PLANO DE RESPOSTA A INCIDENTES

PARTES ENVOLVIDAS:

• Notificador – pessoa física ou sistema de monitoração que comunica incidente.

• TRI – Time/equipe de Resposta a Incidentes. É composto por três componentes, um deles, necessariamente, será o Encarregado pelo Tratamento de Dados Pessoais (DPO) e outro deverá fazer parte da Equipe de Segurança da Informação. Todos terão ciência de suas responsabilidades, treinamento e conhecimentos para responder aos mais variados tipos de incidentes. O TRI tem reuniões periódicas para definir melhorias e estratégias.

• Equipe de Segurança da Informação.

• Encarregado pelo Tratamento de Dados Pessoais (DPO) - membro importante do TRI, responsável por encaminhar comunicações formais em incidentes envolvendo vazamentos de dados pessoais.

INTRODUÇÃO:

Incidente é definido como situação imprevista, apta a alterar a ordem normal das coisas e, em se tratando de proteção de dados, colocar em risco dados pessoais dos indivíduos que se relacionam com a RAPIDONET.

A gestão de incidente tem por objetivo garantir resposta de forma mais rápida, organizada e eficiente ao evento, minimizando suas consequências, em consonância com a Lei Geral de Proteção de Dados e Lei 20.489/2019.

Nos termos do artigo 46 da Lei Geral de Proteção de Dados (LGPD), os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas

de destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado ou ilícito.

Em qualquer hipótese, os colaboradores deverão ficar atentos as seguintes situações:

- ✓ Encaminhamento de e-mails com caracteres e/ou arquivos suspeitos;
- ✓ Comportamento impróprio de dispositivos;
- ✓ Problema no acesso a determinados arquivos e/ou serviços;
- ✓ Roubo de dispositivos de armazenamento ou computadores com informações;
- ✓ Alerta de software antivírus;
- ✓ Consumo excessivo e repentino de memória em servidores ou computadores;
- ✓ Tráfego de rede incomum;
- ✓ Conexões bloqueadas por firewall;
- ✓ logs de tentativas de acesso não autorizado aos servidores;
- ✓ Não cumprimento dos procedimentos internos.

Não obstante as ações preventivas, existindo incidentes, a RAPIDONET observará as etapas a seguir:

ETAPAS:

1. **Notificação**: Todos os funcionários e/ou parceiros da RAPIDONET são responsáveis por reportar qualquer tipo de eventos, que possam causar danos à segurança da informação e proteção de dados.

O incidente pode ser noticiado, por pessoa externa ou não, através dos mecanismos de comunicação – e-mail institucional do Encarregado pelo Tratamento de Dados Pessoais (cristhian@rapidonet.com.br) ou endereço postal da empresa (ouvidoria@rapidonet.com.br).

Encarregado pelo tratamento de dados pessoais:

Nome: Cristhian Alessander de Queiroz, brasileiro, casado, inscrito no CPF sob o nº. 723.751.671-04

E-mail: cristhian@rapidonet.com.br
Endereço: Rua BM-16, Quadra 31, Lote 20 Casa 2 Residencial Brisas da Mata Goiânia – Goiás Cep: 74475366

O conhecimento de um incidente por qualquer pessoa enseja, necessariamente, uma notificação ao Encarregado, o mais rápido possível, para as adotar as medidas previstas na LGPD e no portal da Autoridade Nacional sobre comunicação de incidentes de segurança.

2. **Triagem**: Após a notificação, a equipe do TRI vai fazer uma avaliação preliminar. Deverá quantidade de titulares de dados pessoais afetados, categoria e quantidade de dados afetados, consequências do incidente para os agentes de tratamento de dados pessoais. Poderá, inclusive, acionar técnico com expertise para auxiliar na avaliação, deverá buscar/colher informações, avaliar o risco da situação e, ainda, poderá, se for o caso, descartar as notificações nulas ou claramente improcedentes.

