**PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E DADOS PESSOAIS**

**PREFEITURA MUNICIPAL DE CARACOL/MS**

**INTRODUÇÃO**

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018), conhecida como LGPD, impõe aos agentes de tratamento de dados pessoais a responsabilidade de garantir a segurança dessas informações, conforme previsto no artigo 47. Essa obrigação de proteção permanece vigente mesmo após o término do tratamento dos dados. A ausência de medidas técnicas e administrativas adequadas para proteger os dados sob custódia do controlador pode ser tão prejudicial como um ataque cibernético.

O artigo 46 da LGPD reforça a necessidade de adotar precauções que protejam os dados pessoais de acessos não autorizados e de situações acidentais ou de tratamento inadequado. Essas precauções não se limitam apenas ao uso de tecnologias e padrões de segurança, mas também envolvem a elaboração, manutenção e revisão de documentos. Essas práticas visam otimizar os processos internos, resguardando a reputação da organização, bem como seus servidores, prestadores de serviço e colaboradores. Este guia foi criado para auxiliar os profissionais responsáveis pelo tratamento de dados pessoais e demais servidores subordinados ao Encarregado da Proteção de Dados. Seu objetivo é incentivar a adoção de boas práticas de segurança e proteção de dados, especialmente no que tange à resposta a incidentes. As informações apresentadas serão constantemente atualizadas, incorporando melhorias e novas normas à medida que os processos de proteção de dados evoluem, assegurando uma abordagem dinâmica e eficiente na preservação dos dados pessoais. Assim, ao seguir as diretrizes deste guia e adotar as diligências indicadas pela LGPD, as organizações estarão melhor preparadas para mitigar riscos, garantindo não apenas a conformidade legal, mas também a proteção eficaz de suas informações e a manutenção de sua credibilidade.

**1. OBJETIVO GERAL**

Estabelecer diretrizes e procedimentos para detectar, avaliar, comunicar, conter e remediar incidentes de segurança da informação e vazamento de dados pessoais, garantindo a continuidade dos serviços públicos e o cumprimento da LGPD.

**1.1. OBJETIVOS ESPECÍFICOS**

Determina-se como objetivos específicos deste plano:

* Conferir clareza sobre o fluxo de procedimentos adequados e responsáveis no caso de incidentes;
* Preservar a reputação e imagem da prefeitura Municipal de Caracol/MS;
* Assegurar respostas rápidas, efetivas e coordenadas;
* Quantificar e monitorar desempenho; e
* Evoluir continuamente com as lições aprendidas.

**2. ABRANGÊNCIA**

Este plano aplica-se a todos os setores da Prefeitura Municipal de Caracol/MS, incluindo servidores efetivos, comissionados, estagiários, prestadores de serviço, e empresas terceirizadas que tenham acesso a sistemas e dados da administração pública.

**3. DEFINIÇÕES**

No contexto deste plano e com base na Lei Geral de Proteção de dados (Lei 13.709/2018- LGPD), são definidos:

