NÃO PODE FALTAR

ARMAZENAMENTO DE DADOS

Emilio Tissato Nakamura

O VALOR DA INFORMAÇÃO E SUA PROTEÇÃO

Em um mundo interconectado, a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações, são informações que, como outros ativos importantes, têm valor para o negócio da organização e, consequentemente, requerem proteção contra vários riscos (ISO 27002, 2013).

Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

PRATICAR PARA APRENDER

Olá, aluno, nesta seção você irá se aprofundar na proteção de dados, partindo do entendimento entre o dado e a informação. Entender os dados é importante porque eles são armazenados em ativos de TI, e são a base para a informação, que por sua vez é a base para o conhecimento. Como têm valor, devem ser protegidos. E a proteção não é simples, já que os dados e a informação existem em meios físicos, como no papel, em meios digitais, como em banco de dados e, ainda, na cabeça das pessoas. Para tornar a vida do profissional de segurança e privacidade mais complexa ainda, os dados e a informação existem em estados diferentes: em transmissão, em processamento ou em armazenamento.

Com a Lei Geral de Proteção de Dados Pessoais, a LGPD, o entendimento sobre estes aspectos ganha ainda mais importância. O foco da LGPD é nos dados pessoais, mas o que você irá ver aqui se aplica também a outros tipos de dados, como os confidenciais e secretos.

E a proteção dos dados vai além do uso da criptografia, a qual apresenta vários desafios de aplicação, principalmente com relação à gestão de chaves criptográficas, que podem estar com o usuário, com a aplicação ou com o banco de dados. Além da criptografia, há mecanismos como a anonimização, pseudonimização e mascaramento de dados. E o ciclo de vida dos dados e da informação é um aliado importante para que você possa proteger da melhor forma possível a sua empresa.

Outro aspecto importante é que cada vez mais os dados estão distribuídos, e os provedores de serviços de nuvem têm um papel importante neste contexto. Já vimos que as responsabilidades de segurança mudam de acordo com o tipo de serviço contratado dos provedores de nuvem. E isto precisa ser reforçado.

Uma empresa com foco em energias renováveis é composta por uma matriz em Natal, no Rio Grande do Norte, e filial em Belo Horizonte, em Minas Gerais. O desenvolvimento de novas tecnologias é feito por uma

equipe que fica em Santiago, no Chile. Há laboratórios conectados em Belo Horizonte e Santiago. A empresa tem projetos com militares argentinos, o que exige um alto nível de segurança, já que envolve aspectos de segurança nacional.

A empresa tem um diretor de segurança da informação, que é o responsável por uma estrutura que inclui uma gerência de governança de segurança, uma gerência de tecnologias de segurança e outra gerência de processos de segurança.

Você é o gerente de processos de segurança, e deve trabalhar em sinergia com os outros dois gerentes para alinhar os planos e atividades de segurança da informação da empresa.

O diretor de segurança da informação da empresa solicitou um status de alguns aspectos de armazenamento de dados da empresa, principalmente aqueles relacionados com a Lei Geral de Proteção de Dados Pessoais (LGPD). Você deve preparar uma apresentação, então, com as informações solicitadas.

Estruture sua apresentação com os seguintes tópicos:

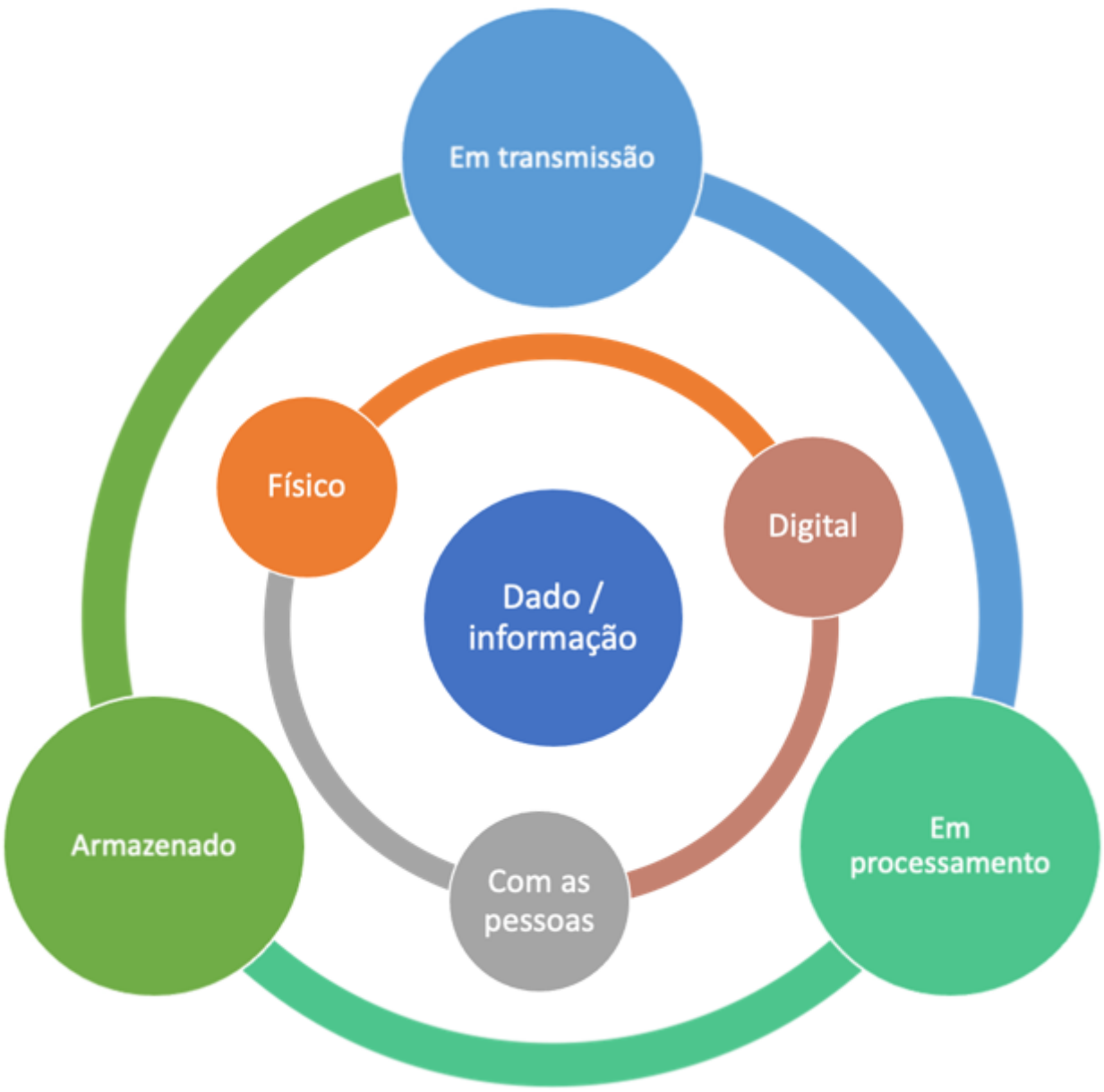
1. Tratamento de dados pessoais.
2. Controles de segurança para proteção dos dados pessoais.
3. Uso de provedores de nuvem.

