Guia Informativo de
Boas Práticas

Considerando a Lei Geral de Proteção de Dados Pessoais - 13.709/2018

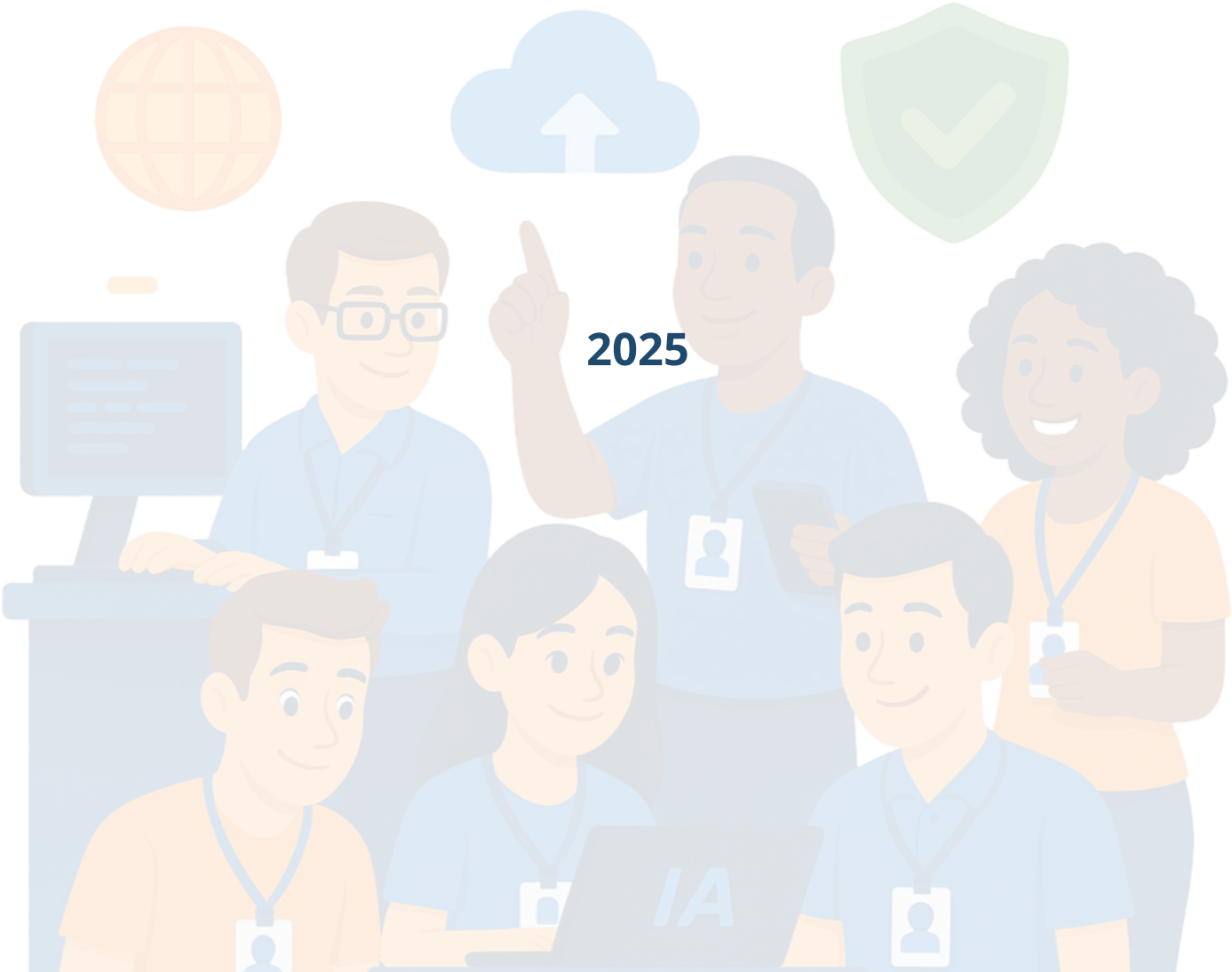
CAGEPA
COMPANHIA DE ÁGUA E ESGOTOS DA PARAÍBA

CAGEPA
COMPANHIA DE ÁGUA E ESGOTOS DA PARAÍBA

ASSESSORIA DE PROTEÇÃO DE DADOS PESSOAIS E DA PRIVACIDADE

João Paulo Delfino da Silva
Chefe de Assessoria

Fábio Costa dos Santos



2025

Sumário

Apresentação

Compilado das orientações produzidas pela Assessoria de Proteção de Dados Pessoais e Privacidade (APD) divulgadas através do projeto LGPD no seu Dia a Dia.

