Guia de Resposta a Incidentes de Segurança

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO (PPSI)

Versão 3.1

Brasília, fevereiro de 2024

GUIA DE RESPOSTA A INCIDENTES DE SEGURANÇA

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

Esther Dweck

Ministra

SECRETARIA DE GOVERNO DIGITAL

Rogério Souza Mascarenhas

Secretário de Governo Digital

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Leonardo Rodrigo Ferreira

Diretor de Privacidade e Segurança da Informação

COORDENAÇÃO-GERAL DE PRIVACIDADE

Julierme Rodrigues da Silva

Coordenador-Geral de Privacidade

COORDENAÇÃO-GERAL DE SEGURANÇA DA INFORMAÇÃO

Loriza Andrade Vaz de Melo

Coordenadora-Geral de Segurança da Informação

Equipe Técnica de Elaboração

Álvaro Sergio de Souza Junior

Amaury C. da Silveira Junior

Bruno Pierre Rodrigues de Sousa

Eder Ferreira de Andrade

Francisco Magno Felix Nobre

Heráclito Ricardo Ferreira Gomes

Ivaldo Jeferson de Santana Castro

Raphael César Estevão

Yuri Arcanjo de Carvalho

Equipe Revisora

Marcelo de Lima

Marcus Paulo Barbosa Vasconcelos

Equipe Técnica de Revisão – Versão 3.1

Adriano de Andrade Moura

Francisco Magno Felix Nobre

Ivaldo Jeferson De Santana Castro

Rodrigo Duran Lima

Rogério Vinícius Matos Rocha

Histórico de Versões

Data	Versão	Descrição	Autor
27/08/2021	1.0	Primeira versão do Guia Resposta a Incidentes.	Equipe Técnica de Elaboração
20/12/2021	2.0	Atualização do item 2.6 - Notificar os titulares de dados pessoais.	Equipe Técnica de Elaboração
31/03/2023	3.0	Atualização para alinhamento com o Guia do Framework de Privacidade e Segurança da Informação, conforme destacado no Anexo I.	Equipe Técnica de Revisão
29/02/2024	3.1	Revisão para alinhamento com as medidas 22.10 e 22.11 do Guia do Framework de Privacidade e Segurança da Informação, conforme destacado no Anexo I.	Equipe Técnica de Revisão

SUMÁRIO

AVISO PRELIMINAR E AGRADECIMENTOS

O presente Guia, especialmente recomendado e dirigido aos órgãos e às entidades da Administração Pública Federal - APF, visa a auxiliar na Gestão de Resposta a Incidentes, em atendimento ao previsto no Capítulo VII - DA SEGURANÇA E DAS BOAS PRÁTICAS da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), que determina que a Administração Pública, ao prestar diversos serviços que tratam dados pessoais à sociedade, 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 dos dados que estão sob sua custódia, bem como gerir a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares de dados pessoais. Adicionalmente, a Gestão de Resposta a Incidentes visa a atender, além da LGPD, a outros normativos vigentes sobre o tema de privacidade e segurança da informação.

Este documento é de autoria exclusiva da Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos e tem como referência fundamental o Guia do Framework de Privacidade e Segurança da Informação baseado em diversas publicações e documentos técnicos já existentes que são utilizados amplamente por profissionais da área de privacidade e segurança da informação. Destacam-se as publicações do *Center for Internet Security* (CIS), da *International Organization for Standardization* (ISO) e do *National Institute of Standards and Technology* (NIST). Em complemento ao Guia do Framework de Privacidade e Segurança da Informação, este **Guia** também foi inspirado em publicações das Autoridades de Proteção de Dados do Reino Unido (ICO), da França (CNIL), da União Europeia (EDPS) e do Brasil (ANPD). Com o objetivo de facilitar a difusão de conhecimentos sobre privacidade e segurança da informação, tais referências, quando escritas em línguas estrangeiras, foram traduzidas para o português pela equipe técnica do Diretoria de Privacidade e Segurança da Informação da Secretaria de Governo Digital.

Nesse cenário, a Secretaria de Governo Digital enfatiza que:

a) não representa, tampouco se manifesta em nome do CIS, da ISO e do NIST e vice-versa;

b) não se manifesta em nome de autoridades de privacidade e segurança da informação;

c) não é coautora das publicações internacionais abordadas;

d) não assume nenhuma responsabilidade administrativa, técnica ou jurídica por usos ou interpretações inadequadas, fragmentados ou parciais do presente guia; e

e) caso o leitor deseje se certificar de que atende integralmente os requisitos das publicações das instituições mencionadas, deverá consultar diretamente as fontes oficiais de informação ofertadas por elas, que foram listadas na seção "Referências Bibliográficas" **deste documento**.

Finalmente, um agradecimento especial deve ser registrado ao CIS, à ISO, às autoridades de proteção de dados referenciadas, ao NIST e aos profissionais de privacidade e segurança da informação consultados, por suas valiosas contribuições para a comunidade e para elaboração **deste documento**.

Este Guia será atualizado frequentemente, de acordo com as novas diretrizes determinadas pelas autoridades em privacidade e segurança da informação ou segundo eventuais alterações que ocorram nos normativos vigentes relacionados a privacidade e segurança da informação e outras referências utilizadas **neste documento**.

INTRODUÇÃO

Este Guia tem por finalidade apresentar orientações com o intuito de auxiliar os órgãos e entidades da Administração Pública Federal, direta, autárquica e fundacional a realizar a Gestão de Resposta à Incidentes de Segurança da Informação no âmbito institucional.

Os Controles 17 e 22 do Guia do Framework de Privacidade e Segurança da Informação (p. 57 e 62), estabelecem que:

Controle 17: Resposta a Incidentes – *Proteger as informações e a reputação da organização, desenvolvendo e implementando uma infraestrutura de resposta a incidentes (por exemplo: planos, definição de papéis, treinamento, comunicações, gerenciamento de supervisão) para descobrir um ataque de forma ágil, e depois, conter efetivamente o impacto, eliminar a presença do atacante, e restaurar a integridade da rede e dos sistemas da organização.*

Controle 22: Políticas, Processos e Procedimentos – *Definir, desenvolver, divulgar, implementar e atualizar políticas, processos e procedimentos operacionais, internos e externos que regem as ações relativas à proteção de dados pessoais e privacidade, e controles para programas, sistemas de informação ou tecnologias que envolvam o tratamento de dados pessoais.*

O presente Guia serve como um modelo prático a ser utilizado para auxiliar na adoção de medidas dos Controles 17 e 22 do Guia do Framework de Privacidade e Segurança da Informação[1] v1 e respectivas evoluções desta versão (1.1, 1.2 etc.) elaborado e publicado pela SGD. As medidas dos Controles 17 e 22 que estão contempladas por este Guia são: 17.1, 17.2, 17.3, 17.4, 17.5, 17.6, 17.7, 17.8, 17.9, 22.10 e 22.11.

A Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020 prevê a obrigatoriedade da implementação de uma política de segurança da informação órgãos que compõem a administração pública federal. Neste contexto, o órgão ou a entidade pública deve estabelecer processo de gestão de incidentes cibernéticos, que por sua vez deve abranger os requisitos de segurança expostos na LGPD, além de outros normativos

[1] < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf >. Acesso em 03/02/2023.

referentes ao tema abordados neste guia, tal como o Decreto nº 10.748, de 16 de julho de 2021, que institui a Rede Federal de Gestão de Incidentes Cibernéticos[2].

[2] https://www.in.gov.br/en/web/dou/-/decreto-n-10.748-de-16-de-julho-de-2021-332610022

1 DEFINIÇÕES GERAIS

Para auxílio na leitura desse guia, serão adotadas as seguintes definições no que se refere a incidentes ocorridos nos órgãos da administração pública federal:

AGENTES DE TRATAMENTO: de acordo com a LGPD, são agentes de tratamento:

- **CONTROLADOR:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
- **OPERADOR:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

A depender do contexto, uma mesma operação de tratamento de dados pessoais pode envolver mais de um operador ou controlador (controladoria conjunta, ou co-controladores).

ENCARREGADO: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

APF: administração pública federal.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS: os arts. 5° inciso XIX, 55-A e seguintes da LGPD definem a Autoridade Nacional de Proteção de Dados (ANPD) como Autarquia de Natureza Especial, responsável por zelar, implementar e fiscalizar o cumprimento da Lei nº 13.709, de 14 de agosto de 2018 - LGPD em todo o território nacional, conforme as atribuições descritas no art. 55-J da LGPD e no Decreto nº 10.474, de 26 de agosto de 2020.

CTIR Gov: O Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) é integrante do Departamento de Segurança de Informação e Cibernética (DSIC) da Secretaria de Segurança da Informação e Cibernética (SSIC) do Gabinete de Segurança Institucional (GSI) da Presidência da República (PR). Tem o papel de coordenar e integrar as ações destinadas à gestão de incidentes de TI em órgãos e entidades da administração pública federal (APF). Os incidentes de segurança e de privacidade estão inclusos no escopo de ação do CTIR. Em caso de incidentes de

segurança em redes computacionais, devem-se observar as diretrizes constantes na Norma Complementar nº 21/IN01/DSIC/GSIPR, que trata do registro de eventos, coleta e preservação de evidências de incidentes de segurança em redes.

DADO PESSOAL: toda informação relacionada a pessoa natural identificada ou identificável.

ETIR: Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos internos de órgãos da administração pública federal (APF).

IDP: O Inventário de Dados Pessoais representa um artefato primordial para documentar o tratamento de dados pessoais realizados pela instituição em alinhamento ao previsto pelo art. 37[3].

INCIDENTE: interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, 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.

INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS: de acordo com a Autoridade Nacional de Proteção de Dados (ANPD), incidente de segurança à proteção de dados pessoais é qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação de dados pessoais, sendo acesso não autorizado, acidental ou ilícito que resulte em destruição, perda, alteração vazamento ou qualquer forma de tratamento de dados ilícita

[3] https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_inventario_dados_pessoais.pdf

ou inadequada, que tem a capacidade de pôr em risco os direitos e as liberdades dos titulares dos dados pessoais[4].

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 privacidade e de liberdade de cada indivíduo.

RELATÓRIO FINAL: relatório que contenha todas as evidências e ações realizadas para tratamento do incidente e que deve ser emitido ao final das tratativas.

RIPD: conforme a LGPD, o Relatório de Impacto a Proteção de Dados (RIPD) é uma documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que tem o potencial de gerar riscos às liberdades civis e aos direitos fundamentais dos titulares, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

SGD: Secretaria de Governo Digital é responsável pela definição de políticas e diretrizes, por orientar normativamente e supervisionar as atividades de gestão dos recursos de tecnologia da informação e comunicação do sistema.

[4] https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca, acesso em 22 mar. 2023

2 INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

Um incidente de segurança com dados pessoais é qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte em destruição, perda, alteração, vazamento ou, ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

O art. 46 da LGPD estabelece que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, e que tais medidas de segurança deverão ser observadas desde a concepção do produto ou serviço até a sua execução.

> Atenção
>
> O agente de tratamento de dados pessoais, poderá sofrer sanções administrativas ou civis caso não cumpra com suas obrigações legais expostas na LGPD. A incorreta ou inadequada gestão de incidentes pode suscitar tais penalidades.

O art. 50 da mesma lei estabelece que controladores e operadores, no âmbito de suas competências, poderão formular regras de boas práticas de governança para o tratamento de dados pessoais. O § 2º, inciso I do mesmo artigo dispõe que deve ser implementado um programa de governança em privacidade que conte com planos de resposta a incidentes e remediação.

