PLANO DE RESPOSTAS A INCIDENTES DE SEGURANÇA E PRIVACIDADE

1. Introdução

O presente documento estabelece o Plano de Resposta a Incidentes de Segurança e Privacidade de Dados para o Instituto de Previdência Social dos Servidores Públicos do Município de Joinville – Ipreville. Sua elaboração é uma resposta direta à exigência contida no *art. 47, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD)*, que impõe aos agentes de tratamento de dados pessoais a adoção de medidas de segurança, tanto técnicas quanto administrativas, para proteger os dados pessoais contra acessos não autorizados, bem como contra situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Este plano visa garantir uma atuação organizada, eficiente e em conformidade com a legislação vigente, orientando as ações a serem adotadas pelo Ipreville em caso de ocorrência ou suspeita de incidentes relacionados à segurança ou à privacidade de dados pessoais sob sua tutela ou custódia.

Natureza do Documento: Sigiloso – O acesso a este Plano de Resposta é restrito às pessoas diretamente envolvidas em sua execução e gestão, garantindo a proteção das informações e estratégias contidas para a defesa contra ameaças à segurança da informação.

2. Objetivos do Plano

São objetivos deste Plano de Resposta a Incidentes:

a) Orientar Ações: Fornecer um guia claro e prático para as ações a serem tomadas em caso de incidentes de segurança e privacidade de dados;
b) Minimizar Impactos: Reduzir o impacto, a duração e os custos associados a incidentes, por meio de uma resposta rápida e eficaz;

c) Garantir Conformidade: Assegurar a conformidade do Ipreville com as obrigações legais e regulatórias, especialmente a LGPD, no que tange à proteção de dados pessoais;
d) Proteger Direitos dos Titulares: Salvaguardar os direitos e liberdades dos titulares de dados pessoais, mitigando riscos e danos potenciais decorrentes de incidentes;
e) Preservar Evidências: Manter a integridade de evidências forenses para análise pós-incidente, visando prevenir futuras ocorrências e subsidiar ações legais, se necessário;
f) Fomentar a Melhoria Contínua: Promover a análise e o aprendizado com cada incidente, buscando aprimorar continuamente as políticas, procedimentos e controles de segurança da informação do Ipreville.

3. Definições Importantes

Para os fins deste plano, considera-se:

a) Incidente de Segurança com Dados Pessoais: Qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de dados pessoais, como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou qualquer forma de tratamento inadequado ou ilícito, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais;
b) Dados Pessoais: Informações relacionadas a pessoa natural identificada ou identificável;
c) Tratamento de Dados: 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;
d) PSTI: Política de Segurança da Tecnologia da Informação do Ipreville;

e) RD – Relatório de Descumprimento: Documento formal para registro de possíveis descumprimentos à PSTI.

4. Atores e Responsabilidades no Plano de Resposta

A resposta a incidentes é um esforço multidisciplinar que envolve diversos atores e o engajamento de várias áreas do Ipreville.

4.1. Comitê Gestor de Proteção de Dados e Segurança da Informação (CGPD)

O Comitê Gestor de Proteção de Dados e Segurança da Informação (CGPD) do Ipreville, instituído pela Resolução do Conselho nº 28772368/2026, é o organismo deliberativo central e a principal instância consultiva e de apoio à presidência do Ipreville, para a gestão de incidentes de segurança e privacidade de dados no âmbito do Ipreville.

É importante que, em caso de impedimento, os membros do CGPD deleguem um servidor de suas respectivas áreas para substituí-los, garantindo a continuidade do trabalho.

Competências do CGPD no contexto de Resposta a Incidentes:

a) Analisar possíveis descumprimentos das políticas relacionadas à proteção e à privacidade de dados pessoais e dados sensíveis, registrados por Relatório de Descumprimento (RD) e propondo ações corretivas e/ou sanções;
b) Dar suporte para às iniciativas do setor de Tecnologia da Informação do Ipreville, relacionadas à segurança e proteção de dados;
c) Avaliar e aprimorar a Política de Segurança da Tecnologia da Informação do Ipreville, a análise das ocorrências registradas através dos RD's e as ações adotadas para sua correção e/ou sanção (conforme Art. 2º, VIII da Resolução que institui o CGPD).

O CGPD será presidido pelo membro eleito entre os titulares, para a função de Presidente. As convocações para o desenvolvimento dos trabalhos do Comitê, especialmente em casos de incidentes de segurança, serão de responsabilidade do

Presidente do Comitê ou do Encarregado de Proteção de Dados (DPO), conforme as atribuições estabelecidas na Resolução do Conselho nº 28772368/2026.

