

NÃO PODE FALTAR

CONTROLES GERAIS DE AUDITORIA DE SISTEMAS

Emilio Tissato Nakamura

0

Ver anotações

QUAIS SÃO OS TIPOS DE CONTROLES DE SEGURANÇA E PRIVACIDADE?

Os controles podem ser físicos (como monitoramento de circuito fechado de TV), tecnológicos (como *firewall*, VPN) ou processuais (como atualização periódica de sistema operacional).



Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

PRATICAR PARA APRENDER

Olá, aluno. Você sabia que existem diversos tipos de controles? Há os controles lógicos, técnicos ou tecnológicos, que são aqueles corriqueiros de TI. Há os controles processuais, administrativos ou operacionais, que são aqueles que

estabelecem pontos de controle a serem executados pelos envolvidos. E há os controles físicos, que são aqueles mais palpáveis, visíveis, como o controle de acesso físico a uma área segura.

E os controles têm objetivos diversos, como para o processo de aquisição, desenvolvimento e manutenção de sistemas, ou para o controle de acesso lógico e físico. Há controles voltados para a segurança e privacidade, como os definidos na norma ABNT NBR ISO/IEC 27002. E há controles voltados para outras finalidades, como para a governança de TI (COBIT) ou para o gerenciamento de serviços (ITIL). O importante é que eles têm relação com a segurança e privacidade, como a continuidade de serviços do ITIL, que é importante para a proteção da disponibilidade da informação.

O auditor precisa conhecer as normas, padrões, *frameworks*, regulações e leis que exigem a implantação de controles, assim como conhecer esses últimos. A auditoria visa garantir que os controles sejam adequados, tanto na definição quanto na implantação, de modo que os objetivos da empresa estejam sendo alcançados de uma forma eficiente e eficaz. Assim, a auditoria de sistemas é essencial para a efetiva proteção da empresa, ao analisar a eficiência e eficácia dos controles definidos e implementados.

A definição dos controles a serem implantados é feita a partir de uma visão de riscos, que prioriza as necessidades dos controles de acordo com o cálculo da probabilidade e do impacto, no caso da segurança da informação, de um agente de ameaça explorar vulnerabilidades de um ativo, fazendo com que uma ameaça se torne um incidente de segurança.

Você trabalha para um provedor de nuvem que está crescendo de uma forma muito rápida e tem recebido como clientes muitas empresas tradicionais, principalmente pelo processo de transformação digital. Como sua empresa tem clientes de diferentes setores, como financeiro, saúde e governo, há uma exigência para que os serviços sejam seguros e que estejam em conformidade com regulamentos e leis específicas.

o

Ver anotações

Você já montou um planejamento para melhorar a segurança da empresa e para fortalecer a imagem do provedor de nuvem perante o mercado quanto ao tratamento das necessidades de segurança e conformidade. Agora, você deve partir para o detalhamento do planejamento, com foco nos controles. Justifique cada ponto de seu material sobre os controles, já ele será distribuído para a diretoria executiva para aprovação.

Uma sugestão de itens do material que você irá desenvolver sobre controles que não podem faltar são:

- Tipos de controles considerados e para que servem.
- Como os controles são definidos.
- Normas ou *frameworks* que podem ser a base para a definição dos controles.
- Controles para aquisição, desenvolvimento e manutenção de sistemas.
- Controle de acesso.
- Auditoria.

O auditor precisa ter conhecimentos e competências para avaliar os controles quanto à eficiência e eficácia. Isto faz com que os controles discutidos nesta aula sejam importantes para a construção deste conhecimento e desta competência. Além disso, normas e frameworks como a ISO 27001, de Sistema de Gestão de Segurança da Informação (SGSI), COBIT e ITIL são frequentemente utilizados nas auditorias.

Boa aula!

CONCEITO-CHAVE

As empresas evoluem o tempo todo e o papel da segurança e privacidade aumenta cada vez mais com a transformação digital, que traz o uso mais intenso das tecnologias e sistemas de informação. A gestão de riscos é essencial para as empresas ao trazer uma visão de oportunidades e ameaças para o cumprimento da missão, além de possibilitar a priorização de ações e investimentos. Ela também

o

Ver anotações

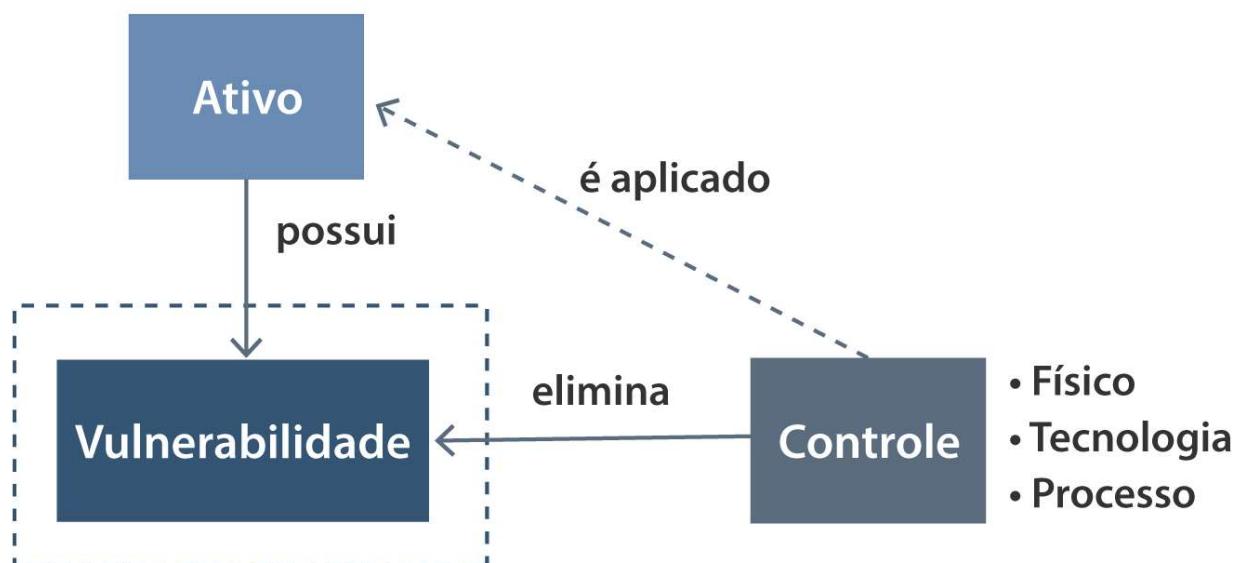
direciona a definição dos controles da empresa, incluindo os de segurança e privacidade. Do ponto de vista de segurança e privacidade, a proteção da empresa contra os riscos identificados na avaliação de riscos é feita após a implementação dos controles definidos. A auditoria de sistemas visa garantir que os controles sejam adequados, tanto na definição quanto na implantação, de modo que os objetivos da empresa estejam sendo alcançados de uma forma eficiente e eficaz. Assim, a auditoria de sistemas é essencial para a efetiva proteção da empresa, ao analisar a eficiência e eficácia dos controles definidos e implementados. O foco desta seção está nos controles, que podem ser de diferentes tipos, com variadas finalidades.

