Prefeitura da Cidade do Rio de Janeiro
Conselho Municipal de Proteção de Dados Pessoais e da Privacidade

Boas práticas para a realização de comunicação de incidentes de segurança à ANPD e aos titulares, bem como de registro destas ocorrências.

2025

Prefeitura da Cidade do Rio de Janeiro
Conselho Municipal de Proteção de Dados Pessoais e da Privacidade

Título do Grupo de Trabalho: Boas práticas para a realização de comunicação de incidentes de segurança à ANPD e aos titulares, bem como de registro destas ocorrências.

Composição do Grupo de Trabalho:

Alessandra Lapa
Ana Paula Vasconcellos
Nuno Caminada
Silvio Maciel E Silva Junior
Vitor Paludetto

Relatores:
Rafael Moraes da Silva
Rafael Pereira Barboza

Sumário

Introdução

A proteção de dados pessoais consolidou-se como um direito fundamental, conforme está previsto no artigo 5º, inciso LXXIX, da Constituição Federal de 1988. Esse reconhecimento coloca a privacidade e a autodeterminação informativa como pilares essenciais para uma governança democrática nos dias de hoje. Tal avanço foi concretizado com a promulgação da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD), que não apenas assegurou direitos aos titulares, mas também atribuiu responsabilidades aos controladores. Ao instituir um sistema normativo de responsabilização, a LGPD incorporou ao cotidiano da administração pública a necessidade de gerenciar riscos e implementar mecanismos de comunicação transparente e tempestiva sobre incidentes de segurança, elementos hoje reconhecidos como boas práticas de governança de dados pessoais.

No âmbito da administração pública municipal, devido à natureza de suas atribuições, há tratamento diário de bases de dados sensíveis e diversificadas, entre elas, informações sobre saúde e educação até dados fiscais, urbanísticos e sociais. A relevância desses dados no dia a dia da população faz com que os impactos de possíveis incidentes de segurança sejam ainda mais significativos, seja em casos de vazamentos, acessos indevidos, perdas acidentais ou mesmo ataques cibernéticos. Portanto, ao discutir a obrigação de comunicar incidentes, é fundamental vê-la como um instrumento de defesa dos direitos fundamentais e, ao mesmo tempo, como uma estratégia para manter a legitimidade e a transparência da gestão pública local.

Neste sentido, é importante destacar que a comunicação de incidentes não deve ser compreendida como ato isolado ou meramente burocrático. Ao contrário, ela integra o fluxo estruturado de um Plano de Resposta a Incidentes (PRI), documento que orienta a atuação coordenada da Administração Pública diante de eventos que comprometem a segurança da informação e a proteção de dados pessoais. Assim, o PRI define papéis, responsabilidades, prazos e mecanismos de registro, de modo que a comunicação à ANPD e aos titulares seja realizada de forma tempestiva, transparente e em conformidade com a legislação.

Portanto, ao propor boas práticas de comunicação de incidentes, ressalta-se que elas apenas se consolidam quando integradas a um PRI, capaz de assegurar não apenas a conformidade regulatória, mas também a responsabilização institucional e a proteção efetiva dos direitos dos titulares.

I. O Papel da LGPD na definição das obrigações de comunicação

De acordo com o artigo 48 da LGPD, quando ocorrem incidentes de segurança da informação que possam gerar risco ou dano significativo aos

titulares, a situação precisa ser comunicada à Agência Nacional de Proteção de Dados (ANPD) e, quando necessário, aos próprios titulares. Essa regra se alinha ao princípio da responsabilização e prestação de contas (art. 6º, X, da LGPD), na medida que estabelece uma ligação entre a ocorrência do incidente e a necessidade de comunicação eficiente.

Essa normatização foi aprimorada pela Resolução CD/ANPD nº 15/2024, que aprovou o Regulamento de Comunicação de Incidente de Segurança. Com isso, foram definidos critérios claros para identificar riscos ou danos relevantes (art. 5º), além de condições e formatos de comunicação, e especificações sobre os campos obrigatórios no Formulário de Comunicação de Incidente de Segurança (CIS). O objetivo do Formulário é padronizar as boas práticas e evitar respostas fragmentadas ou insuficientes de órgãos públicos e privados.

II. Importância da comunicação de incidentes

Comunicar incidentes em tempo hábil não deve ser visto apenas como uma obrigação legal, mas como um pilar para as boas práticas públicas. Uma comunicação eficiente demonstra, principalmente, três aspectos:

- **Proteção dos direitos e liberdades fundamentais –** ajuda os titulares a serem informados e tomarem medidas para mitigar riscos, como mudar senhas ou monitorar possíveis fraudes;
- **Preservação da confiança pública –** mostra que a Administração atua com boa fé, se posicionando de forma ativa em face de falhas ou vulnerabilidades;
- **Transparência institucional –** facilita a supervisão da ANPD e da sociedade, promovendo uma cultura administrativa que respeita padrões de integridade e governança.

III. Marco regulatório, benchmark e diretrizes técnicas

O marco regulatório brasileiro sobre proteção de dados deve ser analisado de maneira integrada:

- O art. 48 da LGPD determina a obrigação básica de comunicação;
- A Resolução CD/ANPD nº 15/2024 regulamenta essa obrigação, oferecendo critérios de avaliação, prazos e parâmetros técnicos;
- Os princípios gerais da LGPD (art. 6º), como prevenção, segurança, necessidade e responsabilização, servem como diretrizes hermenêuticas na aplicação prática da comunicação de incidentes.

No entanto, para que essas obrigações sejam eficazes, é crucial que haja diálogo com boas práticas nacionais e internacionais já estabelecidas. Alguns exemplos relevantes são:

A. **Experiências nacionais:**

1) O TRT da 15ª Região, por meio da instituição de seu PRI, criou fluxos internos para responder a incidentes, com responsabilidades bem definidas, envolvendo tecnologia, jurídico e corregedoria, o que possibilitou comunicações rápidas e padronizadas para a ANPD.
2) O TCE-MS implementou o PRI, prevendo o registro detalhado de eventos e a elaboração de relatórios regulares ao comitê de governança de dados, o que reforça a rastreabilidade e a transparência institucional.
3) O IBAMA estruturou seu PRI integrando Ouvidoria, EIAPD, CGTI e ETIR, com fluxos para comunicação em até 3 dias úteis, elaboração de RIPD e relatórios finais, reforçando efetividade e governança.

B. **Experiências internacionais:**

Na União Europeia, o GDPR (art. 33) estabelece um prazo de 72 horas para comunicar à autoridade supervisora, levando à formação de equipes especializadas para respostas rápidas.

O modelo europeu conta ainda com diretrizes do European Data Protection Board (EDPB), que destacam a importância de avaliar o risco no contexto e comunicar claramente aos titulares.

No âmbito técnico, a norma ISO/IEC 27035 dá diretrizes sobre gestão de incidentes de segurança da informação, incluindo detecção, análise, contenção e comunicação estruturada — uma referência amplamente utilizada no setor público de países da OCDE.

Essas experiências mostram que a comunicação de incidentes não deve ser vista como uma ação isolada e reativa, mas como parte de um processo contínuo de governança que envolve prevenção, preparação, resposta e aprendizado institucional. Nesse cenário, o PRI assume papel estratégico por traduzir as obrigações legais e os referenciais de boas práticas em procedimentos concretos de atuação. Mais do que um documento formal, o PRI funciona como ponte entre o marco regulatório e a prática administrativa, ao organizar fluxos, integrar áreas técnicas e administrativas e consolidar mecanismos de registro e acompanhamento. Dessa forma, garante não apenas a conformidade regulatória, mas também a institucionalização de uma cultura de segurança e proteção de dados no setor público.

4. **Escopo Temático do Estudo**

Para aprofundar a análise e sugerir recomendações práticas, o presente relatório foi segmentado em quatro eixos principais:

Apresentação do Problema – definição de incidentes de segurança, critérios legais e regulatórios aplicáveis, desafios do setor público municipal e os impactos relacionados;

Benchmark e Boas Práticas – análise de experiências nacionais (TRT-15, TCE-MS, IBAMA) e internacionais (GDPR, EDPB, ISO/IEC 27035), destacando que a comunicação de incidentes à ANPD e aos titulares integra os fluxos estruturados de um PRI. O eixo aborda como diferentes instituições documentaram responsabilidades, prazos e mecanismos de registro em seus PRIs, transformando a comunicação em etapa essencial de um processo mais amplo de governança de dados pessoais.

Esse delineamento metodológico garante que o trabalho do Comitê permaneça alinhado ao marco regulatório atual, ao mesmo tempo que fornece à Administração Municipal ferramentas técnicas e jurídicas para melhorar a gestão de incidentes de segurança da informação e a proteção de dados pessoais.

Apresentação do problema

A compreensão de incidentes de segurança exige a articulação entre o campo da Segurança da Informação (SI) e o regime jurídico de proteção de dados pessoais inaugurado pela Lei nº 13.709/2018 – LGPD.

Desta feita, a LGPD dispõe em seu art. 48, que “o controlador deverá comunicar à Agência nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares”.

