DEPARTAMENTO DE TRÂNSITO DO ESTADO
DO RIO DE JANEIRO
ATO DO PRESIDENTE
PORTARIA DETRAN SEI Nº 6835 DE 30 DE JUNHO DE 2025

DISPÕE SOBRE O PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO (PRISIC) NO ÂMBITO DO DETRAN/RJ E DÁ OUTRAS PROVIDÊNCIAS.

O **PRESIDENTE DO DEPARTAMENTO DE TRÂNSITO DO ESTADO DO RIO DE JANEIRO**, no uso das atribuições que lhe são conferidas e de acordo com o que consta no processo administrativo nº SEI-150016/084722/2025, emite a seguinte Política de Privacidade e Proteção de Dados Pessoais (PPPDP), a vigorar a partir da data de sua assinatura, revogando todas as disposições contrárias, e

CONSIDERANDO:

- A necessidade de assegurar a resposta tempestiva, coordenada e efetiva a incidentes de segurança da informação e da comunicação;

- A LEI Nº 13.709, DE 14 DE AGOSTO DE 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD);

- A PORTARIA PRODERJ/PRE Nº 825, DE 26 DE FEVEREIRO DE 2021

– que institui a Estratégia da Governança de Tecnologia da Informação e Comunicação do Estado do Rio de Janeiro – EGTIC/RJ;

- A INSTRUÇÃO NORMATIVA PRODERJ/PRE N.º 02, DE 28 DE ABRIL DE 2022 - Regulamenta os procedimentos de Segurança da Informação em soluções de Tecnologia da Informação e Comunicação (TIC);

- A PORTARIA DETRAN/RJ Nº 6.739, DE 07 DE JANEIRO DE 2025, que institui a Política de Segurança da Informação e Comunicação (POSIC);

- A PORTARIA DETRAN/RJ Nº 6.759, DE 16 DE MAIO DE 2025, que institui a Política de Privacidade e Proteção de Dados Pessoais (PPPDP);

- A PORTARIA DETRAN/RJ Nº 6.790, DE 25 DE ABRIL DE 2025, que institui a Política de Gestão e Controle de Riscos (PGCR);

- As normas ABNT NBR ISO/IEC 27001:2022 e ABNT NBR ISO/IEC 27701:2019;

- O disposto no DECRETO ESTADUAL Nº 48.891/2024, que institui a Política de Governança em Privacidade e Proteção de Dados Pessoais no Estado do Rio de Janeiro.

RESOLVE:

Art. 1º - Fica instituído, no âmbito do Departamento de Trânsito do Estado do Rio de Janeiro – DETRAN/RJ, o Plano de Resposta a Incidentes de Segurança da Informação e Comunicação (PRISIC), que integra o Programa de Governança em Privacidade e Proteção de Dados Pessoais (PGPPDP) da Autarquia.

§ 1º O Plano de Resposta a Incidentes de Segurança com Dados Pessoais, que contém o fluxo detalhado, está descrito no Anexo I deste Plano.

§ 2º O Formulário de Comunicação de Incidentes de Segurança com Dados Pessoais, consta Anexo II deste Plano.

Art. 2º - O PRISIC visa estabelecer:

I – O fluxo institucional de notificação, tratamento e comunicação de incidentes;

II – Os papéis e responsabilidades dos agentes envolvidos na resposta a incidentes;

III – A articulação entre os processos de segurança da informação, proteção de dados pessoais e gestão de riscos;

IV – A conformidade com os dispositivos legais e regulatórios, em especial a LGPD e as normas estaduais de governança.

Parágrafo único. O PRISIC integra esta Portaria como Anexo I e deverá ser periodicamente revisado pela Diretoria de Tecnologia da Informação e Comunicação (DIRTIC), com o apoio do Encarregado pelo Tratamento de Dados Pessoais.

Art. 3º - São considerados incidentes de segurança da informação e comunicação os eventos confirmados ou sob suspeita, capazes de comprometer a confidencialidade, integridade, disponibilidade ou autenticidade de dados, sistemas ou serviços institucionais, inclusive os que envolvam dados pessoais.

Art. 4º - A resposta a incidentes será estruturada nas seguintes etapas:

I – Identificação da ocorrência ou suspeita de incidente;

II – Análise, confirmação e classificação do incidente;

III – Preenchimento do Formulário de Comunicação de Incidente de Segurança com Dados Pessoais;

IV – Comunicação às partes interessadas, nos termos da LGPD;

V – Elaboração de relatório técnico final de ação, prevenção e de lições aprendidas.

Parágrafo único. Quando o incidente envolver dados pessoais, deverá ser obrigatoriamente comunicado ao Encarregado pelo Tratamento de Dados Pessoais para avaliação quanto à necessidade de notificação à Autoridade Nacional de Proteção de Dados (ANPD), ao Encarregado Central do Governo do Estado do Rio de Janeiro, e aos titulares.

Art. 5º - Compete ao Responsável pelo Tratamento e Resposta a Incidentes, formalmente designado pela Portaria DETRAN/RJ Nº 6.800, no âmbito do Plano de Resposta a Incidentes de Segurança da Informação e Comunicação (PRISIC), com base no art. 18 da Instrução Normativa PRODERJ/PRE nº 02:

I – Monitorar continuamente os ativos e recursos de tecnologia da informação e comunicação da Autarquia, com foco na detecção de anomalias, vulnerabilidades ou eventos que possam caracterizar incidentes de segurança;

II – Realizar, em articulação com o Gestor de Segurança da Informação (**GSI**), a análise técnica e a classificação dos incidentes, considerando criticidade, impacto e abrangência institucional;

III – Executar ou coordenar as ações de contenção, mitigação, erradicação e recuperação relacionadas ao incidente, em conjunto com as equipes técnicas competentes;

IV – Manter registros atualizados de incidentes, evidências, providências adotadas e lições aprendidas, com vistas à melhoria contínua da segurança e à prevenção de recorrências;

V – Notificar de forma imediata o Encarregado pelo Tratamento de Dados Pessoais, em caso de incidente envolvendo dados pessoais ou sensíveis, prestando o suporte necessário à elaboração de relatório de impacto ou comunicação à ANPD, quando cabível;

VI – Propor, sempre que necessário, medidas corretivas e recomendações técnicas à DIRTIC, ao GSI ou aos dirigentes das unidades afetadas;

VII – Atuar de forma coordenada com a estrutura de gestão de riscos, conforme diretrizes da Portaria DETRAN/RJ nº 6.790, reportando os eventos que impliquem riscos relevantes à segurança da informação ou à privacidade de dados.

Art. 6º - As ações previstas no Plano deverão observar os princípios e diretrizes estabelecidos pela Política de Gestão e Controle de Riscos (PGCR), sendo obrigatória a análise de impacto e risco em qualquer evento de segurança classificado como relevante.

