ORIENTAÇÕES DA CARTILHA DA LGPD

8. Boas práticas para segurança e proteção dos dados pessoais

Abaixo, listamos as boas práticas recomendadas e obrigatoriedades que todos os colaboradores da instituição devem seguir, com o objetivo de evitar qualquer desconformidade com a LGPD, ou incidentes de segurança com dados pessoais.

8.2. Política de telas e mesas limpas

A política da mesa limpa consiste em organizar sua mesa de trabalho, não deixando expostos documentos manuscritos ou impressos acessíveis a terceiros. Por isso, devemos nos atentar ao ciclo de vida dos dados pessoais: criação, armazenamento, manipulação e descarte. Documentos com dados pessoais sensíveis devem ser tratados com medidas adicionais de segurança adicionais, ou seja, não podem ser acessados por pessoas não autorizadas. Para isso, devemos nos atentar onde os documentos serão impressos, armazenados e descartados.

Siga as diretrizes da SPDM/PAIS sobre imprimir o mínimo possível de documentos para preservar o meio ambiente e os dados pessoais, bem como busque orientação de sua liderança sobre o correto descarte de papéis, preferencialmente com o uso de máquinas fragmentadoras para a adequada de descaracterização do documento.

Senhas, logins, dados telefônicos, lista de e-mails, números e códigos de documentos, não devem ser expostos e anexados ao monitor do computador, CPU ou qualquer objeto. Cadernos, agendas e outros documentos impressos devem sempre ser armazenados em gavetas com chave. Devemos nos atentar também ao “post it”, recurso que pode ser físico ou digital que é amplamente utilizado, onde lembretes ficam expostos a todo momento nas telas de computadores. Caso seja necessário o uso, não exponha dados pessoais.

8.3. Uso adequado de senhas

Recomendamos que as senhas sejam periodicamente atualizadas, conforme o conceito de senha segura que será apresentado a seguir:

Conforme comunicado de mudança de senha de acesso à rede SPDM/PAIS, com objetivo de manter seguro as informações/dados institucionais e evitar ataques de cibercriminosos, é necessário alterar periodicamente as senhas de acesso, preferencialmente a cada trimestre.

A senha de acesso é pessoal e intransferível, sendo o usuário responsável por todas as atividades desenvolvidas através dela, bem como por sua guarda com segurança e sigilo.

A nova senha deverá conter no mínimo oito caracteres, com os seguintes parâmetros: letras maiúsculas, letras minúsculas, números, caracteres especiais (“$”, ”%”, ”&”), evitando senhas contendo somente sequências numéricas (123...) ou alfabéticas (abc...), além de senhas de fácil dedução (nome da máquina, nome do usuário, data de nascimento e outros).

8.4. Utilização de e-mail

O uso do e-mail institucional deverá ser feito única e exclusivamente para finalidades profissionais, obedecendo os princípios de confidencialidade, práticas de compartilhamento de e-mail com pessoas não autorizadas e a impressão e/ou o armazenamento, sem o consentimento institucional, são proibidos.

Devemos nos atentar aos e-mails recebidos de fontes duvidosas, ou até mesmo de um outro membro da instituição em caso de suspeitas sobre seu conteúdo do e-mail. Muitas ameaças virtuais utilizam táticas relativamente antigas para invadir uma rede de computadores ou, simplesmente para coletar dados da vítima que abre um arquivo zipado ou um link no corpo do e-mail com código malicioso.

O e-mail é uma das principais ferramentas de comunicação da instituição, sendo utilizado para compartilhar e armazenar dados pessoais, sensíveis e sigilosos. Exemplos: uma pessoa interessada em algum serviço enviou um e-mail solicitando orçamento e fornecendo dados pessoais, como nome, telefone e endereço; um cliente enviou um e-mail para um processo administrativo com dados pessoais, como RG, CPF e dados bancários; uma unidade de saúde enviou por e-mail os prontuários de um paciente, contendo diversos dados sensíveis de saúde.

Para cumprir a LGPD e proteger os dados pessoais no uso dos e-mails, orientamos que você:

- Não clique em links suspeitos ou pop-ups de ofertas e promoções;
- Não abra arquivos desconhecidos e/ou detectados como não seguros;
- Não inclua em cópia endereços de e-mail que não estejam diretamente envolvidos na demanda;
- Não desabilite filtros anti-spam, filtros de e-mail e antivírus integrado.
- De acordo com a pesquisa da IBM sobre o custo das violações de dados, entre 2021-2022 os incidentes de segurança causados por e-mails corrompidos impactaram as empresas em 4.91 milhões de dólares. Por isso, em caso de suspeita ou incidentes de

segurança relacionados a ameaças virtuais, recomendamos que acionem o D.T.I imediatamente, para que as tratativas e ações adequadas sejam rapidamente tomadas.

8.5. Bloqueio da estação de trabalho (computador)

Ao se ausentar, mesmo que por um período curto, sua estação de trabalho deverá ser bloqueada. Caso este procedimento não seja colocado em prática seus dados pessoais e aqueles tratados pela instituição estarão expostos a outros colaboradores ou, até mesmo, a pessoas que não tenham qualquer vínculo com a Instituição.

Os riscos associados à exposição da informação podem variar, desde a alteração proposital ou acidental de algum documento ou registro em sistema até a exclusão definitiva dos dados pessoais.

O procedimento para o bloqueio da tela é simples e prático, bastando apenas que o colaborador pressione simultaneamente duas teclas do teclado (Windows + L).

8.8. Tramitação de documentos via malote

O uso do malote deve seguir os cuidados necessários para não violação da proteção das informações. É importante lembrar que estamos transitando dados sigilosos ou documentos institucionais, assim é necessário lembrar:

- Evitar o uso de embalagens transparentes em que é possível identificar o conteúdo do documento;
- Manter os envelopes sempre lacrados;
- É necessário o preenchimento correto e completo das informações do destinatário, assim como do remetente;
- Respeitar o destinatário