Política de **RESPOSTA A INCIDENTES**

Postal Saúde
Sua vida, nossa existência

POLÍTICA DE RESPOSTA A INCIDENTE	
Unidade Administrativa Gestora (UAG) do Instrumento Normativo	Assembleia Geral (ASGER) Secretaria de Governança (SEGOV)
Unidade Administrativa Gestora (UAG) pela Análise Técnica Administrativa e Padronização do Instrumento Normativo	Presidência (PRESI) Gerência de Estratégia, Processos, Riscos e Controles Internos (GEPRO)
Unidade Administrativa Gestora (UAG) pela Conformidade Legal do Instrumento Normativo	Presidência (PRESI) Gerência Jurídica (GEJUR)
Numeração	007
Versão	002
Data da Apreciação Diretoria-Executiva	DIREX Nº 345, de 14 de junho de 2023
Data da Aprovação Conselho Deliberativo	CODEL Nº 197, de 29 de junho de 2023
Data de Publicação	04/07/2023
Advertência	Este normativo é de **uso exclusivo** da Postal Saúde. A divulgação não autorizada estará sujeita às penalidades cabíveis por lei. Toda e qualquer autorização para cópia, divulgação, apresentação ou qualquer outra finalidade deverá ser obtida junto à Postal Saúde.

Sumário

Sumário

01 DO OBJETIVO

CAPÍTULO 1 - DO OBJETIVO

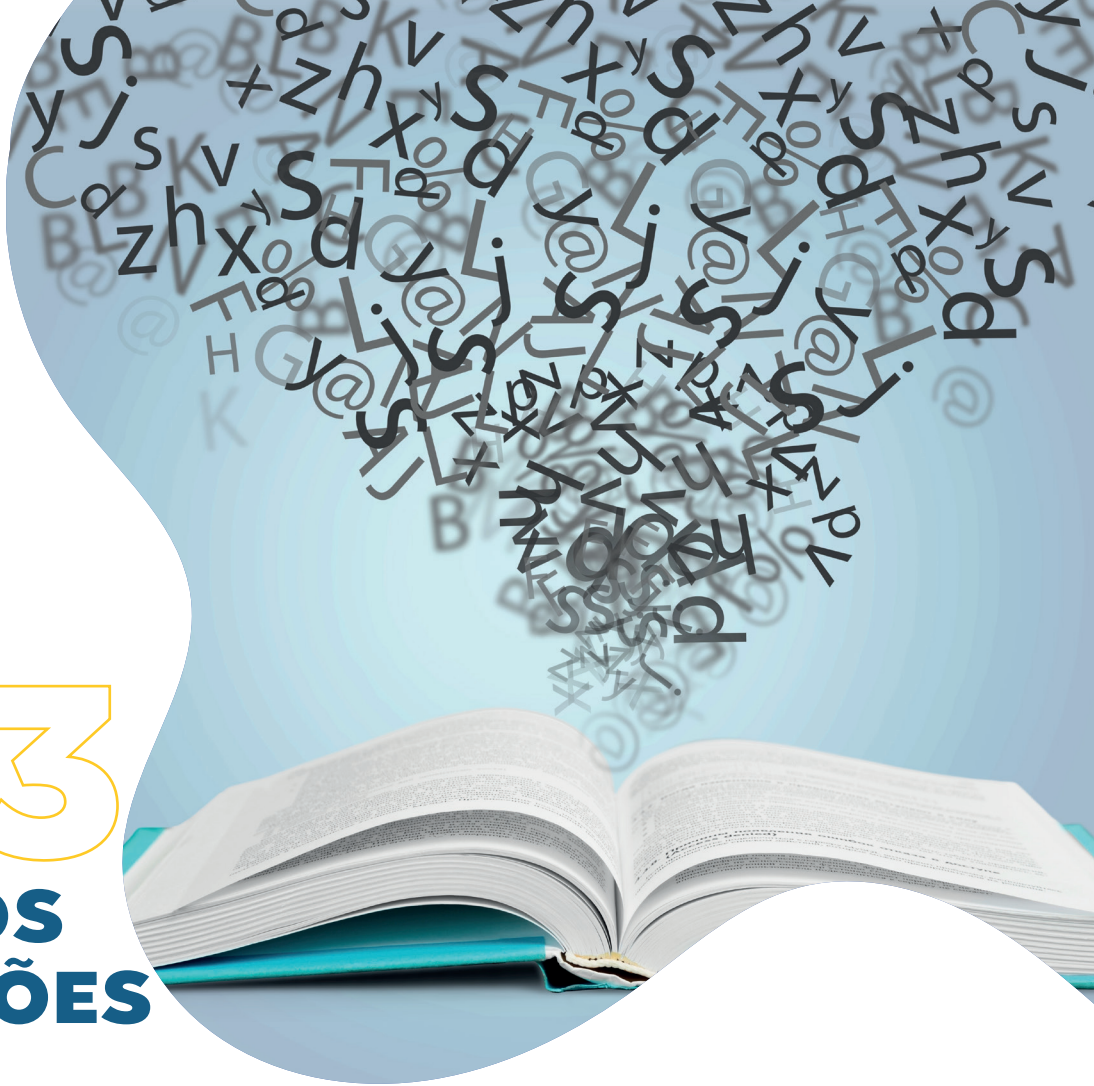
A presente Política de Resposta a Incidentes tem por finalidade orientar os responsáveis pelo tratamento de dados corporativos e pessoais, armazenados nesta Operadora, sobre como agir em caso de violações dos protocolos de segurança da informação que envolvam dados pessoais, a fim de mitigar ou, se possível, eliminar os prejuízos causados aos titulares dos dados e às operações da Postal Saúde, atendendo às exigências legais de comunicação e transparência.