Art. 7º - Compete ao Encarregado pelo Tratamento de Dados Pessoais, no âmbito do Plano de Resposta a Incidentes de Segurança da Informação e Comunicação (PRISIC):

I – Avaliar, com base nas evidências recebidas do Responsável pelo Tratamento e Resposta a Incidentes, a existência de risco ou dano relevante aos titulares de dados pessoais;

II – Coordenar, junto à DIRTIC e à unidade afetada, a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), quando exigido pela LGPD ou recomendado pelas boas práticas;

III – Providenciar, quando cabível, a comunicação formal do incidente à **ANPD**, contendo as informações previstas no art. 48 da **LGPD** e nos guias da **ANPD**;

IV – Assegurar que os titulares dos dados afetados sejam informados com clareza, transparência e tempestividade sobre o incidente, conforme as diretrizes da **PPPDP**, instituída na **Portaria DETRAN-RJ Nº 6.759**;

V – Manter controle documental dos incidentes que envolvam dados pessoais, bem como das medidas adotadas para correção e prevenção de reincidências;

VI – Articular com o Comitê de Implantação do Programa de Governança em Privacidade (**COMPGP**) e com o Comitê Gestor de Tecnologia da Informação e Comunicação (**COMGTIC**) a revisão de controles e fluxos afetados;

VII – Emitir pareceres e orientações sobre incidentes que envolvam dúvidas quanto à aplicação da **LGPD** e à responsabilização institucional.

Art. 8º - Compete ao Gestor de Segurança da Informação (**GSI**), no âmbito do Plano de Resposta a Incidentes de Segurança da Informação e Comunicação (**PRISIC**):

I – Apoiar tecnicamente o Responsável pelo Tratamento e Resposta a Incidentes na análise de impacto, identificação de vulnerabilidades e proposição de medidas de mitigação;

II – Assessorar o Comitê de Implantação do Programa de Governança em Privacidade (**COMPGP**) e o Encarregado de Dados nos processos de comunicação de incidentes e no atendimento a obrigações legais e regulamentares;

III – Supervisionar a conformidade dos registros, ações e relatórios gerados no processo de tratamento de incidentes com as políticas institucionais de segurança da informação;

IV – Integrar os procedimentos de resposta a incidentes com a estrutura de Gestão de Riscos Corporativos, conforme disposto na **PGCR**;

V – Manter interlocução com os titulares das áreas técnicas, promovendo capacitação e conscientização sobre resposta a incidentes, prevenção de falhas e boas práticas de segurança.

Art. 9º - Integra a equipe multidisciplinar responsável pela resposta a incidentes de segurança da informação e comunicação envolvendo dados pessoais no âmbito do DETRAN/RJ, para os fins do Plano de Resposta a Incidentes de Segurança da Informação e Comunicação (PRISIC), os seguintes órgãos e unidades administrativas:

I – a Presidência (**PRESI**) do DETRAN/RJ, na qualidade de autoridade superior da Autarquia;

II – o Encarregado pelo Tratamento de Dados Pessoais, designado na forma da legislação vigente;

III – a Diretoria de Tecnologia da Informação e Comunicação (**DIRTIC**), unidade responsável pelas ações de prevenção, contenção e recuperação de incidentes em ambiente tecnológico;

IV – o Comitê de Implantação do Programa de Governança em Privacidade e Proteção de Dados Pessoais (**COMPGP**), responsável pelo acompanhamento da governança em privacidade no órgão;

V – o Comitê Gestor de Tecnologia da Informação e Comunicação (**COMGTIC**), responsável por apoiar a integração das diretrizes de TIC à resposta a incidentes;

VI – a Diretoria Jurídica (**DIRJUR**), responsável por avaliar os aspectos legais e regulatórios relacionados aos incidentes, inclusive quanto à comunicação à Autoridade Nacional de Proteção de Dados (ANPD) e outras instâncias competentes;

VII – a Assessoria de Comunicação (**ASSCOM**), responsável pela comunicação institucional, interna e externa, relacionada a incidentes que demandem pronunciamento público.

§ 1º Os membros da equipe multidisciplinar deverão atuar de forma coordenada, garantindo a efetividade na prevenção, detecção, resposta, comunicação e correção de incidentes de segurança da informação que envolvam dados pessoais.

Art. 10 - O Plano de Resposta a Incidentes de Segurança da Informação e Comunicação (**PRISIC**), instituído por esta Portaria, será publicado em anexo e amplamente divulgado a todos os setores do **DETRAN/RJ**, sendo de observância obrigatória por todas as áreas da autarquia.

Art. 11 - Esta Portaria entra em vigor na data de sua publicação.

Rio de Janeiro, 30 de junho de 2025.

VINÍCIUS MEDEIROS FARAH
Presidente do DETRAN/RJ

DETRAN.RJ

GOVERNO DO ESTADO RIO DE JANEIRO

Rio2030

PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA

com DADOS PESSOAIS

Programa de Governança em Privacidade e Proteção de Dados Pessoais

Cláudio Castro
Governador

Vinícius Farah
Presidente do DETRAN-RJ

André Mônica
Vice-Presidente do DETRAN-RJ

Jorge Felipe
Encarregado pelo Tratamento de Dados Pessoais do DETRAN-RJ

Elaboração e Revisão:

Assessoria da Presidência do DETRAN-RJ
Jorge Felipe
Wanderson Neto
Michelle Gama

Diretoria de Tecnologia da Informação e Comunicação do DETRAN-RJ
Glaucio Paz
Alexandre Mattioli

Apoio e Suporte

Diretoria Jurídica do DETRAN-RJ
Sérgio Pimentel
Andreia Clemente
Bruna Nogueira
Renata Saldanha

Maio de 2025
VERSÃO 1.0

www.detran.rj.gov.br

SUMÁRIO

INTRODUÇÃO

Um incidente de segurança com dados pessoais é um evento adverso envolvendo dados de titulares. Ele acontece quando algum tipo de uso não autorizado, destruição, perda, exposição, alteração, vazamento ou ataque compromete a confidencialidade, a integridade ou a disponibilidade de dados pessoais.

Incidentes podem decorrer de ações voluntárias ou acidentais que resultem em divulgação, alteração, perda ou acesso não autorizado a dados armazenados em sistemas de informação ou em banco de dados, publicação não intencional de dados dos titulares ou até mesmo no envio de informações para o destinatário incorreto.

Mas também podem ocorrer por meio de atos intencionais, como a invasão de um sistema de informação, o sequestro de dados ou furto de um dispositivo de armazenamento de dados.

A mera existência de uma vulnerabilidade em um sistema de informação não constitui um incidente de segurança. A exploração da referida vulnerabilidade, no entanto, pode resultar em um incidente.

Um incidente de roubo de um dispositivo eletrônico, por exemplo, pode ou não ser capaz de causar um risco relevante aos titulares de dados. A avaliação vai depender do tipo de dado armazenado, do contexto da atividade de tratamento e do fato de os dados estarem ou não protegidos por criptografia.

São considerados incidentes capazes de causar risco ou dano relevante, aqueles que possam causar danos materiais ou morais aos titulares, expô-los a situações de discriminação ou de roubo de identidade, especialmente se envolverem dados em larga escala, sensíveis e de grupos vulneráveis como crianças, adolescentes ou idosos.

Merecem destaque os seguintes exemplos de incidentes de segurança da informação:

- Acesso de terceiro não autorizado na rede de computadores, que ocorre quando algum agente externo, ou mesmo um servidor ou terceirizado, acessa uma parte do sistema que não deveria;

- Vírus e códigos maliciosos, cuja detecção requer o uso de ferramentas próprias, como antivírus;

- Uso impróprio de sistemas ou de informações, que ocorrem quando um servidor ou terceirizado usa um e-mail corporativo para a promoção de negócios pessoais, ou quando instala uma ferramenta não autorizada no computador do Órgão ou utiliza um pen drive de forma não autorizada ou, ainda, quando imprime documentos sigilosos de forma não autorizada e os repassa para terceiros.

