PLANO DE RESPOSTAS A INCIDENTES

PREFEITURA MUNICIPAL DE REALEZA

A **Política de Resposta a Incidentes de Segurança em Dados Pessoais** tem por objetivo definir diretrizes, procedimentos e ações a serem seguidos por todas as pessoas, departamentos, secretarias e entidades que, direta ou indiretamente, se relacionam com a **Prefeitura Municipal de Realeza**. Isso inclui servidores, prestadores de serviços, parceiros e quaisquer agentes que, no exercício de suas funções, realizem operações de tratamento de dados pessoais, seja na coleta, armazenamento, processamento, compartilhamento ou descarte dessas informações.

Este documento foi desenvolvido para garantir o alinhamento institucional com os dispositivos da **Lei Geral de Proteção de Dados Pessoais (LGPD)** – Lei nº 13.709/2018 – e outras normas e regulamentações aplicáveis, estabelecendo um compromisso com a gestão eficaz e a resposta a incidentes de segurança, com foco na proteção da privacidade e da integridade dos dados pessoais sob custódia da Prefeitura.

Reconhecendo a responsabilidade pública no tratamento de dados pessoais, a Prefeitura Municipal de Realeza adota este documento para garantir uma resposta estruturada e ágil a incidentes de segurança, minimizando riscos e impactos, promovendo a continuidade das operações e fortalecendo a confiança dos cidadãos na administração pública. O objetivo é proteger os direitos dos titulares de dados pessoais, sensíveis ou não, e assegurar que todas as atividades relacionadas ao tratamento de dados sejam realizadas com total transparência, ética e segurança.

Este documento busca ainda alinhar as práticas institucionais aos princípios de privacidade por design e privacidade por padrão, garantindo que todas as operações de resposta a incidentes sejam planejadas e implementadas com o máximo nível de proteção, desde a identificação até a mitigação e recuperação de possíveis falhas ou violações de dados.

a) **Define padrões e procedimentos claros**: este documento estabelece padrões e procedimentos detalhados para a gestão e resposta a incidentes de segurança em dados pessoais, com o objetivo de orientar o uso ético, seguro e responsável desses dados. Todas as áreas da Prefeitura Municipal de Realeza devem seguir diretrizes claras para garantir que as atividades administrativas, legislativas e de relacionamento com a sociedade sejam conduzidas com rigor, transparência e alinhamento às melhores práticas de proteção de dados.

b) **Garante a conformidade com as obrigações legais**: este documento assegura o cumprimento das obrigações legais relacionadas à proteção de dados, em conformidade com a LGPD e demais regulamentos aplicáveis. A adesão rigorosa a essas regras visa mitigar riscos jurídicos, técnicos e reputacionais, além de promover a confiança da sociedade na integridade das práticas institucionais. A resposta a incidentes segue os prazos e diretrizes estabelecidos pela legislação vigente, reforçando a conformidade e a transparência na gestão dos dados pessoais.

c) **Promove a educação e a conscientização**: a Prefeitura Municipal de Realeza investe na capacitação contínua dos servidores, colaboradores e parceiros, com o objetivo de disseminar conhecimentos sobre segurança da informação e proteção de dados pessoais. A formação e a conscientização são fundamentais para a criação de uma cultura organizacional que valoriza a privacidade e a segurança das informações. A educação contínua garante que todos os envolvidos estejam cientes dos riscos e capacitados a adotar boas práticas na resposta a incidentes.

d) **Estabelece a governança de dados pessoais**: este documento define os papéis, responsabilidades e processos relacionados à gestão e resposta a incidentes de segurança em dados pessoais. A governança de dados pessoais é essencial para assegurar a integridade, a confidencialidade e a disponibilidade das informações tratadas. Medidas técnicas e administrativas robustas são implementadas para garantir a proteção dos dados em todas as etapas do ciclo de vida dos incidentes.

e) **Fortalece a transparência e a acessibilidade**: este documento assegura que os titulares de dados pessoais tenham acesso facilitado a informações claras e detalhadas sobre como seus dados estão sendo tratados. Além disso, reforça a garantia de que os titulares possam exercer seus direitos de forma ágil e eficiente, promovendo a confiança e a transparência na gestão dos dados pessoais pela Prefeitura Municipal de Realeza.

