Tribunal Regional do Trabalho
da 15ª Região

PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA

2023

ASSESSORIA DE GESTÃO ESTRATÉGICA

JUSTIÇA DO TRABALHO
Tribunal Regional do Trabalho da 15ª Região (Campinas)

SUMÁRIO

INTRODUÇÃO

Escândalos de vazamentos de dados e de ataques cibernéticos tornaram-se comuns atualmente e são provenientes de meios cada vez mais sofisticados para burlarem os controles e medidas de segurança da informação.

Considerando o volume de dados que o Tribunal Regional do Trabalho da 15ª Região trata e a relevância de seu papel institucional na entrega de serviços públicos, é importante que o órgão esteja consciente de que incidentes de segurança revestem-se de uma realidade possível, os quais devem ser evitados com medidas de salvaguarda e prevenção.

No entanto, é necessário também que o Tribunal 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).

Ademais, assim determina a LGPD (Lei Geral de Proteção de Dados):

> ***Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.***
> ***§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:***
> ***I - a descrição da natureza dos dados pessoais afetados;***
> ***II - as informações sobre os titulares envolvidos;***
> ***III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;***
> ***IV - os riscos relacionados ao incidente;***
> ***V - os motivos da demora, no caso de a comunicação não ter sido imediata; e***
> ***VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.***
> ***§ 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 de Resposta a Incidentes de Segurança** é apresentado pela Assessoria de Gestão Estratégica para conhecimento de todos os magistrados, servidores, terceirizados e demais colaboradores do TRT-15 e dispõe sobre as medidas que devam ser adotadas no caso de uma situação de emergência ou evento de risco que possam ocasionar danos aos ativos tecnológicos do Tribunal, viabilizando, inclusive, a comunicação apropriada e tempestiva à ANPD, quando for o caso.

OBJETIVOS

Com a implementação deste Plano, pretende-se alcançar o seguinte objetivo geral:

Orientar o TRT 15 nas respostas às situações de emergência e exceção, 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.

Além disso, busca-se atingir os seguintes objetivos 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.**

Esclarece-se que este Plano não aborda um tipo único ou específico de incidente. Todavia, estabelece etapas acionáveis, com linhas de comunicação, funções e notificações necessárias para responder a qualquer violação de segurança.

Cumpre informar que na hipótese de um incidente, não há tempo hábil para estudo de uma política complexa e detalhada para, então, agir.

TERMOS E DEFINIÇÕES

Para facilitar o entendimento na compreensão deste **Plano de Resposta a Incidentes de Segurança** são adotadas as seguintes definições:

- **Agentes de tratamento:** corresponde ao Controlador e 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;
- ***Bot*:** código malicioso o qual permite que o invasor controle remotamente o computador ou dispositivo que hospeda;
- **Controlador:** é toda pessoa física ou jurídica, de direito público ou privado, a quem competem decisões referentes ao tratamento de dados pessoais;
- **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;
- **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;

- **Encarregado 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*;

- ***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;

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

- **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;
- ***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 TRT 15 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;
- **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

Dentre os principais responsáveis, em caso de incidente de segurança envolvendo o tratamento de dados pessoais, identificam-se a seguir aqueles que atuarão diretamente no processo de trabalho descrito neste Plano. Cabe destacar que, em 8 de fevereiro de 2022, a Portaria nº 032/2022 do TRT-15 instituiu o Comitê Gestor de Crises do Tribunal Regional do Trabalho (CGC), o qual tem competência para atuar em situações que envolvam crises cibernéticas. Nessa mesma data, foi publicada a Portaria GP nº030/2022 tratando da Norma Técnica Complementar DGSI-GISI (Diretriz para Gestão de Segurança da Informação para Gestão de Incidentes de Segurança da Informação), para criação da Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR), no âmbito deste Regional.

- **Comitê Gestor de Crises do Tribunal Regional do Trabalho (CGC)**: comitê responsável por gerenciar as ações necessárias para o tratamento de crises cibernéticas, respaldar as ações da ETIR, atuar como porta-voz aos órgãos externos referente ao tratamento de crises cibernéticas entre outras competências.

- **Comitê de Governança de Segurança da Informação (CGSI)**: comitê responsável, dentre outras atribuições, por acompanhar os processos de segurança da informação e de proteção de dados pessoais (Ato Regulamentar GP nº 009/2021).

- **Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR)**: grupo de servidores com responsabilidade de receber, analisar e responder as notificações e atividades relacionadas a incidentes de segurança da informação em ambiente tecnológico (ANEXO ÚNICO - Portaria GP nº 030/2022).

INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

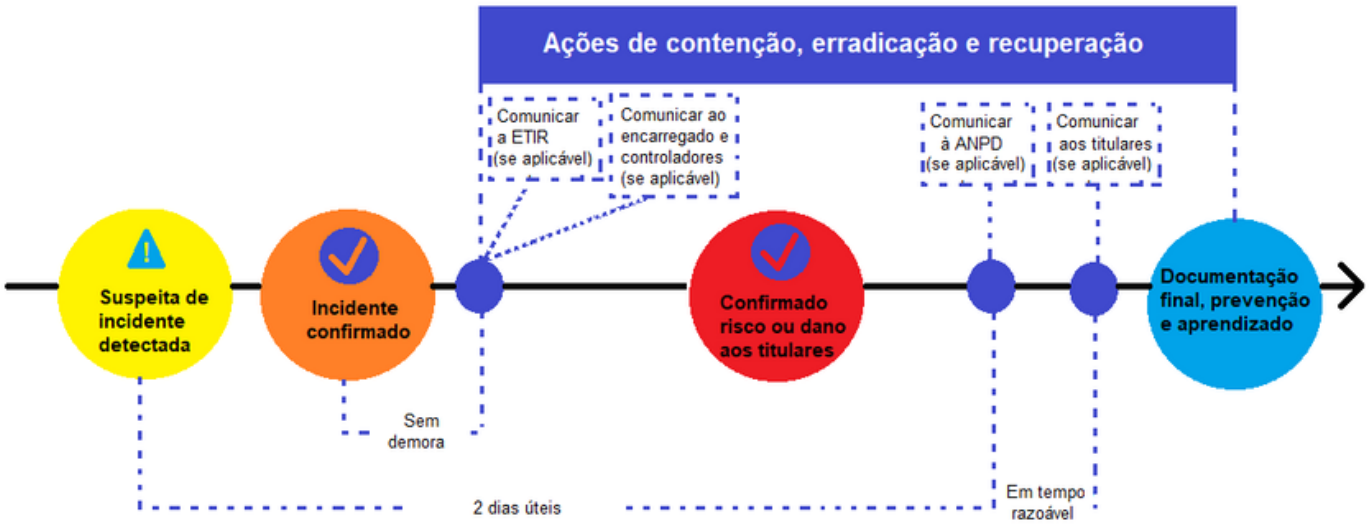
Conforme o art. 46 da LGPD, os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado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

