MANUAL DE BOAS PRÁTICAS

I - INTRODUÇÃO

Considerando a necessidade de adequar-se aos modernos preceitos da Administração Pública e recomendações dos órgãos de controle quanto as Políticas de Integridade, tendo em vista os serviços de Ouvidoria Institucional, Lei de Acesso à Informação e, Lei Geral de Proteção de Dados Pessoais para cumprimento a legislações e princípios administrativos, instituiu-se o Programa de Integridade no âmbito do Conselho Regional de Odontologia de Pernambuco, através da Decisão CRO-PE nº 03/2022[1].

A efetiva governança no compartilhamento de dados tornou-se uma prioridade alinhada com os protocolos de segurança da informação.

Este manual é um guia dinâmico e essencial, elaborado com o intuito de fornecer diretrizes de excelência aos conselheiros, integrante das comissões e das câmaras de instruções, funcionários, estagiários, prestadores de serviços e colaboradores do CRO/PE.

Além de cumprir os requisitos legais, a adoção de uma governança robusta demonstra o compromisso da Autarquia em assegurar a conformidade com suas políticas.

Prezamos pela segurança de dados e pela transparência, com fulcro principalmente nos seguintes normativos:

Lei Federal nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais;

Lei Federal nº 12.965, de 23 de abril de 2014 - Marco Civil da Internet;

Lei Federal nº 12.527, de 18 de novembro de 2011 - Lei de Acesso à Informação;

Regulamentos e orientações da Autoridade Nacional de Proteção de Dados - ANPD, Conselho Nacional de Proteção de Dados Pessoais, Compesa, Governo Federal e Empresas de soluções digitais: Megaged, Kaspersky, Rohr, A; Scalzaretto e Voxage Soluções Digitais.

II - OBJETIVO

Este Manual de Boas Práticas tem os seguintes objetivos:

II. I - Apresentar as necessidades de adequação trazidas pelo Programa de Integridade;

II.II - Orientar os conselheiros, integrante das comissões e das câmaras de instruções, funcionários, estagiários, prestadores de serviços e colaboradores do Regional quanto às suas responsabilidades na condução ou manipulação das informações pela sua equipe;

II.III - Fomentar a importância da mudança cultural em relação ao Programa de Integridade;

[1] https://www.cro-pe.org.br/site/adm_syscomm/legislacao/foto/975.pdf

II. IV - Incutir nos conselheiros, integrante das comissões e das câmaras de instruções, funcionários, estagiários, prestadores de serviços e colaboradores do Regional a autorresponsabilidade no quesito do Programa de Integridade;

II. V - Promover a conscientização contínua acerca da importância do Programa de Integridade e segurança da informação.

III - A QUEM SE APLICA

Este Manual se aplica a todos os conselheiros, integrante das comissões e das câmaras de instruções, funcionários, estagiários, prestadores de serviços e colaboradores do Regional.

IV - CONCEITOS E ATRIBUIÇÕES DO PROJETO DE ADEQUAÇÃO À LGPD

Para melhor elucidar o Projeto de Adequação à LGPD, faz-se necessário esclarecer alguns conceitos e ter em mente que cada pessoa que se relaciona com as informações armazenadas e trafegadas desempenha um papel importante e bem definido conforme indicado a seguir:

IV. I - **Dado pessoal**: informação relacionada à pessoa natural identificada ou identificável;

IV. II - **Dado pessoal sensível**: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

IV. III - **Dado anonimizado**: dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

IV. IV- **Banco de dados:** conjunto de dados pessoais, determinado em um ou em vários locais, em suporte eletrônico ou físico;

IV. V - **Titular:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

IV. VI - **Controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

IV. VII - **Operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

IV. VIII - **Encarregado:** pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

IV. IX - **Agentes de Tratamento:** o controlador e o operador;

IV. X - **Tratamento:** toda operação realizada com dados pessoais, como as que dizem respeito à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão,

distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

IV. XI - Autoridade Nacional de Proteção de Dados - ANPD: é o órgão responsável por garantir o cumprimento da Lei Geral de Proteção de Dados e aplicar sanções administrativas, dentre outras tarefas.