Em caso de incidente que coloque em risco a segurança de dados pessoais, devem ser realizados alguns procedimentos específicos. São eles:

a) **Avaliar internamente o incidente** com o objetivo de obter informações iniciais sobre impacto do evento; natureza, categoria e quantidade de titulares de dados pessoais afetados; categoria e quantidade de dados afetados, consequências do incidente para os titulares e a entidade, criticidade e probabilidade; além disso, é necessário preservar todas as evidências do incidente.

b) **Comunicar ao encarregado** da entidade a existência do incidente, caso envolva dados pessoais.

c) **Comunicar ao controlador** (nos termos da LGPD) a existência do incidente, caso envolva dados pessoais.

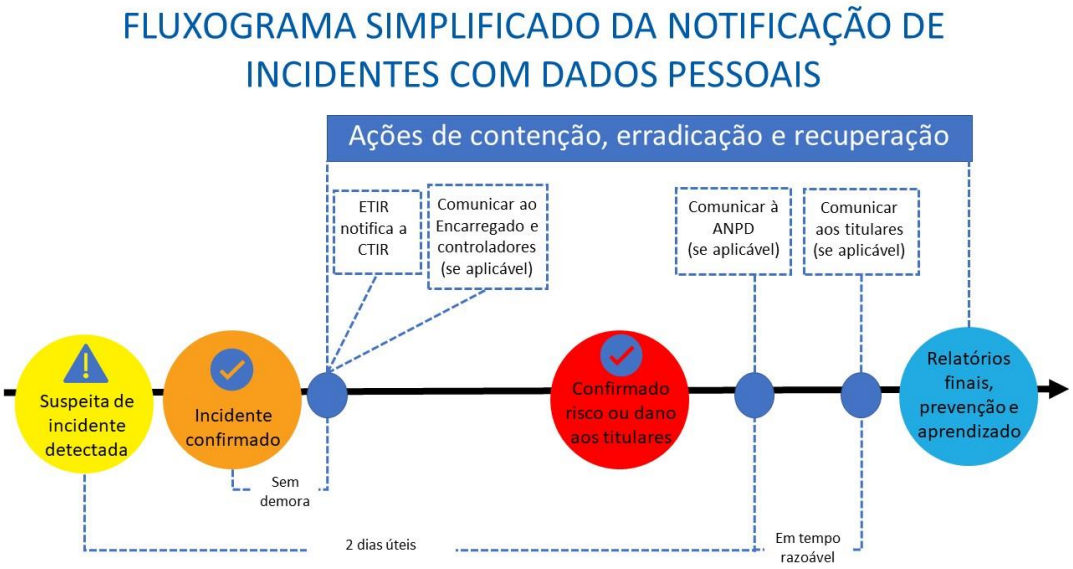
d) **Comunicar à ANPD e ao titular de dados pessoais** (conforme art. 48 da LGPD) a existência do incidente.

e) **Comunicar à ETIR do órgão** em caso de incidentes na rede computacional.

f) **Comunicar ao CTIR GOV** caso a entidade faça parte da administração pública federal, ao realizar a confirmação de um evento de incidente, deve ser realizada a comunicação ao CTIR Gov, e se necessária, deve ser realizada ação conjunta entre a entidade e o CTIR Gov para a correspondente resolução.

g) **Emitir o relatório final** com todas as informações coletadas, as ações realizadas para o tratamento efetivo do evento e as considerações necessárias para promover a melhoria contínua no atendimento de incidentes e para atualizar o RIPD.

A figura abaixo detalha de maneira simplificada este processo:



O art. 48 da LGPD determina que o controlador tem a obrigação de comunicar à ANPD e ao titular dos dados pessoais a ocorrência de incidente de segurança que venha a gerar risco ou dano considerado relevante aos titulares.

A ANPD recomenda que o prazo razoável para a comunicação de incidente seja de 2 (dois) dias úteis. Recomenda também que os controladores tenham cautela quanto ao julgamento acerca da relevância dos riscos e danos referentes ao incidente e, em caso de dúvida, realizem a comunicação do incidente o mais breve possível para que não ocorra eventual descumprimento da LGPD.

A ANPD afirma que, embora a responsabilidade e a obrigação pela comunicação do incidente sejam do controlador, podem ocorrer casos excepcionais em que tal comunicação provenha do operador, caso em que tal comunicação será devidamente analisada pela autoridade de proteção de dados[5].

2.1 Avaliar internamente o incidente

Quando a entidade tem conhecimento do incidente de segurança, deve ser realizada uma avaliação interna para que sejam obtidas informações como:

a) **Qual vulnerabilidade** foi explorada no evento, abrangendo situações como: acesso indevido aos dados pessoais; roubo de dados; ataques cibernéticos; erros de programação de aplicativos e sistemas internos; engenharia social; descartes indevidos; repasse de dados pessoais; roubo, venda e utilização de dados tutelados pela entidade; comprometimento de senhas de acesso; e outras.

b) **Fonte dos dados pessoais:** meio pelo qual foram obtidos os dados pessoais, tais como preenchimento de formulário eletrônico ou não eletrônico por parte do titular, API, uso compartilhado de dados, XML e cookies.

c) **Categoria de dados pessoais:** dados sensíveis, dados pessoais de crianças e adolescentes.

d) **Extensão do vazamento:** quantificar os titulares e os dados pessoais que tiveram a sua segurança violada neste evento.

e) **Avaliação do impacto ao titular:** avaliar quais são os impactos que o incidente pode gerar aos titulares.

[5] https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca, acesso em 22 de março de 2023,

f) **Avaliação do impacto no serviço:** avaliar os impactos que o incidente pode gerar a entidade como perda de confiabilidade do cidadão, ações judiciais, danos à imagem da instituição em âmbito nacional e internacional, prejuízo à entidade em contratos com fornecedores e clientes, e impacto total ou parcial nas atividades desenvolvidas pela entidade.

A figura abaixo mostra, de forma ilustrativa, as atividades da avaliação interna acima abordada:

Devem ser preservados o máximo de evidências do incidente e de todas as medidas adotadas a partir da sua ciência, a fim de que se possa demonstrar, para eventuais autoridades que posteriormente vierem a apurar os fatos, todas as ações realizadas para compreender o evento e reduzir seus efeitos. Isso permitirá uma compreensão completa da cadeia de diligências adotadas para lidar com a situação.

Nesse cenário, todos os passos devem ser devidamente documentados, desde o momento inicial de atuação até a contenção e os efeitos. Isso inclui, mas não se limita a:

a) Todos os logs dos sistemas internos e externos envolvidos no incidente;
b) Interações do time envolvido e todas as medidas adotadas;
c) Eventuais contratações de ferramentas e equipes de especialistas e auditores para atuação pontual no incidente a ser tratado.
d) Atas das reuniões relevantes.

À medida que o tratamento do incidente avançar, as informações de tal avaliação preliminar podem ser atualizadas.

2.1.1 – Relatório de Impacto à Proteção de Dados Pessoais

Diante de todas as evidências, é importante que a entidade avalie a necessidade de elaborar o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), pois o RIPD poderá ou deverá ser solicitado em casos específicos previstos na LGPD. São eles:

- Para tratamento de dados pessoais realizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (exceções previstas pelo inciso art. 4º, inciso III da LGPD);
- Quando houver infração da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos (arts. 31 e 32 da LGPD, combinados); e
- A qualquer momento, sob determinação da ANPD (art. 38).

O órgão deverá implementar o processo de elaboração e manutenção do Inventário de Dados Pessoais (IDP). Esse documento mostra detalhes da utilização dos dados pessoais por diversos programas, sistemas de informação ou processos existentes. O IDP contribui para a avaliação daquelas atividades que possam gerar impactos à proteção dos dados pessoais, a fim de decidir sobre a elaboração ou atualização do RIPD.

Além dos casos específicos previstos pela LGPD relativos à elaboração do RIPD, é indicada a elaboração ou atualização do Relatório de Impacto sempre que existir a possibilidade de ocorrer impacto na privacidade dos dados pessoais.

Fique por dentro
Consulte a seção 2 do modelo de RIPD publicado pela SGD para obter melhor entendimento sobre a necessidade de elaboração do RIPD.

Em síntese, o RIPD é um documento que pode ser solicitado pela ANPD e servirá de subsídio para o processo de gestão de incidentes com dados pessoais. Por essa razão, deve estar inserido no contexto mais amplo de gestão de riscos para todo órgão ou entidade federal. Sobre a gestão de riscos, recomenda-se a leitura da página específica

da SGD sobre o tema[6], dos demais guias operacionais disponíveis[7] e do Decreto nº 9.203, de 22 de novembro de 2017.

2.2 Comunicar ao encarregado da entidade

O art. 41 da LGPD determina que o controlador deverá indicar o encarregado pelo tratamento de dados pessoais. O § 1º do mesmo artigo estabelece que a identidade e os dados de contato do encarregado deverão ser divulgados de forma clara e objetiva, de preferência no site do controlador.

É importante que os órgãos e as entidades da administração pública federal criem mecanismos para facilitar que seus colaboradores internos (servidores, estagiários e terceirizados) notifiquem o Encarregado, a ETIR e os demais interessados nas situações necessárias.

O conhecimento de um incidente por qualquer colaborador, fornecedor ou parte interessada deve ensejar uma comunicação ao Encarregado, o mais rápido possível, para as providências previstas na LGPD e no portal da ANPD sobre comunicação de incidentes de segurança[8]. Ainda neste guia, o item 3.3.2.6 (notificação) explicará o processo de notificação de incidentes com mais detalhes.

2.3 Comunicar ao controlador

O Operador deve comunicar incidentes com dados pessoais ao Controlador o mais rápido possível, a fim de viabilizar que o Controlador exerça seu papel tempestivamente. O controlador é responsável em comunicar incidentes com dados pessoais a ANPD e aos titulares de dados.

Caso a relação entre Controlador e Operador seja feita em razão de contrato administrativo, tal obrigação de notificação tempestiva deve constar nas cláusulas contratuais, conforme a Instrução Normativa SGD/ME nº 31, de 23 de março de 2021.

[6] https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/gestao-riscos, acesso em 22 mar. 2023.
[7] https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd, acesso em 22 mar. 2023.
[8] https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca, acesso em 22 mar. 2023.

2.4 Comunicar à ANPD e ao titular de dados pessoais

A ANPD estipula o prazo de 2 (dois) dias úteis para comunicação de incidente de segurança a proteção de dados[9]. O art. 48 da LGPD determina que o controlador tem o dever de comunicar à ANPD e ao titular dos dados pessoais a ocorrência de incidente de segurança que tenha potencial de risco ou dano relevante ao titular.

Nesse contexto, é importante que a organização crie critérios, com base na LGPD e nos normativos e nas orientações da ANPD, que definam o que é um incidente que possa acarretar risco ou dano relevante aos titulares. Especialmente nos incidentes que envolvam dados do titular, é importante que se elabore um procedimento para potenciais questionamentos que venham a surgir.

