PLANO DE GESTÃO DE CRISE EM CASO DE INCIDENTE/ VIOLAÇÃO DE DADOS

Março de 2026

Equipe Técnica do Grupo ADX

Adriano Lima Head de Projetos	**Adgenison Nascimento** Head de Negócios
Hendrick Arcanjo Consultor de Tecnologia	**Gessica Alcântara** Gestora de projetos
Saulo Santos Advogado	**Laís Gomes** Head de Processos

Histórico de revisões			
Versão	**Data**	**Autor**	**Descrição**
1.0	03/03/2026	Grupo ADX	Elaboração do documento

SUMÁRIO

ÍNDICE DE FIGURAS

1 – OBJETIVO

O objetivo deste documento é estabelecer a metodologia de gestão para incidentes, no âmbito da Ytech, para atender às exigências legais previstas na Lei Geral de Proteção de Dados (LGPD), no tocante a gestão de segurança da informação e privacidade.

2 – CONCEITOS IMPORTANTES

- **AMEAÇA** - conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;
- **ANÁLISE DE IMPACTO NOS NEGÓCIOS (AIN)** - visa estimar os impactos resultantes da interrupção de serviços e de cenários de desastres que possam afetar o desempenho dos órgãos ou entidades da APF, bem como as técnicas para qualificar e quantificar esses impactos. Define também a criticidade dos processos de negócio, suas prioridades de recuperação, interdependências e os requisitos de segurança da informação para que os objetivos de recuperação sejam atendidos nos prazos estabelecidos;
- **ANÁLISE DE INCIDENTES** - consiste em examinar todas as informações disponíveis sobre o incidente, incluindo artefatos e outras evidências relacionadas ao evento. O propósito da análise é identificar o escopo do incidente, sua extensão, sua natureza e quais os prejuízos causados. Também faz parte da análise do incidente propor estratégias de contenção e recuperação;
- **ANÁLISE DE RISCOS** - uso sistemático de informações para identificar fontes e estimar o risco;
- **ANONIMIZAÇÃO** - utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
- **ATAQUE** - ação que constitui uma tentativa deliberada e não autorizada para acessar/manipular informações, ou tornar um sistema inacessível, não integro, ou indisponível;
- **ATIVOS DE INFORMAÇÃO -** os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso;
- **AUTENTICAÇÃO** - processo que busca verificar a identidade digital de uma entidade de um sistema no momento em que ela requisita acesso a esse sistema. O processo é realizado por meio de regras preestabelecidas, geralmente pela comparação das

credenciais apresentadas pela entidade com outras já pré-definidas no sistema, reconhecendo como verdadeiras ou legítimas as partes envolvidas em um processo;

- **AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)** - órgão da APF responsável por zelar, implementar e fiscalizar o cumprimento da Lei 13.709, de 14 de agosto de 2018;
- **AUTORIZAÇÃO** - processo que ocorre após a autenticação e tem a função de diferenciar os privilégios atribuídos ao usuário que foi autenticado. Os atributos de autorização normalmente são definidos em grupos mantidos em uma base de dados centralizada, sendo que cada usuário herda as características do grupo a que ele pertence. Portanto, autorização é o direito ou permissão de acesso a um recurso de um sistema;
- **AVALIAÇÃO DE RISCOS** - processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco.
- **BACKUP OU CÓPIA DE SEGURANÇA** - conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;
- **BANCO DE DADOS** - coleção de dados inter-relacionados, representando informações sobre um domínio específico. São coleções organizadas de dados que se relacionam de forma a criar algum sentido (informação) e dar mais eficiência durante uma consulta ou a geração de informações ou conhecimento;
- **BIOMETRIA** - verificação da identidade de um indivíduo por meio de uma característica física ou comportamental única, através de meios automatizados;
- **COMPUTAÇÃO EM NUVEM** - modelo computacional que permite acesso por demanda, e independentemente da localização, a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou de interação com o provedor de serviços;
- **CONSENTIMENTO** - manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
- **CONTINUIDADE DE NEGÓCIOS -** capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido;
- **CONTROLE DE ACESSO** - conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação;
- **CONTROLES DE SEGURANÇA** - medidas adotadas para evitar ou diminuir o risco de um ataque. Exemplos de controles de segurança são: criptografia, funções de hash,

validação de entrada, balanceamento de carga, trilhas de auditoria, controle de acesso, expiração de sessão e backups, entre outros;

- **CRIPTOGRAFIA** - arte de proteção da informação através de sua transformação em um texto cifrado (criptografado), com o uso de uma chave de cifragem e de procedimentos computacionais previamente estabelecidos, a fim de que somente o(s) possuidor(es) da chave de decifragem possa(m) reverter o texto criptografado de volta ao original (texto pleno). A chave de decifragem pode ser igual (criptografia simétrica) ou diferente (criptografia assimétrica) da chave de cifragem;
- **CSIRT (COMPUTER SECURITY INCIDENT RESPONSE TEAM)** - acrônimo internacional para designar um grupo de resposta a incidentes de segurança, responsável por tratar incidentes de segurança para um público alvo específico;
- **DADO ANONIMIZADO** - dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;
- **DADO PESSOAL** - informação relacionada a pessoa natural identificada ou identificável;
- **DADO PESSOAL SENSÍVEL** - dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
- **ENCARREGADO** - pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados;
- **ENGENHARIA SOCIAL** - técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações. No contexto da SI, é considerada uma prática de má-fé, usada por indivíduos para tentar explorar a boa-fé ou abusar da ingenuidade e da confiança de outras pessoas, a fim de aplicar golpes, ludibriar ou obter informações sigilosas e importantes;
- **EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES EM REDES COMPUTACIONAIS (ETIR)** - grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;
- **EVENTO DE SEGURANÇA** - qualquer ocorrência identificada em um sistema, serviço ou rede que indique uma possível falha da política de segurança, falha das salvaguardas ou mesmo uma situação até então desconhecida que possa se tornar relevante em termos de segurança;
- **FIREWALL** - recurso destinado a evitar acesso não autorizado a uma determinada rede, ou um conjunto de redes, ou a partir dela. Podem ser implementados em hardware ou software, ou em ambos. Cada mensagem que entra ou sai da rede passa pelo firewall, que a examina a fim de determinar se atende ou não os critérios de segurança especificados;

