LGPD - PROCEMPA

Plano de Resposta a Incidentes de Segurança e Privacidade

Agosto/2020

Preparação Prévia

O Plano de Resposta a Incidentes de Segurança e Privacidade é essencialmente um processo. Descreve a forma como a PROCEMPA vai responder às situações de emergência e exceção. Pela potencial gravidade, a resposta da Companhia deve ser rápida e confiável, ao mesmo tempo resguardando evidências forenses que podem ajudar a prevenir novos incidentes e atendendo as exigências legais de comunicação e transparência. Para o processo funcionar e ser estabelecido é pré-requisito a preparação prévia e contínua, atendendo os seguintes itens:

- **Formação do Time de Resposta a Incidentes (TRI)**. Este é um grupo de empregados que deve ser designado através de Resolução de Diretoria, com acessos, habilidades, responsabilidades, treinamento e conhecimentos chave para responder aos mais variados tipos de incidentes. O TRI deve ter reuniões periódicas para definir melhorias neste plano, verificação de pré-requisitos, mecanismos, atribuições, necessidade de preparo, bem como divulgação e treinamentos para os membros e demais empregados. O Encarregado pelo Tratamento de Dados Pessoais (DPO) e pelo menos um representante da Equipe de Segurança da Informação devem fazer parte desse grupo.
- **Instalação e divulgação dos mecanismos de comunicação de incidente**. Devem ser criadas, disponibilizadas e publicadas as formas de notificação à Companhia quando ocorrerem incidentes. O §1º, do Artigo 41, da Lei 13709/2018, a LGPD, estabelece: "*A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.*" Portanto, devem ser divulgados os e-mails: **dpo@PROCEMPA.com.br** e **seguranca@PROCEMPA.com.br**, bem como os contatos do **Callcente**r. Deve haver indicação de quais mecanismos são considerados rápidos e seguros e se sugere o esclarecimento de quais as expectativas de anonimato que o notificador deve ter.
- **Definição do grupo de Acionadores do TR**I. Responsáveis por receberem as notificações e a realização do tratamento inicial. Para a cobertura 24 horas, este grupo deve incluir membros do Callcenter e contatos qualificados para executar a triagem.
- **Instalação, configuração e definição de ferramentas de monitoria e alarmes.** Devem informar diretamente o TRI através de mecanismos de comunicação direta como o Rocket Chat, WhatsApp ou SMS.
- **Preparo de um Plano de Comunicação de Incidentes**. Para facilitar a comunicação da Companhia deve ser criada uma biblioteca com modelos de documentos (templates) para comunicação formal do Encarregado pelo Tratamento de Dados Pessoais com a ANPD, titulares de dados, notificadores e imprensa.

Plano de Resposta a Incidentes

Atores

- **Notificador** - pessoa ou sistema de monitoração que notifica incidente.
- **TRI** - Time de Resposta a Incidentes, definido na preparação prévia.
- **Acionadores do TR**I - grupo que receberá notificações de incidentes em primeira mão para triagem, estruturado em níveis distintos para viabilizar a importante cobertura 24 horas.
- **Responsável por Sistema ou Controlador de Sistema**, indicado que deve ser contatado e pode autorizar ou vetar procedimentos de emergência. Deve estar documentado na CMDB, inclusive forma de contato para emergências
- **Equipe de Segurança da Informação**
- **Encarregado pelo Tratamento de Dados Pessoais (DPO)** - membro especial do TRI, responsável por encaminhar comunicações formais em incidentes envolvendo vazamentos de dados pessoais.
- **Desenvolvedores/Operadores/Fornecedores dos sistemas** - atuam no desenvolvimento de solução e instalação da mesma.

