PLANO DE RESPOSTA A INCIDENTES DE DADOS

ASSOCIAÇÃO DOS MUNICÍPIOS DO MEIO OESTE CATARINENSE - AMMOC

2025

Histórico de versões

Data	Versão	Descrição	Autor
18/08/2025	1.0	Plano de Resposta a Incidentes de Dados	Consultora

1. INTRODUÇÃO

Este Plano de Resposta a Incidentes de Segurança da Informação Envolvendo Dados Pessoais ("Plano de Resposta a Incidente" ou "PRI") estabelece o procedimento para a gestão de situações após a identificação da ocorrência, ou mera suspeita, de um incidente de segurança da informação que envolva dados de pessoa natural identificada ou identificável ("Dados Pessoais") que são tratados pela **ASSOCIAÇÃO DOS MUNICÍPIOS DO MEIO OESTE CATARINENSE - AMMOC (Controlador de Dados)**, visando o combate dos riscos e a minimização de eventuais efeitos relacionados a incidentes desta natureza.

O presente PRI foi elaborado de acordo com a Lei nº 13.709/18 ("Lei Geral de Proteção de Dados Pessoais").

2. OBJETIVO

Este PRI tem como objetivo estabelecer as funções e responsabilidades da **ASSOCIAÇÃO DOS MUNICÍPIOS DO MEIO OESTE CATARINENSE - AMMOC**, bem como as medidas a serem tomadas que respondam adequadamente a um incidente, sempre prezando pela integridade dos sistemas, proteção de todas e quaisquer informações que possam viabilizar, direta ou indiretamente, a identificação de uma pessoa física ("Dados Pessoais") e privacidade dos seus titulares, possibilitando a AMMOC manter a confiabilidade de suas marcas, produtos e serviços. Também estão compreendidas dentro do conceito de Dados Pessoais todas as informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, informações referentes à saúde ou à vida sexual, dados genéticos ou biométricos e quaisquer dados que, quando tratados de forma combinada com outras informações, possam permitir inferir informações dessa natureza ("Dados Sensíveis").

O presente PRI se aplica em qualquer caso de incidentes envolvendo Dados Pessoais e deverá ser cumprida, em conjunto com as demais políticas da AMMOC incluindo, sem limitação, os agentes públicos, servidores, empregados, terceiros prestadores de serviços e parceiros que, no âmbito das suas relações com a Associação possam vir a ter acesso às áreas, equipamentos, informações, redes e aos arquivos e dados de sua responsabilidade.

Aplicam-se a este PRI, de forma complementar, as disposições da Política de Segurança da Informação, a fim de mitigar a ocorrência de incidentes de segurança da informação.

3. O QUE É UM INCIDENTE DE SEGURANÇA DA INFORMAÇÃO ENVOLVENDO DADOS PESSOAIS?

Para fins do presente PRI, entende-se por "Incidente" toda e qualquer violação de segurança que, de forma acidental ou dolosa, enseje ou seja capaz de dar ensejo à destruição, perda, alteração, divulgação ou ao uso ou acesso não autorizados a Dados Pessoais tratados pela AMMOC.

Um Incidente pode ocorrer de forma maliciosa, ser o resultado de um erro humano ou, até mesmo, de falha nos sistemas que processam Dados Pessoais ou nos seus mecanismos de segurança. Isso pode incluir por exemplo, o furto de um documento, o envio de um e-mail contendo Dados Pessoais para destinatários indesejados, tentativas de invasão a sistemas da AMMOC ou outras ações, culposas ou dolosas.

Os Incidentes podem ser de vários tipos, como por exemplo:

(i) **Vazamento de Dados Pessoais.** É o Incidente no qual Dados Pessoais são indevidamente expostos e disponibilizados, por meios físicos ou digitais, para um número indeterminado de pessoas, no Brasil ou em qualquer país;
(ii) **Negação de Serviço.** É o Incidente no qual o acesso (lógico ou físico) a um sistema que armazene Dados Pessoais é prejudicado ou impossibilitado, de forma que a integridade dos Dados Pessoais (existência e/ou veracidade) pode ser comprometida permanentemente, dada a indisponibilidade do acesso;
(iii) **Acesso Não Autorizado.** É o Incidente no qual o acesso (lógico ou físico) a um sistema que possua Dados Pessoais é tentado ou obtido, sem que se tenha a devida autorização para tal acesso. Considera-se acesso não autorizado qualquer acesso cuja permissão para conexão, leitura, gravação, autenticação, modificação, eliminação ou criação não tenha sido concedida; e
(iv) **Uso Inapropriado.** É o Incidente no qual há a violação das políticas de uso de dados, informações e sistemas da AMMOC, incluindo a Política de Segurança da Informação, Manual de conduta e outras normas internas.