Termos e Definições [Glossário]

A seguir, apresentamos os termos e definições essenciais para a compreensão da Política de Resposta a Incidentes de Segurança em Dados Pessoais da Prefeitura Municipal de Realeza. As definições adotadas neste glossário seguem as orientações estabelecidas pela Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente com base no Art. 5º da LGPD, bem como na Portaria GSI/PR nº 93, de 18 de outubro de 2021, que estabelece um glossário de segurança da informação aplicável às entidades públicas. Essas definições são fundamentais para garantir que todos os envolvidos no tratamento de dados pessoais dentro da Prefeitura Municipal de Realeza compreendam suas responsabilidades e os limites legais para a gestão, proteção e resposta a incidentes envolvendo dados pessoais. Além disso, asseguram que a política de resposta a incidentes seja aplicada de forma consistente, alinhada à legislação vigente e às melhores práticas de segurança.

- **Agentes de tratamento**: referem-se ao **controlador** e ao **operador** em conjunto. O controlador é a entidade responsável pelas decisões estratégicas relacionadas ao tratamento de dados pessoais, enquanto o operador executa as tarefas operacionais sob as diretrizes do controlador. Não são considerados controladores ou operadores os servidores ou equipes de trabalho diretamente subordinados ao controlador, já que suas ações são reguladas por diretrizes e ordens específicas fornecidas pelo agente de tratamento. Esses servidores ou equipes não têm autonomia para decidir sobre as finalidades ou os meios de tratamento dos dados.

- **Anonimização**: Utilização de técnicas e ferramentas tecnológicas apropriadas e disponíveis no momento do tratamento de dados, visando a impossibilidade de vinculação dos dados a um indivíduo específico. O dado anonimizado não é considerado dado pessoal para os fins da LGPD

- **Ataque**: é definido como qualquer evento de exploração de vulnerabilidades ou tentativas maliciosas de invadir sistemas, acessar informações confidenciais ou interromper o funcionamento normal dos serviços. Esses atos podem envolver o uso de técnicas como phishing, ransomware, ataques DDoS (negação de serviço) ou exploração de falhas de segurança. Os ataques comprometem a confidencialidade, integridade ou a disponibilidade das informações, resultando em danos significativos ao ambiente de dados da entidade.

- **Autoridade Nacional de Proteção de Dados (ANPD)**: a ANPD é o órgão responsável por fiscalizar, aplicar a legislação e zelar pelo cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) em todo o território nacional. Sua função é garantir que as normas de proteção de dados pessoais sejam cumpridas, promovendo a supervisão, a orientação e a fiscalização das atividades de tratamento de dados pessoais realizadas por controladores e operadores.

- **Dado Pessoal**: Todos os dados que permitam, direta ou indiretamente, a identificação de uma pessoa física. Dados pessoais podem incluir nome, endereço, telefone, e-mail, entre outros dados que permitam identificar um indivíduo. Para a Prefeitura Municipal de Realeza, dados pessoais podem ser coletados em diversos processos administrativos e de atendimento ao público.

- **Dado Pessoal Sensível**: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a 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. Este tipo de dado exige uma proteção reforçada, sendo tratado com mais cuidado e exigindo consentimento expresso dos titulares para seu tratamento, de acordo com a LGPD.

- **Encarregado ou Data Protection Officer (DPO):** Encarregado, ou DPO, é a pessoa indicada pelo controlador para assegurar o cumprimento da legislação de proteção de dados e atuar como canal de comunicação entre a entidade, os titulares dos dados e a ANPD. O DPO desempenha um papel essencial na supervisão das práticas de tratamento de dados, orientando sobre a conformidade e promovendo a educação e conscientização interna.

