Privacidade e Proteção de Dados

Privacidade e proteção de dados na nuvem

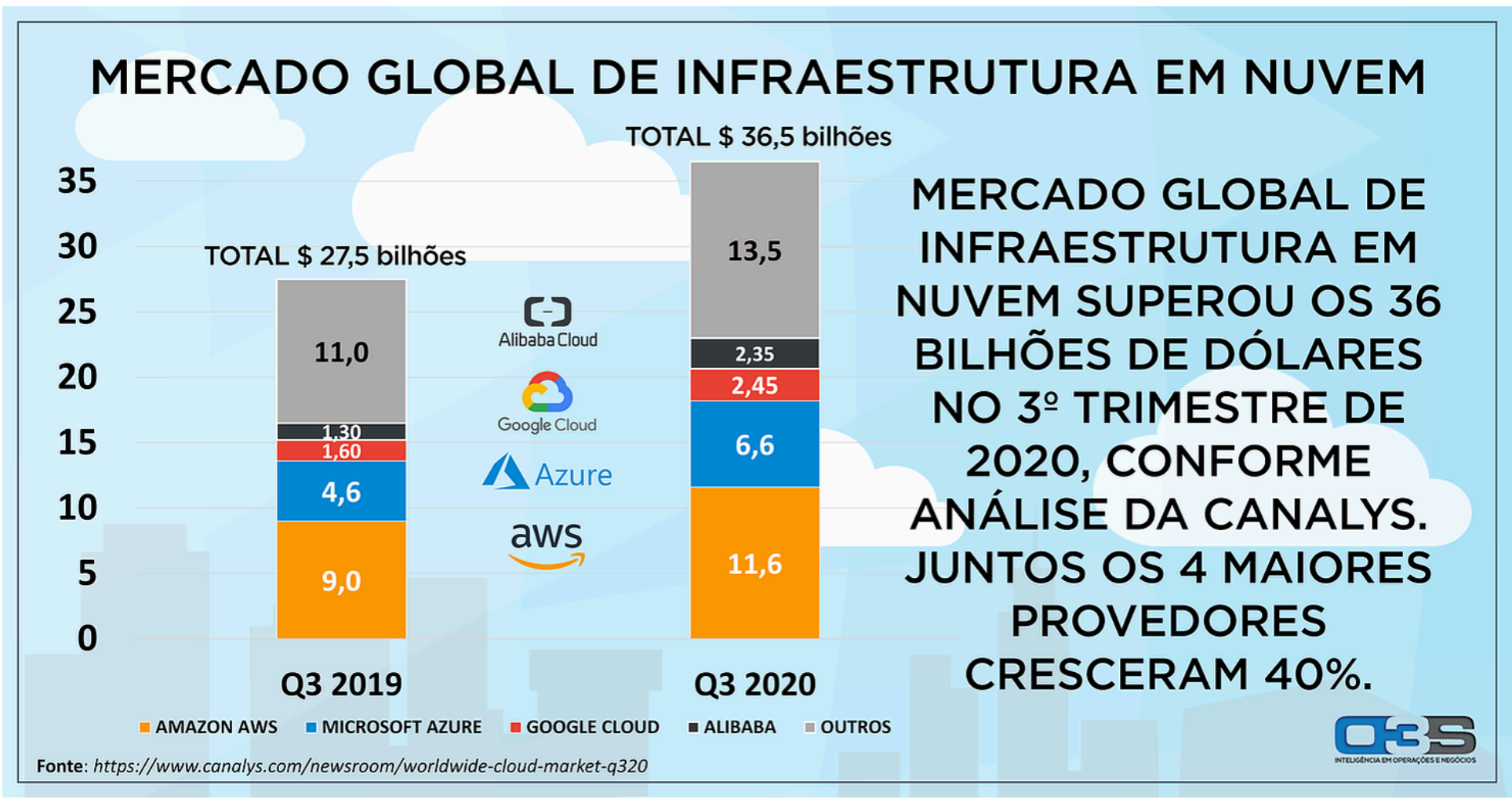
Você sabia que seu material didático é interativo e multimídia? Isso significa que você pode interagir com o conteúdo de diversas formas, a qualquer hora e lugar. Na versão impressa, porém, alguns conteúdos interativos ficam desabilitados. Por essa razão, fique atento: sempre que possível, opte pela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

Nesta webaula, estudaremos os principais elementos para a privacidade e proteção de dados em nuvem, que vem sendo cada vez mais utilizado pelas empresas.