A proteção de dados é cada vez mais importante para você. Com os dados pessoais, você, como cidadão, precisa ter a sua privacidade preservada e a LGPD cumprida pelas empresas com as quais você se relaciona. Você deve exigir isto das empresas. E para você como profissional, porque as empresas precisam adequar seus sistemas e processos para proteger os dados e as informações, incluindo as confidenciais e sigilosas, sem deixar de lado as pessoas, já que a segurança e privacidade são de responsabilidade de todos. Vamos estudar os elementos importantes neste contexto.

CONCEITO-CHAVE

Caro aluno, nesta seção, você conhecerá diferentes aspectos da segurança de dados, principalmente daqueles que estão armazenados. Pode-se considerar que a segurança da informação se aplica na segurança de dados, e a diferença está na especificidade do que está sendo protegido. O que você deve conhecer é que os dados e a informação estão em fluxo constante e existem em diferentes estados: a transmissão, o processamento, o armazenamento. Estão em meio físico, em meio digital e, ainda, na cabeça das pessoas. A Figura 2.23 resume os dados e informações que fluem o tempo todo. E os dados e as informações precisam de segurança em todo este fluxo que envolve seus diferentes estados e meios em que existem, conforme o momento.

Figura 2.23 | Dados e informação fluem



Fonte: elaborada pelo autor.

DADOS, INFORMAÇÃO, CONHECIMENTO

Segundo Zeferino (2018), os dados são registros que servem como matéria-prima para a construção da informação e do conhecimento, por meio da análise, manipulação e processamento de dados. A informação

é a estruturação e organização de dados, ou seja, ela é o resultado da aplicação de contexto aos dados, necessário para compreender determinado assunto em específico. O objetivo da informação é de esclarecer e reduzir incertezas, a fim de levar ao conhecimento e sabedoria. Já o conhecimento é a informação processada e transformada. Também é resultado de aprendizagem que ocorre quando somos expostos a diversas informações novas, que alteram nosso comportamento e relacionamento com o que está a nossa volta. Em outras palavras, a informação são os dados processados sobre algo ou alguém, e o conhecimento é um conjunto de informações úteis que foram adquiridas por meio de aprendizados e experiência (ZEFERINO, 2018).

A norma ABNT NBR ISO/IEC 27002 coloca o contexto de que as organizações de todos os tipos e tamanhos (incluindo o setor privado e público, organizações comerciais e sem fins lucrativos), coletam, processam, armazenam e transmitem informações em diferentes formatos, incluindo o eletrônico, físico e verbal (por exemplo, conversações e apresentações) (ISO 27002, 2013).

Além disso, segundo a norma, o valor da informação vai além das palavras escritas, números e imagens: conhecimento, conceitos, ideias e marcas são exemplos de formas intangíveis da informação. Em um mundo interconectado, a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações, são informações que, como outros ativos importantes, têm valor para o negócio da organização e, consequentemente, requerem proteção contra vários riscos (ISO 27002, 2013).

DADOS PESSOAIS, DADOS PESSOAIS SENSÍVEIS, DADOS CONFIDENCIAIS

A Lei nº 13.709, Lei Geral de Proteção de Dados Pessoais (LGPD), visa proteger os dados pessoais. Segundo a LGPD, dado pessoal é a informação relacionada a pessoa natural identificada ou identificável

(BRASIL, 2020). Um outro tipo de dado importante definido na LGPD e que requer um nível de proteção maior é o dado pessoal sensível, que é o 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 (BRASIL, 2020). Ou seja, o dado sensível é aquele que discrimina uma pessoa ou indivíduo e pode ser utilizado contra ele ou contra a sua reputação.

É importante você diferenciar dados pessoais, que dizem respeito ao indivíduo, de dados confidenciais, que envolvem também dados de empresas. Os dados e informações confidenciais são definidos com a classificação da informação, que iremos discutir ainda nesta seção. Uma informação confidencial é aquela que, se divulgada tem um impacto significativo nas operações ou nos objetivos táticos da empresa e, portanto, pode ser acessado somente por um grupo de pessoas.

ESTADO DOS DADOS EM MEIOS DIGITAIS: DIU, DAR, DIM

Os dados em meios digitais existem em três estados (Figura 2.24).

Figura 2.24 | Estados dos dados

Fonte: elaborada pelo autor.

Dados transmitidos, seja em redes sem fio ou em qualquer tipo de conexão, incluindo a internet, são conhecidos com *Data-In-Motion* (DIM). Estes dados podem ser comprometidos durante a transmissão, o que pode comprometer a sua confidencialidade, integridade ou disponibilidade.

> **EXEMPLIFICANDO**
>
> Um usuário pode acessar um serviço pela internet, via navegador. O caminho dos dados inseridos pelo usuário em seu dispositivo, até chegar ao servidor que executa o serviço, na nuvem ou no datacenter da empresa, é composto por uma série de pontos que podem levar ao ataque cibernético. Há riscos envolvidos com uma rede Wi-Fi, o provedor *internet* do usuário e o link internet da empresa. Equipamentos de rede vulneráveis podem ser explorados nestes ataques, ou caso os dados sejam transmitidos em claro, podem ser acessados indevidamente ou mesmo modificados. O controle de segurança mais comum que deve ser utilizado pelo provedor de serviço é o uso de um canal seguro *Hyper Text*

Transfer Protocol Secure (HTTPS), que protege as conexões *Hyper Text Transfer Protocol* (HTTP) com o *Transport Layer Security* (TLS).

Já os **dados em processamento** são conhecidos como *Data-In-Use* (DIU), que realizam as transformações dos dados necessários para as operações e possibilitam as interações necessárias entre o usuário e o serviço. Há um espaço limitado de oportunidade para que ataques cibernéticos aconteçam com o DIU, já que as aplicações realizam as operações necessárias e os dados continuam o seu fluxo, normalmente para o armazenamento.

EXEMPLIFICANDO

Dados em processamento existem nas aplicações e em outros ativos como sistema operacional e protocolos. Há uma intensa interação entre esses elementos computacionais quando um dado está em processamento, envolvendo ainda ativos físicos como a memória RAM e a memória virtual, que podem conter dados relevantes e são alvos naturais de ataques cibernéticos. Um dos principais controles de segurança para evitar incidentes envolvendo DIU é o desenvolvimento seguro, que vimos na seção anterior. Porém, na prática, o que protege o DIU é o conjunto de controles de segurança, envolvendo gestão de vulnerabilidades, gestão de identidades e controle de acesso, por exemplo.

Os **dados armazenados**, conhecidos como *Data-At-Rest* (DAR), têm uma grande exposição aos agentes de ameaça, e recebem grande parte da atenção de segurança. Porém, é preciso entender que para que um atacante chegue aos dados armazenados, é preciso passar pelos ativos que estão custodiando os dados.