Ver anotações

CONTROLES DE SEGURANÇA E PRIVACIDADE

No contexto de segurança e privacidade, controles podem ser físicos (como monitoramento de acesso a data center), tecnológicos (como *firewall*) ou processuais (como a atualização das regras do *firewall*) e são aplicados nos ativos para que as vulnerabilidades sejam tratadas. A Figura 4.5 mostra a relação entre estes elementos.

Figura 4.5 | Controles são aplicados nos ativos para tratar as vulnerabilidades

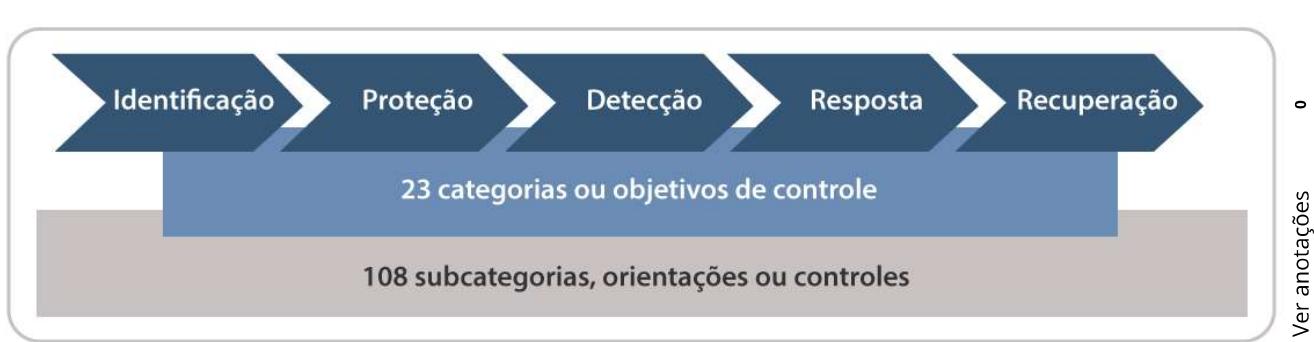


Fonte: elaborada pelo autor.

Os controles de segurança são salvaguardas ou contramedidas aplicadas em sistemas ou organizações para proteger a confidencialidade, integridade e disponibilidade dos sistemas e suas informações e para gerenciar os riscos de segurança. Os controles de privacidade são salvaguardas administrativas, técnicas e físicas aplicadas em sistemas e organizações para gerenciar riscos de privacidade e para assegurar conformidade com requisitos de privacidade aplicáveis. Os requisitos de segurança e privacidade direcionam a seleção e implementação de controles de segurança e privacidade e são derivados de leis, ordens executivas, diretrizes, regulações, políticas, padrões e necessidades de missão para assegurar a confidencialidade, integridade e disponibilidade das informações processadas, armazenadas e transmitidas, e também para gerenciar riscos (NIST, 2020).

O NIST *Cybersecurity Framework* (NIST, 2018) define as cinco funções da segurança: identificação, proteção, detecção, resposta e recuperação (Figura 4.6).

