BOAS PRÁTICAS DA LGPD - PROTEÇÃO DE DADOS PESSOAIS E SENSÍVEIS

A LGPD lei Geral de Proteção de Dados surgiu para garantir mais transparência na coleta e armazenamento de dados digitais. Visando algumas boas práticas é importante lembrar:

- Sobre a importância do USO ADEQUADO DE SENHAS institucionais: É de acesso pessoal e intransferível, o usuário é responsável por todas as atividades desenvolvidas através dela, por guardá-la com segurança e sigilo, é necessário que sejam feitas alterações periódicas de todas as senhas de acesso à rede, conforme comunicado de Mudança de senha de acesso à rede SPDM/PAIS. Além da criação de senhas fortes, a utilização de caracteres diferentes, não utilizar a mesma senha em todas as contas e sistemas, e efetuar a troca periódica da senha.
- Somos responsáveis pelo conteúdo de mensagens enviadas via E-MAIL CORPORATIVO sob nossa identificação, sendo uma das principais ferramentas de comunicação da instituição, utilizado para compartilhar e armazenar dados, deverá ser feito única e exclusivamente para finalidades profissionais, obedecendo a princípios de confidencialidade, e práticas de compartilhamento de e-mail com pessoas não autorizadas, a impressão, 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.
- Toda e qualquer mensagem distribuída pelo e-mail da instituição são de propriedade da mesma, a caixa de entrada corporativa pode ser monitorada sem que haja notificação prévia caso a instituição achar necessário, havendo evidências de que o funcionário não está aderindo às regras citadas nas políticas institucionais e Manual de Conformidade Administrativa, Políticas e Princípios de Integridade a instituição terá o direito de tomar as medidas disciplinares cabíveis.
- Não é permitido compartilhar mensagens, contendo dados confidenciais, sensíveis, pessoais ou anexo pertencente a outros sem obter primeiro a permissão do responsável, ou enviar e-mails contendo comentários ofensivos. É recomendado a utilização de identificação digital ou assinatura padrão de conhecimento prévio de outros colaboradores, citando o nome completo e função.

- Importante os cuidados quanto a UTILIZAÇÃO DE EQUIPAMENTOS INSTITUCIONAIS, não é permitida a modificação das características do sistema operacional, alteração, ou instalação de software não homologado pela SPDM/PAIS. A utilização de desktops, notebook, smartphone e outros recursos de TI devem observar os termos e formulários específicos e ser restrita ao uso profissional, sendo seu uso vetado para finalidades particulares.
- Devemos nos atentar sobre COMENTÁRIOS SOBRE A INSTITUIÇÃO, atenção ao que falamos e se o local é apropriado para determinadas conversas. Um risco significativo que, muitas vezes, não detém a necessária atenção, é quando a informação vai além dos dados contidos em redes de computadores ou documentos físicos. Ou seja, a informação "falada" também faz parte de dados que devem ser protegidos na instituição e, inclusive, fora dela. Imagine que você está em um elevador com um colaborador, que é detentor de uma informação confidencial, em razão da boa relação de amizade, vocês decidem iniciar uma conversa relacionada a assuntos da empresa, que não deveriam ser trocados entre departamentos e que estão sendo expostos em áreas de acesso ao público. Dessa forma, informações sigilosas e privilegiadas, não devem ser discutidas em ambientes públicos nem compartilhadas com familiares ou amigos.