A Proteção de dados pessoais é um compromisso institucional e também uma responsabilidade individual de todos que integram a Companhia de Água e Esgotos da Paraíba (CAGEPA). A Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece princípios e regras que visam garantir a privacidade, a segurança e o uso responsável das informações e dados pessoais, fortalecendo a confiança entre a Companhia , seus colaboradores, clientes e a sociedade.

Este guia foi elaborado com base nas orientações da Assessoria de Proteção de Dados Pessoais e da Privacidade (APD) e tem como objetivo apresentar, de forma prática e acessível, recomendações de conduta para o dia a dia de trabalho. Aqui você encontrará orientações claras sobre como lidar corretamente com dados pessoais, prevenir incidentes e contribuir para a conformidade da CAGEPA com a LGPD, além de narrar para cada temática casos práticos fictícios para melhor compreensão da temática.

Mais do que um guia informativo, este documento é um aliado no fortalecimento da cultura de proteção de dados pessoais dentro da Companhia, reforçando a importância de cada colaborador como agente ativo na preservação da privacidade e da confiança.

Uso de Inteligência Artificial (IA)

O uso de IA consiste na aplicação de sistemas e tecnologias capazes de executar tarefas que normalmente requerem inteligência humana, como análise de dados, reconhecimento de padrões, tomada de decisões e aprendizado a partir de experiências.

O uso da IA visa automatizar, otimizar ou apoiar processos, garantindo eficiência e inovação, sempre observando princípios éticos, segurança, privacidade e conformidade legal.

As Inteligências Artificiais otimizam a criação de conteúdos, mas é essencial utilizá-las com responsabilidade para atender à LGPD. Confira boas práticas para proteger os dados pessoais quando utilizar tal ferramenta:

- **Anonimize Informações:** Remova ou substitua dados que possam identificar pessoas ou expor informações sensíveis, garantindo a privacidade.
- **Evite Dados Identificáveis:** Não insira nomes, documentos ou qualquer dado que possa ser vinculado a indivíduos em redes neurais compartilhadas.
- **Proteja Dados Corporativos:** Mantenha informações estratégicas ou internas da empresa fora de plataformas de IA's de acesso público.
- **Atenção aos Riscos:** Dados inseridos podem ser utilizados por terceiros, já que algumas plataformas compartilham informações para alimentar suas bases. Segurança é indispensável.
- **Não compartilhe credenciais de plataforma de IA:** Cada credencial é destinada exclusivamente a área de atuação. O compartilhamento pode expor informações além do necessário, ampliando os riscos de incidentes de segurança e de vazamento de dados pessoais.
- **Mantenha-se atualizado:** Faça a leitura do REDIR 025/2025 e demais normativas que regram o bom uso da IA no ambiente de trabalho.

Caso Prático

SITUAÇÃO

Marcelo, analista de comunicação, está elaborando um relatório para divulgação interna. Para agilizar, decide usar uma plataforma gratuita de IA online.

Ele insere na ferramenta um texto contendo dados pessoais de clientes, incluindo nomes, números de contrato e registros de atendimento, para que a IA gere um resumo. Sem perceber, a política da plataforma permite armazenar e usar as informações fornecidas para treinar seus modelos.

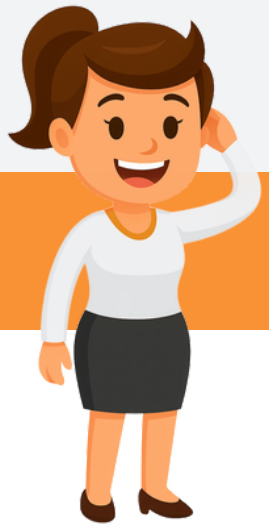
Algumas semanas depois, um cliente questiona como informações internas apareceram em um conteúdo gerado por outra pessoa usando a mesma plataforma.

CONSEQUÊNCIAS

- Vazamento de dados pessoais para terceiros sem consentimento ou base legal.
- Violação aos princípios da segurança (Art. 6º, VII) e da finalidade (Art. 6º, I) da LGPD.
- Risco de responsabilização administrativa, cível, penal e danos à reputação da empresa.