Os profissionais que estarão na linha de frente do atendimento dos impactados pelo evento devem ser capacitados para conseguir lidar, satisfatoriamente e com segurança, com aspectos sobre o incidente. Isso inclui, mas não se limita a responder às seguintes questões:

a) **Quais informações foram objeto do incidente?**
b) **O titular pode ser vítima de fraude em razão do incidente?**
c) **O incidente foi devidamente comunicado às autoridades?**
d) **O que o titular pode fazer em benefício da sua proteção?**
e) **Onde o titular pode obter mais informações sobre o incidente?**

Esses questionamentos são apresentados apenas como direcionamento inicial e precisam ser aprofundados e ajustados em consonância com as particularidades do incidente. Desse modo, mitigam-se os riscos de que determinado titular fique sem respostas efetivas, por intermédio de mecanismos e instrumentos próprios da instituição para conferir uma resposta efetiva em incidentes.

Cabe ao Encarregado, diante das informações levantadas internamente e dos parâmetros estabelecidos pelo órgão, pela ANPD ou com base em boas práticas, avaliar

[9] https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca acesso em 22 de março de 2023

a necessidade e a profundidade da comunicação com a ANPD e com os titulares de dados. Nessas tarefas, a LGPD e os demais normativos infralegais vigentes sobre proteção de dados pessoais deverão ser sempre consultados e utilizados como balizas.

A Autoridade Nacional de Proteção de Dados disponibiliza, em seu sítio eletrônico, uma página com as orientações para a comunicação de incidentes de segurança. A página pode ser acessada no site da ANPD através do seguinte link: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca.

2.5 Comunicar à ETIR interna e ao CTIR Gov

A entidade deve estabelecer os métodos para realizar a comunicação ao Centro de Tratamento e Resposta a Incidentes Cibernéticos do Governo (CTIR Gov)[10] e à equipe de tratamento de incidentes cibernéticos internos do órgão (ETIR), quando houver. É fundamental que ambos tenham ciência do incidente de segurança. Tal comunicação permite a realização de ações conjuntas durante o tratamento do incidente com dados pessoais e pode igualmente ensejar uma resposta mais célere, técnica e eficaz.

O GSI estipulou na NC21 um modelo de relatório de comunicação de incidente de segurança[11] em redes computacionais com itens mínimos que devem conter em tais comunicações com o CTIR GOV.

2.6 Notificar os titulares de dados pessoais

Conforme a LGPD, cabe ao controlador comunicar ao titular dos dados pessoais a ocorrência de incidente de segurança que tenha potencial de lhe gerar riscos ou danos relevantes. Cabe à ANPD a regulamentação das situações de risco ou dano relevante ao titular. Até o momento da publicação deste guia, a ANPD ainda não havia regulamentado o tema, mas se recomenda que os leitores acompanham continuamente o site e os demais canais oficiais da Autoridade para novidades e atualizações.

[10] https://www.ctir.gov.br/, acesso em 22 mar. 2023.
[11] Consulte o Anexo A da Norma Complementar 21 disponível em https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=10/10/2014&jornal=1&pagina=7&totalArquivos=224

Paralelamente, a organização deverá avaliar o risco no âmbito interno, com objetivo de estipular se há ou não risco ou dano relevante para a comunicação do incidente ao titular. A SGD publicou guia de avaliação de riscos[12] que pode ser utilizado como referência para tal mensuração.

O que e como comunicar aos titulares de dados?

A comunicação do incidente aos titulares deve ser feita em linguagem clara e simplificada e mencionar, no que couber, os elementos previstos no §1º do Art. 48 da LGPD, tais como:

- A descrição geral do incidente e a data da ocorrência;
- A natureza dos dados pessoais afetados e os riscos relacionados ao incidente;
- As medidas tomadas e recomendadas para mitigar os efeitos do incidente;
- O contato do encarregado ou o ponto de contato para que os titulares obtenham informações a respeito do incidente;
- Outras informações que possam auxiliar os titulares a prevenir possíveis danos.

A comunicação deve ser feita de forma individual e diretamente aos titulares, sempre que possível.

Se, pela natureza do incidente, não for possível identificar individualmente os titulares afetados, devem ser comunicados todos os presentes na base de dados comprometida.

2.7 Emitir o relatório final do incidente

É importante que todas as informações e evidências coletadas e as ações do processo de tratamento de incidente de segurança à proteção de dados sejam documentadas, de modo a possibilitar a elaboração de um relatório final do incidente. Este documento deve: a) conter as devidas considerações para a promoção da melhoria

[12] https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_avaliacao_riscos.pdf, acesso em 22 mar. 2023.

contínua dos processos de tratamento de incidentes; e b) estar disponível para consulta em caso de atualização do relatório de impacto a proteção de dados (RIPD).

A ANPD pode solicitar o mencionado relatório para análise, com o propósito de:

- avaliar as ações tomadas durante um incidente em que dados pessoais tenham sido expostos ou comprometidos;
- publicar e atualizar normas referentes à proteção de dados;
- cumprir o princípio da responsabilização (art. 6º, inciso X da LGPD);
- Utilizá-lo como subsídio para eventuais questionamentos, facilitando a comprovação de conformidade.

2.8 Canais de comunicação de incidentes com dados pessoais

Os canais abaixo de contato poderão ser explorados no processo de comunicação de incidentes. Recorde-se, entretanto, que cada um dos órgãos listados a seguir possui atribuições legais e regimentais distintas, e que a ANPD é o ponto focal para LGPD e a autoridade administrativa fiscalizatória para recebimento de incidentes envolvendo dados pessoais:

- **ANPD**: formulário de comunicação de incidentes disponível no link[13];
- **Coordenação-Geral de Segurança da Informação (CGSIN/SGD/SEDGG/ME)**: e-mail para cgsin@economia.gov.br;
- **CTIR Gov**: e-mail para ctir@ctir.gov.br; a comunicação deve ser realizada preferencialmente pela equipe especializada (ETIR) ou pelo profissional que cumpre esse papel dentro da organização, seguindo os padrões de notificação de incidentes de segurança do CTIR Gov[14];
- **Polícia Federal**: apenas quando houver indícios de crime, de acordo com a Lei nº 12.737, de 30 de novembro de 2012, ou outras normas presentes na legislação penal extravagante, a Polícia Federal deverá ser comunicada através de ofício diretamente enviado ao Diretor.

[13] https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis

[14] https://www.gov.br/ctir/pt-br/canais_atendimento/padroes-para-notificacao-de-incidentes-de-seguranca-ao-ctir-gov, acesso em 10 mai. 2023.

3 RESPOSTA A INCIDENTES CIBERNÉTICOS

3.1 Estrutura organizacional de tratamento de incidentes cibernéticos na APF

No âmbito da APF, o Gabinete de Segurança Institucional (GSI) da Presidência da República, por meio do Departamento de Segurança da Informação e Cibernética (DSIC), é responsável por planejar, coordenar e supervisionar a atividade de segurança da informação no âmbito da administração pública federal, incluídos a segurança cibernética, a gestão de incidentes computacionais, a proteção de dados, o credenciamento de segurança e o tratamento de informações sigilosas[15].

Também são atribuições do DSIC: estimular a formação e a qualificação de recursos humanos na área de segurança da informação; elaborar normativos e requisitos metodológicos relativos à atividade nacional de segurança da informação, no âmbito da administração pública federal; manter o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, de responsabilidade nacional, para a proteção cibernética; coordenar e realizar ações destinadas à gestão de incidentes cibernéticos, quanto à prevenção, ao monitoramento, ao tratamento e à resposta a incidentes cibernéticos de responsabilidade nacional; coordenar a rede de equipes de prevenção, de tratamento e de resposta a incidentes cibernéticos formada por órgãos e entidades da administração pública federal; propor, implementar, acompanhar e avaliar tratados, acordos e outros atos internacionais relacionados à segurança da informação, em especial, ao tratamento e à troca de informações sigilosas; entre outras atribuições. O Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) faz parte do DSIC. Trata-se de um "Computer Security Incident Response Team (CSIRT)" ou Grupo de Resposta a Incidentes de Segurança, responsável por receber, analisar e responder a notificações e atividades relacionadas à segurança da informação de toda a APF.

O CTIR Gov tem ainda o objetivo coordenar e integrar as ações destinadas à gestão de incidentes computacionais em órgãos ou entidades da APF, bem como: prevenir, monitorar, analisar e mitigar os incidentes de segurança da informação; promover o

[15] Art. 19, do Decreto nº 11.331, de 1º de janeiro de 2023

intercâmbio científico-tecnológico; participar da articulação para o estabelecimento de diretrizes sobre gestão de incidentes computacionais; e criar processo de inteligência de ameaças cibernéticas para subsidiar criação de políticas públicas e tomada de decisão[16].

O Decreto nº 10.748, de 16 de julho de 2021, estabelece a criação da Rede Federal de Gestão de Incidentes Cibernéticos - Regic, que tem por finalidade aprimorar e manter a coordenação entre órgãos e entidades da administração pública federal direta, autárquica e fundacional para prevenção, tratamento e resposta a incidentes cibernéticos, de modo a elevar o nível de resiliência em segurança cibernética de seus ativos de informação. O CTIR Gov é o responsável por coordenar tal rede.

A participação dos órgãos da administração federal direta, autárquica e fundacional será obrigatória. Nesse sentido, aprovou-se em dezembro de 2022, o Plano de Gestão de Incidentes Cibernéticos para a Administração Pública Federal – PlangicL[17], que tem como objetivo estabelecer procedimentos de gestão de incidentes cibernéticos para os participantes da Regic. Ele complementa as políticas, estratégias e instruções normativas sobre o tema e deve ser observado pelos gestores e profissionais de segurança da informação dos órgãos e entidades participantes da Regic.

3.2 Planejamento de resposta a incidentes computacionais

É uma boa prática que cada entidade estabeleça e crie uma política de gestão de incidentes. Isso implica a criação de portfólios internos e procedimentos para o tratamento e a resposta a incidentes, seja o incidente de proteção com dados pessoais ou não.

A entidade deverá criar planos de resposta específicos para incidentes que violem a proteção de dados pessoais sob sua responsabilidade. Tais planos devem prever ações para a minimização de impactos aos titulares, em caso de vazamentos, e trilhas de comunicação tanto à ANPD quando aos titulares de dados pessoais quando a violação acarretar dano relevante aos titulares de dados pessoais.

[16] https://www.gov.br/ctir/pt-br/acesso-a-informacao/institucional/apresentacao, acesso 20 mar. 2023
[17] https://in.gov.br/en/web/dou/-/portaria-gsi/pr-n-120-de-21-de-dezembro-de-2022-452767918, acesso 20 mar. 2023

Recomenda-se que as organizações devem desenvolver a política de gestão de resposta a incidentes através dos seguintes mecanismos (NIST):

a) **Plano de resposta a incidentes:** criar planos de resposta a incidentes de acordo com a vulnerabilidade explorada, serviço impactado, severidade do incidente. Os planos de resposta a incidentes computacionais devem ter aprovação da alta gestão da entidade, e levar em conta aspectos como cultura organizacional, missão, valores e serviços prestados.

b) **Equipes para o tratamento de incidentes computacionais:** criar e treinar equipes especializadas para o tratamento de incidentes computacionais, cabendo-lhes o papel de atuação para resolução do incidente, restauração do ambiente e comunicação interna e externa à organização. No âmbito da APF, a Norma Complementar nº 05/IN01/DSIC/GSIPR disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais.

c) **Procedimentos internos e relatórios para ações de resposta:** criar plano de resposta a incidentes computacionais que contenha procedimentos com tarefas específicas a serem executadas por uma determinada equipe para a contenção e mitigação de incidentes e restauração dos serviços ao estado pré-incidente, quando possível.

d) **Diretrizes e o plano de comunicação:** informar através do plano de resposta a incidentes quando e como devem ser realizadas as comunicações de incidentes, seja com fornecedores, empresas e órgãos parceiros como o CTIR Gov (para auxiliar a resolução do incidente), seja com clientes, (para informar sobre os impactos que o incidente pode gerar aos clientes e titulares de dados pessoais), seja com entidades de controle como a ANPD.

e) **Linhas de comunicação entre as equipes que podem atuar na resposta a incidentes:** estabelecer comunicação com outros departamentos internos da organização, tais como jurídico, de pessoal e de comunicação externa.

