GOVERNO DO ESTADO DE PERNAMBUCO

SECRETARIA DE DESENVOLVIMENTO PROFISSIONAL E EMPREENDEDORISMO DO ESTADO DE PERNAMBUCO – SEDEPE

PLANO DE RESPOSTA A INCIDENTES A DADOS PESSOAIS

SUMÁRIO

1. GLOSSÁRIO

Agentes de tratamento: o controlador e o operador de dados;

Anonimização: 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): órgão da administração pública nacional responsável por fiscalizar e zelar pelo cumprimento da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) 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 que o invasor controle remotamente o computador ou dispositivo que hospeda;

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

Co-controlador: SEDEPE, MINISTÉRIO DO TRABALHO E EMPREGO e INSTITUTO TAVARES BURIL;

Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

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

Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

Dado pseudonimizado: dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

Eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

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 pessoais, confidenciais, infectar seus computadores com malware ou abrir links para sites infectados;

Expurgo de dados: 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;

Finalidade do tratamento de dados: motivo para coleta, armazenamento, acesso e descarte dos dados pessoais;

Incidente: evento, ação ou om
issão 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, 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: 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;

Manutenção dos dados pessoais: manutenção dos dados após a execução do serviço;

Operador: pessoa natural 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 Segurança institucional: conjunto de medidas voltadas a prevenir, detectar, obstruir e neutralizar ações adversas de qualquer natureza que possam intervir ou ameaçar o bom andamento das atividades desenvolvidas no âmbito da organização;

Servidores: todos os servidores permanentes ou temporários, estagiários, jovens aprendizes, terceiros contratados, alocados ou não nas dependências da SEDEPE;

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

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

Spam: 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: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro (art. 5º, inciso XV, da LGPD);

Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

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;

Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos ou entre entes privados;

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

2. INFORMAÇÕES SOBRE O CONTROLADOR E RESPONSABILIDADES

Segundo a LGPD, o controlador é a pessoa natural ou jurídica a quem competem as decisões referentes ao tratamento de dados pessoais.

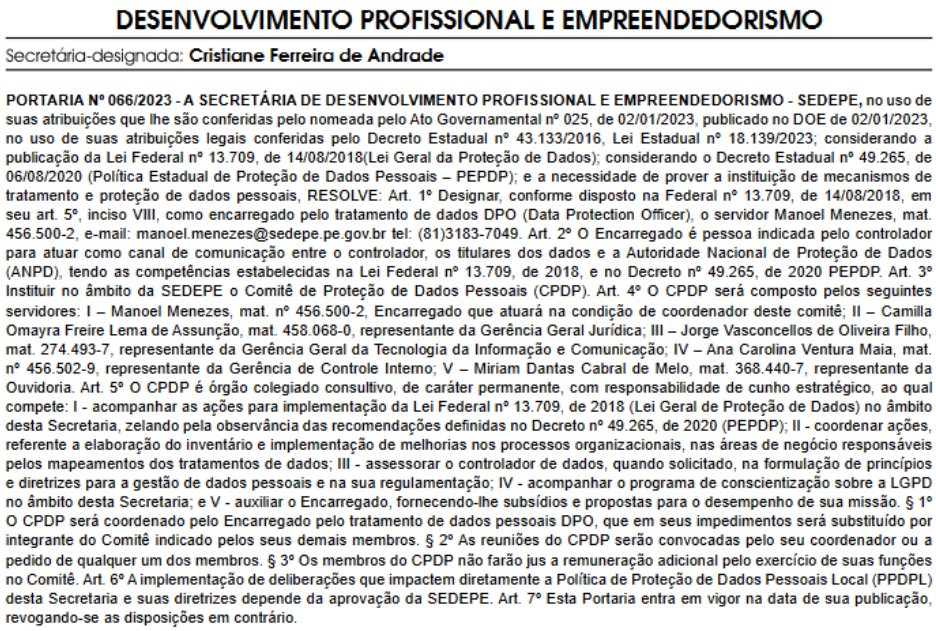
Como a SEDEPE apenas opera o sistema do MINISTÉRIO DO TRABALHO - Sistema Nacional de Emprego (SINE), não atua como controlador. Sendo assim, o controlador é o próprio ministério.

Embora, para fins da LGPD, a SEDEPE não possa ser enquadrado como controlador, assume algumas atribuições de controlador no exercício de suas competências constitucionais e legais. Entre essas atribuições, por exemplo, estão o dever de indicar o encarregado pelo tratamento de dados pessoais (art. 41 c/c o art. 23, inciso III, da LGPD) e o atendimento aos direitos do titular nas hipóteses aplicáveis à relação titular-Administração Pública (art. 18 c/c o art. 23, inciso I, LGPD). No entanto, nem todas as atribuições de controlador se aplicam, a exemplo da responsabilidade e do ressarcimento de danos.