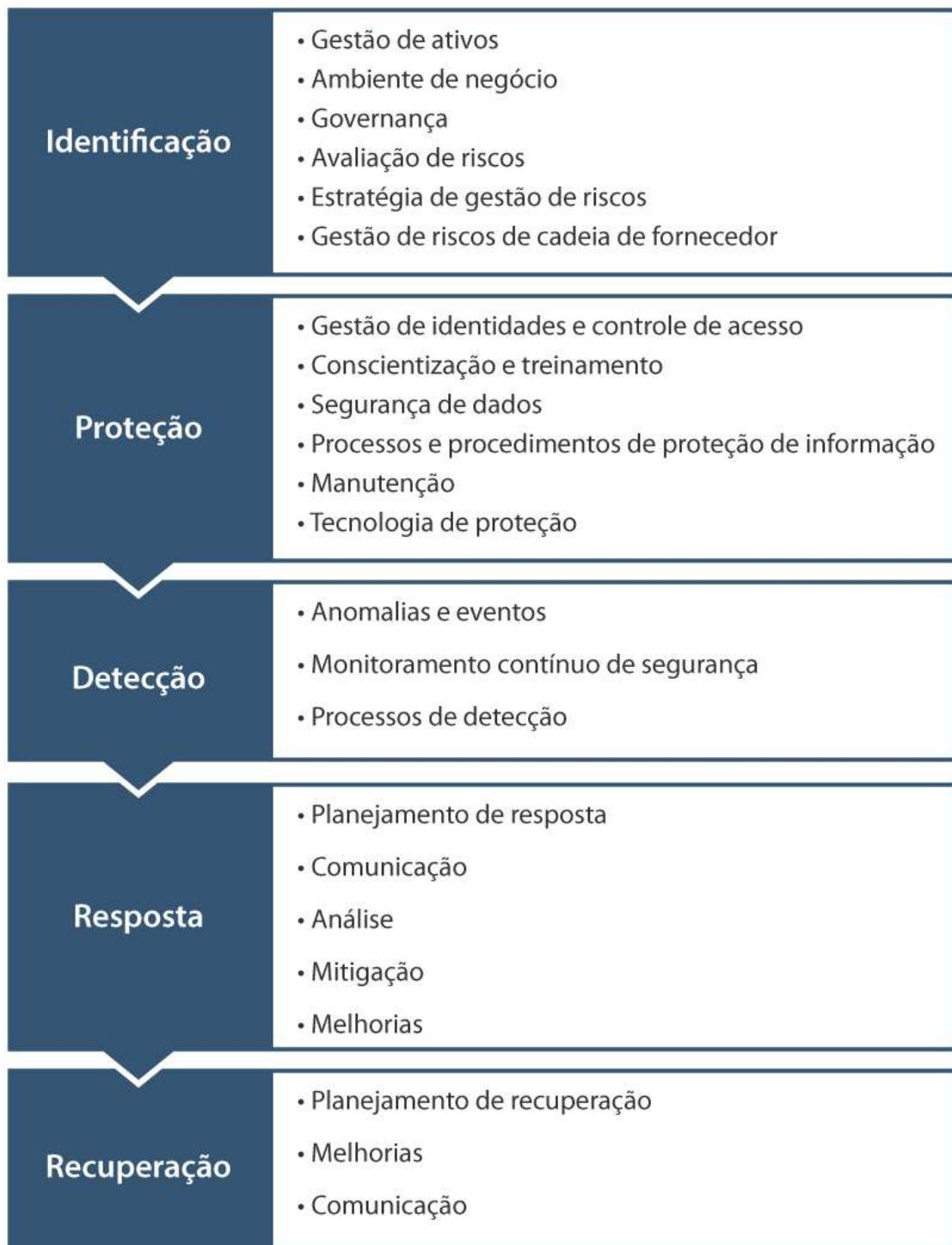
Ver anotações



Fonte: adaptada de NIST (2018).

As funções de segurança podem ser executadas com um conjunto de controles que estão divididos em 23 categorias e 108 controles. As categorias dos controles podem ser vistas na Figura 4.7, separadas para cada uma das funções de segurança.

Figura 4.7 | Categorias ou objetivos de controle do NIST *Cybersecurity Framework*



Fonte: adaptada de NIST (2018).

O NIST 800-53 provê um catálogo de controles de segurança e privacidade para sistemas de informação e organizações para proteger as operações e ativos, indivíduos, outras organizações e o país de um conjunto de ameaças e riscos, que incluem ataques hostis, erros humanos, desastres naturais, falhas estruturais, entidades de inteligência estrangeiras e riscos. Os controles são flexíveis e

0

Ver anotações

customizáveis e implementados como parte do processo de gestão de riscos, além de derivados de necessidades de missão e negócios, leis, ordens executivas, diretrivas, regulações, políticas, padrões e guias (NIST, 2020).

o

Ver anotações

CONTROLES ORGANIZACIONAIS E RELAÇÃO COM SEGURANÇA E CONTINUIDADE DO SERVIÇO

A segurança e privacidade fazem parte do contexto das empresas e estão integradas com outros assuntos, como a governança de TI. A governança de TI visa a transformação digital e a relação com a entrega de valor, a mitigação dos riscos de negócios e a otimização de recursos. A governança tem como principais objetivos (COBIT, 2018):

- Avaliação de necessidades, condições e opções de todos os atores envolvidos, em busca de determinar objetivos corporativos平衡ados.
- Direcionamento para a priorização e tomada de decisão.
- Monitoramento do desempenho e conformidade de acordo com os direcionamentos e objetivos definidos.

REFLITA

Para que a segurança seja efetiva, é importante que os processos estejam bem definidos e a equipe tenha as competências para as ações necessárias. A governança garante que as ações do cotidiano sejam tratadas para que as ameaças correntes e emergentes sejam sempre tratadas e alinhadas com a alta gestão (ISACA, 2017).

COBIT

O COBIT, de *Control Objectives for Information and Related Technology*, é um framework de governança de TI que trata de uma visão organizacional, a qual tem relação com a segurança e privacidade. O COBIT define os componentes para construir e sustentar um sistema de governança, composto por processos, estrutura organizacional, políticas, procedimentos, fluxos de informação, cultura, comportamentos, qualificações e infraestrutura.

Há cinco domínios no COBIT, um para a governança e quatro para o gerenciamento (COBIT, 2018), sendo composto por um total de 40 processos, que podem ser entendidos como controles organizacionais. Os exemplos citados dos 40 processos organizacionais são referentes aos controles de segurança:

- **Avaliar, direcionar e monitorar ou *Evaluate, Direct and Monitor (EDM)*:** é o objetivo da governança e avalia opções estratégicas, direciona a gestão e monitora a execução da estratégia. Exemplos de processos são garantir a definição e manutenção do *framework* de governança (EDM01) e garantir a otimização do risco (EDM04).
- **Alinhar, planejar e organizar ou *Align, Plan and Organize (APO)*:** é o objetivo do gerenciamento e trata de toda a organização, da estratégia e das atividades de suporte para TI. Exemplos de processos são gerenciar a arquitetura corporativa (APO03), gerenciar riscos (APO12) e gerenciar segurança (APO13).
- **Construir, adquirir e implementar ou *Build, Acquire and Implement (BAI)*:** é o objetivo do gerenciamento e trata da definição, aquisição e implementação de soluções de TI e sua integração nos processos de negócios. Exemplos de processos são gerenciar disponibilidade e capacidade (BAI04), gerenciar mudanças de TI (BAI06), gerenciar ativos (BAI09) e gerenciar configuração (BAI10).
- **Entregar serviço e suporte ou *Deliver, Service and Support (DSS)*:** é o objetivo do gerenciamento e trata da entrega operacional e suporte de serviços de TI, incluindo a segurança. Exemplos de processo são gerenciar operações (DSS01), gerenciar requisição de serviços e incidentes (DSS02), gerenciar continuidade (DSS04) e gerenciar serviços de segurança (DSS05).
- **Monitorar, verificar e avaliar ou *Monitor, Evaluate and Assess (MEA)*:** é o objetivo do gerenciamento e trata do monitoramento do desempenho e a conformidade de TI com os objetivos internos de desempenho, objetivos de controles internos e requisitos externos. Exemplos de processos são gerenciar

o

Ver anotações

monitoramento de desempenho e conformidade (MEA01), gerenciar sistema de controle interno (MEA02) e gerenciar garantia (*assurance*) (MEA04).

Ver anotações

Dentre os 40 processos ou objetivos de controle organizacionais definidos no COBIT, estão alguns voltados diretamente para a segurança, que foram destacados nos exemplos acima. Por exemplo, o processo de gerenciar segurança (APO13) está no domínio de alinhar, planejar e organizar (APO) e a condução de auditorias do sistema de gestão da segurança da informação em intervalos definidos é uma das atividades que devem ser feitas (COBIT, 2018).