Neste sentido, como leciona o Professor Maurício Temer:

> Todas as providências associadas ao programa são vocacionadas a garantir a conformidade do agente de tratamento com o Direito da Proteção de Dados Pessoais e assegurar os níveis necessários de segurança da informação. Caso, porém, a confidencialidade, a integridade, a disponibilidade ou a autenticidade sejam comprometidas, nos termos da Resolução CD/ANPD n. 15/2024, fica caracterizado o incidente de segurança: “qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais” (art. 3º, XII). (Tamer, Maurício, 2025).

Desta forma, a publicação da Resolução CD/ANPD Nº 15/2024 representa um avanço significativo na operacionalização, em especial, do art. 48 da LGPD, detalhando com clareza os procedimentos que os agentes de tratamento deverão seguir na comunicação de incidentes.

Assim, a ANPD, de maneira restrita, definiu, no art. 3º, inciso XII, da Resolução CD/ANPD nº 15/202, que incidente de segurança seria "qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais".

A Resolução em comento ainda detalha critérios objetivos para essa avaliação, estabelecendo que a comunicação à Agência Nacional de Proteção de Dados (ANPD) e aos titulares deve ocorrer em situações que envolvam cumulativamente o critério geral com um dos critérios específicos:

a) **Critério Geral:** risco ou dano relevante: quando afetar significativamente interesses e direitos fundamentais dos titulares, ou seja, quando impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade.

b) **Critérios específicos:**

b.1) dados pessoais sensíveis;
b.2) dados de crianças, de adolescentes ou de idosos;
b.3) dados financeiros;
b.4) dados de autenticação em sistemas;
b.5)dados protegidos por sigilo legal, judicial ou profissional; ou
dados em larga escala.

Ressalte-se que se considera incidente com dados em larga escala aquele que abranger número significativo de titulares, considerando, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica de localização dos titulares.

Por outro lado, é relevante pontuar entendimento da Agência Nacional de que "incidentes que envolvam somente dados anonimizados ou que não estejam relacionados a pessoas naturais identificadas ou identificáveis não precisam ser comunicados à ANPD".

Para além das normas supracitadas, é relevante destacar que a entrada em vigor dos decretos federais nº 12.572 e 12.573, de 4 de agosto de 2025, representa um divisor de águas no ordenamento jurídico brasileiro voltado à segurança da informação e à proteção de dados pessoais, à medida que não se trata apenas de mais uma camada normativa, mas se trata da fundação técnica e institucional para sustentar o "edifício" da LGPD.

Ademais, consoante o TCU,

> a ausência de PSI, de nomeação do encarregado de dados e de comunicação padronizada dos incidentes de segurança à ANPD e aos titulares são fatores que prejudicam bastante o processo de implementação da LGPD. Os dois primeiros, principalmente, por se tratar de elementos-chave na estruturação do órgão/entidade para se adequar à lei: a PSI é a política que definirá os objetivos da organização relativos à segurança da informação e o DPO é o principal ator na condução desse processo

Pilares da Segurança da Informação

De acordo com a Resolução CD/ANPD nº 15/2024, o Laboratório Nacional de Computação Científica - LNCC e o Glossário de Segurança da Informação, a SI é estruturada em quatro pilares:

1) Confidencialidade – garantia de acesso apenas por pessoas autorizadas.
2) Integridade – proteção contra alterações indevidas ou destruição não autorizada.
3) Disponibilidade – manutenção do acesso contínuo e confiável à informação.
4) Autenticidade – confirmação da identidade e legitimidade das partes envolvidas.

A violação de qualquer desses princípios caracteriza incidente de segurança de dados pessoais e, dependendo do preenchimento dos requisitos indicados na Resolução em comento, pode gerar a obrigação de comunicação à ANPD e aos titulares de dados pessoais.

Cenário Atual e Desafios

Relatórios como o *Data Breach Investigations Report* (Verizon, 2024) e o *Cost of a Data Breach Report* (IBM, 2025) evidenciam que a detecção tardia e a falta de coordenação institucional elevam exponencialmente os custos médios de um incidente.

Na esfera pública, essa deficiência poderá resultar em:

1) respostas fragmentadas entre áreas técnicas, jurídicas e administrativas;
2) dificuldade de comunicação clara com os titulares;
3) e risco de descumprimento das normas da LGPD e das Resoluções da ANPD.

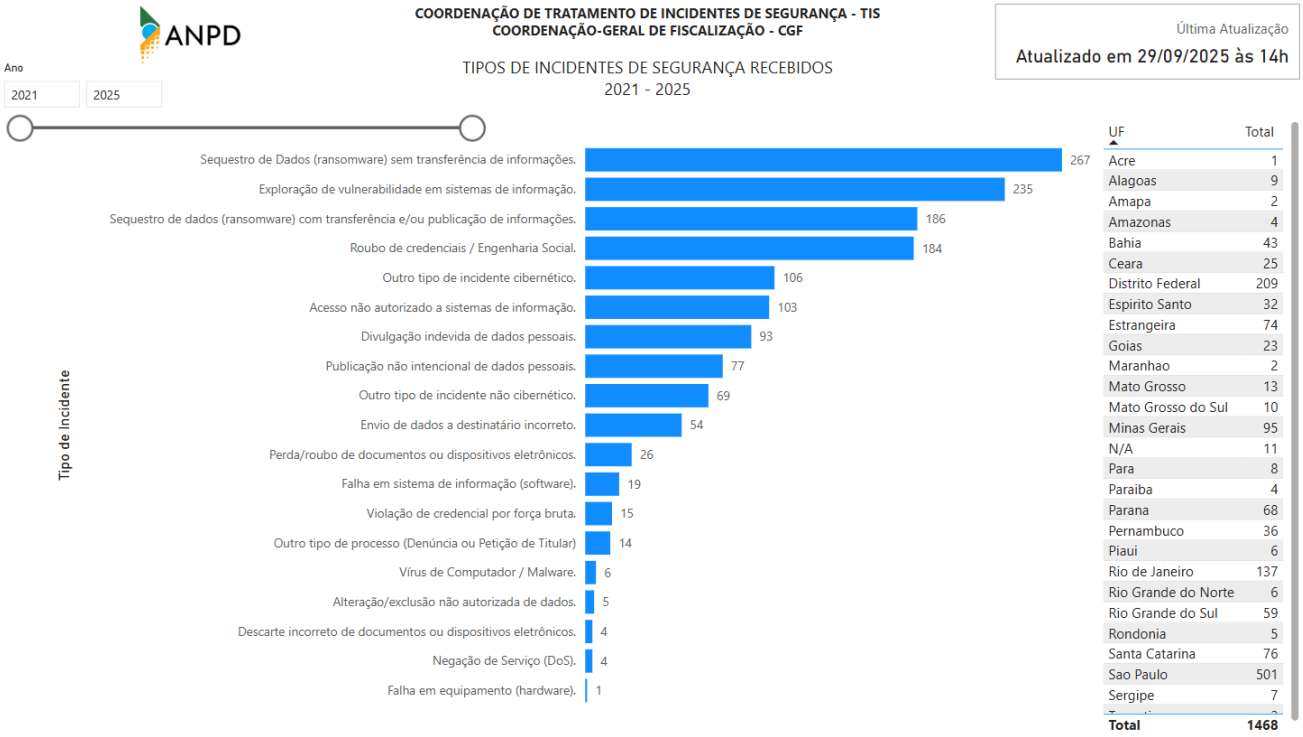
No que tange aos desafios supracitados, é relevante pontuar, nas palavras de Silvio Maciel e Silva Junior, que a efetividade da legislação depende não apenas do arcabouço normativo e das ferramentas tecnológicas, mas também da preparação das pessoas envolvidas. Nesse sentido, a capacitação e a sensibilização contínuas emergem como fatores estratégicos para mitigar riscos e garantir uma resposta ágil e coordenada. (Junior, Silvio Maciel e Silva, 2025).

Principais Tipos de Incidentes

Segundo dados apresentados pela ANPD, os incidentes mais recorrentes são:

1) Sequestro de Dados (*ransomware*) sem transferência de informações;
2) Exploração de vulnerabilidade em sistemas de informação;
3) Sequestro de dados (*ransomware*) com transferência e/ou publicação de informações;
4) Roubo de credenciais / Engenharia Social;
5) Outro tipo de incidente cibernético;
6) Acesso não autorizado a sistemas de informação;
7) Divulgação indevida de dados pessoais;
8) Publicação não intencional de dados pessoais;
9) Outro tipo de incidente não cibernético;
10) Envio de dados a destinatário incorreto;
11) Perda/roubo de documentos ou dispositivos eletrônicos;
12) Falha em sistema de informação (software);
13) Violação de credencial por força bruta;
14) Outro tipo de processo (Denúncia ou Petição de Titular);
15) Vírus de Computador / Malware;
16) Alteração/exclusão não autorizada de dados;
17) Descarte incorreto de documentos ou dispositivos eletrônicos;
18) Negação de Serviço (DoS);
19) Falha em equipamento (hardware).

Segue abaixo o gráfico apresentado pela ANPD:



Impactos e Custos

No que diz respeito às medidas preventivas, Maurício Tamer opina, que

> A rigor, diante do conceito de incidente, toda e qualquer medida adotada pelo agente em prol da sua conformidade com o Direito da Proteção de Dados Pessoais e para garantir a boa governança e segurança da informação pode ser considerada uma medida preventiva. Assim, todas essas medidas são vocacionadas a prevenir a ocorrência de incidentes. (Tamer, Maurício, 2025).

