PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA (PRI)

v1

INTRODUÇÃO

Este Plano de Resposta a Incidentes (PRI) define os procedimentos para a gestão de situações após a identificação ou suspeita de um incidente de segurança da informação que envolva dados pessoais identificados ou identificáveis tratados pela Equipo Info Serviços De Tecnologia Da Informação Ltda.

O objetivo é combater os riscos e minimizar os efeitos de tais incidentes.

O PRI foi elaborado em conformidade com a Lei 13.709/18 (Lei Geral de Proteção de Dados Pessoais).

OBJETIVO

Este Plano de Resposta a Incidentes (PRI) tem como objetivo definir as funções e responsabilidades das equipes da empresa, bem como as medidas a serem adotadas para que a empresa responda adequadamente a um incidente. O foco é sempre manter a integridade dos sistemas e proteger todas as informações que possam identificar, direta ou indiretamente, uma pessoa física (“Dados Pessoais”), garantindo a privacidade dos titulares. Isso permite à empresa manter a confiabilidade de suas marcas, produtos e serviços.

Este PRI aplica-se a qualquer incidente envolvendo Dados Pessoais e deve ser seguido, em conjunto com as demais políticas da Empresa, por todas as áreas e colaboradores, incluindo sócios, diretores, administradores, empregados e determinados prestadores de serviços e parceiros que, no âmbito de suas relações com a empresa, possam ter acesso a áreas, equipamentos, informações, redes e dados de propriedade da Empresa.

Como objetivos específicos, destacam-se:

• comunicar incidentes à ANPD sempre que necessário, evitando comunicações paralelas com a Autoridade;

• primar pela adequada comunicação com os titulares, quando necessário;

• criar um fluxo de tratamento eficaz de incidentes que envolvam dados pessoais;

• manter atualizado o registro dos incidentes comunicados ao encarregado;

• possibilitar que lições aprendidas com o tratamento de incidentes gerem subsídios para o aprimoramento deste Plano.

DEFINIÇÕES GERAIS

Para auxílio na leitura desse guia, serão adotadas as seguintes definições, que em sua maioria foram extraídas do Glossário do GSI (Portaria GSI/PR nº 93, de 18 de outubro de 2021) e de publicações e resoluções da ANPD, no que se refere a incidentes ocorridos na empresa.

AGENTES DE TRATAMENTO: de acordo com a LGPD, são agentes de tratamento:

• **CONTROLADOR:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

• **OPERADOR:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

A depender do contexto, uma mesma operação de tratamento de dados pessoais pode envolver mais de um operador ou controlador (controladoria conjunta, ou co-controladores).

INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

Um incidente de segurança da informação envolvendo dados pessoais é qualquer evento adverso que resulte na violação da segurança desses dados. Isso pode incluir acesso não autorizado, acidental ou ilícito, que leve à destruição, perda, alteração, vazamento ou qualquer forma de tratamento inadequado ou ilícito dos dados pessoais. Esses incidentes podem representar riscos significativos para os direitos e liberdades dos titulares dos dados.

Um Incidente pode ocorrer de forma maliciosa, ser resultado de erro humano ou até mesmo de falhas nos sistemas que processam Dados Pessoais ou em seus mecanismos de segurança. Exemplos incluem o furto de documentos, envio de e-mails contendo Dados Pessoais para destinatários não autorizados, tentativas de invasão aos sistemas da Empresa, entre outras ações, culposas ou dolosas.

Os Incidentes podem ser classificados em diversos tipos, como por exemplo:

1. 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;

2. 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;

3. 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;

4. Uso Inapropriado: É o Incidente no qual há a violação das políticas de uso de dados, informações e sistemas da Empresa, incluindo a Política de Privacidade e de Segurança da Informação.

Em caso de incidente que coloque em risco a segurança de dados pessoais, devem ser realizados alguns procedimentos específicos. São eles:

- Avaliar internamente o incidente com o objetivo de obter informações iniciais sobre impacto do evento; natureza, categoria e quantidade de titulares de dados pessoais afetados; consequências do incidente para os titulares e a entidade, criticidade e probabilidade; além disso, é necessário preservar todas as evidências do incidente.

