ANEXO II
MANUAL DE INSTRUÇÕES DA LGPD

LGPD

Manual de Orientação para a Câmara de Palmital

Lei NR 13.709/18

SUMÁRIO

1. DOS AGENTES DA LGPD
1.1. Definição 3
1.2. Obrigações e Responsabilidades 3
1.3. Encarregado pelo tratamento de Dados Pessoais - DPO 4
1.4. Comitê de Privacidade e Proteção de Dados Pessoais 5
2. DO ÓRGÃO PÚBLICO COMO CONTROLADOR 5
3. DA GOVERNANÇA EM PROTEÇÃO DE DADOS? 6
3.1. Diagnóstico 7
3.2. Execução das Prioridades 8
3.3. Execução dos Pontos Complementares 8
3.4. Monitoramento 8
4. SEGURANÇA DA INFORMAÇÃO 10
4.1. Políticas de Segurança da Informação 12
4.2. Incidentes 12
4.2.1. Plano de Resposta a Incidentes de Segurança da Informação envolvendo Dados Pessoais e Dados Pessoais Sensíveis 13
4.2.2. Fluxo de Medidas Necessárias em caso de incidentes com Dados Pessoais 14
4.2.3. Plano de resposta a incidentes de segurança da informação envolvendo Dados Pessoais Sensíveis 15
4.3. Supervisão 16
4.3.1. Medidas para Mitigação de Riscos 16

1. DOS AGENTES DA LGPD

1.1. Definição

A LGPD define a figura dos agentes de tratamento de dados pessoais como os indivíduos que controlam ou tratam informações que contenham dados pessoais.

No artigo 5.º, inciso IX, que os agentes de tratamento são definidos como

- Controlador e o
- Operador.

A diferença entre o controlador e o operador está no escopo da função:

- ✓ O controlador coleta os dados pessoais dos titulares de dados e a ele compete as decisões quanto ao tratamento dos dados pessoais obtidos.
- ✓ O operador tratará os dados pessoais em nome do controlador, isto é, realizará o tratamento de dados pessoais em virtude de contrato, respeitando as instruções do controlador

1.2. Obrigações e Responsabilidades

A LGPD diferencia os agentes de tratamento e dispõe sobre as obrigações e responsabilidades no caso de ressarcimento de danos decorrentes do tratamento inadequado de dados pessoais, bem como no caso de incidentes de segurança da informação.

A principal obrigação que a lei atribui aos agentes acima citados é a de manterem um registro das operações de tratamento que realizarem, especialmente quando esse tratamento for realizado segundo a **base legal do legítimo interesse.**

Por sua vez, é dever do operador realizar o tratamento de dados pessoais conforme as instruções fornecidas pelo controlador, que verificará a observância das **Normas e Políticas sobre o Evento**.

- **É necessário que todas as instruções a serem cumpridas sejam claras e, preferencialmente, formais, para que não haja incerteza ou falha no processo de tratamento de dados pessoais.**

O agente de tratamento que, em razão do tratamento inadequado de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

Nesse sentido, o operador, apesar de tratar os dados conforme as instruções fornecidas pelo controlador, também poderá ser responsabilizado a reparar o dano causado.

1.3. Encarregado pelo tratamento de Dados Pessoais - DPO

A LGPD, em seu artigo 5.º, inciso VIII, designa a criação do cargo de encarregado de proteção de dados pessoais, figura também conhecida como ***data protection officer*** **(DPO).** Esse profissional será o responsável por acompanhar todas as atividades que dizem respeito à proteção de dados pessoais, bem como será o ponto focal para a comunicação interna do município, para a comunicação com os titulares de dados pessoais e para a comunicação com a ANPD.

- ✓ A imputação de uma necessidade de um encarregado busca garantir que as informações sobre proteção de dados pessoais sejam centralizadas dentro da organização.
- ✓ O cargo poderá ser ocupado por uma pessoa física ou jurídica, que poderá ser interna ou externa, ou até mesmo em um modelo híbrido, com contratados internos e externos, ao mesmo tempo.
- ✓ Poderá, ainda, ser um departamento com pessoas de diversas áreas, a fim de que possam cumprir com as diversas funções que o encarregado possui.