- **Incidente**: Um incidente refere-se a qualquer ato, suspeita, ameaça ou circunstância que comprometa a confidencialidade, integridade ou a disponibilidade dos dados pessoais que estão sob a posse da JUCEMG ou que esta venha a acessar. Incidentes podem incluir vazamentos, acessos não autorizados, falhas em sistemas ou qualquer evento que ponha em risco a proteção dos dados pessoais

- **IP (Internet Protocol):** O IP é um número usado para identificar dispositivos em redes de computadores, como a internet. Ele permite a comunicação e a troca de informações entre diferentes dispositivos. No contexto de segurança da informação, o endereço IP pode ser utilizado para rastrear acessos indevidos ou suspeitos a sistemas e redes.

- **Tratamento**: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. O Tratamento de dados pessoais é uma atividade cotidiana da Prefeitura Municipal de Realeza, realizada em diversas plataformas e sistemas administrativos.

- **Vazamento de dados:** ocorre quando informações pessoais são divulgadas ou acessadas de forma não autorizada, resultando na perda, alteração, compartilhamento, transmissão ou armazenamento de dados em desconformidade com as normas de segurança. O vazamento pode ter implicações jurídicas, técnicas e de reputação.

- **Violação de privacidade:** acontece quando há qualquer infração à legislação aplicável ou condutas que resultam em danos, como a destruição, perda, roubo, acesso não autorizado ou alteração dos dados pessoais. Isso pode levar a consequências legais e à perda da confiança dos titulares de dados.

- **Vírus:** programas ou partes de programas maliciosos que se espalham, inserindo cópias de si mesmos em outros programas e arquivos, com o objetivo de danificar sistemas, roubar informações ou interromper o funcionamento de serviços. Eles representam uma grave ameaça à segurança da informação.

Etapas do Processo (Resumo)

A estrutura deste Plano de Resposta a Incidentes é baseada nas seguintes macros etapas:

1) Identificação

A identificação de qualquer incidente de segurança em dados pessoais é fundamental para garantir uma resposta eficiente. É essencial que ferramentas de monitoramento, registros de log, mensagens de erro, firewalls, e sistemas automatizados de detecção estejam em funcionamento para alertar proativamente sobre anomalias e atividades suspeitas. A capacitação contínua dos servidores, colaboradores e fornecedores é necessária para que eles possam reconhecer e relatar rapidamente eventos de vazamento ou comprometimento de dados pessoais.

2) Preparação

A resposta a um incidente deve ser ágil e bem estruturada, pois erros ou atrasos podem ampliar o impacto e os danos. As práticas de resposta a incidentes, como a realização de testes de simulados, devem ser regularmente exercitadas para medir os tempos de resposta e verificar a eficácia das medidas implementadas. A preparação envolve a definição de papéis, responsabilidades, fluxos de comunicação e a disponibilidade de recursos para atuar rapidamente em caso de um incidente.

3) Contenção

Após a identificação, o incidente deve ser imediatamente contido e isolado, a fim de evitar a propagação para outros sistemas e reduzir os danos potenciais ao ambiente. A contenção envolve ações de curto prazo, como a suspensão de acessos e a aplicação de patches, e de longo prazo, como a revisão e atualização de políticas de segurança e a remoção das causas raiz do incidente. Nesta etapa, deve-se registrar todas as ações realizadas para garantir que provas e evidências do incidente sejam preservadas.

4) Erradicação

Na etapa de erradicação, as causas do incidente são completamente removidas, e os sistemas e processos afetados são restaurados ao seu estado original. Isso pode incluir a revisão e a atualização de políticas de segurança, a implementação de novos controles e a execução de auditorias para garantir que a ameaça não se repita. A erradicação busca assegurar que o ambiente de TI esteja livre de vulnerabilidades exploradas no incidente.