COMO EVITAR

- Nunca inserir dados pessoais ou informações sensíveis em plataformas públicas de IA ou sem contrato que assegure proteção necessária das informações.
- Anonimizar qualquer informação antes de utilizar a ferramenta.
- Confirmar se a plataforma segue regras de segurança e confidencialidade compatíveis com a LGPD.
- Preferir ferramentas corporativas sugeridas pela área de TI e pela Assessoria de Proteção de Dados Pessoais e da Privacidade.



LIÇÃO APRENDIDA

A conveniência da IA não pode comprometer a privacidade e a segurança. Dados pessoais e dados estratégicos devem ser protegidos mesmo em processos de automação e otimização de tarefas.

Mesa Limpa e Tela Bloqueada

Mesa Limpa e Tela Bloqueada é a prática de segurança da informação que consiste em manter o ambiente de trabalho organizado e livre de documentos, mídias ou dispositivos contendo informações pessoais ou privadas quando não estiverem em uso, além de bloquear o acesso ao computador ou outros equipamentos sempre que o usuário se ausentar. O objetivo é prevenir acessos não autorizados, proteger dados confidenciais e reduzir riscos de vazamento de informações.

A segurança da informação vai além de sistemas e senhas. Pequenos hábitos diários ajudam a proteger dados pessoais e sensíveis dentro da Cagepa.

Mesa Limpa

- Guarde documentos físicos em locais seguros.
- Não anote senhas em papéis visíveis.
- Proteja pendrives e dispositivos de armazenamento.
- Descarte documentos com dados pessoais corretamente.
- Após a reunião, recolha documentos e anotações e apague os registros em quadros ou superfícies de apoio.

Tela Bloqueada

- Bloqueie a tela ao sair (Windows + L).
- Configure o bloqueio automático.
- Nunca compartilhe sua senha.
- Ao acessar dados pessoais, certifique-se que as informações visualizadas não esteja ao alcance de terceiros não autorizados.

A segurança dos dados pessoais é um compromisso de todos!
Adote essas práticas e proteja as informações processadas pela Cagepa.

Caso Prático

SITUAÇÃO

Fernanda, secretária, ao encerrar o expediente, deixou sobre a mesa formulários contendo dados de clientes e manteve seu computador ligado, com o sistema interno ainda aberto.

Na manhã seguinte, um prestador de serviço entrou na sala para realizar manutenção elétrica e foi surpreendido utilizando o celular pessoal para capturar informações expostas, tanto nos documentos quanto no sistema acessível. Entre os dados visualizados estavam nomes, CPFs e informações de contas de clientes.

CONSEQUÊNCIAS

- Exposição indevida de dados pessoais a pessoa não autorizada.
- Descumprimento de práticas de segurança da informação e violação de princípios da LGPD.
- Necessidade de registro de incidente e comunicação à área de Proteção de Dados Pessoais e da Privacidade para avaliação.

COMO EVITAR

- Guardar documentos físicos em armários ou gavetas trancadas ao final do expediente.
- Descartar documentos desnecessários usando métodos seguros, como fragmentadoras.
- Bloquear a tela ao se afastar do computador, usando Windows + L ou equivalente.
- Configurar bloqueio automático após alguns minutos de inatividade.

LIÇÃO APRENDIDA

Manter a mesa limpa e a tela bloqueada não é apenas organização, é proteção de informação. Esses cuidados simples evitam incidentes e preservam a confiança no trabalho da Cagepa.

Princípio da Necessidade

O Princípio da Necessidade é um dos princípio previsto na Lei Geral de Proteção de Dados Pessoais (LGPD), tal tema determina que o tratamento de dados pessoais deve se limitar ao mínimo necessário para a realização de suas finalidades legítimas, específicas e previamente informadas ao titular. Isso significa coletar, processar e armazenar apenas os dados estritamente adequados, pertinentes e proporcionais para atingir o objetivo pretendido, evitando excessos e reduzindo riscos à privacidade.

No dia a dia corporativo, lidamos com uma grande quantidade de informações e, para garantir a conformidade com a LGPD, devemos seguir o princípio da necessidade, ou seja, coletar e utilizar apenas os dados essenciais para a execução da atividade.