Por essa razão, é necessário que o DETRAN-RJ esteja preparado para agir em caso de "violação da segurança que provoque, de modo acidental ou ilícito a destruição, a perda, a alteração, a divulgação ou o acesso não autorizados a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento" (definição constante no art. 4º do GDPR - *General Data Protection Regulation* - Regulamento Geral de Proteção de Dados).

Em atenção à Lei nº 13.709/2018, Lei Geral de Proteção de Dados - LGPD, que regula as atividades de tratamento de dados pessoais:

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

§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I- a descrição da natureza dos dados pessoais afetados;
II- as informações sobre os titulares envolvidos;
III- a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comerciale industrial;
IV- os riscos relacionados ao incidente;
V- os motivos da demora, no caso de a comunicação não ter sido imediata; e
VI- as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

§ 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:

I- ampla divulgação do fato em meios de comunicação; e
II- medidas para reverter ou mitigar os efeitos do incidente.

§ 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

Neste sentido, o presente Plano dispõe sobre as medidas que devem ser adotadas no caso de uma situação de emergência ou evento de risco que possam ocasionar danos aos ativos tecnológicos do Órgão, viabilizando, inclusive, a comunicação apropriada e tempestiva à Autoridade Nacional de Proteção de Dados - ANPD, quando for o caso.

OBJETIVOS

GERAL

Promover uma estratégia de comunicação para prevenção e ação efetiva nas respostas às situações emergenciais e imprevistas, de forma documentada, formalizada, rápida e confiável, resguardando as evidências que possam ajudar a prevenir novos incidentes e a atender às exigências legais de comunicação e transparência.

A fim de preservar a reputação das atividades prestadas pelo DETRAN RJ, evitar custos indesejados, minimizara ocorrência de problemas legais e preservar a confiança dos usuários externos e internos.

ESPECÍFICOS

- Conferir clareza sobre o fluxo de procedimentos adequados e os responsáveis, no caso de incidentes.
- Assegurar respostas rápidas, efetivas e coordenadas.
- Evoluir continuamente com as lições aprendidas.

TERMOS E DEFINIÇÕES

Agentes de tratamento: corresponde ao Controlador e ao Operador em conjunto, não são considerados controladores ou operadores os indivíduos subordinados, tais como os funcionários, os servidores públicos ou as equipes de trabalho de uma organização, já que atuam sob o poder diretivo do agente de tratamento;

Anonimização: é a utilização de meios técnicos razoáveis e disponíveis por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

Ataque: evento de exploração de vulnerabilidades, ocorre quando um atacante tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais ou tornar um serviço inacessível;

Autoridade Nacional de Proteção de Dados (ANPD): é o órgão da administração pública nacional responsável por fiscalizar e zelar pelo cumprimento da Lei Geral de Proteção de Dados em todo o território brasileiro;

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

Bot: código malicioso que permite ao invasor controlar remotamente o computador ou o dispositivo que hospeda;

Consentimento: a LGPD definiu algumas hipóteses para tratamento dos dados pessoais, sendo uma delas o consentimento. Entretanto, para a coleta desse consentimento, foram impostos alguns requisitos, devendo, a manifestação do consentimento, ser livre, informada e inequívoca;

Controlador: é toda pessoa física ou jurídica, de direito público ou privado, a quem competem decisões referentes ao tratamento de dados pessoais;

Dado anonimizado: é o dado pessoal que, apesar de estar relacionado a uma pessoa natural, passou por um processo de anonimização e não pode mais ser identificado;

Dados pessoais: qualquer informação relacionada a um indivíduo que possa ser usada para identificá-lo, direta ou indiretamente, por conta própria ou quando combinada com outras informações;

Dados que identificam uma pessoa natural: são as informações que identificam uma pessoa por si só (nome completo, caso não exista homônimo; número do CPF, do RG, do passaporte, entre outros);

Dados que possam identificar pessoa natural: são as informações que, somadas, passam a identificar alguém (primeiro nome, endereço, características físicas, entre outros);

Dados pessoais sensíveis: são dados pessoais que digam respeito a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Data center: é um ambiente projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados e sistemas de ativos de rede;

Documento físico e documento digital: os documentos físicos são aqueles elaborados em suportes físicos, por exemplo, em papel. Já os documentos digitais são informações registradas, codificadas em forma analógica ou em dígitos binários, acessíveis e interpretáveis por meio de um equipamento eletrônico;

Encarregado pelo Tratamento de Dados Pessoais ou Data Privacy Officer (DPO): 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);

Engenharia social: técnica empregada por criminosos virtuais para induzir usuários desavisados a enviar dados confidenciais, infectar seus computadores com malware ou abrir links para sites infectados;

Expurgo de dados: significa destruição segura e definitiva de informações, ou seja, quando os dados não existem mais ou não podem mais ser acessados pelo Controlador de qualquer forma;

GMT (Greenwich Mean Time): Horário Médio de Greenwich, baseado no primeiro meridiano de Greenwich, que passa pelo Observatório Real, perto de Londres;

Incidente: evento, ação ou omissão que tenha permitido ou possa vir a permitir acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou, ainda, 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 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 ou inadequada, que tem a capacidade de pôr em risco os direitos e as liberdades dos titulares de dados pessoais;

IP: Protocolo da Internet (Internet Protocol), número utilizado para identificar um dispositivo de tecnologia da informação em uma rede, ou Internet;

LGPD: Lei Geral de Proteção de Dados – Lei n. 13.709/2018 que possui, como objetivo, regulamentar as atividades que se utilizam de dados pessoais em território nacional, por pessoa natural ou jurídica de direito público ou privado, em ambientes físicos ou digitais. Dessa forma, a LGPD poderá compreender uma relação com estrangeiro, caso parte do processo seja realizado no Brasil. Importante mencionar que a LGPD foi elaborada para proteção de dados que identifiquem uma pessoa natural, e não informações sigilosas de empresas ou negócios;

Log: processo de registro de eventos relevantes num sistema computacional;

Malware: é um termo genérico para qualquer tipo de "malicious software" ("software malicioso") projetado para se infiltrar em dispositivos eletrônicos sem o devido conhecimento do usuário. Existem muitos tipos de malware, e cada um funciona de maneira diferente na busca de seus objetivos;

Manifestação inequívoca: não pode haver dúvidas sobre a manifestação do consentimento do titular, ou seja, deve existir a certeza de que o titular consentiu com o tratamento dos seus dados pessoais;

Manifestação informada: antes de dar o consentimento, o titular deverá ter acesso prévio, completo e detalhado sobre o tratamento de seus dados pessoais, incluindo sua natureza, objetivos, métodos, duração, justificativa, finalidades, risco, responsabilidades dos agentes de tratamento e benefícios antes de proferir o Consentimento;

Manifestação livre: a manifestação do consentimento deve partir do titular sem que haja qualquer tipo de pressão ou direcionamento;

Operador: é toda pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador;

Pessoa natural: todos os seres humanos, independentemente de sexo, etnia, idade, orientação sexual, religião, nacionalidade, filiação partidária ou quaisquer outras características, possuindo direitos e obrigações;

Phishing: é uma técnica de engenharia social usada para enganar usuários de internet usando fraude eletrônica para obter informações confidenciais, como nome de usuário, senha e detalhes do cartão de crédito;