Além dos controles relacionados com a visão de governança provida pelo COBIT, há a visão relacionada ao gerenciamento de serviços, provido pelo *Information Technology Infrastructure Library* (ITIL). Ambos podem ser utilizados nos processos de auditoria para medir o nível de conformidade das empresas.

ATENÇÃO

A versão atual do COBIT é a 2019, que foi projetada para a criação de estratégias de governança mais flexíveis, colaborativas e voltadas para tecnologias recentes, considerando a TI como negócio da organização e contando com atualizações mais frequentes e fluidas.

ITIL

O ITIL é um *framework* de melhores práticas que visa auxiliar as empresas a entregar e suportar serviços de TI, provendo uma estrutura alinhada com a visão, missão, estratégia e objetivos da organização. Há um sistema de valor dos serviços, composto por (AXELOS, 2018):

- Cadeia de valor de serviços.
- Princípios.
- Governança.
- Melhoria contínua.
- 34 práticas de gerenciamento.

Dentre os benefícios do ITIL para as empresas, estão (AXELOS, 2018):

- Padronização do modelo de operação de TI.
- Cumprimento dos requisitos de clientes e funcionários.
- Maior agilidade e capacidade para inovação.
- Entregas em ambientes em constante mudança.
- Maior controle e governança.
- Demonstração do valor de TI.
- Oportunidade para melhorias.

As 34 práticas do ITIL envolvem guias que são agrupadas em três categorias e estão indicadas no Quadro 4.1 (ITIL, 2019):

- Práticas de gerenciamento geral.
- Práticas de gerenciamento de serviço.
- Práticas de gerenciamento técnico.

Quadro 4.1 | As 34 práticas do ITIL

Práticas de gerenciamento geral		
Gerenciamento de estratégia	Gerenciamento de portfólio	Gerenciamento de arquitetura
Gerenciamento financeiro de serviços	Gerenciamento de força de trabalho e talento	Melhoria contínua
Mensuração e reporte	Gerenciamento de riscos	Gerenciamento de segurança da informação
Gerenciamento de conhecimento	Gerenciamento de mudança organizacional	Gerenciamento de projetos

Gerenciamento de relacionamentos	Gerenciamento de fornecedores	
Práticas de gerenciamento de serviço		
Análise de negócio	Gerenciamento de catálogos de serviços	<i>Design</i> de serviço
Gerenciamento de nível de serviços	Gerenciamento de disponibilidade	Gerenciamento de capacidade e desempenho
Gerenciamento de continuidade de serviços	Gerenciamento de monitoramento e eventos	<i>Service desk</i>
Gerenciamento de incidentes	Gerenciamento de requisição de serviços	Gerenciamento de problemas
Gerenciamento de lançamento	Habilitação de mudanças	Validação e teste de serviços
Gerenciamento de configuração de serviços	Gerenciamento de ativos de TI	
Práticas de gerenciamento técnico		
Gerenciamento de implantação	Gerenciamento de infraestrutura e plataforma	Gerenciamento e desenvolvimento de <i>software</i>

Fonte: adaptado de ITIL (2019).

0

Ver anotações

O gerenciamento de continuidade de serviços é uma das 34 práticas do ITIL e tem como objetivo gerenciar riscos que podem causar sérios impactos aos serviços de TI. O processo do ITIL assegura que o provedor de serviço de TI possa prover sempre um nível de serviço mínimo, reduzindo os riscos de desastres para um nível aceitável e planejando a recuperação dos serviços de TI (ITIL, 2020). Os subprocessos do gerenciamento de continuidade de serviço são (ITIL, 2020):

- **Suporte:** assegurar que todos os membros com responsabilidades em combater os desastres tenham conhecimento sobre suas obrigações e garantir que toda informação relevante esteja disponível prontamente quando um desastre acontece.
- **Definir os serviços para a continuidade:** definir mecanismos e procedimentos de continuidade apropriados e com custos efetivos, de acordo com os objetivos da continuidade de negócios. Inclui a definição das medidas de redução de riscos e os planos de recuperação.
- **Treinamento e testes:** garantir que todas as medidas preventivas e os mecanismos de recuperação para casos de eventos de desastres sejam testados regularmente.
- **Revisão:** revisar as medidas de prevenção de desastres com relação ao alinhamento com as percepções de risco do ponto de vista do negócio, e verificar se as medidas e procedimentos de continuidade são mantidos e testados regularmente.

EXEMPLIFICANDO

O COBIT também trata da continuidade, como o gerenciar continuidade (DSS04) no domínio de entregar serviço e suporte. Além do ITIL e do COBIT, o assunto é tratado também na norma ABNT NBR ISO/IEC 27001:2013 e 27002:2013, em um objetivo de controle específico para aspectos da segurança da informação na gestão da continuidade do negócio. O sistema de gestão de continuidade de negócios é tratado na norma ABNT NBR ISO

Ver anotações

22301:2020, que considera a segurança e resiliência. E a norma ABNT NBR ISO/IEC 27031:2015 trata de diretrizes para a prontidão para a continuidade dos negócios da tecnologia da informação e comunicação.