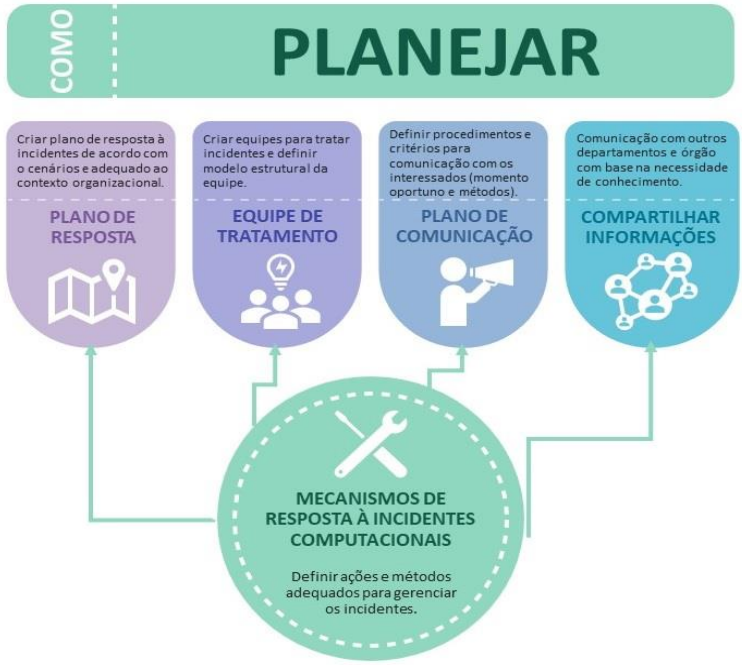
f) **Modelo estrutural das equipes de pessoal envolvidas:** definir qual modelo de equipe para tratamento de incidente será utilizado: interno, misto ou terceirizada:

- ✓ **Interno:** equipe de reposta a incidentes na qual todos os integrantes são funcionários da organização, podendo atuar em outros departamentos de forma simultânea;
- ✓ **Equipe mista:** quando parte da equipe de resposta a incidentes é terceirizada e os demais integrantes são servidores;
- ✓ **Equipe terceirizada:** toda a equipe é composta por terceirizados; neste modelo, é importante que a gerência da equipe seja exercida por um servidor.

Fique por dentro

O DSIC sugere ainda um quarto modelo de equipe de tratamento de incidente: o **centralizado**, no qual todos os integrantes atuam

g) **Serviços providos pela equipe de resposta a incidentes:** informar qual equipe é responsável por aquele determinado incidente e quais são os serviços que esta equipe deve prover; se necessário, informar também a quem a equipe deve recorrer caso necessite de recursos extras, tais como especialistas e equipamentos.



A resposta a incidentes de segurança ajuda as equipes envolvidas a minimizar os impactos causados pela perda ou pelo roubo de informações, bem como pela

interrupção de serviços causados por incidentes. Outro benefício esperado pela implementação de um processo de resposta a incidentes é poder utilizar todas as informações obtidas durante um evento de incidente para atualizar e melhorar os procedimentos de tratamento de incidente.

3.3 Tratamento de incidentes computacionais

Segundo o NIST[18], o processo de resposta a incidentes possui 4 (quatro) fases:

Preparação: a entidade deve criar e treinar equipes para atuar na resposta a incidentes, além de limitar o número de incidentes, selecionando e implementando controles com base em avaliações de risco.

Detecção e análise de incidentes: a entidade deve adotar meios para detecção de incidentes e analisar tais eventos, buscando documentar, priorizar e notificar; esta fase também pode ser executada em conjunto com a fase posterior.

Contenção, erradicação e recuperação: fase em que são implementadas ações para contenção, erradicação e recuperação do incidente; aqui, também são identificadas as origens de ataques e coletadas as evidências.

Atividades pós-incidente: a entidade deve realizar atividades para melhorar o tratamento de novos incidentes.

[18] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf página 21

3.3.1 Preparação

É importante que as organizações e as entidades se preparem não somente no que concerne à ação em caso de incidentes, mas também na prevenção a incidentes que venham a ocorrer. Isso garante que sistemas, redes e aplicativos estejam seguros o suficiente.

Durante o processo de resposta a incidentes, faz-se necessário que o profissional integrante da equipe de resposta a incidentes tenha acesso a ferramentas de comunicação que venham auxiliar e apoiar todo o tratamento do incidente. Seguem algumas destas ferramentas:

a) Lista com os contatos de outros integrantes da equipe de resposta a incidentes, fornecedores, representantes e plantonistas de outras equipes e departamentos, além de ferramentas para acionamento.
b) Ferramenta para registro dos incidentes, ações da equipe de tratamento de incidentes, upload de logs e evidências, e status do incidente. É importante que seja disponibilizado um canal para registro anônimo de incidentes.
c) Ferramenta que tenha a capacidade de rastrear problemas recorrentes e novos, com repositório de informações referentes a incidentes tratados anteriormente e suas respectivas evidências de tratamento.
d) Repositório de procedimentos para resolução de incidentes.
e) Smartphones para acionamento de plantonistas.
f) Local para reunião de equipes durante a resolução de incidentes graves, chamada informalmente de “sala de guerra” ou “sala de crise”.

g) Equipamentos de tecnologia como impressoras, câmeras, estações de trabalho e sobressalentes para uso emergencial em caso de necessidade.
h) Software para obtenção, análise e perícia forense de evidências.
i) Ferramentas para recuperação de backup de sistemas e dados.

É importante que a organização consiga realizar de forma constante, exercícios e simulações de casos reais de incidentes, para treinar as equipes envolvidas nos processos de resposta a incidentes, neste momento podem ser identificados pontos de melhoria, e implementados novas ferramentas e métodos de trabalho.

3.3.1.1. Prevenção de Incidentes Computacionais

Caso a organização não tenha controles de segurança suficientes, os eventos de incidentes de forma recorrente podem sobrecarregar a equipe de resposta a incidentes, o que pode levar a tratamentos mais lentos e até mesmo incompletos, que por sua vez se revertem em impactos negativos maiores ao negócio.

A equipe de resposta a incidentes pode ter capacidade de identificar problemas dos quais a organização não está ciente. Logo, possui potencial de desempenhar um importante papel na avaliação de riscos e no treinamento, identificando vulnerabilidades.

A seguir, são apresentadas algumas boas práticas para a proteção de redes, sistemas e aplicativos:

a) **Avaliação de riscos:** realizar avaliações de riscos de forma periódica, visando a levantar o cenário de exposição a ameaças e vulnerabilidades. A LGPD tornou necessária a elaboração do RIPD para o tratamento de dados pessoais.
b) **Segurança de host:** o ambiente computacional deve ser protegido de forma apropriada, usando configurações de segurança adequadas. Além disso, é essencial manter a política de privilégio mínimo ao ambiente computacional, concedendo aos usuários somente os privilégios necessários para execução de tarefas previamente autorizadas. É importante manter habilitadas as

funções de auditoria para que os logs registrem eventos considerados significativos à segurança do host.

c) **Segurança de rede:** estabelecer e configurar o perímetro de segurança de rede a fim de negar quaisquer tentativas de acessos não permitidas.

d) **Prevenção contra malware:** instalar software de detecção, bloqueio e remoção de malwares em todos os hosts e serviços de e-mail da organização.

e) **Conscientização e treinamento de usuários:** manter os usuários cientes das principais ameaças do mundo cibernético e das políticas de segurança da organização, tais como o uso adequado de equipamentos, redes de Internet e Intranet, sistemas e acesso adequado as instalações físicas.

f) **Treinamento da equipe:** treinar as equipes de TI da organização para que usem e mantenham seus equipamentos e sistemas seguros de acordo com as políticas de segurança da organização.

3.3.2 Detecção e análise de incidentes computacionais

Para muitas organizações, a parte mais desafiadora do processo de resposta a incidentes é detectar e analisar de forma correta a magnitude e os impactos do possível incidente dentro da organização.

Os incidentes podem ser detectados por vários meios. Alguns deles são a monitoração automatizada e a manual dos recursos computacionais da organização:

a) **Monitoração automatizada:** monitorar todo o ambiente de infraestrutura tecnológica e respectivos logs por intermédio de softwares específicos.

b) **Monitoração manual:** relato de usuários através de e-mail, central de atendimento, ferramenta de registro de incidentes e até mesmo de forma presencial.

3.3.2.1 Vetores de ataques

Um incidente pode acontecer de inúmeras maneiras. Portanto, é difícil desenvolver planos e procedimentos para a resposta de todos os incidentes que venham a ocorrer. A organização deve atuar na resposta de todos os incidentes. Entretanto, deve direcionar seus planos de incidentes para aqueles tipos que utilizam vetores de ataque comuns e corriqueiros., alguns exemplos destes vetores são:

a) Dispositivos de armazenamento externo removíveis;
b) DDOS - ataque distribuído de negação de serviço;
c) Sítios da web;
d) E-mail;
e) Engenharia social;
f) Perda ou roubo de equipamentos; e
g) Uso inadequado de equipamentos.

3.3.2.2 Sinais de incidente computacional

Existem duas categorias de sinais de um incidente:

- **Precursores:** sinal de que um incidente pode ocorrer no futuro;
- **Indicador:** sinal de que um incidente já ocorreu ou está ocorrendo agora.

Se for possível identificar um precursor, a organização poderá preparar-se na prevenção a um incidente, realizando as ações necessárias.

3.3.2.3 Análise

A detecção e a análise de incidentes são atividades complexas, pois cada alerta e cada indicador de indisponibilidade podem ser imprecisos, gerando assim alertas de falso positivo. O ideal seria analisar cada alerta e indicador de maneira separada, para assim identificar se um alerta específico pode ser interpretado como um incidente. Contudo, tal tarefa é vista como inviável em organizações de grande porte, devido ao grande volume de alarmes que podem surgir. Indicadores como modificação de arquivos

importantes, indisponibilidade de sistemas e falhas em hosts podem ser consequência de erro humano durante a execução de tarefas corriqueiras.

Mesmo assim, a existência de indicadores e alarmes podem indicar a ocorrência de um evento que venha a ser classificado como incidente de segurança. Nesse ponto, é importante utilizar equipes com ferramentas para monitoração e detecção de alarmes e indicadores que possam filtrar e identificar possíveis incidentes. Uma boa prática é a implementação de *Security Operations Center* (SOC) (em português, Centro de Operações de Segurança), que é uma equipe dedicada que utiliza ferramentas específicas e cujo objetivo é prestar serviços de detecção e reação a incidentes de segurança.

Em muitos casos, tal equipe pode ser a primeira a lidar com o incidente. É fundamental que ela tenha em mãos procedimentos padrão para ação imediata. Caso o incidente não seja solucionado mesmo após a atuação desta equipe, competir-lhe-á comunicar e escalar o evento para outras equipes que possam solucionar o incidente.

