PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO ENVOLVENDO DADOS PESSOAIS

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 **CÂMARA MUNICIPAL DE VEREADORES DE CACIQUE DOBLE,** 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 13.709/18 ("Lei Geral de Proteção de Dados Pessoais").

2. OBJETIVO

Este PRI tem como objetivo estabelecer as funções e responsabilidades, bem como as medidas a serem tomadas pela Câmara de Cacique Doble para que responda 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. 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, incluindo, sem limitação, terceiros que, no âmbito das suas relações com a Câmara possam vir a ter acesso à equipamentos, informações, redes e aos arquivos e dados pessoais e sensíveis.

Aplicam-se a este PRI, de forma complementar, as disposições da Política de Privacidade e Proteção de Dados Pessoais e a 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 Câmara.

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 do grupo ou outras ações, culposas ou dolosas.

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

✓ 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;

✓ 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;

✓ 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

✓ Uso Inapropriado. É o Incidente no qual há a violação das políticas de uso de dados, informações e sistemas do órgão incluindo, mas não se limitando à Política de Segurança da Informação e Política de Privacidade e Proteção de Dados Pessoais.

4. PAPÉIS E RESPONSABILIDADES

Cada pessoa seja diretamente envolvida na governança ou não, têm responsabilidades quando da ocorrência ou mera suspeita de um Incidente, conforme descritas a seguir:

4.1. Obrigações

✓ Comunicar imediatamente a Equipe de Resposta (conforme descrito abaixo), sobre a ocorrência ou a mera suspeita de um Incidente;

✓ Cumprir rigorosamente a Política de Segurança da Informação da Câmara, contribuindo para a mitigação de riscos; e

✓ Participar de treinamentos e programas de conscientização para mitigação de Incidentes.

4.2. Obrigações da Equipe de Resposta

A Equipe de Resposta a Incidentes da Câmara é formada pelos designados abaixo para atuar nas respostas a Incidentes:

Departamento /Departamento	Pessoa Responsável
Mesa Diretora	Presidente: Lenir Nunes
Encarregado	Juliano de Mattos Salles
Jurídico	Assessor: Somer Idea

Entre suas principais responsabilidades, destacamos:

- Atuar para detectar e corrigir os Incidentes;
- Alertar, comunicar e aconselhar os servidores sobre Incidentes emergentes;
- Educar e conscientizar os servidors sobre a detecção e resposta aos Incidentes;
- Adotar demais medidas necessárias para prevenir Incidentes e minimizar o impacto de seus efeitos, e
- Auxiliar na resolução das questões técnicas relacionadas ao Incidente e na investigação da origem e das razões para ocorrência do Incidente.

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 deve-se atentar, 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, deverá ser comunicado ao Encarregado por meio do e-mail: secretaria@camaracaciquedoble.rs.gov.br

Na medida do possível, essa comunicação deverá conter (1) a hora e a data em que a suspeita do Incidente foi descoberta; (2) o tipo de informações envolvidas; (3) a causa e a extensão do Incidente; (4) o contexto do ocorrido; bem como (5) qualquer informação adicional que sirva para facilitar o entendimento do evento, suas causas e consequências.

5.1. 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 Câmara e aos titulares dos Dados Pessoais eventualmente afetados e a gravidade da ocorrência. O impacto do Incidente deve ser aferido da seguinte forma:

SENSIBILIDADE DOS DADOS PESSOAIS AFETADOS

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**

De acordo com a matriz acima definida, deverão ser tomadas as seguintes ações, simultaneamente ou, quando não for possível, em rápida sucessão:

Baixa Gravidade

Tão logo tenha ciência, trabalhar prioritariamente na resolução do Incidente:

✓ tomar as medidas adequadas para minimizar os efeitos causados pelo Incidente e para promover sua rápida correção;

✓ comunicar o Encarregado;

✓ uma vez que as medidas de resolução sejam tomadas, documentar o Incidente, conforme modelo anexo a este PRI; e

✓ reunir-se para analisar o Incidente e antecipar, prevenir e melhor identificar incidentes semelhantes no futuro, devendo esta reunião ser transcrita em ata.

Média Gravidade

✓ tão logo tenha ciência, trabalhar de forma exclusiva na resolução do Incidente;

✓ 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;

✓ comunicar o Encarregado;

✓ uma vez que as medidas de resolução sejam tomadas, documentar o Incidente, o mais breve possível, conforme modelo anexo a este PRI;

✓ 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;

✓ realizar, imediatamente, treinamento interno sobre o Incidente e medidas preventivas.

Alta Gravidade

✓ tão logo tenha ciência, trabalhar de forma exclusiva na resolução do Incidente;

✓ uma vez que as medidas de resolução sejam tomadas, documentar o Incidente, imediatamente, conforme modelo anexo a este PRI;

✓ reunir-se, imediatamente, para avaliar o Incidente e antecipar, prevenir e melhor identificar Incidentes semelhantes no futuro, devendo esta reunião ser transcrita em ata;

✓ realizar, imediatamente, treinamento interno conscientizar sobre o Incidente e medidas preventivas (se for o caso);

5.2. Comunicação do Incidente

Em cumprimento à legislação brasileira, incidentes considerados relevantes devem ser comunicados à Autoridade Nacional de Proteção de Dados (ANPD). A avaliação sobre quais incidentes são materialmente relevantes cabe ao responsável em conjunto com a Mas Diretora.