Assim, em caso de incidente que coloque em risco a segurança de dados, recomenda-se a adoção dos seguintes procedimentos:

1. **Avaliar internamente o incidente** com o objetivo de obter informações iniciais sobre o impacto do evento; natureza, categoria e quantidade de titulares de dados **pessoais** afetados; categoria e quantidade de dados afetados, consequências do incidente para os titulares e a Corte Regional da 15ª Região, criticidade e probabilidade; além disso, é importante preservar todas as evidências do incidente.
2. **Comunicar ao Encarregado** do TRT 15 a existência do incidente, caso envolva dados pessoais (art. 5º, VIII da LGPD).
3. **Comunicar ao Controlador** (nos termos da LGPD) a existência do incidente, caso envolva dados pessoais.
4. **Comunicar à ANPD e ao titular de dados pessoais** a existência do incidente, em caso de risco ou dano relevante aos titulares (art. 48 da LGPD), mencionando no mínimo:
   a. a descrição da natureza dos dados pessoais afetados;
   b. as informações sobre os titulares envolvidos;
   c. a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
   d. os riscos relacionados ao incidente;
   e. os motivos da morosidade, no caso de a comunicação não ter sido imediata; e
   f. as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.
5. **Comunicar à ETIR do TRT 15** em caso de incidentes na rede computacional.
6. **Elaborar documentação** com todas as informações coletadas, as ações realizadas para o tratamento efetivo do incidente e as considerações necessárias para promover a melhoria contínua no atendimento de tais eventos, para atualizar o RIPD (Relatório de Impacto à Proteção dos Dados Pessoais) e para fins de cumprimento do princípio de responsabilização e prestação de contas (art. 6º, X da LGPD).

A figura abaixo detalha de forma simplificada este processo:

FLUXOGRAMA DA NOTIFICAÇÃO DE INCIDENTES COM DADOS PESSOAIS



O art. 48 da LGPD determina que o Controlador tem a obrigação de comunicar à ANPD e ao titular dos dados pessoais a ocorrência de incidente de segurança que venha a gerar risco ou dano considerado relevante aos titulares. Todavia, a ANPD afirma que, embora a responsabilidade e a obrigação pela comunicação do incidente sejam do Controlador, podem ocorrer casos excepcionais em que tal comunicação provenha do Operador, caso em que tal comunicação será devidamente analisada pela ANPD.

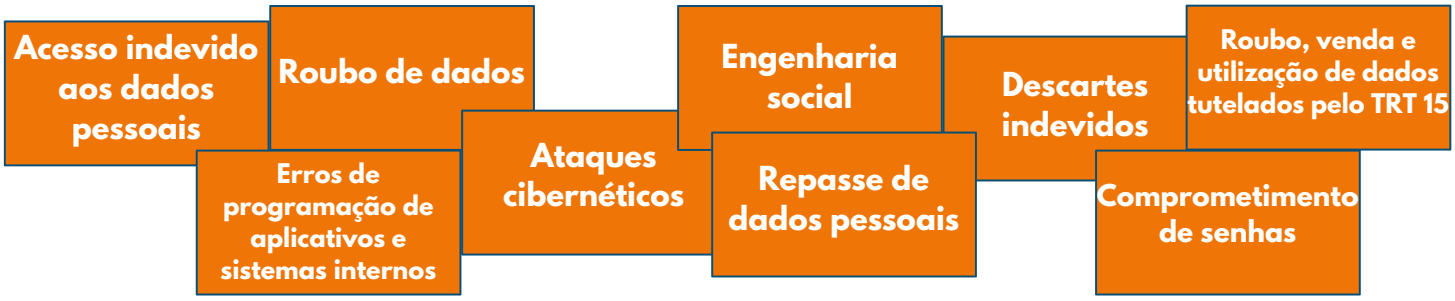
A Autoridade Nacional de Proteção de Dados recomenda ainda (enquanto pendente a regulamentação), conforme Decreto nº 9936/2019, que o prazo razoável para a comunicação de incidente seja de **dois dias úteis**. Reforça que os Controladores tenham cautela quanto ao julgamento acerca da relevância dos riscos e danos referentes ao incidente e, em caso de dúvida, realizem a comunicação do incidente o mais breve possível para que não ocorra eventual descumprimento da LGPD.