4. PAPEIS E RESPONSABILIDADES

A AMMOC tem responsabilidades quando da ocorrência ou mera suspeita de um Incidente, conforme descritas a seguir:

4.1. Obrigações de todas as áreas

(i) comunicar imediatamente ao Encarregado de dados, representante de Comitê de Privacidade e Proteção de Dados ou ao superior imediato sobre a ocorrência ou a mera suspeita de um Incidente;

(ii) cumprir rigorosamente a Política de Segurança da Informação, Política de privacidade e outros regramentos da AMMOC, contribuindo para a mitigação de riscos; e
(iii) participar de treinamentos e programas de conscientização para mitigação de Incidentes.

4.2. Obrigações do Comitê de Privacidade e Proteção de Dados e do Encarregado

Entre suas principais responsabilidades, com o apoio dos demais servidores, destacamos:
(i) atuar para detectar e corrigir os Incidentes;
(ii) alertar, comunicar e aconselhar sobre Incidentes emergentes;
(iii) educar e conscientizar sobre a detecção e resposta aos Incidentes; e
(iv) adotar demais medidas necessárias para prevenir Incidentes e minimizar o impacto de seus efeitos.

5. DETECÇÃO DO INCIDENTE

Detectar um Incidente de forma rápida e eficiente é essencial para uma resolução bem-sucedida. São várias as formas de detecção, de modo que é impossível desenvolver uma metodologia que contemple cada uma. Desta forma, **todos os servidores** devem atentar-se, principalmente, aos sinais mais comuns que podem desencadear um Incidente, como invasões de rede, perda ou furto de documentos, arquivos ou dispositivos, *phishing*, *malware*, instabilidades sistêmicas etc.

Uma vez detectado um Incidente ou detectada a mera suspeita de um Incidente, o responsável deverá comunicar imediatamente o Encarregado de Dados ou um representante do Comitê de Privacidade e Proteção de Dados, por meio do contato do Encarregado de Dados Lauri Nora: encarregadodedados@ammoc.org.br e telefone: (49) 3522 2800.

Na medida do possível, essa comunicação deverá conter (i) a hora e a data em que a suspeita do Incidente foi descoberta; (ii) o tipo de informações envolvidas; (iii) a causa e a extensão do Incidente; (iv) o contexto do ocorrido; bem como (v) qualquer informação adicional que sirva para facilitar o entendimento do evento, suas causas e consequências.

A comunicação sobre a suspeita de um incidente é vital para a AMMOC. Assim, caso o servidor suspeite de um incidente e não o comunique, sanções disciplinares poderão ser-lhe aplicadas, a depender da gravidade do incidente e após apuração da responsabilidade.

5.1. Avaliação do incidente

Quando a AMMOC tem conhecimento do incidente de segurança, deve ser realizada uma avaliação interna pelo Encarregado de Dados para que sejam obtidas informações como:
a) Vulnerabilidade: explorada no evento, abrangendo situações como: acesso indevido aos dados pessoais; roubo de dados; ataques cibernéticos; erros de programação de

aplicativos e sistemas internos; engenharia social; descartes indevidos; repasse de dados pessoais; roubo, venda e utilização de dados tutelados pela entidade; comprometimento de senhas de acesso; e outras.

b) Fonte dos dados pessoais: meio pelo qual foram obtidos os dados pessoais, tais como preenchimento de formulário eletrônico ou não eletrônico por parte do titular, aplicativos, uso compartilhado de dados.

c) Categoria de dados pessoais: dados sensíveis, dados pessoais de crianças e adolescentes ou idosos.

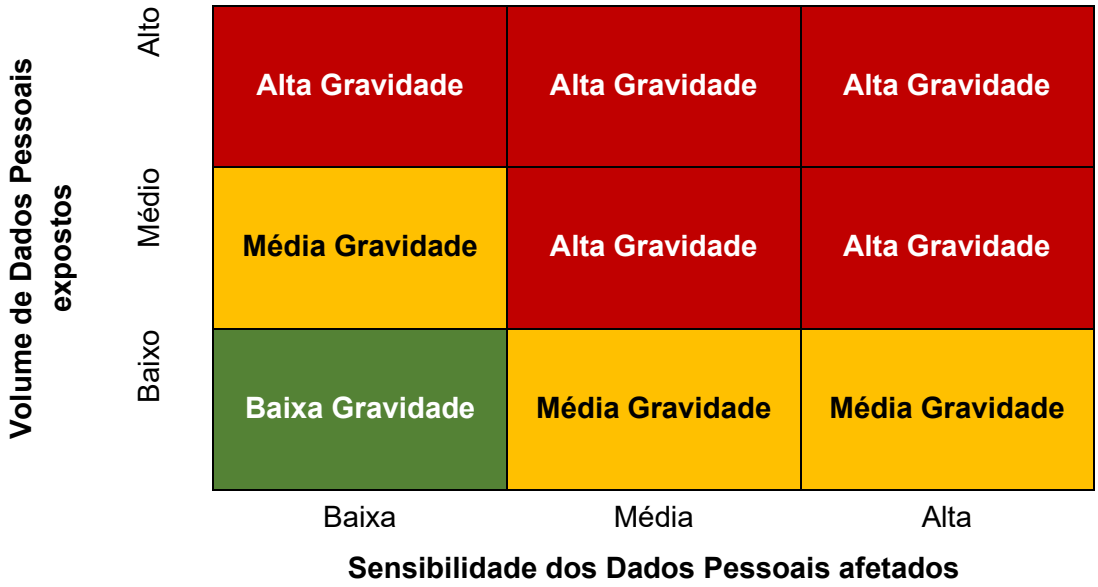
d) Extensão do vazamento: quantificar os titulares e os dados pessoais que tiveram a sua segurança violada neste evento.