Dados institucionais da SEDEPE: **SECRETARIA DE DESENVOLVIMENTO PROFISSIONAL E EMPREENDEDORISMO. CNPJ/MF 08.693.255/0001-99. Endereço: RUA DA AURORA, 425. CEP 50.050-000. BOA VISTA. RECIFE/PE. Fone: (81) 3183-7018/ (81) 3183-7007. Website: www.sedepe.pe.gov.br . e-mail: gabinete@sedepe.pe.gov.br .**

Entre 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 de Resposta a Incidentes a Dados Pessoais. São eles:

Comitê de Proteção de Dados Pessoais (CPDP): comitê responsável, entre outras atribuições, por acompanhar os processos de segurança da informação e de proteção de dados pessoais **(Portaria SEDEPE nº 066/2023).**



DESENVOLVIMENTO PROFISSIONAL E EMPREENDEDORISMO

Secretária-designada: **Cristiane Ferreira de Andrade**

PORTARIA Nº 066/2023 - A SECRETÁRIA DE DESENVOLVIMENTO PROFISSIONAL E EMPREENDEDORISMO - SEDEPE, no uso de suas atribuições que lhe são conferidas pelo nomeada pelo Ato Governamental nº 025, de 02/01/2023, publicado no DOE de 02/01/2023, no uso de suas atribuições legais conferidas pelo Decreto Estadual nº 43.133/2016, Lei Estadual nº 18.139/2023; considerando a publicação da Lei Federal nº 13.709, de 14/08/2018(Lei Geral da Proteção de Dados); considerando o Decreto Estadual nº 49.265, de 06/08/2020 (Política Estadual de Proteção de Dados Pessoais – PEPDP); e a necessidade de prover a instituição de mecanismos de tratamento e proteção de dados pessoais, RESOLVE: Art. 1º Designar, conforme disposto na Federal nº 13.709, de 14/08/2018, em seu art. 5º, inciso VIII, como encarregado pelo tratamento de dados DPO (Data Protection Officer), o servidor Manoel Menezes, mat. 456.500-2, e-mail: manoel.menezes@sedepe.pe.gov.br tel: (81)3183-7049. Art. 2º O Encarregado é pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), tendo as competências estabelecidas na Lei Federal nº 13.709, de 2018, e no Decreto nº 49.265, de 2020 PEPDP. Art. 3º Instituir no âmbito da SEDEPE o Comitê de Proteção de Dados Pessoais (CPDP). Art. 4º O CPDP será composto pelos seguintes servidores: I – Manoel Menezes, mat. nº 456.500-2, Encarregado que atuará na condição de coordenador deste comitê; II – Camilla Omayra Freire Lema de Assunção, mat. 458.068-0, representante da Gerência Geral Jurídica; III – Jorge Vasconcellos de Oliveira Filho, mat. 274.493-7, representante da Gerência Geral da Tecnologia da Informação e Comunicação; IV – Ana Carolina Ventura Maia, mat. nº 456.502-9, representante da Gerência de Controle Interno; V – Miriam Dantas Cabral de Melo, mat. 368.440-7, representante da Ouvidoria. Art. 5º O CPDP é órgão colegiado consultivo, de caráter permanente, com responsabilidade de cunho estratégico, ao qual compete: I - acompanhar as ações para implementação da Lei Federal nº 13.709, de 2018 (Lei Geral de Proteção de Dados) no âmbito desta Secretaria, zelando pela observância das recomendações definidas no Decreto nº 49.265, de 2020 (PEPDP); II - coordenar ações, referente a elaboração do inventário e implementação de melhorias nos processos organizacionais, nas áreas de negócio responsáveis pelos mapeamentos dos tratamentos de dados; III - assessorar o controlador de dados, quando solicitado, na formulação de princípios e diretrizes para a gestão de dados pessoais e na sua regulamentação; IV - acompanhar o programa de conscientização sobre a LGPD no âmbito desta Secretaria; e V - auxiliar o Encarregado, fornecendo-lhe subsídios e propostas para o desempenho de sua missão. § 1º O CPDP será coordenado pelo Encarregado pelo tratamento de dados pessoais DPO, que em seus impedimentos será substituído por integrante do Comitê indicado pelos seus demais membros. § 2º As reuniões do CPDP serão convocadas pelo seu coordenador ou a pedido de qualquer um dos membros. § 3º Os membros do CPDP não farão jus a remuneração adicional pelo exercício de suas funções no Comitê. Art. 6º A implementação de deliberações que impactem diretamente a Política de Proteção de Dados Pessoais Local (PPDPL) desta Secretaria e suas diretrizes depende da aprovação da SEDEPE. Art. 7º Esta Portaria entra em vigor na data de sua publicação, revogando-se as disposições em contrário.

O **Comitê de Proteção de Dados Pessoais (CPDP),** grupo de servidores, designados via portaria, com responsabilidade de receber, analisar e responder as notificações e atividades relacionadas a incidentes de segurança da informação em ambiente tecnológico.

3. NOME E ENDEREÇO DO ENCARREGADO DE DADOS

O Encarregado que representa o controlador é o Assistente Técnico DPO Manoel Guilherme Fontes de Menezes, cujo contato poderá ser realizado por meio do e-mail: manoel.menezes@sedepe.pe.gpv.br. O nome e o contato do Encarregado estão disponíveis em www.sedepe.pe.gov.br.

4. REFERÊNCIA LEGAL (CONFORMIDADE)

Este documento foi elaborado com base no art. 5º, inciso XVII, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD), no art. 5º, inciso LXXIX, da Constituição da República Federativa do Brasil de 1988 (CRFB/1988), na Lei nº 10.406/2002 (Código Civil), na Lei nº 12.965/2014 (Marco Civil da Internet), no Guia Orientativo para o Tratamento de Dados Pessoais pelo Poder Público da Autoridade Nacional de Proteção de Dados (ANPD) e orientações pela Secretaria da Controladoria Geral do Estado de Pernambuco – SCGE.

