PLANO DE RESPOSTAS A INCIDENTES DE SEGURANÇA EM DADOS PESSOAIS LABORATÓRIO SÃO GERALDO

ÍNDICE

CONTEXTUALIZAÇÃO

A Lei nº 13.709/2018, Lei Geral de Proteção de Dados – LGPD, tem como um de seus pilares centrais a implementação de medidas de Segurança da Informação que podem trazer às entidades públicas e privadas, uma cultura de maior conscientização na área. A LGPD considera que, mais grave do que sofrer um ataque ou passar por um vazamento de dados, é não se prevenir e nem adotar as medidas e práticas necessárias e possíveis para a proteção dos seus dados e de todos os que são afetados por eventuais acessos não autorizados.

A atividade de conformidade com as disposições da Lei Geral de Proteção de Dados (LGPD) não se limita à implementação de medidas tecnológicas e padrões de segurança. Abrange também a elaboração, manutenção e revisão de documentos que não apenas asseguram a conformidade com a mencionada lei, mas também contribuem para uma maior organização e otimização dos processos internos. Além disso, essas medidas visam proteger a entidade, sua reputação, seus servidores, usuários dos serviços prestados e parceiros.

Na Era Tecnológica, onde os computadores pessoais são amplamente populares e o acesso à internet é facilmente alcançável, observamos uma crescente dependência de processos digitais para a manutenção de modelos de negócios e o cumprimento de obrigações legais. Embora a informatização desses processos proporcione praticidade, redução de custos e economia de tempo, ela também acarreta riscos de segurança que não podem ser negligenciados. Com tempo e recursos adequados, qualquer sistema pode ser vulnerável a comprometimentos.

Considerando esses aspectos, torna-se essencial a elaboração de estratégias e planos para o controle de danos, destacando a importância dos Planos de Respostas a Incidentes de Segurança em Dados Pessoais. Incidente de segurança é definido como uma violação da segurança que, de modo acidental ou ilícito, resulta na destruição, perda, alteração, divulgação ou acesso não autorizados a dados pessoais transmitidos, armazenados ou sujeitos a qualquer outro tipo de tratamento.

A Resposta a Incidentes é o processo que delineia como uma organização deve lidar com incidentes de segurança, seja um ataque cibernético, violação de dados, presença de aplicativos maliciosos (como vírus) ou violações das políticas e padrões de segurança da

entidade, entre outros. O objetivo é minimizar os danos causados pelo incidente, reduzir o tempo de ação e os custos de recuperação.

O Plano de Respostas a Incidentes (PRI) constitui um documento interno que deve ser amplamente familiarizado por todos os servidores, funcionários e colaboradores. Ele detalha as medidas a serem adotadas no caso de um Incidente de Segurança em Dados Pessoais. O LABORATÓRIO SÃO GERALDO, sendo uma entidade de direito privado, especialmente no âmbito de saúde, deve observar cuidados adicionais devido à legislação que confere proteção diferenciada aos dados sensíveis, incluindo os dados de saúde, com bases legais específicas para seu tratamento (art. 11).

Nesse contexto, o Plano de Respostas a Incidentes (PRI) do LABORATÓRIO SÃO GERALDO visa orientar a organização na resposta eficiente a situações de emergência e exceção, garantindo a integridade dos sistemas, a proteção de informações e a privacidade dos titulares de dados.

OBJETIVO, ABRANGÊNCIA E VIGÊNCIA DO PLANO DE RESPOSTAS A INCIDENTES (PRI) DO LABORATÓRIO SÃO GERALDO

O propósito fundamental deste Plano é guiar o LABORATÓRIO SÃO GERALDO na resposta à situações de emergências e exceção, de maneira documentada, formal, ágil e confiável. Além disso, visa preservar as evidências que possam contribuir para prevenir novos incidentes e cumprir as exigências legais de comunicação e transparência.

Dentro deste Plano de Respostas a Incidentes (PRI), serão definidas as funções e responsabilidades tanto individuais quanto de equipes. Serão também delineadas as medidas a serem implementadas para assegurar que o LABORATÓRIO SÃO GERALDO responda de maneira apropriada a um incidente, mantendo sempre o compromisso com a integridade dos sistemas/processos, proteção de informações e privacidade dos titulares, a fim de garantir a confiabilidade contínua dos serviços oferecidos.