- **GESTÃO DE MUDANÇAS NOS ASPECTOS RELATIVOS À SI** - aplicação de um processo estruturado e de um conjunto de ferramentas de gerenciamento de mudanças, de modo a aumentar a probabilidade de sucesso e fazer com que as mudanças transcorram com mínimos impactos no âmbito de órgão da APF, visando viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação;
- **INCIDENTE** - evento, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;
- **INCIDENTE DE SEGURANÇA** - qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;
- **INVASÃO** - incidente de segurança no qual o ataque foi bem sucedido, resultando no acesso, na manipulação ou na destruição de informações em um computador ou em um sistema da organização;
- **MALWARE** -software malicioso projetado para infiltrar um sistema computacional com a intenção de roubar dados ou danificar aplicativos ou o sistema operacional. Esse tipo de software costuma entrar em uma rede por meio de diversas atividades aprovadas pela empresa, como e-mail ou sites. Entre os exemplos de malware estão os vírus, worms, trojans (ou cavalos de Troia),spyware, adware e rootkits;
- **PERFIL DE ACESSO -** conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso;
- **PLANO DE CONTINUIDADE DE NEGÓCIOS** - documentação dos procedimentos e informações necessárias para que os órgãos ou entidades da APF mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo em um nível previamente definido, em casos de incidentes;
- **PLANO DE GERENCIAMENTO DE INCIDENTES** - plano de ação claramente definido e documentado, para ser usado em caso de incidente que basicamente englobe os principais recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes;
- **PLANO DE RECUPERAÇÃO DE NEGÓCIOS** - documentação dos procedimentos e de informações necessárias para que o órgão ou entidade da APF operacionalize o retorno das atividades críticas à normalidade;
- **POLÍTICA DE GESTÃO DE RISCOS** - declaração das intenções e diretrizes gerais de uma organização relacionadas à gestão de risco;
- **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO** - documento aprovado pela autoridade responsável pelo órgão ou entidade da APF, direta e indireta, com o

objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da SI (Este termo substituiu o termo Política de Segurança da Informação e Comunicações);

- **POSIC** - acrônimo de Política de Segurança da Informação e Comunicações. Foi substituído pelo acrônimo POSIN;
- **REDE PRIVADA VIRTUAL** - mais conhecida por VPN, refere-se a construção de uma rede privada utilizando redes públicas (por exemplo, a Internet) como infraestrutura. Esses sistemas utilizam criptografia e outros mecanismos de segurança para garantir que somente usuários autorizados possam ter acesso à rede privada e que nenhum dado será interceptado enquanto estiver passando pela rede pública;
- **RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS** - documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
- **TRATAMENTO DA INFORMAÇÃO** - conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;
- **TRATAMENTO DE INCIDENTES DE SEGURANÇA EM REDES COMPUTACIONAIS** - serviço que consiste em receber, filtrar, classificar e responder às solicitações e aos alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;
- **VAZAMENTO DE DADOS** - transmissão não-autorizada de dados de dentro de uma organização para um destino ou recipiente externo. O termo pode ser usado para descrever dados que são transferidos eletronicamente ou fisicamente. Pode ocorrer de forma acidental ou intencional (pela ação de agentes internos, pela ação de agentes externos ou pelo uso de software malicioso).
- **VULNERABILIDADE** - conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou por uma organização, os quais podem ser evitados por uma ação interna de segurança da informação;
- **VULNERABILIDADE DE DIA ZERO** - falha na segurança de um software que ainda não é conhecida por seus desenvolvedores, pelos fabricantes de soluções de segurança e pelo público em geral. Também é considerada uma Vulnerabilidade de Dia Zero a falha de segurança que já é conhecida pelo fornecedor do produto, mas para a qual ainda não existe um pacote de segurança para corrigi-la. Por não ser conhecida ou por não haver ainda um patch de segurança para essa falha, ela pode ser explorada por hackers em Explorações de Dia Zero. A correção de uma

vulnerabilidade de dia zero geralmente é tarefa do fabricante do software, que precisará lançar um pacote de segurança para consertar a falha.

3 – INCIDENTES

Segundo o CERT.br, um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado a segurança de sistemas de computação ou de Redes de Computadores. Em geral, qualquer situação em que um ou mais ativos da informação está(ão) sob risco, é considerado um incidente de segurança.

A LGPD exige que as empresas gerenciem de forma completa os incidentes de segurança e privacidade ocorridos para prestação de contas aos titulares e para a ANPD. Um incidente é sempre gerado pela exploração de alguma vulnerabilidade existente nos ativos organizacionais. A **Figura 1** descreve esse fluxo.