4.2. Encarregado pelo Tratamento de Dados Pessoais (DPO)

O DPO é um membro especial do CGPD e possui um papel vital na gestão de incidentes, especialmente aqueles que envolvem vazamento de dados pessoais.

Suas responsabilidades devem incluir:

a) Comunicações Formais: Encaminhar comunicações formais à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares dos dados afetados, conforme exigido pela LGPD;
b) Dossiê do Incidente: Elaborar um dossiê detalhado com a avaliação interna do incidente, as medidas tomadas e a análise de risco, para fins de cumprimento do princípio de responsabilização e prestação de contas (Art. 6º, X da LGPD);
c) Avaliação de Dano: Avaliar o nível de dano que um incidente pode ter causado aos titulares de dados pessoais.

4.3. Setor de Tecnologia da Informação (TI)

O Setor de TI, que terá assento no comitê, é fundamental na preparação e resposta técnica aos incidentes e suas atribuições devem incluir:

a) Preparação: Manter mecanismos automatizados de monitoramento (antivírus, firewalls) e implementar o Plano de Continuidade de Negócio dos sistemas;
b) Suporte Técnico: Fornecer o suporte técnico necessário nas fases de avaliação, contenção, erradicação e recuperação, incluindo restauração de backups e reinstalação de sistemas;
c) Desenvolvedores/Operadores/Fornecedores: Atuam no desenvolvimento de soluções tecnológicas, fornecimento, instalação e manutenção dos sistemas lógicos e softwares utilizados pelo Ipreville, sendo acionados pela TI conforme a necessidade do incidente.

4.4. Colaboradores do Ipreville

Todos os colaboradores do Ipreville têm um papel crucial na detecção e reporte inicial de incidentes. A conscientização e sensibilização são essenciais para que eventuais incidentes identificados por agentes internos cheguem ao conhecimento do CGPD (e do DPO).

5. Preparação Prévia para a Resposta a Incidentes

A eficácia da resposta a incidentes depende significativamente da preparação prévia, que envolve:

a) Plano de Continuidade de Negócio (PCN): O setor de TI deve manter um PCN dos sistemas utilizados pelo Ipreville, com medidas mitigadoras pré-definidas para conter ou solucionar situações de emergência;

b) Ferramentas de Monitoramento e Alarmes: Instalação e configuração de mecanismos automatizados de monitoramento e identificação de incidentes, como antivírus, firewalls e sistemas de detecção de intrusão, em todos os terminais de processamento de dados pessoais. É fundamental que, tão logo um incidente seja identificado por essas ferramentas, o CGPD seja informado através de mecanismos de comunicação direta e eficazes (e-mail, WhatsApp, SMS, etc.);

c) Mecanismos de Comunicação: Criação, disponibilização e publicação das formas de notificação à Agência Nacional de Proteção de Dados (ANPD), incluindo o e-mail de contato do Encarregado (DPO) publicamente no site do Ipreville, para que os titulares possam comunicar eventuais incidentes;

d) Modelos de Documentos (Templates): Preparação prévia de uma biblioteca com modelos de documentos para comunicação formal do DPO com a ANPD, titulares de dados, órgãos fiscalizadores e imprensa;

6. Procedimento de Reporte e Gestão de Incidentes

Este é o procedimento detalhado para o reporte e gestão de incidentes de segurança e vazamento de dados no Ipreville, integrando as funções do CGPD.

6.1. Detecção e Reporte Inicial do Incidente

Um incidente pode ser detectado por diversas fontes, sejam elas internas (colaboradores, auditorias internas, sistemas de monitoramento) ou externas (titulares de dados, parceiros, órgãos reguladores).

6.1.1. Como Reportar um Incidente ao CGPD:

Para garantir um processo claro e específico, o Ipreville estabelece o seguinte fluxo para o reporte de incidentes.

6.1.1.1. Identificação: Qualquer colaborador do Ipreville que identifique ou suspeite de um incidente de segurança ou privacidade de dados pessoais (ex: acesso não autorizado a arquivos, e-mail com anexo suspeito, perda de dispositivo contendo dados, alteração indevida de informações, erro de sistema que expõe dados, etc.) deve agir imediatamente.

6.1.1.2. Notificação Imediata: O incidente deve ser comunicado o mais rápido possível através de algum dos seguintes canais prioritários:

a) Canal Principal (DPO): Em casos de suspeita de vazamento de dados pessoais ou violação de privacidade, deve ser notificado diretamente ao Encarregado de Dados (DPO) através de seu contato institucional, já que ele é o responsável pelas comunicações formais;
b) Canal Secundário (TI): Através de um e-mail dedicado ou sistema de abertura de chamado para o setor de Tecnologia da Informação (TI). Este canal deve ser divulgado internamente para todos os colaboradores.