Em relação ao risco, será considerado ALTO se for atingido dados pessoais de crianças e/ou adolescentes, dados sensíveis, que possam gerar discriminação ao titular e dados bancários. Acaso o incidente atinja dados pessoais imediatamente identificáveis (nome, e-mail, CPF, dentre outros), o risco será moderado. Por fim, se for atingido, tão somente, dados pessoais de difícil identificação o risco é caracterizado como leve.

3. **Avaliação**: Nesta fase será realizada uma avaliação mais detalhada/minuciosa. Para tanto, a equipe verificará a causa do incidente (endereços IP, credenciais e/ou logins envolvidos, varredura no sistema, os possíveis responsáveis e donos das informações, hora e data de cada ocorrência, transferências de dados irregulares, sistemas e serviços afetados, existência de outros eventos e alertas relacionados com o incidente).

Deve ser registrada toda a cadeia de diligências realizadas para entendimento do evento e mitigação dos danos.

4. **Contenção e erradicação**: o intuito desta fase é limitar o dano e isolar os sistemas afetados para inibir maiores problemas. Sistemas podem ser desligados após o *Snapshot*, procedimentos alterados, funcionários/parceiros afastados. Sempre com muito cuidado

para não apagar evidências que poderiam ser usadas para identificar autoria, origem e método usado para quebrar a segurança.

5. **Recuperação**: é um conjunto de medidas que pode ser gradual ou total, a depender da situação. Neste momento, o TRI tem a responsabilidade de passar as informações que obteve para aplicação da solução.

Em regra, pode ser realizado restauração de backups, clonagem de máquinas virtuais e reinstalação de sistemas. Acaso o sistema afetado seja restabelecido, deve ser realizada uma análise técnica para examinar detalhadamente a integridade dos dados.

Após a resolução do incidente, um Relatório de Resposta a Incidentes (IRR) deverá ser elaborado e disponibilizado para gerenciamento da Área de Tecnologia da Informação (TI), Área de Compliance e Setor Jurídico.

6. **Lições aprendidas**: o TRI deverá fazer reuniões com o objetivo de discutir erros e dificuldades encontradas, propor melhorias para os sistemas e processos e realizar treinamento da equipe. É fundamental que os mesmos erros não voltem a acontecer.

7. **Documentação**: Todo incidente deve ser documentado. Para tanto será registrado os atores envolvidos, informações/provas colhidas, decisões preliminares e finais, medidas de contenção ou reparação e, ainda, as lições aprendidas.

8. **Comunicações**: no caso de incidente com vazamento de dados pessoais, o Encarregado de Tratamento de Dados (DPO) deve, diante das informações levantadas internamente, de acordo com os parâmetros estabelecidos pelo Autoridade Nacional, realizar a comunicação. Existindo necessidade, as comunicações à Autoridade Nacional devem acontecer no prazo de 02 (dois) dias úteis. Eis que o art. 48 da LGPD determina que o controlador tem a obrigação de comunicar à ANPD e ao titular dos dados pessoais a ocorrência de incidente de segurança que venha a gerar risco ou dano considerado relevante aos titulares.

Na comunicação deverá conter as seguintes informações:

- ✓ A descrição da natureza dos dados pessoais afetados;
- ✓ As informações sobre os titulares envolvidos; A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados;
- ✓ Os riscos relacionados ao incidente;
- ✓ Os motivos da demora, no caso de a comunicação não ter sido imediata;
- ✓ As medidas que foram ou que estão sendo tomadas para reverter ou mitigar os efeitos do prejuízo.

É importante que todas as informações, provas/documentos coletados sejam arquivadas para propiciar relatório final do incidente.

DISPOSIÇÕES FINAIS

Em caso de questionamentos, observações e/ou sugestões relacionadas a este PLANO DE RESPOSTA A INCIDENTES, entre em contato com o Encarregado da Empresa, através do e-mail cristhian@rapidonet.com.br ou ouvidoria@rapidonet.com.br.

Última modificação: 01/06/2023.