Este PRI é aplicável em qualquer caso de incidentes envolvendo Dados Pessoais e deve ser seguido em conjunto com outras políticas do LABORATÓRIO SÃO GERALDO por todas as áreas, colaboradores e prestadores de serviços que possam ter acesso às informações, arquivos e dados sob a responsabilidade da entidade.

A entrada em vigor do PRI do LABORATÓRIO SÃO GERALDO ocorrerá na data de sua publicação, permanecendo em vigor por tempo indeterminado. Este plano pode ser revisado e alterado conforme necessário, sempre que houver identificação de tal necessidade.

TERMOS E DEFINIÇÕES

- Agentes de Tratamento: Representa a união do controlador, responsável pelas decisões sobre o tratamento de dados, e do operador, que realiza efetivamente o tratamento. Importante notar que servidores ou equipes de trabalho não são considerados controladores ou operadores, uma vez que atuam sob a direção do agente de tratamento.
- Anonimização: Refere-se à aplicação de meios técnicos que, de maneira razoável e disponível, tornam um dado incapaz de ser associado, direta ou indiretamente, a um indivíduo. Esse processo contribui para a privacidade e segurança dos dados.
- Ataque: Trata-se de um evento onde vulnerabilidades são exploradas. Pode ocorrer quando um atacante busca realizar ações maliciosas, como invadir sistemas, acessar informações confidenciais ou tornar um serviço inacessível. A prevenção e detecção de ataques são essenciais para a segurança da informação.
- Autoridade Nacional de Proteção de Dados - ANPD: Órgão da administração pública nacional encarregado de fiscalizar e garantir o cumprimento da Lei Geral de Proteção de Dados em todo o território nacional. Sua atuação é fundamental para assegurar a conformidade das organizações com as normas de proteção de dados.
- Controlador: Refere-se a pessoa física ou jurídica, de direito público ou privado, que toma decisões relacionadas ao tratamento de dados pessoais. É o responsável pela definição dos propósitos e meios do tratamento, assumindo a liderança nas práticas de privacidade.
- Dados Pessoais: Englobam qualquer informação relacionada a um indivíduo que possa ser utilizada para identificá-lo, direta ou indiretamente. Inclui dados como nome, endereço, telefone, entre outros, sendo essencial seu tratamento com respeito à privacidade.
- Dados Pessoais Sensíveis: Consistem em informações que abordam a origem racial ou étnica, convicção religiosa, prática ou orientação sexual, dados médicos ou de saúde,

informações genéticas ou biométricas, crenças políticas ou filosóficas, filiação política ou sindical, número do seguro social, número da carteirinha do plano de saúde e dados bancários. Esses dados demandam cuidados especiais devido à sua natureza mais sensível.

- Encarregado ou Data Protection Officer (DPO): Pessoa física designada pelo controlador para garantir a conformidade com a legislação de proteção de dados. Atua como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).
- GT LGPD LABORATÓRIO SÃO GERALDO: Grupo de Trabalho estabelecido pela Portaria P nº 55/2020 com o propósito de implementar as disposições da Lei Geral de Proteção de Dados. Contribui para a aplicação efetiva dos princípios e normas da LGPD no contexto específico do LABORATÓRIO SÃO GERALDO.
- Incidente: Refere-se a qualquer ato, suspeita, ameaça ou circunstância que comprometa a confidencialidade, integridade ou disponibilidade de informações em posse do LABORATÓRIO SÃO GERALDO ou que ela venha a ter acesso. A identificação e resposta rápida a incidentes são cruciais para a segurança da informação.
- IP (Protocolo da Internet): Número utilizado para identificar dispositivos de tecnologia da informação em uma rede ou Internet. Essa identificação é fundamental para o roteamento eficiente de dados, sendo parte integrante da comunicação na internet.
- LGPD: Sigla que identifica a Lei Geral de Proteção de Dados, Lei nº 13.709/2018, que estabelece regras e princípios para o tratamento de dados pessoais no Brasil. Sua implementação é crucial para garantir a proteção da privacidade e segurança dos dados.
- Log: Processo de registro de eventos relevantes em um sistema computacional. A análise de logs é uma prática essencial para a detecção de atividades suspeitas e manutenção da integridade dos sistemas.
- Operador: Pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados em nome do controlador. Essa distinção é importante para definir as responsabilidades e obrigações de cada parte envolvida no tratamento de dados.