Por que isso é importante?

- **Menos dados, menos riscos:** reduzimos a exposição a vazamentos e acessos indevidos.
- **Mais segurança para a Cagepa e para os titulares:** protegemos empregados, clientes, fornecedores e demais colaboradores.
- **Adequação legal:** cumprimos as diretrizes da LGPD, garantimos proteção à dignidade da pessoa humana e evitamos penalidades.

Quais boas práticas devo ter em mente no momento da coleta?

- Antes de solicitar qualquer dado pessoal, verifique se a informação é realmente necessária para a finalidade pretendida previamente informada ao titular.
- Solicite apenas os dados pessoais estritamente essenciais para a finalidade da atividade.
- Evite armazenar informações desnecessárias ou sem uma justificativa clara.
- Caso precise descartar documentos com dados pessoais, faça isso de forma segura.
- Nunca compartilhe informações sem autorização e sem verificar a necessidade real do repasse.

SITUAÇÃO

Caso Prático

Ricardo, administrador, está realizando um cadastro para abertura de um chamado técnico. O formulário exige apenas nome, endereço e telefone para contato.

Por hábito, Ricardo também anota a data de nascimento e o número do RG do cliente, mesmo sem que haja qualquer exigência para o serviço solicitado. Ele arquiva essas informações junto ao processo físico, sem base legal ou justificativa clara para a coleta.

Meses depois, ocorre um vazamento interno de documentos e esses dados adicionais, que nunca foram necessários para a execução do serviço, também são expostos.

CONSEQUÊNCIAS

- Exposição indevida de dados pessoais sem relação com a finalidade do tratamento.
- Perda de confiança por parte do titular dos dados.
- Risco de sanções pela ANPD por violar o princípio da necessidade (Art. 6º, III da LGPD).

COMO EVITAR

- Antes de solicitar qualquer informação, avaliar se é realmente necessária para a finalidade.
- Coletar e armazenar apenas o mínimo de dados pessoais possível.
- Garantir que formulários e sistemas estejam ajustados para não exigir campos desnecessários.
- Treinar equipes para compreender o conceito de minimização de dados.

LIÇÃO APRENDIDA

Coletar dados pessoais “por precaução” ou “para uso futuro” sem finalidade clara aumenta riscos, dificulta a gestão da privacidade e fere a LGPD. Menos é mais quando se trata de proteção de dados pessoais.

Prevenção de Incidentes

Prevenção de Incidentes de segurança é um conjunto de medidas, práticas e procedimentos adotados para identificar, reduzir e eliminar vulnerabilidades que possam gerar falhas, vazamentos, perdas ou acessos não autorizados a informações sigilosas e dados pessoais. Envolve em ações proativas de monitoramento, capacitação, manutenção de sistemas e aplicação de controles de segurança, com o objetivo de proteger dados, garantir a continuidade das operações e minimizar impactos antes que ocorram incidentes.

Proteger dados pessoais é um compromisso com a segurança, privacidade e credibilidade da Cagepa.

Com a LGPD em vigor, a prevenção é essencial:

- **Previna falhas:** Preservar a privacidade evita incidentes e protege a reputação.
- **Reduza riscos:** Pequenas atitudes impedem acessos indevidos.
- **Atue dentro da lei:** Cumprir a LGPD reforça nossa responsabilidade e integridade.

Boas práticas que fazem a diferença:

- Use senhas fortes e não compartilhe.
- Certifique-se de uma base legal para armazenar ou compartilhar dados.
- Evite links suspeitos e anexos desconhecidos.
- Sempre descarte papéis de forma correta, principalmente quando possuírem informações sigilosas e dados pessoais.

Prevenir incidentes é responsabilidade de todos. Pequenas ações hoje garantem a segurança para amanhã!

Caso Prático

SITUAÇÃO

Thiago, coordenador, costuma usar a mesma senha para o e-mail corporativo e para suas redes sociais pessoais. Durante um acesso a um site de promoções, sua senha é capturada por um vazamento externo.