Pseudonimização: é a substituição de informação encontrável por identificadores artificiais, cifragem, codificação de mensagens e outros, sendo que o controlador mantém a informação em local separado;

Porta: uma porta de conexão está sempre associada a um endereço IP de um host e ao tipo de protocolo de transporte utilizado para a comunicação. Exemplo: o servidor de e-mail que executa um serviço de SMTP usa a porta 25 do protocolo TCP;

Privacy by default (privacidade por padrão): significa assegurar que são colocados em prática, dentro de uma organização, mecanismos para garantir que, por padrão, apenas será recolhida/coletada, utilizada e conservada, para cada atividade, a quantidade necessária de dados pessoais;

Privacy by design (privacidade desde a concepção): significa levar o risco de privacidade em conta em todo o processo de concepção de um novo produto ou serviço;

Relatório de impacto à proteção de dados pessoais (RIPD): quando o tratamento de dados puder gerar riscos à liberdade civil e aos direitos fundamentais do titular, o controlador deverá elaborar uma documentação contendo a descrição dos processos de tratamento de dados pessoais;

Ransomware: é um tipo de malware de sequestro de dados, feito por meio de criptografia, que usa como refém arquivos pessoais da própria vítima e cobra resgate para restabelecer o acesso a estes arquivos. O resgate é cobrado em criptomoedas, que, na prática, o torna quase impossível de se rastrear o criminoso.

Scripts: conjunto de instruções para que uma função seja executada em determinado aplicativo;

Sistemas: hardware, software, network de dados, armazenador de mídias e demais sistemas usados, adquiridos, desenvolvidos, acessados, controlados, cedidos ou operados pelo DETRAN RJ para dar suporte na execução de suas atividades;

Sniffing: corresponde ao roubo ou interceptação de dados capturando o tráfego de rede usando um sniffer (aplicativo destinado a capturar pacotes de rede);

Spam: termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas;

Spyware: programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros;

Titular de dados pessoais: a pessoa natural a quem pertence o dado pessoal;

Transferência internacional: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;

Tratamento: qualquer operação ou conjunto de operações efetuadas sobre os dados, por meios automatizados ou não, incluindo, mas não se limitando, a coleta, gravação, organização, estruturação, alteração, uso, acesso, divulgação, cópia, transferência, armazenamento, exclusão, combinação, restrição, adaptação, recuperação, consulta, destruição ou anonimização;

Trojan (Cavalo de Troia): programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário;

Vazamento de dados: qualquer quebra de sigilo ou vazamento de dados que possa resultar, criminosamente ou não, na perda, alteração, compartilhamento, acesso, transmissão, armazenamento ou processamento de dados não autorizado;

Violação de privacidade: qualquer violação à legislação aplicável ou conduta e evento que resulte na destruição acidental ou ilícita dos dados, bem como sua perda, roubo, alteração, divulgação ou acesso não autorizado, danos ou desvio de finalidade em seu tratamento;

Vírus: programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos;

Worm: programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador.

ATORES E RESPONSABILIDADES

Comitê de Implantação do Programa Governança em Privacidade (COMPGP): comitê de caráter consultivo, multisetorial, de apoio técnico-jurídico, com a finalidade de formular e conduzir princípios, diretrizes e estratégias para a gestão da segurança da informação e da proteção e privacidade de dados pessoais no âmbito do DETRAN RJ. Instituído pela PORTARIA DETRAN SEI N.º 6636 DE 26 DE junho DE 2024.

Encarregado pelo Tratamento de Dados Pessoais ou Data Privacy Officer (DPO): pessoa indicada pelo controlador atuar como canal de comunicação entre a instituição, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Designado pela PORTARIA DETRAN SEI N.º 6621 DE 29 DE maio DE 2024.

Gestor de Segurança da Informação (GSI): pessoa designada pela alta administração como responsável pelas ações de segurança da informação no âmbito do órgão. No DETRAN RJ, instituído pela PORTARIA DETRAN SEI N.º 6800/2025.

Responsável pelo Tratamento e Resposta a Incidentes (RTRI): responsável por receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança na rede computacional do DETRAN RJ, conforme PORTARIA DETRAN SEI N.º 6800/2025.

Comitê Gestor de Tecnologia da Informação e Comunicações (COMGTIC): responsável por zelar pela adequada execução dos processos de gestão de Tecnologia da Informação e Comunicação estabelecidos no âmbito do DETRAN RJ, de acordo com PORTARIA PRES DETRAN N.º 5697/2019.

INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

1.O que é um incidente de segurança e um vazamento de dados pessoais?

Considerando as definições da LGPD, um incidente de segurança é um acontecimento indesejado ou inesperado, hábil a comprometer a segurança dos dados pessoais, de modo a expô-los a acessos não autorizados e a situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Vazamento de dados é um tipo de incidente de segurança que se refere especificamente à situação em que informações privadas e sigilosas são expostas publicamente ou a terceiros sem autorização.

Dessa forma, as informações podem ser acessadas, visualizadas, copiadas, vendidas, compradas e usadas para golpes financeiros, extorsões e tentativas de prejudicar as atividades e a imagem do Órgão, colocando pessoas e organização em risco.

2. Onde, quando e de que forma podem ocorrer vazamentos de dados?

De acordo com estudos realizados no ano de 2023 sobre o tema pela IBM em diversos países, incluindo o Brasil, observam-se os seguintes percentuais em relação à ocorrência de vazamento de dados:

- Cerca de 80% envolvem perda ou roubo de dados pessoais de usuários dos serviços;
- 32% referem-se à propriedade intelectual;
- 24% a dados anonimizados de usuários;
- 23% a dados corporativos em geral e 21% a dados pessoais de colaboradores.

No Brasil, as principais causas de vazamento de dados se referem a:

- 47% ataques maliciosos;
- 28% erros de sistema;
- 25% erro humano.

Dentre os ataques maliciosos estão ameaças como malwares comuns e ransomwares, focados em sequestrar dados e exigir o pagamento de resgate.

Sendo identificados como os principais fatores que permitiram que elas fossem executadas:

- Credenciais roubadas ou comprometidas;
- Falhas na configuração de infraestrutura em nuvem;
- Vulnerabilidades em softwares de terceiros e
- Phishing.

3. Como evitar um vazamento de dados?

Para evitar a ocorrência de vazamentos de dados é necessário que a Instituição adote as seguintes recomendações relacionadas à Segurança da Informação:

- Investimento em ferramentas de prevenção contra ameaças, como firewall, antivírus corporativo (antiransomware), e-mail gateway e SIEM (Security Information and Event Management, ou Gestão de Informações e Eventos de Segurança);
- Manutenção de sistemas e softwares sempre atualizados;
- Estabelecimento de políticas e ferramentas de autenticação e controle de acesso;
- Garantia de segurança do acesso físico ao ambiente de TI;
- Realização de análises de vulnerabilidade frequentemente;
- Atenção às configurações de segurança de ambientes em nuvem;
- Atenção à Política de Segurança da Informação da organização;
- Promoção de campanhas de conscientização e treinamento de servidores e colaboradores, ensinando-os a reconhecer as principais ameaças, como phishing;

4.Quais as consequências de um vazamento de dados para o Órgão?