Através de uma análise inicial, a equipe deve obter informações suficientes para definir as atividades a serem executadas posteriormente como contenção do incidente e análise detalhada dos efeitos do incidente.

a) Visando tornar a análise de incidentes mais fácil e eficaz, seguem abaixo algumas recomendações: **Perfis de redes e sistemas:** criar perfil para registrar as atividades esperadas, facilitando o registro e a detecção de tarefas que não são corriqueiras e que podem gerar como consequência um incidente.
b) **Comportamento normal:** estudar sistemas, aplicativos e redes para conseguir identificar quando há um comportamento anormal de um dos ativos supracitados. Caso a equipe de resposta a incidentes não tenha esse conhecimento, a equipe deve conseguir entrar em contato com quem consiga realizar essa análise comportamental de forma eficiente.
c) **Obtenção e retenção de log:** utilizar ferramentas obtenção e análise de logs é fundamental para identificar se há anormalidade em alguns dos equipamentos e sistemas de tecnologia. As ferramentas devem seguir uma política de segurança que informe onde e por quanto tempo os logs devem

ser mantidos. Segundo a Norma Complementar nº 21/IN01/DSIC/GSIPR[19], o tempo mínimo de retenção de logs é de 6 (seis) meses, mas cabe à organização, por meio de sua política de segurança da informação, definir este prazo. A SGD publicou o Modelo de Política de Gestão de Registros (Logs)[20] de Auditoria com o objetivo de auxiliar os órgãos da APF quanto a obtenção e retenção de log.

d) **Correlação de eventos:** executar a correlação de eventos, pois as evidências de um incidente podem ser obtidas através de vários registros que contenham diferentes tipos de dados; ao realizar a correlação de vários eventos e de indicadores, será possível identificar se um incidente de segurança de fato ocorreu.

e) **Relógio dos hosts sincronizados:** manter os relógios dos hosts sincronizados através de protocolos como Network Time Protocol (NTP) faz com que a correlação de hosts seja mais fácil.

f) **Base de conhecimento de informações:** manter e usar uma base de conhecimento de informações que contenha procedimentos que a equipe de resposta a incidentes precisa para utilizar como referência de ações a serem realizadas.

g) **Motores de busca da Internet:** motores de pesquisa da internet como Google e Bing podem ajudar a equipe de resposta a incidentes a encontrar informações sobre atividades comuns.

h) **Analisadores de pacotes:** realizar execução de *sniffers* (analisadores) de pacotes para coletar dados adicionais, pois alarmes e indicadores podem não registrar e podem apresentar informações com dados insuficientes para

> Caso a ETIR identifique que o incidente envolve dados pessoais, é importante iniciar o plano de comunicação envolvendo o encarregado e controlador da organização.

19 https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=10/10/2014&jornal=1&pagina=5&totalArquivos=224, acesso em 23 mar. 2023

20 https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/modelo_politica_logs_auditoria.pdf

a equipe de resposta a incidentes. Por motivo de privacidade, pode ser necessária a autorização especial para execução de *sniffers* em algumas redes.

i) **Filtro de alarmes:** realizar o filtro de alarmes, visto que pode não haver tempo suficiente para análise de toda uma massa de dados exposta em um alarme; assim, é interessante possuir o recurso de filtragem de alarme dentro das ferramentas que apresentam os alarmes à equipe de resposta a incidentes.

j) **Ajuda de terceiros:** procurar a ajuda de outras equipes de tratamento de incidente de redes computacionais, fornecedores e organizações parceiras, pois pode acontecer de a equipe de resposta a incidentes ser incapaz de determinar com exatidão a causa e a natureza de um incidente sem o auxílio de terceiros. Essa comunicação pode ser estendida por todo o processo de tratamento. A Rede Federal de Gestão de Incidentes pode auxiliar com a análise de informações, assim como os outros centros de referências que podem ser encontrados no link https://www.cert.br/csirts/brasil/.

3.3.2.4 Documentação

A partir do momento em que há a suspeita de um incidente, a equipe de reposta a incidentes deve registrar todas as ações relativas ao incidente, criando um ou mais documentos de tratamento de um incidente específico, como citado anteriormente no item 3.2.1 (preparação para o incidente).

É fundamental que a equipe de resposta a incidentes atualize o status e o histórico do incidente, sempre que possível. Como citado anteriormente, usar uma ferramenta de rastreamento de problemas anteriores pode ajudar bastante na resolução de novos incidentes, além de prover dados para fiscalização e controle da equipe de resposta a incidentes, buscando garantir a resolução e tratamento de incidente em tempo hábil. Este sistema de rastreamento de problemas pode conter as seguintes informações:

a) Status atual dos incidentes: novo, em andamento, encaminhado para investigação, pendente de informações ou ações de terceiros, resolvido, fechado etc.;

b) Resumo do incidente;

c) Indicadores relacionados ao incidente;

d) Outros incidentes relacionados a este evento específico;

e) Ações realizadas pela equipe de resposta e demais equipes que venham atuar neste incidente;

f) Cadeia de escalonamento, se aplicável;

g) Avaliações de impactos relacionados ao incidente;

h) Informações de contato com outras equipes envolvidas, terceiros e organizações parceiras;

i) Relação de evidências coletadas durante o tratamento do incidente;

j) Comentários e notas das pessoas que atuaram no incidente;

k) Próximas etapas a serem executas após a resolução do incidente.

A equipe de resposta a incidentes tem o dever de proteger os dados coletados e restringir o acesso a eles, pois tais dados podem ter informações confidenciais, e apenas o pessoal autorizado deve ter acesso a estas informações.

3.3.2.5 Priorização

A priorização do tratamento de incidentes é importante para a correta alocação de recursos em áreas e sistemas que sejam chave para o contexto da APF. As seguintes informações devem ser utilizadas para a definição da ordem de prioridade no tratamento dos incidentes:

a) **Impacto no negócio**: a equipe de resposta a incidentes deve considerar como o incidente em tratamento pode impactar negativamente o negócio da organização, devendo realizar uma avaliação que leve em consideração os impactos futuros que o incidente pode trazer a organização. A seguir, compartilha-se uma tabela com os possíveis níveis de impacto no negócio:

Categoria	Definição
Nenhum	Não afeta a capacidade da organização de fornecer todos os serviços a todos os usuários.
Baixo	Efeito mínimo; a organização ainda pode fornecer todos os serviços essenciais para todos os usuários, mas perdeu eficiência.

Médio	A organização perdeu a capacidade de fornecer um serviço crítico a um subconjunto de usuários do sistema.
Alto	A organização não é mais capaz de fornecer alguns serviços essenciais a nenhum usuário.

b) **Impacto em dados e informações:** incidentes podem afetar a confidencialidade, a integridade e a disponibilidade dos dados e informações de uma organização. A equipe de resposta a incidentes deve, diante das opções para tratamento, mensurar os impactos que tais alternativas possam gerar tanto para a própria organização como para outros entes parceiros. A seguir, compartilha-se uma tabela com os possíveis níveis de impacto em dados e informações:

Categoria	Definição
Nenhum	Nenhuma informação relevante foi exposta, alterada, excluída ou de alguma maneira comprometida.
Violação de privacidade	Informações confidenciais de identificação pessoal (DP) de contribuintes, funcionários, beneficiários etc. foram acessadas ou expostas.
Violação Proprietária	Informações proprietárias não classificadas, como informações de infraestrutura crítica protegida (PCII), foram acessadas ou expostas.
Perda de Integridade	Informações confidenciais ou proprietárias foram alteradas ou excluídas.

c) **Recuperabilidade:** os impactos de um incidente determinam os recursos e o tempo necessários para a recuperação. A equipe responsável tem o papel de identificar e avaliar os recursos disponíveis, bem como a relevância da recuperação do incidente para a organização. Compartilha-se a seguir uma tabela com níveis de recuperabilidade:

Categoria	Definição
Regular	O tempo de recuperação é previsível com os recursos existentes.
Suplementado	O tempo de recuperação é previsível com recursos adicionais.
Estendido	O tempo de recuperação é imprevisível; recursos adicionais e ajuda externa são necessários.
Não Recuperável	A recuperação do incidente não é possível (por exemplo, dados confidenciais expostos e postados publicamente); lançar investigação.

A capacidade de recuperação de um incidente determina os possíveis procedimentos que a equipe de resposta a incidentes deve seguir para o tratamento. Um incidente de alto impacto aos negócios da organização e de fácil recuperação pode ser aquele em que a equipe de resposta a incidentes atue primeiro, tratando e solucionando o incidente. No entanto, pode haver casos de vazamento de dados pessoais em que seria necessário envolver não só pessoas e equipes internas da organização, mas titulares de dados e órgão de fiscalização (ANPD). Dessa forma, a comunicação e a recuperação podem ser realizadas de forma simultânea.

A equipe de resposta a incidentes deve priorizar a resposta a cada incidente de acordo com as estimativas de impacto e os recursos e esforços necessários para a sua recuperação.

Exemplos nesse sentido podem ser abordados para ilustrar as ideias acima. Um órgão hipotético que gerencia vários sistemas e serviços sofreu dois ataques diferentes. As situações são descritas no quadro abaixo.

Exemplo 1	**Exemplo 2**
A base de dados do cadastro de um dos seus serviços disponibilizados pelo órgão foi atacada. Como resultado, o atacante teve acesso direto aos dados desta base. Seguindo as etapas de priorização, foi definido que o impacto ao negócio é “alto”, pois a estratégia de contenção é desligar a base de dados, tornando indisponível a realização de novos cadastros. Já o impacto aos dados e informações foi classificado como “Violação de privacidade”, pois o atacante obteve acesso a base de dados do serviço e os publicou. Sua recuperabilidade foi classificada como “não recuperável”, pois a base de dados do serviço foi publicada em fóruns da internet.	O serviço de biblioteca do órgão foi impactado e ficou indisponível durante o ataque. Seguindo as etapas de priorização, foi definido que o impacto deste incidente ao negócio é “baixo”, pois a indisponibilidade deste serviço afetaria poucos usuários. Já o impacto aos dados e informações do serviço também foi classificado como “nenhum”, pois o catálogo de dados é público e seu acesso indevido não gera danos ao proprietário dos dados. Enfim, sua recuperabilidade foi classificada como “regular”, pois o órgão consegue aplicar as ações de recuperação de forma rápida sem a necessidade de empenho de recursos adicionais.

Utilizando como base os cenários expostos, a tabela de classificação seria definida desta forma:

	Exemplo 1	**Exemplo 2**
Impacto ao negócio	Alto	Baixo
Impacto aos dados e informações	Violação de privacidade	Nenhum
Recuperabilidade	Não recuperável	Regular

Com base na tabela de análise acima, o cenário do exemplo 1 teria prioridade de tratamento, pois tal incidente tem maior potencial de impacto e sua recuperabilidade é mais complexa.

É importante ressaltar que os exemplos aqui demonstrados são meramente ilustrativos. Assim, **a organização deve realizar a avaliação de riscos de forma contínua para que assim consiga mensurar o grau de severidade de um determinado incidente que venha a ocorrer**. O guia de avaliação de riscos de segurança e privacidade elaborado pela SGD pode auxiliar na classificação de impactos de um incidente e, assim, definir sua escala de priorização dentro de uma organização.

É importante que a organização crie métodos com base na LGPD, nos normativos e nas orientações da ANPD, que possam definir o que é um incidente que venha acarretar risco ou dano relevante aos titulares dos dados pessoais, bem como a priorização do tratamento desse incidente em relação aos demais.

