🛡️ PROTOCOLO DE RESPOSTA A INCIDENTES DE SEGURANÇA (PRI)

(Vazamento de Dados Pessoais - Conforme a Lei Geral de Proteção de Dados - LGPD)

Empresa: [NOME DA SUA EMPRESA/RAZÃO SOCIAL]

Versão: [1.1] (Revisado com base na Política Interna)

Data de Emissão: 08 de Novembro de 2025

Responsável: Encarregado de Dados (DPO)

I. ACIONAMENTO E COMITÊ DE CRISE

Este protocolo é acionado imediatamente após a detecção ou suspeita de um Incidente de Segurança (como vazamento, acesso indevido ou perda de dados - **Item 9 da sua Política**).

A. Membros do Comitê de Resposta a Incidentes (CRI)

Função	Nome / Departamento	Contato (Telefone /E-mail)	Responsabilidade Principal
Liderança Sênior/CEO	[Nome]	[Contato]	Tomada de Decisão Estratégica e Alocação de Recursos
Encarregado de Dados (DPO)	[Nome]	**[dpo@seudominio.com]**	Coordenador do PRI, Assegurar a Conformidade e Comunicação com ANPD e Titulares.
Segurança da Informação/ TI	[Nome]	[Contato]	Contenção Técnica, Investigação Forense e Remediação. **(Implementar controles técnicos - Item 10)**
Jurídico/ Compliance	[Nome]	[Contato]	Análise de Risco, Conformidade Legal e Suporte em Litígios.

Comunicação /Marketing	[Nome]	[Contato]	Comunicação Externa, Relações Públicas e Mídia.

II. FASES DE RESPOSTA AO INCIDENTE

FASE 1: Detecção e Contenção Imediata

Objetivo: Interromper o incidente, limitar o dano e preservar as evidências.

- **1.1. Verificação e Registro (Item 9 da Política):** Confirmar a ocorrência e registrar imediatamente o evento, que será analisado pela equipe de segurança.
- **1.2. Isolamento:** A equipe de TI/Segurança deve isolar ou desconectar o sistema/rede comprometido da rede principal. **NÃO DESLIGAR** equipamentos afetados.
- **1.3. Preservação de Evidências:** Iniciar a criação de cópias forenses (imagens de disco, logs) dos sistemas afetados, garantindo a cadeia de custódia das provas.
- **1.4. Controles de Acesso (Item 8 da Política):** Trocar imediatamente todas as credenciais de acesso (senhas, chaves API, tokens) que possam ter sido expostas. Reforçar a **Autenticação Multifator** para acessos administrativos.

FASE 2: Avaliação e Análise de Risco (DPO e Jurídico)

Objetivo: Determinar a causa, a extensão do dano e o grau de risco aos titulares para fins de *accountability*.

- **2.1. Análise da Causa Raiz:** A equipe de TI deve identificar a **vulnerabilidade** explorada e o **vetor de ataque**.
- **2.2. Determinação do Escopo:**
  - **Quais dados foram afetados?** (Ex: Dados Sensíveis, Dados Financeiros, Dados de Autenticação, etc.).
  - **Qual o volume/número de titulares afetados?**
- **2.3. Avaliação de Risco e Dano Relevante (LGPD Art. 48):** O Jurídico e o DPO avaliarão, com base no Art. 48 da LGPD, se o incidente pode acarretar **risco ou dano relevante** aos titulares.
- **2.4. Documentação (*Accountability*):** Registrar em relatório (Relatório de Impacto de Incidente) toda a linha do tempo, as descobertas da investigação e a justificativa para a classificação de risco, para comprovação de conformidade e boas práticas **(Item 3 da sua Política)**.

FASE 3: Notificação Legal e Comunicação Externa

Objetivo: Cumprir as obrigações legais de comunicação à ANPD e aos titulares, garantindo a Transparência **(Item 3 da sua Política)**.

- **3.1. Comunicação à ANPD (LGPD Art. 48 - Responsável: DPO):**
  - O DPO deve comunicar a ocorrência à Autoridade Nacional de Proteção de Dados (ANPD) em **prazo de 3 (três) dias úteis**, a contar da data de conhecimento, se houver risco ou dano relevante.
  - A comunicação será realizada através do formulário oficial da ANPD e deverá conter as informações mínimas detalhadas no **ANEXO I** deste protocolo.
- **3.2. Comunicação aos Titulares (LGPD Art. 48 - Responsável: DPO e Comunicação):**
  - Comunicar os titulares afetados em linguagem **clara, simples e concisa**.
  - A comunicação deve incluir as **medidas que o titular deve tomar para se proteger de danos** (ex: troca de senhas, monitoramento de extratos bancários).
  - Disponibilizar o contato do DPO **([dpo@seudominio.com])** como ponto de contato para que os titulares possam exercer seus direitos (LGPD Art. 41).

FASE 4: Remediação e Aprimoramento

Objetivo: Restaurar a operação, reforçar a segurança e comprovar a conformidade (Responsabilização - **Item 3 da sua Política**).

- **4.1. Remediação Técnica:** Corrigir a causa raiz (vulnerabilidade) e reestabelecer os sistemas de forma segura.
- **4.2. Fortalecimento de Segurança (Item 8 da Política):** Reforçar os controles de segurança adotando novas medidas administrativas e técnicas, como: **Segmentação de redes** e otimização da **Criptografia** de dados sensíveis (em trânsito e em repouso).
- **4.3. Treinamento e Revisão (Item 8 e 11 da Política):** O DPO deve garantir que o **Treinamento Periódico em Segurança da Informação e LGPD** seja reforçado, focando no vetor de ataque que causou o incidente.
- **4.4. Plano de Continuidade (Item 8 da Política):** Colocar o **Plano de Continuidade de Negócios (PCN)** e de **Backup** em prática para garantir o retorno à normalidade.

- **4.5. Registro e Revisão (Item 9 e 11 da Política):** Manter o registro detalhado do incidente por **pelo menos 5 anos** e realizar a **Revisão e Atualização** deste Protocolo imediatamente após a conclusão do caso.

ANEXO I: Informações Mínimas para Comunicação à ANPD

(Conforme Art. 48, §1º da LGPD e regulamentação da ANPD)

A comunicação será conduzida pelo DPO e deve incluir, no mínimo, os seguintes elementos:

1. **Descrição da Natureza dos Dados Pessoais Afetados:** Detalhar as categorias de dados (ex: CPF, dados de geolocalização, dados de saúde).
2. **Informações sobre os Titulares Envolvidos:** O número de titulares afetados (e, se possível, a distinção entre adultos e menores/idosos).
3. **Indicação das Medidas Técnicas e de Segurança Utilizadas:** Detalhar as medidas que a empresa *já possuía* e as *adotadas após o incidente*.
4. **Riscos Relacionados ao Incidente:** Os impactos prováveis (ex: chance de roubo de identidade, fraudes financeiras).
5. **Motivos da Demora na Comunicação:** Justificativa detalhada se o prazo de 3 dias úteis for ultrapassado.
6. **Medidas que Foram ou Serão Adotadas para Reverter ou Mitigar o Prejuízo.**
7. **Forma e o Conteúdo da Comunicação** aos titulares.
8. **Solicitação de Sigilo:** O Controlador poderá solicitar o sigilo de informações estratégicas (ex: segredos comercial ou industrial), desde que devidamente fundamentado.