Vazamento de dados podem acarretar diversas consequências, tais como:

- Sanções administrativas, como multas;
- Perdas financeiras por conta de negócios cancelados, fuga de investidores e vazamento de informações sensíveis à instituição;
- Quebra de confiança na relação com o usuário de serviços e com os titulares de dados em geral;
- Danos de reputação e imagem;
- Ações judiciais individuais e coletivas por parte dos titulares de dados e de entidades de defesa do consumidor.

De acordo com determinação prevista no artigo 42 da LGPD, caso o usuário sofra algum dano como consequência do vazamento dos seus dados pessoais, ele pode acionar judicialmente o Órgão para garantir uma reparação.

"Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo."

Se o titular sofreu um dano moral ou material por conta de um vazamento de dados, o recomendado é que ele entre em contato com o Órgão e busque uma reparação amigável.

Caso o contato seja infrutífero, o titular pode acionar a instituição judicialmente para garantir os seus direitos.

5.Quem responde legalmente caso ocorra um vazamento de dados?

Cabe destacar que a LGPD se refere apenas ao tratamento de dados pessoais, ou seja, a dados que identifiquem uma pessoa ou que, quando associados a outros dados, permitam identificar uma pessoa.

A Lei recomenda, em seu artigo 46, que os agentes de tratamento adotem medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais. Isso inclui protegê-los de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Caso essas medidas não sejam adotadas e isso leve à uma violação da segurança dos dados, o controlador ou o operador terão que responder pelos danos causados.

"Art.44(...)
Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano."

Contudo, os agentes de tratamento não serão responsabilizados caso consigam provar que:

- Não realizaram o tratamento de dados pessoais que lhes é atribuído;
- Embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
- O dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

PROCESSO DE NOTIFICAÇÃO E TRATAMENTO DO INCIDENTE

Apresentam-se a seguir as etapas do processo de notificação e tratamento do incidente com dados pessoais:

IDENTIFICAÇÃO DO INCIDENTE

Um incidente com dados pessoais pode ser notificado ao Comitê de Implantação do Programa Governança em Privacidade - COMPGP e ao Encarregado pelo Tratamento de Dados Pessoais por meio de e-mail ou processo SEI.

Apresentam-se a seguir as etapas do processo de notificação e tratamento do incidente com dados pessoais:

Confirmação da ocorrência do incidente

Recebida a notificação, o Comitê de Implantação do Programa Governança em Privacidade - COMPGP, com o apoio do Comitê Gestor de Tecnologia da Informação e Comunicações - COMGTIC, deverá imediatamente identificar os dados vinculados ao incidente, analisando cautelosa e detalhadamente, todas as informações envolvidas no episódio, a fim de:

1. Confirmar se os dados compõem ou não a base de dados do DETRAN RJ;

2. Verificar se os dados do incidente são ou não caracterizados como dados pessoais, relacionados à pessoa natural identificada ou identificável, de acordo com o art. 5º, I, LGPD;

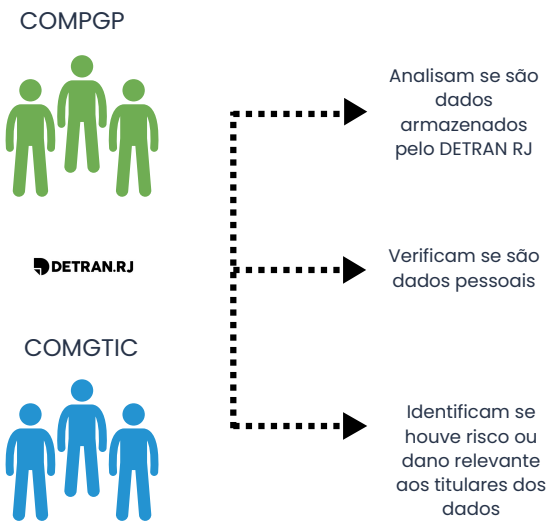
3. Identificar se houve algum tipo de tratamento dos dados pessoais, que acarrete risco ou dano relevante aos titulares dos dados, como, por exemplo:

- A invasão dos sistemas utilizados pelo Sistema de Identificação Civil por um agente malicioso que realize a cópia não autorizada da base de dados contendo dados pessoais de cidadãos, tais como nome, CPF, telefone, endereço, etc.

- A indisponibilidade prolongada do sistema RENACH, RENAVAM, ou CFC em razão de um incidente de sequestro de dados, impedindo o acesso aos dados ou a realização de procedimentos, pode expor dados pessoais sensíveis dos titulares e causar-lhes riscos de fraudes e danos materiais;

- A perda ou roubo de documentos ou dispositivos de armazenamento de dados que contenham dados pessoais protegidos por sigilo profissional, cópia de documentos de identificação oficial e dados de contato dos titulares pode expô-los a riscos reputacionais e de sofrer fraudes financeiras.

Processo de Confirmação da ocorrência do incidente



Tratamento de resposta ao incidente:

1.Avaliação do incidente

Após identificação da ocorrência ou suspeita do incidente, o Comitê de Implantação do Programa Governança em Privacidade - COMPGP, juntamente com a Comitê Gestor de Tecnologia da Informação e Comunicações - COMGTIC, deverá iniciar a avaliação do incidente para a apuração da gravidade dos dados envolvidos. O documento, específico e direcionado à sinalização de criticidade e gravidade do evento, permitirá que o DETRAN-RJ entenda melhor os riscos aos quais está sujeito, possibilitando uma melhor compreensão do tratamento que deverá dar à comunicação com os titulares dos dados vazados e às autoridades competentes.

A avaliação deverá identificar:

1. O contexto da atividade de tratamento de dados;

2. A classificação do incidente:

- Conteúdo abusivo: spam, assédio, etc.;
- Código malicioso: bot, worm, vírus, trojan, spyware, scripts;
- Prospecção por informações: varredura, sniffing, engenharia social;
- Tentativa de intrusão: tentativa de exploração de vulnerabilidades, tentativa de acesso lógico;

- Intrusão: acesso lógico indesejável, comprometimento de conta de usuário, de aplicação;

- Indisponibilidade de serviço ou informação: negação de serviço, sabotagem;

- Segurança da informação: acesso não-autorizado à informação, modificação não autorizada da informação;

- Fraude: violação de direitos autorais, fingir ou falsificar identidade pessoal ou institucional, uso de recursos de forma não-autorizada;

- Outros: incidente especificamente categorizado.

3. As categorias e quantidades de titulares afetados;

4. Os tipos e quantidade de dados violados;

5. Os potenciais danos materiais, morais, reputacionais causados aos titulares;

6. Se os dados violados estavam protegidos de forma a impossibilitar a identificação de seus titulares;

7. As medidas de mitigação adotadas após o incidente.

Em função da combinação desses critérios, realizar a classificação de criticidade do incidente de acordo com as definições a seguir:

- ALTA (impacto grave): incidente que afeta sistemas relevantes ou informações críticas, com potencial para gerar impacto negativo sobre o DETRAN RJ;

- MÉDIA (impacto significativo): incidente que afeta sistemas ou informações não críticas, sem impacto negativo ao DETRAN RJ;

- BAIXA (impacto mínimo): possível incidente, sistemas não críticos; investigações de incidentes ou de colaboradores; investigações de longo prazo envolvendo pesquisa extensa e/ou trabalho forense detalhado.

