC	Risco de acesso indevido e exposição indevida de dados
Conceder permissões de acesso a dados sensíveis ou informações restritas sob sua guarda individual	Risco de acesso indevido e exposição indevida de dados
O Gestor deixar de informar à área de TIC e à Unidade responsável pelos terceirizados do Tribunal qualquer alteração interna que implique mudança na concessão de acessos	Risco de acesso indevido e exposição indevida de dados
Gestor deixar de gerenciar os perfis de acesso ao sistema PJE, de acordo com as funções desempenhadas pelos usuários lotados na unidade, principalmente desativar os acessos sempre que houver a remoção ou desligamento desses usuários	Risco de acesso indevido e exposição indevida de dados
Permitir que estagiários acessem convênios como Renajud, Detran, Infojud, Bacen e qualquer outro que transpareça a situação das partes, em virtude da necessidade de restringir o acesso a informações sigilosas	Acesso indevido, violação da confidencialidade e perda de rastreabilidade de ações
Invadir a privacidade de terceiros, buscando acesso a senhas e dados privativos, violando sistemas de segurança de informação ou redes privadas internas ou externas de computadores conectadas à Internet	Acesso indevido e violação da confidencialidade
Acessar, facilitar o acesso ou não comunicar o acesso indevido a sistemas de convênios institucionais, para consulta de dados pessoais de terceiros, inclusive de geolocalização, sem base legal ou para fins particulares	Acesso indevido e violação da confidencialidade

Deixar de comunicar a ausência de cláusula de LGPD em contratos e convênios que envolvam compartilhamento de dados pessoais e outras operações de tratamento	Acesso indevido e violação da confidencialidade
Não adotar as cautelas de praxe, quanto à proteção de dados pessoais, na rotina da sua unidade	Risco de incidente, com impacto a privacidade do titular e a confiança na instituição

Categoria do Risco: Comportamental / Organizacional

Situação/Conduta	Impacto à Privacidade do Titular
Não apagar imediatamente e/ou compartilhar dados pessoais recebidos acidentalmente por email institucional	Tratamento inadequado por falhas de processo, ampliando a exposição de dados e dificultando o controle e a responsabilização. Pode envolver dado pessoal sensível de saúde, agravando o risco de discriminação e violação da intimidade. Impacta a privacidade do titular e a confiança na instituição
Não participar de treinamentos e programas de conscientização sobre segurança e privacidade recomendados à unidade pelo Controlador ou juiz Encarregado de Dados	Risco de incidente, com impacto a privacidade do titular e a confiança na instituição
Assumir conduta passiva e pensar que a proteção de dados e a segurança da informação são atribuições exclusivas das unidades especializadas	Risco de incidente, com impacto a privacidade do titular e a confiança na instituição
Boa prática: limpar regularmente os cookies e/ou o histórico de navegação para remover rastros de sua atividade online	Evita rastreamento de atividades online por terceiros e minimiza a chance de perfilamento do usuário, utilizado para publicidade direcionada

Categoria do Risco: Comportamental / Tecnológico

Situação/Conduta	Impacto à Privacidade do Titular
Fazer backup de processos sigilosos em dispositivo pessoal	Risco de vazamento por armazenamento inseguro
Permitir acesso irrestrito a processos sigilosos no PJe	Violação de confidencialidade processual
Manter arquivos pessoais de ex-servidores da unidade	Retenção indevida de dados; violação do princípio da minimização

Copiar dados pessoais, extraídos a partir de sistemas corporativos, para planilhas particulares, sem autorização	Perda de controle sobre o uso e destino dos dados, para a Instituição. Armazenamento indevido pelo operador
Utilizar senhas fracas ou compartilhadas	Acesso indevido a sistemas com dados pessoais e risco de vazamento de dados
Compartilhar senhas de e-mail da unidade, durante férias do gestor, ao invés de usar a opção 'conta delegada'	Acesso indevido e perda de rastreabilidade de ações
Usar e-mail pessoal para tratar dados institucionais	Perda de controle sobre guarda e destino dos dados
Enviar e-mail com dados pessoais ao destinatário errado	Vazamento acidental de dados