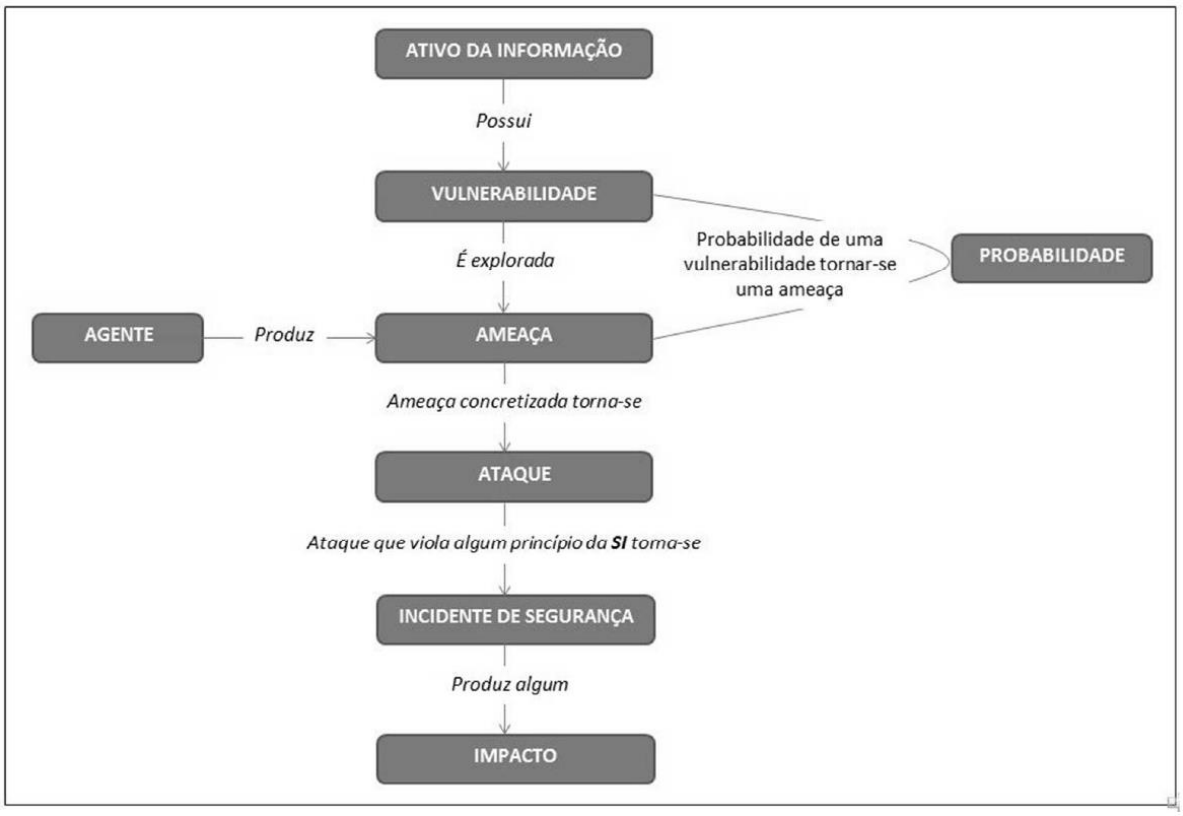

Figura 1 - Fluxo de um incidente de segurança da informação.

É importante diferenciar uma violação de segurança de uma violação de privacidade. A **Figura 2** mostra que a violação de dados pode ou não acontecer quando uma violação de segurança ocorre. No exemplo dado, se o pen drive ou laptop perdido tiver os dados criptografados, não será categorizada uma violação de dados.

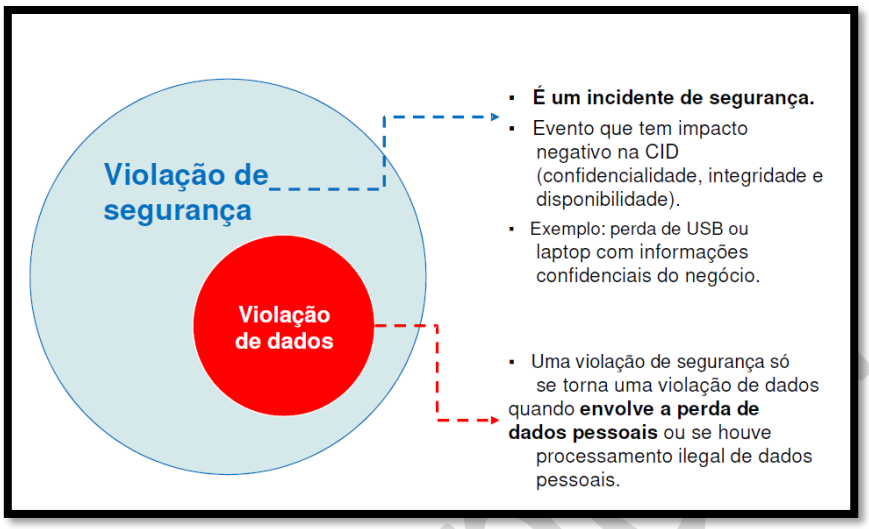

Figura 2 - Violação de segurança X Violação de dados.

No texto da LGPD, a previsão legal para a resposta a incidentes de segurança vem no capítulo VII, justamente o que trata da segurança da informação e das boas práticas a serem adotadas para tanto. Em seu artigo 48, consta:

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

- § 1º A comunicação será feita em **prazo razoável**, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:
- I - a descrição da natureza dos dados pessoais afetados;
- II - as informações sobre os titulares envolvidos;
- III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- IV - os riscos relacionados ao incidente;

- V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
- VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Dessa forma, será extremamente importante a criação de um processo para gerenciamento de todos os incidentes, bem como para o registro das deliberações realizadas pelo comitê de privacidade e pelo DPO. Para potencializar esse processo, recomenda-se que seja usado um software especialista nessa função. Esse software deve catalogar cada registro de incidentes ocorridos dentro da empresa. O registro de incidente normalmente contempla os seguintes dados:

- Quando ocorreu o incidente;
- Quais dados foram afetados;
- Quais e quantos titulares foram afetados;
- Quais as causas do incidente;
- Quais seus efeitos e consequências;
- Qual o plano para mitigação desses efeitos e suas respectivas consequências;
- Uma linha do tempo do incidente, incluindo quando houve o primeiro alerta quanto ao incidente e quando de fato foi determinado que o mesmo ocorreu;
- As decisões relativas à notificação.

