Plano de Resposta a Incidentes de Segurança da Informação

1. Introdução

O Oficial de Registro de Imóveis, Títulos e Documentos e Civil das Pessoas Jurídicas da Comarca de Novo Horizonte - SP é um feixe de competências públicas exercido, em caráter privado, pelo Oficial de Registro, que atua como controlador de dados pessoais. O presente documento destina-se a todos os empregados da serventia, bem como aos usuários do serviço, e possui função orientativa, explicativa e de controle.

Este Plano de Resposta a Incidentes de Segurança da Informação ("Plano de Resposta a Incidente", "Plano" ou "PRI") estabelece o procedimento para a gestão de situações após a identificação da ocorrência, ou suspeita, de um incidente de segurança da informação que envolva dados de pessoa natural identificada ou identificável ("Dados Pessoais") que são tratados pelo controlador, visando ao combate dos riscos e à mitigação dos 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").

Este plano é apenas um dos diversos mecanismos de controle do fluxo de dados pessoais, e deve ser lido e interpretado em conjunto com os demais, a seguir arrolados:

- Política de Privacidade e Tratamento de Dados Pessoais;
- Inventário de Dados Pessoais;
- Política de Segurança da Informação;
- Política de Privacidade do Website;
- Política de Direitos dos Titulares dos Dados Pessoais;
- Bem como as leis e regulamentos em vigor.

Caso subsistam dúvidas sobre qualquer dos procedimentos aqui explicados, os titulares, as autoridades judiciárias e a Autoridade Nacional de Proteção de Dados Pessoais (ANPD) poderão entrar em contato com o encarregado ou com o controlador por qualquer dos meios indicados ao final deste documento.

2. Objetivo

Este plano tem como objetivo estabelecer as funções e as responsabilidades do controlador, do encarregado e do pessoal da serventia extrajudicial, bem como as medidas a serem tomadas para adequada e tempestiva resposta a um incidente de segurança da informação. O objetivo dessas medidas é zelar pela integridade dos sistemas, bem como pela proteção das informações e dos dados que possam viabilizar, direta ou indiretamente, a identificação de uma pessoa natural.

Por sua vez, são considerados dados pessoais sensíveis as informações vinculadas ou que possam ser vinculadas a uma pessoa natural, que estejam relacionadas com: origem racial ou étnica; convicção religiosa; opinião política; filiação a sindicato ou a organização de caráter religioso, filosófico ou político; saúde ou vida sexual; bem como os dados genéticos ou biométricos, e aqueles que, quando tratados de forma combinada com outras informações, possam permitir inferir informações dessa natureza.

O presente plano se aplica a quaisquer incidentes envolvendo dados pessoais, e deverá ser cumprido em conjunto com as demais políticas e determinações do controlador, por todas as pessoas que possam vir a ter acesso às áreas, equipamentos, informações, redes e aos arquivos e dados geridos pela serventia.

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. Conceito de “Incidente de Segurança da Informação”

Para os fins do presente plano, entende-se por “incidente de segurança da informação” 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 transmissão não autorizada de dados pessoais tratados pelo controlador.

Um incidente pode ocorrer de forma maliciosa, ser o resultado de um erro humano ou de falha nos sistemas que processam e armazenam dados pessoais. São exemplos de incidentes: o furto de um documento do cartório; o envio de um e-mail contendo dados pessoais para destinatários indesejados; uma tentativa de invasão a sistemas informáticos.

Os incidentes podem ser de vários tipos, dentre eles:

- **Vazamento:** dados pessoais são indevidamente expostos e disponibilizados, por meios físicos ou digitais, para um número indeterminado de pessoas, no Brasil ou no exterior.
- **Negação de serviço:** o acesso (lógico ou físico) a um sistema que armazene dados pessoais é prejudicado ou impossibilitado, de forma que a integridade das informações nele contidas (existência e/ou veracidade) possa ser comprometida permanentemente, dada a indisponibilidade do acesso.
- **Acesso clandestino:** o acesso (lógico ou físico) a um sistema que possua dados pessoais é obtido sem que se tenha a devida autorização. Considera-se acesso clandestino ou irregular aqueles cuja permissão para conexão, leitura, gravação, autenticação, modificação, eliminação ou criação não tenha sido concedida, ou seja insuficiente.
- **Uso inapropriado:** nesse incidente, o tratamento de dados pessoais ocorre em desacordo com as políticas definidas pelo controlador, ou com as diretrizes legais ou regulamentares.