5. ACCOUNTABILITY (RESPONSABILIDADES)

5.1 Encarregado pelo tratamento de dados pessoais

a) Organizar e/ou ministrar treinamentos sobre proteção de dados pessoais aos servidores, promovendo a cultura de proteção de dados pessoais na SEDEPE;

b) Elaborar e/ou revisar os procedimentos internos relativos à proteção de dados pessoais e auxiliar na definição de controles para garantir a integridade, confidencialidade e disponibilidade dos dados pessoais;

c) Auxiliar na definição de controles para garantir a existência de registros auditáveis de todo o ciclo de vida dos dados pessoais;

d) Apoiar na resposta aos incidentes de segurança que envolvam dados pessoais;

e) Realizar acompanhamento legislativo/regulatório sobre o tema;

f) Orientar as unidades da estrutura organizacional em caso de mudanças de finalidades de tratamento;

g) Apoiar na manutenção atualizada do mapeamento dos fluxos de dados pessoais;

h) Recomendar os requisitos adequados no caso de transferência de dados entre agentes de tratamento, especialmente transferências internacionais;

i) Responder consultas e apresentar recomendações sobre a aplicação das regras de privacidade junto às unidades da estrutura organizacional e demais agentes de tratamento;

j) Participar do processo de avaliação dos demais agentes de tratamento de dados pessoais (aderência e maturidade do tema), quando necessário;

k) Zelar para que os titulares dos dados sejam informados sobre seus direitos, obrigações e responsabilidades referentes à proteção de dados;

l) Sensibilizar os servidores sobre proteção de dados e privacidade;

m) Apoiar investigações para apuração de responsabilidade dos envolvidos em eventual violação de dados pessoais e auxiliar na definição de aplicação das penalidades internas, quando necessário;

n) Avaliar Relatórios de Impacto à Proteção de Dados Pessoais;

o) Aceitar reclamações e comunicações dos titulares, bem como prestar esclarecimentos e adotar providências;

p) Receber comunicações da ANPD e adotar providências;

q) Orientar os servidores e os contratados da SEDEPE a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

r) Assegurar a divulgação e a disponibilidade dos documentos que compõem esta Política e outros documentos internos para proteção de dados pessoais na SEDEPE;

5.2 Tecnologia da Informação da SEDEPE

a) Assegurar que todos os sistemas, serviços e equipamentos usados para o tratamento de dados pessoais estejam dentro de um padrão aceitável de segurança;

b) Analisar os aspectos técnicos de todo e qualquer produto ou serviço de terceiros que a SEDEPE esteja considerando contratar para processar ou armazenar dados pessoais (exemplos: nuvem, hardware, equipamentos de rede);

c) Auxiliar na implementação de procedimentos, controles e rotinas necessárias para o tratamento de dados pessoais;

d) Implementar medidas necessárias e apropriadas para manutenção da confidencialidade, integridade e disponibilidade dos sistemas, da privacidade e dos dados pessoais;

5.3 Consultoria Jurídica Geral

a) Apoiar o Encarregado na elaboração de repostas à ANPD;

b) Apoiar o Encarregado em relação à possiblidade de tratamento de dados pessoais no exterior, auxiliando no entendimento de validação do nível de proteção de dados pessoais do país destino;

c) Fornecer orientação legal nos casos de ocorrência de incidentes de violação de dados pessoais.

5.4 Comitê de Proteção de Dados Pessoais (CPDP):

a) Promover, com o Encarregado, a cultura de proteção de dados pessoais da SEDEPE, realizando campanhas de capacitação e divulgação da proteção dos dados pessoais;

b) Assegurar a divulgação dos documentos que compõem este Plano e outros documentos internos para proteção de dados pessoais na SEDEPE;

c) Assegurar que os servidores estejam cientes do tratamento realizado aos seus dados pessoais.

5.5 Demais unidades da estrutura organizacional e servidores da SEDEPE:

a) Cumprir as diretrizes deste Plano e seus documentos complementares;

b) Tratar os dados pessoais sob responsabilidade da SEDEPE somente para os fins autorizados, de forma ética e legal, respeitando os direitos do titular dos dados pessoais, bem como respeitando as orientações da legislação aplicável, deste Plano e de outros instrumentos regulamentares relacionados à proteção de dados pessoais;

c) Zelar pela integridade, disponibilidade, confidencialidade, autenticidade e legalidade dos dados pessoais acessados ou manipulados, não utilizando, enviando, transmitindo ou compartilhando indevidamente esses dados pessoais em qualquer local ou mídia, inclusive na Internet;

d) Reportar formalmente ao Encarregado quaisquer eventos relativos à violação ou possibilidade de violação de dados pessoais, ou outras atividades suspeitas de que tiver conhecimento.

6. OBJETIVO E ÂMBITO

6.1 Incidentes de Segurança com dados pessoais A SEDEPE cumpre os fundamentos da Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais, a chamada Lei Geral de Proteção de Dados Pessoais (LGPD).