Após a análise do incidente pela equipe de segurança, comitê e DPO, as seguintes informações devem ser registradas para determinação do plano ação.

- O tipo do incidente/vazamento;
- O tipo de dados pessoais afetados;
- A sensibilidade dos dados afetados;
- O volume de dados afetados;
- O número de titulares atingidos;
- A natureza do processamento;

- A facilidade ou não de identificação dos titulares (se por exemplo, os dados estavam criptografados ou anonimizados, o risco reduz);
- A gravidade das consequências para os titulares;
- A extensão das consequências para os titulares;
- Se houve menores entre os titulares;

4 – REQUISITOS GERAIS PARA O SISTEMA DE GESTÃO DE INCIDENTES

Durante o funcionamento do seu modelo de negócio, a Ytech deve estabelecer, requisitos gerais de estruturação de segurança e privacidade (**Figura 3**), considerando que o tratamento de dados pessoais está sujeito à conformidade com a Lei 13.709/2018. É importante dar atenção especial aos acessos realizados aos dados pessoais pelos colaboradores e operadores externos que atuam no fornecimento de serviços sobre dados pessoais.

Figura 3 - Requisitos gerais de estruturação de segurança e privacidade (Guias Operacionais para adequação a LGPD).

4.1 – Política de Segurança da Informação

A empresa deve possuir uma Política de Segurança da Informação, ou equivalente, incluindo políticas ou normas para proteção de dados pessoais vigentes e atualizadas, com processo de revisão periódico formalizado e institucionalizado, de forma a garantir, dentre outros requisitos, o uso de sistemática e procedimentos de segurança da informação para assegurar não apenas a disponibilidade, a integridade, a confidencialidade e a autenticidade, mas também a consistência, a privacidade e a confiabilidade dos dados e informações tratados pela empresa.;

4.2 – Análise de Impacto na Privacidade de Dados Pessoais

A empresa deve realizar a análise de impacto na privacidade dos dados pessoais relacionada a todos os processos e sistemas existentes, elaborando o RIPD em todos aqueles casos que possam gerar riscos aos titulares dos dados pessoais, conforme previsto na Lei nº 13.709/2018, quando da concepção de qualquer novo projeto, produto ou serviço;

4.3 – Análise e Avaliação de Riscos

A empresa deve realizar periodicamente uma análise/avaliação de riscos da arquitetura de Solução de TIC, indicando os eventos de risco ao qual os sistemas estão expostos, baseada em prévia análise de vulnerabilidades dos ativos que compõem a Solução de TIC, resguardando os segredos de negócio, direitos autorais e direitos de propriedade intelectual aplicáveis, conforme metodologia utilizada.

4.4– Arquitetura, Controles de Segurança e Matriz de Responsabilidades

A empresa deve elaborar:

a) Documentação que descreve a arquitetura física e lógica da Solução de TIC;

b) Uma descrição dos controles de segurança da informação e privacidade implementados em cada componente descrito na arquitetura física e lógica;

c) Matriz de responsabilidades descrevendo a atribuição das responsabilidades pela segurança da informação na organização, pela privacidade (encarregado), identificação dos gestores de serviços com dados pessoais, operador(es) de tratamento de dados, relacionada ao objeto da contratação e com relação aos itens aqui descritos.

4.5 – Continuidade do Negócio

A empresa deve possuir e implementar um Plano de Continuidade de Negócio relacionado aos serviços críticos para a organização, que garantam o nível requerido de continuidade para a segurança da informação durante uma situação adversa;

4.6 Coleta e preservação de evidências

A empresa deve implementar os controles necessários para coleta e preservação de evidências de incidentes de segurança da informação e privacidade;

4.7 Gestão de Mudanças

A empresa deve possuir e implementar processo de gestão de mudanças adequado para que mudanças na organização, nos processos de negócio e nos recursos de

processamento da informação sejam controlados e não afetem a segurança da informação e privacidade, reduzindo o nível de risco ao qual o objeto do contrato e/ou a contratante está exposta, considerando os critérios de aceitabilidade de riscos definidos pela contratante. No caso de contratação de sistemas de informação, se aplicável, considerar ainda na gestão de mudanças o processo referente a migração dos dados do sistema legado para o novo sistema;

4.8 Gestão de Capacidade

A empresa deve implementar o processo de gestão de capacidade e recursos para redundância de forma que a utilização dos recursos seja monitorada, ajustada e as projeções das necessidades de capacidade futura sejam avaliadas para garantir o desempenho dos ativos, assegurando também a disponibilidade e recuperação de dados e informações, em conformidade com um plano de continuidade, que garanta o nível requerido de continuidade para a segurança da informação durante uma situação adversa;

4.9 Desenvolvimento Seguro

A empresa deve possuir e manter trilhas de qualidade e teste de software, e realizar desenvolvimento seguro. Os seguintes requisitos devem ser cumpridos:

- ✓ Os dados pessoais utilizados em ambiente de TDH (teste, desenvolvimento e homologação) devem passar por um processo de anonimização;
- ✓ A utilização dos dados pessoais em ambiente de TDH (teste, desenvolvimento e homologação), não anonimizados, deve ser autorizada pelo proprietário do ativo de informação;
- ✓ A empresa deve utilizar técnicas ou métodos apropriados para garantir exclusão ou destruição segura de dados pessoais (incluindo originais, cópias e registros arquivados), de modo a impedir sua recuperação no processo;