A seguir um detalhamento dos procedimentos (mencionados acima) a serem adotados em caso de possível incidente de segurança:

AVALIAR INTERNAMENTE O INCIDENTE

Quando for detectado um incidente de segurança no Tribunal, é necessário realizar uma avaliação interna, a fim de que sejam obtidas informações como:

a) Qual **vulnerabilidade** foi explorada no evento, abrangendo, entre outras, situações como:



b) **Fonte dos dados pessoais:** meio pelo qual foram obtidos os dados pessoais, tais como:

- **Preenchimento de formulário eletrônico ou não eletrônico por parte do titular**
- **API (*Application Programming Interface* ou Interface de Programação de Aplicação)**
- **Uso compartilhado de dados**
- **XML (*Extensible Markup Language*)**
- ***Cookies***

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

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

e) **Avaliação do impacto ao titular:** avaliar os impactos que o incidente pode gerar a entidade como perda de confiabilidade do cidadão, ações judiciais, dano à imagem do TRT 15 em âmbito nacional e internacional, prejuízo à Corte em contratos com fornecedores e clientes, e impacto total ou parcial nas atividades desenvolvidas pelo Tribunal.

A figura abaixo mostra as atividades da avaliação interna acima abordadas.

Reforça-se que nesta etapa deve ser preservado o máximo de evidências do incidente e de todas as medidas adotadas a partir de sua ciência, a fim de que se demonstre, para eventuais autoridades que posteriormente vierem a apurar os fatos, inteiramente a cadeia de diligências realizadas para entendimento do evento e mitigação dos seus efeitos.

COMUNICAR AO ENCARREGADO DO TRT 15

O conhecimento de um incidente por qualquer magistrado, servidor, colaborador, fornecedor ou parte interessada deve ensejar uma comunicação ao Encarregado, o mais breve possível, para as providências previstas na LGPD e no portal da ANPD sobre comunicação de incidentes de segurança.

COMUNICAR AO CONTROLADOR

O Operador deve comunicar incidentes com dados pessoais ao Controlador o mais breve possível, a fim de viabilizar que este exerça o seu papel tempestivamente. Conforme art. 48 da LGPD, é obrigação do Controlador comunicar incidentes com dados pessoais à ANPD e aos titulares de dados.

Recomenda-se que o Controlador adote posição de cautela, de modo que a comunicação seja efetuada mesmo nos casos em que houver dúvida sobre a relevância dos riscos e danos envolvidos. Ressalte-se, ainda, que eventual e comprovada subavaliação dos riscos e danos por parte do Controlador pode ser considerada descumprimento à legislação de proteção de dados pessoais.

Embora a responsabilidade e a obrigação pela comunicação à ANPD sejam do Controlador, caso excepcionalmente sejam apresentadas informações pelo Operador, serão devidamente analisadas pela ANPD.

COMUNICAR À ANPD E AO TITULAR DE DADOS PESSOAIS

A ANPD, enquanto pendente a regulamentação, estipula o prazo de **dois dias úteis** para comunicação do incidente de segurança a proteção de dados. Nesse contexto, é importante que a organização crie critérios - com base na LGPD e nos normativos e nas orientações da ANPD - que definam o que é um incidente que possa acarretar risco ou dano relevante aos titulares. Especialmente nos incidentes que envolvam dados do titular, é importante que se elabore um procedimento para potenciais questionamentos que possam surgir.

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

Quais informações foram objeto do incidente?

O titular pode ser vítima de fraude em razão do incidente?

O incidente foi devidamente comunicado às autoridades?

O que o titular pode fazer em benefício da sua proteção?

Onde o titular pode obter mais informações sobre o incidente?

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

Cabe ao Encarregado, diante das informações levantadas internamente e dos parâmetros estabelecidos pelo órgão, pela ANPD ou com base em boas práticas, avaliar a necessidade e a profundidade da comunicação com a Autoridade e com os titulares de dados. A ANPD orienta que as informações prestadas devem ser claras e concisas. Recomenda ainda que a comunicação contenha as seguintes informações:

Identificação e dados de contato de:

- Instituição ou pessoa responsável pelo tratamento;
- Encarregado de dados ou outra pessoa de contato;
- Indicação se a notificação é completa ou parcial. Em caso de comunicação parcial, indicar que se trata de uma comunicação preliminar ou de uma comunicação complementar.

Informações sobre o incidente de segurança com dados pessoais:

- Data e hora da detecção;
- Data e hora do incidente e sua duração;
- Circunstâncias em que ocorreu a violação de segurança de dados pessoais, por exemplo, perda, roubo, cópia, vazamento, dentre outros;
- Descrição dos dados pessoais e informações afetadas, como: natureza e conteúdo dos dados pessoais, categoria e quantidade de dados e de titulares afetados;
- Resumo do incidente de segurança com dados pessoais, com indicação da localização física e meio de armazenamento;
- Possíveis consequências e efeitos negativos sobre os titulares dos dados afetados;
- Medidas de segurança, técnicas e administrativas preventivas tomadas pelo Controlador de acordo com a LGPD;
- Resumo das medidas implementadas até o momento para controlar os possíveis danos;
- Possíveis problemas de natureza transfronteiriça;
- Outras informações úteis às pessoas afetadas para proteger seus dados ou prevenir possíveis danos.

A ANPD esclarece que, caso não seja possível fornecer todas as informações no momento da comunicação preliminar, poderão ser feitos esclarecimentos adicionais posteriormente. Entretanto, no momento da comunicação preliminar, deverá ser informado à ANPD se serão fornecidos outros elementos posteriormente, bem como os meios que estão sendo utilizados para obtê-las. A ANPD também poderá requerer informações adicionais a qualquer momento.

A Autoridade Nacional de Proteção de Dados disponibiliza, em seu sítio eletrônico, um formulário modelo para notificação de incidentes de segurança com proteção de dados. O formulário pode ser acessado no site da ANPD ou através do seguinte link: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca.

COMUNICAR A ETIR DO TRT 15

É necessário que o TRT 15 estabeleça os métodos para realizar a comunicação à Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) quando da ocorrência de incidentes de segurança com dados pessoais. Há previsão no anexo único da Portaria GP 030/2022 (item 9.2) de que: ***"No processo de trabalho deverá ser definida a forma de comunicação de todos os incidentes de segurança e problemas de Segurança de Informação relacionados ao escopo da ETIR".*** Ainda no mesmo anexo, consta que: ***"É competência da ETIR estabelecer, manter, revisar - no mínimo anualmente e aperfeiçoar quando necessário - o Processo de Gerenciamento de Incidentes de Segurança da Informação..."***. Tal comunicação permite a realização de ações conjuntas durante o tratamento do incidente com dados pessoais e pode igualmente ensejar uma resposta mais célere, técnica e eficaz.