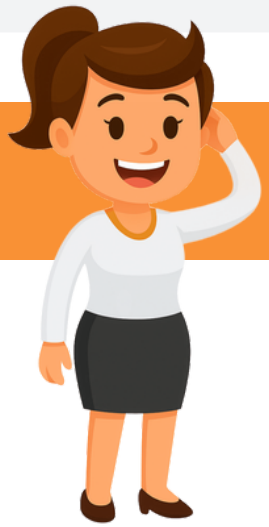
Dias depois, criminosos tentam acessar seu e-mail corporativo utilizando a mesma senha. Como a conta não tinha autenticação em dois fatores, eles conseguem entrar, leem mensagens internas e baixam anexos que continham dados pessoais de clientes.

CONSEQUÊNCIAS

- Acesso indevido a informações internas e dados pessoais de clientes.
- Incidente de segurança notificado internamente e possível necessidade de comunicação à ANPD e aos titulares afetados.
- Necessidade de troca imediata de senhas e reforço de segurança em outros sistemas corporativos.

COMO EVITAR

- Utilizar senhas fortes, únicas e não compartilhá-las entre sistemas.
- Ativar autenticação em dois fatores sempre que possível.
- Não clicar em links ou abrir anexos de remetentes desconhecidos.
- Garantir que todo armazenamento e compartilhamento de dados esteja respaldado por base legal.



LIÇÃO APRENDIDA

Medidas preventivas simples, como criar senhas fortes e evitar práticas inseguras, por exemplo, compartilhar credenciais, clicar em links suspeitos ou utilizar dispositivos não confiáveis, são essenciais para proteger dados pessoais e a reputação da Cagepa.

Classificação de Dados Pessoais

Classificação de dados pessoais é o processo de identificar, categorizar e rotular os dados de acordo com seu tipo, sensibilidade e nível de criticidade, considerando o risco associado ao seu uso e à sua divulgação. Na LGPD, essa classificação distingue, por exemplo, “dados pessoais” e “dados pessoais sensíveis”, permitindo aplicar medidas de segurança e controles de acesso adequados para proteger a privacidade e garantir o tratamento conforme a legislação vigente.

No cotidiano digital, lidamos com diferentes tipos de informações e precisamos tratá-las com a devida atenção. Pensando nisso, a Lei Geral de Proteção de Dados Pessoais (LGPD) classifica os dados em duas categorias

Classificação dos dados:

- **Dados pessoais:** identificam alguém diretamente ou indiretamente (nome, CPF, e-mail, telefone, endereço e etc).
- **Dados pessoais sensíveis:** revelam aspectos íntimos da pessoa (estado de saúde, religião, orientação sexual, política, etnia, biometria e etc) e, por isso, seu tratamento deve ser mais criterioso e justificado.

De acordo com a LGPD, o tratamento de dados sensíveis geralmente exige consentimento específico, exceto em casos previstos na legislação, como os de proteção da vida, prevenção à fraude, tutela da saúde ou cumprimento de obrigação legal.

Mais do que cumprir a lei, tratar dados com responsabilidade é um compromisso com o respeito, a transparência e a confiança. Um cuidado que protege tanto as pessoas como a imagem da Cagepa.

Caso Prático

SITUAÇÃO

Júlia, assistente administrativa, está elaborando um relatório sobre atestados do último semestre. Para ilustrar a apresentação, ela decide incluir uma lista com nomes, telefones e e-mails de funcionários que estiveram de atestado neste período.

Além disso, para justificar sua apresentação, Júlia menciona no relatório informações de saúde de dois funcionários que apresentaram atestados médicos. O documento é enviado por e-mail para diversos setores, incluindo áreas que não têm relação com o caso.

CONSEQUÊNCIAS

- Exposição indevida de dados pessoais (nomes, e-mails, telefones) e dados pessoais sensíveis (informações de saúde) para pessoas sem necessidade de acesso.
- Violação dos princípios da necessidade (Art. 6º, III) e da segurança (Art. 6º, VII) da LGPD.
- Risco de incidente de segurança e necessidade de adoção de medidas corretivas.

COMO EVITAR

- Antes de compartilhar informações, avaliar se todos os destinatários precisam realmente ter acesso aos dados.
- Anonimizar ou pseudonimizar dados sempre que possível, especialmente os sensíveis.
- Tratar dados sensíveis apenas com consentimento ou nas demais hipóteses legais previstas na LGPD.
- Disponibilizar relatórios e apresentações apenas às pessoas autorizadas.