o

Ver anotações

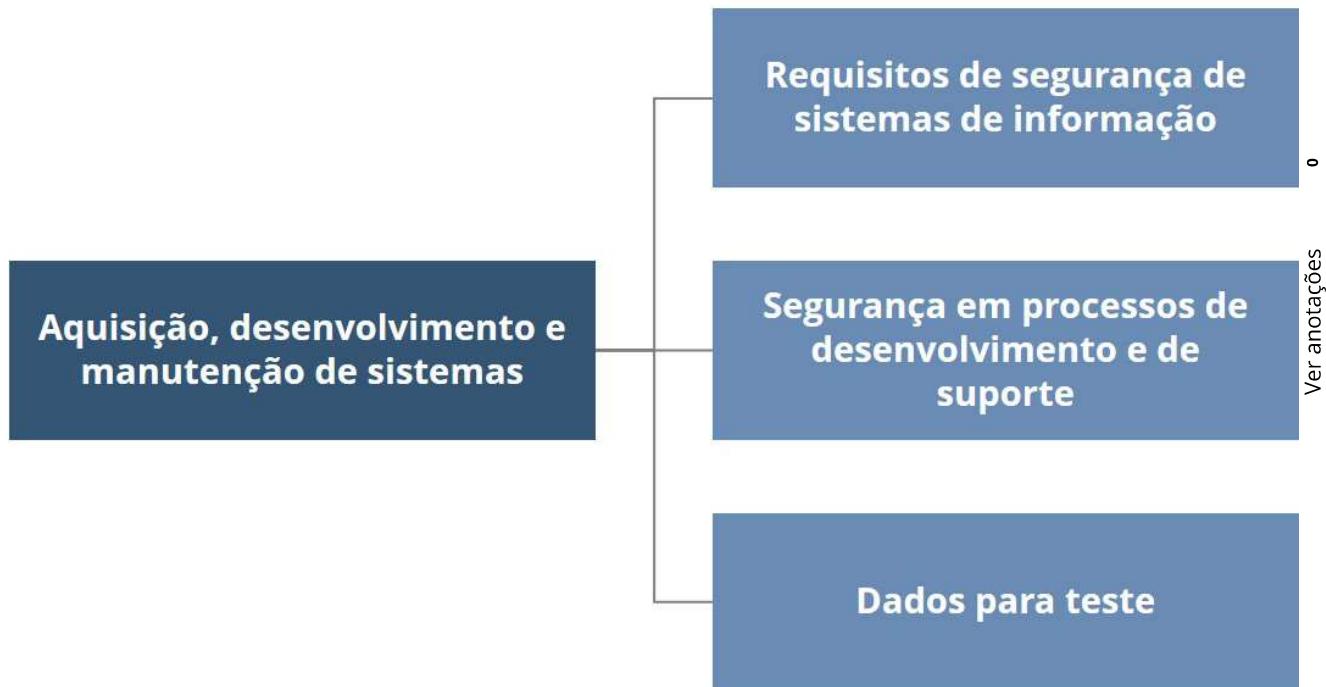
CONTROLES DE SEGURANÇA PARA AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

As empresas utilizam *software* de diferentes funções e a abordagem das empresas para o uso é variada. Há empresas que fazem o desenvolvimento do *software* internamente, enquanto há outras empresas que terceirizam o desenvolvimento para uma empresa especializada. E há ainda as empresas que adquirem o *software* a ser utilizado pela empresa. E, uma vez definido o *software*, há outros elementos relevantes, como o modelo de operação do *software*, que pode ser interno, em um provedor de nuvem, ou no modelo de uso direto no fornecedor, no modelo de *Software as a Service* (SaaS). Essa variação de abordagem é cada vez mais abrangente, pois os *softwares* precisam acompanhar a evolução e transformação das empresas e são assim atualizados constantemente. A abrangência de canais atendidos pelo *software* também é importante, uma vez que podem existir para serem utilizados em dispositivos móveis, para acesso via web ou ainda por meio de aplicações instaladas ou aplicativos.

A complexidade envolvida com aquisição, desenvolvimento e manutenção de sistemas é grande e exige um conjunto de controles que precisam ser auditados. E, considerando a essência da segurança, que precisa proteger os ativos contra a exploração de vulnerabilidades que resultam em incidentes de segurança, a verificação da eficiência e eficácia dos controles de segurança e privacidade é fundamental.

A norma ABNT NBR ISO/IEC 27002 (ISO 27002, 2013) define um conjunto de objetivos de controles de segurança e apresenta um conjunto para a aquisição, desenvolvimento e manutenção de sistemas, possuía qual tem os seguintes controles definidos: requisitos de segurança de sistemas de informação, segurança em processos de desenvolvimento e de suporte e dados para teste (Figura 4.8).

Figura 4.8 | Controles da ISO 27002 para aquisição, desenvolvimento e manutenção de sistemas

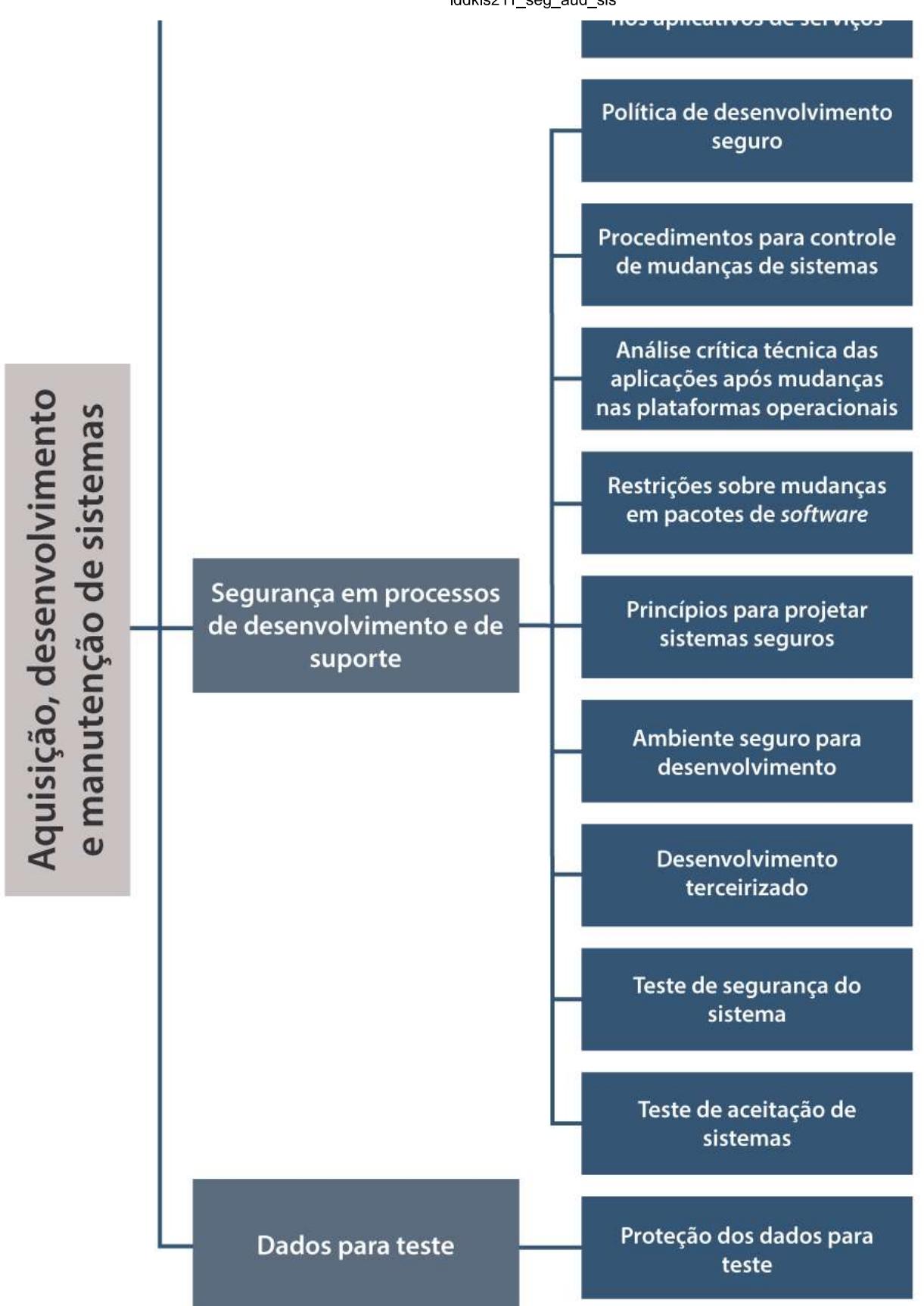


Fonte: adaptada de ISO 27002 (2013).