02 DA ABRANGÊNCIA

CAPÍTULO 2 - DA ABRANGÊNCIA

A Política de Resposta a Incidentes da Postal Saúde abrangerá todos os colaboradores da Operadora, sejam eles próprios ou cedidos, pessoas e empresas com os quais a Postal Saúde tenha ou possa vir a ter relacionamento direto ou indireto e os que atuam a serviço ou em nome da Operadora, tais como terceiros, prestadores de serviços, fornecedores e parceiros agentes de tratamento: o Controlador e o Operador, responsáveis pela preservação e intervenção no tratamento de dados pessoais, na ocorrência de incidentes que coloquem em risco a segurança desses dados.

03 DOS CONCEITOS E DEFINIÇÕES



CAPÍTULO 3 - DOS CONCEITOS E DEFINIÇÕES

Agentes de tratamento: o controlador e o operador, responsáveis pela preservação e intervenção no tratamento de dados pessoais, na ocorrência de incidentes que coloquem em risco a segurança destes dados.

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.

Ativos organizacionais: insumos tangíveis e intangíveis envolvidos na segurança das informações corporativas e no tratamento dos dados pessoais, tais como: bases de dados, documentos, equipamentos, locais físicos, força de trabalho, sistemas, unidades organizacionais, processos corporativos etc.

Autenticidade: propriedade pela qual se assegura que o dado pessoal foi produzido, expedido, modificado ou destruído por uma determinada pessoa física, equipamento, sistema, órgão ou entidade.

Autoridade Nacional de Proteção de Dados (ANPD): órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento da Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) em todo o território nacional.

Banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

Bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.

Categoria de dados pessoais: classificação dos dados pessoais de acordo com o contexto de sua utilização, como identificação pessoal, autenticação em sistemas, financeiro, saúde, educação e judicial.

Cibersegurança: prática para proteger ativos de informação tais como computadores e servidores, entre outros, contra ameaças cibernéticas ou ataques maliciosos.

Comunicação do incidente de segurança: ato do Controlador que comunica à ANPD e ao titular de dados a ocorrência de incidente de segurança com dados pessoais que possa acarretar risco ou dano relevante aos titulares.

Confidencialidade: propriedade pela qual se assegura que o dado pessoal não esteja disponível ou não seja revelado a pessoas, sistemas, órgãos ou entidades não autorizadas e nem credenciadas.

Consentimento: manifestação livre, informada e inequívoca em que o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

Dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

Dado pessoal afetado: dado pessoal cuja confidencialidade, integridade, disponibilidade ou autenticidade tenha sido comprometida em um incidente de segurança.

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.

Disponibilidade: propriedade pela qual se assegura que o dado pessoal esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados.

Encarregado de Tratamento de Dados (ETD): 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.

Incidente de Segurança com dados pessoais: evento adverso confirmado que comprometa a confidencialidade, integridade ou disponibilidade de dados pessoais. Pode decorrer de ações voluntárias ou acidentais que resultem na divulgação, alteração, perdas indevidas ou acessos não autorizados a dados pessoais, independentemente do meio em que estejam armazenados.

Incidente de Segurança da Informação: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

Integridade: propriedade pela qual se assegura que o dado pessoal não seja modificado ou destruído de maneira não autorizada ou acidental.

LGPD: Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), cujo objetivo é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Medidas de segurança relacionadas a dados pessoais: medidas técnicas e administrativas adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração ou comunicação.

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

Pseudonimização: processos e técnicas por meio dos quais um dado tem sua possibilidade de associação dificultada. O dado pseudonimizado é considerado dado pessoal para fins de aplicação da LGPD, tendo em vista a possibilidade de associação desse dado a uma pessoa natural.

Relatório de impacto à proteção de dados pessoais - RIPD: 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.

Titular: pessoa natural a quem se referem os dados pessoais que são objetos de tratamento.

Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção,

04 DAS ATRIBUIÇÕES E RESPONSABILIDADES

4.1. DE TODOS OS COLABORADORES E DOS PROVEDORES EXTERNOS

4.1.1. Assumir com a Postal Saúde o compromisso de confidencialidade de tratamento dos dados pessoais, não podendo revelar ou utilizá-los, a não ser em casos previstos em Lei ou determinação judicial.

4.1.2. Cumprir com as disposições constantes nesta Política.

4.1.3. Relatar, de imediato, quaisquer fatos que possam configurar incidentes de segurança ou descumprimento das normas contidas nesta Política.

4.1.4. Sempre que necessário, buscar apoio e orientação dos superiores hierárquicos.

4.1.5. Elaborar os Relatórios de Impacto e Proteção de Dados (RIPD) quando necessário ou quando solicitado.

4.2. DA UNIDADE DE COMPLIANCE

4.2.1. Fiscalizar a execução de atividades relativas ao tratamento de dados pessoais.

4.2.2. Conduzir investigações, dentro de suas atribuições, em situação de incidentes de segurança com dados pessoais.

4.2.3. Encarregar-se, dentro de suas atribuições, das providencias a serem tomadas para resposta aos incidentes de segurança com dados pessoais.