ELABORAR A DOCUMENTAÇÃO

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

a) conter as devidas considerações sobre a promoção da melhoria contínua dos processos de tratamento de incidentes;

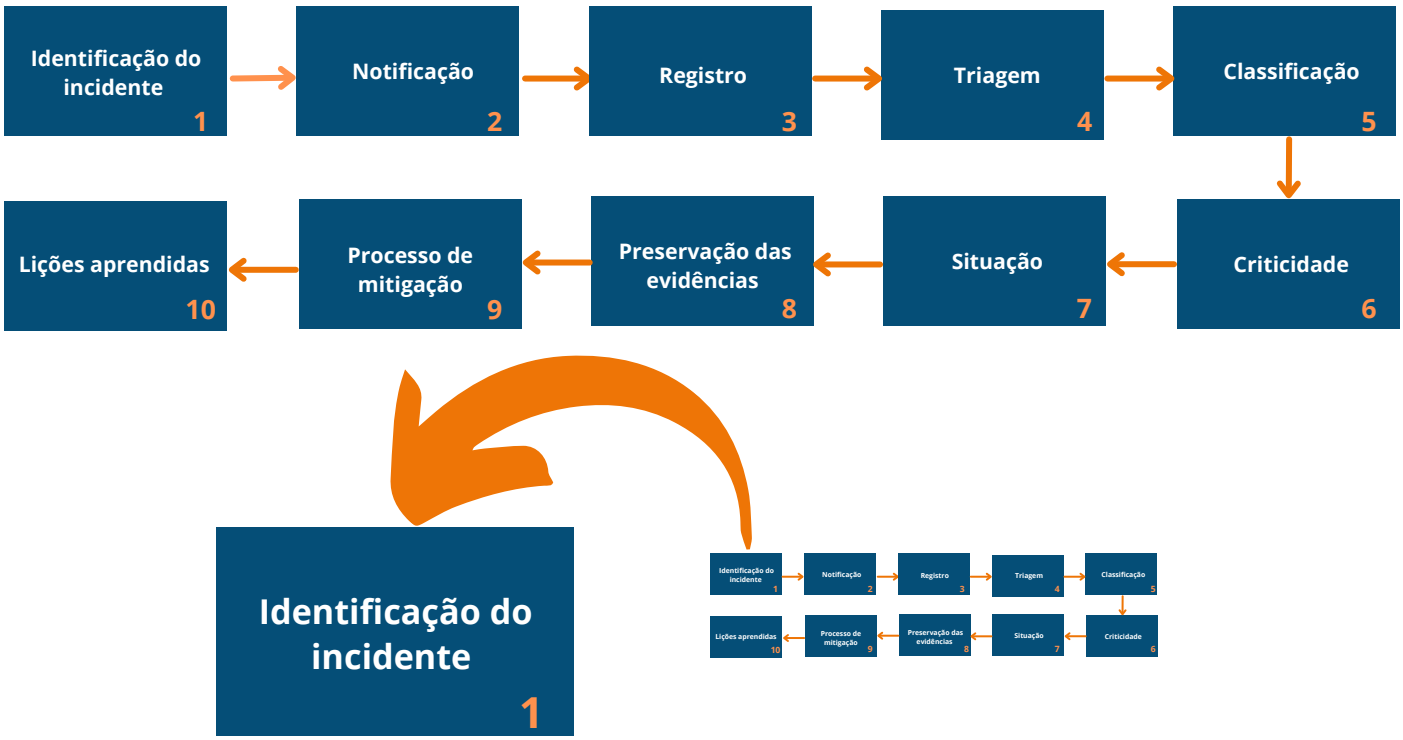
b) estar disponível para consulta em caso de atualização do Relatório de Impacto a Proteção de Dados (RIPD).

A Autoridade Nacional de Proteção de Dados pode solicitar tal relatório para análise, com o propósito de:

- **avaliar as ações tomadas durante o incidente em que dados pessoais tenham sido expostos ou comprometidos;**
- **publicar e atualizar normas referentes à proteção de dados;**
- **cumprir o príncipio da responsabilização;**
- **utilizá-lo como subsídio para eventuais questionamentos, facilitando a comprovação de conformidade.**

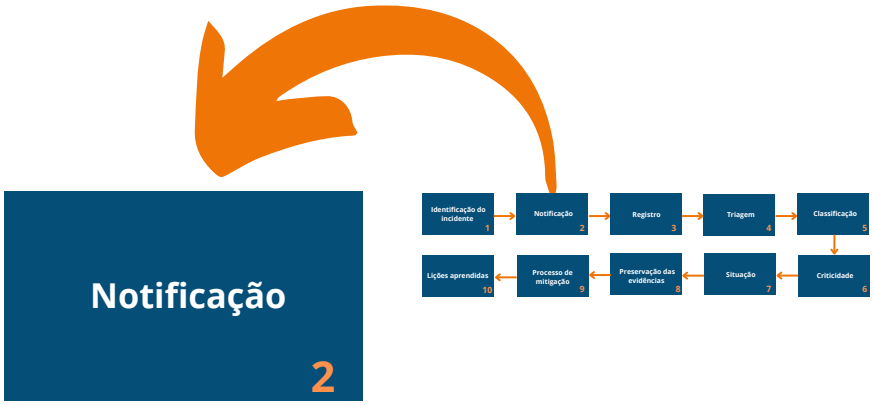
PROCESSO DE RESPOSTA AO INCIDENTE

Com base no exposto, apresenta-se a seguir as etapas do processo de resposta ao incidente com dados pessoais.