- Comunicar ao encarregado da entidade a existência do incidente, caso envolva dados pessoais.

- Comunicar ao controlador (nos termos da LGPD) a existência do incidente, caso envolva dados pessoais.

- Comunicar à ANPD e ao titular de dados pessoais (conforme art. 48 da LGPD e art. 17 da Resolução CD/ANPD Nº 15/2024) a existência do incidente.

- Elaborar relatório interno detalhando o incidente, as medidas tomadas e as recomendações para evitar futuros incidentes.

- Após a resolução do incidente, revisar as políticas e procedimentos de segurança para identificar melhorias e prevenir futuros incidente.

PAPÉIS E RESPONSABILIDADES

Todas as áreas da Empresa, independentemente de estarem diretamente envolvidas na governança, têm responsabilidades em caso de ocorrência ou suspeita de um Incidente.

Obrigações de Todas as Áreas

- comunicar imediatamente a Equipe de Resposta sobre a ocorrência ou a mera suspeita de um Incidente;

- cumprir rigorosamente a Política de Segurança da Informação da Empresa, contribuindo para a mitigação de riscos;

1.1 Obrigações de Outras Áreas

As obrigações de outras áreas da empresa em caso de um incidente de segurança podem variar, mas geralmente incluem:

Comitê de Proteção de Dados: Todas as áreas devem reportar imediatamente qualquer suspeita ou ocorrência de incidente de segurança à equipe de TI ou ao responsável pela segurança da informação;

Tecnologia e Sistemas da Informação: Auxilia na resolução das questões técnicas relacionadas ao Incidente e na investigação da origem e das razões para ocorrência do Incidente;

Jurídico: Avalia a situação decorrente do Incidente e toma as medidas apropriadas quanto aos impactos jurídicos à Empresa ou a Colaboradores, clientes, parceiros comerciais ou titulares dos Dados Pessoais afetados;

Relações Públicas: Coordena as comunicações entre a Empresa e seus colaboradores, parceiros comerciais estratégicos, principais clientes, bem como o público em geral para mitigar eventuais riscos reputacionais e assegurar a continuidade dos negócios;

Atendimento ao Consumidor: Coordena a comunicação da Empresa com os seus clientes sobre o Incidente, incluindo o esclarecimento sobre o ocorrido e as ações tomadas para mitigar os efeitos e prevenir novos Incidentes semelhantes no futuro, sempre de acordo com as orientações das demais áreas; e

Compliance: Investiga as origens e as razões da ocorrência do Incidente, bem como avalia, junto aos gestores das áreas, a necessidade da aplicação de medidas disciplinares aos Colaboradores cujas condutas foram culposas ou intencionais na ocorrência de um Incidente.

DETECÇÃO DO INCIDENTE

A detecção rápida e eficiente de um Incidente é crucial para uma resolução bem-sucedida. Existem diversas formas de detecção, tornando inviável a criação de uma metodologia que abranja todas. Portanto, todos os Colaboradores devem estar atentos aos sinais mais comuns que podem indicar um Incidente, como invasões de rede, perda ou furto de documentos, arquivos ou dispositivos, e instabilidades sistêmicas.

Uma vez detectado um Incidente ou detectada a mera suspeita de um Incidente, o Colaborador deverá comunicar imediatamente a Equipe de Resposta a Incidentes, por meio do e-mail **suporte.dpo@eqpcm.com** e mantendo o seu supervisor sempre em cópia.

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 qualquer informação adicional que sirva para facilitar o entendimento do evento, suas causas e consequências.

PRIORIZAÇÃO DO INCIDENTE E PROCEDIMENTOS PARA RESPOSTA

A priorização de um incidente envolve avaliar a gravidade e o impacto potencial do incidente para determinar a ordem em que ele deve ser tratado. Isso geralmente inclui:

1. **Avaliação da Gravidade**: Determinar a extensão do dano ou potencial dano causado pelo incidente. Incidentes que comprometem dados sensíveis ou afetam muitos usuários são geralmente considerados de alta gravidade.