Desta maneira, a não adoção de medidas preventivas e proativas pelos agentes de tratamento, podem gerar impactos vão além do prejuízo financeiro direto, na ocorrência de incidentes de segurança, englobando também:

1) danos reputacionais e perda de confiança institucional;
2) responsabilização administrativa, com aplicação de sanções pela ANPD (art. 52 da LGPD);
3) responsabilização civil, inclusive com indenizações coletivas;
4) prejuízos sociais, especialmente em serviços públicos essenciais, quando a indisponibilidade de dados atinge diretamente a população.

Neste contexto, o relatório da IBM (2025) destaca que o custo médio global de um incidente de violação de dados alcançou USD 4,4 milhões, com acréscimos quando envolvem entidades governamentais e dados sensíveis.

Consequências de Comunicação Ineficiente ou Tardia

A Resolução CD/ANPD nº 15/2024 fixa prazos e requisitos para a comunicação dos incidentes de segurança identificados. Nesse cenário, as seguintes consequências em relação à comunicação ineficiente ou tardia poderão ser elencadas:

1) ampliação dos riscos de fraudes e danos aos titulares;
2) comprometimento da transparência e da confiança entre cidadão e a Administração Pública;
3) exposição da Municipalidade ao descumprimento legal, ensejando processos sancionatórios e judiciais.

De acordo com a ANPD, “demora injustificada na comunicação de incidente de segurança que possa causar risco ou dano relevante aos titulares pode sujeitar os agentes às sanções administrativas previstas na LGPD.”

Portanto, a ausência de um Plano de Resposta a Incidentes robusto e ágil no setor público municipal não é apenas um problema técnico, mas também jurídico e estratégico, com repercussões diretas na proteção de direitos fundamentais, na governança pública e na segurança jurídica institucional.

Por fim, de acordo com o TCU, a ausência de processo padronizado de comunicação dos incidentes que possam acarretar risco ou dano relevante aos titulares de dados afeta negativamente alguns dos pilares nos quais se baseia a própria LGPD, a exemplo dos princípios da transparência (fornecimento de informações claras e precisas acerca dos tratamentos de dados) e da prevenção (adoção de medidas para prevenir a ocorrência de danos em virtude desses tratamentos) (Lei 13.709/2018, art. 6º, incisos VI e VIII).

Benchmark / Boas Práticas

A adoção de boas práticas para a comunicação de incidentes de segurança da informação com dados pessoais, tanto à Agência Nacional de Proteção de Dados (ANPD) quanto aos titulares, revela-se um eixo estratégico de governança de dados no setor público. A experiência nacional e internacional demonstra que incidentes de segurança não podem ser tratados apenas como falhas técnicas pontuais, mas como

eventos que afetam diretamente a confiança social, a proteção dos direitos fundamentais e a accountability institucional.

No Brasil, a LGPD (Lei nº 13.709/2018), em seu artigo 48, estabeleceu a obrigação de que controladores comuniquem à ANPD e aos titulares a ocorrência de incidentes que possam acarretar risco ou dano relevante. Essa obrigação foi detalhada pela Resolução CD/ANPD nº 15/2024, que regulamentou o processo de comunicação, estabelecendo prazos, conteúdos mínimos e a forma de registro. Dessa forma, o cumprimento do dispositivo legal não se resume a um ato burocrático, mas deve estar alinhado a uma cultura organizacional de segurança e transparência.

Neste sentido, a observância de boas práticas nesse campo contribui para:

1) Reduzir riscos secundários: uma comunicação tempestiva e clara pode mitigar impactos adicionais sobre os titulares, orientando-os sobre medidas preventivas;

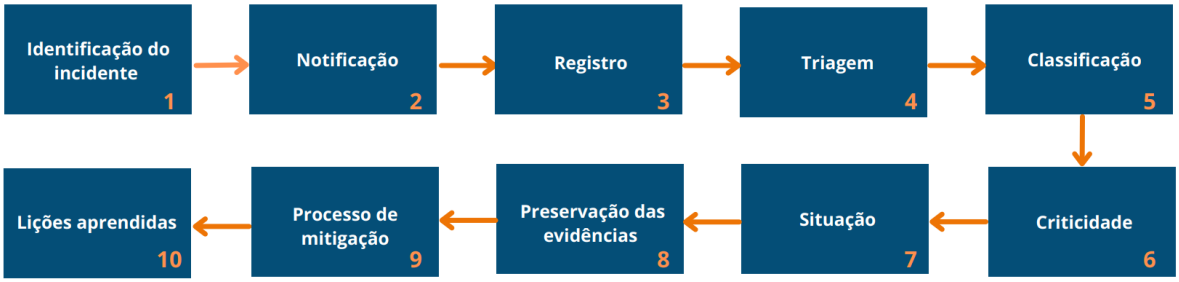
2) Evitar sanções regulatórias: a ANPD tem competência para sancionar organizações que falham em comunicar adequadamente incidentes relevantes;

3) Preservar a imagem institucional: órgãos públicos que comunicam de maneira transparente fortalecem a relação de confiança com a sociedade;

4) Promover aprendizado organizacional: a análise pós-incidente, associada ao registro interno, gera conhecimento valioso para aprimorar processos de segurança e governança.

Nesse contexto, destaca-se a importância da estruturação de um Plano de Resposta a Incidentes (PRI), que sistematiza como a instituição deve agir desde a detecção de uma ocorrência até a sua comunicação formal aos órgãos competentes e aos titulares de dados pessoais. O plano funciona como guia prático, permitindo que cada etapa seja conduzida de forma coordenada, transparente e em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD) e com a Resolução CD/ANPD nº 15/2024.

Vejamos a seguir um modelo de fluxo que busca padronizar as ações para facilitar a ação das áreas envolvidas.



O fluxo de resposta a incidentes, embora estruturado em etapas sequenciais, pode ser adaptado conforme a gravidade e as circunstâncias específicas de cada situação. Em casos críticos, como o vazamento de dados que expõe senhas de cartões de uma instituição financeira, a ordem tradicional do processo pode ser alterada para priorizar ações que mitiguem os impactos imediatos. Por exemplo, o plano de comunicação, que normalmente ocorre após a avaliação de gravidade, pode ser antecipado para informar rapidamente os clientes e parceiros, reduzir danos à reputação e orientar medidas de proteção. Essa flexibilidade é essencial para garantir uma resposta eficaz e proporcional ao risco envolvido.

A experiência internacional e nacional demonstra que a existência de um plano bem delineado faz a diferença na efetividade da resposta. O Regulamento Europeu de Proteção de Dados (GDPR), por exemplo, consolidou a obrigatoriedade de comunicação de incidentes em prazos curtos, levando as organizações a desenvolverem estruturas próprias de governança em segurança. No Brasil, a Agência Nacional de Proteção de Dados (ANPD) já orienta, em guias e regulamentos, que os agentes de tratamento adotem procedimentos documentados, evidenciando a relevância de planos de resposta no setor público e privado.

Além disso, órgãos e entidades públicas brasileiras já caminham nesse sentido. O Tribunal Regional do Trabalho da 15ª Região (TRT-15) e o Tribunal de Contas do Estado do Mato Grosso do Sul (TCE-MS) instituíram planos de resposta a incidentes que detalham fluxos de comunicação, papéis e responsabilidades dos atores envolvidos, etapas de registro e mitigação dos riscos. Essas iniciativas se tornaram importantes referências para a Administração Pública, servindo como parâmetro para o desenvolvimento de políticas locais.

A partir dessa perspectiva, o termo “Benchmark / Boas Práticas” neste relatório vai além de uma análise meramente descritiva de normas. O benchmark se propõe a:

1) Comparar experiências nacionais e internacionais, identificando práticas já consolidadas e aplicáveis ao contexto municipal;
2) Avaliar a maturidade organizacional dos órgãos públicos na implementação de processos de resposta a incidentes;

3) Consolidar diretrizes aplicáveis que possam orientar a administração pública municipal no desenvolvimento de seus próprios fluxos, formulários e registros.

Documentos institucionais já produzidos por órgãos brasileiros ilustram como o benchmark pode ser útil. Por exemplo:

1) O Plano de Resposta a Incidentes do TRT-15 estabelece fluxos claros de notificação e a participação de comitês internos na decisão sobre comunicação aos titulares.

2) O Plano do TCE/MS inclui checklist com responsabilidades do Encarregado de Dados e gestores de Segurança da Informação, reforçando a necessidade de documentação detalhada de cada etapa.

3) O Plano do IBAMA apresenta diretrizes aplicadas à esfera federal, permitindo observar como órgãos públicos com alta complexidade operacional tratam a resposta a incidentes.

Esses exemplos demonstram que o benchmarking permite identificar convergências entre diferentes setores e níveis de governo, servindo como base para propostas normativas locais mais eficazes.

Assim, o capítulo “Benchmark / Boas Práticas” do presente relatório não deve ser entendido apenas como descrição de práticas existentes, mas como instrumento analítico e comparativo, destinado a subsidiar recomendações concretas que fortaleçam a proteção de dados pessoais na esfera municipal.