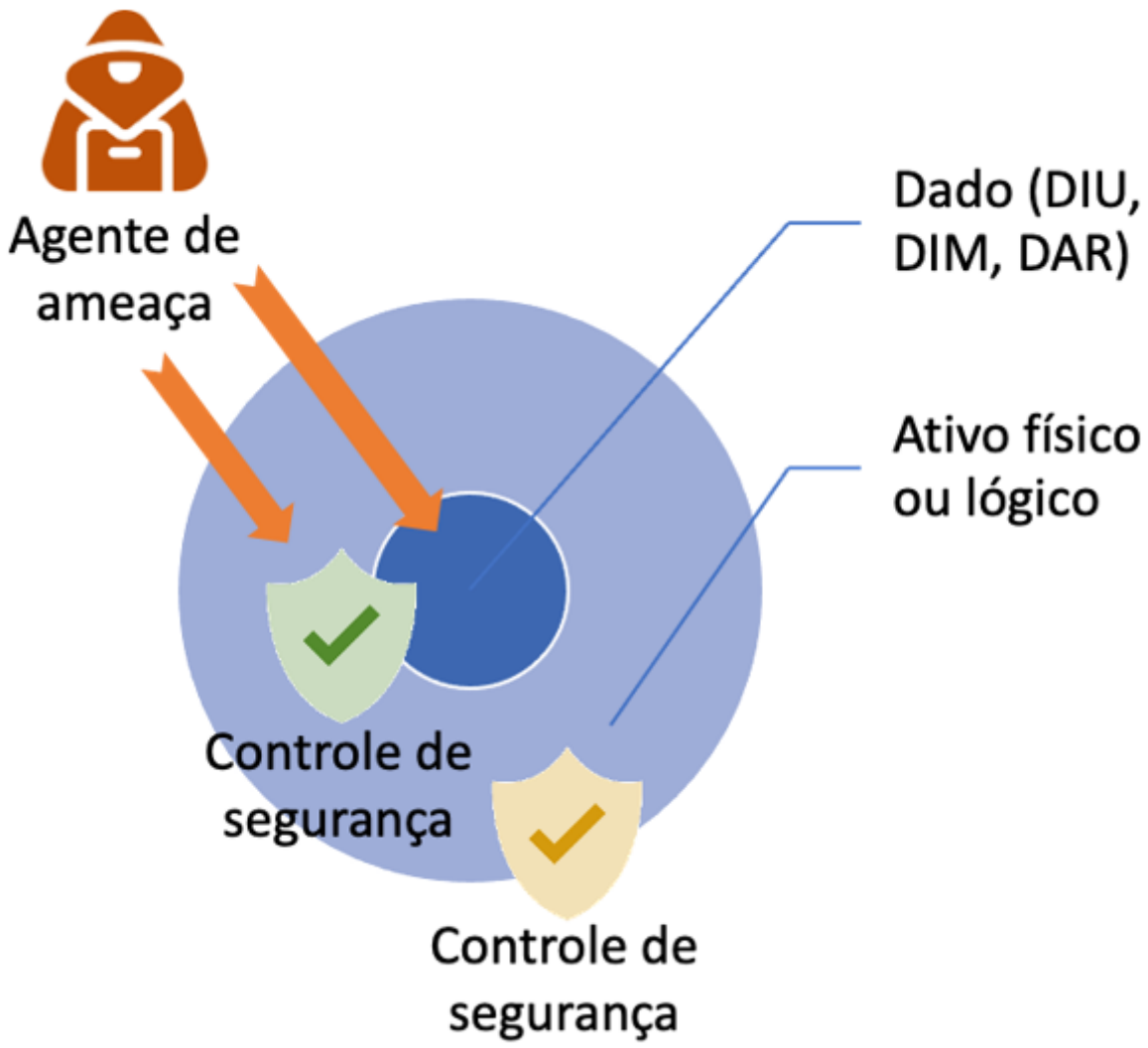
EXEMPLIFICANDO

Os dados podem estar armazenados em ativos lógicos como em um banco de dados ou servidor de arquivos e em meios físicos, como em papéis, *pendrives* e mídias de *backup*. Um dos principais controles de segurança aplicado diretamente aos dados armazenados é a criptografia. Para que o agente de ameaça tenha acesso aos dados, deve passar pelos ativos, que possuem seus próprios controles de segurança, como a gestão de identidades e acessos.

DEVEMOS PROTEGER OS DADOS EM TODOS OS SEUS ESTADOS

Os dados existem em diferentes estados (DIU, DIM e DAR), em ativos físicos ou lógicos, como mostra a Figura 2.25. Quando um dado está em processamento, há uma aplicação, por exemplo, realizando as operações nos dados. Já quando um dado está em transmissão, há a rede envolvida, bem como os equipamentos de rede. E quando um dado está armazenado, há um banco de dados, por exemplo, ou um servidor de arquivos. Em backups, os dados estão em mídias físicas como discos rígidos ou mídias de backup.

Figura 2.25 | Estados dos dados



Fonte: elaborada pelo autor.

Você deve conhecer estas possibilidades de existência dos dados, em seus diferentes estados, definir e implementar os controles de segurança mais adequados, de acordo com uma visão de riscos. Considere que um agente de ameaça sempre chega aos dados, que estão em um ativo físico ou lógico. E os controles de segurança podem ser aplicados nos dados, ou nos ativos físicos ou lógicos. O objetivo é fazer com que o agente de ameaça tenha o mínimo de acesso possível aos dados, o que significa o mínimo de acesso possível aos ativos físicos ou lógicos (NAKAMURA, 2016).

Os acessos aos ativos podem ser controlados com mecanismos de controle de acesso, que envolvem a identificação, autenticação e autorização. Um banco de dados é um exemplo de ativo que gerencia os dados. O controle de acesso faz com que os dados sejam acessados somente por usuários legítimos. Porém, em caso de vulnerabilidades em banco de dados, ou de qualquer outro componente que faz parte do sistema, como no sistema operacional, o agente de ameaça pode acessar indevidamente os dados. Neste caso, é importante o uso de controles de segurança como a criptografia, que protege a confidencialidade dos dados.

ASSIMILE

Controles de segurança podem ser aplicados nos dados, como a criptografia, ou nos ativos que gerenciam os dados, como o controle de acesso do banco de dados. O uso de múltiplos controles de segurança é importante porque constituem uma segurança em camadas. Neste exemplo, caso o controle de acesso do banco de dados ou do servidor de arquivos seja comprometido, a criptografia pode fazer com que o conteúdo dos dados não seja acessado, devido à

criptografia. Além disso, outro controle de segurança importante são os logs ou registros de quem acessa os dados, principalmente aqueles mais sensíveis.