O encarregado tem, também, a atribuição de fazer a gestão das reclamações e comunicações dos titulares de dados pessoais, receber comunicações da ANPD, orientar os funcionários e contratados da Câmara Municipal sobre boas práticas a serem adotadas em relação à proteção de dados, o que compreende:

- ✓ Elaborar treinamentos,
- ✓ Revisar normas,
- ✓ Políticas e
- ✓ Procedimentos internos,
- ✓ Educar os servidores sobre a importância da LGPD e
- ✓ Mitigar riscos de incidentes de segurança da informação, e, por fim,
- ✓ Executar as demais atribuições que o município lhe atribuir.

O profissional deverá ter autonomia para auditar e fiscalizar as possíveis irregularidades, a fim de serem corrigidas e notificadas conforme rege a lei, **não podendo, portanto, haver conflito de interesses entre suas funções**, caso as acumule.

1.4. Comitê de Privacidade e Proteção de Dados Pessoais

O Comitê de Privacidade e Proteção de dados pessoais deve atuar em conjunto com o DPO, para auxiliar no desenvolvimento de algumas atividades ligadas à organização, como, por exemplo:

I. Facilitar a promoção de uma cultura de proteção aos dados pessoais dentro da organização;
II. Propor políticas de segurança da informação;
III. Gerenciar atividades relacionadas ao tratamento de dados pessoais, bem como avaliar se estão de acordo com as normas de proteção aos dados pessoais;
IV. Fiscalizar processos que envolvam o tratamento de dados pessoais;
V. Realizar treinamentos para os funcionários da organização, fornecedores e terceiros sobre a importância da proteção aos dados pessoais.

2. DO ÓRGÃO PÚBLICO COMO CONTROLADOR

Os municípios, assim como as empresas e demais instituições, em regra, são controladores de dados pessoais; afinal, realizam o cadastro dos seus habitantes para questões relacionadas a moradia, saúde, emprego, transporte e diversas outras atividades. Além disso, realizam o cadastro e utilizam os dados pessoais para realizar a cobrança de impostos, promover demandas judiciais e implementar políticas públicas. Outra forma de tratamento de dados pessoais realizado pelo município é o cadastro dos seus funcionários.

Desse modo, resta claro que o município figura como agente de tratamento, devendo ser considerado como controlador.

Mas quais as principais implicações a partir disso? O município deverá:

• **nomear encarregado/*data protection officer* (DPO):** cada órgão público deverá nomear um responsável pela comunicação entre os titulares, o próprio município e a ANPD, divulgando o contato do DPO, de preferência em seu website;

• **responder aos titulares de dados pessoais:** a LGPD elencou um rol de direito ao titular, sendo possível solicitar o acesso, a retificação e a confirmação de tratamento, entre outros direitos. A LGPD estabeleceu o prazo de **quinze dias** para resposta dos agentes de tratamento, sob pena de multa por descumprimento;

• **manter um registro das atividades:** conforme mencionado anteriormente, o município deve passar por um projeto de adequação, tendo que mapear as atividades de tratamento de dados e deixar os fluxos registrados, bem como suas alterações;

• **comunicar incidente:** caso ocorra um incidente de segurança que possa acarretar risco ou dano relevante aos titulares, o município deverá informar à ANPD em prazo razoável;

• **elaborar um RIPD:** conforme mencionamos acima, caso o município realize o tratamento de dados pessoais que possa gerar riscos às liberdades civis e aos direitos fundamentais dos titulares, deverá elaborar um relatório de impacto (RIPD). Caso o tratamento seja realizado a partir da base legal do legítimo interesse, a ANPD também poderá solicitar um relatório de impacto ao município;

• **ônus da prova no consentimento:** caso o município realize o tratamento de dados pessoais com suporte na base legal do consentimento, deverá provar que o titular manifestou claramente esse consentimento;

• **Transparência sobre os tipos de dados coletados de crianças:** quando o município realizar o tratamento de dados pessoais de crianças, além de ter que solicitar o consentimento de um dos pais ou representantes legais, deverá manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos utilizados.

Ao estabelecer as boas práticas adotadas internacionalmente, as instituições serão reconhecidas perante a população, elevando seu patamar de confiabilidade e transparência.

3. DA GOVERNANÇA EM PROTEÇÃO DE DADOS?

Cada município deverá passar por um processo de adequação à LGPD, que compreende algumas etapas, como veremos a seguir.

