Privacidade e Proteção de Dados

Ameaça, ataques e a LGPD

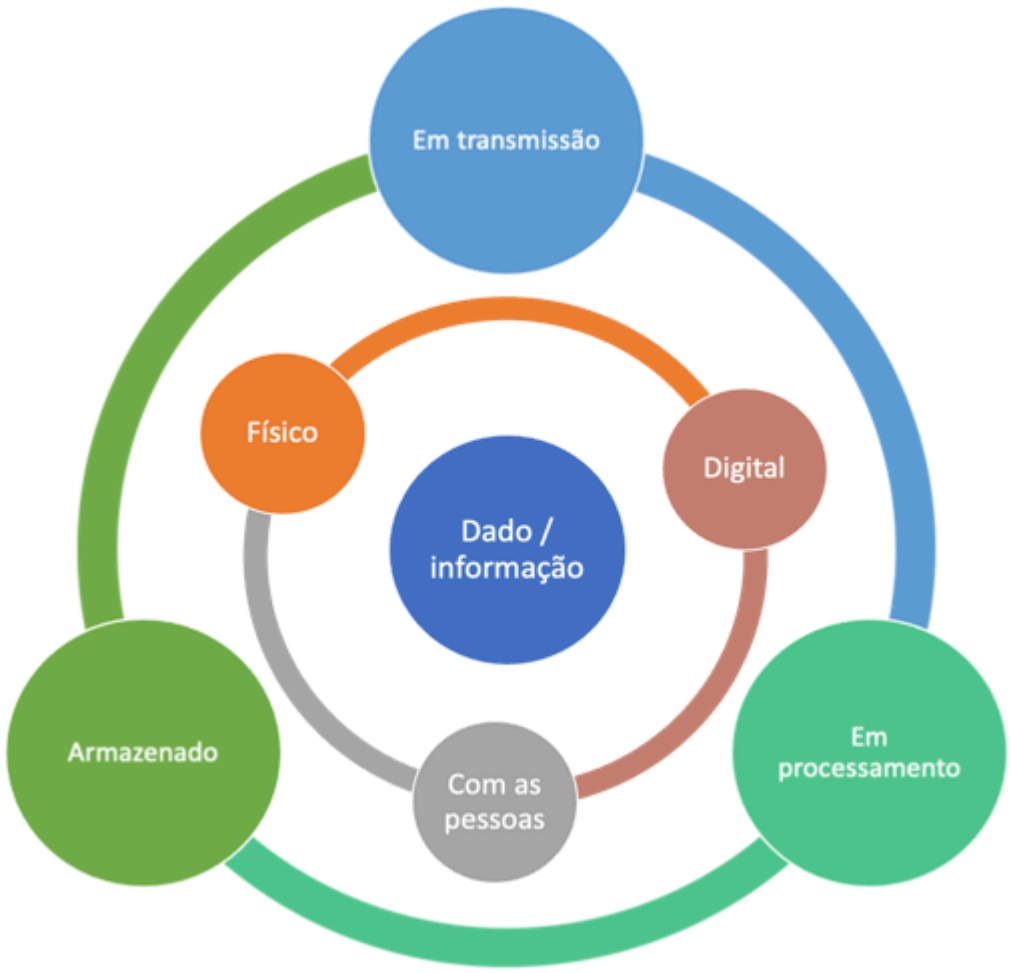
Você sabia que seu material didático é interativo e multimídia? Isso significa que você pode interagir com o conteúdo de diversas formas, a qualquer hora e lugar. Na versão impressa, porém, alguns conteúdos interativos ficam desabilitados. Por essa razão, fique atento: sempre que possível, opte pela versão digital. Bons estudos!

Nesta webaula, entenderemos a abrangência necessária para a proteção de dados pessoais, partindo das diferentes formas que os dados podem existir e as formas que eles podem ser obtidos de forma maliciosa.

Formas dos dados e estados dos dados digitais

Com a LGPD, precisamos proteger os dados pessoais. E onde estão esses dados pessoais, quais são as suas formas e seus estados?

Formas dos dados e estados dos dados digitais



Fonte: elaborada pelo autor.