4.2.4. Planejar e conduzir treinamentos relativos à privacidade e proteção de dados pessoais e prevenção de vazamento de dados.

4.2.5. Apoiar a elaboração de Relatórios de Impacto e Proteção de Dados (RIPD), quando solicitado ou quando necessário.

4.3. DA UNIDADE DE TECNOLOGIA

4.3.1. Encarregar-se, dentro de suas atribuições, da avaliação de risco dos incidentes de segurança com dados pessoais, bem como da elaboração dos relatórios pertinentes.

4.3.2. Planejar e conduzir os treinamentos sobre cibersegurança, a fim de proteger a Postal Saúde de ameaças cibernéticas ou ataques maliciosos.

4.3.3. Apoiar as investigações, dentro de suas atribuições, em situação de incidentes de segurança com dados pessoais.

4.3.4. Verificar a conformidade dos procedimentos da Operadora em relação às melhores práticas da segurança da informação.

4.4. DO ENCARREGADO PELO TRATAMENTO DE DADOS (ETD)

4.4.1. Comunicar à Autoridade Nacional de Proteção de Dados - ANDP e aos titulares dos dados pessoais, situação de incidente de segurança confirmado que comprometa a confidencialidade, integridade ou disponibilidade de dados pessoais, conforme o artigo 41 da LGPD.

4.4.2. Manter o Diretor-Presidente permanentemente informado sobre a implementação das medidas relacionadas com a privacidade e o tratamento de dados pessoais.

4.4.3. Verificar a conformidade dos procedimentos da Operadora em relação às melhores práticas de Proteção de Dados Pessoais.

4.4.4. Responder às solicitações dos titulares de dados.

4.4.5. Mediante consentimento do Diretor-Presidente, provocar a Unidade Jurídica, de Tecnologia, ou qualquer outra Gerência e/ou Unidade que realize o tratamento de dados pessoais, a participar da investigação e preparação de respostas a incidentes de segurança com dados pessoais.

4.4.6. Convocar treinamentos obrigatórios para tratar de aspectos relacionados com as diretrizes contidas nesta Política.

4.5. DA ALTA ADMINISTRAÇÃO

4.5.1. Valendo-se do assessoramento do Encarregado pelo Tratamento de Dados - ETD, da Unidade de Tecnologia, e da Unidade de *Compliance*, avaliar a implementação das medidas de segurança da informação, privacidade e de tratamento de dados pessoais contidas nesta Política.

4.5.2. Sempre que solicitado, deliberar de forma tempestiva sobre as questões relacionadas com a privacidade e tratamento de dados pessoais que lhe forem encaminhadas.

05 DO INCIDENTE DE SEGURANÇA DA INFORMAÇÃO ENVOLVENDO DADOS PESSOAIS

CAPÍTULO 5 - DO INCIDENTE DE SEGURANÇA DA INFORMAÇÃO ENVOLVENDO DADOS PESSOAIS

5.1. Considera-se que um incidente de segurança com dados pessoais pode acarretar risco ou dano relevante aos titulares quando tiver potencial de afetar significativamente interesses e direitos fundamentais dos titulares, aqueles que possam:

a) Impedir ou limitar o exercício de direitos ou a utilização de um serviço; ou

b) Ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito de imagem e à reputação, fraudes financeiras ou uso indevido de identidade.

5.2. Serão caracterizados incidentes de segurança com dados pessoais em larga escala quando abrangerem número significativo de titulares, considerando, ainda, o volume de dados envolvidos e a extensão geográfica de localização dos titulares.

5.3. Conforme o artigo 46 da LGPD, a Postal Saúde, como Controlador de Dados, deve 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 forma de tratamento inadequado ou ilícito.

5.4. Tais medidas deverão ser observadas desde a concepção do produto ou serviço até a sua execução. A seguir, exemplos práticos de situações de incidentes de segurança com ou sem dados pessoais:

a) Sequestro e/ou o vazamento de dados após um ataque cibernético;

b) Modificação indevida de informações por parte dos próprios colaboradores;

c) Eliminação indesejada de dados;

d) Perda de informações em razão, por exemplo, de atualizações do *software*, quedas de energia e, até mesmo, catástrofes naturais;

e) Exposição acidental de informações nas redes sociais, em comunicados e/ou em sites;

f) Acesso de qualquer indivíduo não autorizado aos dados;

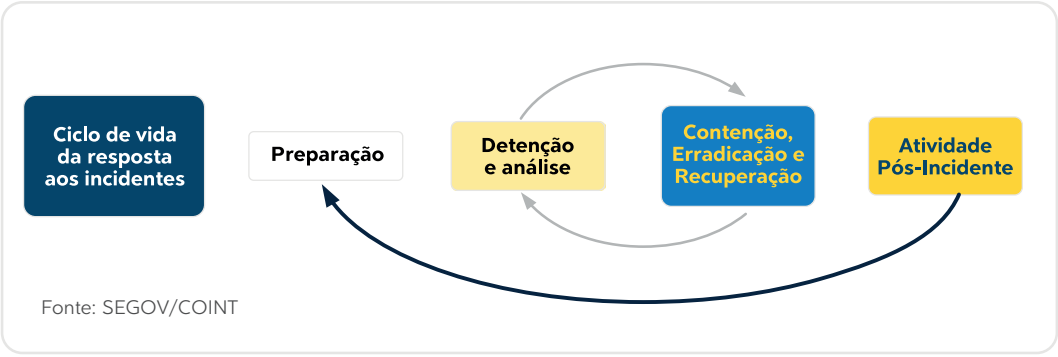
g) Uso inapropriado, quando há a violação das políticas de privacidade e proteção de dados pessoais e de segurança da informação.