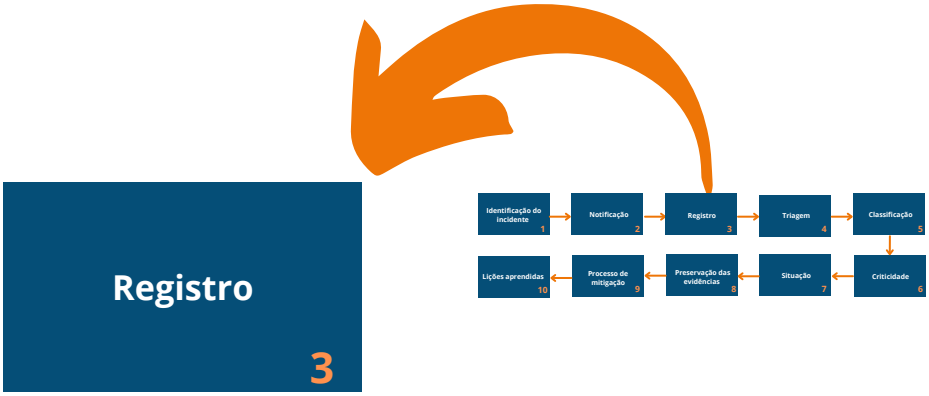
Um novo incidente é notificado por pessoa, externa ou não ao TRT 15, ou por alarme da monitoração, a partir de um dos mecanismos de comunicação a ser definido. A comunicação inicial do incidente pode ser proveniente de qualquer fonte. A comunicação com a Ouvidoria, por exemplo, poderá ser feita por intermédio de formulário eletrônico (disponível no site do TRT 15), por manifestações escritas, que serão inseridas no sistema eletrônico, pessoalmente, ou, ainda, por telefone.

A identificação de um incidente também pode ocorrer pela interrupção não planejada de um serviço de TI; por recebimento de e-mails com *links* suspeitos para clicar ou contendo código malicioso, o qual permite que o invasor controle remotamente o computador ou dispositivo que hospeda; entre outras ocorrências suspeitas como vírus, ataques cibernéticos e outros.

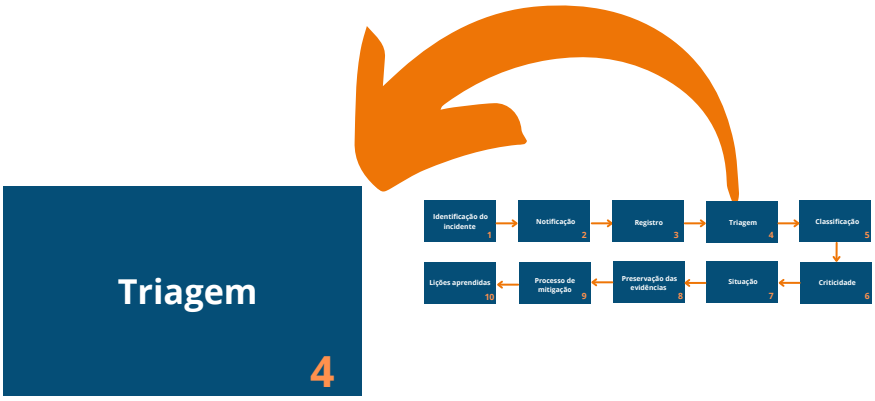


Em seguida, ao se registrar uma notificação de incidente de segurança da informação e privacidade, sugere-se inserir as seguintes informações para controle e armazenamento:

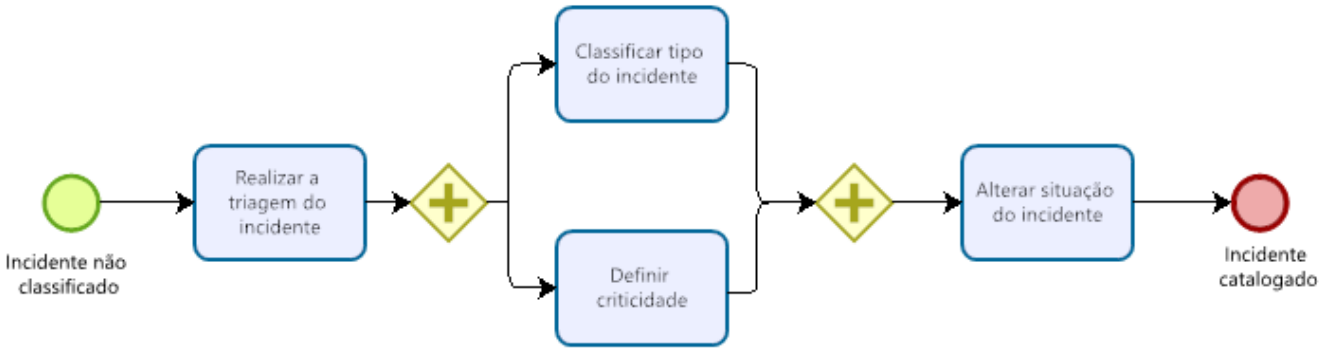
1. **Origem do incidente**: unidade, setor ou organização à qual o dispositivo ou o processo que originou o incidente pertence;
2. **Contato da origem:** e-mail, telefone ou outro contato disponível do informante do incidente;
3. **Registro do tempo da ocorrência do incidente:** data e hora em formato GMT (*Greenwich Mean Time*) na qual o incidente foi identificado. Exemplo: "10:23, 20 de Março de 2021".
4. **Local onde originou o incidente:** endereço IP (IPv4 ou IPv6) do dispositivo ou serviço que originou o incidente;
5. **Recursos utilizados pela origem do incidente**: especificação do tipo do protocolo (IP, TCP, UDP, etc) e portas, ou procedimentos operacionais, adotados na ação do incidente;
6. **Endereço do alvo:** endereço IP (IPv4 ou IPv6) do dispositivo ou endereço de acesso do serviço que foi o alvo do incidente;
7. **Protocolos e portas alvos do incidente:** especificação do tipo do protocolo (IP, TCP, UDP, etc.) e portas utilizados no destino do incidente;
8. **Serviços envolvidos:** especificação do serviço que foi alvo do incidente (http, ftp, smtp, etc.) e versões de sistemas utilizados;
9. **Descrição do incidente:** breve descrição do incidente, tais como tipo do ataque, motivação aparente, ou outras características relevantes;
10. ***Logs* ou evidências:** anexação das porções de *log*, imagens, códigos de erro ou outros registros que evidenciem a ocorrência do incidente;