3.1. *Diagnóstico*

Nesta fase inicial, o órgão público deve levantar todas as suas atividades que compreendem o tratamento de dados pessoais, verificando todo o caminho percorrido pelos dados pessoais e identificando os riscos em cada processo.

A partir dessas informações, é possível identificar o nível de aderência do município à LGPD e recomendar as alterações necessárias.

Em um projeto de adequação à LGPD, o mapeamento de dados é dividido da seguinte forma:

Nesse momento, será possível detalhar cada dado pessoal tratado, entendendo as fases do seu ciclo de vida.

Será possível entender como os dados são recebidos, como e onde estão armazenados, quem tem acesso, se os dados são compartilhados com terceiros, quais os riscos associados a cada operação e a base legal adequada.

Dessa forma, será possível analisar a forma como o órgão público lida com os dados pessoais de seus servidores, munícipes, fornecedores e parceiros.

Após o mapeamento dos processos, será possível identificar diversas questões em desacordo com a LGPD ou com as melhores práticas de segurança da informação, ou, ainda, com as práticas setoriais aplicáveis.

Nesse momento, deve-se definir as bases legais adequadas para cada atividade de tratamento de dados pessoais executada na Câmara de Palmital, bem como elaborar um relatório com os principais gaps, apontando quais as medidas necessárias para a mitigação de riscos envolvendo incidentes de segurança da informação.

3.2. *Execução das Prioridades*

Após mapear os riscos e recomendar as ações necessárias para a sua mitigação, chega o momento de colocá-las em prática.

Entretanto, nesse primeiro momento, a Câmara Municipal deve separar as ações em prioritárias e complementares, iniciando por aquelas que trazem um risco maior.

Após analisados os gaps encontrados, será necessário verificar quais as prioridades do órgão público e elaborar um cronograma para mitigar os riscos localizados nas etapas anteriores.

Será necessária a indicação de responsáveis para cada atividade de tratamento com necessidade de alteração e a verificação dos diferentes níveis de criticidade de cada medida.

É chegada a hora de implementar as medidas encontradas em desconformidade com a legislação.

Nesse momento, será necessário adequar plataformas, processos, contratos, práticas e documentos que versem sobre o tratamento de dados pessoais.

3.3. *Execução dos Pontos Complementares*

Após a realização da adequação e mitigação dos principais riscos, a Câmara poderá dar ênfase à formação de uma cultura de dados, desenvolvendo e aplicando palestras, treinamentos e comunicações com o intuito de demonstrar a importância da privacidade e da proteção dos dados para cada indivíduo, para o próprio município e para a sociedade.

3.4. *Monitoramento*

Após a realização do diagnóstico, da implementação das ações prioritárias e complementares, é necessário que haja um monitoramento do projeto de adequação à LGPD e seus resultados, sendo o monitoramento um dos principais pontos da governança.

Nesse momento, chegamos ao final do nosso projeto de adequação à LGPD, porém não seria correto dizer que o projeto chegou ao fim, pois sempre será necessário manter as informações em ordem, sendo monitoradas e avaliadas com frequência.

Além disso, a Câmara é um organismo vivo que sofre constantes mudanças, assim como as leis podem sofrer alterações; desse modo, a etapa de monitoramento acaba não tendo um fim.

Dessa maneira, é essencial que a Câmara tenha colaboradores (internos, externos ou mesmo uma equipe híbrida) que sejam capazes de monitorar todas as novidades que podem ocorrer, para nunca deixar a organização desatualizada, oportunizando o risco de sofrer sanções pela ANPD.

Outro ponto fundamental do monitoramento é a necessidade de treinamentos com certa periodicidade, para que a cultura da proteção aos dados pessoais seja parte do dia a dia da Câmara Municipal.

Além disso, para a correta adequação à LGPD pela Câmara Municipal, sugerimos a estruturação de um grupo de trabalho que seja responsável pelo projeto e pelo estudo do tema.

É essencial que, nesse grupo, estejam presentes e engajadas pessoas da alta Diretoria, bem como pessoas de **setores** que tratam dados pessoais em seu dia a dia.

4. SEGURANÇA DA INFORMAÇÃO

Segurança da informação é um conjunto de mecanismos e ferramentas que uma instituição utiliza com a finalidade de proteger um conjunto de informações, para proteger o valor que tais informações geradas pela instituição possuem.