MASCARAMENTO, ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO

Além da criptografia, há outros controles de segurança que devem ser conhecidos e considerados para serem utilizados para a proteção de dados. Um dos controles que protegem os dados, limitando a exposição, é o **mascaramento de dados**. Com esta técnica, os dados não são expostos em toda a sua totalidade, com apenas trechos que sejam suficientes para as operações. No contexto do *Payment Card Industry Data Security Standard* (PCI DSS), o mascaramento é um método para ocultar um segmento de dados ao ser exibido ou impresso (PCI, 2014). Já o truncamento é um método que remove permanentemente um segmento dos dados no armazenamento (PCI, 2014). Um exemplo é ilustrado na Figura 2.26, com o mascaramento sendo aplicado na exibição. Caso haja o armazenamento, há o truncamento ao invés do mascaramento, que é utilizado apenas na sua exibição ou impressão. Como no caso do truncamento utilizado no armazenamento a remoção é permanente, as substituições podem ser feitas de uma forma mais geral, sem indicar o número de algarismos substituídos.

Figura 2.26 | Mascaramento de dados quando exibido e truncamento quando armazenado

Fonte: elaborada pelo autor.

EXEMPLIFICANDO

Ver anotações 0

Há casos muito específicos em que números de cartões de créditos precisam ser armazenados, como em pré-autorizações ou em bancos emissores. Para os demais casos, que são a grande maioria, os dados completos do cartão não podem ser armazenados, de acordo com o PCI DSS. No atendimento aos clientes dos bancos emissores, em que há o acesso dos atendentes aos dados, os riscos envolvidos podem ser reduzidos com o uso de mascaramento. O atendente pode realizar as operações utilizando os dados com mascaramento, o que limita a possibilidade de vazamentos e posterior uso indevido dos cartões.

Outra técnica de proteção de dados é o uso da **anonimização**. Segundo a Lei Geral de Proteção de Dados Pessoais (LGPD), a anonimização é a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo (BRASIL, 2020).

Já a **pseudonimização** é tratada pela lei como o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro (BRASIL, 2020).

O Quadro 2.5 mostra a diferença entre a anonimização e a pseudonimização. Uma forma simples é que no primeiro caso o processo inverso, ou seja, o retorno ao dado original não é possível, enquanto no segundo caso (pseudonimização) é possível retornar ao dado original com o uso de uma informação adicional. No exemplo, José, Paulo, Maria e Rita podem ser anonimizados, sendo representado por “xxxx”. Já no caso de serem pseudonimizados, eles são identificados como sendo, respectivamente, “N1”, “N2”, “N3” e “N4”. O armazenamento, assim, deve ser feito utilizando-se uma das duas técnicas.

No caso do uso da anonimização, são armazenados os dados referentes ao nome anonimizado, cidade e faixa etária. Qualquer necessidade de uso destes dados não possibilita o processo reverso de identificar o titular dos dados. A empresa que adota esta técnica, assim, não pode trabalhar com dados individualizados.

Já no caso do uso da pseudonimização, são armazenados os dados referentes ao nome pseudonimizado, cidade e faixa etária. Além disso, há uma outra base, com informações de nome e nome pseudonimizado, que permite a reversão e a identificação do indivíduo. Como definido na LGPD, essa base adicional deve ser mantida separadamente pela empresa em ambiente controlado e seguro.

Quadro 2.5 | Anonimização e pseudonimização

Nome	Nome anonimizado	Nome pseudonimizado	Cidade	Faixa Etária
José	xxxx	N1	Manaus	18-20
Paulo	xxxx	N2	Recife	21-23
Maria	xxxx	N3	Manaus	24-26
Rita	xxxx	N4	Recife	18-20

Fonte: elaborado pelo autor.

REFLITA

Com o uso da pseudonimização, há duas bases. Uma com os dados, que são ligados a um indivíduo pseudonimizado ou codificado, e outra, com a relação entre o indivíduo e o pseudônimo ou código. Essas duas bases devem ser mantidas isoladas. No caso de um incidente de segurança envolvendo somente a base com dados pseudonimizados, não se sabe a quem pertence aqueles dados. Já no caso de um outro incidente de segurança envolvendo somente a base

de ligação entre o indivíduo e o pseudônimo, não há dados envolvidos. No caso de um incidente de segurança envolvendo as duas bases, o agente de ameaça passa a ter acesso a todos os dados. Você deve também considerar que, dependendo da base de dados pseudonimizado, há a possibilidade de inferências ou uso de outras informações para se chegar ao indivíduo, principalmente quando há dados mais detalhados envolvidos. Por exemplo, um indivíduo “N1” que mora em Manaus e possui entre 18 e 20 anos dá poucas informações para se chegar ao indivíduo “N1”. Porém, caso esta base de dados possua um dado a mais, como o endereço residencial, “N1” pode ser facilmente descoberto. Neste caso, uma técnica é o uso de bancos de dados mais segmentados.

ASSIMILE

Um ponto importante da LGPD é aquela que determina que os dados anonimizados não serão considerados dados pessoais para os fins desta lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. Segundo a lei, a determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios (BRASIL, 2020). Assim, em alguns casos, não é necessário identificar o titular dos dados pessoais, e sempre que possível, a anonimização simplifica a adequação à LGPD.

CLASSIFICAÇÃO DA INFORMAÇÃO

A norma ABNT NBR ISO 27002, que define os objetivos de controle e os controles de segurança da informação, define que convém que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada (ISO 27002, 2013).

> **REFLITA**
>
> A informação deve ser classificada. E quanto aos ativos que armazenam, processam, manuseiam ou protegem a informação? A norma ABNT NBR ISO 27002 estabelece que convém que estes ativos também sejam classificados, de acordo com as informações relacionadas (ISO 27002, 2013).

Um exemplo de esquema de classificação de confidencialidade da informação define quatro níveis:

- **Pública**: quando sua divulgação não causa nenhum dano.
- **Interna**: quando a divulgação causa constrangimento menor ou inconveniência operacional menor.
- **Confidencial**: quando a divulgação tem um impacto significativo nas operações ou objetivos táticos.
- **Sigilosa**: quando a divulgação tem um sério impacto sobre os objetivos estratégicos de longo prazo, ou coloca a sobrevivência da organização em risco.

Como um dos objetivos da classificação da informação é evitar a divulgação não autorizada, é importante que haja um alinhamento com a política de controle de acesso.

O controle de acesso considera a classificação da informação, como no exemplo:

- **Pública**: pode ser disponibilizado para o público em geral, e acessado por todos.

- **Interna**: pode ser acessado somente por colaboradores.
- **Confidencial**: pode ser acessado por um grupo de pessoas.
- **Sigilosa**: pode ser acessado somente por algumas pessoas específicas.