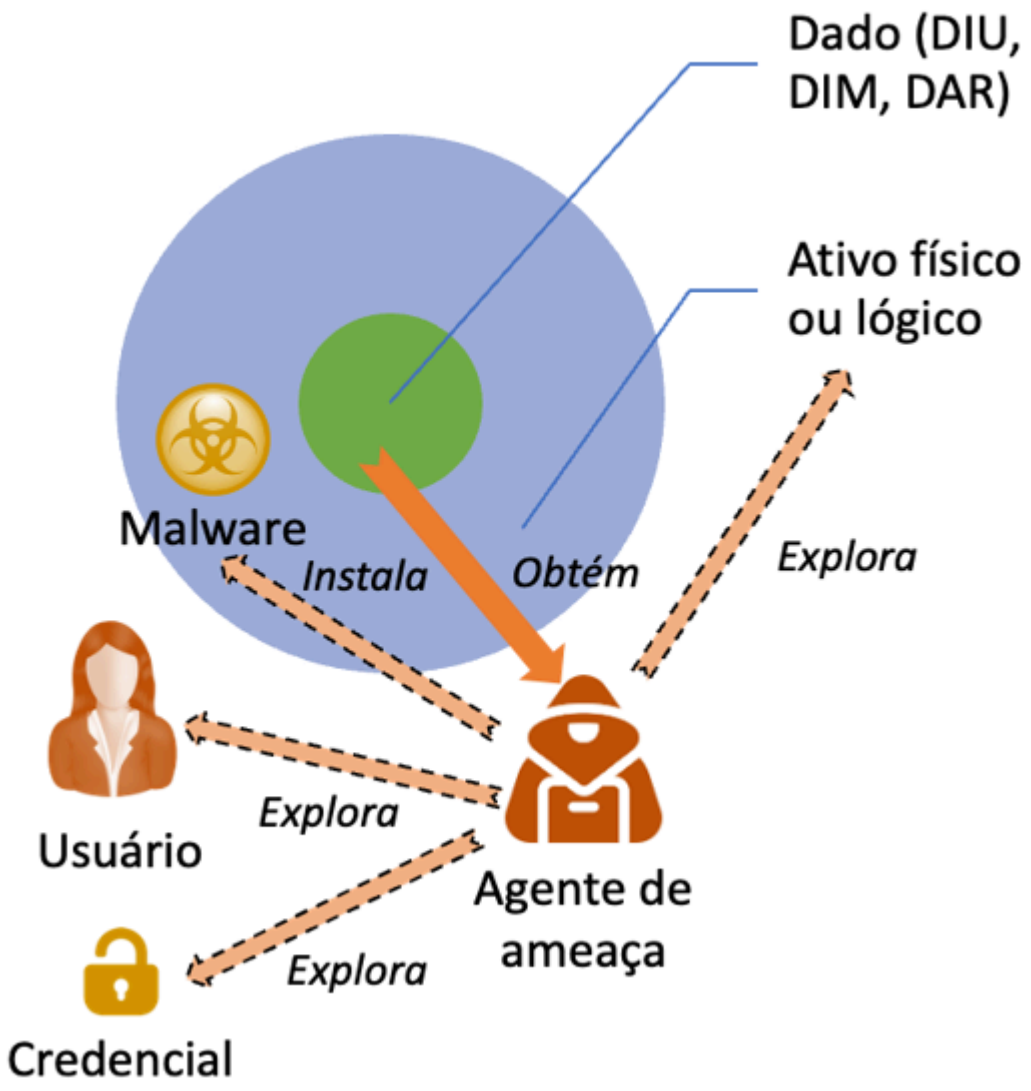
Os dados pessoais podem existir em meio físico (como em papel), em meio digital (como em um banco de dados), ou na cabeça das pessoas. Precisamos mapear esses dados em todas as suas formas para que possam ser protegidos.

Os dados em meio digital podem estar em três estados diferentes:

- Em processamento, ou Data-In-Use (DIU).
- Em transmissão, ou Data-In-Motion (DIM).
- Em armazenamento, ou Data-At-Rest (DAR).