5) Recuperação

A recuperação é o retorno dos sistemas e processos afetados ao ambiente operacional de produção. Esta etapa inclui testes rigorosos para validar que as medidas corretivas foram eficazes e que o sistema está funcionando sem riscos. A recuperação também envolve a revisão das estratégias de contingência, a continuidade dos negócios e a garantia de que os serviços essenciais foram restabelecidos com segurança.

6) Preceitos Assimilados

Nesta etapa, todas as ações realizadas durante o processo de resposta são documentadas e analisadas para identificar pontos de melhoria. O aprendizado derivado dos incidentes contribui para a atualização contínua do Plano de Respostas a Incidentes, facilitando futuras ações e aprimorando a capacidade da entidade em lidar com incidentes de segurança em dados pessoais de forma mais eficaz e eficiente.

7) Documentação do Incidente

A documentação detalhada de cada incidente é crucial para o histórico e a análise posterior. O registro deve incluir todas as ações implementadas nas etapas anteriores, desde a identificação até a erradicação, além das lições aprendidas. Esta documentação assegura a transparência e facilita o acompanhamento contínuo dos processos e a adaptação do plano de resposta.

8) Comunicações

A ocorrência de incidentes de segurança com potencial de gerar danos relevantes aos titulares deve ser comunicada à ANPD e aos titulares, conforme previsto na legislação. As informações fornecidas à ANPD podem ser realizadas por meio de solicitações, relatórios ou auditorias, com o objetivo de demonstrar a conformidade com a LGPD e a adequação das medidas tomadas pela Prefeitura Municipal de Realeza.

CAPÍTULO I

Descrição do Processo

a) Início/Detecção

Um novo incidente de segurança envolvendo dados pessoais pode ser notificado por qualquer pessoa interna ou externa à Prefeitura Municipal de Realeza, ou ainda, por meio de alarme de monitoração automatizada. A comunicação inicial pode ocorrer através de diversos canais, como e-mails, telefone, “Fale Conosco”, Disk Denúncia, sistemas internos da Prefeitura, ou ainda, por notificações recebidas diretamente pelo Encarregado de Dados (DPO), no caso de reclamações feitas pelos titulares de dados pessoais. Todas as notificações devem ser registradas diretamente pelo notificador, assegurando que todas as informações relevantes sejam documentadas.

b) Triagem

A notificação é recebida pelo Encarregado de Dados – DPO da Prefeitura de Municipal de Realeza, que deve realizar uma avaliação preliminar ou, se necessário, convocar o comitê gestor para análise do incidente. A triagem pode descartar notificações consideradas nulas ou claramente improcedentes.

Durante a avaliação preliminar, devem ser verificadas informações sobre os sistemas ou processos alegadamente impactados, bem como a criticidade deles, os danos aparentes e o risco de agravamento da situação caso não haja resposta imediata.

Incidentes que não envolvam sistemas online e que não apresentem riscos aumentados pela falta de ação imediata podem ser

reencaminhados para os trâmites regulares dos setores responsáveis na Prefeitura

c) Avaliação

Nesta fase, deve-se proceder com uma análise aprofundada do incidente, conduzida pelo Encarregado de Dados (DPO) ou pelo Comitê Gestor. O objetivo é compreender a extensão, o impacto e os riscos associados ao incidente, além de classificar sua criticidade. A avaliação considera os seguintes aspectos:

Crítica do Sistema

- **Definição da Importância**: Identificar o papel do sistema ou processo afetado para as operações da organização.
    - Exemplo: Sistemas essenciais, como bases de dados de servidores ou plataformas de atendimento ao cidadão, possuem prioridade máxima.

- **Avaliação de Dependências**: Verificar se outros sistemas ou processos dependem diretamente do sistema afetado.

- **Impacto na Disponibilidade**: Analisar se a indisponibilidade do sistema afetado compromete serviços essenciais ou a continuidade das operações.

Impacto Potencial

- **Análise de Titulares de Dados Afetados**:
    - Estimar o número de titulares potencialmente impactados.
    - Verificar se há exposição de dados pessoais sensíveis ou de grupos vulneráveis (ex.: crianças, idosos, minorias).