2. Preenchimento do Formulário de Comunicação de Incidente de Segurança com Dados Pessoais

Em seguida, o Comitê de Implementação do Programa de Governança em Privacidade (COMPGP) juntamente com o Comitê Gestor de Tecnologia da Informação e Comunicações (COMGTIC), realizarão o preenchimento do Formulário de Comunicação de Incidente de Segurança com Dados Pessoais, a fim de demonstrar a coleta de evidências técnicas necessárias à formatação de prova sobre o incidente, apontar eventuais falhas de segurança que permitiram ou contribuíram com a ocorrência do incidente e direcionar as correções necessárias, fundamentais para que o DETRAN RJ evolua em relação às boas práticas de governança em privacidade.

3.Criação do plano de comunicação do incidente

Adicionalmente, a COMPGP providenciará, em parceria com a Comitê Gestor de Tecnologia da Informação e Comunicações - COMGTIC, a elaboração de um plano de comunicação do incidente, composto de documentos a serem enviados à ANPD, aos titulares de dados e à imprensa, caso necessário.

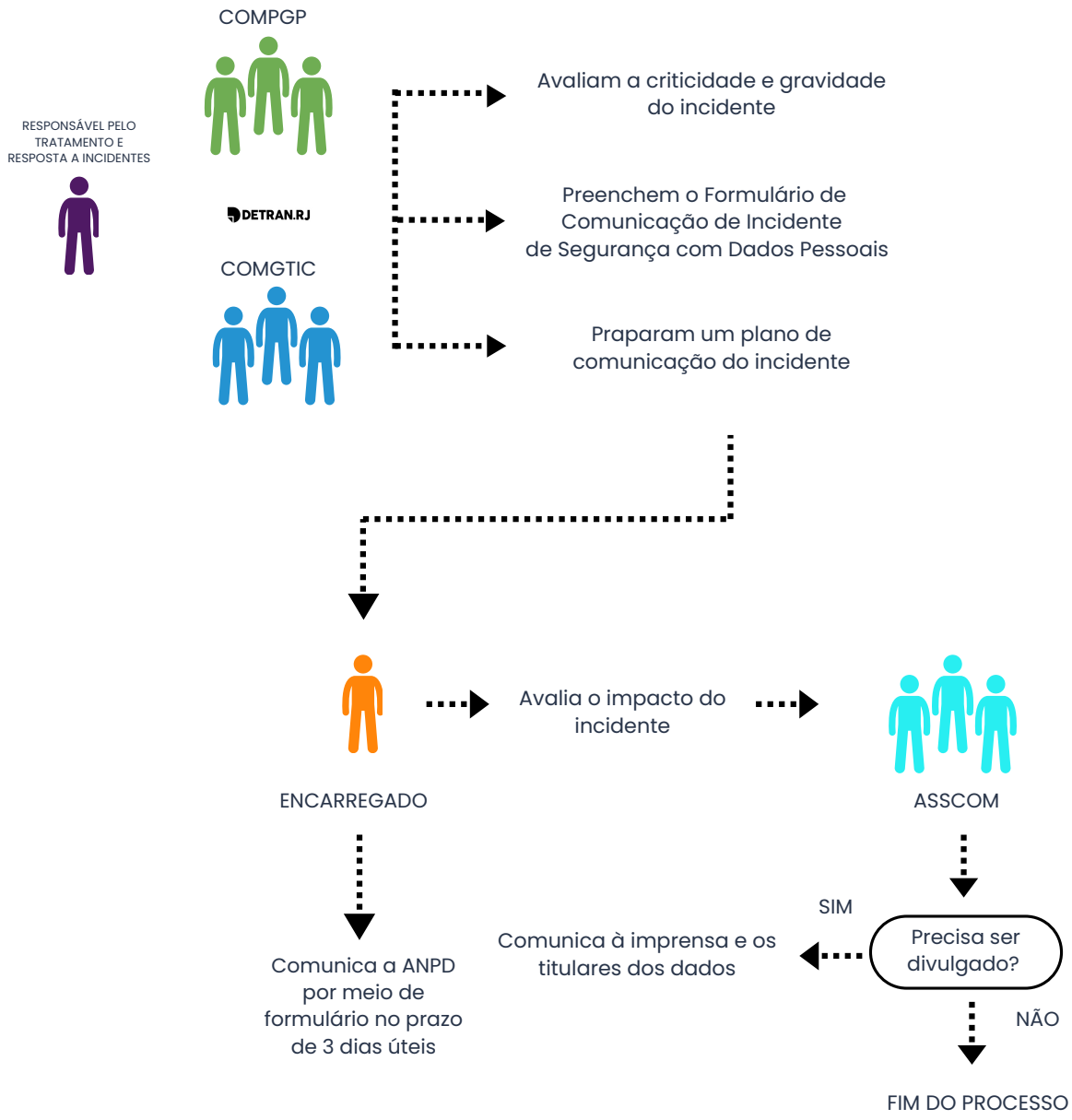
Notificação do incidente

Em atenção às disposições normativas que versam sobre a comunicação do incidente, sob pena de aplicação de sanções em face do Órgão pela ANPD, visando preservar os direitos dos titulares e tentar diminuir os possíveis prejuízos que um incidente de segurança possa causar, observando o prazo recomendado de 3 (três) dias úteis da ciência do fato, o DETRAN RJ providenciará a comunicação do incidente de segurança, nos seguintes termos:

Para quem?	Quem?	Como?
ANPD	Encarregado	Por meio do preenchimento do formulário disponibilizado para ser protocolado por peticionamento eletrônico no sistema SUPER da ANPD (https://www.gov.br/anpd/pt-br/canais_atendimento/peticionamento-eletronico-anpd)
Imprensa	ASSCOM	Através de canais já habitualmente utilizados pelo DETRAN RJ para se comunicar com a imprensa

Para quem?	Quem?	Como?
Titular de Dados	ASSCOM	De forma individual e diretamente aos titulares, sempre que possível. Por meio de e-mail, carta ou mensagem eletrônica ou através de outro canal já habitualmente utilizado pelo DETRAN RJ para se comunicar com o titular. Caso não seja possível individualizar os titulares afetados, a comunicação deverá ser direcionadas a todos cujos dados estejam presentes na base de dados violada. Excepcionalmente, e de forma justificada, pode ser feita a comunicação indireta por meio de publicação em meios de comunicação. O meio utilizado deve ser capaz de alcançar o maior número possível de titulares, e deve ser dado o devido destaque à divulgação. O comunicado deve fazer uso de linguagem clara e conter as seguintes informações: • a descrição da natureza e da categoria de dados pessoais afetados; • as medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; • os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares; • os motivos da demora, no caso de a comunicação não ter sido feita no prazo de 3 (três) dias úteis; • as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente, quando cabíveis; • a data do conhecimento do incidente de segurança; e o contato para obtenção de informações e, quando aplicável, os dados de contato do encarregado (e-mail: encarregado@detran.rj.gov.br).

Processo de tratamento de resposta e notificação do incidente



Elaboração de relatório final de ação, prevenção e aprendizado

Esta última etapa visa registrar a ocorrência do incidente e as providências adotadas, a partir da elaboração de um relatório técnico final de ação, detalhando os resultados identificados, a fim de que o DETRAN-RJ adote as medidas necessárias para a prevenção de novos episódios envolvendo vulnerabilidades tecnológicas.