Privacidade e proteção dados em nuvem

O uso de serviços de nuvem vem crescendo em todo o mundo. Em 2020, os quatro maiores provedores globais de infraestrutura em nuvem (Infrastructure as a Service, IaaS) cresceram 40% comparado com o mesmo trimestre de 2019, em um mercado que atingiu US$ 36,5 milhões.

Dados (DIU, DIM e DAR) existem em ativos físicos ou lógicos



Fonte: Fonte: Mercado... (2021, [s.p.]).

Quando os sistemas e os dados estão em provedores em nuvem, definir as responsabilidades (que são das empresas ou dos provedores, dependendo do modelo utilizado) é fundamental. Veremos a seguir mais sobre esses modelos.

On premises

No modelo *on premises*, que é o tradicional em que a empresa possui um datacenter, a responsabilidade de todos os elementos é da própria empresa: aplicações, dados, execução (*runtime*), *middleware*, sistema operacional (O/S), virtualização, servidores, armazenamento (storage) e redes.

Software as a *Service* (*SaaS*)

No modelo *Software* as a *Service* (SaaS), o fornecedor ou provedor do software como serviço é o responsável por toda a segurança daquele software.

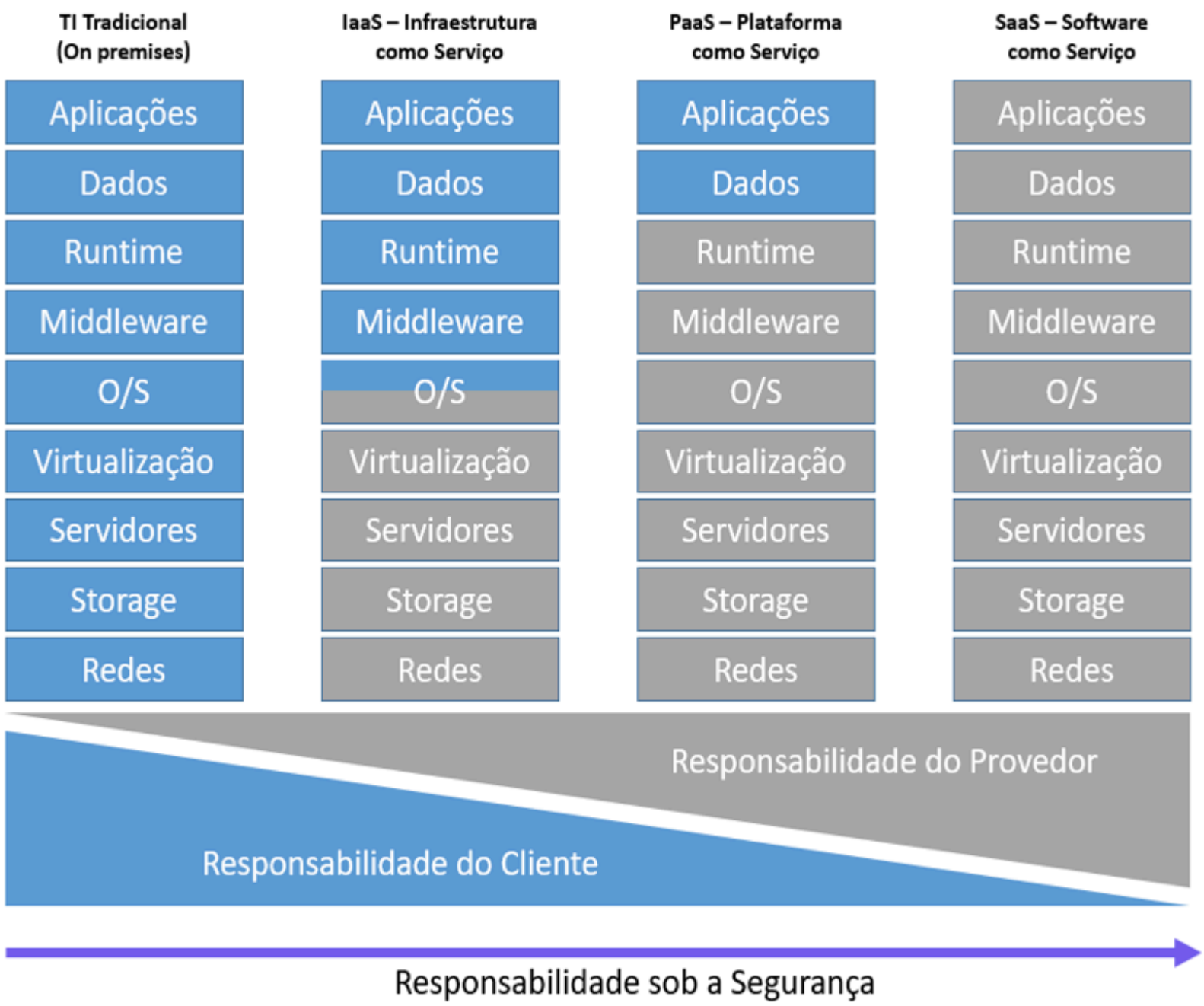
Plataform as a *Service* (*PaaS*)