e) Avaliação do impacto ao titular: avaliar quais são os impactos que o incidente pode gerar aos titulares.

f) Avaliação do impacto no serviço: avaliar os impactos que o incidente pode gerar a entidade como perda de confiabilidade do cidadão, ações judiciais, danos à imagem da instituição em âmbito nacional e internacional, prejuízo à entidade em contratos com fornecedores e clientes, e impacto total ou parcial nas atividades desenvolvidas pela entidade.

5.2. Priorização do Incidente e Procedimentos para Resposta

Uma vez que o Incidente seja identificado e classificado, é necessário priorizá-lo conforme o nível de risco oferecido à AMMOC ou aos titulares dos Dados Pessoais eventualmente afetados e a gravidade da ocorrência. O impacto do Incidente deve ser aferido da seguinte forma:



VOLUME DE DADOS PESSOAIS EXPOSTOS	
Criticidade	**Descrição**
Alto	volume de Dados Pessoais afetado superior a 10% da base

SENSIBILIDADE DOS DADOS PESSOAIS AFETADOS	
Criticidade	**Descrição**
Alta	Dados Pessoais de crianças ou adolescentes, Dados Pessoais Dados Sensíveis ou que possam

	de dados controlada pela AMMOC		gerar discriminação ao titular; dados bancários, de pagamento ou de proteção ao crédito
Médio	volume de Dados Pessoais afetado inferior a 10% e superior a 2% da base de dados controlada pela AMMOC	Média	Dados Pessoais imediatamente identificáveis (e.g. nome, e-mail, CPF), combinados ou não com informações comportamentais (e.g. histórico de atividades, preferências etc.)
Baixo	volume de Dados Pessoais afetado inferior a 2% da base de dados controlada pela AMMOC	Baixa	Dados anonimizados, Dados Pessoais pseudonimizados (desde que a chave de desanonimização também não tenha sido comprometida), Dados Pessoais de difícil identificação (e.g. IP)

De acordo com a matriz acima definida, o Encarregado de Dados, com o apoio do Comitê de Privacidade e Proteção de Dados Pessoais deverá tomar as seguintes ações, simultaneamente ou, quando não for possível, em rápida sucessão:

a) Baixa Gravidade

(i) tão logo tenha ciência, trabalhar prioritariamente na resolução do Incidente;
(ii) tomar as medidas adequadas para minimizar os efeitos causados pelo Incidente e para promover sua rápida correção;
(iii) comunicar as Áreas Envolvidas, que deverão estar à disposição;
(iv) uma vez que as medidas de resolução sejam tomadas, documentar o Incidente, conforme modelo anexo a este PRI; e
(v) reunir-se para analisar o Incidente e antecipar, prevenir e melhor identificar Incidentes semelhantes no futuro, devendo esta reunião ser transcrita em ata, que deverá ser apresentada ao gestor da AMMOC.

b) Média Gravidade

(i) tão logo tenha ciência, trabalhar de forma exclusiva na resolução do Incidente;
(ii) tomar as medidas imediatas para minimizar os efeitos causados pelo Incidente e para promover sua rápida correção e, se a correção não for possível de forma imediata, deve adotar as medidas temporárias para minimização de riscos;
(iii) comunicar as Áreas Envolvidas, que deverão estar à disposição para atender, com prioridade;
(iv) uma vez que as medidas de resolução sejam tomadas, documentar o Incidente, o mais breve possível, conforme modelo anexo a este PRI;
(v) reunir-se o mais breve possível para analisar o Incidente e antecipar, prevenir e melhor identificar Incidentes semelhantes no futuro, devendo esta reunião ser transcrita em ata documentada, que deverá ser apresentada ao gestor da AMMOC.