Categoria do Risco: Físico / Procedimental

Situação/Conduta	Impacto à Privacidade do Titular
Jogar documentos impressos com dados pessoais ou sigilosos no lixo comum, sem fragmentação mecânica e/ou anonimização	Possível acesso indevido a informações pessoais por terceiros

Categoria do Risco: Jurídico / Legal

Situação/Conduta	Impacto à Privacidade do Titular
Reutilizar laudos médicos em processos distintos, sem autorização ou base legal	Desvio de finalidade; tratamento indevido e sem base legal.
Divulgar informações médicas em laudos anexados sem sigilo	Violação de dado sensível de saúde
Divulgar dados pessoais e/ou informações de processo/documentos gravados com sigilo judicial	Violação de segredo de justiça e de privacidade
Não orientar estagiários e terceirizados sobre tratamento de dados pessoais	Risco de incidentes recorrentes por desconhecimento da LGPD
Permitir que estagiários manuseiem processos sigilosos sem supervisão	Risco de divulgação acidental de dados pessoais

Imprimir documentos com dados sensíveis e deixá-los expostos em mesas públicas	Acesso indevido e risco de extravio
Não diligenciar pelo segredo de justiça em processos envolvendo doenças estigmatizantes (HIV, Hepatite crônica, Hanseníase e tuberculose) de que trata a Lei 14.289/2022	Divulgação indevida de dados pessoais sensíveis relacionados à saúde, violando o dever de sigilo estabelecido pela Lei nº 14.289/2022. A falta de diligência no resguardo do segredo de justiça em casos de doenças estigmatizantes (HIV, hepatite crônica, hanseníase e tuberculose) pode causar constrangimento pela exposição pública da doença, discriminação, danos morais e abalo à dignidade do titular, além de responsabilização administrativa e judicial da instituição. Impacta severamente a privacidade, o sigilo médico e a confiança social na Justiça do Trabalho
Disponibilizar consulta a processo físico com segredo de justiça a terceiros	Exposição indevida de dados em peças processuais ou atos oficiais, com violação de sigilo e potencial dano moral ao titular. Violação direta de segredo de justiça, com impacto institucional e sanções. Impacta a privacidade do titular e a confiança na instituição
Permitir acesso de pesquisadores a processos/documentos em arquivo permanente e/ou histórico, sem prévia autorização do juiz encarregado de dados e/ou controlador	Risco de divulgação de dados sigilosos. Impacta a privacidade do titular e a confiança na instituição
Compartilhar dados pessoais do público interno para fins de pesquisa externa, sem prévia autorização do controlador e/ou juiz encarregado	Impacta a privacidade do titular e a confiança na instituição.
Permitir consulta pública a documento sigiloso ou gravado com segredo de justiça	Exposição indevida de dados em peças processuais ou atos oficiais, com violação de sigilo e potencial dano moral ao titular. Violação direta de segredo de justiça, com impacto institucional e sanções. Impacta a privacidade do titular e a confiança na instituição
Deixar de comunicar caso ou suspeita de incidente de segurança envolvendo dados pessoais ao juiz Encarregado pelo tratamento de dados pessoais	Risco de vazamento de dados pessoais, informações confidenciais ou sigilosas. Impacta a privacidade do titular e a confiança na instituição
Passar informações pessoais em consulta processual realizada por telefone, sem prévia e inequívoca identificação do requerente	Exposição indevida de dado pessoal, risco de fraude financeira (golpes), potencial prejuízo ao trabalhador (listas de discriminação) e invasão de privacidade
Publicar decisões com endereço residencial do reclamante	Exposição de dados pessoais e risco à segurança física