6.1.1.3. Informações Essenciais no Reporte: A notificação inicial deve conter, no mínimo, as seguintes informações para auxiliar na triagem:

a) Nome e contato do reportante;

b) Data e hora da detecção do incidente;
c) Breve descrição do ocorrido (o que aconteceu?);
d) Localização ou sistema afetado (onde ocorreu?);
e) Impacto percebido (o que foi afetado, se dados pessoais, quais?);
f) Quaisquer evidências disponíveis (capturas de tela, mensagens de erro, etc.).

6.1.1.4. Registro Formal – Relatório de Descumprimento (RD): Após a notificação inicial, o DPO será responsável por formalizar o reporte através do preenchimento de um Relatório de Descumprimento (RD) com apoio do CGPD.

6.2. Ativação do Plano e Ações do CGPD

Assim que um incidente é notificado, seja por pessoa interna ou externa ao Ipreville, ou por alarme de monitoramento, a notificação é recebida pelo CGPD por meio do Presidente ou DPO. O plano de resposta é então ativado, e as seguintes fases são executadas sob a coordenação do CGPD:

6.2.1. Triagem (Fase 1)

Os integrantes do CGPD devem realizar uma avaliação preliminar da notificação.

6.2.1.1. Objetivo: Determinar a validade e a gravidade inicial do incidente.

6.2.1.2. Ações:

a) Arquivar notificações nulas ou claramente improcedentes, com cautela para não descartar denúncias legítimas.

6.2.1.3. Buscar informações sobre:

a) O contexto da atividade de tratamento de dados envolvida;
b) Os sistemas alegadamente impactados;
c) Se os dados violados estavam protegidos (ex: criptografados) de forma a impossibilitar a identificação dos titulares;
d) A quantidade, volume e tipo de dados pessoais potencialmente atingidos;

e) Identificação dos titulares ou conjunto de titulares atingidos ou potencialmente atingidos;
f) Consequências imediatas identificadas ou potenciais danos (materiais, morais ou reputacionais) aos titulares (Dados sensíveis, dados de grupos vulneráveis; exposição a situações de discriminação ou roubo de identidade);
g) Medidas de mitigação já adotadas.

6.2.1.4. Decisão: Incidentes de baixa gravidade, que não envolvam sistemas online e que seguramente não apresentam riscos aumentados pela falta de ação imediata, podem ser encaminhados para trâmites regulares. Casos que exigem resposta imediata ou melhor avaliação, avançam para as fases seguintes.

6.2.2. Avaliação (Fase 2)

Nesta fase, o CGPD inicia uma avaliação mais detalhada do incidente.

6.2.2.1. Objetivo: Identificar a causa raiz, a extensão do incidente e as vulnerabilidades exploradas.

6.2.2.2. Ações:

a) Identificar a causa do incidente, endereços IP e credenciais envolvidas, transações e transferências de dados irregulares;
b) Determinar os métodos e vulnerabilidades exploradas;
c) Engajar especialistas dos sistemas afetados, a critério do CGPD, para colaborar na investigação.

6.2.3. Contenção e Erradicação (Fase 3)

Esta fase visa limitar o dano e isolar os sistemas afetados.

6.2.3.1. Objetivo: Evitar que o incidente se espalhe e remover a causa raiz.

6.2.3.2. Ações:

a) O CGPD notifica os responsáveis pelos sistemas impactados para que se manifestem, em prazo máximo de 24 horas, prestando informações e orientações adequadas à contenção, erradicação ou mitigação dos danos;

b) Realizar o desligamento do sistema (ou dos sistemas) ou de funcionalidades específicas, se necessário e autorizado;
c) Colocar avisos de indisponibilidade para manutenção, quando aplicável;
d) Tomar cuidados para não impactar evidências forenses que possam ser usadas para identificar autoria, origem e método do ataque;
e) Em caso de máquinas virtuais, fazer snapshot para posterior análise.

6.2.4. Recuperação (Fase 4)

Após a contenção, inicia-se a recuperação dos serviços.

6.2.4.1. Objetivo: Restaurar os serviços à sua normalidade de forma segura.

6.2.4.2. Ações:

a) Ativar o Plano de Continuidade de Negócio dos sistemas impactados, se existente;
b) Restaurar serviços gradualmente, conforme viabilidade e decisão do responsável pelo sistema;
c) Repassar, através do CGPD, as informações obtidas para o desenvolvimento da solução e sua instalação;
d) Tomar medidas identificadas na Avaliação, como restauração de backups, clonagem de máquinas virtuais, reinstalação de sistemas;
e) Avaliar a necessidade de desenvolvimento e instalação de atualizações de aplicações, antivírus, firewall ou Sistema Operacional.