IV. XII – Do Controlador, Operador E Encarregado

O Conselho Regional de Odontologia de Pernambuco é o controlador dos dados pessoais tratado, nos moldes das suas competências legal e institucional.

Os dados pessoais são operados por uma empresa prestadora de serviços, contratada para realização de atribuições fundamentais, sempre que, para a realização daqueles, for indispensável o acesso ao fluxo e tratamento de dados pessoais.

A Encarregada pelo Tratamento de Dados Pessoais foi determinada através da PORTARIA CRO-PE Nº 68/2023.

V - PASSO A PASSO PARA BOA GESTÃO DOS DADOS PESSOAIS

Disponibilizamos algumas recomendações para os conselheiros, integrante das comissões e das câmaras de instruções, funcionários, estagiários, prestadores de serviços e colaboradores do Regional que podem ser usadas no dia a dia para evitar o vazamento de informações:

V.I - Prevenir a ocorrência de danos ao titular ou a terceiros em virtude do tratamento de dados pessoais (princípio da prevenção);

V.II - Não realizar o tratamento do dado para fins discriminatórios, ilícitos ou abusivos (princípio da não discriminação);

V.III - Comprovar a observância e o cumprimento das normas de proteção de dados pessoais através da execução das atividades em conformidade com a LGPD (princípio da responsabilização e prestação de contas);

V.IV - Garantir que o tratamento do dado será apenas para a finalidade informada ao titular (princípio da adequação).

VI - PRÁTICAS DE PREVENÇÃO DE VAZAMENTO DE INFORMAÇÕES

A adesão há alguns hábitos no seu cotidiano irá auxiliar na prevenção de vazamento de informações. São boas práticas de prevenção:

VI. I – Eliminar os documentos físicos após o uso, como, por exemplo, cópias de documentos de jurisdicionados ou de qualquer colaborador (CPF, RG, CNH, comprovante de residência, etc.);

VI. II - Fazer revisão periódica dos arquivos que estão no computador para eliminar documentos que foram digitalizados dos jurisdicionados ou qualquer colaborador (CPF, RG, CNH, comprovante de residência, etc.);

VI. III – Ter um cuidado especial para os documentos dos jurisdicionados;

VI. IV – Não compartilhar arquivos que contenham dados pessoais para terceiros estranhos à atividade do CRO-PE sem autorização prévia;

VI.V- Verificar arquivos digitais que contenham dados pessoais dos jurisdicionados e conselheiros, integrante das comissões e das câmaras de instruções, funcionários, estagiários, prestadores de serviços e colaboradores do Regional armazenados em planilhas e eliminá-los;

VI.VI - Não utilizar rascunhos que contenham dados pessoais;

VI .VII - Na eliminação de documentos físicos, rasgar e picotar antes de jogar no lixo;

VI .VIII - Sempre que um colaborador for remanejado para outro setor, lembrar que os acessos de sistemas devem ser revisados;

VI .IX - Não manter contracheques de colegas em seu computador;

VI. X - Não utilizar aplicativos de mensagens através de números corporativos ou pessoais para tramitação de arquivos;

VI .XI – Verificar se há dados armazenados de forma física no seu ambiente de trabalho e em caso afirmativo, questionar: preciso manter esses arquivos? Se positivo, estão armazenados de forma segura? Se negativo, eliminá-los;

VI. XII - Realizar regularmente revisões das permissões de acesso aos dados pessoais, e-mails institucionais e sistemas que garantam o acesso somente a pessoas que realmente precisam ter acesso;

VI. XIII – Questionar: Há procedimento no meu setor para prevenir pessoas desligadas ou remanejadas de acesso a dados? Sejam conselheiros, integrante das comissões e das câmaras de instruções, funcionários, estagiários, prestadores de serviços e colaboradores do Regional;

VI .XIV - Não descartar documentos contendo dados pessoais em local inapropriado;

VI .XV - Não deixar documentos que contenham dados pessoais ou informações sigilosas nas máquinas de xerox nem em cima das mesas;

VI.XVI - Não manter em seu computador lista de jurisdicionados ou lista contendo nomes, endereços e CPF;

VI. XVII - Não utilizar ordens de serviço ou registro de atendimento que contenha dados dos jurisdicionados e/ou conselheiros, integrante das comissões e das câmaras de instruções, funcionários, estagiários, prestadores de serviços e colaboradores do Regional como rascunho;

VI. XVIII – Ter cuidado com seu computador e sempre manter os arquivos com dados na rede do CRO-PE, para garantir a proteção desta Autarquia.