1.1 Plano de Resposta a Incidente

Um Plano de Resposta a Incidentes (PRI) é um instrumento organizacional que estabelece, de forma estruturada e documentada, as diretrizes, procedimentos e responsabilidades que devem ser adotados quando ocorre um incidente de segurança da informação. O objetivo central de um PRI é garantir que a instituição responda de maneira rápida, coordenada e eficaz, minimizando os impactos técnicos, jurídicos, operacionais e reputacionais decorrentes do evento.

Um plano bem elaborado não se limita à reação imediata, mas abrange todas as fases do ciclo de vida do incidente: detecção, análise, contenção, comunicação, tratamento, registro e lições aprendidas. Ao sistematizar essas etapas, o PRI assegura previsibilidade às ações, evita improvisos, garante a melhor gestão do tempo e fortalece a cultura organizacional de segurança.

Esse tipo de instrumento é amplamente recomendado em normas internacionais, como a ISO/IEC 27035, que trata da gestão de incidentes de segurança da informação, e é reconhecido como uma boa prática de governança em diversos setores públicos e privados.

Neste sentido, o título deste relatório, “Boas práticas para a realização de comunicação de incidentes de segurança à ANPD e aos titulares, bem como de

registro destas ocorrências", guarda relação direta com a lógica de um Plano de Resposta a Incidentes.

Isso porque a comunicação à Agência Nacional de Proteção de Dados (ANPD) e aos titulares não ocorre de forma isolada: ela é uma das etapas críticas dentro do PRI. Para que essa comunicação seja efetiva, transparente e dentro dos prazos legais, é indispensável que haja previamente um plano estruturado que defina fluxos, responsabilidades, formulários e registros.

Portanto, ao tratar de boas práticas de comunicação de incidentes, este trabalho se ancora na compreensão de que tais práticas precisam estar integradas a um plano de resposta robusto, capaz de alinhar:

1) conformidade legal (LGPD, art. 48, e Resolução CD/ANPD nº 15/2024);
2) governança organizacional (responsabilização e prestação de contas);
3) proteção de direitos fundamentais (informação clara e tempestiva aos titulares);
4) aprendizado institucional (registros e relatórios que alimentam melhorias contínuas).

Assim, a elaboração de um PRI não é apenas uma medida técnica, mas a concretização prática do que este trabalho se propõe a construir: diretrizes que garantam que incidentes de segurança sejam tratados com responsabilidade, transparência e foco na proteção de dados pessoais.

1.2 Objetivos de um Plano de Resposta a Incidentes

O Plano de Resposta a Incidentes (PRI) tem como finalidade principal assegurar que a organização esteja preparada para lidar de forma eficiente e coordenada com eventos que comprometam a segurança da informação e a proteção de dados pessoais.

Entre seus objetivos estratégicos, destacam-se:

1. Garantir a proteção dos titulares de dados pessoais
   - Minimizar os riscos de danos materiais e imateriais, como fraudes, discriminação, constrangimentos ou violação da privacidade.
   - Cumprir a obrigação legal prevista no artigo 48 da LGPD e no Regulamento de Comunicação de Incidentes da ANPD.
2. Assegurar conformidade legal e regulatória
   - Atender aos prazos e requisitos estabelecidos pela Resolução CD/ANPD nº 15/2024, garantindo comunicações tempestivas e completas.
   - Demonstrar, por meio de registros e relatórios, a adoção de medidas de responsabilização e prestação de contas (accountability).
3. Reduzir os impactos organizacionais e reputacionais

- Limitar os efeitos de incidentes sobre as operações, serviços e a imagem institucional.
- Preservar a confiança da sociedade e dos usuários nos serviços públicos prestados.

4. Definir papéis e responsabilidades
   - Estabelecer a atuação coordenada entre encarregado, gestores de segurança, áreas técnicas, comitês e alta administração.
   - Garantir que todos os envolvidos conheçam previamente suas atribuições, evitando improvisos em situações de crise.
5. Promover aprendizado contínuo e melhoria de processos
   - Utilizar o registro e a análise dos incidentes para fortalecer políticas de segurança da informação e privacidade.
   - Incorporar lições aprendidas na atualização do próprio plano, em um ciclo de melhoria contínua.
6. Fortalecer a cultura de segurança e transparência
   - Integrar a gestão de incidentes à governança de dados da instituição.
   - Estimular boas práticas preventivas, reconhecendo que a comunicação transparente é parte essencial da proteção de dados.

1.3 Termos e Definições

Para garantir clareza e uniformidade na aplicação do Plano de Resposta a Incidentes (PRI), é fundamental adotar um conjunto mínimo de termos e definições. Estes conceitos orientam tanto a compreensão das etapas do plano quanto a comunicação entre os atores envolvidos.

I. **Incidente de Segurança:** Qualquer evento adverso confirmado que comprometa a confidencialidade, integridade, disponibilidade ou autenticidade de dados pessoais, incluindo acessos não autorizados, vazamentos, perdas, alterações ou destruição de informações.

II. **Comunicação de Incidente de Segurança:** Ato do controlador de informar à ANPD e aos titulares a ocorrência de incidente que possa acarretar risco ou dano relevante, nos termos do artigo 48 da LGPD e da Resolução CD/ANPD nº 15/2024.

III. **Dados Pessoais Afetados:** Informações que tiveram sua segurança comprometida em razão do incidente, podendo incluir dados de identificação, financeiros, sensíveis, de autenticação, entre outros.

IV. **Titulares de Dados Pessoais:** Pessoa natural a quem se referem os dados pessoais objeto do tratamento (art. 5º, V, LGPD). Em incidentes, podem ser diretamente afetados e devem ser comunicados sempre que houver risco ou dano relevante.

V. **Controlador:** Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (art. 5º, VI, LGPD). É responsável pela comunicação dos incidentes à ANPD e aos titulares.

VI. **Operador:** Pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador (art. 5º, VII, LGPD). Em caso de incidente, deve comunicar imediatamente ao controlador para que este avalie a necessidade de notificação.

VII. **Encarregado de Dados (DPO):** Pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares e a ANPD (art. 5º, VIII, LGPD). No contexto do PRI, é ator central na coordenação da comunicação de incidentes.

VIII. **Relatório de Tratamento de Incidente:** Documento exigido pela Resolução CD/ANPD nº 15/2024, contendo informações detalhadas sobre o incidente, medidas adotadas e providências para reverter ou mitigar seus efeitos

IX. **Resposta a Incidentes:** Conjunto de ações adotadas pela organização para conter, mitigar e tratar os impactos de um incidente de segurança, incluindo a comunicação formal e a posterior análise para prevenção de novos eventos

X. **Accountability (Responsabilização e Prestação de Contas):** Princípio da LGPD que exige que os agentes de tratamento demonstrem de forma proativa a adoção de medidas eficazes para garantir o cumprimento da legislação (art. 6º, X, LGPD).

1.4 Atores e Responsabilidades

A efetividade de um Plano de Resposta a Incidentes depende da definição clara dos atores envolvidos e de suas responsabilidades. A ausência de papéis bem estabelecidos pode comprometer tanto a resposta técnica quanto a comunicação à ANPD e aos titulares.

A estrutura apresentada justifica-se por três razões principais:

1) Conformidade normativa – A LGPD (art. 48) e a Resolução CD/ANPD nº 15/2024 determinam que a comunicação de incidentes seja realizada de forma tempestiva, com informações completas e verificáveis. Para que isso seja possível, é indispensável que os atores tenham funções pré-definidas, evitando lacunas ou sobreposição de responsabilidades.

2) Eficiência operacional – A gestão de incidentes exige tanto resposta técnica imediata (para conter e mitigar os efeitos) quanto resposta administrativa e legal (para comunicação oficial e registro). A separação entre gestor de SI, gestor de TI, encarregado e comitês garante que cada dimensão seja atendida com a especialização necessária.

3) Governança e accountability – Estruturas colegiadas, como comitês de governança ou de crise, asseguram que as decisões mais sensíveis (ex.: comunicar publicamente um incidente grave) sejam tomadas de forma transparente e respaldada pela alta administração. Isso reforça o princípio da responsabilização e prestação de contas, fortalecendo a confiança social e institucional.

A partir dessa lógica de organização, o Plano de Resposta a Incidentes define um conjunto de atores com papéis específicos, que atuam de forma integrada para assegurar a eficácia do processo de resposta. Entre os principais, destacam-se:

I. Encarregado de Dados (DPO)

1) Atua como ponto focal entre a instituição, os titulares e a ANPD.
2) Coordena a comunicação de incidentes, garantindo que os prazos e requisitos legais sejam cumpridos.
3) Trabalha em conjunto com gestores de segurança e tecnologia para consolidar as informações necessárias à notificação.
4) Zela pelo registro adequado de cada incidente e pela atualização do Relatório de Impacto à Proteção de Dados (RIPD), quando aplicável.

II. Gestor de Segurança da Informação (GSI)

1) Responsável pela análise técnica preliminar do incidente, classificando sua gravidade e impacto.
2) Recomenda medidas imediatas de contenção (ex.: bloqueio de acessos, suspensão de sistemas comprometidos).
3) Apoia a coleta de evidências e orienta sobre medidas de mitigação.
4) Fornece subsídios técnicos para a avaliação de risco, em conjunto com a área de tecnologia.