Nesta etapa, sugere-se que o incidente seja documentado em base de conhecimento apropriada, detalhando as informações obtidas, linha do tempo, atores envolvidos, evidências, conclusões, decisões, autorizações e ações tomadas, inclusive as da reunião de lições aprendidas.



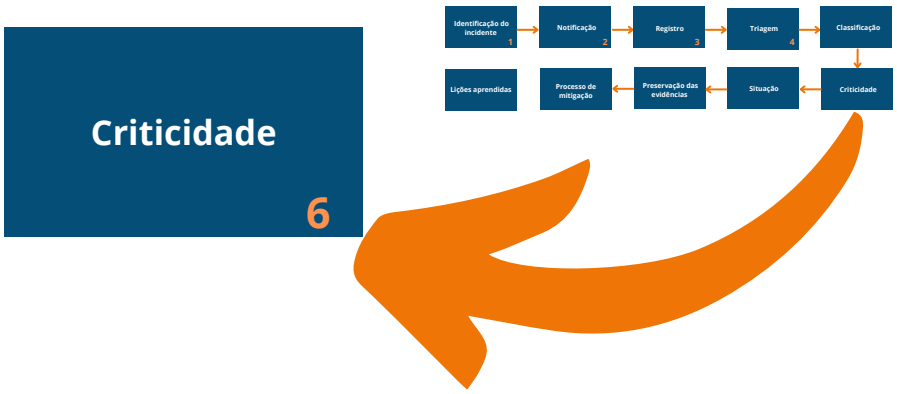
A etapa de triagem tem como objetivo reunir informações sobre o evento, avaliar a sua natureza, e classificá-lo como incidente para que, adiante, se inicie o processo de tratamento. A seguir um exemplo de fluxograma desse processo de trabalho.



A próxima etapa, classificar o incidente, é importante para esclarecer e auxiliar no tipo de atendimento a ser realizado e também na definição da sua criticidade. As classificações sugeridas neste Plano são:

1. **Conteúdo abusivo**: *spam*, assédio, etc.;
2. **Código malicioso**: *bot*, *worm*, vírus, *trojan*, *spyware*, *scripts*;
3. **Prospecção por informações**: varredura, *sniffing*, engenharia social;
4. **Tentativa de intrusão**: tentativa de exploração de vulnerabilidades, tentativa de acesso lógico;
5. **Intrusão**: Acesso lógico indesejável, comprometimento de conta de usuário, de aplicação;

6. **Indisponibilidade de serviço ou informação**: negação de serviço, sabotagem;
7. **Segurança da informação**: acesso não-autorizado à informação, modificação não autorizada da informação;
8. **Fraude**: violação de direitos autorais, fingir ou falsificar identidade pessoal ou institucional, uso de recursos de forma não-autorizada;
9. **Outros**: incidente não categorizado.

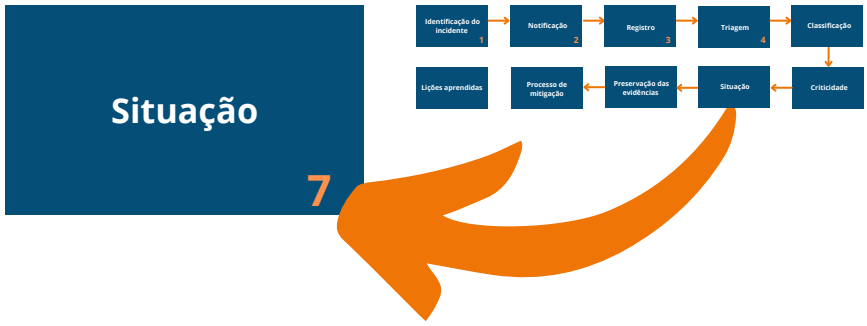


Esta etapa tem como objetivo definir uma ordem de atendimento dos incidentes e um SLA (*Service Level Agreement* - Acordo de Nível de Serviço) de acordo com a urgência de tratamento e o impacto nas áreas administrativas do TRT 15. Assim, sugere-se determinar a classificação de criticidade do incidente de acordo com as definições a seguir:

ALTO (impacto grave): incidente que afeta sistemas relevantes ou informações críticas, com potencial para gerar impacto negativo sobre o 15º Regional;

MÉDIO (impacto significativo): incidente que afeta sistemas ou informações não críticas, sem impacto negativo ao Tribunal;

BAIXO (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.



Em seguida, sugere-se definir uma **situação** para cada incidente, a qual tem como escopo acompanhar o andamento de tal evento dentro do processo de tratamento.

1. **Aberto:** nesse momento foi realizado apenas o registro das informações.
2. **Processamento:** o chamado é assumido por um técnico e está em tratamento.
3. **Pendente:** necessário confirmar alguma informação com o solicitante antes de dar prosseguimento. Tentativas de contato devem ser realizadas e registradas.
4. **Transferido (pendente de terceiros):** ocorre quando uma equipe solucionadora não tem ação no chamado, o qual é repassado.
5. **Solucionado:** indica que o procedimento técnico foi aplicado e aparentemente o chamado foi solucionado.
6. **Fechado:** a solução do chamado foi confirmada pelo solicitante. O fechamento pode ocorrer automaticamente ou por contato.