É, assim, um conjunto de normas e políticas essenciais às instituições, principalmente para aquelas que lidam com informações valiosas e sigilosas.

Sob a LGPD, os controladores e operadores devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acesso não autorizado, destruição, perda, modificação, comunicação ou outros tipos de tratamento não autorizados ou ilegais.

- Espera-se que a ANPD forneça diretrizes para padrões técnicos mínimos no futuro.

O Marco Civil da Internet e sua Resolução regulamentadora estabelecem as seguintes diretrizes sobre normas de segurança que devem ser observadas pelos provedores de conexão e de aplicação no tratamento de dados pessoais e de comunicações privadas que trafegam pela internet:

I. O estabelecimento de controles rígidos sobre o acesso a dados pessoais, estabelecendo responsabilidades para aqueles que terão acesso a dados pessoais;
II. O fornecimento de mecanismos de autenticação para o acesso a registros, usando, por exemplo, sistemas de autenticação dupla para garantir a individualização dos responsáveis pelo tratamento de dados pessoais;
III. A criação de inventários detalhados de *logs* referentes à conexão e ao acesso aos aplicativos, que devem conter data, hora, minuto, segundo e a duração do acesso, a identidade do indivíduo que acessou os arquivos e quais arquivos foram acessados; e
IV. O uso de soluções de gerenciamento de registros por meio de técnicas que garantam a inviolabilidade dos dados pessoais, como criptografia ou medidas de proteção equivalentes.

Além disso, cada setor possui regras específicas quanto a padrões mínimos ou esperados que garantam a segurança da informação das organizações.

Alguns princípios que podem nortear uma política de segurança da informação são:

I. Confidencialidade, para que as informações sejam acessadas apenas por pessoas autorizadas;

II. Integridade, para que as informações apenas sejam alteradas por pessoas autorizadas; e

III. Disponibilidade, as informações devem sempre estar disponíveis para quem é autorizado, evitando interrupções no fluxo de trabalho.

4.1. Políticas de Segurança da Informação

Parte fundamental no programa de governança são as políticas, normas e procedimentos de segurança da informação.

Abaixo, listamos as principais políticas presentes em no programa de governança em proteção de dados pessoais e privacidade da Câmara Municipal de Palmital:

1. Mapeamento de Processos
2. Resolução da LGPD-Câmara de Palmital - SP
3. Portaria de Nomeação do Encarregado de Dados
4. Manual de Instrução da LGPD
5. Código de Conduta e Integridade
6. Política de Uso Geral de Dados Pessoais
7. Política de Privacidade
8. Política de Segurança da Informação
9. Política de Acesso e Classificação de Dados
10. Política de Resposta a Incidentes e Segurança de Privacidade
11. Política para Desenvolvimento de Aplicações e Sistemas
12. Política de Backups e Cópias de Segurança
13. Política de Cookies
14. Política de Tratamento ao Titular de Dados e
15. Apresentação da LGPD no Portal de Transparência

4.2. Incidentes

De acordo com a página da ANPD no site do Governo Federal, um incidente de segurança com dados pessoais é "qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou, ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais".

Como exemplos de incidentes de segurança da informação, podemos mencionar o acesso de terceiro não autorizado em redes de computadores, ou seja, quando algum agente

externo, ou mesmo um colaborador da organização acessa (ou tenta acessar) uma parte do sistema que não deveria.

Os vírus e códigos maliciosos também são caracterizados como incidentes de segurança da informação e sua detecção requer o uso de ferramentas próprias, como antivírus.

Por fim, como último exemplo, podemos citar o uso impróprio de sistemas ou de informações, que ocorrem quando um funcionário da organização usa um e-mail corporativo para a promoção de negócios pessoais, ou quando instala uma ferramenta não autorizada no computador da organização, utiliza um *pen drive* de forma não autorizada ou, ainda, exemplificando com documentos físicos, imprime documentos sigilosos de forma não autorizada e os repassa para terceiros.

O art. 47 da LGPD diz que "Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término". Dessa forma, é imprescindível que a Câmara Municipal adote medidas técnicas e administrativas de segurança capazes de proteger os dados pessoais de acessos não autorizados e de situações acidentais ou maliciosas.