Isso significa que os dados pessoais podem sofrer incidentes de segurança nesses estados (DIU, DIM, DAR). No contexto da LGPD, o principal incidente de segurança é o vazamento dos dados pessoais. Mas qualquer ataque cibernético pode levar ao vazamento de dados, já que há uma escalada dos acessos ou uma movimentação lateral que pode levar ao acesso indevido aos dados pessoais.

Anatomia de um vazamento de dados pessoais



Fonte: elaborada pelo autor.

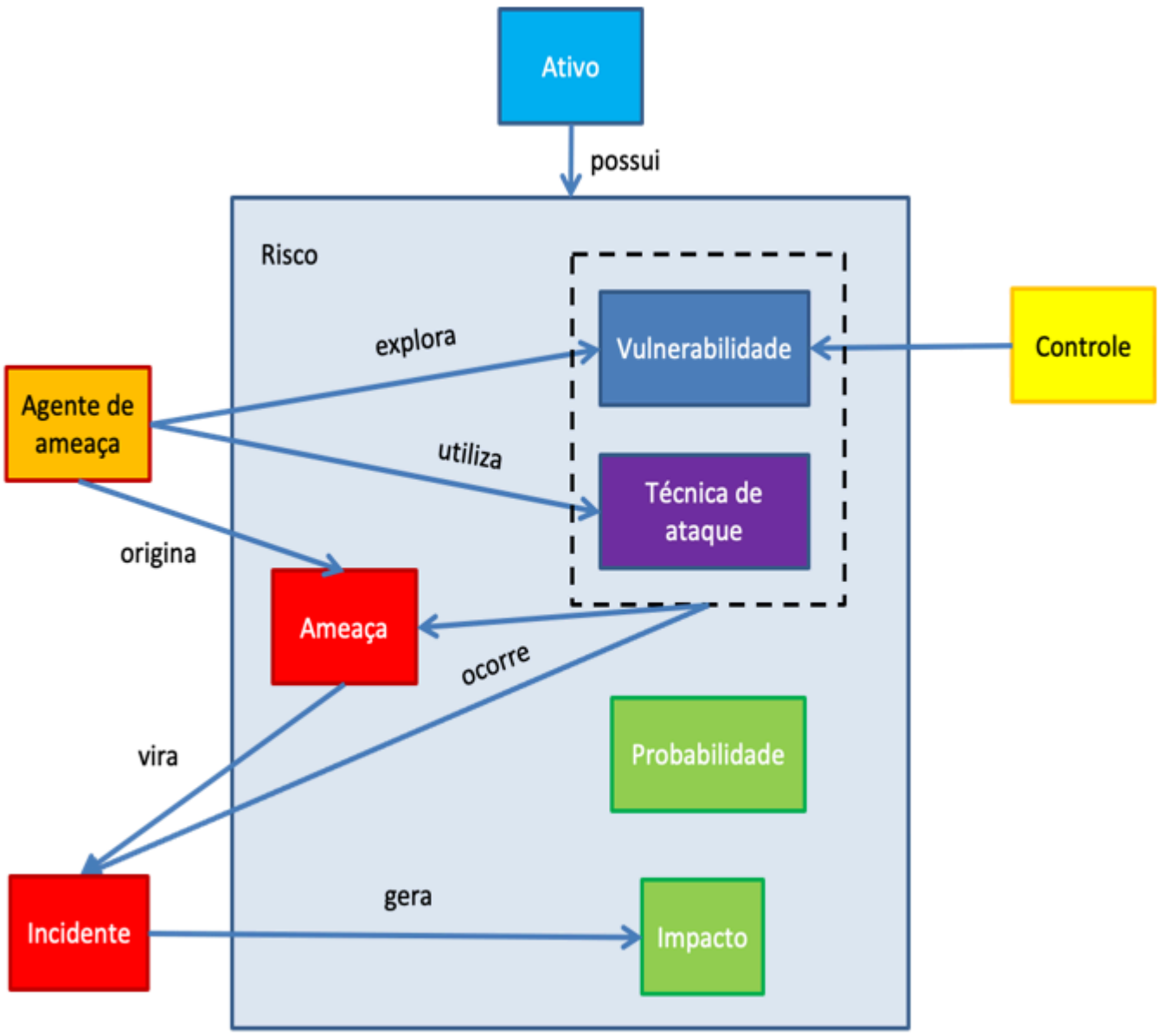
Um agente de ameaça pode vazar dados pessoais a partir de um conjunto de possibilidades:

1. Explorar um ativo físico ou lógico que processa, armazena ou transmite dados pessoais, realizando um ataque cibernético direto.
2. Explorar um usuário, via engenharia social, por exemplo, e instalar um *malware* que realiza a exfiltração de dados pessoais.
3. Explorar uma credencial de usuário, acessar um serviço e ir se movimentando no sistema até que se chegue aos dados pessoais.

Ameaças, ataques e vulnerabilidade

Qual a diferença entre ameaças, ataques e vulnerabilidades? No contexto da privacidade e proteção de dados pessoais, uma ameaça é algo que pode ocorrer com um dado pessoal, como um vazamento. E um vazamento é ameaça que pode se tornar um incidente de segurança, quando um agente de ameaça explora vulnerabilidades de um ativo utilizando uma técnica de ataque. O risco é o cálculo da probabilidade e do impacto envolvido com cada situação relacionada com a ameaça.

Elementos do risco



Fonte: elaborada pelo autor.

A principal ameaça relacionada com a privacidade e dados pessoais é o vazamento ou exfiltração de dados ou data exfiltration. A exfiltração de dados pode ser feita com a exploração de vulnerabilidades e uso de técnicas de ataques pelo agente de ameaça.

A rede pode ser explorada com o sniffing, que captura os dados em trânsito.

O ataque do homem do meio e o ARP spoofing direciona o tráfego ao atacante, que pode então vazar dados pessoais.

Com o DNS spoofing, o atacante manipula o serviço de resolução de nomes da internet para que a vítima acesse sites falsos e entregue seus dados pessoais.

E o phishing explora a engenharia social para ludibriar usuários para entregar seus dados pessoais ou instalar malwares que realizam a exfiltração de dados.

> A engenharia social também é um dos principais vetores de ransomwares, que além de tornarem os dados indisponíveis com a criptografia, realizam a exfiltração de dados, podendo, assim, comprometer a confidencialidade e a privacidade dos usuários.

A LGPD prevê as seguintes sanções administrativas aplicáveis pela autoridade nacional (BRASIL, 2018, [s.p.]):

> “
>
> I. advertência, com indicação de prazo para adoção de medidas corretivas;
>
> II. multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
>
> III. multa diária, observado o limite total a que se refere o inciso II;
>
> IV. publicização da infração após devidamente apurada e confirmada a sua ocorrência;
>
> V. bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
>
> VI. eliminação dos dados pessoais a que se refere a infração;
>
> X. suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
>
> XI. suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
>
> XII. proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.
>
> — (BRASIL, 2018, [s.p.]).
>
> ”

Uma observação é que as sanções de VII a IX foram vetadas.

E um ponto relevante é que as sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios (BRASIL, 2018, [s.p.]):

> “
>
> I. a gravidade e a natureza das infrações e dos direitos pessoais afetados;
>
> II. a boa-fé do infrator;
>
> III. a vantagem auferida ou pretendida pelo infrator;
>
> IV. a condição econômica do infrator;
>
> V. a reincidência;
>
> VI. o grau do dano;
>
> VII. a cooperação do infrator;
>
> VIII. a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados;
>
> IX. a adoção de política de boas práticas e governança;
>
> X. a pronta adoção de medidas corretivas; e
>
> XI. a proporcionalidade entre a gravidade da falta e a intensidade da sanção.
>
> — (BRASIL, 2018, [s.p.]).
>
> ”

Para finalizar esta webaula, é importante saber que além das vulnerabilidades e ataques que foram vistos nesta seção, OLIVEIRA (2017) apresenta os principais ataques lógicos que uma rede pode sofrer, incluindo o DNS *spoofing*, no Capítulo 4 de Segurança em Redes de Computadores.

OLIVEIRA, R. C. Q. **Segurança em Redes de Computadores**. São Paulo: Editora Senac São Paulo, 2017.