- ✓ A aplicação desenvolvida deve ter funcionalidade para, ao fornecer a base de informações para órgãos de pesquisa, os dados pessoais sejam anonimizados ou pseudoanonimizados;

- ✓ A empresa deve possuir e implementar política de privacidade que atenda aos princípios da Lei Geral de Proteção de Dados Pessoais (LGPD), assegurando o adequado tratamento dos dados pessoais e principalmente sua classificação em sensíveis e não sensíveis, incluindo categorias de informações pessoais de saúde e informações pessoais financeiras;

4.10 Política de Backup

A empresa deve possuir e implementar política de backup das informações e dos registros de log, em conformidade com os dispositivos legais aplicáveis, que assegure a manutenção de cópias de segurança de todos os componentes de software dos sistemas, de suas bases de dados e da documentação associada, observando a técnica, os cuidados requeridos para cada caso, de modo a ser possível a plena recuperação de versões dos sistemas e dados salvaguardados em caso de falha.

5 – GESTÃO DE INCIDENTES

Gestão de incidentes são as ações que uma empresa toma para prevenir ou conter o impacto de um incidente enquanto este está ocorrendo ou brevemente após ter ocorrido (NIST). O processo de resposta a incidentes deve estar muito bem alinhado às políticas estabelecidas e aos objetivos de negócios da companhia.

Todo documento de Plano de Respostas a Incidentes deve possuir pelo menos as principais fases listadas abaixo:

- **Preparação**: como estar preparado e agir diante de um incidente?

- **Identificação**: quais os critérios de identificação de incidentes?
- **Contenção**: como conter o incidente?
- **Erradicação**: como eliminar a causa-raiz do problema?
- **Recuperação**: o que fazer para restabelecer a normalidade de todos os sistemas?
- **Lições aprendidas**: o que fazer para que os mesmos erros não ocorram novamente?

5.1 Preparação

A preparação aborda como a equipe vai lidar com a ocorrência de um incidente. Isso inclui comunicação externa e interna, bem como documentação de incidentes. Para essa finalidade é fundamental ter uma política de segurança corporativa definida contendo diretrizes sobre quais riscos a empresa está exposta e quais medidas preventivas devem ser tomadas. Algumas atividades importantes dessa fase são:

- ✓ Formalize, treine e capacite a equipe que atuará no incidente. Analise o conhecimento técnico/ comportamental necessário da equipe.
- ✓ Discrimine as funções de cada integrante. As funções e responsabilidades devem ser definidas em toda a organização para identificar, detectar, analisar, conter e responder os incidentes.
- ✓ Mantenha uma lista atualizada dos principais contatos para serem acionados. Ex: departamentos, seguradora, corretora, prestadores de suporte no incidente, polícia etc.
- ✓ Elabore uma diretriz sobre quem deve ser notificado para determinado assunto e em qual janela de tempo. Lembre-se de manter a lista de contatos atualizada.
- ✓ Mantenha treinados os principais envolvidos no plano.

- ✓ Verifique quais são os processos necessários para a atuação no caso de um incidente. Faça um levantamento de quais já estão implementados e quais precisam de ajustes (ausência de atividades ou serviços, fluxos mal definidos, gargalos etc.).

- ✓ Faça um levantamento de quais são os ativos críticos da sua empresa, quais são as vulnerabilidades, os tipos de incidentes mais recorrentes e quais respostas seriam necessárias para cada um deles.

- ✓ Elabore cenários para o tratamento de ameaças específicas. Ex: infecção vírus/malware, ataque de ransomware, extorsão, vazamento de dados pessoais, vazamento de dados do negócio/ dados confidenciais, ataque DDoS etc.

- ✓ Defina qual será a sua estratégia de comunicação/notificação para cada tipo de incidente. Esta, por sua vez, deve estar alinhada à estratégia e às políticas da empresa.

- ✓ Oriente como os dados devem ser processados e manuseados, garantindo sua disponibilidade, integridade e confidencialidade. Lembre-se: os dados de incidentes devem ser protegidos por questões legais, necessidade de negócio e ameaça de potencial invasão.

- ✓ Disponibilize fluxos/políticas/modelos aprovados e disponíveis para:

    - funcionários relatarem atividades suspeitas;
    - processo de escalonamento de incidentes;
    - políticas internas que contribuam para resposta dos incidentes;
    - ativos críticos da sua empresa, quais as vulnerabilidades encontradas neles e como seriam as respostas ao incidente, caso ocorra;
    - modelos de comunicação interna;
    - modelos de comunicação externa;
    - política de descarte de dados;

- protocolo de comunicação de sinistro da seguradora.

✓ Defina como serão os testes do Plano de Resposta a Incidentes e em qual periodicidade ele ocorrerá.

5.2 Identificação

Esta etapa define os critérios que vão ativar o CSIRT (Grupo técnico responsável por resolver incidentes relacionados à segurança em sistemas computacionais). Por exemplo, quando um ataque de força bruta é detectado, imediatamente o plano de resposta a incidentes é acionado e a equipe entra em ação. Todo conjunto de atividade incomum deve ser tratado o mais rápido possível pelo time assim que identificado e os alertas emitidos. Algumas atividades importantes dessa fase são:

✓ Elabore um processo de identificação do incidente, para que seja determinado se ele é realmente um incidente de segurança.

✓ Determine quais são as fontes de detecção que a empresa possui. Identifique como os incidentes atuais são detectados e relatados, quem executa funções como gerenciamento de vulnerabilidades, avaliações de risco, monitoramento e controle de rede. As fontes de detecção podem ser humanas, internas e externas.