Esse documento tem como objetivos:

- Avaliar o processo de tratamento do incidente e verificar a eficácia das soluções adotadas;

- Relacionar e documentar as falhas e os recursos inexistentes ou insuficientes, para que sejam providenciados em futuras ocasiões;

- Compartilhar as lições aprendidas, com outros atores se necessário, com o objetivo de discutir erros e dificuldades encontradas na atenuação do evento ocorrido, propor melhoria na infraestrutura computacional e nos processos de resposta a incidentes;

- Comunicar a área de negócio afetada sobre as decisões tomadas para prevenção de incidentes da mesma natureza, buscando implementar melhorias na infraestrutura de segurança; e

- Realizar os ajustes necessários no Programa de Governança em Privacidade e Proteção de Dados Pessoais - PGPPDP.

Processo de elaboração de relatório final de ação, prevenção e aprendizado

DETRAN.RJ	**Formulário de Comunicação de Incidente de Segurança com Dados Pessoais**

Dados do Controlador			
Razão Social / Nome:			
CNPJ/CPF:			
Endereço:			
Cidade:		Estado:	
CEP:			
Telefone:		E-mail:	
Declara ser Microempresa ou Empresa de Pequeno Porte:		☐ Sim	☐ Não
Declara ser Agente de Tratamento de Pequeno Porte[1]:		☐ Sim	☐ Não
Informe o número aproximado de titulares cujos dados são tratados por sua organização:			

Dados do Encarregado			
Possui um encarregado pela proteção de dados pessoais?		☐ Sim	☐ Não
Nome:			
CNPJ/CPF:			
Telefone:		E-mail:	

Dados do Notificante / Representante Legal	
☐ O próprio encarregado pela proteção de dados.	
☐ Outros (especifique):	
Nome:	
CNPJ/CPF:	
Telefone:	
E-mail:	

A documentação comprobatória da legitimidade para representação do controlador junto à ANPD deve ser protocolada em conjunto com o formulário de comunicação de incidente.

- *Encarregado*: ato de designação/nomeação/procuração.
- *Representante*: contrato social e procuração, se cabível.

[1] Nos termos do REGULAMENTO DE APLICAÇÃO DA LEI Nº 13.709, DE 14 DE AGOSTO DE 2018, aprovado pela RESOLUÇÃO CD/ANPD Nº 2, DE 27 DE JANEIRO DE 2022. (https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019)

Tipo de Comunicação	
☐ Completa	*Todas as informações a respeito do incidente estão disponíveis e* ***a comunicação aos titulares já foi realizada****.*
☐ Preliminar	*Nem todas as informações sobre o incidente estão disponíveis, justificadamente, ou a* ***comunicação aos titulares ainda não foi realizada****.* *A complementação deverá ser encaminhada no prazo de* ***20 dias úteis*** *a contar da data da comunicação* – Art. 6º § 3º do Regulamento de Comunicação de Incidentes.
☐ Complementar	*Complementação de informações prestadas em comunicação preliminar.*

A comunicação complementar deve ser protocolada no mesmo processo que a comunicação preliminar.

- A comunicação preliminar é insuficiente para o cumprimento da obrigação estabelecida pelo art. 48 da LGPD e deve ser complementada pelo controlador no prazo estabelecido.

Avaliação do Risco do Incidente

☐ O incidente de segurança pode acarretar risco ou dano relevante aos titulares.

☐ O incidente não acarretou risco ou dano relevante aos titulares. **(Comunicação Complementar)**

☐ O risco do incidente aos titulares ainda está sendo apurado. **(Comunicação Preliminar)**

Justifique, se cabível, a avaliação do risco do incidente:

Da Ciência da Ocorrência do Incidente

Por qual meio se tomou conhecimento do incidente?

☐ Identificado pelo próprio controlador.	☐ Notificação do operador de dados.	☐ Denúncia de titulares/terceiros.
☐ Notícias ou redes sociais.	☐ Notificação da ANPD.	☐ Outros. (especifique)

Descreva, resumidamente, de que forma a ocorrência do incidente foi conhecida:

Caso o incidente tenha sido comunicado ao controlador por um operador, informe:

Dados do Operador

Razão Social / Nome:	
CNPJ/CPF:	
E-mail:	

Cabe ao controlador solicitar ao operador as informações necessárias à comunicação do incidente.

Da Tempestividade da Comunicação do Incidente	
Informe as seguintes datas, sobre o incidente:	
Quando ocorreu	
Quando tomou ciência	
Quando comunicou à ANPD	
Quando comunicou aos titulares	
Justifique, se cabível, a não realização da comunicação à ANPD e aos titulares de dados afetados no prazo de 3 (três) dias úteis conforme prevê o Art. 6º da Resolução CD/ANPD nº 15, de 24 de abril de 2024 que aprova o Regulamento de Comunicação de Incidente de Segurança.	
Se cabível, informe quando e a quais outras autoridades o incidente foi comunicado:	

Da Comunicação do Incidente aos Titulares dos Dados	
Os titulares dos dados afetados foram comunicados sobre o incidente?	
☐ Sim.	☐ Não, por não haver risco ou dano relevante a eles.
☐ Não, mas o processo de comunicação está em andamento.	☐ Não, vez que o risco do incidente ainda está sendo apurado. (**comunicação preliminar**)
Se cabível, quando os titulares serão comunicados sobre o incidente?	
De que forma a ocorrência do incidente foi comunicada aos titulares?	
☐ Comunicado individual por escrito. *(mensagem eletrônica / carta / e-mail / etc.)*	☐ Anúncio público no sítio eletrônico, mídias sociais ou aplicativos do controlador.
☐ Comunicado individual por escrito com confirmação de recebimento. *(mensagem eletrônica / carta / e-mail / etc.)*	☐ Ampla divulgação do fato em meios de comunicação, por iniciativa do controlador. (*especifique abaixo*)
☐ Outros. (*especifique abaixo*)	☐ Não se aplica.
Descreva como ocorreu a comunicação:	
Quantos titulares foram comunicados individualmente sobre o incidente?	
Justifique, se cabível, o que motivou a não realização da comunicação individual aos titulares:	

O comunicado aos titulares deve utilizar linguagem clara e conter, ao menos, as seguintes informações:

1. resumo e data de ocorrência do incidente;
2. descrição dos dados pessoais afetados;
3. riscos e consequências aos titulares de dados;
4. medidas tomadas e recomendadas par mitigar seus efeitos, se cabíveis;
5. dados de contato do controlador para obtenção de informações adicionais sobre o incidente.

O comunicado aos titulares atendeu os requisitos acima?	
☐ Sim	☐ Não

- Se não atendidos os requisitos, o comunicado aos titulares deverá ser devidamente retificado.
- Poderá ser solicitada pela ANPD, a qualquer tempo, cópia do comunicado aos titulares para fins de fiscalização.

Descrição do Incidente

Qual o tipo de incidente? (Informe o tipo mais específico)	
☐ Sequestro de Dados (*ransomware*) sem transferência de informações.	☐ Sequestro de dados (*ransomware*) com transferência e/ou publicação de informações.
☐ Exploração de vulnerabilidade em sistemas de informação.	☐ Vírus de Computador / *Malware*.
☐ Roubo de credenciais / Engenharia Social.	☐ Violação de credencial por força bruta.
☐ Publicação não intencional de dados pessoais.	☐ Divulgação indevida de dados pessoais.
☐ Envio de dados a destinatário incorreto.	☐ Acesso não autorizado a sistemas de informação.
☐ Negação de Serviço (DoS).	☐ Alteração/exclusão não autorizada de dados.
☐ Perda/roubo de documentos ou dispositivos eletrônicos.	☐ Descarte incorreto de documentos ou dispositivos eletrônicos.
☐ Falha em equipamento (hardware).	☐ Falha em sistema de informação (*software*).
☐ Outro tipo de incidente cibernético. (especifique abaixo)	☐ Outro tipo de incidente não cibernético. (especifique abaixo)

Descreva, resumidamente, como ocorreu o incidente:

Explique, resumidamente, por que o incidente ocorreu (identifique a causa raiz, se conhecida):

Que medidas foram adotadas para corrigir as causas do incidente?