III. Gestor de Tecnologia da Informação (TI)

1) Atua na execução técnica das medidas de contenção e recuperação.
2) Assegura a preservação de logs, cópias de segurança e demais evidências digitais.
3) Trabalha de forma integrada ao GSI para restaurar serviços afetados, reduzindo indisponibilidades.
4) Apoia a elaboração do relatório final com dados técnicos sobre o incidente.

IV. ETIR – Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos

1) Atua na linha de frente da resposta a incidentes, executando análises técnicas detalhadas.
2) Conduz a investigação da causa raiz e preservar evidências digitais.
3) Implementa medidas imediatas de contenção, erradicação e recuperação de ambientes afetados.
4) Apoia o gestor de SI e o gestor de TI na avaliação técnica e nos relatórios de incidente.

5) Subsidia o Encarregado (DPO) e os Comitês com informações técnicas para a tomada de decisão e para a comunicação formal.

V. Comitê de Governança ou Comitê de Crise

1) Órgão colegiado que pode ser acionado em incidentes de maior gravidade ou impacto reputacional.
2) Decide sobre medidas estratégicas, incluindo a forma de comunicação aos titulares e à sociedade.
3) Aprova recomendações de mitigação de longo prazo e revisões de políticas internas.
4) Garante o alinhamento da resposta com a alta administração.

VI. Alta Administração

1) Responsável por assegurar recursos humanos, tecnológicos e financeiros para a execução do PRI.
2) Deve apoiar institucionalmente o Encarregado e os Comitês, reforçando a cultura de segurança e transparência.
3) Aprova relatórios consolidados e acompanha as recomendações de melhoria.

A definição desses atores e de suas respectivas atribuições demonstra que a efetividade de um Plano de Resposta a Incidentes depende tanto da atuação técnica quanto da governança institucional. Nesse sentido, a análise de experiências já aplicadas em órgãos públicos permite identificar boas práticas que reforçam a importância dessa integração.

1) O TRT-15 instituiu uma Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR) integrada a comitês gestores, destacando a importância da cooperação entre áreas técnicas e de governança.
2) O TCE-MS previu a atuação de um Núcleo de Gestão de Incidentes (NGI) com papéis definidos para o Encarregado e os gestores de SI, além de checklist de responsabilidades.

Esses exemplos reforçam que um PRI deve ser adaptado à realidade de cada instituição, mas sempre garantir papéis claros, responsabilidades documentadas e coordenação integrada entre áreas técnicas, jurídicas e administrativas.

1.5 **Incidente de Segurança com Dados Pessoais e Informações**

A ocorrência de incidentes de segurança é uma realidade inevitável em qualquer organização que trata dados pessoais ou informações sensíveis. Esses eventos podem se originar de falhas técnicas, erros humanos ou ações maliciosas, e possuem potencial de gerar impactos significativos tanto para os titulares quanto para a instituição responsável pelo tratamento.

De acordo com a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018), um incidente de segurança com dados pessoais é qualquer evento adverso confirmado que resulte em situações como acesso não autorizado, destruição, perda, alteração, vazamento ou qualquer forma de tratamento inadequado ou ilícito de dados pessoais, capaz de acarretar risco ou dano relevante aos direitos dos titulares. Esse conceito foi reforçado pela Resolução CD/ANPD nº 15/2024, que detalhou critérios de relevância, prazos e requisitos para a comunicação obrigatória à Agência Nacional de Proteção de Dados (ANPD).

É importante distinguir que nem todo incidente de segurança da informação envolve dados pessoais. Por exemplo, falhas em servidores de arquivos institucionais podem não demandar comunicação à ANPD se não houver tratamento de dados de pessoas naturais. No entanto, incidentes que comprometam a confidencialidade, integridade, disponibilidade ou autenticidade de dados pessoais devem ser tratados com prioridade, pois afetam diretamente a proteção de direitos fundamentais.

Os impactos de um incidente dessa natureza podem ser múltiplos:

1) Para os titulares, incluem riscos de fraude, golpes financeiros, discriminação, constrangimentos ou violação de privacidade.
2) Para as organizações, podem representar sanções administrativas, responsabilização civil, perda de credibilidade institucional e custos de mitigação e recuperação.

No âmbito da Administração Pública, esses eventos assumem relevância ainda maior, já que envolvem dados de cidadãos coletados em razão do interesse público e da prestação de serviços essenciais. Dessa forma, a gestão estruturada de incidentes é condição indispensável para assegurar transparência, responsabilidade e confiança social.

O tratamento adequado de incidentes envolve não apenas medidas técnicas imediatas, mas também processos documentados de avaliação de risco, comunicação às autoridades e aos titulares e registro das providências adotadas. Essa abordagem sistemática fortalece a governança de dados e está alinhada ao princípio da accountability previsto na LGPD.

Assim, este tópico apresenta uma visão geral sobre os incidentes de segurança com dados pessoais, contextualizando seu conceito, impactos e relevância normativa. A partir dessa introdução, os próximos subitens aprofundarão as etapas de resposta, a atuação dos atores envolvidos e as práticas de comunicação que devem ser observadas no âmbito do Plano de Resposta a Incidentes.

1.5.1 – Etapas de Resposta a Incidentes

A resposta a incidentes de segurança com dados pessoais deve seguir um fluxo estruturado e documentado, capaz de assegurar tanto a eficácia técnica na contenção e mitigação quanto a conformidade legal nas comunicações obrigatórias.

Esse encadeamento de etapas reduz riscos de improviso, garante a preservação de evidências e fortalece a transparência institucional.

De acordo com as boas práticas internacionais (ISO/IEC 27035, NIST) e nacionais (Resolução CD/ANPD nº 15/2024; Guia de Resposta a Incidentes – SGD/MGI), o tratamento de incidentes envolve fases sequenciais, mas que podem se sobrepor dependendo da gravidade e da urgência do evento.

O fluxo mínimo de um Plano de Resposta a Incidentes contempla:

1) detecção e registro inicial, para identificar e documentar a ocorrência;
2) análise preliminar e classificação, para confirmar se há risco ou dano relevante;
3) adoção de medidas imediatas de contenção, a fim de evitar a propagação do impacto;
4) consolidação das informações, reunindo dados necessários ao preenchimento do relatório;
5) comunicação formal à ANPD e, quando aplicável, aos titulares;
6) registro e acompanhamento, incluindo a elaboração de relatório final e lições aprendidas.

1.5.2 – Detecção e Registro Inicial

A primeira etapa de um processo de resposta a incidentes consiste na detecção e registro inicial do evento. Esta fase é decisiva porque define a velocidade e a precisão de toda a resposta subsequente. Um incidente não identificado ou mal registrado pode atrasar medidas de contenção, dificultar a análise de riscos e comprometer a comunicação à ANPD e aos titulares.

A detecção pode ocorrer por diferentes meios, como:

1) sistemas automatizados de monitoramento e alerta, que identificam acessos não autorizados, falhas de integridade ou tráfego anômalo;
2) auditorias e controles internos, que sinalizam desvios de procedimentos ou vulnerabilidades;
3) comunicação de usuários ou colaboradores, que reportam comportamentos suspeitos ou falhas em sistemas;
4) denúncias externas ou notícias públicas, que podem revelar incidentes de maior amplitude.

Uma vez detectado, o incidente deve ser registrado imediatamente em sistema próprio ou formulário interno, contendo, no mínimo:

1) data e hora da ocorrência (ou da detecção, se não houver precisão quanto ao momento exato);
2) descrição sumária do evento observado;
3) possível origem ou vetor de ataque;

4) dados ou sistemas potencialmente afetados;
5) nome do responsável pelo registro.

Esse registro inicial cumpre três funções essenciais:

1) garantir rastreabilidade das ações desde o primeiro momento, reforçando a accountability institucional;
2) facilitar a análise preliminar do incidente, ao organizar informações básicas de forma padronizada;
3) documentar evidências que poderão ser usadas tanto na apuração técnica quanto na elaboração do relatório final exigido pela ANPD.

É importante destacar que a celeridade nesta fase é crítica, pois o prazo legal para comunicação à ANPD é de até 3 dias úteis, contados da ciência do incidente (Resolução CD/ANPD nº 15/2024, art. 5º). Assim, quanto mais rápido e preciso for o registro inicial, maior a capacidade da instituição de cumprir esse prazo, ainda que inicialmente com uma comunicação preliminar a ser complementada posteriormente.

1.5.3 – Análise Preliminar e Classificação

Após o registro inicial de um incidente de segurança envolvendo dados pessoais, deve-se proceder à análise preliminar, etapa essencial para confirmar a ocorrência, avaliar sua gravidade e orientar as ações subsequentes. Esta fase é determinante para a tomada de decisão quanto à comunicação obrigatória à Agência Nacional de Proteção de Dados (ANPD) e, quando aplicável, aos titulares afetados, além de definir o nível de mobilização dos recursos internos da organização.

A análise preliminar deve ser conduzida de forma estruturada, multidisciplinar e com base em critérios objetivos, visando garantir a consistência das decisões e a conformidade com a legislação vigente. Para tanto, recomenda-se a identificação dos seguintes elementos:

I. Natureza do incidente: A primeira etapa consiste em compreender a origem do evento, classificando-o conforme sua natureza: falha técnica (como erros de configuração ou indisponibilidade de sistemas), erro humano (envio indevido de informações, acesso não autorizado por engano), ação maliciosa interna (vazamento proposital por colaborador) ou ação maliciosa externa (ataques cibernéticos, como phishing ou ransomware). A correta identificação da causa raiz é fundamental para orientar medidas de contenção e prevenção.