A LGPD enfatiza a importância do relatório (RIPD). A Secretaria de Governo Digital também elaborou um guia para orientação a organizações quanto à elaboração do RIPD, que está disponível na página de Guias Operacionais para Adequação à LGPD[21].

[21] https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd, acesso em 23 mar. 2023

3.3.2.6 Notificação

Convém que o plano de resposta a incidentes informe qual equipe é responsável pela notificação do incidente logo após a análise e a priorização, e quem deve ser notificado. A seguir, são listados exemplos de atores que devem ser notificados em caso de incidentes:

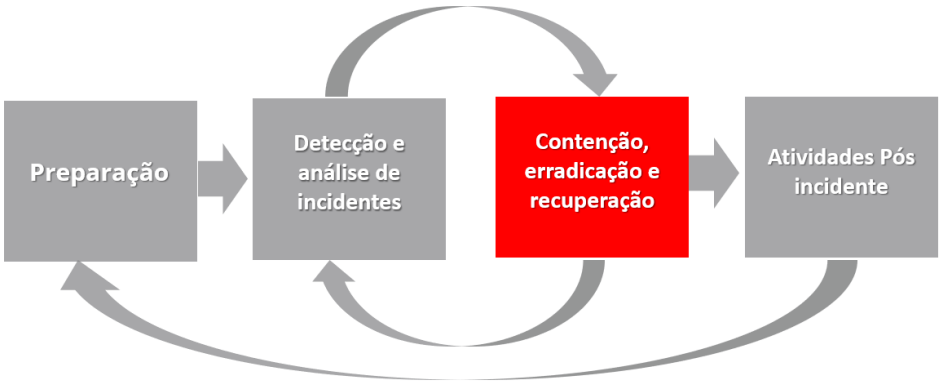
a) CIO (responsável por todo o departamento de TI de uma organização);
b) Chefe de segurança da informação;
c) Líder técnico de segurança da informação;
d) Equipes internas de resposta a incidentes;
e) Responsável pelo recurso afetado;
f) Recursos humanos (em casos que envolvam funcionários);
g) Departamento de comunicação Social;
h) Departamento jurídico;
i) CTIR Gov e ETIR interno (no segundo caso, quando houver tal estrutura dentro da organização);
j) Encarregado, controlador, ANPD e titulares de dados (em caso de incidentes envolvendo dados pessoais);
k) Polícia Federal (quando houver indícios de crimes).

Durante o tratamento do incidente, a equipe responsável pela comunicação pode se utilizar de alguns meios para notificar os indivíduos e atualizar o relatório de tratamento de incidente. Alguns desses meios são:

a) E-mail;
b) Site e portal de comunicação;
c) Ligação telefônica;
d) Aplicativos de mensagens instantâneas;
e) SMS;
f) Reuniões;
g) Avisos em quadros e cartazes.

Para notificação ao CTIR Gov, a entidade deve seguir os padrões de notificação de incidentes de segurança ao CTIR Gov[22].

3.3.3 Contenção, erradicação e recuperação



Após a detecção e a análise do incidente, devem ser realizadas ações buscando a remediação ou a restauração dos recursos atacados e, quando possível, a recuperação de tais recursos ao estado anterior ao ataque. Para isso, devem ser seguidos os procedimentos já estabelecidos internamente para resposta a incidentes.

3.3.3.1 Estratégia de contenção

É importante que sejam realizadas tarefas de contenção do incidente antes que este comece a sobrecarregar os recursos e aumente os danos para a organização. A contenção ajuda aumentar a janela de tempo para o desenvolvimento de medidas que venham a erradicar o incidente.

A tomada de decisão é parte importante durante o processo de contenção. Exemplos de tomadas de decisão podem abranger desligar um host, realizar ou cancelar o backup, ou desconectar um equipamento à rede. Tais decisões devem ser descritas nos procedimentos para ação em caso de incidentes, de forma que a equipe de resposta consiga tomá-las de forma ágil.

As estratégias de contenção variam de acordo com o tipo de incidente que a organização pode ter que lidar. A estratégia de contenção de malware, por exemplo, é

[22] https://www.gov.br/ctir/pt-br/canais_atendimento/padroes-para-notificacao-de-incidentes-de-seguranca-ao-ctir-gov, acesso em 10 mai. 2023

diferente da estratégia de contenção de um ataque de negação de serviço distribuído (DDoS).

Criar e documentar estratégias de contenção separadas para cada tipo de incidente é de grande relevância. Os critérios para determinar se uma estratégia de contenção pode ser aplicada a um determinado incidente incluem:

a) Danos potenciais e roubo de recursos;
b) Necessidade de preservação de evidências;
c) Disponibilidade do serviço;
d) Tempo e recursos necessários para implementar a estratégia;
e) Eficácia da estratégia (contenção parcial ou total);
f) Duração da solução (quanto tempo uma solução temporária ou alternativa deve durar).

Um exemplo de estratégia é a *sandboxing*, em que o invasor é direcionado a uma área restrita para que a equipe de resposta a incidentes consiga monitorar e evidenciar suas ações. Porém, devem ser calculados os impactos exatos e os riscos que tal estratégia pode conter.

Outro exemplo de estratégia de contenção é a *honeypot*, em que o invasor e atraído para um sistema ou ambiente monitorado que não venha impactar de forma substancial os sistemas e serviços da organização. Isso também possibilita a observação do comportamento do invasor, a identificação de padrões de ataque e a criação de contramedidas em benefício da organização. Impactos e riscos também devem ser aferidos nesse caso.

Fique atento

Durante a contenção, é importante que todas as atividades relacionadas ao incidente e as medidas de contenção tomadas sejam registradas, evitando-se a perda de evidências. A inclusão do histórico na base de conhecimento também auxilia as equipes responsáveis na compreensão dos eventos e no ganho de maturidade.

É fundamental, ainda, que todos os atores envolvidos no processo trabalhem de forma coordenada e colaborativa para que a instituição mitigue o quanto antes o incidente.

Nesse contexto, a estratégia de contenção deve ser avaliada com cautela. Há a possibilidade de que a ação de contenção gere impactos maiores e mais substantivos à

organização. Um exemplo prático desse quadro é quando um determinado servidor realiza a replicação de perfis acessos em todos os sistemas da organização. Caso esse servidor esteja comprometido e a estratégia de contenção for desconectá-lo ou desligá-lo, as novas replicações de perfis podem não acontecer. Isso gerará impactos à inclusão e à exclusão dos usuários de sistemas que utilizam tal serviço do servidor atacado.

Como exposto, as estratégias de contenção devem ser bem elaboradas e seguir o plano de incidentes, visto que utilizar a estratégia errada no momento inadequado pode trazer como consequência impactos ainda mais severos à organização.

3.3.3.2 Coleta e manuseio de evidências

A coleta de evidências de um incidente tem como fator principal a busca por resolução do incidente. Contudo, a coleta de tais evidências também pode auxiliar outros departamentos a melhorar procedimentos ou até mesmo a obter informações e provas relevantes em processos judiciais.

A coleta de evidências deve seguir procedimentos pré-estabelecidos. É importante igualmente que a coleta atenda integralmente à legislação e às decisões judiciais que podem ser aplicados em cada situação, observando-se as especificidades do país. Sem prejuízo das boas práticas internacionais, deve ser recordado que, no âmbito jurídico brasileiro, as evidências de tecnologia da informação podem constituir provas e ter efeitos importantes para a resolução de um processo administrativo ou judicial.

As regras aplicáveis no Brasil podem abranger tratados internacionais ratificados pelo país, Constituição Federal, leis ordinárias, leis complementares, decretos, resoluções, instruções normativas, portarias e outros atos administrativos com caráter normativo. Ainda sobre o país, as decisões judiciais podem advir de vários órgãos do Poder Judiciário, incluindo o Supremo Tribunal Federal, o Superior Tribunal de Justiça e os órgãos da Justiça Federal, da Justiça do Trabalho, da Justiça Eleitoral, da Justiça Militar e das Justiças dos Estados e do Distrito Federal e Territórios.

No caso das instituições da administração pública federal (APF), a coleta de evidências é obrigatória, conforme Norma Complementar nº 21/IN01/DSIC/GSIPR. São necessárias a documentação e a preservação de todas as informações de coleta e

manuseio das evidências, garantindo níveis de segurança adequados. É aconselhável manter um registro detalhado de todas as evidências, o que abrange inclusive informações sobre:

a) Identificação (endereços IP e MAC, porta de rede, número de série, sistema operacional, nome do host, localização);
b) Nome, matrícula, equipe e organização do indivíduo que realizou qualquer manuseio da evidência;
c) Hora e data de cada ocorrência de manipulação da evidência;
d) Locais onde as evidências foram armazenadas e podem ser acessadas.

A coleta de evidências de recursos de tecnologia pode apresentar alguns desafios. É desejável adquirir evidências de um sistema quando já existir a suspeita de incidente.

A coleta inicial de evidências pode conter informações que auxiliem a equipe de resposta a incidentes a identificar o problema principal e sua origem de forma ágil, auxiliando na solução do evento com maior celeridade. A coleta instantânea da evidência traz informações de como todo o ambiente se encontra, antes de qualquer ação da equipe de resposta a incidentes e de outros indivíduos que tenham alguma atuação no incidente. Tal medida ajuda, assim, na recuperação eficaz dos recursos e dos serviços.

3.3.3.3 Identificar a origem de ataques

É necessário identificar a origem de ataques durante o tratamento de incidentes. Não obstante, embora isso seja importante, a equipe de resposta a incidentes deve manter o enfoque na contenção, na erradicação e na recuperação.

A identificação de origem pode ser um processo demorado e, de certa maneira, atrapalhar a equipe de resposta a incidentes a atingir seu objetivo principal, que é minimizar o impacto do evento nos serviços e nos negócios da organização. Portanto, tal tarefa deve ser realizada de maneira estratégica, priorizando as ações de contenção e de acordo com a disponibilidade da equipe.

A seguir, são enumeradas algumas das atividades mais comuns para identificar a origem de um ataque:

a) **Validação o endereço IP:** utilizar técnicas para identificar e validar o endereço de IP do host de ataque.

b) **Pesquisa de endereço de IP:** realizar uma pesquisa do IP do atacante em motores de busca pode levar a mais informações sobre o ataque.

c) **Banco de dados de incidentes:** alguns grupos realizam a coleta e consolidação de eventos que ocorreram em diferentes organizações, gerando um banco de dados de incidentes. A organização também pode consultar sua base particular de incidentes para identificar semelhanças com eventos antigos.

d) **Monitorar canais de comunicação:** a equipe de resposta a incidentes pode monitorar canais de comunicação que são utilizados com frequência em ataques.

3.3.3.4 Erradicação e recuperação

Depois da contenção, a erradicação pode ser necessária para eliminar resquícios do incidente, como exclusão de malware, exclusão de contas violadas, e identificação e tratamento das vulnerabilidades exploradas.

Na erradicação, é importante identificar todos os recursos da organização que possam ser corrigidos. Podem ocorrer incidentes em que a erradicação é executada como uma etapa separada, mas continua fazendo parte do processo de recuperação.

Durante a recuperação, os sistemas são restaurados para seu estado normal, e os administradores dos sistemas devem confirmar se tais sistemas estão operando de maneira adequada. A recuperação pode envolver ações como alteração de senhas de rede, reconfiguração de regras de firewall, restauração de backup, reconstrução de sistemas e de toda base de dados, instalação de patches de segurança, substituição de arquivos corrompidos por versões limpas. Evidências coletadas no início da tratativa do incidente podem ser utilizadas para determinar qual o estado em que os recursos devem ser entregues à operação após a recuperação.