O objetivo de controle dos requisitos de segurança de sistemas de informação é garantir que a segurança da informação seja parte integrante de todo o ciclo de vida dos sistemas de informação. Isto também inclui os requisitos para sistemas de informação que fornecem serviços sobre as redes públicas. Já o objetivo da segurança em processos de desenvolvimento e de suporte é garantir que a segurança da informação está projetada e implementada no desenvolvimento do ciclo de vida dos sistemas de informação. O objetivo dos dados para teste é assegurar a proteção dos dados usados para este fim. O detalhamento destes controles pode ser visto na Figura 4.9.

Figura 4.9 | Controles para aquisição, desenvolvimento e manutenção de sistemas





0

Ver anotações

Fonte: adaptada de ISO 27002 (2013).

Além da ABNT NBR ISO/IEC 27002, o ITIL também define algumas práticas que tratam do desenvolvimento de sistemas (AXELOS, 2018), com os seguintes processos:

- Arquitetura da solução.
- *Design* da solução.
- Teste do *software*.
- Gerenciamento do código.
- Criação do pacote.
- Controle de versão

0

Ver anotações

COBIT também possui um processo específico para construir, adquirir e implementar, ou *Build, Acquire and Implement* (BAI), que tem como objetivo o gerenciamento, tratando da definição, aquisição e implementação de soluções de TI e sua integração nos processos de negócios. Este processo trata do gerenciamento de programas, definição de requisitos, identificação e construção de soluções, disponibilidade e capacidade, mudança organizacional, mudanças de TI, aceitação e transição de mudança de TI, conhecimento, ativos, configuração e projetos (COBIT, 2018).

CONTROLE DE ACESSO

O NIST *Cybersecurity Framework* (NIST, 2020) tem uma família de controles de segurança para o controle de acesso. Estes controles são um dos principais alvos de avaliações em auditorias e envolvem controles relacionados à identificação, autenticação e autorização, como pode ser visto no Quadro 4.2.

Quadro 4.2 | Controles de acesso do NIST *Cybersecurity Framework*

Controle de acesso		
Política e procedimentos	Gerenciamento de contas	Aplicação do acesso
Aplicação do fluxo de informação	Separação de deveres	Menor privilégio

Tentativas de acesso sem sucesso	Notificação de uso do sistema	Notificação do acesso anterior
Controle de sessões concorrentes	Bloqueio de dispositivo	Término de sessão
Ações permitidas sem identificação ou autenticação	Atributos de segurança e privacidade	Acesso remoto
Acesso sem fio	Controle de acesso para dispositivos móveis	Uso de sistemas externos
Compartilhamento de informações	Conteúdo acessível publicamente	Proteção contra mineração de dados
Decisões de controle de acesso	Monitor de referência	

Ver anotações

Fonte: adaptado de NIST (2020).

EXEMPLIFICANDO

Os controles de acesso podem ser detalhados, como os referentes ao gerenciamento de contas, que trata de (NIST, 2020): gerenciamento automatizado de contas, gerenciamento automatizado de contas temporárias e emergenciais, desabilitação de contas, ações automatizadas de auditoria, *logout* de inatividade, gerenciamento dinâmico de privilégios, contas de usuários privilegiados, gerenciamento dinâmico de contas, restrição de uso de contas compartilhadas e de grupos, credenciais de contas compartilhadas e de grupos, condições de uso e monitoramento de contas para uso atípico.

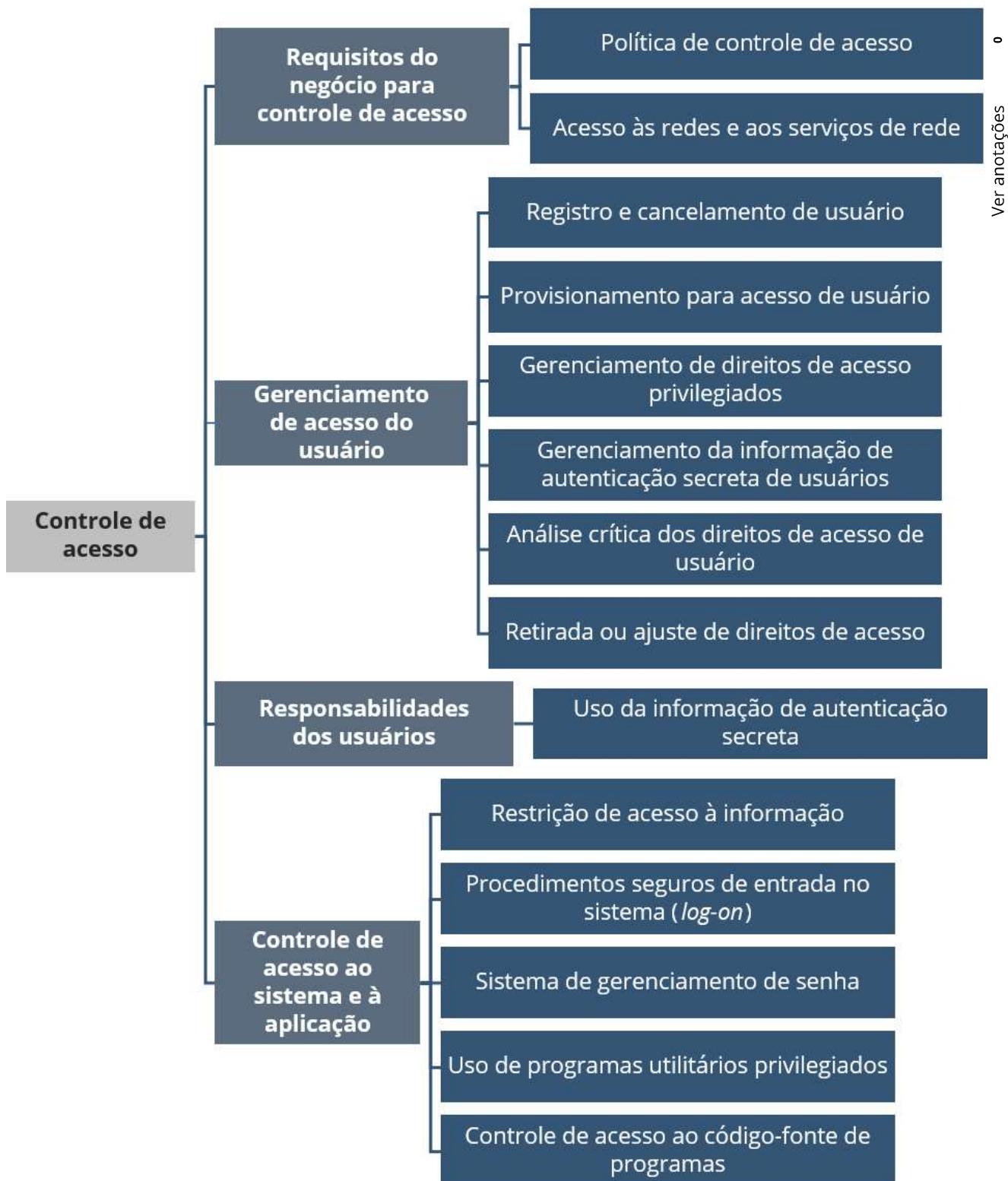
A norma ABNT NBR ISO/IEC 27002 (ISO 27002, 2013) também define um conjunto de objetivos de controles de segurança para o controle de acesso, composto por requisitos do negócio para controle de acesso, gerenciamento de acesso do