As ações de tratamento de dados pessoais da SEDEPE são realizadas para atendimento e execução de suas atribuições constitucional, legal regimental.

Assim, somente os dados pessoais estritamente necessários à finalidade do atendimento dessas atribuições serão tratados (inciso III do art. 6º, inciso II do art. 7º e caput do art. 23, todos da LGPD).

Conforme prevê 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. Essas medidas de segurança deverão ser observadas desde a concepção do produto ou serviço até a sua execução.

6.1.1 Procedimentos a serem adotados em caso de incidentes que coloquem em risco a segurança de dados:

a) 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 –, consequências do incidente para os titulares de dados e para a SEDEPE, criticidade e probabilidade. Além disso, é importante preservar todas as evidências do incidente, conforme “Formulário de Registro Interno de Incidente com Dados Pessoais” (anexo I);

b) Comunicar ao Encarregado a existência do incidente, caso envolva dados pessoais (art. 5º, inciso VIII, da LGPD);

c) Comunicar ao Controlador, nos termos da LGPD, a existência do incidente, caso envolva dados pessoais;

d) Comunicar à ANPD e ao titular de dados pessoais a existência do incidente, em caso de risco ou dano relevante aos titulares (art. 48 da LGPD), mencionando no mínimo:

d.1) a descrição da natureza dos dados pessoais afetados;

d.2) as informações sobre os titulares envolvidos;

d.3) a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

d.4) os riscos relacionados ao incidente;

d.5) os motivos da morosidade, no caso de a comunicação não ter sido imediata; e

d.6) as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

e) Comunicar ao **Comitê de Proteção de Dados Pessoais (CPDP):** em caso de incidentes na rede computacional;

f) 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 Relatório de Impacto à Proteção dos Dados Pessoais (RIPD) e para o cumprimento do princípio de responsabilização e prestação de contas (art. 6º, inciso X, da LGPD);

g) Se os dados envolvidos no incidente estiverem anonimizados não serão dados pessoais e, em razão disso, deverão seguir o processo normal de gestão de incidentes de segurança da informação e não este Plano.

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 será devidamente analisada pela ANPD.

A ANPD recomenda ainda, conforme Decreto nº 9936/2019 (enquanto pendente a regulamentação), que o prazo razoável para a comunicação de incidente seja de dois dias úteis. Ela 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.

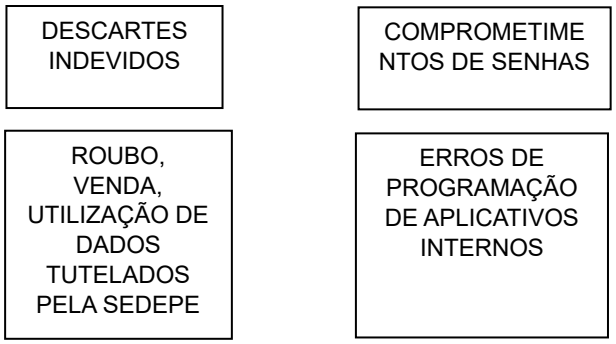
A seguir, detalhamento dos procedimentos (mencionados no item .1.1) a serem adotados em caso de possível incidente de segurança.

6.2 Avalição interna do incidente

Quando for detectado um incidente de segurança da SEDEPE 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:

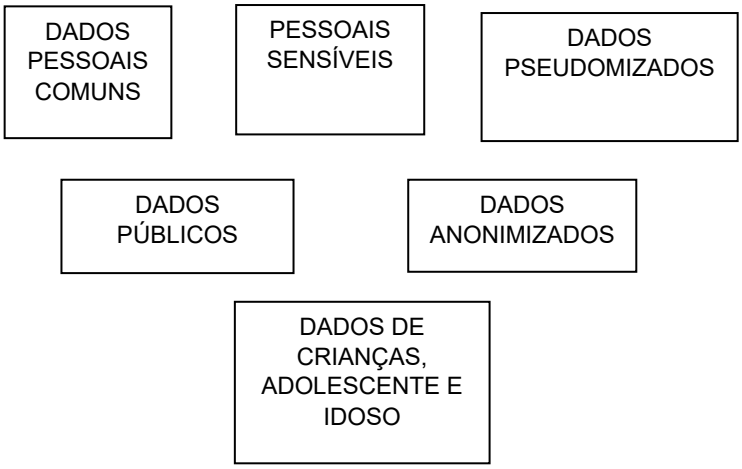
ACESSO INDEVIDO	ROUBO DE DADOS	ATAQUES CIBERNETICOS	ENGENHARIA SOCIAL	REPASSE DE DADOS SOCIAIS



b) Qual fonte dos dados pessoais foi atacada, como por exemplo:

preenchimento de formulários eletrônicos ou não eletrônico pelo titular de dados APIs (Interface de programa de aplicação) uso compartilhado de dados pessoais XML (extensible markup language) Cookies.

c) Qual categoria de dados foi atacada, como por exemplo:



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

e) Qual o resultado da avaliação de impacto ao titular de dados pessoais: avaliar os impactos que o incidente pode gerar a entidade, como perda de confiabilidade do cidadão, ações judiciais, danos à imagem da SEDEPE em âmbito nacional e internacional, prejuízo à Corte de Contas em contratos com fornecedores e clientes, e impacto total ou parcial nas atividades desenvolvidas pelo Tribunal.