Impactos do Incidente Sobre os Dados Pessoais

De que forma o incidente afetou os dados pessoais (admite mais de uma marcação):

☐ Confidencialidade	Houve acesso não autorizado aos dados, violando seu sigilo.
☐ Integridade	Houve alteração ou destruição de dados de maneira não autorizada ou acidental.
☐ Disponibilidade	Houve perda ou dificuldade de acesso aos dados por período significativo.

Se aplicável, quais os tipos de dados pessoais sensíveis foram violados? (admite mais de uma marcação)

☐Origem racial ou étnica. ☐Convicção religiosa. ☐Opinião política.
☐Referente à saúde. ☐Biométrico. ☐Genético.
☐Referente à vida sexual. ☐Filiação a organização sindical, religiosa, filosófica ou política.

Se aplicável, descreva os tipos de dados pessoais sensíveis violados:

Quais os demais tipos de dados pessoais violados? (admite mais de uma marcação)

☐ Dados básicos de identificação *(ex: nome, sobrenome, data de nascimento, matrícula)*	☐ Número de documentos de identificação oficial. *(ex: RG, CPF, CNH, passaporte)*	☐ Dados de contato. (*ex: telefone, endereço, e-mail*)
☐ Dados de meios de pagamento. *(ex: cartão de crédito/débito)*	☐ Cópias de documentos de identificação oficial.	☐ Dados protegidos por sigilo profissional/legal.
☐ Dado financeiro ou econômico.	☐ Nomes de usuário de sistemas de informação.	☐ Dado de autenticação de sistema. (*ex: senhas, PIN ou tokens)*
☐ Imagens / Áudio / Vídeo	☐ Dado de geolocalização. *(ex: coordenadas geográficas)*	☐ Outros (especifique abaixo)

Descreva os tipos de dados pessoais não sensíveis violados:

Riscos e Consequências aos Titulares dos Dados

Foi elaborado um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) das atividades de tratamento afetadas pelo incidente?

☐ Sim ☐ Não

Qual o número total de titulares cujos dados são tratados nas atividades afetadas pelo incidente?	
Qual a quantidade aproximada de titulares afetados[2] pelo incidente?	
Total de titulares afetados	
Crianças e/ou adolescentes	
Outros titulares vulneráveis	
Se aplicável, descreva as categorias de titulares vulneráveis afetados:	

Quais a categorias de titulares foram afetadas pelo incidente? (admite mais de uma marcação)		
☐ Funcionários.	☐Prestadores de serviços.	☐ Estudantes/Alunos.
☐ Clientes/Cidadãos.	☐ Usuários.	☐ Inscritos/Filiados.
☐ Pacientes de serviço de saúde.	☐Ainda não identificadas.	☐ Outros. (especifique abaixo)
Informe o quantitativo de titulares afetados, por categoria:		

Quais as prováveis consequências do incidente para os titulares? (admite mais de uma marcação)		
☐ Danos morais.	☐ Danos materiais.	☐ Violação à integridade física
☐ Discriminação social.	☐ Danos reputacionais.	☐ Roubo de identidade.
☐ Engenharia social / Fraudes.	☐ Limitação de acesso a um serviço.	☐ Exposição de dados protegidos por sigilo profissional/legal.
☐ Restrições de direitos.	☐ Perda de acesso a dados pessoais.	☐ Outros (especifique abaixo).
Se cabível, descreva as prováveis consequências do incidente para cada grupo de titulares:		

Qual o provável impacto do incidente sobre os titulares? (admite só uma marcação)
☐ Podem não sofrer danos, sofrer danos negligenciáveis ou superáveis sem dificuldade.
☐ Podem sofrer danos, superáveis com certa dificuldade.
☐ Podem sofrer danos importantes, superáveis com muita dificuldade.
☐ Podem sofrer lesão ou ofensa a direitos ou interesses difusos, coletivos ou individuais, que, dadas as circunstâncias, ocasionam ou tem potencial para ocasionar dano significativo ou irreversível.

[2] Titular afetado é aquele cujos dados podem ter tido a confidencialidade, integridade ou disponibilidade violadas e que ficará exposto a novos riscos relevantes em razão do incidente.

Se cabível, quais medidas foram adotadas para mitigação dos riscos causados pelo incidente aos titulares?

Medidas de Segurança Técnicas e Administrativas para a Proteção dos Dados Pessoais

Os dados violados estavam protegidos de forma a impossibilitar a identificação de seus titulares?

☐ Sim, integralmente protegidos por criptografia / pseudonimização. ☐ Sim, parcialmente protegidos por criptografia / pseudonimização. ☐ Não.

Descreva os meios utilizados para proteger a identidade dos titulares, e a quais tipos dados foram aplicados:

Antes do incidente, quais das seguintes medidas de segurança eram adotadas? (admite mais de uma marcação)

☐ Políticas de segurança da informação e privacidade.	☐ Processo de Gestão de Riscos.	☐ Registro de incidentes.
☐ Controle de acesso físico.	☐ Controle de acesso lógico.	☐ Segregação de rede.
☐ Criptografia/Anonimização.	☐ Cópias de segurança. (*backups*)	☐ Gestão de ativos.
☐ Antivírus.	☐ Firewall.	☐ Atualização de Sistemas.
☐ Registros de acesso (logs).	☐ Monitoramento de uso de rede e sistemas.	☐ Múltiplos fatores de autenticação.
☐ Testes de invasão.	☐ Plano de resposta a incidentes.	☐ Outras (especifique).

Descreva as demais medidas de segurança técnicas e administrativas adotadas antes do incidente:

Após o incidente, foi adotada alguma nova medida de segurança? (admite mais de uma marcação)

☐ Políticas de segurança da informação e privacidade.	☐ Processo de Gestão de Riscos.	☐ Registro de incidentes.
☐ Controle de acesso físico.	☐ Controle de acesso lógico.	☐ Segregação de rede.
☐ Criptografia/Anonimização.	☐ Cópias de segurança. (*backups*)	☐ Gestão de ativos.
☐ Antivírus.	☐ Firewall.	☐ Atualização de Sistemas.
☐ Registros de acesso (logs).	☐ Monitoramento de uso de rede e sistemas.	☐ Múltiplos fatores de autenticação.
☐ Testes de invasão.	☐ Plano de resposta a incidentes.	☐ Outras (especifique).

Se cabível, descreva as medidas de segurança adicionais adotadas após o incidente:	
As atividades de tratamento de dados afetadas estão submetidas a regulações de segurança setoriais?	
☐ Sim	☐ Não
Se cabível, indique as regulamentações setoriais de segurança aplicáveis às atividades de tratamento de dados afetadas pelo incidente:	

Declaro, sob as penas da lei, serem verdadeiras as informações prestadas acima.

<ASSINATURA>