Processo

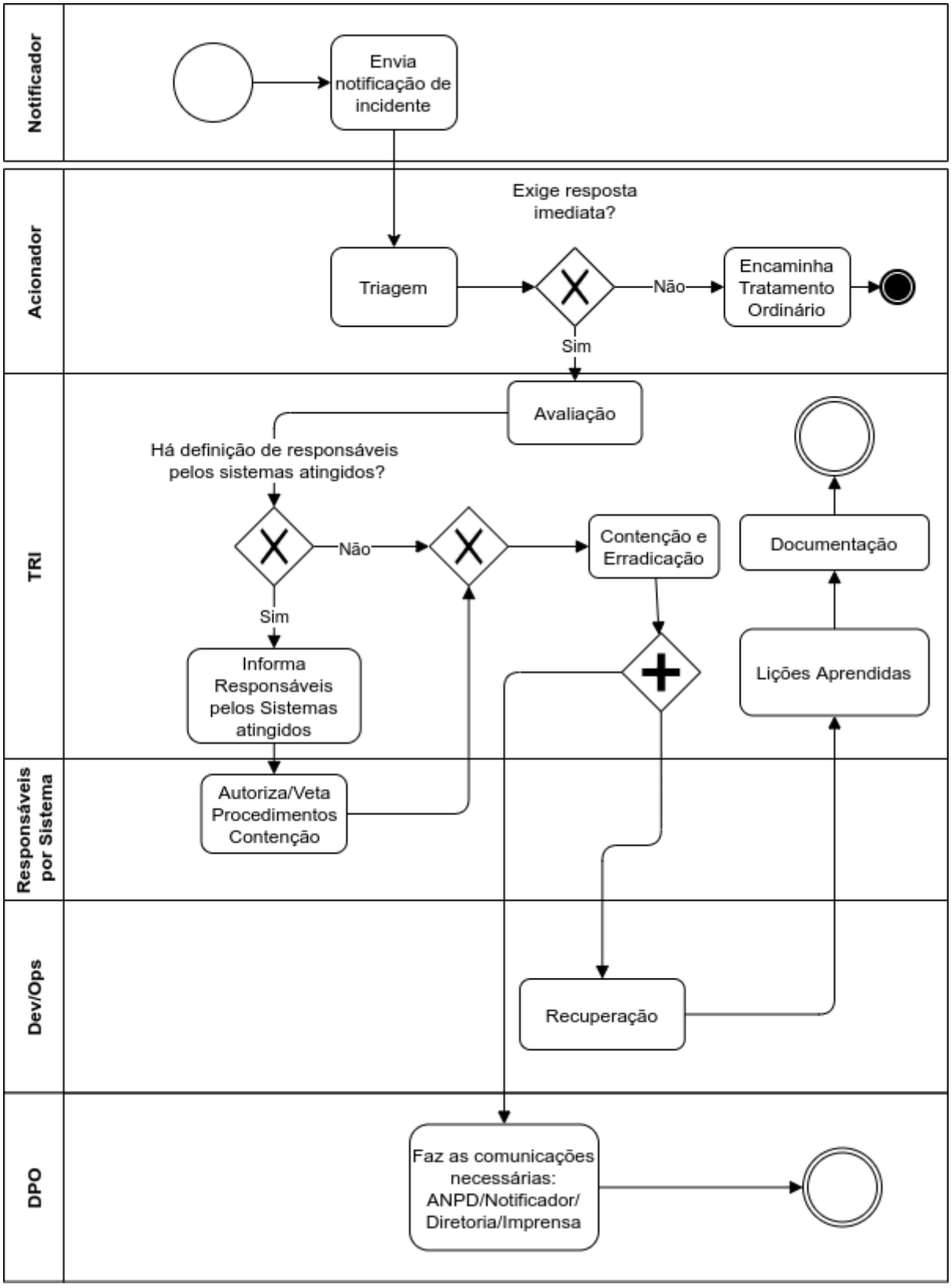

Diagrama BPMN do processo de resposta a incidentes.

Inicio

1) Um novo incidente é notificado, por pessoa externa ou não a Companhia ou por alarme da monitoração, usando um dos mecanismos de comunicação definidos. Notificação é recebida por Acionador do TRI.