4.2.1. Plano de Resposta a Incidentes de Segurança da Informação envolvendo Dados Pessoais e Dados Pessoais Sensíveis

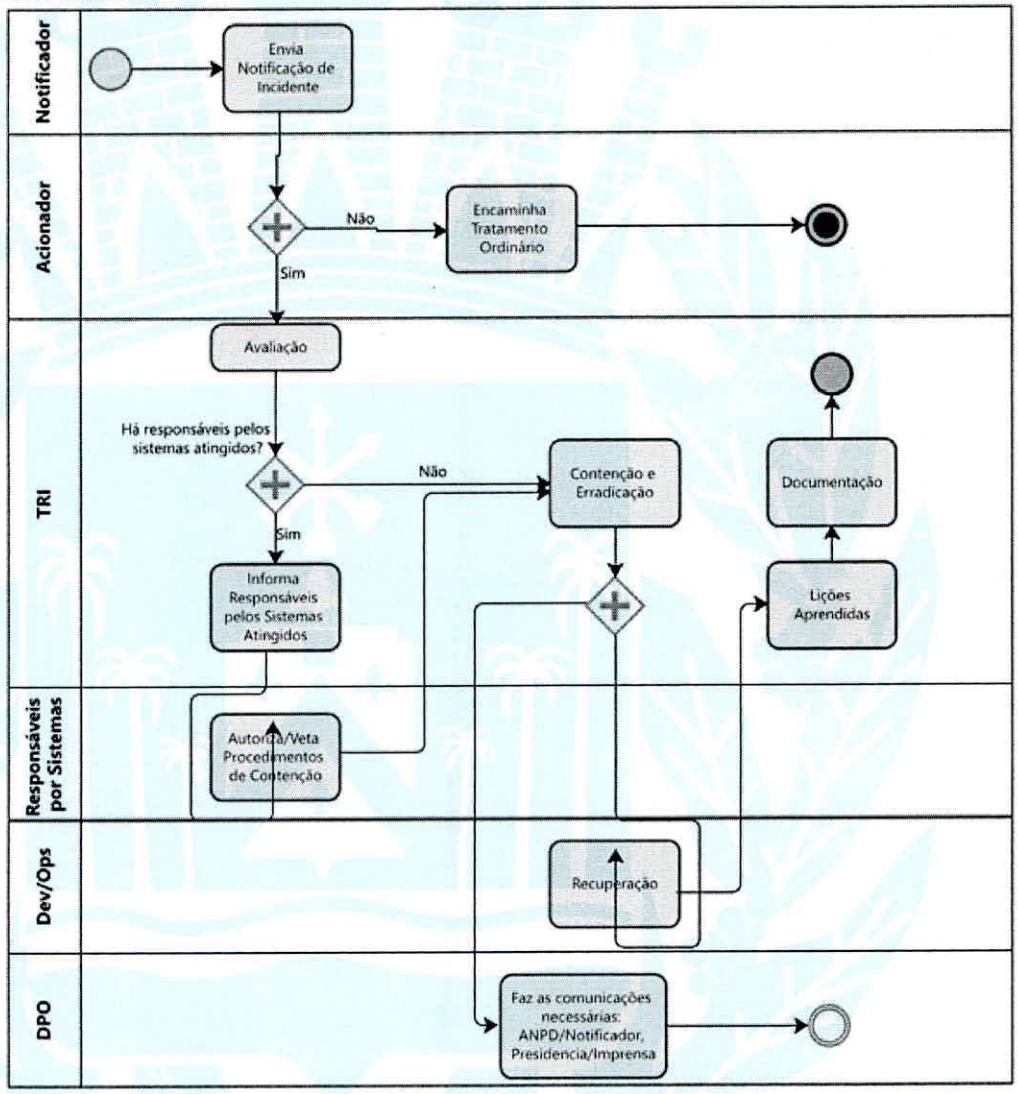
O Plano de Respostas a Incidentes de Segurança envolvendo dados pessoais (Política de Resposta a Incidentes e Segurança da Privacidade) tem, como objetivo, descrever como a Câmara procederá a partir de situações que identifiquem a ocorrência ou suspeita de um incidente de segurança da informação.

Por sua gravidade, a Câmara tem o compromisso de elaborar e aplicar imediatamente as melhores medidas técnicas e jurídicas que visem à transparência, confiança e agilidade.