A identificação do incidente deve ensejar os procedimentos descritos neste plano, ainda que não tenha sido adequadamente classificado.

4. Papéis e responsabilidades

Todos os setores e agentes da serventia (controlador, encarregado, prepostos, empregados, subcontratados, prestadores de serviço, fornecedores e usuários) possuem responsabilidades na gestão e na adequada resposta a um incidente de segurança da informação. São eles:

4.1. Obrigações comuns a todos os agentes

- Comunicar imediatamente ao Controlador ou ao Encarregado a ocorrência ou a suspeita de um incidente;
- Cumprir rigorosamente a Política de Segurança da Informação e a Política de Privacidade e Tratamento de Dados Pessoais, contribuindo para a mitigação de riscos; e

- Participar dos treinamentos e programas de conscientização para prevenção de incidentes e mitigação de efeitos negativos.

4.2. Obrigações do encarregado

- Atuar para detectar e corrigir os incidentes;
- Alertar, comunicar e aconselhar os prepostos, colaboradores e o controlador sobre incidentes potenciais;
- Educar e conscientizar o controlador, os prepostos e a equipe sobre medidas de detecção e reposta aos incidentes;
- Adotar, com prontidão, todas as medidas necessárias para a identificação, comunicação, contenção e mitigação de impacto dos incidentes de segurança da informação;
- Comunicar imediatamente ao controlador quaisquer violações ou incidentes, ainda que potenciais;
- Prestar informações e responder às requisições de autoridade judiciárias, correcionais e da Autoridade Nacional de Proteção de Dados Pessoais (ANDP) em matéria de proteção de dados;

4.3. Obrigações do controlador

- Comunicar à Corregedoria-Geral da Justiça e à Corregedoria Permanente sobre quaisquer incidentes ou vazamentos envolvendo dados pessoais;
- Avaliar a dimensão dos incidentes e propor aos prejudicados alternativas de mitigação, solução e/ou indenização;
- Providenciar os mecanismos de resposta necessários, de acordo com o volume de dados afetados pelo 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, todos os empregados, colaboradores e demais envolvidos devem 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 uma mera suspeita, o colaborador deverá comunicar imediatamente ao Encarregado.

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.

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 serventia e aos titulares dos dados eventualmente afetados, conforme a gravidade da ocorrência. O impacto do incidente deve ser aferido da seguinte forma:

Volume de Dados Pessoais expostos	Baixa	Média	Alta
Alto	**Alta Gravidade**	**Alta Gravidade**	**Alta Gravidade**
Médio	**Média Gravidade**	**Alta Gravidade**	**Alta Gravidade**
Baixo	**Baixa Gravidade**	**Média Gravidade**	**Média Gravidade**

Sensibilidade dos Dados Pessoais Afetados

Para identificação do grau de sensibilidade e do volume de dados pessoais expostos, devem ser levados em conta os seguintes parâmetros:

VOLUME DE DADOS PESSOAIS EXPOSTOS	
Criticidade	**Descrição**
Alto	volume de Dados Pessoais afetado superior a 10% da base de dados controlada pelo Cartório
Médio	volume de Dados Pessoais afetado inferior a 10% e superior a 2% da base de dados controlada pelo Cartório
Baixo	volume de Dados Pessoais afetado inferior a 2% da base de dados controlada pelo Cartório