usuário, responsabilidades dos usuários e controle de acesso ao sistema e à aplicação. O detalhamento do controle de acesso pode ser visto na Figura 4.10

0

Ver anotações

Figura 4.10 | Controles da ISO 27002 para controle de acesso



Fonte: adaptada de ISO 27002 (2013).

CONTROLES LÓGICOS, FÍSICOS E PROCESSUAIS

Os controles podem ser de diferentes tipos, como foi visto nesta aula, com vários exemplos principalmente da ABNT NBR ISO/IEC 27002 (ISO 27002, 2013), COBIT (COBIT, 2018), ITIL (AXELOS, 2018) e NIST 800-53 (NIST, 2020).

Os controles de segurança envolvem investimentos em pessoas, processos e tecnologias, principalmente para o desenvolvimento de uma cultura de segurança, e podem ser administrativos, técnicos ou operacionais. Alguns exemplos são (ISACA, 2017):

- Conscientização.
- Políticas.
- Sistemas de detecção de intrusão.
- Registro de eventos (*logging*).
- Varredura de vulnerabilidades.
- Classificação da informação.
- *Hardening* de arquitetura e de tecnologia.
- *Hardening* de sistemas.

Outra classificação utilizada é os controles de segurança e privacidade serem lógicos ou tecnológicos, físicos e processuais (NAKAMURA, 2016).

REFLITA

Uma empresa pode ter implementado controles de segurança lógicos ou tecnológicos como *firewalls*, *backups* e antivírus. Porém, sem os controles baseados em processos de segurança, as regras do *firewall* podem estar erradas, o antivírus pode estar desatualizado e os *backups* podem não funcionar quando necessário. A auditoria visa avaliar os diferentes tipos de controles, incluindo os processos, para que a empresa esteja de fato segura.

o

Ver anotações

Um ponto que deve ser considerado é que a informação existe em diferentes estados e em diferentes formas, como pode ser visto na Figura 4.11. Os controles lógicos são normalmente complementados com controles processuais em meios digitais. Porém, controles físicos também fazem parte da proteção da informação, como no caso de dados em equipamentos, que podem ser acessados fisicamente e roubados. Neste caso, o controle de acesso físico é essencial. Outro conjunto de controles físicos diz respeito à proteção contra ameaças externas e do meio ambiente, como um sistema de supressão de incêndio.

Ver anotações

Figura 4.11 | Estados e formas da informação, que precisam ser protegidas



Fonte: elaborada pelo autor.

EXEMPLIFICANDO

Um exemplo de controle físico da ABNT NBR ISO/IEC 27002 (ISO 27002, 2013) é para a escolha do local e proteção do equipamento. O controle diz que convém que sejam adotados controles para minimizar o risco de ameaças físicas potenciais e ambientais, tais como furto, incêndio, explosivos, fumaça, água (ou falha do suprimento de água), poeira, vibração, efeitos químicos, interferência com o suprimento de energia elétrica, interferência com as comunicações, radiação eletromagnética e vandalismo.

Ver anotações

SAIBA MAIS

Níveis de maturidade do COBIT podem ser utilizados para expressar o nível de desempenho da organização. O COBIT estabelece seis níveis de maturidade:

- **0. Incompleto:** trabalho pode ou não pode ser completo para alcançar os objetivos.
- **1. Inicial:** trabalho é completo, mas os objetivos não são alcançados.
- **2. Gerenciado:** há medidas de planejamento e desempenho, porém sem uma padronização.
- **3. Definido:** há padrão corporativo que guia toda a empresa.
- **4. Quantitativo:** a empresa é direcionada a dados, com melhoria de desempenho quantitativo.
- **n:** a empresa é focada em melhoria contínua.

PESQUESE MAIS

O livro *Auditória e controle de acesso*, de Beneton (2017) apresenta no capítulo 7 um conjunto de controles de acesso lógico, incluindo a forma de auditar pastas e compartilhamentos, gerência de identidade do usuário, política de senhas e métodos de autenticação e privilégio mínimo.

BENETON, E. **Auditoria e controle de acesso.** São Paulo: Editora Senac, 2017.

o

Ver anotações

Chegamos assim ao final desta seção, focando nos controles que podem ter naturezas diferentes, como técnicos ou lógicos; administrativos, processuais ou operacionais; ou físicos. Os objetivos são muitos e dependem dos riscos identificados e avaliados. A verificação da eficiência e eficácia dos controles é feita pela auditoria, que tem papel importante para a segurança das empresas e para a conformidade regulatória e legal. Até a próxima seção, que destaca algumas auditorias importantes para a segurança da informação, as principais técnicas e ferramentas.