No modelo *Platform* as a *Service* (PaaS), o que o fornecedor ou provedor oferece é a plataforma de computação, com a aplicação e os dados sendo de responsabilidade da empresa. Nesse caso, os sistemas operacionais e o *middleware* são de responsabilidade do provedor.

Infrastructure as a *Service* (*IaaS*)

No modelo *Infrastructure* as a *Service* (IaaS), a empresa contrata a infraestrutura como serviço, o que inclui as redes, armazenamento, virtualização e parte do sistema operacional. A empresa deve, nesse caso, cuidar da segurança do sistema operacional, *middleware*, ambiente de execução, dados e aplicações.

Responsabilidades de segurança em diferentes ambientes



Fonte: Os 6...([s.d.], [s.p.]).

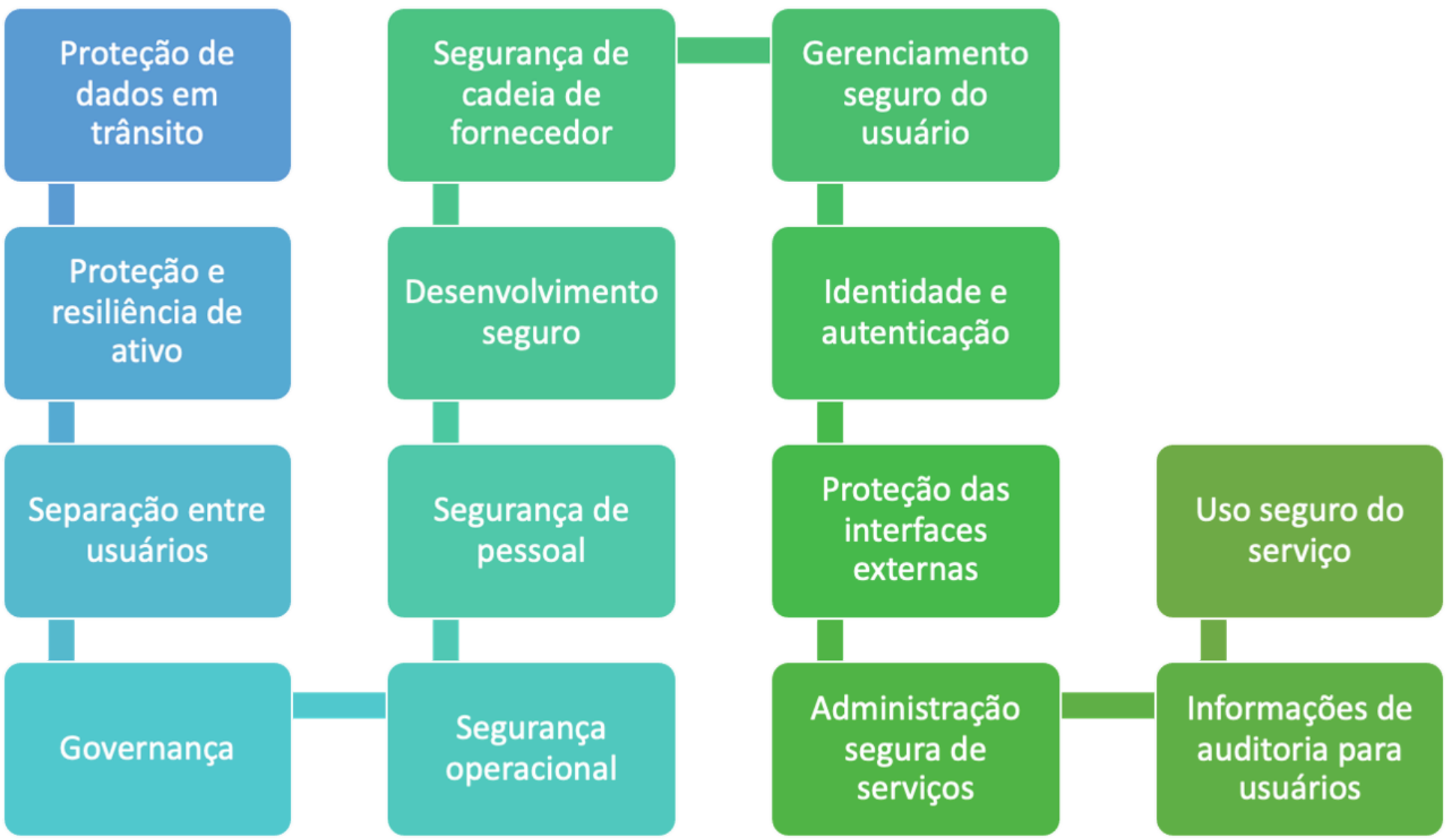
Princípios da segurança em nuvem

Segundo a National Cyber Security Centre (NCSC, [s.d.], [s.p.]), do Reino Unido, os princípios da segurança em nuvem envolvem a proteção dos dados, e são:

1. Proteção de dados em trânsito, principalmente contra alteração e espionagem na rede.
2. Proteção e resiliência de ativo, incluindo dados e ativos que armazenam ou processam os dados, contra adulteração física, perda, dano ou captura.
3. Separação entre usuários, de modo que um usuário comprometido não afete o outro.

4. Governança, para coordenar e direcionar o gerenciamento do serviço e das informações relacionadas.
5. Segurança operacional, que gerencia o serviço para impedir, detectar ou prevenir ataques.
6. Segurança de pessoal, incluindo treinamento e triagem para reduzir as chances de incidentes acidentais ou maliciosos do pessoal do provedor de serviços.
7. Desenvolvimento seguro, com identificação de ameaças e mitigação de riscos que podem comprometer os dados, causar problemas no serviço ou permitir outras atividades maliciosas.
8. Segurança de cadeia de fornecedor, assegurando que todos cumpram a implementação da segurança.
9. Gerenciamento seguro do usuário, com ferramentas para o gerenciamento seguro do serviço, prevenindo acessos não autorizados e alteração de recursos, aplicações e dados.
10. Identidade e autenticação em todos os acessos aos serviços.
11. Proteção das interfaces externas, que devem ser identificadas e protegidas adequadamente.
12. Administração segura de serviços, que possuem acessos privilegiados que resultam em grandes impactos em caso de comprometimento.
13. Informações de auditoria para usuários, monitorando os acessos aos serviços e aos dados relacionados.
14. Uso seguro do serviço, com reponsabilidade.