LIÇÃO APRENDIDA

Nem todos os dados pessoais são iguais. Os dados pessoais sensíveis exigem cuidado redobrado, pois seu uso indevido pode causar danos significativos aos titulares e gerar responsabilização para a Cagepa e para os agentes que processam a informação.

Prevenção contra Phishing

Prevenção contra *Phishing* é o conjunto de práticas e medidas voltadas a identificar, bloquear e evitar tentativas de fraude eletrônica nas quais criminosos se passam por entidades confiáveis para obter informações sigilosas, como senhas, dados pessoais ou financeiros. Envolve ações como conscientização dos usuários, verificação de remetentes, análise de links e anexos suspeitos, uso de ferramentas de segurança e políticas internas para reduzir o risco de ataques.

Phishing é um golpe virtual em que cibercriminosos enganam usuários para obter informações sigilosas, como senhas, dados bancários e documentos pessoais, o que inclui os dados pessoais sob responsabilidade da Cagepa.

Redobre a atenção ao identificar as situações abaixo:

- Mensagens com urgência exagerada (“responda imediatamente” ou “sua conta será bloqueada”);
- Ofertas suspeitas (prêmios, sorteios ou promoções);
- Links estranhos (passe o mouse antes de clicar e verifique o link);
- Anexos inesperados, mesmo de contatos conhecidos;
- Remetentes desconhecidos ou e-mails com domínios incomuns;
- Solicitações indevidas de dados pessoais de fornecedores, empregados ou colaboradores.

Em caso de suspeita, contate imediatamente a **Subgerência de Segurança e Infraestrutura em TI** da Cagepa pelo e-mail *sgis@cagepa.pb.gov.br*

A segurança começa por você!

Caso Prático

SITUAÇÃO

Paulo, analista, recebe um e-mail aparentemente enviado pela "Gerência de TI" com o assunto: "*Ação imediata necessária: sua conta será bloqueada em 24 horas*".

O e-mail contém o logotipo da empresa e um link que solicita login e senha corporativos. Pressionado pela urgência da mensagem, Paulo clica no link e insere suas credenciais.

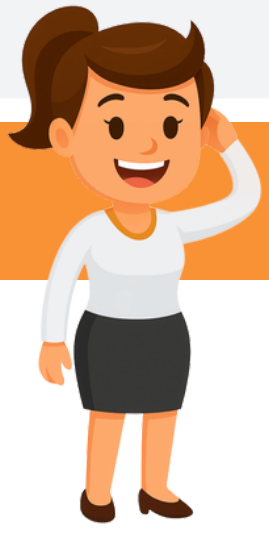
Poucas horas depois, o sistema identifica um acesso não autorizado ao seu e-mail corporativo, de um endereço de IP internacional. Os invasores baixaram anexos contendo dados pessoais de clientes e funcionários.

CONSEQUÊNCIAS

- Vazamento de dados pessoais de clientes e colaboradores, configurando incidente de segurança.
- Necessidade de notificação interna, avaliação de impacto e possível comunicação à ANPD e aos titulares afetados.
- Risco de danos reputacionais e aplicação de sanções administrativas.

COMO EVITAR

- Sempre verificar o remetente e o domínio do e-mail.
- Passar o mouse sobre links antes de clicar para conferir o endereço real.
- Nunca fornecer dados de login ou senha em links recebidos por e-mail ou mensagens não solicitadas.
- Em caso de dúvida, contatar imediatamente a equipe de TI ou a Assessoria de Proteção de Dados Pessoais e da Privacidade antes de agir.



LIÇÃO APRENDIDA

Mensagens com senso de urgência, pedidos inesperados de informações ou links suspeitos são sinais de phishing. Um clique descuidado pode comprometer dados sensíveis e gerar sérias consequências para a Cagepa, para o agente que realizou o processamento e para os titulares dos dados.

Compartilhamento de Dados Pessoais

Compartilhamento de Dado Pessoal é o ato de transmitir, disponibilizar ou conceder acesso a dados pessoais a terceiros, internos ou externos à CAGEPA, por qualquer meio, físico ou digital. Esse processo deve ocorrer apenas para finalidades legítimas, específicas e previamente informadas ao titular, observando os princípios da LGPD, incluindo segurança, necessidade, adequação e transparência, além da adoção de medidas para proteger a privacidade e evitar uso indevido das informações.