(vi) realizar, imediatamente, treinamento interno com as áreas afetadas para conscientizar os servidores sobre o Incidente e medidas preventivas.
(vii) Instaurar sindicância ou processo administrativo disciplinar para apuração de responsabilidades.

c) Alta Gravidade

(i) tão logo tenha ciência, trabalhar de forma exclusiva na resolução do Incidente;
(ii) imediatamente comunicar os responsáveis pelas Áreas Envolvidas, os quais, em conjunto com outra pessoa de cada uma das respectivas Áreas Envolvidas, devem atuar de forma exclusiva no suporte ao Encarregado de Dados preferencialmente no mesmo local em que a Equipe de Resposta esteja trabalhando;
(iii) Fazer a comunicação ao titular de dados pessoais e publicização do incidente, se for o caso;
(iv) uma vez que as medidas de resolução sejam tomadas, documentar o Incidente, imediatamente, conforme modelo anexo a este PRI;
(v) reunir-se, imediatamente, para avaliar o Incidente e antecipar, prevenir e melhor identificar Incidentes semelhantes no futuro, devendo esta reunião ser transcrita em ata, que deverá ser apresentada ao gestor da AMMOC;
(vi) realizar, imediatamente, treinamento interno com todos os servidores da AMMOC para conscientizar sobre o Incidente e medidas preventivas; e
(vii) comunicar, imediatamente, os servidores sobre medidas preventivas.
(viii) Instaurar sindicância ou processo administrativo disciplinar para apuração de responsabilidades.

5.3. Comunicação do Incidente

Em cumprimento à legislação brasileira, incidentes considerados relevantes devem ser comunicados à Autoridade Nacional de Proteção de Dados (ANPD) no prazo de 3 (três) dias úteis. A avaliação sobre quais Incidentes são materialmente relevantes cabe ao Encarregado de Dados, em conjunto com o Comitê de Privacidade e Proteção de Dados da AMMOC (Controlador de dados).

O controlador é responsável por manter o registro do incidente de segurança, mesmo que não tenha sido comunicado à ANPD e aos titulares, conforme art. 10 da Resolução CD/ANPD Nº 15/2024. Tal registro deverá conter minimamente os seguintes itens:
I. a data de conhecimento do incidente;
II. a descrição geral das circunstâncias em que o incidente ocorreu;
III. a natureza e a categoria de dados afetados;
IV. o número de titulares afetados;
V. a avaliação do risco e os possíveis danos aos titulares;
VI. as medidas de correção e mitigação dos efeitos do incidente, quando aplicável;
VII. a forma e o conteúdo da comunicação, se o incidente tiver sido comunicado à ANPD e aos titulares; e
VIII. os motivos da ausência de comunicação, quando for o caso.

O art. 48 da LGPD e o art. 5º da Resolução CD/ANPD Nº 15/2024 determinam que o controlador tem o dever de comunicar à ANPD e ao titular dos dados pessoais a ocorrência de incidente de segurança que **tenha potencial de risco ou dano relevante** que possam afetar consideravelmente seus interesses e direitos fundamentais e, cumulativamente, **envolver, pelo menos, um dos seguintes critérios:**
a) dados pessoais sensíveis;
b) dados de crianças, de adolescentes ou de idosos;
c) dados financeiros;
d) dados de autenticação em sistemas;
e) por sigilo legal, judicial ou profissional; ou
f) dados em larga escala.

5.4. Comunicação aos Titulares de Dados

Caso o Controlador e o Encarregado de Dados, com o apoio do Comitê, determinem a comunicação sobre o Incidente aos titulares dos Dados Pessoais afetados, o setor jurídico irá desenvolver a mensagem da comunicação, priorizando (i) os fatos ocorridos; (ii) as medidas já tomadas pela AMMOC para minimizar o impacto dos efeitos; (iii) as eventuais medidas que possam ser tomadas pelos próprios titulares dos Dados Pessoais afetados para mitigar riscos; e (iv) os canais de contato para sanar dúvidas.

A comunicação deve ser feita de forma individual e diretamente aos titulares, sempre que possível.
Se, pela natureza do incidente, não for possível identificar individualmente os titulares afetados, o controlador deverá comunicar a ocorrência do incidente pelos meios de divulgação disponíveis, tais como seu sítio eletrônico, aplicativos, suas mídias sociais e canais de atendimento ao titular, de modo que a comunicação permita o conhecimento amplo, com direta e fácil visualização, pelo período mínimo de 3 (três) meses, conforme a Resolução CD/ANPD Nº 15/2024.

6. DISPOSIÇÕES FINAIS

Em caso de dúvidas, comentários e/ou sugestões relacionadas a este PRI, entre em contato com a AMMOC pelo Encarregado de dados Lauri Nora: encarregadodedados@ammoc.org.br e telefone: (49) 3522 2800.

Joaçaba – SC, 18 de agosto de 2025.

Presidente da AMMOC

Aprovado em setembro de 2025.