- Sistemas: Compreendem hardware, software, rede de dados, armazenador de mídias e outros componentes utilizados pelo LABORATÓRIO SÃO GERALDO para apoiar suas atividades. O controle e proteção desses sistemas são cruciais para a segurança da informação.
- Tratamento: Refere-se a qualquer operação ou conjunto de operações efetuadas sobre os dados, incluindo coleta, gravação, organização, estruturação, alteração, uso, acesso, divulgação, cópia, transferência, armazenamento, exclusão, combinação, restrição, adaptação, recuperação, consulta, destruição ou anonimização. O tratamento adequado assegura a conformidade com a legislação de proteção de dados.
- Vazamento de Dados: Consiste em qualquer quebra de sigilo ou disseminação de dados que pode resultar, criminosamente ou não, na perda, alteração, compartilhamento, acesso, transmissão, armazenamento ou processamento não autorizado de dados. A prevenção e resposta eficaz a vazamentos são essenciais para proteger a privacidade dos indivíduos e a integridade dos dados.
- Violação de Privacidade: Refere-se a qualquer violação à legislação aplicável ou conduta e evento que resulte na destruição acidental ou ilícita dos dados, bem como na sua perda, roubo, alteração, divulgação ou acesso não autorizado, danos ou desvio de finalidade em seu tratamento. A prevenção e gestão de violações são fundamentais para a preservação da confiança e integridade dos dados pessoais.
- Vírus: Programa ou parte de um programa de computador, geralmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos. A detecção e proteção contra vírus são essenciais para a segurança dos sistemas de informação.

ATORES E RESPONSABILIDADES

Cada departamento dentro da estrutura organizacional do LABORATÓRIO SÃO GERALDO assume responsabilidades específicas ao lidar com a ocorrência ou mesmo a

suspeita de um incidente, sendo imperativo comunicar imediatamente a incidência ao Time de Resposta do LABORATÓRIO SÃO GERALDO. As funções designadas para este propósito são as seguintes:

- Notificador: Esta entidade pode ser uma pessoa ou um sistema de monitoramento encarregado de comunicar a detecção do incidente.
- Acionador(es): Responsável por receber as notificações e conduzir o tratamento inicial, realizando a triagem do incidente.
- Time de Resposta a Incidentes (TRI): Este grupo é composto por colaboradores do LABORATÓRIO SÃO GERALDO que possuem habilidades, acesso, responsabilidades, treinamento e conhecimentos necessários para responder a uma variedade de incidentes. O TRI é designado de acordo com as características específicas de cada incidente e inclui o Encarregado de Dados (DPO) e servidores de outras áreas com especialização no tema ou cujos processos tenham sido impactados pelo incidente.
- Responsável por Sistema: Indivíduo capacitado a propor soluções de resposta, além de autorizar ou vetar procedimentos de emergência relacionados ao sistema afetado.
- Responsável por Processo ou Negócio: Gerente ou chefe de setor identificado na estrutura organizacional, com a capacidade de sugerir soluções de resposta a serem avaliadas pelo TRI.
- GT LGPD LABORATÓRIO SÃO GERALDO: Esta é a principal instância decisória no que diz respeito ao tratamento de Dados Pessoais no LABORATÓRIO SÃO GERALDO. O GT LGPD responde diretamente ao Presidente e desempenha um papel fundamental na definição das estratégias e ações relacionadas à proteção de dados.

MACRO ETAPAS DO PROCESSO

Este Plano de Resposta a Incidentes segue uma estrutura organizada, abordando as seguintes macroetapas:

Identificação:

A detecção eficaz de qualquer Incidente de Segurança é crucial para a implementação bem-sucedida do Plano de Respostas. Medidas essenciais, como ferramentas de monitoramento, registros de eventos, mensagens de erro em firewalls, entre outras, devem estar disponíveis. Além disso, é vital sensibilizar e capacitar proativamente servidores, funcionários e colaboradores para identificar e relatar possíveis vazamentos de dados.

Preparação:

A resposta a um incidente requer decisões rápidas e execução ágil. Dada a margem estreita para erros, a prática regular de procedimentos de emergência e a medição dos tempos de resposta são cruciais. Essa abordagem permite desenvolver uma metodologia que promove agilidade e precisão, minimizando o impacto da falta de recursos e os danos potenciais causados pelo comprometimento de sistemas e processos.