SENSIBILIDADE DOS DADOS PESSOAIS AFETADOS	
Criticidade	**Descrição**
Alta	Dados Pessoais de crianças ou adolescentes, Dados Pessoais Dados Sensíveis ou que possam gerar discriminação ao titular; dados bancários, de pagamento ou de proteção ao crédito
Média	Dados Pessoais imediatamente identificáveis (e.g. nome, e-mail, CPF), combinados ou não com informações comportamentais (e.g. histórico de atividades, preferências etc.)
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 Controlador e o Encarregado deverão tomar as seguintes providências, simultaneamente ou, quando não for possível, em rápida sucessão:

Baixa Gravidade

- Tão logo tenham 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 Juízo Corregedor Permanente;
- Uma vez que as medidas de resolução sejam tomadas, documentar o Incidente; e
- Reunir-se para analisar o Incidente e antecipar, prevenir e melhor identificar incidentes semelhantes no futuro.

Média Gravidade

- Tão logo tenham 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 Juízo Corregedor Permanente;
- Comunicar a Autoridade Nacional de Proteção de Dados (ANPD);
- Uma vez que as medidas de resolução sejam tomadas, documentar o Incidente, o mais breve possível;

- Reunir-se o mais breve possível para analisar o Incidente e antecipar, prevenir e melhor identificar Incidentes semelhantes no futuro;
- Realizar, imediatamente, treinamento interno com as áreas afetadas para conscientizar os colaboradores e demais envolvidos sobre o Incidente e medidas preventivas.

Alta Gravidade

- Tão logo tenham 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 Juízo Corregedor Permanente;
- Comunicar a Autoridade Nacional de Proteção de Dados (ANPD);
- Uma vez que as medidas de resolução sejam tomadas, documentar o Incidente, o mais breve possível;
- Reunir-se o mais breve possível para analisar o Incidente e antecipar, prevenir e melhor identificar Incidentes semelhantes no futuro;
- Realizar, imediatamente, treinamento interno com as áreas afetadas para conscientizar os colaboradores e demais envolvidos sobre o Incidente e medidas preventivas;
- Considerar e planejar medidas de resposta e indenização em face dos titulares afetados.

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 Controlador, em conjunto com o Encarregado.

Caso um incidente seja identificado como relevante, o Encarregado deverá 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 serventia, 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, observados os segredos comercial e industrial;
- 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 as que serão adotadas para reverter ou mitigar os efeitos do incidente;
- os danos causados aos titulares, quando forem mensuráveis.

Caso seja avaliado que o incidente deverá ser comunicado aos titulares dos dados pessoais afetados, caberá ao Encarregado desenvolver a mensagem da comunicação, priorizando (i) os fatos ocorridos; (ii) as medidas já tomadas 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. Dúvidas e informações adicionais

Para tratar de assuntos relacionados à proteção e tratamento de dados pessoais, o titular deve se dirigir, preferencialmente, ao canal dedicado disponibilizado pela serventia, no endereço oritdpjnovohorizonte.com.br.

Alternativamente, poderá entrar em contato com o encarregado de proteção de dados pessoais (DPO), por meio dos meios a seguir:

Dr. Henrique Almeida Bazan Castanheira
OAB/MG 215.984
henrique@bqadvocacia.com

Por fim, também serão recebidas notificações e solicitações por outros canais, como e-mail, correio ou presencialmente. Contudo, note que a escolha desses canais poderá retardar a análise do caso.

7. Alterações e atualizações

Em linha com o objetivo de constante aprimoramento dos serviços prestados, a presente política pode ser atualizada a qualquer tempo. Em caso de alterações, a versão atualizada da política será disponibilizada no mesmo ambiente, e com a mesma publicidade, da versão anterior. As versões anteriores permanecerão disponíveis para consulta, quando necessário. As políticas deverão indicar o início de sua vigência e a data de sua aprovação.

A presente política foi visada e aprovada em 01/12/2025, com vigência a partir de 01/12/2025, devendo ser disponibilizada ao público no primeiro dia útil subsequente Novo Horizonte, 1º de dezembro de 2025.

Henrique Almeida Bazan Castanheira
Encarregado

Henrique Rabelo Quirino
Controlador