Os resultados da classificação devem ser atualizados de acordo com as mudanças do seu valor, sensibilidade e criticidade ao longo do seu ciclo de vida. A informação pode deixar de ser sensível ou crítica após certo período, por exemplo, quando a informação se torna pública. Segundo a norma ABNT NBR ISO/IEC 27002, convém que estes aspectos sejam levados em consideração, pois uma classificação superestimada pode levar à implementação de controles desnecessários, resultando em despesas adicionais ou, pelo contrário, classificações subestimadas podem pôr em perigo o alcance dos objetivos de negócio (ISO 27002, 2013). Um exemplo é o balanço de uma empresa listada na Bolsa de Valores, que é sigiloso antes da publicação no jornal e divulgação pela CVM, pois pode impactar diretamente no preço das ações e causar fraudes na compra ou venda dos papéis. Porém, depois de publicada, essa informação sigilosa passa para pública, apesar de poder interferir no preço dos papéis.

> **REFLITA**
>
> Quem deve classificar a informação? Segundo a norma ABNT NBR ISO/IEC 27002, os proprietários de ativos de informação sejam os responsáveis por sua classificação.

A classificação da informação por seus proprietários é feita a partir de um esquema de classificação que seja consistente e faça parte dos processos da organização. A classificação envolve também o uso de rótulos, considerando informações em formato físico ou digital. E o tratamento das informações envolve o entendimento comum dos

requisitos de proteção para que os controles possam ser aplicados adequadamente. A Figura 2.27 ilustra o fluxo envolvido com a classificação da informação.

Figura 2.27 | Fluxo da classificação da informação

Fonte: elaborada pelo autor.

A rotulagem da informação é um requisito-chave para acordos de compartilhamento de informações e deve ser conhecido por todos os colaboradores. Há casos em que o procedimento pode dispensar a rotulagem, como de informações públicas. Um ponto a ser considerado também é que ativos rotulados são mais fáceis de identificar e selecionar para roubos, por exemplo, já que ativos sigilosos possuem mais valor.

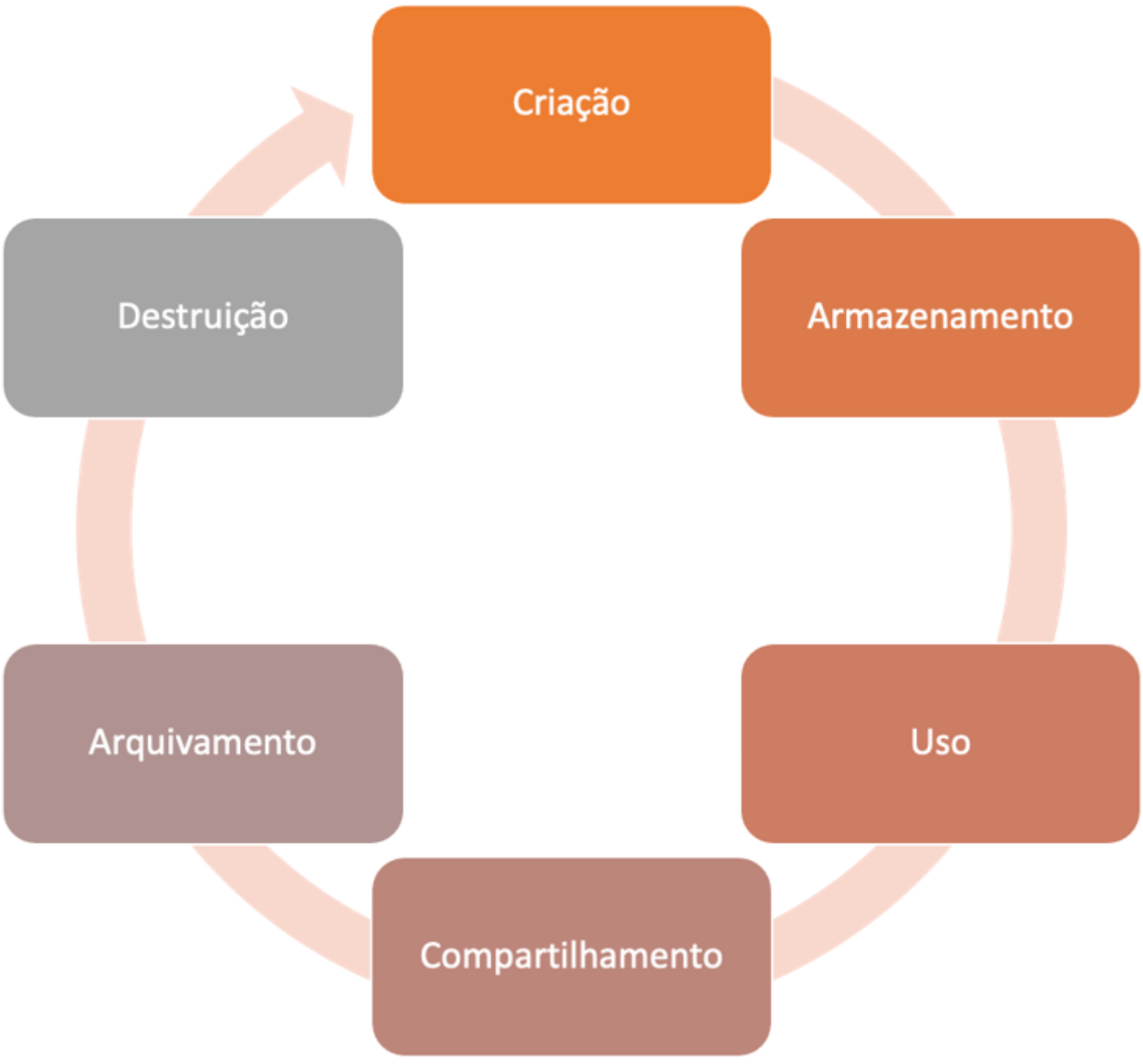
CICLO DE VIDA E TRATAMENTO DOS DADOS/INFORMAÇÃO

Um dado possui um ciclo de vida da criação à destruição (ROTHMAN, 2020), que pode ser visto na Figura 2.28:

- **Criação**: é a geração de um novo conteúdo ou a alteração/atualização de um conteúdo existente, dentro ou fora da nuvem, por um humano ou por uma máquina ou algoritmo.
- **Armazenamento**: é o ato de colocar o dado em um repositório de armazenamento e, tipicamente, ocorre quase simultaneamente à criação.
- **Uso**: dados são vistos, processados ou utilizados em outras atividades, por humanos, por algoritmos e por máquinas.
- **Compartilhamento**: troca de dados entre usuários, consumidores ou parceiros.

- **Arquivamento**: dados deixam de ser utilizados ativamente e vão para o armazenamento de longo prazo, mesmo offline.
- **Destruição**: destruição permanente dos dados utilizando meios físicos ou digitais.