- **Consequências Financeiras**:
    - Identificar possíveis perdas financeiras ou custos para mitigar o incidente (ex.: multas, indenizações, restauração de sistemas).

- **Danos Reputacionais**:
    - Avaliar o risco de perda de confiança por parte dos cidadãos ou parceiros.
    - Considerar impactos na imagem da organização pública perante a sociedade.

- **Consequências Jurídicas e Regulatórias**:
    - Estimar o risco de penalidades por descumprimento da LGPD.
    - Verificar a necessidade de comunicação à ANPD.

Probabilidade de Agravamento

- **Avaliação de Exploração Ativa**:
    - Determinar se o incidente já está sendo explorado por terceiros mal-intencionados (ex.: vazamentos ativos em fóruns ou dark web).

- **Risco de Escalabilidade**:
    - Analisar se a falha pode se propagar para outros sistemas ou afetar mais dados pessoais.
- **Condições de Contenção**:
    - Avaliar se há barreiras já aplicadas que minimizem o risco de agravamento (ex.: firewalls, sistemas de redundância, criptografia).

Necessidade de Ação Imediata

- **Definição de Prioridades**:
    - Classificar o incidente como crítico, importante ou não urgente, dependendo da severidade e do risco de impacto.

- **Implementação de Ações Preventivas**:
    - Identificar ações imediatas para conter o incidente, como:
        - Isolamento do sistema afetado.
        - Alteração de credenciais comprometidas.

- Suspensão temporária de serviços para proteção de dados.

- **Comunicação Rápida**:
  - Estabelecer se é necessário notificar imediatamente a ANPD ou os titulares dos dados afetados.

d) Classificação da Criticidade

A classificação da criticidade dos incidentes é fundamental para a resposta eficaz e está definida nos seguintes termos:

Volume de Dados Pessoais expostos	Alto	Alta Gravidade	Alta Gravidade	Alta Gravidade
	Médio	Média Gravidade	Alta Gravidade	Alta Gravidade
	Baixo	Baixa Gravidade	Média Gravidade	Média Gravidade
		Baixa	Média	Alta
		Sensibilidade dos Dados Pessoais afetados		

Volume de Dados Pessoais expostos	
Criticidade	Descrição
Alto	Volume de Dados Pessoais afetado superior a 10% da base de dados da Controladora.
Médio	Volume de Dados Pessoais afetado inferior a 10% e superior a 2% da base de dados da Controladora.

Sensibilidade dos Dados Pessoais afetados	
Criticidade	Descrição
Alta	Dados Pessoais de crianças/ adolescentes, Dados Pessoais Sensíveis ou que possam gerar discriminação ao titular.
Média	Dados Pessoais imediatamente identificáveis (Ex.: nome, e-mail, CPF, endereço), combinados, ou não, com informações comportamentais (Ex.: histórico de atividades, preferências).

Baixo	Volume de Dados Pessoais afetado inferior a 2% da base de dados da Controladora.	**Baixa**	Dados que passaram por processos de anonimização, pseudonimização (desde que a chave de desanonimização não tenha sido comprometida) e dados pessoais considerados de difícil identificação, como endereços IP.

A **classificação de criticidade** é uma etapa central no gerenciamento de incidentes de segurança, essencial para priorizar ações de resposta, direcionar recursos de forma estratégica e minimizar os impactos do incidente. Esse processo permite uma avaliação sistemática, garantindo que os esforços sejam proporcionais à gravidade e ao potencial de danos gerados.

Ela é estabelecida com base em critérios objetivos, que consideram aspectos técnicos, organizacionais e legais, e busca orientar decisões rápidas e fundamentadas. Além disso, a classificação de criticidade possibilita:

1. **Alocação Eficiente de Recursos**:
    - Direcionar equipes especializadas e ferramentas avançadas para os incidentes mais graves.
    - Otimizar o uso de tempo e orçamento, priorizando medidas corretivas em áreas de maior impacto.