* **LGPD**: Lei Federal nº 13.709/2018, que regula o tratamento de dados pessoais em meios físicos ou digitais, por pessoas físicas ou jurídicas, públicas ou privadas, visando proteger os dados pessoais.
* **ANPD**: Autoridade responsável por fiscalizar e garantir o cumprimento da legislação de proteção de dados pessoais no Brasil.
* **Dado pessoal**: Qualquer informação que permita identificar, direta ou indiretamente, uma pessoa, como nome, documentos, telefone, endereço, e-mail, etc.
* **Dado pessoal sensível**: Informações sobre origem racial, religião, opinião política, saúde, dados genéticos ou biométricos.
* **Anonimização**: Processo que impede a associação de um dado a uma pessoa, direta ou indiretamente.
* **Pseudonimização**: Tratamento de dados que só permite a identificação por meio de informação adicional, mantida em ambiente seguro.
* **Titular**: Pessoa física a quem se referem os dados pessoais.
* **Controlador**: Pessoa ou entidade responsável pelas decisões sobre o tratamento de dados.
* **Operador**: Pessoa ou entidade que realiza o tratamento de dados em nome do controlador (servidor não é operador).
* **Agentes de tratamento**: O controlador e o operador
* **Encarregado da Proteção de Dados**: Responsável pela comunicação entre o controlador, os titulares e a ANPD.
* **Tratamento**: Qualquer operação com dados pessoais, como coleta, armazenamento, eliminação, transmissão, etc.
* **Incidente**: Ato ou evento que compromete a segurança de dados pessoais.
* **Incidente de segurança com dados pessoais**: Violação de dados, como acesso não autorizado, perda, alteração ou vazamento.
* **Relatório de impacto à proteção de dados pessoais (RIPD)**: quando o tratamento de dados puder gerar riscos à liberdade civil e aos direitos fundamentais do titular, o controlador deverá elaborar uma documentação contendo a descrição dos processos de tratamento de dados pessoais;

**4. EQUIPE DE RESPOSTA A INCIDENTES (ERI)**

A equipe será composta por representantes das seguintes áreas:

* Departamento de Tecnologia da Informação (DTI);
* Controladoria Interna;
* Assessoria Jurídica;
* Encarregado de Dados (DPO);
* CONTROLADOR;
* OPERADOR.

**4.1.1 A Responsabilidade da ERI**

É de responsabilidade da ERI:

* Classificar o incidente
* Coordenar ações de contenção e correção
* Comunicar autoridades e titulares
* Elaborar relatórios de lições aprendidas

**5. CLASSIFICAÇÃO DOS INCIDENTES**

| **Nível** | **Descrição** | **Exemplos** |
| --- | --- | --- |
| Baixo | Sem impacto ou impacto mínimo | Acesso indevido isolado |
| Médio | Impacto moderado | Vazamento de dados pessoais sem sensibilidade |
| Alto | Impacto elevado e/ou violação da LGPD | Vazamento de dados sensíveis, indisponibilidade de sistemas essenciais |

**6. PROCEDIMENTOS DE RESPOSTA A INCIDENTES**

**6.1. Identificação**

* Recebimento de denúncia, alerta ou monitoramento técnico.
* Registro imediato em formulário interno.

**6.2. Análise**

* Verificação da natureza, origem e abrangência do incidente.
* Classificação do incidente conforme tabela acima.

**6.3. Contenção**

* Ações imediatas para impedir que o incidente se espalhe (ex: desconexão de rede, suspensão de contas).

**6.4. Erradicação**

* Eliminação da causa do incidente (ex: remoção de malware, correção de falha de configuração).

**6.5. Recuperação**

* Restauração dos sistemas e dados afetados.
* Testes para garantir que o ambiente esteja seguro.

**6.6. Comunicação**

* Comunicação interna aos gestores.
* Comunicação externa aos titulares, quando necessário.
* Notificação à ANPD, quando aplicável (prazo de até 2 dias úteis).

**6.7. Lições Aprendidas**

* Reunião para revisar o ocorrido.
* Atualização dos procedimentos para evitar reincidência.



*Fluxograma 1: Processo de resposta a incidentes****Fonte:*** *O próprio autor*

**7. CANAIS DE COMUNICAÇÃO**

* **Canal de denúncias para titulares de dados:**

ouvidoria@pmcaracol.ms.gov.br

**8. ARMAZENAMENTO E REGISTRO**

Todos os incidentes devem ser documentados em formulário padrão e arquivados por, no mínimo, 5 anos, em repositório seguro.

**9. REVISÃO E ATUALIZAÇÃO**

Este plano deve ser revisado anualmente ou sempre que houver mudanças significativas nos sistemas, legislação ou estrutura da prefeitura.

**10. DISPOSIÇÕES FINAIS**

O descumprimento deste plano poderá ensejar apuração de responsabilidade administrativa, civil e penal conforme legislação vigente.