II. Sistemas e serviços afetados: Deve-se mapear os sistemas comprometidos e avaliar o impacto sobre a disponibilidade, integridade e continuidade das operações. Incidentes que afetam sistemas críticos ou serviços essenciais como, atendimento ao público, emissão de documentos ou autenticação de usuários, tendem a apresentar maior gravidade, mesmo quando não há exposição direta de dados pessoais.

III. Dados pessoais envolvidos: É necessário identificar se houve exposição de dados pessoais, distinguindo entre dados comuns (nome, e-mail, telefone) e dados sensíveis (informações sobre saúde, orientação sexual, religião, biometria). Deve-se também considerar se o incidente afeta grupos vulneráveis, como crianças, adolescentes ou idosos, o que agrava o risco jurídico e reputacional.

IV. Abrangência e escala: A análise deve contemplar a quantidade de titulares impactados, bem como a possibilidade de danos coletivos ou efeitos em cadeia, como o uso indevido das informações para fraudes em outras instituições. A escala do incidente pode transformar um evento pontual em uma crise institucional.

A Resolução CD/ANPD nº 15/2024 estabelece critérios objetivos para definir quando um incidente é considerado de risco ou dano relevante. Entre os principais fatores estão:

1) Envolvimento de dados sensíveis ou de menores de idade;
2) Exposição de dados financeiros ou de autenticação que possam facilitar fraudes;
3) Tratamento em larga escala de dados pessoais;
4) Comprometimento de dados necessários à prestação de serviços públicos essenciais.

Com base nesses critérios, o incidente deve ser classificado em níveis de impacto, conforme a seguinte tipologia:

I. Baixo impacto: não há envolvimento de dados pessoais ou o risco aos titulares é considerado irrelevante. A resposta pode se limitar ao registro interno e monitoramento.
II. Médio impacto: há exposição de dados pessoais comuns, mas medidas de mitigação já foram implementadas. Pode haver necessidade de comunicação à ANPD, dependendo da avaliação de risco.
III. Alto impacto: envolve dados sensíveis, grande número de titulares ou risco concreto de fraude, discriminação ou dano coletivo. Exige comunicação obrigatória à ANPD e aos titulares, além da ativação do plano de resposta a incidentes.

O resultado da análise preliminar deve ser formalizado em relatório sucinto, contendo a descrição do incidente, causa provável, sistemas e dados afetados, medidas adotadas, avaliação de risco e justificativa da classificação. Este documento é essencial para subsidiar decisões técnicas, garantir transparência e servir como base para auditorias e prestação de contas.

Recomenda-se que a análise seja conduzida por equipe multidisciplinar, envolvendo áreas como segurança da informação, tecnologia, jurídico e governança. O uso de checklists, matrizes de risco e simulações periódicas contribui para a padronização e eficácia do processo, promovendo uma cultura organizacional de resposta ágil e responsável a incidentes de segurança.

1.5.4 – Adoção de Medidas Imediatas de Contenção

Confirmado o incidente e avaliado seu nível de gravidade, a instituição deve adotar medidas imediatas de contenção. Essa fase busca impedir que o problema se amplie e reduzir ao máximo os impactos técnicos, jurídicos e sociais decorrentes do evento.

Entre as principais ações de contenção, destacam-se:

1) Isolamento do incidente: desconectar sistemas comprometidos da rede, suspender contas suspeitas ou interromper processos que estejam explorando vulnerabilidades.
2) Bloqueio de acessos indevidos: revogar credenciais, redefinir senhas e aplicar controles adicionais de autenticação.
3) Suspensão temporária de serviços: em situações críticas, pode ser necessário interromper funcionalidades para evitar propagação do incidente.
4) Preservação de evidências: assegurar cópias de logs, registros de auditoria e artefatos digitais que permitam investigar a origem e evolução do ataque, em conformidade com as boas práticas de forense digital.
5) Adoção de medidas emergenciais de mitigação: como a restauração de backups, aplicação de patches de segurança ou ativação de planos de contingência.

Essa etapa deve ser registrada de forma documentada, indicando quem autorizou cada medida, quando foi implementada e quais efeitos foram observados. Além disso, é essencial que a contenção seja realizada sem comprometer a integridade das evidências, pois estas serão fundamentais para a análise técnica, para o relatório final e para eventual apuração de responsabilidades.

A agilidade na contenção pode significar a diferença entre um incidente limitado e um evento de grande repercussão. Por isso, deve haver procedimentos previamente definidos no PRI, com fluxos claros de acionamento e autorização, evitando improvisos e atrasos.

1.5.5 – Consolidação das Informações

Após a contenção inicial, a instituição deve concentrar esforços na consolidação das informações relacionadas ao incidente. Essa etapa tem por finalidade reunir, organizar e validar os dados necessários para fundamentar tanto a comunicação à ANPD quanto, quando aplicável, aos titulares.

A consolidação envolve:

1) Descrição detalhada do incidente: circunstâncias em que ocorreu, sistemas impactados e agentes possivelmente envolvidos.
2) Categorias de dados pessoais afetados: distinguir entre dados comuns, sensíveis, financeiros ou de autenticação.

3) Número estimado de titulares impactados: avaliar a abrangência da ocorrência, inclusive se afeta grupos vulneráveis como crianças, adolescentes ou idosos.
4) Medidas de contenção já adotadas: documentar as providências técnicas e administrativas implementadas e seus efeitos.
5) Avaliação preliminar de riscos e danos: identificar consequências prováveis para os titulares e para a instituição, considerando aspectos materiais, morais, reputacionais e operacionais.
6) Ações de mitigação planejadas: indicar próximos passos para reduzir impactos residuais, como reforço de segurança, revisão de processos ou comunicação proativa.

A Resolução CD/ANPD nº 15/2024 exige que a comunicação de incidentes contenha informações completas e verificáveis. Por isso, essa fase de consolidação é indispensável para garantir que os dados transmitidos sejam confiáveis e permitam à autoridade reguladora avaliar a gravidade do incidente.

Além de subsidiar a notificação formal, esse processo gera insumos importantes para o relatório final de tratamento do incidente, fortalecendo a cultura de documentação e de prestação de contas (accountability) prevista na LGPD.

1.5.6 – Comunicação Formal à ANPD

A etapa de comunicação formal à Agência Nacional de Proteção de Dados (ANPD) é uma obrigação prevista no artigo 48 da LGPD e regulamentada pela Resolução CD/ANPD nº 15/2024. Mais do que um ato administrativo, trata-se de um componente estratégico do Plano de Resposta a Incidentes, pois expressa transparência institucional e reforça a responsabilidade do controlador perante a sociedade e a autoridade reguladora.

O prazo legal para comunicação são de até 3 dias úteis contados da ciência do incidente. Quando não for possível apresentar todas as informações nesse prazo, admite-se o envio de uma comunicação preliminar, que deve ser complementada posteriormente com dados adicionais. Essa flexibilidade evita omissões, mas exige que a instituição tenha mecanismos internos para registrar e atualizar as informações de forma ágil.

A comunicação deve ser coordenada pelo Encarregado (DPO) em articulação com a ETIR e comitês gestores, garantindo que os aspectos técnicos e jurídicos estejam alinhados antes do envio. Esse modelo reforça a importância da integração entre áreas técnicas e de governança para evitar falhas ou inconsistências, constituindo uma boa prática para órgãos públicos e privados.

O processo de comunicação à ANPD deve observar os seguintes passos:

1) Abertura de processo eletrônico no SEI/ANPD, sob o tipo “ANPD – Comunicados de Incidentes à Agência Nacional de Proteção de Dados”.

2) Preenchimento do Formulário de Comunicação de Incidente de Segurança (CIS), em versão preliminar ou completa, conforme a maturidade das informações disponíveis.
3) Anexação de documentos comprobatórios, como relatórios técnicos da ETIR, registros de logs e atas de comitês.
4) Indicação do responsável pela comunicação (Encarregado ou representante legal), com a juntada de documentos que comprovem sua legitimidade.

As informações mínimas exigidas incluem:

1) descrição da natureza e categoria do incidente;
2) categorias e volume de dados pessoais afetados;
3) número estimado de titulares impactados;
4) riscos ou danos relevantes identificados;
5) medidas de contenção e mitigação já adotadas;
6) providências futuras planejadas.

Além de atender a uma obrigação legal, essa prática de comunicação estruturada permite que a ANPD avalie com maior precisão a gravidade do incidente, contribui para a adoção de medidas corretivas mais eficazes e fortalece a confiança da sociedade na atuação da instituição.

1.5.7 – Comunicação aos Titulares

A comunicação aos titulares de dados pessoais é uma etapa indispensável do processo de resposta a incidentes, prevista no artigo 48, §1º da LGPD e regulamentada pela Resolução CD/ANPD nº 15/2024. Sempre que o incidente puder acarretar risco ou dano relevante, a instituição deve informar de forma clara e acessível os titulares impactados, possibilitando que adotem medidas de precaução e proteção.