✓ Elabore uma tabela de triagem/fluxo a ser seguido após um incidente confirmado. Essa tabela servirá de guia para que seus colaboradores saibam como agir e quais passos devem ser seguidos. Dessa forma, ela contribuirá para uma resposta mais rápida, eficiente e adequada ao incidente.

✓ Elabore um fluxo de escalonamento de incidentes, de acordo com o tipo e a criticidade, a fim de que a equipe possa usá-lo durante o processo.

✓ Cada incidente possui um tipo de resposta inicial a ser adotado de acordo com a sua criticidade. Desse modo, inclua na sua tabela de triagem as possíveis respostas, de acordo com o incidente. Os tipos de respostas são:

- **Resposta técnica**: em que uma equipe técnica, com foco em resolver o incidente, analisa informações, como o código malicioso e maneiras de mitigar o incidente, assim como o de recuperar o ambiente. Atua também na erradicação, ou seja, na eliminação/limpeza dos arquivos maliciosos.

- **Resposta administrativa**: deve garantir que as diversas áreas atuem em conjunto e em sinergia com o fluxo de respostas do incidente.

- **Resposta legal**: ações relacionadas à investigação, à privacidade, a processos, à imagem etc.

5.3 Contenção

Há dois tipos de contenção: curta e longa. A de curto prazo tem a característica de ser uma resposta imediata, a fim de impedir que o ataque cause danos. Já a contenção de longo prazo abrange o restabelecimento do sistema à sua produção normal após a neutralização dos backdoors e arquivos maliciosos que viabilizaram o ataque. Algumas atividades importantes dessa fase são:

- ✓ Focar em ações rápidas e imediatas, de forma a retirar o acesso indevido ou limitar a extensão de um ataque.
- ✓ Manter a integridade das evidências para a devida cadeia de custódia forense.
- ✓ Ter em mãos os modelos de comunicações interna e externa, para estas serem utilizadas no caso de um incidente, visando à comunicação imediata aos principais envolvidos internos e externos, de modo que estes ajam assim que forem recebidas essas comunicações. Ações como essa podem evitar que o incidente se alastre ainda mais.

5.4 Erradicação

Esta fase é fundamental para a continuidade dos negócios. Ela visa restaurar todos os sistemas corporativos afetados por um incidente de segurança. Isso se dá por meio da aplicação do plano de resposta a incidentes, removendo qualquer vestígio do ataque. A atualização constante dos sistemas e medidas corretivas são essenciais para evitar a repetição da mesma situação. Algumas atividades importantes dessa fase são:

- ✓ Garantir a eliminação da causa-raiz do problema.
- ✓ Analisar o que deve ser realizado, para garantir a continuidade dos negócios.
- ✓ Corrigir os sistemas afetados e fazer as atualizações necessárias.
- ✓ Nem sempre essa fase deve ocorrer antes da fase de recuperação. Às vezes, ambas acontecem juntas.

5.5 Recuperação

A recuperação aborda como trazer todo o sistema a seu funcionamento padrão. Nesse momento é preciso fazer uma varredura para averiguar se não houve perdas e como recuperar possíveis dados perdidos. Isso envolve cópias de segurança armazenadas em um sistema em nuvem para restabelecer todas as informações necessárias para o fluxo de trabalho. Algumas atividades importantes dessa fase são:

- ✓ Focar esforços para restaurar os sistemas afetados, garantindo sua integridade.
- ✓ Desenvolver processo de reativação dos ambientes afetados, nos quais constem a ordem correta dos processos/sistemas a serem disponibilizados novamente.
- ✓ Retornar os sistemas afetados ao ambiente de produção somente após testes e validações, para garantir que nenhuma ameaça permaneça.
- ✓ Instalar os patches e atualizações nos sistemas de segurança, roteadores e firewalls.

- ✓ Reinstalar sistemas operacionais de máquinas afetadas.
- ✓ Alterar senhas de usuários e administradores locais dos equipamentos afetados e, caso identificado o uso de credenciais privilegiadas, estas devem ser bloqueadas.
- ✓ Realizar scan de vulnerabilidades em todas as máquinas afetadas ANTES de conectá-las novamente na rede.
- ✓ Monitorar de perto os sistemas, após reconectados à rede.
- ✓ Realizar pentestes nos sistemas afetados ou explorados pela ameaça.
- ✓ Restaurar sistemas utilizando backups íntegros e não afetados pelo incidente.

5.6 Lições aprendidas

Esta fase aborda a documentação das ocorrências de incidentes e os procedimentos de resposta a eles. Dentro disso, a empresa consegue criar um material com o histórico de ocorrências contra a segurança e as devidas ações tomadas, tornando a organização mais preparada para lidar com transtornos futuros. Algumas atividades importantes dessa fase são:

- ✓ Realizar o registro de lições aprendidas com todos os envolvidos nos ciclos de resposta a incidentes, de modo a atualizar o plano com possíveis melhorias encontradas.
- ✓ Analisar se é possível achar a causa-raiz dos incidentes em comum.
- ✓ Elaborar um modelo de relatório para ser utilizado com template, para que perguntas estratégicas sejam respondidas.
- ✓ Elaborar um relatório de fechamento do incidente. Esse deve conter:

- quem elaborou o relatório;
- qual foi o incidente;
- detalhes do incidente;
- detalhes das consequências;
- detalhes das ações tomadas;
- como foi o processo de recuperação;
- processo de revisão;
- lições aprendidas;
- plano de melhorias a serem aplicadas.

✓ Verificar a necessidade de treinar funcionários, terceiros, fornecedores e pessoas envolvidas no plano, para que o erro do incidente não ocorra novamente.

✓ Elaborar um exercício de lições aprendidas e atualize o plano de resposta a incidentes com as informações relevantes.