Contenção:

Após a identificação de um incidente, é imperativo contê-lo e, se necessário, isolá-lo para evitar impactos adicionais em outros sistemas e processos. Esta etapa inclui medidas de contenção de curto prazo, backup do sistema, contenção a longo prazo, entre outras. Durante essa fase, a documentação e registro do incidente devem ocorrer simultaneamente, evitando a destruição ou perda de evidências.

Erradicação:

Após a contenção da ameaça, a próxima etapa envolve a remoção da ameaça e a restauração dos sistemas/processos afetados ao estado original anterior ao incidente.

Recuperação:

Nesta etapa, os sistemas/processos afetados passam por testes e validações antes de retornar ao ambiente de produção ou ao fluxo normal, assegurando que nenhuma ameaça persista.

Preceitos assimilados (Lições aprendidas):

Esta etapa visa atualizar o Plano de Respostas a Incidentes com as ações realizadas, contribuindo para o aprendizado da equipe e facilitando futuras intervenções em incidentes.

Documentação do Incidente:

O incidente deve ser documentado de forma abrangente, incluindo todas as ações implementadas nas etapas anteriores e as lições aprendidas.

Comunicações:

A ocorrência de incidentes de segurança com potencial risco ou dano significativo aos titulares deve ser comunicada à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular afetado. Dependendo da situação, as informações à ANPD podem ser fornecidas por meio de solicitações, comunicações ou auditorias, com o objetivo principal de demonstrar a conformidade (ou intenção de conformidade) da Entidade com as exigências da lei.

DESCRIÇÃO DO PROCESSO

Início/Detecção

1. A notificação de um novo incidente ocorre quando uma pessoa, interna ou externa ao LABORATÓRIO SÃO GERALDO, comunica a ocorrência ou quando um alarme da monitoração é acionado. A comunicação inicial do incidente pode se originar de diversas fontes, como e-mails, telefonemas e sistemas internos (incluindo notificações feitas pelo Encarregado no caso de notificação pelo titular dos dados pessoais). É imperativo registrar todas essas comunicações diretamente por meio do Notificador.

Triagem

2. A notificação é recebida pelo Acionador, que desempenha o papel de Encarregado de Dados do LABORATÓRIO SÃO GERALDO. Nessa fase, o Acionador realiza uma avaliação preliminar do incidente e determina se é necessário formar um Time de Resposta a Incidentes (TRI) para conduzir a avaliação. Notificações sem relevância ou claramente improcedentes são descartadas. Se a formação do TRI não for necessária, o Acionador assume as fases subsequentes descritas no fluxo do processo que, de outra forma, seriam de responsabilidade do TRI.
3. Durante a avaliação preliminar, busca-se obter informações sobre os sistemas/processos supostamente impactados, avalia-se a criticidade, identificam-se os danos aparentes e avalia-se o risco de a situação se agravar sem uma resposta imediata.

4. Com base na avaliação preliminar, incidentes que não envolvem sistemas online e que não apresentam riscos significativos pela falta de ação imediata podem ser encaminhados para os trâmites regulares dos setores pertinentes da Autarquia.

Avaliação

Nesta etapa, inicia-se uma avaliação mais aprofundada do incidente pelo DPO/TRI, classificando-o e determinando sua criticidade.

A criticidade do incidente pode ser categorizada de acordo com as seguintes classificações:

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.

Sensibilidade dos Dados Pessoais afetados	
Criticidade	Descrição
Alta	Dados Pessoais de crianças/ adolescentes, dados Pessoais Sensíveis ou que possam gerar discriminação ao titular.
Média	Dados Pessoais imediatamente identificáveis (Ex.: nome, e-mail, CPF, endereço), combinados, ou não, com informações comportamentais (Ex.: histórico de atividades, preferências).

Baixo	Volume de Dados Pessoais afetado inferior a 2% da base de dados da Controladora.

Baixa	Dados anonimizados, Dados Pessoais pseudonimizados (desde que a chave de desanonimização também não tenha sido comprometida), Dados Pessoais de difícil identificação (Ex.: IP)

5. Na busca pela identificação do incidente, é imperativo investigar a causa subjacente, os agentes envolvidos, suas ações, bem como as vulnerabilidades exploradas. Este processo visa estabelecer as bases para as fases subsequentes, exigindo, se necessário, a participação de especialistas dos setores afetados. O DPO/TRI, a seu critério e viabilidade, pode optar por envolver especialistas a qualquer momento durante essa investigação.