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.

O Encarregado deverá considerar como agravantes na análise do impacto ao titular de dados pessoais a possibilidade do incidente:

• acarretar danos morais e/ou materiais ao titular de dados pessoais;

• implicar risco à vida dos titulares ou efeitos discriminatórios ilícitos ou abusivos;

• afetar significativamente o exercício dos direitos dos titulares (considerada a relevância do direito) ou o uso do serviço (considerada sua essencialidade).

Caso o tratamento dos dados pessoais, objeto do incidente, não tenha um fundamento legal, também será considerado um agravante.

Para análise da probabilidade, o Encarregado deve considerar as medidas de controles anterior e posteriormente implementadas pela SEDEPE.

Após a análise dos critérios de impacto e probabilidade, o Encarregado deve avaliar o risco com base na “Matriz de Criticidade” (anexo II).

Caso seja identificado que o incidente acarretou dano ou risco relevante aos Titulares de dados pessoais, o encarregado realizará, com apoio do Jurídico, a notificação para a ANPD e aos Titulares dos Dados Pessoais.

6.3 Comunicação ao encarregado pelo tratamento de dados pessoais da SEDEPE

O conhecimento de um incidente por qualquer membro, servidor efetivo ou comissionado, colaborador ou terceirizado da SEDEPE e do Ministério do Trabalho e Emprego ou por parte interessada deve ensejar uma comunicação ao encarregado pelo tratamento de dados da SEDEPE, com a maior brevidade possível, para as providências previstas na LGPD sobre comunicação de incidentes de segurança.

6.4 Comunicação ao controlador e co-controlador

O Operador deve comunicar incidentes com dados pessoais ao controlador/co-controlador o mais breve possível, a fim de viabilizar que este exerça o seu papel tempestivamente. Conforme disposto no 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, efetuando a comunicação mesmo nos casos em que houver dúvida sobre a relevância dos riscos e danos envolvidos. Ressalta-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, as informações apresentadas excepcionalmente pelo Operador serão devidamente analisadas pela ANPD.

6.5 Comunicação à ANPD e ao titular dos dados pessoais

A ANPD 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 essencial que se elabore um procedimento para potenciais questionamentos.

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:

- Que tipos de dados pessoais foram objeto do incidente?
- O titular de dados pode ser vítima de fraude em razão do incidente?
- O incidente foi devidamente comunicado às autoridades de proteção de dados pessoais?
- O que o titular pode fazer em benefício de sua proteção junto a SEDEPE e contra terceiros?
- 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 da SEDEPE para conferir uma resposta efetiva em incidentes.

Cabe ao Encarregado, diante das informações levantadas internamente e dos parâmetros estabelecidos pela SEDEPE, avaliar a necessidade e a profundidade da comunicação com a Autoridade e com os titulares de dados, pela ANPD ou com base em boas práticas.

A ANPD orienta que as informações prestadas devem ser claras e concisas. Recomenda-se, ainda, que a comunicação contenha as seguintes informações:

1. Data e hora da detecção;
2. Data e hora do incidente e sua duração;
3. Circunstâncias em que ocorreu a violação de segurança de dados pessoais, como perda, roubo, cópia, vazamento, dentre outros;
4. Descrição dos dados pessoais e informações aferradas, como natureza.
5. Conteúdo dos dados pessoais, categoria e quantidade de dados e de titulares aferrados;
6. Resumo do incidente de segurança com dados pessoais, com indicação da localização física e meio de armazenamento;
7. Possíveis consequências e efeitos negativos sobre os titulares dos dados afetados;
8. Medidas de segurança, técnicas e administração preventiva tomadas pelo Controlador de acordo com a LGPD;

9. Resumo das medidas implementadas até o momento para controlar os possíveis danos;
10. Possíveis problemas de natureza transfronteiriça;
11. Outras informações úteis as 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.

Assim, a comunicação preliminar a ser encaminhada à ANPD deverá ser justificada pela SEDEPE e encaminhada no prazo de dois dias úteis e, havendo esclarecimentos adicionais, estes deverão ser prestados em 30 (trinta) dias corridos, contados a partir da comunicação do incidente, e protocolados no mesmo processo da comunicação preliminar aberto junto à ANPD.

Os fatos que impossibilitam a comunicação completa podem decorrer de circunstâncias que incluem violações complexas, as quais requerem investigações detalhadas e ainda estão em fase de apuração do risco oferecido aos titulares em razão do incidente, ou que incluem várias violações semelhantes em um curto período.

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-los. A ANPD também poderá requerer informações adicionais a qualquer momento.

A comunicação à ANPD deve ser clara e concisa, sendo necessário o preenchimento e envio do formulário previsto no link: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis, por meio de Peticionamento Eletrônico – Usuário Externo: https://super.presidencia.gov.br/controlador_externo.php?acao=usuario_externo_logar&acao_origem=usuario_externo_gerar_senha&id_orgao_acesso_externo=0.

Se a violação afetar um grande volume de titulares de dados pessoais, o Encarregado decidirá se uma notificação pública em massa é a mais apropriada, ao invés de uma notificação personalizada/individual.