2. **Ações Escaláveis e Proporcionais**:
    - Definir respostas adaptáveis de acordo com o escopo do incidente, desde simples correções a mobilizações completas de equipes de resposta.
    - Garantir que incidentes de menor gravidade não sejam tratados de forma desproporcional, preservando recursos para cenários críticos.

3. **Redução de Impactos ao Titular e à Organização**:
    - Mitigar rapidamente os riscos de prejuízo financeiro, jurídico ou reputacional.
    - Prevenir a evolução do incidente para situações de maior complexidade.

4. **Conformidade Regulatória e Transparência**:
    - Demonstrar alinhamento com a LGPD e outras normas aplicáveis, fortalecendo a confiança dos titulares de dados e das autoridades reguladoras.
    - Estabelecer uma base estruturada para comunicações claras e eficazes com stakeholders internos e externos.

5. **Tomada de Decisão Baseada em Dados**:
    - Utilizar análises objetivas para identificar pontos críticos, como o volume de dados comprometidos, a sensibilidade das informações e o potencial de exploração.
    - Prover insumos para revisões contínuas dos planos de resposta, garantindo melhorias constantes.

O sucesso da classificação de criticidade depende da utilização de ferramentas apropriadas, capacitação das equipes envolvidas e atualização regular dos critérios de avaliação, assegurando uma resposta alinhada às ameaças e desafios em constante evolução.

e) Contenção, Erradicação e Recuperação

- É fundamental a colaboração dos responsáveis pelos sistemas e processos impactados para definir os procedimentos de resposta, contenção e erradicação.
- Os responsáveis pelos sistemas e processos afetados serão notificados imediatamente após a identificação do incidente e deverão ser chamados

a participar das ações de contenção e erradicação, assegurando a coordenação e o controle das atividades de resposta.

- O Encarregado de Dados (DPO) e o Comitê Gestor coordenarão as atividades, assegurando que as ações sejam executadas de acordo com o plano estabelecido.

- As medidas de contenção e erradicação visam restringir os danos e isolar os sistemas comprometidos, prevenindo assim a propagação de novas ameaças.
- As medidas de contenção devem ser implementadas de forma ágil para minimizar o impacto imediato e prevenir a propagação do incidente, interrompendo o acesso não autorizado e isolando sistemas ou serviços críticos.
- Em situações em que seja absolutamente necessário e autorizado, pode-se optar pelo desligamento total ou parcial dos sistemas afetados ou funcionalidades específicas, acompanhados de avisos de indisponibilidade para manutenção, com o objetivo de reduzir o risco e evitar a propagação.
- Todas as ações de contenção e erradicação devem ser realizadas sem comprometer a integridade das evidências, que poderão ser usadas para investigar a autoria, a origem e o método utilizado para quebrar a segurança.

Em caso de incidente envolvendo máquinas virtuais, deve ser feito snapshot (registro do estado de um arquivo, aplicação ou sistema em um certo ponto no tempo) para posterior análise.

- Em situações que envolvam máquinas virtuais, será realizado o **snapshot** para registrar o estado do sistema e assegurar a preservação das evidências necessárias para análise forense.
- O registro deve ser feito antes da contenção para garantir a integridade dos dados durante o processo.

Em se tratando de incidentes não relacionados a recursos computacionais, mas essencialmente de atividade humana, os procedimentos podem envolver sindicância administrativa, processo administrativo disciplinar, entre outras medidas dispostas na legislação aplicável ao caso.

- Incidentes que não envolvam sistemas computacionais, mas resultem de atividades humanas como erros ou condutas indevidas, serão tratados com base nas normas administrativas, como sindicâncias ou processos disciplinares, conforme as leis aplicáveis.
- As medidas corretivas podem incluir ações disciplinares ou ações legais para garantir a conformidade e o respeito à legislação vigente.

A recuperação tem como objetivo a restauração completa dos serviços, porém pode ser implementada de forma progressiva, a critério do gestor responsável e de acordo com as condições técnicas.