A comunicação deve observar os seguintes princípios:

1) Clareza e simplicidade: utilizar linguagem direta, compreensível para qualquer cidadão, evitando jargões técnicos.
2) Transparência: indicar de forma objetiva quais dados foram afetados, qual a natureza do incidente e quais os possíveis riscos envolvidos.
3) Orientação preventiva: fornecer recomendações práticas para que os titulares reduzam os impactos, como troca de senhas, monitoramento de contas ou atenção a tentativas de fraude.
4) Responsabilidade institucional: destacar as medidas já adotadas pela organização e os próximos passos planejados para mitigar o dano.

De acordo com a Resolução nº 15/2024, a comunicação aos titulares deve conter, no mínimo:

1) a descrição da natureza e categoria dos dados pessoais afetados;
2) as medidas técnicas e de segurança utilizadas para proteção dos dados, observadas as limitações de segurança;
3) os riscos relacionados ao incidente;
4) as medidas que foram ou serão adotadas para reverter ou mitigar os efeitos;
5) orientações aos titulares sobre como podem se proteger.

As boas práticas indicam que a comunicação deve ser realizada por múltiplos canais, a depender do público afetado, como:

1) e-mail institucional ou mensagem eletrônica, quando houver cadastro atualizado;
2) carta ou notificação física, em casos que exijam maior formalidade;
3) avisos públicos (sites, imprensa, redes sociais), quando o incidente afetar grande número de titulares ou inviabilizar o contato individualizado.

Assim como a comunicação à ANPD, esta etapa deve ser registrada e documentada, garantindo a rastreabilidade da informação e a comprovação de que a instituição cumpriu com sua obrigação legal.

Ao comunicar de forma tempestiva e transparente, a instituição não apenas reduz os riscos aos titulares, mas também reforça sua credibilidade institucional e fortalece a cultura de proteção de dados pessoais.

1.5.8 – Registro e Acompanhamento

A fase de registro e acompanhamento é a etapa que consolida todo o processo de resposta ao incidente, garantindo que as ações tomadas sejam devidamente documentadas e que a instituição aprenda com a ocorrência para evitar reincidências.

O registro deve contemplar:

1) relato completo do incidente, incluindo data, hora, origem e descrição detalhada do evento;
2) atores envolvidos e respectivas responsabilidades ao longo da resposta;
3) decisões e medidas implementadas, desde a detecção até a comunicação formal;
4) cópia dos documentos enviados à ANPD e das comunicações realizadas aos titulares;
5) evidências preservadas, como logs, relatórios técnicos e pareceres;
6) avaliação dos resultados das medidas de contenção e mitigação.

Esse conjunto de informações deve compor o Relatório Final de Tratamento de Incidente, exigido pela Resolução CD/ANPD nº 15/2024, que deve estar disponível para fiscalização da Agência e para fins de prestação de contas (accountability).

O acompanhamento posterior ao incidente envolve:

1) monitoramento contínuo dos sistemas afetados, para prevenir reincidências;
2) avaliação de impactos residuais sobre titulares e serviços;
3) revisão de controles técnicos e administrativos de segurança;
4) atualização de políticas internas, planos de contingência e do próprio Plano de Resposta a Incidentes (PRI);
5) incorporação das lições aprendidas ao processo de governança de dados e à cultura organizacional.

Boas práticas observadas em planos como os do TRT-15 e do TCE-MS indicam que a elaboração de checklists e relatórios pós-incidente favorece a padronização, facilita auditorias e reforça a transparência das ações institucionais.

Assim, a etapa de registro e acompanhamento fecha o ciclo de resposta, transformando um evento adverso em oportunidade de aprendizado institucional, fortalecendo a governança de dados e a confiança da sociedade nos serviços prestados.

1.6 - Registro Interno de Incidentes – Requisitos e Formatos

O registro interno de incidentes de segurança da informação com dados pessoais é um dos pilares da governança em proteção de dados. Ele não apenas documenta a ocorrência, mas também permite a rastreabilidade das ações, a prestação de contas (accountability) e o aprendizado institucional. A Resolução CD/ANPD nº 15/2024 reforça essa exigência ao estabelecer que os agentes de tratamento devem manter registros completos, organizados e acessíveis para fins de fiscalização e melhoria contínua.

Requisitos mínimos do registro:

1) Identificação do incidente: data e hora da ocorrência ou detecção, origem (interna ou externa), vetor de ataque (ex: phishing, malware, erro humano).
2) Descrição técnica e contextual: detalhamento do evento, sistemas afetados, tipo de falha ou vulnerabilidade explorada.
3) Dados pessoais comprometidos: categorias (comuns, sensíveis, financeiros), volume estimado, perfil dos titulares (ex: crianças, idosos).
4) Impacto potencial e riscos associados: avaliação preliminar dos danos materiais e imateriais, incluindo riscos à privacidade, reputação ou segurança dos titulares.
5) Medidas adotadas: ações de contenção, mitigação, comunicação e recuperação.
6) Atores envolvidos: responsáveis técnicos, jurídicos e administrativos, com registro das decisões tomadas.

7) Evidências preservadas: logs, relatórios técnicos, capturas de tela, pareceres jurídicos e registros de comunicação.

Formatos recomendados:

1) Formulários estruturados: padronizados por tipo de incidente, facilitando a análise comparativa e a consolidação de dados.
2) Sistemas eletrônicos de gestão de incidentes: com trilhas de auditoria, controle de versões e integração com o Plano de Resposta a Incidentes (PRI).
3) Relatórios periódicos e consolidados: utilizados para prestação de contas à alta administração, à ANPD e para fins de auditoria interna.

O registro interno deve ser mantido por prazo compatível com a legislação vigente e deve estar disponível para consulta da autoridade reguladora, auditorias externas e comitês de governança. A padronização e a qualidade desses registros são fundamentais para demonstrar conformidade e maturidade institucional.

Boas Práticas Nacionais

A experiência brasileira na gestão de incidentes de segurança com dados pessoais tem avançado significativamente, especialmente após a vigência da LGPD e a atuação da ANPD. Diversos órgãos públicos e entidades privadas têm adotado práticas que se destacam pela efetividade, transparência e alinhamento com os princípios da proteção de dados.

Exemplos de boas práticas:

1) TRT-15: instituiu um Plano de Resposta com fluxos claros de comunicação, comitês internos e equipe técnica especializada (ETIR), promovendo integração entre áreas.
2) TCE-MS: desenvolveu um checklist de responsabilidades para o Encarregado de Dados e gestores de Segurança da Informação, com foco em documentação e prestação de contas.
3) IBAMA: elaborou diretrizes aplicáveis à esfera federal, considerando a complexidade operacional e a necessidade de coordenação intersetorial.

Diretrizes comuns observadas:

1) Estruturação de equipes multidisciplinares: com atuação técnica, jurídica e administrativa integrada.
2) Procedimentos documentados: desde a detecção até a comunicação formal, com registros padronizados e relatórios pós-incidente.
3) Comunicação proativa aos titulares: com linguagem acessível, orientações práticas e canais de atendimento.
4) Cultura organizacional de segurança: com treinamentos periódicos, simulações de incidentes e revisão contínua de políticas.

Essas práticas demonstram que a maturidade institucional está diretamente relacionada à capacidade de integrar governança, segurança e transparência. O benchmark nacional serve como referência para a construção de políticas locais mais eficazes e alinhadas à realidade da administração pública.

1.7 - Boas Práticas Internacionais

No cenário internacional, a gestão de incidentes de segurança com dados pessoais é regida por normas consolidadas, como o Regulamento Europeu de Proteção de Dados (GDPR), os padrões da ISO/IEC 27035 e os frameworks do NIST. Essas referências oferecem diretrizes robustas para a estruturação de processos, definição de responsabilidades e comunicação eficaz.

Práticas destacadas:

1) GDPR (União Europeia): exige comunicação de incidentes em até 72 horas, incentivando fluxos internos ágeis e bem documentados.
2) ISO/IEC 27035: propõe um ciclo completo de resposta, incluindo detecção, análise, contenção, comunicação, tratamento e aprendizado.
3) NIST (EUA): oferece frameworks para resposta a incidentes com foco em segurança cibernética, proteção de dados e resiliência organizacional.

1.8 - Elementos recorrentes:

1) Playbooks de resposta: com cenários simulados, protocolos de ação e fluxos de decisão.
2) Treinamentos regulares: para equipes técnicas e administrativas, com foco em prevenção e resposta rápida.
3) Avaliação contínua de riscos: com testes de vulnerabilidade, auditorias e revisão de controles.
4) Comunicação multicanal aos titulares: com foco em acessibilidade, orientação e mitigação de danos.

A incorporação dessas práticas ao contexto brasileiro, respeitando as especificidades locais, contribui para o fortalecimento da governança de dados e para a construção de uma cultura institucional de segurança e responsabilidade. O benchmark internacional permite identificar padrões de excelência e adaptar soluções eficazes à realidade municipal.

Recomendações

Diante do cenário analisado, recomenda-se que o Município implemente um conjunto articulado de ações voltadas à melhoria da comunicação de incidentes de segurança da informação envolvendo dados pessoais, com vistas à conformidade legal, à proteção dos titulares e ao fortalecimento da governança pública. Essas

recomendações se desdobram em quatro eixos principais: planejamento estratégico, capacitação institucional, infraestrutura tecnológica e cultura organizacional.