6 GESTÃO DE INCIDENTES SEGUNDO A LGPD

O art. 47 da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) determina que os agentes de tratamento de dados pessoais devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais. Para o cumprimento desses requisitos, os Controladores e Operadores devem:

- Avaliar internamente o incidente – natureza, categoria e quantidade de titulares de dados afetados, consequências concretas e prováveis.
- Comunicar ao Encarregado de Dados (art. 5º, VIII da LGPD);

- Comunicar ao Controlador, se você for o Operador;
- Comunicar à ANPD e ao titular de dados, em caso de risco ou dano relevante aos titulares (art. 48 da LGPD); e
- Elaborar documentação com a avaliação interna do incidente, medidas tomadas e análise de risco, para fins de cumprimento do princípio de responsabilização e prestação de contas (art. 6º, X da LGPD).

A Autoridade Nacional de Proteção de Dados (ANPD) anunciou o início do processo de regulamentação e notificação de incidentes de segurança que possam acarretar risco ou dano relevante a titulares de dados pessoais, bem como publicou o formulário de comunicação dos referidos incidentes. Os detalhes podem ser vistos em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca.

Dentre as orientações trazidas pela ANPD, destaca-se o prazo de **dois dias** úteis a contar da ciência do incidente de segurança, como tempo considerado razoável (texto escrito na lei) para a sua comunicação pelos controladores de dados pessoais.

De acordo com a ANPD, o cuidado deve ser redobrado quando o incidente envolver dados sensíveis ou de pessoas em situação de vulnerabilidade, dentre as quais crianças e adolescentes, e também para casos que potencialmente possam ocasionar danos materiais ou morais, como discriminação, violação do direito de imagem e/ou reputação, fraudes financeiras e roubos de identidade. Serão levados em consideração a quantidade de titulares e de dados envolvidos no incidente, a boa-fé e intenções dos terceiros que tiveram acesso aos dados em razão do incidente e a facilidade de identificação dos titulares por terceiros não autorizados.

A comunicação deve ser feita por meio de formulário eletrônico disponibilizado no próprio site da ANPD e enviada através do Peticionamento Eletrônico – Usuário Externo (SEI). É importante que o DPO da empresa faça o seu cadastro em: https://www.gov.br/secretariageral/pt-br/sei-peticionamento-eletronico.

A partir do momento que a empresa identifica um incidente, seja por meio de um colaborador, de seus monitoramentos ou pela repercussão ou impacto do ocorrido, os times de Segurança da Informação e Resposta a Incidentes devem ser imediatamente

acionados e iniciar o plano de contenção, recuperação e investigação sobre o ocorrido. Da mesma forma, tão logo seja identificado qualquer risco ou suspeita de vazamento de dados pessoais, o Encarregado de Dados (DPO) e o Comitê de privacidade devem ser comunicados e integrar o time de Resposta a Incidentes, juntamente com o Departamento de Tecnologia da Informação e o Departamento Jurídico.

O colaborador que identificou o incidente deve seguir as orientações dos responsáveis, pois a adoção de medidas por conta própria pode agravar o problema ou danificar evidências do Incidente com Dados Pessoais. Ainda, é importante manter sigilo sobre a comunicação recebida, pois tornar a informação pública pode prejudicar a investigação do suposto Incidente.

Se for o caso, empresa realizará a comunicação do Incidente com Dados Pessoais à ANPD, com base nas análises técnicas e jurídicas realizadas pela área de Tecnologia da Informação, pelo Comitê de Privacidade e pelo Departamento Jurídico. A empresa deve aprovar e autorizar a divulgação de comunicado, aos titulares envolvidos no Incidente com Dados Pessoais, validar e assinar quaisquer comunicados ao público, imprensa e clientes, orientar e/ou informar as equipes interessadas a respeito das práticas a serem adotadas com relação ao Incidente com Dados Pessoais, coordenar todas as ações decorrentes do Incidente com Dados, com o intuito de mitigar os impactos percebidos, demais autoridades competentes e os Clientes, supervisionando os contatos e comunicações junto ao público, decorrentes do Incidente com Dados Pessoais, dentre outras atividades.

Para que a plano seja efetivo, é importante que a empresa estabeleça meios para a criação tempestiva de um comitê de crise com áreas de negócio que possam realizar reuniões periódicas de acompanhamento. Esse comitê poderá ser acionado extraordinariamente quando um incidente for identificado. Isso é fundamental para a tomada de decisões estratégicas inerentes aos procedimentos de contensão e recuperação do ambiente, bem como avaliação e investigação da extensão do incidente, bem como a divisão de tarefas e atribuição de responsabilidade na tratativa do vazamento de dados.

Sugere-se que o comitê de crise seja formado por gestores de áreas mais importantes da empresa como segurança da informação, tecnologia (infraestrutura, banco

de dados, sistemas etc.), encarregado de dados, jurídica, equipe de riscos, compliance, relações com investidores, comunicação externa, consultores independentes etc.

Somente com a criação do comitê e gestão coordenada do plano de resposta, os procedimentos de contensão e recuperação – essenciais para continuidade do negócio, poderão ser realizados sem prejuízo para os procedimentos de avaliação e investigação – essenciais para correto mapeamento e mensuração do dado e reporte para os órgãos competentes.

Instaurado o comitê, é importante estabelecer os passos a serem seguidos quando um incidente for identificado. Sugere-se a adoção do framework da NIST (National Institute of Standards and Technology) que sugere que tenha: (i) planejamento – quais ferramentas estão ativas para evitar que o incidente ocorra; (ii) detecção e análise – se ocorrido o incidente, como foi identificado e como será feita a análise inicial; (iii) contenção, erradicação e recuperação – depois de identificado, conter o vazamento, para que seja erradicado e os dados que foi possível ser recuperado; e, (iv) ações pós-incidentes – lições aprendidas, aplicar melhorias na empresa para evitar novos incidentes.