Preservação das evidências 8

Antes de se iniciar as ações para restaurar as operações do ambiente, é necessária a preservação de provas para a identificação correta da causa raiz do incidente e, posteriormente, para a recuperação dos sistemas afetados.

Processo de mitigação 9

O processo de mitigação do incidente envolve as etapas de: preparação, detecção, contenção, erradicação, recuperação e avaliação.

PREPARAÇÃO: gerenciar as ferramentas para análise de incidentes, incluindo o conhecimento de todo o ambiente utilizado.

- Implementar mecanismos de defesa e controle de ameaças.
- Desenvolver procedimentos para lidar com incidentes de forma eficiente.
- Obter recursos e equipe necessária para lidar com os problemas.
- Estabelecer infraestrutura de suporte à atividade de resposta a incidentes.

DETECÇÃO: detectar o incidente, determinar o escopo e as atividades envolvidas com o incidente.

- Identificar todos os sistemas e serviços afetados relacionados com o incidente.
- Avaliar o impacto do incidente e os potenciais riscos dos sistemas afetados (dados vazados, informações de instituições parceiras, impacto na própria organização e na reputação).
- Identificar a existência de outros eventos e alertas relacionados com o incidente em questão.
- Identificar que tipo de informação e processos podem ter sido afetados.

CONTENÇÃO: conter o incidente de maneira a atenuar os danos e evitar que demais recursos sejam comprometidos.

- Desconectar o sistema comprometido ou isolar a rede afetada.
- Desativar o sistema para evitar maiores perdas quando há perda ou roubo de informações durante o ataque.
- Alterar políticas de roteamento dos equipamentos de rede ou bloquear padrões de tráfego, interrompendo o fluxo malicioso.
- Desabilitar serviços vulneráveis, inibindo comprometimento de outros sistemas.

ERRADICAÇÃO: eliminar as causas do incidente, removendo todos os eventos relacionados.

- Garantir que as causas do incidente foram removidas, assim como todas as atividades e arquivos associados ao incidente.
- Assegurar a remoção de todos os métodos de acesso utilizados pelo invasor: novas contas de acessos; *backdoors* e, se aplicável, acesso físico ao sistema comprometido.

RECUPERAÇÃO: restaurar o sistema ao seu estado normal.

- Caso exista Plano de Continuidade de Negócio dos serviços impactados, eles devem ser iniciados, conforme especificado no respectivo plano.
- Restaurar a integridade do sistema.
- Garantir que o sistema foi recuperado corretamente e que as funcionalidades estejam ativas.
- Implementar medidas de segurança para evitar novos comprometimentos
- Restauração do último e íntegro *backup* completo armazenado.

AVALIAÇÃO: avaliar as ações realizadas para resolver o incidente, documentando detalhes, e discutir lições aprendidas.

- Caracterizar o conjunto de lições aprendidas de modo a aprimorar os procedimentos e processos existentes.
- Identificar características de incidentes que podem ser utilizadas para treinar novos membros da equipe.
- Prover estatísticas e métricas relativas ao processo de resposta a incidentes.
- Obter informações que podem ser utilizadas em processos legais.

Lições aprendidas

10

Esta última etapa tem como escopo avaliar o processo de tratamento do incidente e verificar a eficácia das soluções adotadas. Para isso, é importante relacionar e documentar, no chamado do incidente, as falhas e os recursos inexistentes ou insuficientes, para que sejam providenciados em futuras ocasiões. A partir da mitigação do incidente e sua resolução, é necessário conduzir o apanhado de 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 para os processos de resposta a incidentes.

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

OUTRAS RECOMENDAÇÕES NO PROCESSO DE RESPOSTA AO INCIDENTE

- Definir um plano de comunicação para incidentes de violação de dados. O objetivo é propiciar maior celeridade na solução de incidentes e padronização de atividades a serem executadas, assim como prever responsáveis pelo seu cumprimento.
- Documentar violações atestadas e incidentes ocorridos, a fim de analisar riscos de violação periodicamente.
- Alinhar o processo de gestão de vulnerabilidade técnica com as atividades do plano de resposta a incidentes para comunicar dados sobre esse tema às equipes de resposta e fornecer procedimentos técnicos em caso de incidente.
- Promover a gestão adequada dos *softwares* homologados para uso dentro do Tribunal. A instalação de *software* não controlada em dispositivos computadorizados pode introduzir vulnerabilidades e em seguida gerar o vazamento de informações, perda de integridade ou outros incidentes de segurança da informação além da violação de direitos de propriedade intelectual.
- Identificar os requisitos de segurança da informação usando vários métodos, como requisitos de conformidade oriundos de política e regulamentações, modelos de ameaças, análises críticas de incidentes ou o uso de limiares de vulnerabilidade. Convém que os resultados da identificação sejam documentados e analisados criticamente por todas as partes interessadas.
- Considerar a segurança da informação em cada estágio. Desenvolvimentos de sistemas novos e mudanças nos existentes são oportunidades para o Tribunal atualizar melhorar os controles de segurança, levando em conta os incidentes reais e os riscos de segurança da informação, projetados e atuais.

REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecaode-dados/outros-documentos-externos/anpd_guia_agentes_de_tratamento.pdf>
Acesso em 17 de fevereiro de 2022.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Comunicação de Incidentes de segurança. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca>
Acesso em 22 de fevereiro de 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>.
Acesso em: 17 de fevereiro de 2022.

GOVERNO FEDERAL. Guia de boas práticas: Lei Geral de Proteção de Dados (LGPD). Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-dedados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dadospessoais-lgpd>.
Acesso em: 14 de fevereiro de 2022.

GOVERNO FEDERAL. Guia de Resposta a Incidentes de Segurança (LGPD). Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/GuiaderespostaaIncidentes_verso_Minuta_Finalversao_17121.pdf>
Acesso em 14 de fevereiro de 2022.