A erradicação e a recuperação devem ser utilizadas como abordagens de remediação do incidente. Para incidentes de grande escala, a recuperação total ou em

níveis aceitáveis pode levar meses. Desse modo, é importante priorizar o aumento dos níveis gerais de segurança e correções de recursos alto valor agregado para a organização nos primeiros dias, a fim de evitar novos incidentes. As demais etapas podem manter o enfoque em mudanças de longo prazo, com o objetivo de elevar todo o nível de segurança da organização.

3.3.4 Atividades pós-incidente

A organização deve implementar algumas atividades em busca da melhoria contínua de seus processos de resposta a incidentes, além de definir procedimentos para retenção de evidências e uso dos dados coletados em incidentes. Após a ocorrência de um incidente, por exemplo, a organização deve mapear as vulnerabilidades exploradas e aplicar as devidas correções em todos os seus sistemas, elevando o nível de segurança.

3.3.4.1 Lições aprendidas

Uma das partes de maior importância da resposta a incidentes é a de lições aprendidas, em busca de melhoria contínua dos processos. Cada equipe envolvida no processo de tratamento de incidentes deve buscar melhorar seus procedimentos, conduzindo a uma maior eficiência na proteção contra ameaças cibernéticas.

Reuniões periódicas ou até mesmo após a ocorrência de um incidente são importantes para revisar como o evento ocorreu, o que foi feito durante as tratativas e se as ações surtiram efeito positivo. Algumas das perguntas a serem respondidas em tais reuniões:

a) Onde, quando, como e o que de fato aconteceu?

b) Qual a eficácia da equipe de resposta a incidentes e de sua gerência neste(s) evento(s)?
c) Foram seguidos procedimentos já documentados? Em caso afirmativo, eles foram suficientes?
d) Foi necessário executar procedimentos não documentados? Em caso afirmativo, eles foram executados com sucesso e documentados?
e) Quais informações anteriores ao incidente foram necessárias?
f) Foram realizadas quaisquer ações que possam ter prejudicado a recuperação?
g) O que pode ser atualizado para melhorar o tratamento de incidentes?
h) Como melhorar o compartilhamento de informações?
i) Quais ações corretivas podem ou devem ser tomadas para evitar incidentes semelhantes no futuro?
j) Quais alarmes e indicadores devem ser observados para detectar incidentes semelhantes no futuro?
k) Quais recursos adicionais podem ser utilizados para detectar incidentes semelhantes?

Os relatórios dessas reuniões podem ser utilizados para atualizar os procedimentos operacionais já existentes, além de servirem como artefatos iniciais para a elaboração de novos procedimentos operacionais. Podem também ser disponibilizados de forma segura para consulta posterior em casos de incidentes semelhantes.

Ademais, conforme já exposto na Estratégia Nacional de Segurança Cibernética, publicada por meio do Decreto nº 10.222, de 5 de fevereiro de 2020: “empresas brasileiras, principalmente aquelas consideradas como infraestruturas críticas, precisam considerar a segurança cibernética como ação prioritária de investimentos, elaborar planos de gestão de riscos e de tratamento e resposta a incidentes, assim como planejar orçamento adequado para combater os incidentes de segurança”.

Dessa forma, é imprescindível que as instituições incluam a Segurança da Informação em suas ações estratégicas e prevejam os recursos necessários para a

execução de ações que busquem fomentar o ganho de maturidade e o aprimoramento de mecanismos de segurança.

3.3.4.2 Usando dados coletados

As atividades realizadas durante a resposta a incidentes devem ser capazes de produzir um conjunto de dados objetivos e subjetivos a respeito de cada evento. O registro histórico das informações sobre os incidentes ocorridos é útil para diversas finalidades e propósitos.

Um exemplo no qual a utilização desses referidos registros ocorre na análise dos dados de identificação do tempo empenhado na resolução dos incidentes e o custo direto que tais eventos geraram. Tais informações podem ser utilizadas para justificar recursos adicionais para que a equipe de resposta a incidente aponte vulnerabilidades ou ameaças cibernéticas recorrentes no ambiente de tecnologia e determine se as correções realizadas surtiram efeito. O desempenho da equipe de resposta pode ser medido através da análise dos dados coletados.

Os dados coletados também servem de fonte para as necessidades de notificação do órgão. Um exemplo é a utilização dos dados como auxílio no processo de notificação de incidentes de segurança à ANPD, cuja realização é obrigatória para todos os casos em que for identificado risco ou dano relevante ao titular de dados, na forma do art. 48 da LGPD. A inobservância do órgão quanto à adequada coleta de informações pode resultar em atrasos nas notificações e em prejuízos para a administração pública.

É fundamental que os dados coletados estejam inalterados, íntegros e sejam armazenados de forma adequada para serem analisados e agreguem ainda mais valor para todos os envolvidos na resposta de incidentes, para o órgão e para a administração pública, a partir do relacionamento e da troca de informações entre os vários entes da Rede Federal de Gestão de Incidentes Cibernéticos.

Recorde-se mais uma vez, enfim, que existem casos de incidentes de segurança à proteção de dados em que a organização deve efetuar comunicação à ANPD e aos titulares dos dados, de acordo com o art. 48 da LGPD.

3.3.4.3 Retenção de evidência

É importante considerar o conteúdo da Norma Complementar nº 21/IN01/DSIC/GSIPR e os demais aspectos jurídicos na elaboração da política de retenção de evidências. Tal política deve informar por quanto tempo as evidências coletadas devem seguir retidas, sempre harmonizando os aspectos legais supracitados com a realidade e a maturidade institucional da organização no tema.

Há alguns fatores sobre a retenção de evidências que devem ser avaliados durante a elaboração da política de retenção de evidências:

a) **Judicialização:** armazenar as evidências de um incidente deve ser uma atividade que leva em consideração que tais evidências podem ou devem ser consultadas durante um processo judicial.
b) **Retenção:** é preciso elaborar procedimentos para a retenção que definam quanto tempo certos tipos de dados devem ser mantidos.
c) **Custo:** é necessário determinar o custo monetário de manter as evidências seguras e acessíveis.

3.4 Compartilhamento de Informações

A evolução de ataques e ameaças torna a cooperação entre organizações de direito público e privado cada vez mais necessária, tanto durante quanto após o tratamento de incidentes. Tal cooperação pode abranger eventos para elaborar, atualizar e difundir novas técnicas e procedimentos.

A cooperação entre organizações durante os processos de resposta a incidentes tem como objetivos a sua resolução e o compartilhamento de informações, tais como ameaças, ataques e possíveis vulnerabilidades em comum, de modo que o conhecimento de uma organização beneficie as demais – tendo em vista que as últimas podem ser vítimas de ameaças comuns.

No Brasil, o CTIR Gov tem o papel de coordenar e integrar as ações destinadas à gestão de incidentes computacionais em órgãos e entidades da administração pública federal.

A equipe de resposta a incidentes computacionais pode planejar e documentar com antecedência a sua participação na coordenação entre organizações parceiras para tornar o tratamento do evento mais eficiente. Uma única equipe de resposta a incidentes pode fazer parte de várias coordenações simultâneas.

É importante que seja compartilhado o máximo de informações possível entre as equipes integrantes de um grupo de coordenação, mas tal compartilhamento deve ser cauteloso para não expor informações consideras sensíveis. Todas as equipes integrantes da coordenação devem cumprir requisitos de confidencialidade para que os dados não sejam vazados, gerando ainda mais impactos.

3.5 Recomendações

Com base em todas as orientações acima expostas, é recomendado que a organização consiga implementar seus próprios processos de resposta a incidentes. Nesse contexto, existem recomendações específicas cuja implementação pode ser útil e acelerar a referida implementação.

Abaixo, listam-se algumas dessas recomendações:

1. Estabelecer a capacidade de resposta a incidentes dentro da organização.
2. Estabelecer meios em que seus colaboradores possam relatar a ocorrência de um incidente.
3. Implementar o processo de gestão de resposta a incidentes.
4. Desenvolver planos de resposta a incidentes com base na política de resposta a incidentes.
5. Ter um plano de gerenciamento de risco que contemple ameaças e vulnerabilidades à segurança da informação, bem como medidas de proteção de dados, privacidade e procedimentos relativos à identificação, análise e avaliação de riscos.
6. Ter políticas, diretrizes ou normas que subsidiem a tomada de decisão dos profissionais envolvidos no tratamento de incidentes, em relação à identificação da criticidade dos serviços e dos parâmetros para balizar a análise de gravidade, urgência e tendência dos eventos que servirão ao processo de priorização.

7. Possuir o inventário de dados pessoais e implementar um processo de avaliação de risco (e.g. Relatório de Impacto à Proteção de Dados).
8. Criar equipes de resposta a incidentes.
9. Selecionar indivíduos que possuam habilidades apropriadas para integrarem a equipe de resposta a incidentes.
10. Realizar treinamentos constantes com o objetivo de propagar novos conhecimentos para a equipe de resposta a incidentes.
11. Planejar e conduzir periodicamente exercícios de resposta a incidentes, e utilizar relatórios destes exercícios para melhorar seus procedimentos de respostas a incidentes.
12. Determinar quais serviços as equipes de resposta a incidentes devem oferecer.
13. Identificar departamentos que possam auxiliar os processos de resposta a incidentes.
14. Avaliar a aquisição de ferramentas e recursos para que a equipe de resposta a incidentes consiga atuar de forma eficaz durante o tratamento.
15. Garantir a implementação de medidas de segurança da informação adequadas, com o objetivo de prevenir a ocorrência de incidentes de segurança.
16. Utilizar sistemas para detectar e prevenir intrusão e para antivírus, bem como para verificar a integridade de arquivos.
17. Estabelecer e manter processo para manutenção de informações de contato atualizadas que possibilite a notificação da ocorrência de incidentes (e.g. ouvidoria, canais públicos de contato e outros).
18. Estabelecer e manter mecanismos primários e secundários que poderão ser utilizados para comunicação durante a ocorrência de um incidente.
19. Utilizar da análise de logs.
20. Implementar diferentes perfis de redes e sistemas, com níveis de acessos diferentes.
21. Habilitar auditoria de perfis, possibilitando atividades fora do padrão.

22. Fazer com que comportamentos anormais de recursos de tecnologia sejam rapidamente identificados.
23. Criar uma política de retenção de evidências que consiga especificar por quanto tempo e como as evidências devem ser mantidas.
24. Correlacionar eventos distintos a fim de encontrar características comuns entre tais eventos.
25. Sincronizar todos os relógios de host para facilitar a correlação de incidentes.
26. Criar, manter e usar uma base de conhecimento com informações sobre incidentes.
27. Registrar todas as informações do evento a partir do momento em que há uma suspeita da ocorrência de um incidente.
28. Proteger todos os dados dos incidentes.
29. Quando houver incidentes simultâneos, priorizar o tratamento de incidentes com base em características já estabelecidas como relevantes ou não.
30. Criar, documentar e seguir procedimentos de resposta a incidentes durante o tratamento de incidentes.
31. Realizar reuniões pós a ocorrência de um incidente para identificar melhorias no processo de resposta a incidentes.
32. Participar de grupos de discussão entre organizações que atuam com resposta a incidentes, antes da ocorrência de um evento.
33. Efetuar consulta jurídica interna antes de participar de grupos de discussões, pois o compartilhamento de algumas informações pode constituir infração à legislação e a contratos.
34. Realizar o compartilhamento de informações durante todo o tratamento de um incidente, seja por meio de uma reunião de coordenação, seja por contato com fornecedores e departamentos internos da organização.
35. Buscar automatizar o compartilhamento de informações, adotados os devidos cuidados; isso possibilita que todo o processo de compartilhamento de informações seja mais econômico e eficiente; a automatização deve ser

hibrida, pois, algumas tarefas deverão ser realizadas e analisadas por humanos.