06 DO CICLO E ETAPAS DE UM INCIDENTE DE SEGURANÇA

CAPÍTULO 6 - DO CICLO E ETAPAS DE UM INCIDENTE DE SEGURANÇA

6.1. O contexto de uma situação de incidente de segurança pode ser visualizado em ciclos, fluxos, etapas ou fases. Cada momento demandará providências específicas e ações preventivas e corretivas, de acordo com as fases detalhadas no Capítulo 8.

6.2. Abaixo, a representação cíclica e sua respectiva descrição:



Fonte: SEGOV/COINT

6.2.1. Preparação – Consiste em todo o trabalho da Operadora na preparação para a resposta ao incidente, incluindo a capacitação contínua de todos os colaboradores, com instruções de como proceder em situações de incidentes de segurança informação e quem comunicar de forma imediata.

6.2.2. Detecção e Análise – Momento de identificar e apurar o incidente com precisão, de forma que seja possível obter informações sobre o impacto do evento, natureza, categoria e quantidade de titulares de dados e dados pessoais afetados, consequências do incidente para os titulares e para a Postal Saúde, criticidade e probabilidade. Além disso, é necessário preservar todas as evidências do incidente.

6.2.3. Contenção, Erradicação e Recuperação - Tomada de ações baseadas no que a LGPD determina a fim de interromper o impacto do evento, buscando minimizar todas as suas consequências para a não paralização da atividade.

6.2.4. Atividade pós-incidente – Observado o princípio de responsabilização e prestação de contas, a Postal Saúde comunicará à ANPD e aos titulares de dados informações sobre o incidente (Art. 6º, X da LGPD), bem como sobre correção e melhoria dos processos.

6.3. Ressalta-se, que, mesmo antes da ocorrência de um incidente de segurança, existem ações previstas que devem ser observadas por todos os colaboradores, estas ações podem ser categorizadas em linha temporal pelas etapas:

a) Antes do incidente;

b) Durante o incidente;

c) Após o incidente.

6.4. Antes do Incidente

6.4.1. De acordo com o artigo 50 da Lei Geral de Proteção de Dados (LGPD), parágrafo 2º, inciso I, o Controlador de Dados poderá implementar práticas de governança em privacidade que conte, entre outras medidas e políticas, com um plano de resposta a incidentes e remediação, que busca conferir clareza sobre o fluxo de procedimentos adequados e os responsáveis e, em caso de incidentes, assegurar respostas rápidas, efetivas, coordenadas, e evoluir continuamente com as lições aprendidas.

6.4.2. A Postal Saúde deve contar com a infraestrutura de TI e ambiente de segurança, além do tratamento de dados capaz de fazer frente às inúmeras possibilidades de ataques cibernéticos ou quaisquer tentativas de violação à integridade dos dados tratados pela Operadora.

6.4.3. Em nível Estratégico e de Governança, estão disponibilizadas as Políticas e outros normativos que orientam as ações no nível operacional, como esta Política, a de Privacidade e Proteção de Dados Pessoais, a de Segurança da Informação e o Manual de Privacidade e Tratamento de Dados Pessoais.

6.5. Deve ser incentivada e consolidada a cultura de privacidade e proteção de dados por meio de treinamentos periódicos e/ou extraordinários e avaliações serão planejadas e executadas repetidas vezes, a fim de avaliar a maturidade em privacidade e proteção de dados dos colaboradores.

6.6. DURANTE O INCIDENTE

6.6.1. Em situação de evento adverso que comprometa a confidencialidade, integridade ou disponibilidade de dados pessoais, deverá ser realizada a análise das causas e da amplitude, para iniciar de imediato o planejamento e a aplicação das medidas corretivas pertinentes, visando mitigar os efeitos danosos do incidente e garantir a continuidade das operações.

6.6.2. Caso o evento adverso seja confirmado, deverão ser desencadeadas as ações específicas previstas no artigo 48 da LGPD, conforme o item 8.3.

6.7. APÓS O INCIDENTE

6.7.1. Deverá ser conduzida uma análise criteriosa para determinar a causa principal do incidente, além da possível revisão dos protocolos de segurança, das Políticas e dos demais normativos vigentes sobre o assunto.

6.7.2. Nessa fase, os registros de acesso deverão ser analisados para identificação dos envolvidos na violação da segurança, bem como se há responsável pelo incidente.

6.7.3. Deverá ser realizado o relatório final (Relatório do Incidente de Segurança e/ou Relatório de Impacto à Proteção dos Dados - RIPD) para fins de cumprimento do princípio de responsabilização e prestação de contas tanto aos titulares como a prestação de informações sobre o incidente à ANPD (Art. 6º, X da LGPD), que além de ter uma função de comprovação das medidas levadas a efeito pela Postal Saúde, será importante para que se possa compreender as causas do incidente, avaliar a aderência e efetividade do Plano de Respostas a Incidentes, e analisar a atuação dos responsáveis.

6.7.4. Os sistemas/processos afetados retornarão, após testes e validações, ao ambiente de produção ou ao habitual andamento, com vistas a garantir que nenhuma ameaça permaneça.