SECRETARIA DE FINANÇAS DO ESTADO DE RONDÔNIA - SEFIN. PRISIP Plano de Resposta a Incidentes de Segurança da Informação e Privacidade. Disponível em: <https://www.sefin.ro.gov.br/portalsefin/userfiles/PRISIP.pdf>
Acesso em 16 de fevereiro de 2022.

TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E DOS TERRITÓRIOS. Processo de Gerenciamento de Incidente do TJDFT. Disponível em: <https://www.tjdft.jus.br/transparencia/governanca-de-tic/gerenciamento-de-servicos-de-tic/arquivos/2-tjdft-gerenciamento-de-incidentes.pdf >.
Acesso em: 15 de fevereiro de 2022.

UNIVERSIDADE FEDERAL DE LAVRAS. Plano de Gestão de Incidentes de Segurança da Informação e Privacidade. Disponível em: <https://dgti.ufla.br/images/politicas-e-normas/Plano_Gestao_Incidentes_v12_assinado.pdf>
Acesso em: 22 de fevereiro de 2022.

ANEXO - FORMULÁRIO DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS À ANPD

COMUNICAÇÃO

Tipo de comunicação:

- ☐ **Completa.**
- ☐ **Parcial.**

Para comunicação parcial:

- ☐ **Preliminar.**
- ☐ **Complementar.**

Critério para a comunicação:

- ☐ **O incidente de segurança pode acarretar risco ou dano relevante aos titulares.**
- ☐ **Não tenho certeza sobre o nível de risco do incidente de segurança.**

AGENTE DE TRATAMENTO

O notificante é:

- ☐ **Controlador.**
- ☐ **Operador.**

Se operador, informar se já houve comunicação ao controlador: ***[Resposta]***

Dados do agente de tratamento:

- Número do CPF ou CNPJ:
- Nome ou Razão Social:
- Natureza da Organização (Pública ou Privada): *[Resposta]*
- Endereço: *[Resposta]*
- Cidade: *[Resposta]*
- Estado: *[Resposta]*
- Telefone: *[Resposta]*
- E-mail: *[Resposta]*

Dados do notificante:

- Nome: *[Resposta]*
- E-mail: *[Resposta]*
- Telefone: *[Resposta]*

Dados do Encarregado:

☐ **Mesmos dados do notificante.**

- Nome: *[Resposta]*
- E-mail: *[Resposta]*
- Telefone: *[Resposta]*

INCIDENTE DE SEGURANÇA

Descreva de forma resumida como o incidente de segurança com dados pessoais ocorreu. ***[Resposta]***

Quando o incidente ocorreu?

[Data e hora]

☐ **Não tenho conhecimento. Justifique:** ***[Resposta]***

☐ **Não tenho certeza. Justifique:** ***[Resposta]***

Quando a organização teve ciência do incidente de segurança?

[Data e hora]

Descreva como a organização teve ciência do incidente de segurança?

[Resposta]

Se a comunicação inicial do incidente não foi comunicada no prazo de 2 dias úteis após ter tomado ciência do incidente, justifique os motivos.

[Resposta]

Se o incidente não foi comunicado de forma imediata após a sua ciência, justifique os motivos da demora.

[Resposta]

Qual a natureza dos dados afetados?

☐ **Origem racial ou étnica.**

☐ **Convicção religiosa.**

☐ **Opinião política.**

☐ **Filiação a sindicato.**

☐ **Filiação a organização de caráter religioso, filosófico ou político.**

☐ **Dado referente à saúde.**

☐ **Dado referente à vida sexual.**

☐ **Dado genético ou biométrico.**

- [ ] **Dado de comprovação de identidade oficial (por exemplo: nº RG, nº CPF, nº CNH).**
- [ ] **Dado financeiro.**
- [ ] **Nomes de usuário ou senhas de sistemas de informação.**
- [ ] **Dado de geolocalização.**

Outros: *[Resposta]*

Qual a quantidade de titulares afetados?

[Resposta]

Qual a categoria dos titulares afetados?

- [ ] **Funcionários.**
- [ ] **Prestadores de serviço.**
- [ ] **Clientes.**
- [ ] **Consumidores.**
- [ ] **Usuários.**
- [ ] **Pacientes de serviço de saúde.**
- [ ] **Crianças ou adolescentes.**

Outros: *[Resposta]*

MEDIDAS DE SEGURANÇA UTILIZADAS PARA A PROTEÇÃO DOS DADOS

Quais medidas de segurança, técnicas e administrativas, foram tomadas para prevenir a ocorrência do incidente de segurança?

[Resposta]

Quais medidas de segurança, técnicas e administrativas, foram tomadas após a ciência do incidente de segurança?

[Resposta]

Quais medidas de segurança, técnicas e administrativas, foram ou serão adotadas para reverter ou mitigar os efeitos do prejuízo do incidente de segurança aos titulares dos dados?

[Resposta]

O agente de tratamento realizou relatório de impacto à proteção de dados pessoais?

[Resposta]

RISCOS RELACIONADOS AO INCIDENTE DE SEGURANÇA

Quais as prováveis consequências do incidente de segurança para os titulares afetados?

[Resposta]

Considerando os titulares afetados, na sua avaliação, o incidente pode trazer consequências transfronteiriças?

[Resposta]

COMUNICAÇÃO AOS TITULARES DE DADOS

Os titulares foram comunicados sobre o incidente de segurança com dados pessoais?

- ☐ **Sim.**
- ☐ **Não.**
- ☐ **Não sei.**

Forneça detalhes.

[Resposta]

Caso os titulares afetados não tenham sido informados, quais os motivos que justificam a não comunicação ou o seu retardo?

[Resposta]

JUSTIÇA DO TRABALHO

Tribunal Regional do Trabalho da 15ª Região (Campinas)

ASSESSORIA DE GESTÃO ESTRATÉGICA
age.presidencia@trt15.jus.br

Atualizado em 08.02.23