O processo a seguir descreve as atividades que devem ser executadas para gerenciamento de um incidente de segurança da informação.

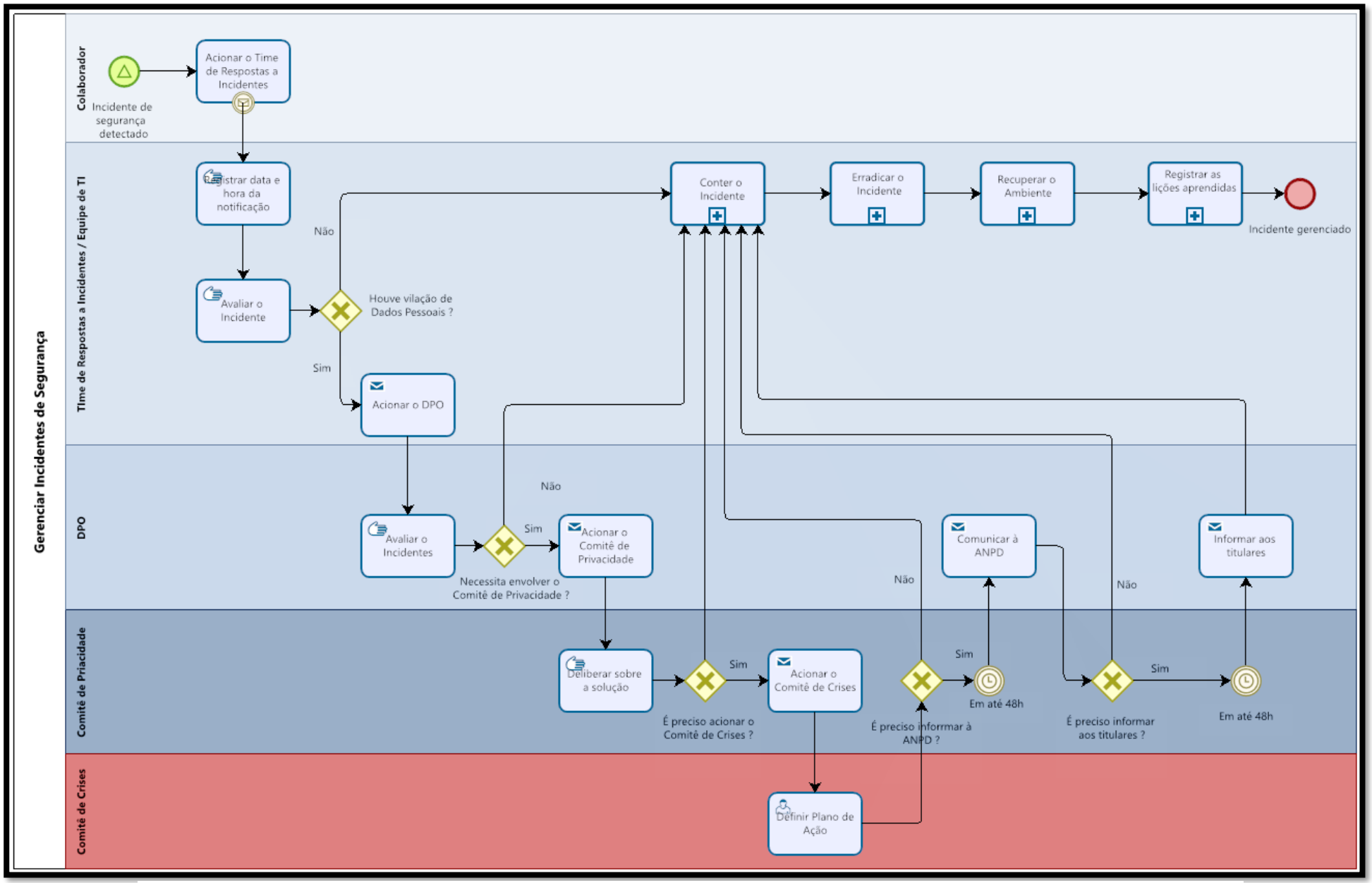

Figura 4 - Processo de gestão de incidentes.

7 CONCLUSÃO

O número de incidentes de segurança da informação e privacidade que acometem as empresas a cada dia está crescendo exponencialmente. É extremamente importante que as empresas implantem todos os controles necessários para a redução da probabilidade e impacto da materialização dos riscos de ocorrência desses eventos de segurança. Tendo a consciência que não existem sistemas 100% seguros, é necessário estar preparado para agir em caso de um problema como esses. Para isso, criar um sistema de gerenciamento de incidentes eficaz passa a ser mais importante do que apenas cumprir um requisito de conformidade com a LGPD. Esse sistema deve proteger a privacidade dos dados pessoais tratados pela empresa e a sua imagem perante a sociedade, no tocante co cuidado com a segurança e privacidade dos cidadãos.

8 REFERÊNCIAS

- NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations
- NIST SP 800-83, Guide to Malware Incident Prevention and Handling
- NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
- NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response
- NIST SP 800-92, Guide to Computer Security Log Management
- NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS)
- NIST SP 800-115, Technical Guide to Information Security Testing and Assessment
- NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems
- NIST SP 800-61 r2, Computer Security Incident Handling Guide
- ISO / IEC 27035: Information technology — Security techniques — Information security incident management
- https://www.zurich.com.br/-/media/project/zwp/brazil/docs/risk-engineering-landing-page/seguranca-ocupacional/plano-de-resposta-a-incidentes-irp.pdf
- https://www.gov.br/conarq/pt-br/assuntos/noticias/guias-operacionais-para-adequacao-a-lgpd