Triagem

2) O Acionador do TRI deve fazer a avaliação preliminar ou contatar imediatamente outro Acionador em condições de realizar a referida avaliação, descartando as notificações nulas ou claramente improcedentes, tomando os devidos cuidados.
3) Na avaliação preliminar, devem ser buscadas informações sobre os sistemas que foram alegadamente impactados, sua criticidade, quais os danos aparentes e o risco da situação se agravar se não houver resposta imediata.
4) Conforme a avaliação preliminar, incidentes que não envolvem sistemas online e que seguramente não apresentam riscos aumentados pela falta de ação imediata podem ser reencaminhados para tramites regulares da Companhia pela Equipe de Segurança da Informação e Encarregado pelo Tratamento de Dados Pessoais, caso o incidente envolva dados pessoais.
5) Em caso de incidentes que exigem resposta imediata ou melhor avaliação, o TRI deve ser acionado e passamos às fases seguintes.

Avaliação

6) Nesta fase deve ser iniciada uma avaliação mais detalhada do incidente. Deve-se procurar identificar a causa do incidente, endereços IP e credenciais envolvidas, transações e transferências de dados irregulares, métodos e vulnerabilidades exploradas, visando determinar ações para as demais fases. Pode ser importante engajar especialistas dos sistemas afetados para colaborar e isso deve ser feito a critério do TRI a qualquer momento que julgar adequado e viável.

Contenção e Erradicação

7) Caso estejam identificados na CMDB, devem ser acionados os responsáveis pelos sistemas impactados, conforme indicado na documentação, que irão orientar e se manifestar sobre os procedimentos de contenção e erradicação.
8) O objetivo das medidas de contenção e erradicação é limitar o dano e isolar os sistemas afetados para evitar mais danos. Aqui, conforme a necessidade e a autorização obtida será realizado o desligamento dos sistemas inteiros ou de funcionalidades especificas, colocação de avisos de indisponibilidade para manutenção, sempre que possível tomando cuidados para não impactar evidências que poderiam ser usadas para identificar autoria, origem e método usado para quebrar a segurança.
9) Em caso de incidente envolvendo máquinas virtuais, deve ser feito snapshot das mesmas para posterior análise.

Recuperação

10) Caso exista Plano de Continuidade de Negócio dos sistemas impactados, eles devem ser iniciados, conforme especificado.

11) A recuperação é o conjunto de medidas para restaurar os serviços completamente, mas pode ser feita de forma gradual, conforme viabilidade e decisão do responsável pelo sistema.
12) O TRI tem a responsabilidade de passar as informações que obteve para o desenvolvimento da solução e sua instalação.
13) Para a recuperação devem ser tomadas medidas identificadas na Avaliação, tais como restauração de backups, clonagem de máquinas virtuais, reinstalação de sistemas.
14) Pode ser necessário o desenvolvimento e instalação de atualizações de aplicação ou do Sistema Operacional, por isso esta fase pode ser prolongada, de acordo com a priorização dada.

Lições Aprendidas

15) Com o incidente contido e sua resolução encaminhada, o TRI deve agendar e conduzir uma reunião de Lições Aprendidas, com convidados a seu critério, com o objetivo de discutir erros e dificuldades encontradas, propor melhorias para os sistemas e processos - inclusive deste Plano de Resposta a Incidentes.
16) As melhorias sugeridas na reunião, com o devido consenso, devem ser encaminhadas aos responsáveis para definição sobre a adoção.

Documentação

17) O TRI deve documentar o incidente em base de conhecimentos apropriada, detalhando as informações obtidas, linha de tempo, atores envolvidos, evidencias, conclusões, decisões, autorizações e ações tomadas, inclusive as da reunião de lições aprendidas.

Comunicações

18) Assim que possível, no caso de incidente com vazamento de dados pessoais, o Encarregado de Tratamento de Dados (DPO) deve avaliar e fazer as comunicações obrigatórias por Lei, se houverem, bem como informar e subsidiar os Encarregados de Tratamento de Dados dos controladores do sistema. Essas comunicações podem incluir agradecimentos ao notificador, informações para os titulares de dados, relatórios formais para a ANPD.