Lembre-se:

- Compartilhe apenas quando necessário, com finalidade legítima, dentro da lei, respaldado em uma base legal e sempre com boa-fé;
- Registre e controle todos os compartilhamentos realizados, pois o titular dos dados pessoais pode solicitar informações sobre com quem os dados foram compartilhados e por qual motivo;
- Use ferramentas institucionais seguras. Evite e-mails pessoais, planilhas desprotegidas ou aplicativos informais;
- Antes de compartilhar dados pessoais com fornecedores, prestadores de serviço, órgãos públicos e terceiros, verifique se estão em conformidade com a LGPD, confirme a existência de cláusulas de proteção de dados pessoais nos contratos firmados e exija termo de sigilo e confidencialidade. (Modelos disponíveis em: www.cagepa.pb.gov.br/lgpd)

Evite erros como:

- Compartilhar dados pessoais com pessoas ou áreas que não precisam acessá-los;
- Enviar informações sem base legal ou sem autorização;
- Ignorar os cuidados e a segurança dos parceiros envolvidos no tratamento de dados pessoais.

SITUAÇÃO

Caso Prático

Carla, analista de RH, recebe uma solicitação urgente de um colega de outro setor pedindo a lista com nomes, CPFs e endereços de e-mail de todos os colaboradores. Ele não informa claramente o motivo, apenas diz que é “para agilizar um trabalho interno”.

Sem verificar se havia base legal ou autorização para seu colega realizar tratamento dos dados solicitados, Carla envia o arquivo por e-mail pessoal, sem criptografia ou senha. Dias depois, alguns colaboradores relatam ter recebido mensagens de propaganda de uma empresa terceirizada que nunca teve relação com a Companhia.

CONSEQUÊNCIAS

- Vazamento de dados pessoais para terceiros não autorizados, caracterizando incidente de segurança e infração à LGPD.
- Necessidade de comunicação interna sobre o incidente, avaliação de impacto e possível notificação à ANPD.
- Exposição da instituição a risco reputacional e possíveis penalidades.

COMO EVITAR

- Confirmar sempre a finalidade e a base legal antes de compartilhar dados pessoais.
- Utilizar somente canais institucionais seguros e, se necessário, proteger o arquivo com senha ou criptografia.
- Compartilhar apenas os dados estritamente necessários para a finalidade informada.
- Registrar o compartilhamento para fins de auditoria.

LIÇÃO APRENDIDA

Compartilhar dados pessoais sem verificação prévia é um risco real. A LGPD exige cautela, rastreabilidade e proteção em todas as etapas do tratamento de dados pessoais, especialmente no compartilhamento.

Princípio da Adequação

Princípio estabelecido pela Lei Geral de Proteção de Dados Pessoais (LGPD) que determina que o tratamento de dados pessoais deve ser compatível com as finalidades previamente informadas ao titular e com o contexto em que os dados foram coletados. Garante que o uso das informações esteja alinhado às expectativas legítimas do titular, evitando desvios de propósito e assegurando transparência e conformidade com a legislação.

Você já pensou se estamos usando os dados pessoais da forma correta? A LGPD diz que só podemos usar os dados pessoais para o que foi informado no momento da coleta. Isso se chama princípio da adequação (Art. 5º, Inciso II – LGPD). Ou seja, não podemos guardar ou usar dados "por precaução" ou "para usar depois", sem um motivo claro e informado.

O que podemos fazer:

- Dizer sempre o porquê do pedido de dados pessoais.
- Usar os dados pessoais só para o que foi informado ou permitido por lei;
- Nunca repassar dados pessoais sem a devida base legal;
- Rever formulários, sistemas e processos se os mesmos estão de acordo com esse princípio.

Cumprir o princípio da *adequação* é mais do que uma exigência legal, é respeito e transparência com quem confia seus dados pessoais à CAGEPA

SITUAÇÃO

Caso Prático

João, atendente, está realizando o cadastro de um cliente para instalação de uma nova ligação de água. No formulário, além dos dados necessários (nome, endereço, CPF e telefone), ele também solicita a data de nascimento, profissão do cliente e orientação sexual.

Quando o cliente pergunta para que servem essas informações adicionais, João responde: "É só para termos no sistema, caso precise no futuro." Nenhum motivo claro e específico foi informado, e essas informações não estavam previstas como necessárias na política de privacidade.