A decisão de notificação pública em massa ou de forma personalizada/individual deve levar em consideração a quantidade de recursos necessários para notificar cada titular de dados pessoais individualmente, além da capacidade da SEDEPE em fornecer adequadamente aos titulares dos dados pessoais a notificação dentro do prazo especificado.

6.6 Decisão de não notificação

O Encarregado avaliará a relevância do risco ou dano do incidente para determinar se deverá comunicar à ANPD e ao titular. Se for tomada a decisão de não notificar, a justificativa para essa decisão deve ser documentada no Formulário de Registro Interno de Incidente de Segurança com Dados Pessoais (anexo I).

A SEDEPE deve continuar a monitorar as circunstâncias e os efeitos de uma violação. Além disso, à medida que novas informações surgirem, a SEDEPE poderá fazer ou atualizar notificações à ANPD ou comunicações do titular dos dados.

6.7 Comunicação ao Comitê de Proteção de Dados Pessoais (CPDP) da SEDEPE

É necessário que a SEDEPE estabeleça os métodos para realizar comunicação à **Comitê de Proteção de Dados Pessoais (CPDP)**, quando da ocorrência de incidentes de segurança com dados pessoais.

A referida comunicação permite a realização de ações conjuntas durante o tratamento do incidente com dados pessoais e pode ensejar uma resposta mais célere, técnica e eficaz.

6.8 Análise da possibilidade de conciliação direta

O Encarregado, quando da ocorrência de incidente envolvendo dados pessoais, avaliará a possibilidade de conciliação direta com o titular envolvido.

A conciliação direta observará, no mínimo, os princípios da independência, imparcialidade, autonomia da vontade, confidencialidade, oralidade, informalidade e decisão informada, podendo, ainda, incluir outros princípios que estão implícitos dentro do ordenamento jurídico.

Em toda tentativa de conciliação deve ser priorizada a separação das pessoas em relação as controvérsias, com foco nos interesses individuais dos envolvidos e não nas suas posições particulares, além de critérios objetivos para legitimar a viabilização da composição das partes.

Diante da possibilidade de conciliação direta, deverá haver a formalização do acordo, mediante termo elaborado pela Consultoria Jurídica Geral, assinado pelos titulares de dados pessoais envolvidos.

6.9 Elaboração da documentação do incidente

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

- conter as devidas considerações sobre a promoção da melhoria contínua dos processos de tratamento de incidentes;
- estar disponível para consulta em caso de atualização do Relatório de Impacto a Proteção de Dados (RIPD).

A ANPD poderá solicitar esse 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 princípio da responsabilização;
- utilizá-lo como subsídio para eventuais questionamentos, facilitando a comprovação de conformidade.

7. PROCESSO DE RESPOSTA AO INCIDENTE

7.1 Fluxograma do processo de resposta ao incidente (anexo III) Com base no exposto, apresenta-se, a seguir, as etapas do processo de resposta ao incidente com dados pessoais:

7.2 Identificação do incidente

Um novo incidente é notificado por pessoa, externa ou não da SEDEPE ou por alarme de 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-Geral, por exemplo, poderá ser feita por intermédio de formulário eletrônico (disponível no site da SEDEPE), 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 tecnologia da informação, por recebimento de e-mails com links suspeitos ou código malicioso que permite o controle remoto do computador ou dispositivo que o hospeda pelo invasor, entre outras ocorrências suspeitas, como vírus, ataques cibernéticos e outros.

7.3 Notificação

Ao registrar uma notificação de incidente de segurança da informação e privacidade, deve-se inserir as seguintes informações para controle e armazenamento:

• Origem do incidente: unidade, setor ou organização à qual dispositivo ou o processo que originou o incidente pertence;
• Contato da origem: e-mail, telefone ou outro contato disponível do informante do incidente;
• 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 agosto de 2023”);
• Local em que se originou o incidente: endereço IP (IPv4 ou IPv6) do dispositivo ou serviço que originou o incidente;
• 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;

• Endereço do alvo: endereço IP (IPv4 ou IPv6) do dispositivo ou endereço de acesso do serviço que foi o alvo do incidente;

• Protocolos e portas alvos do incidente: especificação do tipo do protocolo (IP, TCP, UDP etc.) e portas utilizados no destino do incidente;

• Serviços envolvidos: especificação do serviço que foi alvo do incidente (http, ftp, smtp etc.) e versões de sistemas utilizados;

• Descrição do incidente: breve descrição do incidente, incluindo, por exemplo, o tipo do ataque, a motivação aparente, ou outras características relevantes;

• Logs ou evidências: anexação das porções de log, imagens, códigos de erro ou outros registros que evidenciem a ocorrência do incidente.