Os principais agentes responsáveis por lidar com os incidentes de segurança são:

- **Notificador:** pessoa física ou sistema de monitoramento que comunicará imediatamente a equipe responsável sobre a ocorrência ou a mera suspeita de um Incidente.

• **Time de Resposta a Incidentes-TRI:** grupo formado por pessoas envolvidas diretamente com a execução de tratamento de dados pessoais dentro da corporação, responsável por receber as notificações de incidentes de forma imediata, estruturando medidas ágeis e adequadas sobre o ocorrido, conforme fluxo abaixo.



- **Fluxo de Resposta a Incidentes**

4.2.2. Fluxo de Medidas Necessárias em caso de incidentes com Dados Pessoais

Em 24 horas:

1. Notificar o TRI sobre o incidente;
2. Analisar o mapeamento de dados pessoais.

Em 48 horas:

1. Elaboração de *Data Breach Score* (pontuação de violação de dados) e confecção de parecer técnico;
2. Elaborar um Relatório de Impacto à Proteção de Dados Pessoais (DPIA);
3. Elaborar um plano de notificação do incidente de segurança da informação;
4. Comunicação ao titular dos dados pessoais sobre o incidente de segurança da informação;
5. Comunicação à Autoridade Nacional de Proteção de Dados (ANPD).

Em 72 horas:

1. Elaborar relatório de providências adotadas e revisão do programa de governança em privacidade e proteção de dados pessoais;

4.2.3. Plano de resposta a incidentes de segurança da informação envolvendo Dados Pessoais Sensíveis

Em 24 horas:

1. Notificar o TRI sobre o incidente;
2. Analisar o mapeamento de dados pessoais;
3. Elaboração de *Data Breach Score* e confecção de parecer técnico;
4. Elaborar um Relatório de Impacto à Proteção de Dados Pessoais (DPIA);
5. Elaborar um plano de notificação do incidente de segurança da informação;
6. Comunicação ao titular dos dados pessoais sobre o incidente de segurança da informação;
7. Comunicação à Autoridade Nacional de Proteção de Dados (ANPD);
8. Comunicação ao Banco Central do Brasil.

Em 48 horas:

1. Elaborar relatório de providências adotadas e revisão do programa de governança em privacidade e proteção de dados pessoais.

2. Além disso, a ANPD disponibilizou no site do governo,1 o quê, como, quando e por quem devem ser feitas as comunicações de incidente de segurança da informação com dados pessoais.

4.3. Supervisão

O supervisor de tecnologia da informação (TI) é o profissional responsável por realizar o monitoramento das atividades que suportam a rede da área de informática de uma instituição, envolvendo a elaboração de projetos de implantação, desenvolvimento e integração de sistemas.

O supervisor de TI é responsável pela realização de planejamento de projetos, atendendo às necessidades e negócios da instituição, atuando na parte de dados informáticos, administrando e controlando o centro de processamento da instituição, realizando manutenções e instalações dos equipamentos informáticos, garantindo o cumprimento das políticas de segurança da informação, dentre muitas outras funções.

4.3.1. Medidas para Mitigação de Riscos

Dentre as principais medidas que podemos apresentar para a mitigação de riscos envolvendo incidentes de segurança da informação, encontram-se desde pontos muito simples, que podem ser adotados no dia a dia das pessoas, como a instalação de um antivírus e a recomendação de não abertura de e-mails de endereços desconhecidos, até mesmo questões mais complexas, como a atualização de sistemas (principalmente os sistemas de proteção e operacionais).

Importante mencionar, ainda, a recomendação de estabelecer políticas de segurança da informação e treinamentos a serem ministrados a todos os funcionários de uma organização.

É essencial que os funcionários sejam treinados para que saibam como agir diante de situações que podem configurar riscos de incidentes com dados pessoais.

Como uma tentativa de provocar um incidente e, mesmo, diante de um incidente de segurança da informação propriamente dito.

Por fim, **as políticas são excelentes maneiras de formalizar** como a organização trata os sistemas, informações e processos, e são essenciais para o dia a dia de uma organização.

Plenário Vereador Prof.º Alcides Prado Lacreta, em 06 de março de 2023.

CRISTIAN RODRIGO ALVES NOGUEIRA
Presidente

HOMERO MARQUES FILHO
1ª Secretário