Contenção, Erradicação e Recuperação

6. Os responsáveis pelos sistemas/processos afetados devem ser notificados para fornecerem suas considerações sobre os procedimentos de resposta, contenção e erradicação.
7. O propósito das ações de contenção e erradicação é mitigar os danos, isolando os sistemas afetados para prevenir danos adicionais. Nesse estágio, se necessário e de acordo com as devidas autorizações, pode ocorrer o desligamento de sistemas completos ou de funcionalidades específicas, com a divulgação de avisos de indisponibilidade para manutenção. Todas as precauções devem ser tomadas para não comprometer evidências cruciais que possam ser utilizadas para identificar a autoria, origem e métodos empregados na violação de segurança.
8. Em incidentes que envolvam máquinas virtuais, recomenda-se realizar snapshots (registros do estado de um arquivo, aplicação ou sistema em um determinado ponto no tempo) para análises subsequentes.
9. Caso o incidente não esteja relacionado a recursos computacionais, mas principalmente a atividades humanas, os procedimentos podem incluir sindicância administrativa, processo administrativo disciplinar, ou outras medidas previstas na legislação aplicável ao caso.

10. O processo de recuperação compreende um conjunto de medidas destinadas a restaurar os serviços integralmente, podendo ocorrer de maneira gradual, conforme a viabilidade e decisão do responsável pelo sistema/processo.
11. Pode ser necessário desenvolver e implementar atualizações de aplicativos ou do sistema operacional, além da elaboração de novas rotinas processuais.

Comunicações

12. Logo que possível, a situação deve ser encaminhada para análise do GT LGPD do LABORATÓRIO SÃO GERALDO a fim de avaliar se houve risco ou dano relevante aos titulares dos dados pessoais impactados.
13. Caso o GT LGPD do LABORATÓRIO SÃO GERALDO conclua que o incidente acarretou risco ou dano relevante aos titulares de dados pessoais, o Encarregado de Dados (DPO), possivelmente assessorado pela Assessoria de Comunicação (ASCOM), deverá realizar as comunicações obrigatórias por lei. Tais comunicações podem englobar agradecimentos ao notificador, informações aos titulares de dados e à imprensa, além de relatórios formais enviados à ANPD.

Preceitos assimilados

14. Após o incidente contido e sua resolução encaminhada, o DPO/TRI deve agendar e liderar uma reunião de lições aprendidas, convidando participantes a seu critério. O objetivo é discutir os erros e desafios enfrentados, além de propor aprimoramentos para os sistemas e processos, incluindo este Plano de Resposta a Incidentes.
15. As melhorias sugeridas durante a reunião serão encaminhadas ao GT LGPD do LABORATÓRIO SÃO GERALDO para deliberação sobre a adoção.

Documentação

16. O DPO/TRI deve documentar o incidente em uma base de conhecimento apropriada, detalhando informações obtidas, linha do tempo, participantes, evidências, conclusões, decisões, autorizações e ações executadas, incluindo as da reunião de lições aprendidas.
17. Após a neutralização da ameaça, o Encarregado de Dados (DPO) deve preparar um relatório circunstanciado abordando todas as medidas adotadas. Este relatório incluirá informações relevantes sobre o incidente, como sua identificação, natureza, danos ou potenciais danos causados, a extensão, relevância e repercussão desses danos, entre

outros. Além disso, abrangerá providências para preservação de evidências, procedimentos para contenção da crise, medidas técnicas e de governança corretivas, questionamentos e demandas externas (requerimentos de titulares de dados, autoridades e imprensa, com suas respectivas respostas) e deliberações do TRI e do GT LGPD do LABORATÓRIO SÃO GERALDO.

Observações complementares

Paralelamente à execução do Plano de Respostas a Incidentes, diversas ações devem ser desenvolvidas, antes, durante e depois da ocorrência de um incidente, conforme:

Durante o incidente - Identificação, coleta e preservação das evidências:

Durante o incidente, destaca-se a importância da identificação, coleta e preservação das evidências. Essa abordagem visa garantir que a Entidade possua elementos úteis ou necessários para demonstrar às autoridades a adoção de uma resposta apropriada, evidenciando a seriedade no tratamento do incidente.