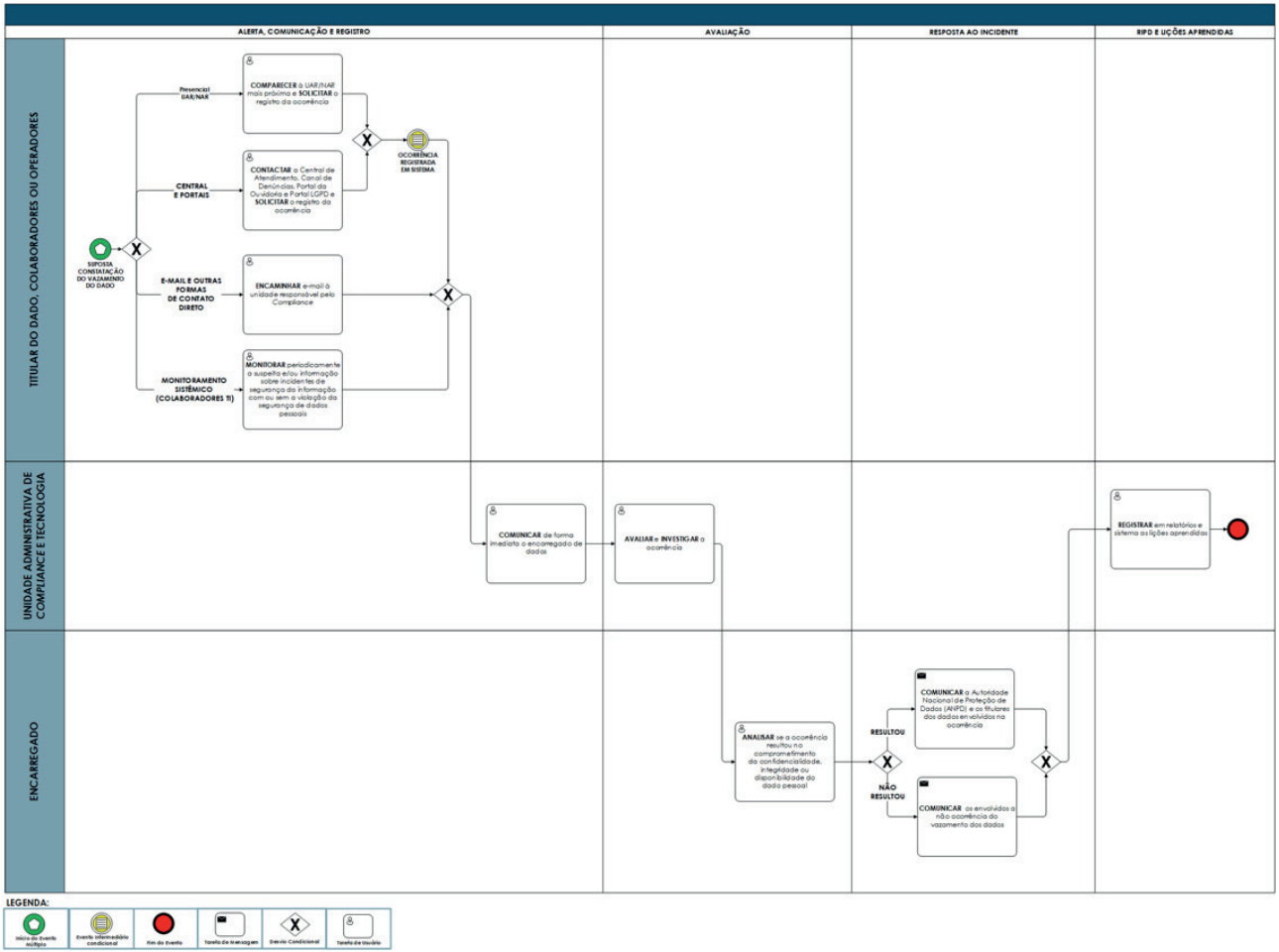
6.7.5. Ao final, será conduzido momento de lições aprendidas e preceitos assimilados, com o fim de atualizar o Fluxo de Respostas a Incidentes com as ações realizadas para tratar o incidente, contribuindo para o aprendizado da equipe e facilitando as próximas atuações em futuros incidentes.

6.7.6. As atividades e a documentação pós-incidente auxiliarão no ajustamento de processos internos e na conformidade regulatória.

07

FLUXO DO PROCESSO DE RESPOSTA AO INCIDENTE DE SEGURANÇA

Fluxo do Processo de Resposta ao Incidente de Segurança



Fonte: SEGOV/COINT - **Legenda: ANPD:** Autoridade Nacional de Proteção de Dados | **RIPD:** Relatório de Impacto à Proteção de Dados Pessoais

08 DAS FASES DO GERENCIAMENTO DO INCIDENTE

8.1. ALERTA, COMUNICAÇÃO E REGISTRO

O alerta de incidente está diretamente vinculado ao processo de monitoramento adotado pela Postal Saúde e será dado a partir da leitura e interpretação por parte dos especialistas em TI das informações constantes dos painéis de controle ou da identificação de qualquer colaborador, que deverá comunicar a situação percebida ao gestor imediato, que acionará as unidades de tecnologia e *Compliance*.

8.1.1. Quando detectado um alerta de incidente, o Encarregado de Tratamento de Dados e a unidade de *Compliance* deverão ser informados de imediato, a fim de adotar as medidas cabíveis à situação para mitigar os danos à segurança e evitar o comprometimento das operações da Postal Saúde.

