PROCEDIMENTOS PARA RESPOSTA À INCIDENTE COM DADOS PESSOAIS

I. CONCEITOS

Nos termos do art. 5º da Lei Geral de Proteção de Dados (LGPD), conceitua-se:

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

b) Operador: a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

c) Encarregado: a 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).

II. IDENTIFICAÇÃO DOS AGENTES E DO ENCARREGADO

Controlador: Universidade Estadual de Ponta Grossa (UEPG)
Operador: Servidores da UEPG
Encarregado: Paulo César Machado Lemos (Portaria R. Nº 2021.450)

III. PROCEDIMENTO DE COMUNICAÇÃO

De acordo com o art. 46 da Lei Geral de Proteção de Dados (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 outra forma de tratamento inadequado ou ilícito.

Ao controlador impõe-se o dever de comunicar à ANPD e ao titular dos dados a ocorrência de incidente de segurança que possa acarretar risco ou relevante dano.

A comunicação deve ser feita em prazo razoável e deve conter:

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;
d) os riscos relacionados ao incidente;
e) os motivos da demora, no caso de a comunicação não ter sido imediata;
f) as medidas que foram ou que estão sendo tomadas para reverter ou mitigar os efeitos do prejuízo.

IV. INCIDENTE

Incidente de segurança é definido como uma violação ou ameaça de violação da política de segurança computacional, política de uso aceitável ou padrões de prática de segurança, conforme o *National Institute of Standards and Technology (NIT)*.

As categorias de violação de segurança a serem consideradas são as seguintes:

a) Material: quando o incidente envolve dados armazenados em dispositivos físicos.
b) Verbal: quando há vazamento de dados de forma verbal, seja por indiscrição (comentários acerca de dados pessoais que são percebidos por terceiros e utilizados em má-fé) ou de forma intencional, repassando indevidamente informações sigilosas.
c) Ciberespaço: quando o incidente está relacionado à Tecnologia da Informação. Nessa categoria enquadram-se o *hackeamento*, mau gerenciamento de *patches*, codificação incorreta, medidas de segurança insuficientes etc.

Para que possa ser avaliado o impacto do incidente, devem ser considerados os seguintes padrões:

a) Risco Baixo: classificação utilizada quando o incidente de segurança de dados afetar apenas dados pessoais, não incluído o número do CPF;
b) Risco Moderado: classificação utilizada quando o incidente de segurança de dados afetar dados pessoais, incluído o número do CPF e/ou, pelo menos, um dado sensível, não incluído raça, religião, nome social e dados de saúde;
c) Risco Alto: classificação utilizada quando o incidente de segurança de dados afetar dados pessoais, incluído o número do CPF e/ou mais que um dado sensível, incluindo raça, religião, nome social e dados de saúde.

V. DESCRIÇÃO DO TRATAMENTO E ESCOPO

O art. 5º, X, da LGPD considera 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”.

A maioria das operações, ou seja, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, armazenamento, eliminação, avaliação ou controle de informação, modificação, comunicação, transferência, difusão ou extração, são por meio de alguma Tecnologia da Informação e Comunicação (TIC). Em casos excepcionais, há ativos de informação por meio físico documental.

A principal tecnologia utilizada que envolve o tratamento de dados é o SEI (Sistema Eletrônico de Informações), desenvolvido pelo Tribunal Regional Federal da 4ª Região. Este possui controle de nível de acesso, havendo gerenciamento na criação e no trâmite de processos e documentos restritos e sigilosos, conferindo acesso somente às unidades envolvidas ou a usuários específicos.

O tratamento para cumprimento de obrigação legal ou regulatória pela Universidade é uma hipótese inerente ao serviço público em geral, ficando assim a Instituição dispensada do consentimento dos titulares para tal.

Destaca-se que perante um incidente de segurança nos ativos digitais e organizacionais, como no SEI, o Controlador e os demais agentes de tratamento de dados

serão autuados por realizar tratamento não condizente com as expectativas dos titulares destes atos, em consonância ao art. 52 da Lei Geral de Proteção de Dados.

O nível de resposta dependerá do tipo de dados e da complexidade do tratamento aplicado.

V.1. PLANEJAMENTO

Nesta fase, se aplicam as ações previamente desenvolvidas que devem ser tomadas frente à detecção ou ao conhecimento de um incidente que possa levar à uma violação de dados pessoais ou de informações institucionais críticas. Estas ações são:

a) Nome e consequência do incidente em relação à Confidencialidade, Integridade, Disponibilidade (CID);
b) Ativo: listar os ativos envolvidos no incidente;
c) Características do incidente;
d) Responsabilidade – gestor responsável pelo ativo envolvido;
e) Ações imediatas – os passos que devem ser executados imediatamente após o conhecimento do incidente pela equipe interna da TI;
f) A criticidade do incidente.

V.2. DESCRIÇÃO DO TRATAMENTO DOS RISCOS

As ações definidas visam ao objetivo principal dos processos dentro do contexto da LGPD, buscando a conformidade com a referida lei. Havendo confirmação de um incidente de segurança, é preciso avaliar rapidamente o risco de propagação da ameaça que o causou.

As ações planejadas devem ser realistas em relação à disponibilidade de recursos humanos, financeiros e de prazo. O responsável pelo processo deve garantir a qualidade das ações definidas, realizando o acompanhamento e as alterações necessárias, sempre que identificadas.

A descrição de cada ação deve ser norteada por uma das 4 categorias, que são:

a) Prevenir: Alterar o processo, deixando de executar a atividade que representa o risco identificado;

b) Transferir/Compartilhar: Transferir parcialmente ou integralmente o risco para terceiros;

c) Mitigar/Melhorar: Reduzir o impacto e/ou a probabilidade de ocorrência do risco para níveis aceitáveis;

d) Aceitar: Definir se a aceitação do risco será de forma passiva, não sendo necessária nenhuma ação, ou ativa, definindo reservas de contingência financeiras, de prazo ou de recursos humanos.

Neste sentido, o tratamento deverá ser realizado observando os seguintes itens:

a) Preservar, na medida do possível, todas as evidências do incidente, para que seja possível rastrear e identificar suas causas posteriormente;
b) Verificar se existe um Plano de Recuperação para o incidente;
c) Agir para que os serviços afetados sejam disponibilizados no menor tempo possível;
d) Utilizar todos os recursos necessários para a contenção do incidente;
e) Utilizar todos os recursos existentes para recuperação de dados e sistemas, como restauração através backups;
f) Avaliar o risco aos titulares de dados pessoais e, se necessário, comunicar o incidente à Autoridade Nacional de Proteção de Dados (ANPD) e aos próprios titulares que tiveram seus dados violados.

VI. CONTENÇÃO E ERRADICAÇÃO

Após um incidente ser identificado como uma violação de segurança, ele deverá ser contido para evitar que outros sistemas sejam afetados ou que ocasionem danos maiores.

Além disso, devem ser previstas ações para a contenção de curto prazo, *backup* do sistema e contenção a longo prazo.

Durante a contenção, deve haver o registro do incidente e das medidas de contenção que foram adotadas, evitando ao máximo a perda de evidências e as provas do ocorrido. É importante lembrar da necessidade de trabalho colaborativo de toda a Instituição.

Após a ameaça ter sido contida, é necessário proceder com a sua remoção e a restauração dos sistemas que foram afetados, de modo que voltem a operar em sua normalidade, devendo haver varredura para identificar as perdas ocorridas e como recuperar o que foi perdido.