No contexto da LGPD e da ANPD, as medidas tomadas para conter o incidente e seus danos podem ser cruciais para minimizar sanções e multas aplicadas ao caso específico. Além disso, essas evidências desempenham um papel fundamental na identificação e responsabilização do usuário responsável pelo vazamento de dados pessoais. Decisões na União Europeia relacionadas à GDPR (Regulamentação Geral de Proteção de Dados da União Europeia) enfatizam que, mais do que o incidente em si, o desprezo por parte da organização é considerado mais grave.

Após o incidente - Elaboração de relatório final do incidente e revisão dos procedimentos:

Após o incidente, a elaboração de um relatório final torna-se essencial. Esse relatório não apenas comprova as medidas implementadas pela Entidade, mas também possibilita compreender as causas do incidente, avaliar a aderência e efetividade do Plano de Respostas a Incidentes, além de analisar a atuação dos responsáveis.

No que diz respeito à Comunicação de Incidente de Segurança, conforme previsto na LGPD e com conteúdo mínimo definido no artigo 48, são considerados aspectos essenciais a serem abordados.

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.

I – a descrição da natureza dos dados pessoais afetados;

Não é suficiente categorizar os dados pessoais como convencionais (conforme definido no artigo 5º, I) ou sensíveis (conforme definido no artigo 5º, II). É imperativo listar com precisão as categorias específicas de dados, tais como contas de e-mail, informações de cartão de crédito, senhas, dados de geolocalização, entre outros. Essa abordagem visa proporcionar ao titular uma compreensão mais detalhada, mesmo que estimada, dos riscos existentes ou dos danos potenciais associados aos seus dados.

II – as informações sobre os titulares envolvidos;

Trata-se da descrição, seja ela precisa ou estimada, que identifica quais e quantos titulares foram impactados.

III – a indicação das medidas técnicas e de segurança utilizadas para a proteção;

A Lei Geral de Proteção de Dados (LGPD), conforme estabelecido no artigo 46, requer que os agentes de tratamento, incluindo controladores e operadores, implementem medidas de segurança, tanto técnicas quanto administrativas, para salvaguardar os dados pessoais. É essencial que essas medidas sejam detalhadamente descritas, evidenciando o comprometimento da entidade com a conformidade legal. Vale ressaltar que essa descrição abrangente pode encontrar limitações, especialmente no que diz respeito aos segredos comerciais e industriais, os quais devem ser resguardados em prol da preservação dos interesses comerciais. Em determinadas situações, a descrição de medidas de segurança específicas pode ser omitida, especialmente quando existe o risco de repetição do incidente, seguindo a abordagem conhecida como "segurança por obscuridade" (Security Through Obscurity - STO). Essa técnica visa privar potenciais adversários ou atacantes de informações que possam ser utilizadas para comprometer a organização.

IV – os riscos relacionados ao incidente;

Trata-se de uma análise prospectiva do incidente, levando em consideração, principalmente, os itens I e II. Poderá mencionar, também, os danos que já ocorreram, como a destruição ou codificação de dados.