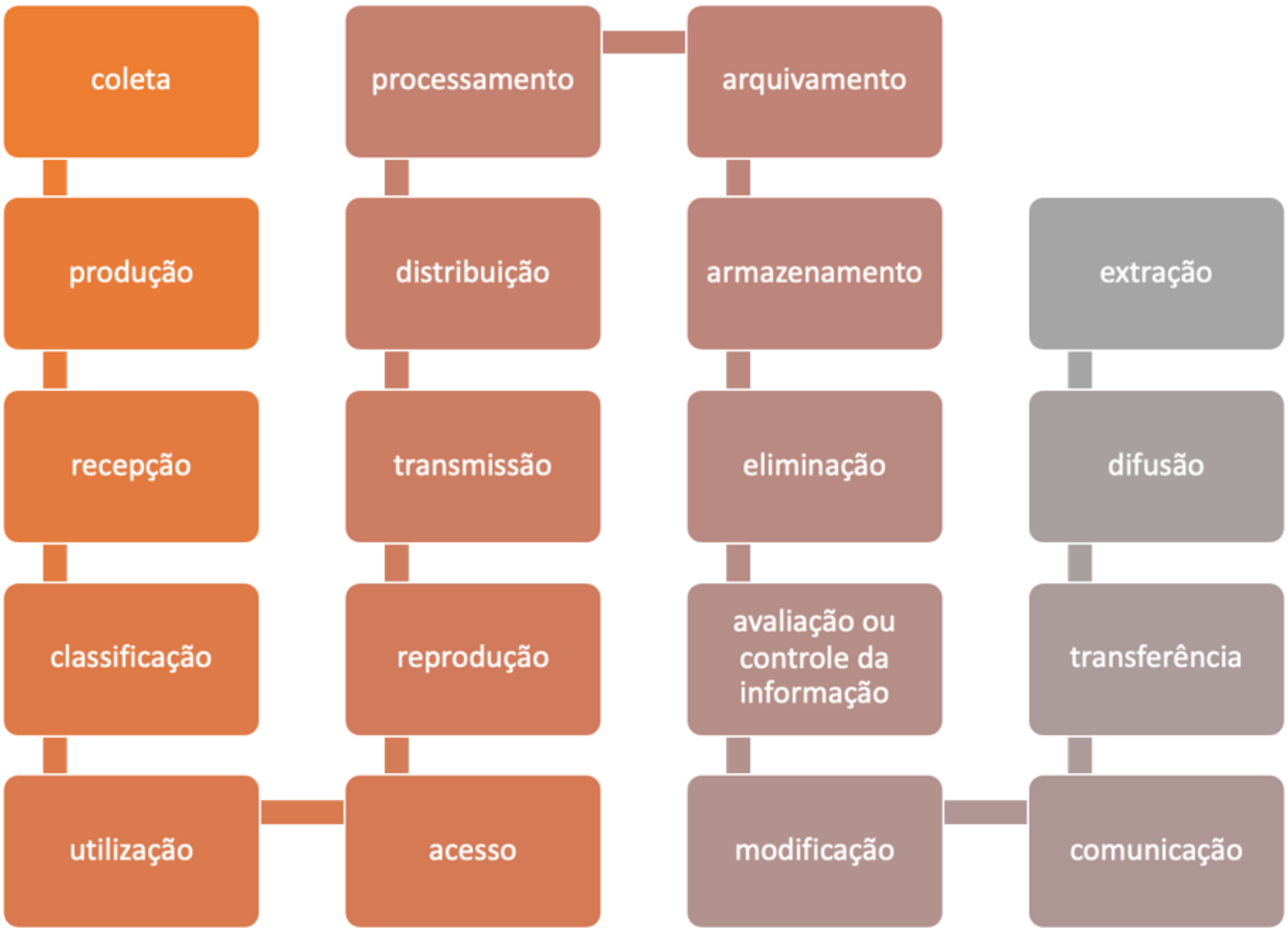
Figura 2.28 | Ciclo de vida da informação



Fonte: adaptado de Rothman (2020).

A LGPD define o tratamento de dados como 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 (BRASIL, 2020), na Figura 2.29.

Figura 2.29 | Tratamento de dados pessoais, segundo a LGPD



Fonte: adaptado de Brasil (2020).

Como há as responsabilidades pelo tratamento de dados, reforçado por leis como a LGPD, é importante considerar o ciclo de vida dos dados para a eliminação ou destruição assim que a finalidade seja alcançada. A LGPD determina as hipóteses em que ocorre o término do tratamento de dados (BRASIL, 2020):

- Verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada.
- Fim do período de tratamento.
- Comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento, resguardado o interesse público.
- Ou, determinação da autoridade nacional, quando houver violação ao disposto nesta Lei.

Sobre a retenção de dados, há aspectos legais e regulatórios que determinam um período de conservação de dados. No caso da LGPD, os dados pessoais podem ser conservados para as seguintes finalidades:

- Cumprimento de obrigação legal ou regulatória pelo controlador.
- Estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.
- Transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei.
- Ou, uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

> **EXEMPLIFICANDO**
>
> O cumprimento da obrigação legal é a necessidade de utilizar o dado para a adequação de alguma lei que peça o seu arquivamento. Por exemplo, a legislação trabalhista e fiscal, que é uma das mais complexas, pede a guarda dos dados dos colaboradores em média por até 5 anos após a sua demissão. Mas, para fins previdenciários, as informações do contrato de trabalho devem ser mantidas indefinidamente e as informações fiscais por até 10 anos. Assim, mesmo que o colaborador peça a remoção dos seus dados, não são todas as informações que a empresa pode descartar.

SEGURANÇA DE DADOS NA NUVEM

Já no contexto de provedores de nuvem, é preciso atentar para os dados tratados pelo provedor de nuvem, considerando ainda o término do contrato. De uma forma geral, o uso de um provedor de nuvem envolve o provisionamento, a migração e o desprovisionamento. Os dados não podem ser acessados indevidamente em nenhum momento pelo provedor de nuvem.