VII - SEGURANÇA DIGITAL

Para saber mais, além das boas práticas explicadas anteriormente, o ambiente digital requer um cuidado ainda maior, pois possui uma natureza dinâmica e é alvo constante de crimes cibernéticos. Dessa forma, é importante seguir as recomendações realizadas por especialistas em segurança da informação, conforme a seguir:

VII. I - Troque suas senhas e faça disso um hábito (trocas regulares);

VII. II - Crie senhas fortes, alternando entre letras maiúsculas e minúsculas, números e usando caracteres especiais;

VII. III - Ative a autenticação de duas etapas em todas as plataformas que você usa que tenham essa função;

VII. III. I - Recomenda-se usar a autenticação de duas etapas através de aplicativos de terceiros, como: Google authenticator e Microsoft authenticator, que são mais complexos em razão da geração de código de segurança específico para acesso ao invés de e-mail e sms que há mais facilidade de vazamento de informações e hackeamento.

VII. IV – Faz-se necessário realizar um backup dos códigos secretos de segurança em QRCODE e guardar em local seguro para caso de perda de login e senhas, roubo de celular, etc;

VII. IV. I – No que diz respeito ao Facebook e ao Instagram, ao gerar os dez códigos secretos de segurança, guardá-los em local seguro e só usá-los em extrema necessidade caso não consiga de alguma forma recuperar a conta;

VII. V – Dar acesso a mais de um colaborador do Setor de Comunicação para administração da conta do Facebook, para se resguardar de eventual cancelamento ou hackeamento de um dos perfis.

VII. VI - Jamais forneça dados pessoais para quem liga, manda e-mail ou SMS solicitando-os;

VII. VII - Desconfie de ligações, mesmo que o interlocutor tenha seu CPF, data de nascimento e outros dados pessoais e afirme falar em nome de uma outra pessoa física ou jurídica;

VII. VIII - Fique atento às transações que acontecem nesta Autarquia;

VII. VIX - Não abra e-mails duvidosos e desconfie de promoções enganosas, ofertas e brindes;

VII. VX - Bloqueie câmeras e microfones se eles não estiverem em uso;

VII. XI - Mantenha um antivírus atualizado e não faça downloads de fontes desconhecidas;

VII. XII- Tome cuidado com o que postar nas redes sociais e não adicione qualquer pessoa;

VII. XIII - Se você não tem certeza da veracidade do e-mail, se você nunca teve contato com essa empresa e/ou com esse e-mail, cheque se o domínio que veio do e-mail é conhecido;

VII.XIV – Publique nos canais oficiais, os cuidados necessários que a Autarquia adota, destacando a não existência de cobrança que não seja através de boleto registrado;

VII. XV - Evite que sejam efetuados downloads de arquivos que deem margem para entrada de spam e vírus.

VIII - ALTERAÇÕES DESTE MANUAL DE BOAS PRÁTICAS

Caso haja necessidade e com o intuito de aperfeiçoar a atividade dos conselheiros, integrante das comissões e das câmaras de instruções, funcionários, estagiários, prestadores de serviços e colaboradores deste Regional, este Manual de Boas Práticas poderá sofrer alterações a partir da inserção de novas funcionalidades e serviços. Portanto, recomenda-se a consulta regular, bem como, a verificação da data de atualização.

IX - FALE CONOSCO

Se necessário mais algum esclarecimento quanto ao Programa de Integridade, entre em contato conosco através do canal abaixo: lgpd@cro-pe.org.br

Data de atualização: 07/02/2024.