6.2.5. Processo de Melhoria Contínua (Fase 5)

Um incidente é uma oportunidade de aprendizado e aprimoramento.

6.2.5.1. Objetivo: Levantar oportunidades de melhoria na resposta dada ao incidente, bem como para mitigação ou eliminação de riscos.

6.2.5.2. Ações:

a) Após a contenção e encaminhamento da resolução, o CGPD deve se reunir, podendo incluir convidados;
b) Discutir erros e dificuldades encontradas durante a resposta;
c) Propor melhorias para os sistemas, processos e, inclusive, para este Plano de Resposta a Incidentes;
d) As melhorias sugeridas e aprovadas devem ser encaminhadas aos responsáveis para definição sobre a adoção.

6.2.6. Formalização das Ações Adotadas (Fase 6)

A documentação é essencial para a responsabilização e prestação de contas.

6.2.6.1. Objetivo: Registrar o histórico completo do incidente e as ações tomadas.

6.2.6.2. Ações:

a) O CGPD deve documentar o incidente tecnicamente, relatando e detalhando as informações obtidas, linha do tempo, atores envolvidos, evidências, conclusões, decisões, autorizações e ações tomadas, incluindo atas das reuniões do CGPD;
b) O DPO deve elaborar um dossiê contendo documentação com a avaliação interna do incidente, medidas tomadas e análise de risco, para cumprimento do princípio de responsabilização e prestação de contas (Art. 6º, X da LGPD).

6.2.7. Comunicações (Fase 7)

As comunicações transparentes são um pilar da gestão de incidentes, especialmente quando há vazamento de dados pessoais.

6.2.7.1. Comunicação ao Titular de Dados: Quando o DPO identificar a ocorrência de dano ou risco relevante ao titular, a comunicação é obrigatória:

a) Assim que possível, se o incidente causar dano ou risco relevante ao titular;
b) O conteúdo da comunicação deve conter, no mínimo:
    a. Resumo e data da ocorrência do incidente;
    b. Descrição dos dados pessoais afetados;
    c. Riscos e consequências aos titulares de dados;

d. Medidas tomadas pelo Ipreville e as recomendadas aos titulares para mitigar os efeitos do incidente, se cabíveis;
e. Dados de contato do Encarregado (DPO) para que os titulares possam solicitar informações adicionais.

c) Forma: Preferencialmente individual e direta (e-mail, SMS, carta ou mensagem eletrônica). Se não for possível identificar os titulares afetados, a comunicação deve ser feita a todos, cujos dados constam na base. Excepcionalmente, pode ser feita de forma indireta por meios adequados, devendo alcançar o maior número de titulares possível.

6.2.7.2 Comunicação para ANPD: É uma obrigação legal em casos de incidentes com vazamento de dados pessoais e deverá:

a) Ocorrer tão logo possível, na hipótese de dano ou risco relevante;
b) Ser comunicada através do sítio eletrônico da ANPD: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca;
c) Considerar informações obrigatórias, **c**onforme regulamentação atualizada da ANPD;
d) Em caso de não dispor de todas as informações, uma comunicação preliminar justificada poderá ser enviada, a ser complementada no prazo máximo de 30 dias;
e) Caso a ANPD exija, após avaliar a gravidade do incidente, deverá ser dada ampla divulgação do fato em meios de comunicação. O CGPD, em conjunto com o DPO e o setor de Comunicação, definirá o modo de publicação para mitigar impactos negativos, mas garantindo o cumprimento da determinação da ANPD.

7. Conformidade e Transparência

Este plano é um compromisso do Ipreville com a transparência e a conformidade regulatória. As comunicações e demais medidas adotadas são consideradas demonstrações de boa-fé e cooperação, e serão levadas em consideração em eventual ação fiscalizadora pela ANPD. A proatividade na gestão de incidentes reforça a postura responsável do Ipreville perante a proteção de dados.

8. Revisão e Aprimoramento Contínuo

O CGPD é responsável por garantir que este Plano de Resposta a Incidentes seja um documento vivo, sujeito a revisões e atualizações periódicas. Alterações poderão ser propostas e aprovadas pelos membros do CGPD, com base nas lições aprendidas em incidentes reais, na evolução das ameaças cibernéticas e nas mudanças regulatórias. Reuniões periódicas do CGPD terão como objetivo a avaliação e o aprimoramento da PSTI e, consequentemente, deste plano.