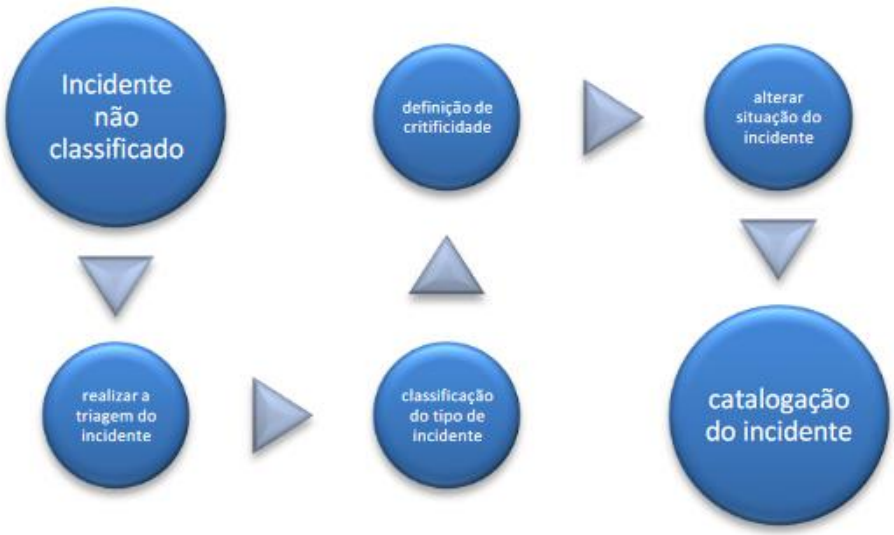
7.4 Registro

Neste momento, o incidente deve ser 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.

7.5 Triagem

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

A seguir, um exemplo de fluxograma desse processo de trabalho:



7.6 Classificação

Classificar o incidente é importante para esclarecer e auxiliar no tipo de atendimento a ser realizado, bem como na definição da sua criticidade.

As classificações sugeridas neste Plano são:

• 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 não categorizado.

7.7 Definição de criticidade

Esta etapa tem como objetivo definir uma ordem de atendimento dos incidentes e um Acordo de Nível de Serviço (Service Level Agreement – SLA), conforme a urgência de tratamento e o impacto nas áreas fim e meio da SEDEPE.

Assim, sugere-se determinar a classificação de criticidade do incidente (Matriz de Criticidade – anexo II) 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 TCE-MT
MÉDIO (IMPACTO SIGNIFICATIVO)	incidente que afeta sistemas ou informações não críticas, sem impacto negativo ao TCE-MT
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

7.8 Definição de situação

É preciso que se defina uma situação para cada incidente, com o objetivo de acompanhar o andamento do evento dentro do processo de tratamento.
Eis a classificação:

• Aberto: nesse momento foi realizado apenas o registro das informações;
• Processamento: o chamado é assumido por um técnico e está em tratamento;
• Pendente: necessário confirmar alguma informação com o solicitante antes de dar prosseguimento. Tentativas de contato devem ser realizadas e registradas;

• Transferido (pendente de terceiros): ocorre quando uma equipe solucionadora não tem ação no chamado, o qual é repassado;

• Solucionado: indica que o procedimento técnico foi aplicado e aparentemente o chamado foi solucionado;

• Fechado: a solução do chamado foi confirmada pelo solicitante. O fechamento pode ocorrer automaticamente ou por contato.

7.9 Preservação das evidências

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.

7.10 Processo de Mitigação

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

7.10.1 Preparação

Na etapa de preparação deve haver o gerenciamento das ferramentas para a análise de incidentes, incluindo o conhecimento de todo o ambiente utilizado. Isso compreende as seguintes ações:

• 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.

7.10.2 Detecção

Na etapa de detecção é feita a identificação do incidente, determinando seu escopo e as atividades envolvidas com ele. Isso compreende as seguintes ações:

• 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.

7.10.3 Contenção

Na etapa de contenção atenua-se os dados, a fim de evitar que outros recursos sejam comprometidos. Isso compreende as seguintes condutas práticas:

• 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 o comprometimento de outros sistemas.

7.10.4 Erradicação

Na etapa de erradicação eliminam-se as causas do incidente, removendo todos os eventos a ele relacionados. Isso compreende as seguintes atividades:

• Garantir que as causas do incidente foram removidas, assim como todas as atividades e arquivos a ele associados;
• 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.

7.10.5 Recuperação

Na etapa de recuperação restaura-se o sistema ao seu estado inicial/normal. Isso compreende as seguintes atividades:

• 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;
• Restaurar o último e íntegro backup completo armazenado.

7.10.6 Avaliação

Na etapa de avaliação são avaliadas as ações realizadas para resolver o incidente, documentando detalhes e lições aprendidas. Isso compreende as seguintes atividades:

• Caracterizar o conjunto de lições aprendidas a fim de 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; e
• Obter informações que podem ser utilizadas em processos legais.

Além disso, temos, ainda, a etapa lições aprendidas, que tem o escopo de avaliar o processo de tratamento do incidente e verificar a eficácia das soluções adotadas.

Por isso, é importante relacionar e documentar, no chamado do incidente, as falhas e os recursos inexistentes ou insuficientes, para que estes 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.