No eixo do planejamento estratégico, é imprescindível que o Município elabore e institucionalize um Plano de Resposta a Incidentes (PRI), com base nas diretrizes da Resolução CD/ANPD nº 15/2024. Esse plano deve conter protocolos claros para identificação, classificação, contenção, análise e comunicação de incidentes, além de prever a atuação coordenada entre os setores jurídico, tecnológico e administrativo. A formalização do PRI deve ser acompanhada da designação de responsáveis, da definição de prazos e da criação de indicadores de desempenho que permitam o monitoramento contínuo da eficácia das ações adotadas.

Quanto à capacitação institucional, recomenda-se a realização de programas permanentes de formação e atualização dos servidores públicos, especialmente daqueles que atuam diretamente no tratamento de dados pessoais. Esses programas devem abordar não apenas os aspectos legais da LGPD, mas também os fundamentos da segurança da informação, a gestão de riscos, a comunicação em situações de crise e a ética no serviço público. A capacitação deve ser ofertada em formatos diversos — presenciais, remotos e híbridos — e adaptada aos diferentes níveis de escolaridade e funções dos servidores.

No eixo da infraestrutura tecnológica, é necessário que o Município invista na modernização de seus sistemas de informação, com foco na segurança, na interoperabilidade e na rastreabilidade. Isso inclui a adoção de soluções de criptografia, controle de acesso, monitoramento de redes e backup automatizado, bem como a implementação de plataformas que permitam o registro e a gestão centralizada de incidentes. A integração desses sistemas com os canais de comunicação interna e com os mecanismos de notificação à Agência Nacional de Proteção de Dados (ANPD) é fundamental para garantir a agilidade e a precisão das respostas.

A cultura organizacional, por sua vez, deve ser fortalecida por meio de campanhas educativas, ações de sensibilização e incentivos à conduta ética. É essencial que os servidores compreendam que a proteção de dados pessoais não é apenas uma obrigação legal, mas um compromisso institucional com a cidadania e com os princípios da administração pública. A criação de um ambiente de confiança, onde os incidentes possam ser reportados sem receio de retaliação, contribui para a detecção precoce de vulnerabilidades e para a construção de soluções mais eficazes.

Recomenda-se que os órgãos e entidades que ainda não tenham instituído seus respectivos Comitês de Proteção de Dados Pessoais o façam, conforme disposto no Art. 20 da Política Municipal de Proteção de Dados. A atuação deve ser integrada ao Encarregado pelo Tratamento de Dados Pessoais (DPO), com vistas a assegurar transparência, responsabilização e conformidade com boas práticas.

Conclusão

Em conclusão, o presente relatório evidencia que a comunicação de incidentes de segurança da informação com dados pessoais é um componente essencial da governança pública digital e da proteção dos direitos fundamentais. A ausência de protocolos claros, de capacitação adequada e de infraestrutura segura compromete não apenas a conformidade com a LGPD, mas também a confiança da população na gestão pública. Por outro lado, a adoção de medidas estruturantes, como as aqui recomendadas, permite ao Município avançar na construção de uma política pública robusta, integrada e orientada por princípios de legalidade, eficiência e transparência.

A consolidação dessas diretrizes representa um passo decisivo rumo à maturidade institucional em proteção de dados, contribuindo para a prevenção de riscos, a mitigação de danos e a promoção de uma cultura de respeito à privacidade. Ao reconhecer a centralidade da informação na era digital e ao assumir a responsabilidade pela sua proteção, o Município reafirma seu compromisso com a cidadania, com a inovação e com a construção de uma administração pública mais segura, justa e confiável.

Fontes e Referências:

ANPD. 1. O que é um incidente de segurança com dados pessoais? Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acesso em 29 set. 2025.

ANPD. 4. Qual o prazo para comunicar um incidente de segurança? Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acesso em 29 set. 2025.

ANPD. Guia de Boas Práticas em Segurança da Informação para Agentes de Tratamento de Pequeno Porte, 2021. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-vf.pdf. Acesso em 15 set. 2025.

ANPD. Painel Tipo de Incidentes Recebidos. Disponível em: https://app.powerbi.com/view?r=eyJrIjoiODUxYzY4NGUtMWUwNy00MGE1LWExMjUtYmY3ZWRkMmExMWQzIiwidCI6IjVhYmEwNGExLWY4NjMtNGI1Ni04MTdkLTQ0MjkxYzkwZDFiOCJ9. Acesso em 29 set. 2025.

ANPD. Resolução CD/ANPD nº 15, de 24 de abril de 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024. Acesso em 15 set. 2025.

Brasil. Lei nº 13.709/2018 – LGPD. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 15 set. 2025.

EUROPA. JORNAL OFICIAL DA UNIÃO EUROPEIA. Regulamento (Ue) 2016/679 Do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 25 set. 2025.

ISO STANDARDS. ISO/IEC 27035-1:2023. Disponível em: https://www.iso.org/standard/78973.html. Acesso em: 25 set. 2025.

Glossário de Segurança da Informação. Disponível em: https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/glossario-de-seguranca-da-informacao-1. Acesso em 15 set. 2025.

IBM. Cost of a Data Breach Report 2025. Disponível em: https://www.ibm.com/br-pt/reports/data-breach. Acesso em 15 set. 2025.

JUNIOR, Silvio Maciel e Silva. Alicerces da LGPD: Decretos federais 12.572 e 12.573/25. Disponível em: https://www.migalhas.com.br/depeso/436290/alicerces-da-lgpd-decretos-federais-12-572-e-12-573-25. Acesso em 15 set. 2025.

JUNIOR, Silvio Maciel e Silva. A Nova Era Da Comunicação De Incidentes De Segurança De Dados Pessoais: Desvendando A Resolução CD/ANPD Nº 15/2024 *In* MONTEIRO, Manuela Cotulio. RUZZI, Mariana (Orgs.). Inovações digitais: proteção de dados, cibersegurança, tecnologias emergentes e neurodireitos. Recife: Editora Império, 2025. p. 69.

JUNIOR, Silvio Maciel e Silva. Segurança De Dados Começa Com Pessoas: O Exemplo Do Município Do Rio De Janeiro *In* LIMA, Ana Paula Canto, ROSAS, Eduarda Chacon (Coord.). LGPD: Debates e Temas Relevantes, Vol. IV. Recife: Editora Império, 2025. p. 347/348. Disponível em: https://drive.google.com/file/d/1P1FJTI2FYQo-eVqyMtJ2RkmYlDaJqBca/view. Acesso em 29 set. 2025.

Laboratório Nacional de Computação Científica - LNCC. Disponível em: https://www.gov.br/lncc/pt-br/centrais-de-conteudo/campanhas-de-conscientizacao/gestao-de-seguranca-da-informacao/os-quatro-pilares-da-seguranca-da-informacao-2013-confidencialidade-disponibilidade-integridade-e-autenticidade . Acesso em 15 set. 2025.

MINISTÉRIO DO MEIO AMBIENTE E MUDANÇA DO CLIMA, INSTITUTO BRASILEIRO DO MEIO AMBIENTE E DOS RECURSOS NATURAIS RENOVÁVEIS. Plano De Resposta a Incidentes De Segurança Com Dados Pessoais. Disponível em: https://www.gov.br/ibama/pt-br/acesso-a-informacao/acoes-e-programas/arquivos/2024-08-13_plano_de_resposta_a_incidentes_com_dados_pessoais_ibama.pdf. Acesso em: 30 set. 2025.

NIST. Cybersecurity and privacy. Disponível em: <https://www.nist.gov/cybersecurity-and-privacy>. Acesso em: 25 set. 2025.

TAMER, Maurício. Manual de Direito da Proteção de Dados Pessoais - 1ª Edição 2025. Rio de Janeiro: SRV, 2024. E-book. p.310 e 316. ISBN 9786553629905. Disponível em: https://app.minhabiblioteca.com.br/reader/books/9786553629905/. Acesso em: 29 set. 2025.

TCU. Acórdão 1372/2025 - PLENÁRIO. Disponível em: https://pesquisa.apps.tcu.gov.br/documento/acordao-completo/*/KEY%253AACORDAO-COMPLETO-2704827/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0. Acesso em 15 set. 2025.

TRIBUNAL DE CONTAS DO ESTADO DE MATO GROSSO DO SUL. Plano de Resposta a Incidentes de Segurança da Informação e Dados Pessoais do Tribunal de Contas do Estado de Mato Grosso do Sul. Disponível em: https://sip-barramento.tce.ms.gov.br/public/Links/25/in-n-44---plano-de-resposta-a-incidentes-de-segurana-da-informao-e-dados-pessoaispdf-64bf9d.pdf. Acesso em: 30 set. 2025.

TRIBUNAL REGIONAL DO TRABALHO DA 15ª REGIÃO. Plano de Resposta a Incidentes de Segurança - 2023. Disponível em: https://trt15.jus.br/sites/portal/files/roles/institucional/gestao-estrategica/lgpd/Plano%20de%20Resposta%20a%20Incidentes%20de%20Seguran%C3%A7a.pdf. Acesso em: 30 set. 2025.

Verizon. Data Breach Investigations Report (DBIR 2024). Disponível em: https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf. Acesso em 15 set. 2025.