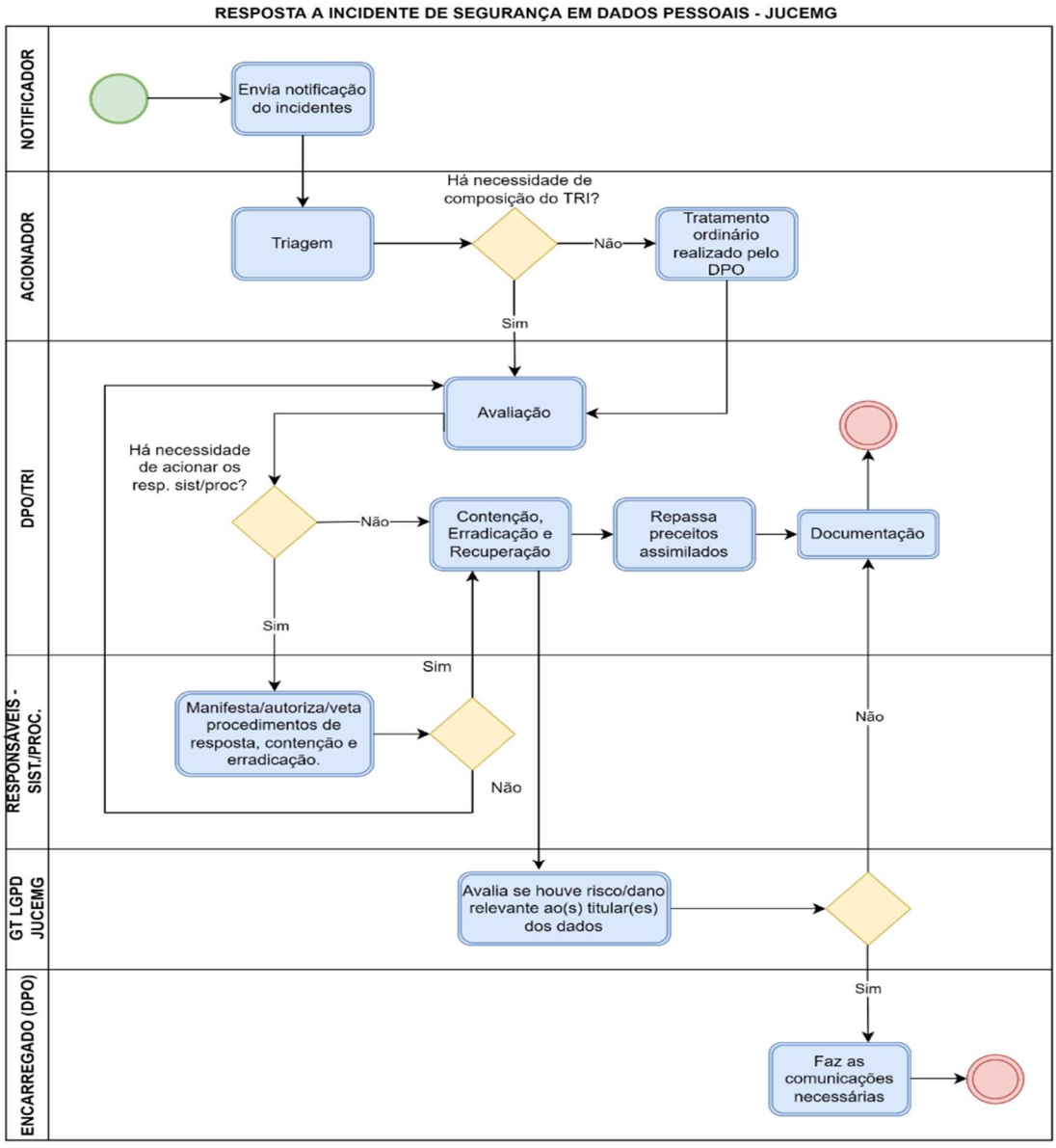
V – os motivos da demora, no caso de a comunicação não ter sido imediata;

A justificativa, devidamente fundamentada, para a não apresentação imediata da notificação pode decorrer, por exemplo, da complexidade e extensão do incidente, incluindo o número de titulares afetados e a quantidade de dados envolvidos.

VI – as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Neste contexto, é fundamental mencionar, de forma clara e objetiva, sem exagero de expressões técnicas, as condutas que foram e serão implementadas para eliminar ou minimizar os efeitos do incidente. Isso pode incluir ações como o contato com as autoridades policiais, a determinação de troca de senhas pelos usuários, a atualização de sistemas e servidores, entre outras medidas específicas adotadas.

FLUXO DO PROCESSO



REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Disponível em: < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/outros-documentosexternos/anpd_guia_agentes_de_tratamento.pdf >.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm >.

PROCEMPA. Empresa de Tecnologia da Informação e Comunicação de Porto Alegre. Plano de Resposta a Incidentes de Segurança e Privacidade da PROCEMPA. Disponível em: < https://prefeitura.poa.br/sites/default/files/usu_doc/sites/procempa/Plano%20de%20Resposta%20a% 20Incidentes.pdf >.

SEFIN RONDÔNIA - Secretaria de Estado de Finanças. Plano de Resposta a Incidentes de Segurança da Informação e Privacidade (PRISIP). Disponível em: < https://www.sefin.ro.gov.br/portalsefin/userfiles/PRISIP.pdf >.