Responsabilidades de segurança em diferentes ambientes



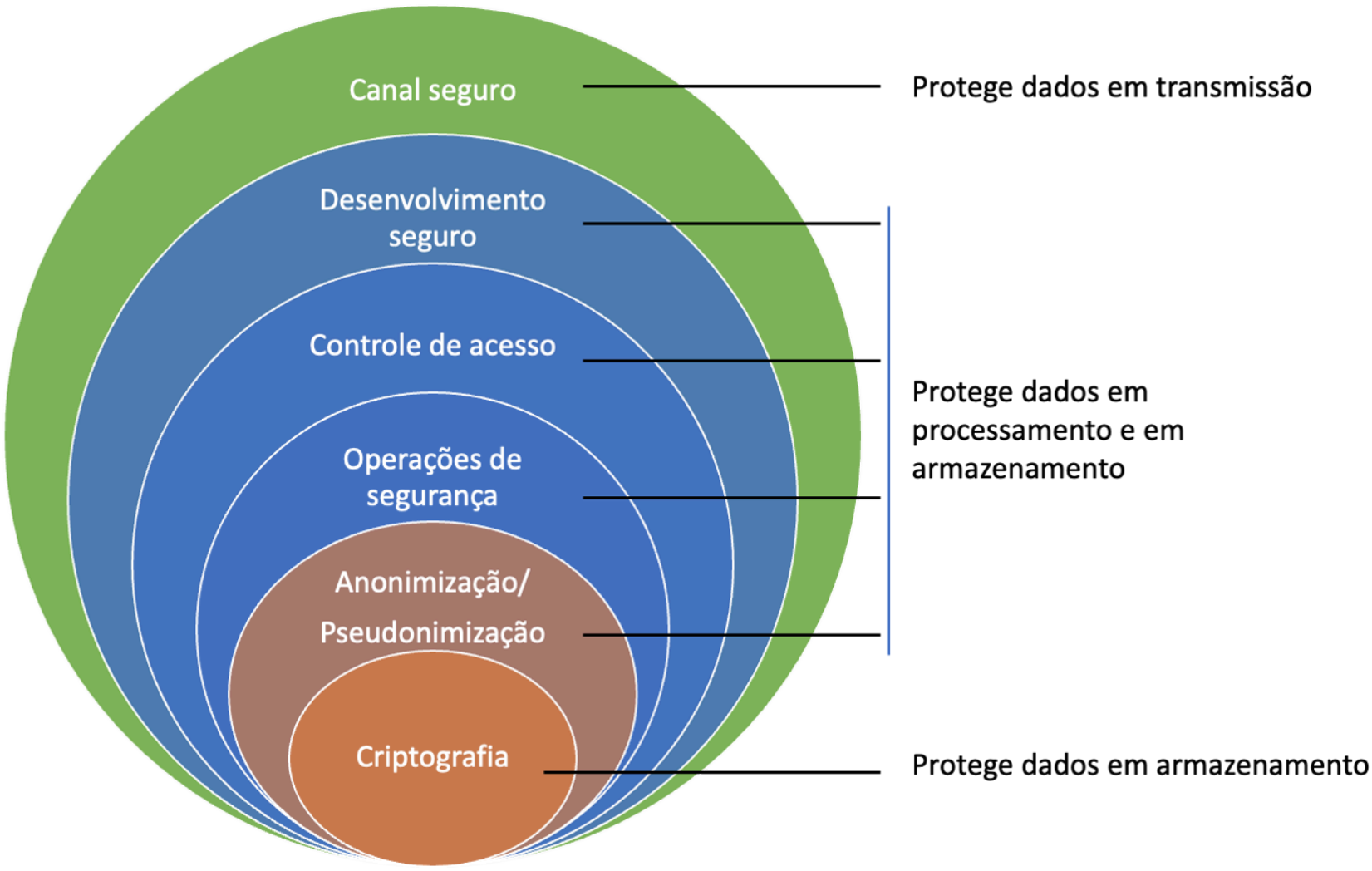
Fonte: Os 6...([s.d.], [s.p.]).

Segurança em camadas

A segurança em camadas é uma abordagem que deve ser adotada com múltiplas camadas de proteção que dificultem o vazamento dos dados. No exemplo, o canal seguro protege os dados em transmissão, enquanto o desenvolvimento seguro, controle de acesso e operações de segurança podem ser adotados em todos os componentes do sistema, protegendo, assim, os dados em processamento e em armazenamento. No caso de um ataque ao sistema, o atacante terá acesso aos dados. No entanto, uma camada adicional de segurança é o uso de

anonimização e pseudonimização, que faz com que os dados acessados não possam ser correlacionados a uma pessoa natural, o que protege a privacidade dos usuários. Contudo, como há técnicas para que a correlação seja refeita, a criptografia pode ser usada como uma camada adicional de segurança.