- Após a contenção, as medidas de recuperação visam a restauração gradual dos serviços afetados. O responsável pelo sistema pode decidir a ordem e a forma como os serviços serão restabelecidos, levando em consideração a viabilidade técnica e a minimização dos riscos residuais.
- A recuperação pode incluir a reconfiguração de sistemas, aplicação de patches, ou mesmo a reinstalação de softwares, conforme necessário.

Pode ser necessário o desenvolvimento e instalação de atualizações de aplicação ou do Sistema Operacional, ou elaboração de novas rotinas processuais.

- A recuperação pode exigir a instalação de atualizações, patches de segurança ou a criação de novas rotinas para prevenir a ocorrência de incidentes futuros.
- As atualizações devem ser testadas para garantir a correção das vulnerabilidades sem impactar os serviços em operação.

f) Comunicações

Assim que possível, a situação deve ser encaminhada para análise para avaliar se houve risco ou dano relevante aos titulares dos dados pessoais impactados.

- Após a contenção e erradicação, a situação do incidente deve ser encaminhada à **Prefeitura Municipal de Realeza** para que seja realizada a avaliação do potencial impacto ou danos aos titulares de dados pessoais.
- O DPO será o responsável por comunicar a ocorrência e as ações realizadas à ANPD e aos titulares de dados, assegurando transparência e conformidade com as obrigações legais.

Caso a Prefeitura Municipal de Realeza conclua que o incidente acarretou risco ou dano relevante aos titulares de dados pessoais, o Encarregado de Dados (DPO), deverá fazer as comunicações obrigatórias por Lei.

- O Encarregado de Dados (DPO) será responsável por realizar as comunicações obrigatórias, incluindo notificações formais aos titulares de dados, conforme determina a LGPD.

g) Preceitos Assimilados

16. Após a contenção e erradicação, o DPO deverá organizar uma reunião de **lições aprendidas**, com a participação de gestores e colaboradores para discutir erros, dificuldades e propor melhorias em sistemas e processos, fortalecendo a eficácia do Plano de Resposta a Incidentes da Prefeitura Municipal de Realeza.

As melhorias sugeridas na reunião devem ser encaminhadas à Prefeitura Municipal de Realeza para deliberação sobre a adoção.

- As recomendações de melhoria discutidas na reunião serão enviadas à **Prefeitura Municipal de Realeza**, para avaliação e deliberação sobre a adoção de novas medidas ou atualizações nas políticas e processos.

h) Documentação

O DPO deve documentar o incidente em base de conhecimentos apropriada, detalhando as informações obtidas, linha de tempo, atores envolvidos, evidências, conclusões, decisões, autorizações e ações executadas, inclusive as da reunião de lições aprendidas.

- O DPO será responsável por documentar detalhadamente o incidente em uma base de conhecimento apropriada, registrando evidências, linha do tempo, decisões, autorizações e as ações tomadas, incluindo o registro das reuniões de lições aprendidas.

Após a neutralização da ameaça, o Encarregado de Dados (DPO) deve elaborar um relatório circunstanciado de todas as medidas que foram adotadas, apresentando informações como a natureza do incidente, danos ou potenciais danos, providências adotadas, e os relatórios enviados à Prefeitura Municipal de Realeza.

- Após a neutralização da ameaça, o DPO deve elaborar um **relatório circunstanciado** com informações detalhadas sobre a natureza do incidente, os riscos envolvidos, as ações tomadas, as providências corretivas implementadas e os relatórios enviados à Prefeitura Municipal de Realeza.

O presente plano de incidentes é uma proposta a ser customizada pela Prefeitura Municipal de Realeza, de acordo com as peculiaridades de cada área e sob a supervisão do Encarregado de Dados e do Comitê Gestor.

São Paulo, 14 de fevereiro de 2025.

MARA CRISTHIANE VENDITTI BORGES:16612640855

Assinado de forma digital por MARA CRISTHIANE VENDITTI BORGES:16612640855
Dados: 2025.01.14 11:06:54 -03'00'