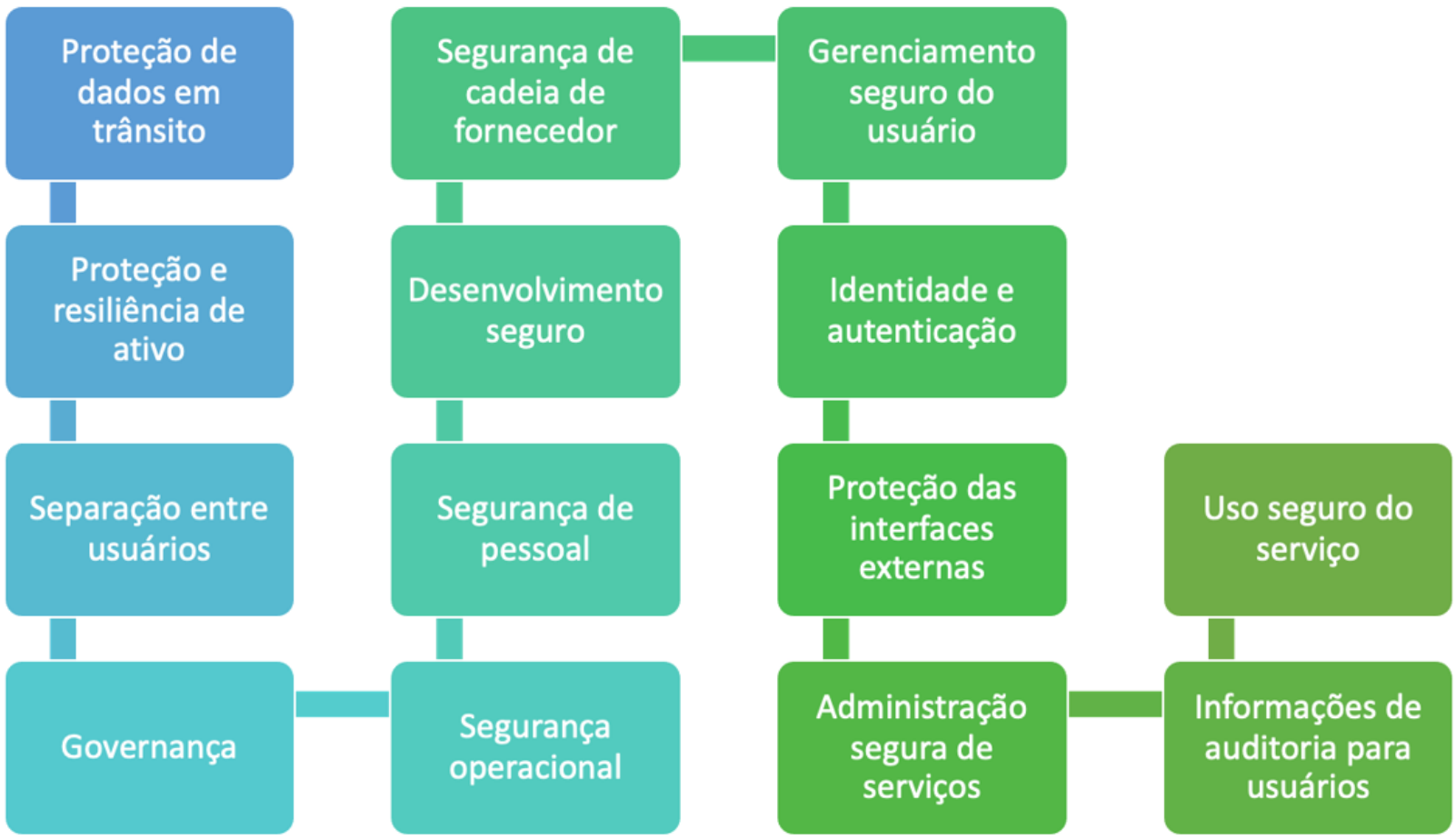
Segundo a *National Cyber Security Centre* (NCSC), do Reino Unido, os princípios da segurança em nuvem envolvem a proteção dos dados (NCSC, 2020) e estão resumidos na Figura 2.30:

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 responsabilidade.

Figura 2.30 | Princípios da segurança em nuvem



Fonte: adaptado de NCSC (2020).

E a proteção dos dados nos provedores de nuvem?

Você deve exigir, como cliente, que os provedores façam a proteção dos dados armazenados (DAR) em diferentes níveis. Os dados estão sob responsabilidade do provedor, existem no centro de dados e também em mídias. Há o acesso físico aos servidores e às mídias, como de backups. E um incidente de segurança pode ser decorrente de acidente ou de atividade maliciosa. Assim, os controles de segurança básicos dos provedores de nuvem são o controle de acesso físico, uso de técnicas como a ofuscação para tornar a identificação de dados mais difícil e o uso de criptografia diretamente na mídia física.

> **REFLITA**
>
> Como foi visto na unidade anterior da disciplina, a criptografia é tão forte quanto a sua chave. E o gerenciamento de chaves criptográficas é um grande desafio

Ver anotações

de quem utiliza a criptografia. Quem tem o acesso às chaves, onde elas são guardadas?

Outro ponto importante envolvido com o uso de provedores de nuvem é quanto à eliminação e destruição dos dados. Quando uma empresa utiliza um provedor de nuvem, a sanitização de dados deve ser exigida.

EXEMPLIFICANDO

A sanitização, destruição ou eliminação de dados do provedor de nuvem deve garantir que, após a finalização do contrato e o desprovisionamento, os dados não permaneçam com o provedor. Um ponto importante é que os dados não possam ser acessados de alguma forma quando os recursos são reutilizados por um outro cliente do provedor de nuvem. Além disso, os dados em mídias físicas também devem se descartados adequadamente, pois podem resultar em acesso indevido aos dados. Há o exemplo da destruição da mídia física (HD) em casos mais críticos, em que o hardware passa por um processo de desmagnetização ou mesmo a destruição física.

NAVEGAÇÃO EM DADOS COM CRIPTOGRAFIA

O uso de criptografia para proteger os dados é importante (STALLINGS, 2015). Porém, é preciso considerar uma série de elementos que fazem com que o nível de segurança seja corretamente avaliado. Os dois principais elementos são a chave criptográfica utilizada para decifrar os dados e a possibilidade de vulnerabilidades em ativos relacionados que dão acesso a estas chaves.

Os dados em trânsito (DIM) são tradicionalmente protegidos com o HTTPS, que é baseado em criptografia. No HTTPS, as chaves criptográficas são geradas dinamicamente, para cada sessão. Em aplicativos como os de mensagens, a criptografia é fim a fim, com um protocolo fazendo a troca de chaves para proteger a comunicação.

Ver anotações

Já no caso dos dados armazenados (DAR), há diferentes possibilidades de uso da criptografia. Os dados armazenados em um banco de dados passam do usuário para uma aplicação, que se conecta ao banco de dados. Há, neste exemplo, três pontos que podem gerenciar a criptografia e as suas chaves criptográficas: usuário, aplicação e banco de dados. Você pode desenvolver uma aplicação em que a criptografia é feita, e a chave criptográfica é definida pelo próprio usuário. Assim, no caso de o usuário esquecer ou perder esta chave, os dados também são perdidos. E os dados só podem ser acessados pelo próprio usuário, de modo que nem a empresa, nem o provedor de nuvem possui o acesso aos dados em claro (NAKAMURA & GEUS, 2007).

Já no caso de DAR protegido pela aplicação, os dados são cifrados pela aplicação antes de serem armazenados em um banco de dados. O desafio é o gerenciamento de chaves, e o que se deve evitar é armazenar a chave criptográfica na própria aplicação, o que representa uma vulnerabilidade que facilita o acesso indevido aos dados.

Outra possibilidade é o uso de criptografia do banco de dados, de modo que todos os dados são gerenciados e cifrados pelo sistema de banco de dados.

É preciso avaliar cada caso, a arquitetura do sistema e as operações da empresa para definir a melhor forma de proteger os dados armazenados (DAR).

REFLITA

Hardware Security Module (HSM) é um dispositivo de criptografia baseado em hardware que fornece funções criptográficas para geração e armazenamento de chaves criptográficas simétricas e assimétricas, fisicamente seguro e resistente à violação (HOSTONE, 2019).