8.1.2. Detectado o incidente de segurança, haverá necessidade de registrar/documentar o evento, por meio formal, a fim de atender aos possíveis aspectos jurídicos decorrentes e para subsidiar resposta adequada ao incidente por parte do ETD à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares de dados.

8.1.3. O registro deverá conter, no mínimo, as seguintes informações:

a) Dados do responsável pela identificação do incidente;

b) Definição sobre o local geográfico do incidente (Sede ou regionais);

c) Indicação de ter havido ou não violação física dos ativos e do responsável local pela segurança das instalações;

d) O contexto da atividade de tratamento de dados;

e) As quantidades de titulares de dados afetados;

f) As categorias de dados pessoais;

g) A quantidade de dados violados;

h) Os potenciais danos materiais, morais ou reputacionais causados aos titulares;

i) Se os dados violados estavam protegidos de forma a impossibilitar a identificação de seus titulares;

j) Histórico ou evidências: imagens, códigos de erro ou outros registros que evidenciem a ocorrência do incidente;

k) Detalhes técnicos complementares sobre o ocorrido.

8.2. AVALIAÇÃO

8.2.1. Nessa etapa será realizada a avaliação da extensão e gravidade do problema, assim como serão adotadas medidas de contenção tecnológicas e administrativas imediatas.

8.2.2. Poderá ser necessário, também, implementar ações de comunicação interna e externa, com o apoio da unidade de Comunicação.

8.2.3. A unidade de *Compliance* não aguardará a conclusão do formulário de registro de incidente citado nos itens 8.1.2. e 8.1.3. para agir, devendo, a partir da tomada de conhecimento do incidente, iniciar a investigação, dentro das suas atribuições, para detectar a dimensão e verificar se resultou em vazamento de dados pessoais.

8.2.4. Após a detecção do incidente, o Encarregado de Tratamento de Dados, com base nas informações recepcionadas, fará a análise do evento para identificar se a confidencialidade, integridade ou disponibilidade de dados pessoais foram comprometidos.

8.2.5. Deve-se levar em consideração que, quanto maior o uso de tecnologias de análise de dados, volume de dados processados e quanto mais significativos forem esses dados, maior será o risco de violação.

8.2.6. O Encarregado de Tratamento de Dados (ETD) deverá avaliar pontualmente o nível de ameaça e exposição dos dados pessoais eventualmente comprometidos.

8.3. RESPOSTA AO INCIDENTE

8.3.1. Com a informação de que o incidente de segurança pode acarretar risco ou dano relevante aos titulares afetados, o Encarregado de Tratamento de Dados – ETD, deverá, de acordo com o artigo 48 da LGPD, comunicar o ocorrido à ANPD, devendo preencher o formulário disponibilizado por esta e protocolá-lo no Portal indicado pela Autoridade.

8.3.2. No que tange à Comunicação de Incidente de Segurança, cujo conteúdo mínimo está definido no artigo 48 da LGPD, temos:

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.

8.3.3. Na Comunicação, o ETD deve atentar para o fato de que:

a) É necessário informar a data e hora do conhecimento do incidente de segurança, os dados do controlador, as informações sobre o operador, os dados do encarregado, quando aplicável, ou do comunicante, acompanhado, nesta hipótese, de procuração ou outro instrumento com poderes para representar o controlador junto à ANPD;

b) Não basta apontar se os dados pessoais são convencionais (artigo 5º, I) ou sensíveis (artigo 5º, II), mas deve-se classificar, com precisão, os tipos de dados: contas de e-mail, dados de cartão de crédito, senhas, informações de geolocalização etc.;

c) Sobre informações dos titulares envolvidos, é necessária uma descrição, precisa ou estimada, de quais e quantos titulares de dados foram afetados, bem como discriminando, quando aplicável, o número de crianças, de adolescentes ou de idosos;

d) Observados os segredos comercial e industrial, a LGPD exige, em seu artigo 46, que a Postal Saúde, como Controladora de Dados, adote medidas de segurança para a proteção de dados pessoais. Tais medidas devem ser descritas para se demonstrar a conformidade com a lei. Deve-se solicitar à ANPD, de maneira fundamentada, o sigilo das informações protegidas por lei, como os segredos comercial e industrial, que devem ser poupados para a preservação do negócio;

e) Sobre os riscos relacionados, trata-se de uma análise prospectiva do incidente, levando em consideração, principalmente, os incisos I e II do artigo 48. Poderá mencionar, também, os danos que já ocorreram, como a destruição ou codificação de dados;

f) A respeito dos motivos da demora, no caso de a comunicação não ter sido imediata, deve-se apresentar justificativa, devidamente fundamentada, da não apresentação imediata da notificação. Poderá decorrer, por exemplo, da complexidade e extensão (número de titulares afetados, quantidade de dados etc.) da situação.

g) Sobre as medidas adotadas para mitigar os efeitos do prejuízo, devem ser mencionadas de forma clara e objetiva, sem exagero de expressões técnicas, detalhando as condutas que foram e que serão implementadas para eliminar ou minimizar os efeitos do incidente ocorrido, como o contato com as autoridades policiais, determinação de troca de senhas pelos usuários, atualização de sistemas e sanções aplicáveis após apuração.