Permitir download de processos trabalhistas, com dados de identificação pessoal, em locais públicos (abertos)	Risco de exposição de dados em dispositivos de terceiros. Risco à proteção do trabalhador (listas de discriminação), com prejuízo material e moral ao titular do dado pessoal
Enviar áudio de audiência por aplicativo não institucional	Risco de interceptação e vazamento de conteúdo sensível
Compartilhar documentos de processos via aplicativos pessoais	Perda de rastreabilidade e segurança da informação
Tornar público dado pessoal sensível em processo administrativo disciplinar	Divulgação desproporcional e indevida
Não diligenciar pela eliminação de dado pessoal a termo, com temporalidade expirada (retenção prolongada de dados pessoais sem necessidade/base legal)	Armazenamento indevido de dados, com risco de incidente de segurança e responsabilização do controlador frente ao titular
Fornecer certidão trabalhista explicativa a terceiro, a partir de consulta pelo nome do trabalhador, sem autorização ou base legal	Exposição indevida de dados em peças processuais ou atos oficiais, com potencial dano ao titular, inclusive material (listas discriminatórias). Impacta a privacidade do titular e a confiança na instituição
Gravar reuniões de mediação do CEJUSC	Desrespeito ao princípio da confidencialidade (Resolução CSJT nº 415/2025 - art. 18, § 1º). Impacta a confiança na instituição

Categoria do Risco: Organizacional / Legal

Situação/Conduta	Impacto à Privacidade do Titular
Solicitar informações de saúde de titular integrante do público interno do Tribunal, sem autorização ou base legal	Risco de quebra de sigilo médico
Manter público processos administrativos sigilosos (PROAD, Vetor etc)	Exposição indevida de dados em peças processuais ou atos oficiais, com violação de sigilo e potencial dano moral ao titular. Violação direta de segredo de justiça, com impacto institucional e sanções. Impacta a privacidade do titular e a confiança na instituição

Publicar atas do Colegiado Temático contendo informações sigilosas	Exposição indevida de dados, com violação de sigilo e potencial dano moral ao titular. Violação direta de segredo de justiça, com impacto institucional e sanções. A publicidade indevida em atos judiciais amplia o alcance do dano e dificulta a remediação. Impacta a privacidade do titular e a confiança na instituição
Fornecer senha de correio eletrônico da unidade, em vez de optar pelo acesso de forma delegada	Acesso indevido e perda de rastreabilidade de ações
Reutilizar folha de papel contendo dados pessoais, sensíveis ou sigilosos	Exposição indevida de dados em peças processuais ou atos oficiais, com potencial violação de sigilo e dano moral ao titular. Impacta a privacidade do titular e a confiança na instituição
Manter os logins de acesso a público interno não mais pertencente à unidade	Acesso indevido e perda de rastreabilidade de ações
Público interno deixar de informar o antigo gestor sobre login de acesso mantidos após sua saída da unidade	Acesso indevido e perda de rastreabilidade de ações

Categoria do Risco: Organizacional / Processual

Situação/Conduta	Impacto à Privacidade do Titular
Inserir documento médico em documentos público, sem tarja de CID	Divulgação de dado de saúde sensível
Guardar documentos físicos sigilosos em armários sem tranca ou envelope lacrado	Risco de acesso indevido e extravio. Impacta a privacidade do titular e a confiança na instituição
Arquivar formulários impressos sem controle quanto à identificação do dado pessoal e restrição de acesso	Risco de acesso indevido a dados sigilosos e perda de confidencialidade
Fotografar documentos funcionais e armazená-los no celular pessoal	Risco de exposição acidental em aplicativos ou backup automático
Exibir informações pessoais em relatórios estatísticos	Possibilidade de reidentificação de titulares

Categoria do Risco: Técnico / Tecnológico

Situação/Conduta	Impacto à Privacidade do Titular
Usar Wi-Fi público para acessar sistemas corporativos	Interceptação de comunicações; roubo de credenciais
Constar número de telefone ou e-mail pessoal nas atas de audiência	Exposição pública de meio de contato pessoal
Guardar cópias de documentos pessoais em pen drives sem senha	Perda ou roubo pode expor dados pessoais
Cadastrar familiares em sistemas institucionais, sem base legal	Coleta desnecessária e não consentida
Exibir prints de sistemas, contendo dados pessoais, em treinamentos	Divulgação acidental em ambientes abertos
Não registrar logs de acesso a sistemas contendo dados pessoais	Impossibilidade de rastrear incidentes de privacidade
Permitir que estagiários utilizem senhas de servidores para realizar quaisquer atividades, ainda que relacionadas ao estágio	Acesso indevido e perda de rastreabilidade de ações
Permitir que estagiários utilizem-se de Mídia Criptográfica (token) de servidores para realização de atividades nos sistemas deste tribunal.	Acesso indevido e perda de rastreabilidade de ações