36. Buscar o equilíbrio entre os benefícios do compartilhamento de informações e as desvantagens de compartilhar informações confidenciais e sensíveis.
37. Compartilhar com a Rede Federal de Gestão de Incidentes Cibernéticos o máximo possível de informações (desde que classificadas como apropriadas) a respeito de incidentes cibernéticos.
38. Em caso de incidentes que gerem impactos a dados pessoais, elaborar o plano de comunicação entre equipes internas e atores externos, tais como a ANPD e os titulares de dados pessoais.
39. Em caso de incidentes que tenham resultado em impactos a dados pessoais, elaborar um relatório final detalhando o processo de tratamento do incidente contendo um resumo executivo do que aconteceu e como a capacidade de resposta ao incidente teria ajudado a lidar com a situação, a mitigar o risco e a limitar os danos mais rapidamente.

A seguir, apresenta-se também um checklist para verificação do tratamento de incidentes. Ressalta-se que a implementação de tal checklist não é obrigatória, competindo ao órgão optar pela adoção e/ou personalizá-la:

	Ação	Realizado?
	Detecção e análise	
1.	Determinar se ocorreu um incidente	
1.1	Analisar os precursores e os indicadores	
1.2	Buscar por informações correlatas	
1.3	Realizar pesquisa do incidente (via mecanismos de busca e bases de conhecimento)	
1.4	Documentar, investigar e reunir evidências assim que a equipe identificar a ocorrência do incidente	

2.	Priorizar o tratamento com base em sua relevância (impacto de negócio, impacto de informação e recuperabilidade)	
3.	Comunicar o incidente às equipes internas envolvidas e, quando necessário, aos atores externos	
Contenção, erradicação e recuperação		
4.	Adquirir, preservar, proteger e documentar as evidências	
5.	Conter o incidente	
6.	Erradicar o incidente	
6.1	Identificar e mitigar todas as vulnerabilidades exploradas	
6.2	Remover malware, materiais impróprios e outros componentes	
6.3	Se mais hosts afetados forem descobertos (por exemplo, novas infecções por malware), repetir as etapas de detecção e análise (1.1, 1.2) para identificar todos os outros hosts afetados, para então conter (5) e erradicar (6) o incidente em tais hosts	
7.	Recuperar-se do incidente	
7.1	Retornar os sistemas afetados ao estado operacional	
7.2	Confirmar se os sistemas afetados estão funcionando normalmente	
7.3	Se necessário, implementar monitoração adicional para encontrar futuras atividades relacionadas	
Atividades pós-incidente		
8.	Criar o relatório de acompanhamento	
9.	Realizar uma reunião de lições aprendidas (tal reunião é obrigatória para incidentes graves e opcional para os demais incidentes)	
10.	Realizar análise pós-incidente para prevenir sua recorrência por meio da identificação de lições aprendidas e ações de acompanhamento.	

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001:2013: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação - Requisitos**. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002:2013: Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação**. Rio de Janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27005:2019: Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação**. Rio de Janeiro, 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27701:2019: Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes**. Rio de Janeiro, 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 31000:2018: Gestão de Riscos** — Diretrizes. Rio de Janeiro, 2018.

BRASIL. Autoridade Nacional de Proteção de dados. **Comunicação de incidentes de segurança**. Disponível em: < https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca >. Acesso em: 23 de março de 2023.

BRASIL. Presidência da República. **Decreto nº 10.748, de 16 de julho de 2021. Rede Federal de Gestão de Incidentes Cibernéticos**. Disponível em: <https://www.in.gov.br/en/web/dou/-/decreto-n-10.748-de-16-de-julho-de-2021-332610022> Acesso em: 23 de março de 2023

BRASIL. Presidência da República. **Decreto nº 11.331, de 1º de janeiro de 2023. Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão, das Funções de Confiança e das Gratificações do Gabinete de Segurança Institucional da Presidência da República e remaneja cargos em comissão, funções de confiança e gratificações**. Disponível em: <

https://legislacao.presidencia.gov.br/atos/?tipo=DEC&numero=11331&ano=2023&ato=d41ITTU9kMZpWT436 >. Acesso em 23 de março de 2023.

BRASIL. Presidência da República. **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 >. Acesso em: 23 de março de 2023.

BRASIL. Presidência da República. **Gabinete de Segurança Institucional. Portaria nº 93, de 18 de outubro de 2021**. Glossário de Segurança da Informação. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-gsi/pr-n-93-de-18-de-outubro-de-2021-353056370 >. Acesso em: 23 de março de 2023.

BRASIL. Presidência da República. **Secretaria de Segurança da Informação e Cibernética. Departamento de Segurança da Informação e Cibernética. Gabinete de Segurança Institucional**. Legislação< https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/legislacao > Acesso em 23 março 2023.

BRASIL. Presidência da República. **Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa nº 01, de 27 de maio de 2020**. Brasília, DF, GSI/PR, 2020. Disponível em: < http://dsic.planalto.gov.br/assuntos/editoria-c/documentos-pdf-1/instrucao-normativa-no-1-de-27-de-maio-de-2020-1.pdf >. Acesso em: 23 de março 2023.

BRASIL. Presidência da República. **Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa nº 21, de 08 de outubro de 2014**. Brasília, DF, GSI/PR, 2021. Disponível em: <https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=10/10/2014&jornal=1&pagina=5&totalArquivos=224 >. Acesso em: 23 de março de 2023.

CENTER INTERNET SECURITY. **CIS Controls, versão de 8 maio de 2021**. Disponível em: < https://learn.cisecurity.org/control-download >. Acesso em: 23 de março de 2023.

COMITÊ CENTRAL DE GOVERNANÇA DE DADOS - CCGD. **Guia de Boas Práticas LGPD**. Disponível em: < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf >. Acesso em: 23 de março de 2023.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS. CNIL. **Chapitre IV - Responsable du traitement et sous-traitant**. Disponível em: < https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article33 > Acesso em: 23 de março de 2023.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS. CNIL. **Notifier une violation de données personnelles**. Disponível em: < https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles >. Acesso em: 23 março 2023.

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO DA SECRETARIA DE GOVERNO DIGITAL – DPSI/SGD. **Guia de Avaliação de Riscos de Segurança e Privacidade**. Disponível em: < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_avaliacao_riscos.pdf >. Acesso em: 06 mar. 2023.

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO DA SECRETARIA DE GOVERNO DIGITAL – DPSI/SGD. **Guia de Inventário de Dados Pessoais**. Disponível em: < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_inventario_dados_pessoais.pdf >. Acesso em: 23 mar. 2023.

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO DA SECRETARIA DE GOVERNO DIGITAL – DPSI/SGD. **Guia do Framework de Privacidade e Segurança da Informação**. Novembro 2022. Disponível em: < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf >. Acesso em: 23 mar. 2023.

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO DA SECRETARIA DE GOVERNO DIGITAL – DPSI/SGD. **Guias Operacionais para adequação à LGPD**. Disponível em: < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd >. Acesso em: 23 mar. 2023.

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO DA SECRETARIA DE GOVERNO DIGITAL – DPSI/SGD. **Modelo de Política de Gestão de Registros (Logs) de Auditoria**. Disponível em: < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/modelo_politica_logs_auditoria.pdf >. Acesso em: 23 mar. 2023.

EUROPEAN DATA PROTECTION SUPERVISOR. EDPS. **Our role as a supervisor**. Disponível em: < https://edps.europa.eu/data-protection/our-role-supervisor_en > Acesso em: 20 de abril de 2021.

INFORMATION COMMISSIONER'S OFFICE. ICO. **Report a breach. Report a breach**. Disponível em: < https://ico.org.uk/for-organisations/report-a-breach/ >. Acesso em: 23 de março de 2023.

INTERNATIONAL STANDARD. **ISO/IEC 29100:2011: Information technology — Security techniques — Privacy framework**. Genebra, 2011.

INTERNATIONAL STANDARD. **ISO/IEC 29134:2017: Information technology — Security techniques – Guidelines for privacy impact assessment**. Genebra, 2017.

INTERNATIONAL STANDARD. **ISO/IEC 29151:2017: Information technology — Security techniques — Code of practice for personally identifiable information protection**. Genebra, 2017.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Framework for Improving Critical Infrastructure Cybersecurity, versão 1.1, 2018**. Disponível em: < https://doi.org/10.6028/NIST.CSWP.04162018 >. Acesso em: 23 de março de 2023.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **NIST Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response**. Disponível em < https://csrc.nist.gov/publications/detail/sp/800-86/final >. Acesso em: 23 de março de 2023.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **NIST Special Publication 800-61 revisão 2: Computer Security Incident Handling Guide**. Disponível em: < https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf >. Acesso em: 23 de março de 2023.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **NIST Special Publication 800-53 revisão 5: Security and Privacy Controls for Information Systems and Organizations**. Gaithersburg, 2020.

PDPC. **GUIDE ON MANAGING AND NOTIFYING DATA BREACHES**. Disponível em: < https://www.pdpc.gov.sg/help-and-resources/2021/01/data-breach-management-guide>. Acesso em: 23 de março de 2023.

ANEXO I

Este anexo tem a finalidade de fornecer os destaques das mudanças inseridas nas versões do Guia de Resposta a Incidentes de Segurança em comparação com o documento originalmente publicado em agosto de 2021.

Mudanças da Versão 3.0

Primeiramente, ressalta-se que as mudanças inseridas nesta versão em comparação com a anterior visam a adequação do mesmo com o Guia do Framework de Privacidade e Segurança da Informação v1 elaborado e publicado pela SGD em novembro de 2022.

Foram realizadas inclusões de: seção sobre aviso preliminar e agradecimentos; e referência de que controle e medidas do Framework de Privacidade e Segurança da Informação são atendidos pelo Guia de Elaboração de Programa de Governança de Privacidade.

Dentre os ajustes pontuais, cumpre destacar:

- atualização das Definições Gerais para alinhamento com o Glossário de Segurança da Informação;
- inclusões de itens, atualizações e ajustes nas seções 2 e 3 visando a adequação ao Guia do Framework de Privacidade e Segurança da Informação;
- remoção do tópico 4 “Considerações Finais” sem prejuízo para o conteúdo e qualidade do documento; e
- atualização e validação de todas as referências ao longo do documento visando a manutenção do arcabouço referencial.

Mudanças da Versão 3.1

Foram realizadas inclusões com o objetivo de reforçar o alinhamento com as medidas 22.10 e 22.11 do Guia do Framework de Privacidade e Segurança da Informação.

Dentre os ajustes pontuais, cumpre destacar:

- Inclusão de parágrafo no item 2.4 sobre a comunicação à ANPD incluindo o endereço de URL;
- Inclusão de parágrafo no item 3.2 sobre a criação de planos específicos para incidentes que violam a proteção de dados pessoais;
- Inclusão do tópico 39 do item 3.5 que trata de recomendações, orientando a criação de um relatório final detalhando o processo de tratamento do incidente ocorrido.