2. **Impacto no Negócio**: Avaliar como o incidente afeta as operações da empresa. Incidentes que interrompem serviços críticos ou causam perda financeira significativa são priorizados mais alto.

3. **Urgência**: Considerar a rapidez com que o incidente precisa ser resolvido para minimizar danos adicionais. Incidentes que estão em andamento ou que podem se agravar rapidamente são tratados com maior urgência.

O impacto do Incidente deve ser aferido da seguinte forma:

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
		sensibilidade dos Dados Pessoais afetados		

Volume de Dados Pessoais expostos	
Criticidade	**Descrição**
Alto	Volume de Dados Pessoais afetado superior a 10% da base de dados da Controladora.
Médio	Volume de Dados Pessoais afetado inferior a 10% e superior a 2% da base de dados da Controladora.
Baixo	Volume de Dados Pessoais afetado inferior a 2% da base de dados da Controladora.

Sensibilidade dos Dados Pessoais afetados	
Criticidade	**Descrição**
Alta	Dados Pessoais Sensíveis ou que possam gerar discriminação ao titular.
Média	Dados Pessoais imediatamente identificáveis (Ex.: nome, e-mail, CPF, endereço)
Baixa	Dados anonimizados, Dados Pessoais pseudonimizados (desde que a chave de desanonimização não tenha sido comprometida) e Dados Pessoais de difícil identificação (como IP

De acordo com a matriz acima definida, a Equipe de Resposta a Incidentes deverá tomar as seguintes ações, simultaneamente ou, quando não for possível, em rápida sucessão:

Baixa Gravidade

1. tão logo tenha ciência, trabalhar prioritariamente na resolução do Incidente;

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

3. comunicar o Comitê de Proteção de Dados;

4. comunicar as Áreas Envolvidas, que deverão estar à disposição da Equipe de Resposta;

5. uma vez que as medidas de resolução sejam tomadas, documentar o Incidente

Média Gravidade

1. tão logo tenha ciência, trabalhar de forma exclusiva na resolução do Incidente; 2. 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;

3. comunicar o Comitê de Proteção de Dados;

4. comunicar as Áreas Envolvidas, que deverão estar à disposição para atender, com prioridade, a Equipe de Resposta;

5. uma vez que as medidas de resolução sejam tomadas, documentar o Incidente, o mais breve possível;

6. 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 Comitê de Proteção de Dados; e

7. realizar, imediatamente, treinamento interno com as áreas afetadas para conscientizar os seus Colaboradores sobre o Incidente e medidas preventivas.

Alta Gravidade

1. tão logo tenha ciência, trabalhar de forma exclusiva na resolução do Incidente; 2. imediatamente comunicar os diretores 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 à Equipe de Resposta e preferencialmente no mesmo local em que a Equipe de Resposta esteja trabalhando;

3. uma vez que as medidas de resolução sejam tomadas, documentar o Incidente,

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 Comitê de Proteção de Dados;

4. realizar, imediatamente, treinamento interno com todos os Colaboradores da Empresa para conscientizar sobre o Incidente e medidas preventivas;
5. comunicar, imediatamente, os Colaboradores internos sobre medidas preventivas.

Se o Comitê de Proteção de Dados decidir comunicar o Incidente aos titulares dos Dados Pessoais afetados, a área de Relações Públicas, com o suporte do Jurídico, Atendimento ao Consumidor e da Equipe de Resposta, desenvolverá a mensagem de comunicação. Esta mensagem deve priorizar: (i) os fatos ocorridos; (ii) as medidas já tomadas pela Empresa para minimizar o impacto; (iii) as ações que os próprios titulares dos Dados Pessoais podem tomar para mitigar riscos; e (iv) os canais de contato para esclarecer dúvidas.

DISPOSIÇÕES FINAIS

A resposta a incidentes de segurança é um processo crítico que exige preparação, coordenação e comunicação eficazes. Cada área da empresa tem um papel importante a desempenhar, desde a detecção inicial até a recuperação e análise pós-incidente. A priorização adequada e a implementação de procedimentos estruturados garantem que os impactos sejam minimizados e que a empresa possa aprender e melhorar continuamente suas práticas de segurança.