Caso um Incidente seja identificado como relevante e a sua comunicação à ANPD seja determinada, o departamento Jurídico deverá, com suporte dos representantes legais, elaborar a documentação aplicável à comunicação, contendo:

✓ a descrição da natureza e da categoria dos Dados Pessoais afetados (ex. Dados sensíveis, dados de criança, dados cadastrais etc.);

✓ As informações sobre os titulares dos Dados Pessoais envolvidos, a relação dos titulares dos Dados Pessoais afetados com a Câmara, o número de titulares afetados e o país de residência dos titulares dos Dados Pessoais afetados;

✓ a indicação das medidas técnicas e de segurança utilizadas para a proteção dos Dados Pessoais;

✓ os riscos relacionados ao Incidente;

✓ os motivos da demora, no caso de a comunicação não ter sido feita de forma imediata; e

✓ as medidas que foram e que serão adotadas para reverter ou mitigar os efeitos do Incidente.

Caso os responsáveis determinem a comunicação sobre o Incidente aos titulares dos Dados Pessoais afetados, o departamento Jurídico, irá desenvolver a mensagem da comunicação, priorizando (i) os fatos ocorridos; (ii) as medidas já tomadas pelo órgão 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.

6. DISPOSIÇÕES FINAIS

Em caso de dúvidas, comentários e/ou sugestões relacionadas a este PRI, entre em contato com o Encarregado que está à disposição no seguinte endereço de contato:

O Presente Plano poderá ser atualizado sempre que necessário, ficando a cargo dos agentes envolvidos realizar uma verificação periódica, não superior a 1 (um) ano a fim de identificar possíveis alterações/atualizações.

ANEXO
MODELO DE DOCUMENTAÇÃO DE INCIDENTES

1. AGENTES		
1.1	papel da Câmara com relação aos Dados Pessoais afetados	[controlador/operador]
1.2	caso a Câmara atue como Controlador, informe quem é o Operador	[completar se houver]
1.3	informação de contato do Operador	[completar se houver]
1.4	caso a Câmara atue como Operador, informe quem é o Controlador	[completar se houver]
1.5	informação de contato do Controlador	[completar se houver]
2. INCIDENTE		
2.1	resumo do Incidente (explicação sobre o ocorrido)	
2.2	resumo das causas do Incidente (motivações e circunstâncias técnicas e fáticas)	
2.3	data de ocorrência do Incidente	
2.4	data da identificação do Incidente	
2.5	forma de identificação do Incidente	[reporte pelo departamento responsável; procedimentos automatizados; rotinas de verificação de sistemas; etc.]
2.6	data de término do Incidente, se houver	[completar se houver. Ex.: um sequestro de banco de dados pode estar ocorrendo no momento da comunicação à autoridade.]
2.7	natureza do Incidente	[ex.: perda de um dossiê físico ou de um dispositivo; ataques externos; destruição incorreta; acesso indevido; envio de Dados Pessoais ao destinatário incorreto etc.]
2.8	consequência geral do Incidente	[quebra de confidencialidade; perda de integridade dos dados; perda da disponibilidade dos dados etc.]
2.9	Dados Pessoais afetados pelo Incidente	[Exemplo: Dados de identificação (nome, RG, CPF, login, chapa); Dados financeiros e bancários (agência, conta e remuneração); Dados de contato (telefone, endereço, e-mail); e Dados de saúde (ASO e resultados de exames toxicológicos)]

3. TITULARES DOS DADOS PESSOAIS		
3.1	relação dos titulares dos Dados Pessoais afetados com a Câmara (caso a Câmara seja o controlador)	[empregados; clientes; fornecedores]
3.2	número de titulares afetados pelo Incidente	
3.3	país de residência dos titulares dos Dados Pessoais afetados	
4. RISCOS		
4.1	natureza do risco potencial aos titulares dos Dados Pessoais afetados e probabilidade estimada de materialização do risco	[ex.: perda financeira – risco alto; impacto reputacional – risco baixo; discriminação etc.]
5. MEDIDAS		
5.1	medidas de segurança da informação (técnicas) adotadas até a ocorrência do Incidente	
5.2	medidas de governança adotadas até a ocorrência do Incidente	
5.3.	medidas (técnicas e de governança) adotadas ou previstas para minimizar o impacto dos efeitos do Incidente	[sugere-se indicar as datas/horários e medidas adotadas do momento da identificação do Incidente até agora]
5.4	medidas (técnicas e de governança) adotadas ou previstas para impedir que o Incidente aconteça novamente	
6. COMUNICAÇÃO		
6.1	medidas adotadas ou previstas para comunicar os titulares dos Dados Pessoais afetados	
6.2	Necessidade de comunicar autoridades? Em caso positivo, quais?	