Até lá!

FAÇA VALER A PENA

Questão 1

Os controles de segurança são salvaguardas ou contramedidas aplicadas em sistemas ou organizações para proteger a confidencialidade, integridade e disponibilidade dos sistemas e suas informações e para gerenciar os riscos de segurança. No contexto de segurança e privacidade, controles podem ser físicos (como o controle de acesso a uma área segura), tecnológicos (como autenticação de usuários para acesso a sistemas) ou processuais (como os registros de quem acessa o datacenter).

Assinale a alternativa que contém os elementos em que são aplicados os controles de segurança e privacidade.

a. Aplicados nos ativos para tratar as vulnerabilidades.

Correto!

Os controles são aplicados nos ativos para tratar as vulnerabilidades. Uma ameaça é uma condição que pode se tornar um incidente de segurança em caso da exploração de vulnerabilidade de um ativo por um agente de ameaça.

b. Aplicados nas vulnerabilidades para tratar os ativos.

c. Aplicados nas ameaças para tratar os agentes de ameaça.

d. Aplicados nos agentes de ameaça para tratar as ameaças.

e. Aplicados nas ameaças para tratar as vulnerabilidades.

Questão 2

Os requisitos de segurança e privacidade direcionam a seleção e implementação de controles de segurança e privacidade e são derivados de leis, ordens executivas, diretrizes, regulações, políticas, padrões e necessidades de missão para assegurar a confidencialidade, integridade e disponibilidade das informações processadas, armazenadas, transmitidas e para gerenciar riscos.

Considerar normas e *frameworks* que organizam controles, listadas a seguir.

I. ABNT NBR ISO/IEC 27002.

II. COBIT.

III. ITIL.

As três normas e *frameworks* possuem foco em quais assuntos, respectivamente?

a. I. Governança / II. Governança / III. Auditoria.

b. I. Auditoria / II. Governança / III. Auditoria.

c. I. Segurança da informação / II. Governança / III. Governança.

d. I. Segurança da informação / II. Governança / III. Gerenciamento de serviços.

Correto!

A norma ABNT NBR ISO/IEC 27002 relaciona controles de segurança da informação. COBIT é um *framework* de governança de TI. ITIL é um conjunto de melhores práticas para gerenciamento de serviços.

e. I. Auditoria / II. Governança / III. Gerenciamento de serviços.

Questão 3

Considere os seguintes controles: gerenciamento automatizado de contas, gerenciamento automatizado de contas temporárias e emergenciais, desabilitação de contas, ações automatizadas de auditoria, *logout* de inatividade, gerenciamento dinâmico de privilégios, contas de usuários privilegiados, gerenciamento dinâmico de contas, restrição de uso de contas compartilhadas e de grupos, credenciais de contas compartilhadas e de grupos, condições de uso e monitoramento de contas para uso atípico.

Assinale a alternativa que representa a área dos controles citados.

a. Automatização.

b. Gerenciamento dinâmico.

c. Gerenciamento de contas

Correto!

O conjunto de controles está relacionado com o gerenciamento de contas. As demais alternativas podem representar segurança e privacidade, mas em um outro contexto que não está diretamente relacionado com os controles citados na questão.

d. Monitoramento.

e. Restrição de uso.

REFERÊNCIAS

ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos. Rio de Janeiro, Associação Brasileira de Normas Técnicas, 2013.

ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação. Rio de Janeiro, Associação Brasileira de Normas Técnicas, 2013.

AXELOS. **Building IT and Digital Excellence with ITIL 4.** 2018. Disponível em: <https://bit.ly/31A1tDp>. Acesso em: 10 jan. 2021.

BENETON, E. **Auditória e controle de acesso.** São Paulo: Editora Senac, 2017. Disponível em: <https://bit.ly/3cFwagE>. Acesso em: 13 jan. 2021.

ISACA, Information Systems Audit and Control Association. **COBIT 2019 Framework.** Introduction and Methodology, 2018. Disponível em: <https://bit.ly/31B8Jz6>. Acesso em: 4 jan. 2021.

ISACA, Information Systems Audit and Control Association. **COBIT 2019 Framework.** Governance and Management Objectives, 2018. Disponível em: <https://bit.ly/3cEPTNS>. Acesso em: 7 jan. 2021.

ISACA, Information Systems Audit and Control Association. **Information Systems**

Auditing: Tools and Techniques Creating Audit Programs, 2016. Disponível em:

<https://bit.ly/3rJ3KXn>. Acesso em: 7 jan. 2021.

ISACA, Information Systems Audit and Control Association. **Auditing Cyber**

Security: Evaluating Risk and Auditing Controls, 2017. Disponível em:

<https://bit.ly/3rJHtJ2>. Acesso em: 9 jan. 2021.

ISACA, Information Systems Audit and Control Association. **IT Audit**

Framework (ITAF™). A Professional Practices Framework IT Audit. 4th Edition,

2020. Disponível em: <https://bit.ly/3ubsoBG>. Acesso em: 4 jan. 2021.

ISACA, Information Systems Audit and Control Association. **IT Audit's Perspectives**

on the Top Technology Risks for 2021. Protiviti, 2020. Disponível em:

<https://bit.ly/3m6FU73>. Acesso em: 4 jan. 2021.

ITIL Process Map & ITIL Wiki. **ITIL 4**, 3 dez. 2019. Disponível em:

<https://bit.ly/3wir3La>. Acesso em: 10 jan. 2021.

ITIL Process Map & ITIL Wiki. **IT Service Continuity Management**, 24 jul.

2020. Disponível em: <https://bit.ly/3funAmV>. Acesso em: 10 jan. 2021.

NAKAMURA, E. T. **Segurança da informação e de redes**. Londrina: Editora e

Distribuidora Educacional S.A., 2016.

NATIONAL Institute of Standards and Technology, NIST. **Framework for**

Improving Critical Infrastructure Cybersecurity. Version 1.1, 16 abr. 2018.

Disponível em: <https://bit.ly/3rG9GjV>. Acesso em: 24 out. 2020.

NATIONAL Institute of Standards and Technology, NIST. Security and Privacy

Controls for Information Systems and Organizations. **NIST Special Publication**

800-53 Revision 5, set. 2020. Disponível em: <https://bit.ly/3wfcjJ4>. Acesso em: 9 jan.

2021.