8. OUTRAS RECOMENDAÇÕES NO PROCESSO DE RESPOSTA AO INCIDENTE

a) Definir um plano de comunicação para incidentes de violação de dados. O objetivo desse plano de comunicação é propiciar maior celeridade na solução de incidentes e padronização de atividades a serem executadas, assim como prever responsáveis pelo seu cumprimento;

b) Documentar violações atestadas e incidentes ocorridos, a fim de analisar riscos de violação periodicamente;

c) 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;

d) Promover a gestão adequada dos softwares homologados para uso na SEDEPE. A instalação de software não controlada em dispositivos computadorizados pode introduzir vulnerabilidades e gerar o vazamento de informações, perda de integridade ou outros incidentes de segurança da informação, além da violação de direitos de propriedade intelectual;

e) Identificar os requisitos de segurança da informação usando vários métodos, como requisitos de conformidade oriundos de políticas e regulamentações, modelos de ameaças, análises críticas de incidentes ou o uso de limiares de vulnerabilidade;

f) Convém que os resultados da identificação sejam documentados e analisados criticamente por todas as partes interessadas;

g) Considerar a segurança da informação em cada estágio. Desenvolvimentos de sistemas novos e mudanças nos existentes são oportunidades para a SEDEPE atualizar e melhorar os controles de segurança, levando em consideração os incidentes reais e os riscos de segurança da informação, projetados e atuais.

x x x

REFERÊNCIAS

GOVERNO DE PERNAMBUCO. Secretaria da Controladoria Geral do Estado de Pernambuco – SCGE. https://www.scge.pe.gov.br/lgpd-rede-de-encarregados/

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Comunicação de Incidentes de segurança. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis.

BRASIL. Secretaria de Tecnologia da Informação do TCE/MT.

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.

ANEXO I – FORMULÁRIO DE REGISTRO INTERNO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

PARTE 1 – DESCRIÇÃO DO INCIDENTE	
Preenchimento pelas Secretarias envolvidas	
Data e hora do incidente	
Data e hora de descoberta do incidente	
Local do incidente	
Países afetados	
Nome e contato do servidor responsável por identificar os incidentes	
Descrição de como a ALMT teve ciência do incidente	
Breve descrição do incidente	
Categoria do Titular	
Duração do Tratamento	
Natureza do Incidente	
Evento que desencadeou o incidente	Ex.: incidente cibernético: ransomware, phishing, acesso não autorizado; dados pessoais enviados por engano; dispositivo perdido ou roubado etc.
Detalhes de Sistema, equipamentos, recursos envolvidos no incidente	

Preenchimento pelo Encarregado pelo Tratamento de Dados Pessoais	
Recebido por	
Data de recebimento	
Áreas/Comitês a serem envolvidos	
Data de notificação de envolvimento das demais Áreas	
Possíveis motivos do incidente não ter sido notificado de forma imediata	

PARTE 2 – AVALIAÇÃO DO IMPACTO	
Detalhes de quais dados foram alvo de violação (destruição, alteração indevida, compartilhamento indevido etc.)	
Há dados pessoais sensíveis envolvidas?	

Há dados pessoais de crianças e adolescentes envolvidos?	
Há dados pessoais de idosos envolvidos?	
Abrangência Geográfica	Ex. Nacional, Internacional, Regional.
Quantidade de titulares de dados pessoais afetados	
Disseminação	Ex. limitada a terceiros conhecidos, limitada a terceiros desconhecidos ou ilimitada a terceiros desconhecidos
Natureza do incidente	Perda da confidencialidade, integridade ou disponibilidade
Contexto e finalidade do tratamento	
Perfil do titular	Ex.: servidor, cidadão, prestador
Facilidade da Identificação do Titular	
Existência de agravantes:	Ex.: Danos morais e/ou materiais ocasionados ao titular de dados, em decorrência do incidente identificado; Possibilidade de implicar risco à vida dos titulares, ou efeitos discriminatórios ilícitos ou abusivos; Possibilidade de afetar significativamente o exercício dos direitos dos titulares (considerada a relevância do direito) ou uso do serviço (considerada sua essencialidade); Ausência de fundamento legal para o tratamento de dados pessoais.
Os riscos afetam os direitos fundamentais e a liberdade do titular?	
Quais possíveis danos foram identificados? Ex.: Dano moral, Dano material, Discriminação, dano reputacional	

PARTE 3 – AVALIAÇÃO DA PROBABILIDADE	
Medidas de segurança, técnicas e organizacionais anteriormente implementadas	
Medidas de segurança, técnicas e organizacionais tomadas após a identificação do incidente que serão adotadas para reverter ou mitigar os efeitos do prejuízo do incidente de segurança aos Titulares de dados pessoais	

PARTE 4 – AVALIAÇÃO DOS RISCOS/DANOS AOS TITULARES	
Impacto	**Baixo, Médio, Alto, Muito Alto**
Probabilidade	**Baixa, Média, Alta, Muito Alta**

PARTE 5 – RESULTADO	
Risco	Probabilidade X Impacto = Risco
Necessário notificação para Autoridade Nacional de Proteção de dados? Justifique.	
Necessário notificação para Titulares de Dados Pessoais? Justifique.	
Necessário notificação para outras partes interessadas? Justifique.	
Caso não seja necessário comunicação, justifique.	

PARTE 6 – ASSINATURAS	
Gestor da Área / Unidade estrutural Originária:	
Encarregado pelo Tratamento de Dados Pessoais:	
Data:	

MATRIZ DE CRITICIDADE – ANEXO II

ALTO (IMPACTO GRAVE)	incidente que afeta sistemas relevantes ou informações críticas, com potencial para gerar impacto negativo sobre o TCE-MT
MÉDIO (IMPACTO SIGNIFICATIVO)	incidente que afeta sistemas ou informações não críticas, sem impacto negativo ao TCE-MT
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

ANEXO III FLUXOGRAMA RESPOSTA AO INCIDENTE