Para alguns sistemas mais críticos, as chaves criptográficas podem ser geradas e gerenciadas por HSM, de modo que os sistemas se tornam mais seguros, eliminando a possibilidade

de inserção de vulnerabilidades como chaves *hardcoded* ou inseridas no próprio código, o que é fatal.

Um outro tipo de criptografia, a **homomórfica**, pode tratar, ao mesmo tempo, de proteção de DIU, DIM e DAR. Por meio de operações matemáticas diretas nos dados cifrados, a criptografia homomórfica faz com que os dados permaneçam cifrados mesmo enquanto são manipulados. Assim, ela permite ao usuário realizar uma pesquisa em um banco de dados sem que mesmo o administrador do sistema saiba sobre os termos pesquisados pelo usuário e os resultados mostrados. Ambas as partes podem descobrir intersecções dos conjuntos de dados, mas sem revelar o real conteúdo vasculhado (ROLFINI, 2020).

SAIBA MAIS

A criptografia de dados é um dos principais controles de segurança que podem ser utilizados pelas empresas. A criptografia funciona com as chaves criptográficas. Você pode proteger os dados utilizando a criptografia, mas tem que pensar como será o gerenciamento das chaves, e precisa saber dos aspectos envolvidos, que estão em forma de perguntas:

- Cada usuário terá sua própria chave criptográfica para proteger seus dados? E se ele esquecer ou perder a chave, como sua empresa atuará?
- Você usará chave criptográfica na sua aplicação, que fará a criptografia dos dados antes de serem armazenados no banco de dados? E onde estará esta chave, na própria aplicação? E no caso de um comprometimento desta chave, como você fará a atualização?
- Ou você utilizará a criptografia do banco de dados? Quem terá acesso a esta chave? E o provedor de nuvem? O que você fará em caso de comprometimento desta chave?

PESQUISE MAIS

Uma discussão interessante sobre a segurança da informação, proteção da privacidade e dos dados pessoais é feita em Vaz (2007). Leia o artigo, principalmente nas seções sobre proteção da privacidade e dos dados pessoais, que indica os caminhos trilhados por Portugal.

VAZ, A. Segurança da Informação, Protecção da Privacidade e dos Dados Pessoais, **Nação e Defesa**, Verão 2007, n. 117, 3ª série, p. 35-63.

Ver anotações 0

Chegamos ao fim desta seção, que foca da proteção dos dados, que é cada vez mais importante para você, como cidadão, porque precisa ter a sua privacidade preservada e a LGPD cumprida pelas empresas com as quais você se relaciona. E para você como profissional, porque as empresas precisam adequar seus sistemas e processos para proteger os dados e as informações, incluindo as confidenciais e sigilosas, sem deixar de lado as pessoas, já que a segurança e privacidade é de responsabilidade de todos.

Até a próxima aula!

FAÇA VALER A PENA

Questão 1

As empresas precisam preservar a confidencialidade, integridade e disponibilidade das informações. Os dados e as informações existem em meios físicos, meios digitais e na cabeça das pessoas. E uma das necessidades é proteger o armazenamento de dados.

Assinale a alternativa que apresenta o tipo de controle de segurança relacionado diretamente com a proteção dos dados armazenados.

a. Criptografia.

b. IPS.

c. *Malware*.

d. *Firewall*.

e. Conscientização.

Questão 2

Segundo a Lei Geral de Proteção de Dados Pessoais (LGPD), o tratamento de dados pessoais exige que eles sejam protegidos, com a implementação de controles de segurança em todo o fluxo dos dados para preservar a privacidade dos brasileiros.

O mecanismo de segurança que faz com que os dados não sejam considerados dados pessoais é?

a. Criptografia.

b. Pseudonimização.

c. Anonimização.

d. *Firewall*.

e. Conscientização.

Questão 3

Dados e informações devem ser protegidos com a implementação de controles de segurança. Há diferentes tipos de dados e informações, os quais devem ser classificados. Há dados e informações pessoais, públicos, internos, secretos, confidenciais, entre outros.

Análise as afirmativas a seguir.

I. Dados e informações devem ser protegidos, independentemente de sua classificação.

II. Dados e informações devem ser descartados no fim de seu ciclo de vida.

III. Dados e informações devem ser armazenados em um provedor de nuvem.

Assinale V para as afirmações verdadeiras, e F para as afirmações falsas, e indique a alternativa correta para as respectivas três afirmações.

a. F – F – F.

b. F –V – V.

c. F – V – F.

d. V – V – F.

e. F – V – V.

Ver anotações 0

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002:2013 Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação**. Rio de Janeiro. 2013.

BRASIL. **Lei Geral de Proteção de Dados Pessoais**. Presidência da República – Secretaria-Geral – Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://bit.ly/3qbyuzO. Acesso em: 25 out. 2020.

HOSTONE. **Descubra o que é HSM e quais são seus benefícios**, 24 dez. 2019. Disponível em: https://bit.ly/389xoOR. Acesso em: 14 nov. 2020.

JORNADA para Nuvem. **Os 6 pilares fundamentais para sua longa e única Jornada para Nuvem**. Disponível em: https://bit.ly/3benzRz. Acesso em: 7 nov. 2020.

NAKAMURA, E. T., GEUS, P. L. **Segurança de redes em ambientes cooperativos**. São Paulo: Editora Novatec, 2007.

NAKAMURA, E. T. **Segurança da Informação e de Redes**. São Paulo: Editora e Distribuidora Educacional S.A., 2016.

NATIONAL Cyber Security Centre. **Implementing the *Cloud* Security Principles**. Disponível em: https://bit.ly/3kFRi9b. Acesso em: 11 nov. 2020.

NEXOR. **Enabling Secure Information Exchange in *Cloud* Environments.** Disponível em: https://bit.ly/2Ol3Ne0. Acesso em: 11 nov. 2020.

ROLFINI, F. Testes apontam eficácia de criptografia totalmente homomórfica. **Olhar Digital**, 8 ago. 2020. Disponível em: https://bit.ly/3e6O9xG. Acesso em: 14 nov. 2020.

ROTHMAN, M. Data Security in the SaaS Age: Focus on What You Control. **Securosis**, 15 jun. 2020. Disponível em: https://bit.ly/3kI6ulZ. Acesso em: 12 nov. 2020.

PCI Security Standards Council. **Indústria de cartões de pagamento (PCI) Padrão de segurança de dados (DSS) e Padrão de segurança de dados de aplicativos de pagamento (PA-DSS)**, janeiro de 2014. Disponível em: https://bit.ly/3kGnU2q. Acesso em: 14 nov. 2020.

STALLINGS, W. **Criptografia e segurança de redes**. 6 ed. São Paulo: Pearson, 2015. Disponível em: https://bit.ly/3kIrr0d. Acesso em: 9 dez. 2020.

ZEFERINO, D. **Dados, informação e conhecimento**: qual a diferença dos conceitos?, 12 de agosto de 2018. Disponível em: https://bit.ly/3e5vqTf. Acesso em: 14 nov. 2020.