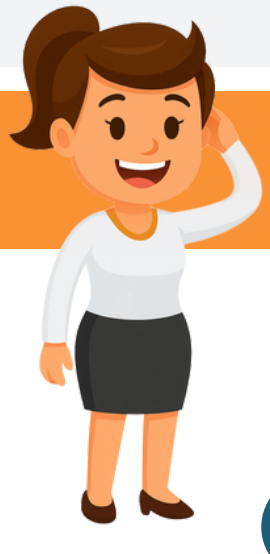
CONSEQUÊNCIAS

- Coleta de dados sem finalidade legítima clara e previamente informada, ferindo o princípio da adequação (Art. 6º, II da LGPD).
- Risco de questionamentos por parte do titular e eventual necessidade de exclusão dos dados coletados de forma inadequada.
- Possibilidade de autuação ou sanções pela Autoridade Nacional de Proteção de Dados (ANPD) em caso de reclamação.

COMO EVITAR

- Solicitar apenas os dados necessários para a finalidade informada ao cliente.
- Se for realmente preciso coletar novas informações, explicar claramente o motivo e obter consentimento, quando aplicável.
- Garantir que formulários e sistemas estejam configurados para não exigir dados sem necessidade justificada.

LIÇÃO APRENDIDA



Guardar ou usar dados pessoais "por precaução" ou "para usar depois" sem finalidade legítima e clara é uma violação à LGPD. Respeitar o princípio da adequação protege a privacidade do titular e fortalece a confiança na CAGEPA.

Reutilização de Papéis Impressos

Reutilização de papéis impressos é uma prática sustentável que consiste em aproveitar folhas já utilizadas, total ou parcialmente, para novas impressões ou anotações, desde que não contenham informações confidenciais ou sensíveis. Essa medida contribui para a redução do desperdício, otimização de recursos, diminuição do impacto ambiental e incentivo a hábitos mais conscientes no ambiente de trabalho.

Reaproveitar papéis é, sim, uma prática sustentável. Mas é fundamental garantir que essa atitude não exponha dados pessoais eventualmente presentes nos documentos, conforme estabelece o princípio da segurança previsto na LGPD.

Muitos documentos físicos podem conter informações sigilosas, estratégicas ou dados pessoais. Reutilizá-los sem a devida atenção pode resultar em exposição indevida. Por isso, antes de usar uma folha antiga como rascunho ou repassá-la a outra pessoa, verifique se ela contém informações que não devem ser compartilhadas.

A LGPD exige responsabilidade em todas as etapas do tratamento de dados pessoais, inclusive nos pequenos hábitos do dia a dia. Então lembre-se: sempre que um documento não for mais necessário, ou contiver informações sensíveis, realize o descarte de forma segura, utilizando fragmentadoras ou métodos apropriados.

SITUAÇÃO

Caso Prático

Maria, assistente administrativa, durante uma reunião, percebe que está sem folhas para anotações e decide reaproveitar alguns papéis já impressos que encontrou na impressora da copa.

Sem verificar o conteúdo, começa a usar o verso desses papéis para anotar pautas da reunião. No final do dia, deixa o bloco de folhas sobre a mesa da sala de reuniões. No dia seguinte, um visitante externo, aguardando atendimento, folheia os papéis e encontra em uma das folhas reutilizadas uma lista com dados de contato e CPF de clientes.

CONSEQUÊNCIAS

- Os dados pessoais foram expostos a um terceiro não autorizado, caracterizando incidente de segurança.
- O incidente foi registrado internamente e comunicado à área de Proteção de Dados Pessoais e da Privacidade.
- Houve necessidade de notificar os titulares dos dados e registrar o incidente junto à ANPD, conforme gravidade da exposição.

COMO EVITAR

- Antes de reutilizar papéis impressos, verificar se contêm dados pessoais ou informações sigilosas.
- Caso contenham, destruir com fragmentadora ou utilizar outro método seguro de descarte.
- Implementar campanhas internas de conscientização sobre reutilização segura de papel.

LIÇÃO APRENDIDA

Sustentabilidade e proteção de dados pessoais podem caminhar juntas, mas é necessário cuidado para que práticas ambientais não se tornem fonte de incidentes de segurança.

CAGEPA
COMPANHIA DE ÁGUA E ESGOTOS DA PARAÍBA

GOVERNO DA PARAÍBA