8.3.4. Na hipótese de o ETD não dispor de informações completas a respeito do incidente ou não conseguir notificar todos os titulares no prazo recomendado, a comunicação à ANPD poderá ser realizada em duas etapas: preliminar e complementar.

8.3.5. A impossibilidade de realizar a comunicação completa deve ser devidamente justificada pela Postal Saúde, representada pelo ETD.

8.3.6. A complementação deverá ser encaminhada o mais breve possível e, no mais tardar, no prazo definido pela ANPD, a partir da comunicação preliminar. A comunicação complementar deve ser protocolada no mesmo processo que a comunicação preliminar, por meio de petição intercorrente.

8.3.7. O conhecimento das condições do incidente, assim como o conteúdo dos documentos produzidos durante o seu tratamento, deverá ficar restrito à alta administração, ao ETD, às unidades jurídica, tecnológica e de *Compliance*, e à Autoridade Nacional de Proteção de Dados (ANPD), quando esta for notificada ou solicitar o RIPD.

8.3.8. Em ato contínuo (a notificação à ANPD), o ETD deverá comunicar o mais rápido possível aos titulares de dados envolvidos no incidente de segurança com dados pessoais, de forma individual, por quaisquer meios, tais como: e-mail, SMS, carta ou mensagem eletrônica e, preferencialmente, por meio do canal já habitualmente utilizado pelo agente para se comunicar com o titular.

8.3.9. O comunicado aos titulares deve fazer uso de linguagem clara, ser realizado de forma individualizada (caso seja possível identificá-los) e conter, ao menos, as seguintes informações:

a) Resumo e data da ocorrência do incidente;

b) Descrição da natureza e da categoria de dados pessoais afetados;

c) Riscos e consequências aos titulares de dados;

d) Data de conhecimento do incidente de segurança;

e) Medidas tomadas pelo Controlador e as recomendadas aos titulares para mitigar os efeitos do incidente, se cabíveis;

f) Dados de contato do encarregado da Postal Saúde para que os titulares possam solicitar informações adicionais a respeito do incidente.

8.3.10. Excepcionalmente, e de forma justificada, pode ser feita a comunicação indireta por meio de publicação em meios de comunicação. O meio utilizado deve ser capaz de alcançar o maior número possível de titulares, e deve ser dado o devido destaque à divulgação.

8.3.11. A ANPD poderá solicitar à Postal Saúde, a qualquer tempo, a apresentação de cópia do comunicado aos titulares para fins de fiscalização, bem como determinar que seja realizada nova comunicação, caso a primeira não contenha todas as informações necessárias ou tenha se utilizado meios inadequados.

8.4. RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS (RIPD) E LIÇÕES APRENDIDAS

8.4.1. Segundo os artigos 4°, parágrafo 3º, 5° inciso XVII, 10, parágrafo 3º e 38, parágrafo único da LGPD, a ANPD poderá solicitar à Postal Saúde o envio do RIPD nos casos de impacto à integridade dos dados pessoais ou quando fundamentar o tratamento desses dados no seu legítimo interesse.

8.4.2. A estrutura do Relatório básico de Impacto de Dados (RIPD) da Postal Saúde seguirá modelo padronizado, IOT 288 (Orientação para confecção do Relatório de Impacto à Proteção de Dados Pessoais - RIPD) e constante de normativos específicos, contendo os seguintes dados:

a) Dados cadastrais da Postal Saúde;

b) Identificação do Encarregado de Tratamento de Dados;

c) Necessidade de elaboração do Relatório;

d) Tipos de dados coletados (pessoais, sensíveis e dados anônimos);

e) Descrição do tratamento geral dos dados contendo a sua natureza, escopo, contexto, criptografia nas fases de tratamento, finalidade e descrição das medidas de segurança adotadas em cada fase de tratamento;

f) Partes interessadas consultadas;

g) Necessidade dos dados e finalidade do tratamento.

8.4.3. Além do encaminhamento do formulário e/ou do RIPD à ANPD, caso seja por esta última solicitado, serão tomadas providências administrativas e/ou técnicas de contenção e acompanhamento pós-incidente que poderão envolver:

a) Alterações nas configurações de segurança;

b) Revisão dos normativos corporativos;

c) Intensificação dos treinamentos internos;

Plano de comunicação contendo orientações aos Operadores, Controladores Conjuntos e Titulares de Dados;

8.4.4. Com o incidente contido e os dados e serviços restaura-

dos, será realizada uma análise crítica da situação e documentadas as lições aprendidas.

8.5. MONITORAMENTO DE EVENTOS

8.5.1. Medidas técnicas e administrativas destinadas a proteger os dados pessoais de acessos não autorizados compõem o portfólio de monitoramento adotado pela Postal Saúde para detectar incidentes de segurança com dados pessoais.

8.5.2. A Operadora deverá contar com mecanismos e procedimentos simples, eficazes e documentados que permitam monitorar seus ativos organizacionais e emitir comunicados sobre eventuais incidentes.

8.5.3. Com o incidente contido e sua resolução encaminhada, o ETD deverá agendar e conduzir uma reunião de Lições Aprendidas, com os atores envolvidos e unidades de *Compliance*, Jurídica, Riscos e Tecnologia, com o objetivo de discutir erros e dificuldades encontradas, propor melhorias para os processos de segurança e de privacidade da informação da Postal Saúde, avaliar a eficácia deste Plano de Resposta a Incidentes de Segurança de Informação e Privacidade e subsidiar a documentação da causa-raiz, bem como outras provas.