Exemplos de segurança em camadas

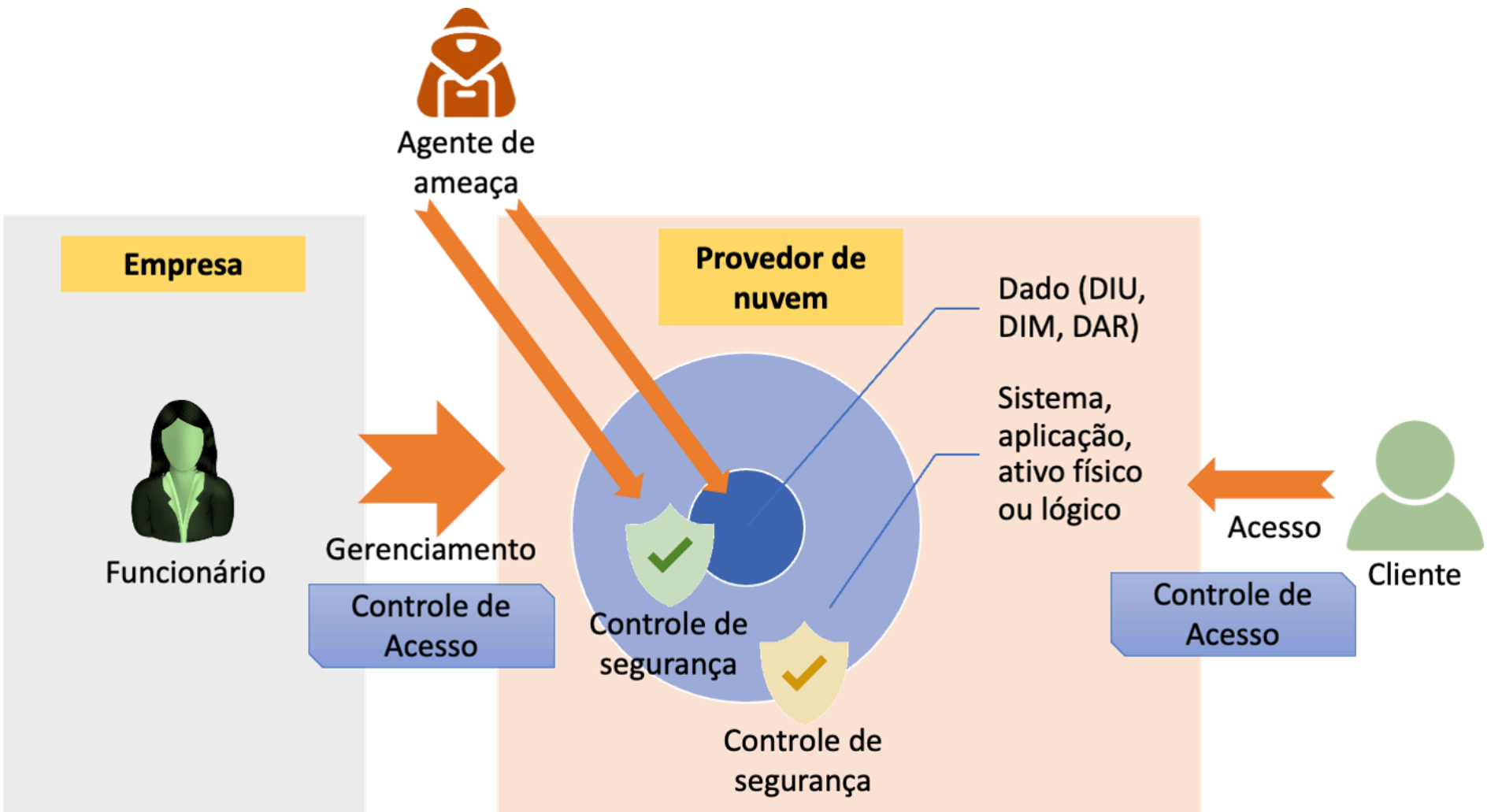


Fonte: elaborada pelo autor.

Quando um agente de ameaça obtém a senha de um usuário ou de um administrador de sistemas (conforme ilustrado a seguir), ele começa a se passar pela vítima, podendo realizar uma série de ações, tais como:

- Ler, exfiltrar, modificar ou remover dados.
- Administrar os recursos da nuvem com as funções de plano de controle e gerenciamento.
- Acessar dados em transmissão.
- Disseminar *malwares*.

Controle de acesso na nuvem



Fonte: elaborada pelo autor.

Criptografia

A criptografia é uma das principais medidas de segurança para a segurança de dados. Ela pode ser aplicada em diferentes níveis, e deve ser avaliada de acordo com cada caso de uso:

- No banco de dados, de modo a proteger os dados armazenados.
- No serviço ou aplicação, de modo que os dados cheguem ao banco de dados já cifrados. O gerenciamento de chaves é feito pelo serviço ou aplicação.
- Pelo usuário, de modo que os dados cheguem ao banco de dados já cifrados. O gerenciamento de chaves é de responsabilidade do usuário.

Para finalizar esta webaula, destacamos que Vazamentos de dados pessoais, como o de 223 milhões de CPFs de brasileiros, tem aumentado em todo o mundo, e também no Brasil. Como é a responsabilização pelos danos causados aos titulares dos dados vazados, a relação com a LGPD? (VEIRANO ADVOGADOS, 2021).

VEIRANO ADVOGADOS. Vazamentos de dados aumentaram 493% no Brasil, segundo pesquisa do MIT. Você S/A, 24 fev. 2021.

Para visualizar o vídeo, acesse seu material digital.