8.5.4. É válido também que a unidade afetada seja comunicada das decisões tomadas para prevenção de incidentes da mesma natureza, caso haja consenso de implementar melhorias na infraestrutura de segurança.

8.5.5. A Postal Saúde deverá manter o registro de incidentes de segurança com dados pessoais, inclusive daqueles não comunicados à ANPD e aos titulares de dados, pelo prazo definido pela ANPD, contados a partir do registro, exceto se constatadas obrigações adicionais que demandem maior prazo de manutenção.

8.5.6. O monitoramento possibilitará a identificação de eventuais erros, vulnerabilidades, dificuldades e melhorias necessárias a subsidiar a tomada de decisão para alteração e melhorias.

8.5.7. Sugestões de aprimoramento de processo e do próprio Plano de Resposta a Incidentes devem ser levadas para apreciação da unidade de *Compliance*.

09 DO COMPROMISSO E PENALIDADES

CAPÍTULO 9 - DO COMPROMISSO E PENALIDADES

9.1. Todas as garantias e instruções necessárias ao tratamento de dados pessoais devem ser estabelecidas formalmente com os colaboradores da Postal Saúde por meio do FOP 381 - Termo de Compromisso e Confidencialidade pelo Uso e Manuseio de Dados Pessoais e Sensíveis.

9.2. O descumprimento desta Política será considerado infração disciplinar e poderá acarretar a aplicação de sanções previstas nos regramentos corporativos e disposições contratuais.

9.3. Esta Política de Resposta a incidentes, juntamente com o Código de Conduta e Integridade, o Programa de Integridade, a Política de Privacidade e Proteção de Dados Pessoais, e outros, compõem o conjunto de normativos da Postal Saúde que tratam de atitudes e comportamentos exigidos dos colaboradores da Postal Saúde no tocante à proteção de dados pessoais, devendo ser rigorosamente observados.

10 DAS DISPOSIÇÕES FINAIS

CAPÍTULO 10 - DAS DISPOSIÇÕES FINAIS

10.1. A Política de Resposta a Incidentes da Postal Saúde poderá ser modificada a qualquer momento, sendo de fundamental importância a consulta regular deste documento, que se encontra disponível no portal da Instituição e na internet.

10.2. Cumprindo o que lhe faculta a LGPD, a Postal Saúde adota medidas administrativas para garantir a segurança dos dados pessoais existentes, implicando a adoção de protocolos de controle quanto ao exercício do trabalho de seus colaboradores, incluindo o monitoramento dos seus e-mails corporativos e acesso à internet.

10.3. A ocorrência de qualquer violação ou suspeita de violação das disposições desta Política deverá ser comunicada por meio do Canal de LGPD disponível no site da Postal Saúde, que permite o tratamento adequado das comunicações de irregularidades identificadas de maneira segura.

10.4. A Postal Saúde manterá um plano de treinamento periódico e constante para os abrangidos, com o intuito de divulgar e conscientizar sobre a importância do cumprimento das regras desta Política.

11 DOS DOCUMENTOS ASSOCIADOS

CAPÍTULO 11 - DOS DOCUMENTOS ASSOCIADOS

DOS DOCUMENTOS INTERNOS:

- Estatuto Social;
- Regimentos Internos dos órgãos de governança;
- Código de Conduta e Integridade;
- Programa de Integridade;
- Política de Governança Corporativa;
- Política de Segurança da Informação;
- Política de Gestão de Pessoas;
- Manual de privacidade e tratamento de dados pessoais.

DOS DOCUMENTOS EXTERNOS:

- Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);
- General Data Protection Regulation (GDPR);
- Diretiva de e Privacy 2002/58/CE (ou Lei dos Cookies);
- Lei nº 12.965/2014 (Marco Civil da Internet);
- Lei 8.068/1990 (Estatuto da Criança e do Adolescente – ECA);
- Lei nº 8.078/1990 (Código de Defesa do Consumidor);
- Lei nº 9.507/1997 (Lei do Habeas Data);
- Lei nº 9.784/1999 (Lei Geral do Processo Administrativo);
- Lei nº 12.527/2011 (Lei de Acesso à Informação);
- Lei nº 13.853/2019 (ANPD);
- Lei nº 12.737/2012 (Lei de Crimes Cibernéticos);
- ISO nº 27.701(Segurança da Informação);
- ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos;
- ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação;
- Decreto-Lei nº 5.452, de 1º de maio de 1943 (Consolidação das Leis Trabalhistas-CLT);
- Normas da Agência Nacional de Saúde (ANS);
- Resoluções CD/ANPD;
- Guia de Boas Práticas Lei Geral de Proteção de Dados (LGPD) do GOV.BR;
- Guia Orientativo Autoridade Nacional de Proteção de Dados Pessoais (ANPD) – Cookies e proteção de dados pessoais;
- Guia Orientativo Autoridade Nacional de Proteção de Dados Pessoais (ANPD) – Definições dos agentes de tratamento de dados pessoais e do encarregado.

Postal Saúde
Sua vida, nossa existência

Caixa de Assistência e Saúde dos Empregados dos Correios

Setor Hoteleiro Sul (SHS) - Quadra 02, Bloco B

Edifício Telex - Asa Sul - Brasília/DF

CEP: 70312-970

ANS - nº 41913-3

www.**postalsaude**.com.br