Princípios de Segurança da Informação

Prof. Me. Wallace Rodrigues de Santana

www.neutronica.com.br

Atribuição-NãoComercial-CompartilhaIgual 3.0 Brasil (CC BY-NC-SA 3.0)

Você tem a liberdade de:

Compartilhar — copiar, distribuir e transmitir a obra.

Remixar — criar obras derivadas.

Sob as seguintes condições:

Atribuição — Você deve creditar a obra da forma especificada pelo autor ou licenciante (mas não de maneira que sugira que estes concedem qualquer aval a você ou ao seu uso da obra).

Uso não comercial — Você não pode usar esta obra para fins comerciais.

Compartilhamento pela mesma licença — Se você alterar, transformar ou criar em cima desta obra, você poderá distribuir a obra resultante apenas sob a mesma licença, ou sob uma licença similar à presente.

Ficando claro que:

Renúncia — Qualquer das condições acima pode ser **renunciada** se você obtiver permissão do titular dos direitos autorais.

Domínio Público — Onde a obra ou qualquer de seus elementos estiver em **domínio público** sob o direito aplicável, esta condição não é, de maneira alguma, afetada pela licença.

Outros Direitos — Os seguintes direitos não são, de maneira alguma, afetados pela licença:

- Limitações e exceções aos direitos autorais ou quaisquer **usos livres** aplicáveis;
- Os **direitos morais** do autor;
- Direitos que outras pessoas podem ter sobre a obra ou sobre a utilização da obra, tais como **direitos de imagem** ou privacidade.

Aviso — Para qualquer reutilização ou distribuição, você deve deixar claro a terceiros os termos da licença a que se encontra submetida esta obra. A melhor maneira de fazer isso é com um link para esta página.

Diversidade e inclusão

Este material foi escrito visando promover a diversidade e a inclusão, respeitando e valorizando as relações humanas de modo a propiciar uma cultura mais inclusiva e que impacte positivamente a sociedade.

Ao adotar uma linguagem inclusiva, este material busca repensar os termos usados na literatura técnica para reduzir as barreiras à equidade e promover o respeito, buscando estar livre de linguagem ofensiva ou sugestiva.

A indústria de Tecnologia da Informação tem trabalhado arduamente para mudar estes termos para alternativas mais apropriadas, mas sistemas legados ainda poderão contê-los.

Quem é Wallace Santana?

Formação Acadêmica:

- Tecnólogo em Mecânica de Precisão pela FATEC-SP [2001]
- Tecnólogo em Informática pela FATEC Mauá [2005]
- Mestre em Engenharia da Informação pela UFABC [2010]
- Especialista em Gestão Pública pela UNIFESP [2019]
- Engenheiro de Computação pela UNIVESP [2022]

Experiência Profissional

- Analista de Sistemas na CEAGESP [2005-2008]
- Analista de Tecnologia da Informação e Comunicação na PRODAM [2008-2010]
- Consultor Técnico Legislativo na Câmara Municipal de São Paulo [desde 2010]

Docência

- Faculdade de Mauá [2011-2015]
- FATEC São Caetano do Sul [2016-2017] [desde 2021]
- Centro Universitário Drummond [2018-2022]
- Universidade Presbiteriana Mackenzie [desde 2022]

Módulo Zero

Apresentação da disciplina

Objetivo

Compreender o papel da Segurança da Informação nas organizações, ter uma visão abrangente sobre os aspectos que envolvem essa atividade bem como sobre os profissionais que atuam nesta área e de seu relacionamento com o restante da organização.

Compreender a necessidade de elaboração e aplicação de controles no que diz respeito à Segurança Física e Lógica (incluindo acesso) dos recursos de Tecnologia da Informação nas organizações.

Compreender as funções de Gestão da Segurança da Informação e que estão inter-relacionadas na definição de um planejamento global, estratégico e operacional de Segurança da Informação nas organizações.

Módulos

PARTE I

1. Conceitos sobre requisitos de Segurança da Informação
2. Visão geral de Segurança da Informação no Brasil
3. Conceitos de vulnerabilidades e ameaças
4. Tipos de malware e principais ataques
5. Norma ISO/IEC série 27000
6. Políticas e procedimentos de Segurança da Informação
7. Plano de continuidade do negócio
8. Plano de recuperação de desastres

Módulos

PARTE II

9. Criptografia e certificados digitais
10. Infraestrutura de chaves públicas
11. Privacidade
12. Oportunidades no mercado de Segurança da Informação
13. Oportunidades de pesquisa em Segurança da Informação
14. Return on Security Investment (opcional)

Ementa

Abordagem dos principais conceitos relacionados à Segurança da Informação como requisitos de segurança, políticas, vulnerabilidades e outros tópicos relacionados, assim como discutir o panorama da área de Segurança da Informação no Brasil e em outros países possibilitando a elaboração de uma visão geral sobre as funções dessa área.

Referências

BÁSICAS

FONTES, Edison. **Praticando a Segurança da Informação**. Rio de Janeiro: Brasport, 2008.

HARRIS, Shon. **CISSP All-in-One Exam Guide**, Fifth Edition. 5.ed. McGraw-Hill Osborne Media, 2010.

VACCA, John. **Computer and Information Security Handbook**. Morgan Kaufmann, 2009.

COMPLEMENTARES

ABNT. **ABNT NBR ISO/IEC 27001:2006 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos**. São Paulo: Associação Brasileira de Normas Técnicas, 2006.

_____. **ABNT NBR ISO/IEC 27002:2005 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação**. São Paulo: Associação Brasileira de Normas Técnicas, 2005.

_____. **ABNT NBR ISO/IEC 27004:2010 – Tecnologia da informação – Técnicas de segurança – Gestão de segurança da informação – Medição**. São Paulo: Associação Brasileira de Normas Técnicas, 2010.

Módulo 1

Conceitos sobre requisitos de Segurança da Informação

Motivação

Redes de computadores nas primeiras décadas de existência eram usadas para fins acadêmicos ou para compartilhamento de recursos. Segurança não era uma prioridade.

Popularização da Internet e de outras tecnologias permitem o uso muito mais frequente de redes, com um grande incremento no número de usuários. Segurança passa a ser uma prioridade.

Fonte: TANENBAUM, A. S.; WETHERALL, D. Redes de Computadores. 5ª. ed. São Paulo: Pearson Prentice Hall, 2011.

O que é segurança?

De acordo com o **Dicionário Houaiss**:

1. ação ou efeito de tornar seguro; estabilidade, firmeza, seguração
2. ação ou efeito de assegurar e garantir alguma coisa; garantia, fiança, caução
3. estado, qualidade ou condição de uma pessoa ou coisa que está livre de perigos, de incertezas, assegurada de danos e riscos eventuais, afastada de todo mal
4. estado, condição ou caráter daquilo que é firme, seguro, inabalável, ou daquele com quem se pode contar ou em quem se pode confiar inteiramente
5. situação em que não há nada a temer; a tranquilidade que dela resulta
6. conjunto de processos, de dispositivos, de medidas de precaução que asseguram o sucesso de um empreendimento, do funcionamento preciso de um objeto, do cumprimento de algum plano, etc.
7. etc.

O que proteger?

De acordo com a ISO/IEC 27002:2005, **ativos alvo** de uma política de **segurança da informação** podem ser de vários tipos, incluindo:

a) **ativos de informação**: base de dados e arquivos, contratos e acordos, documentação de sistema, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e informações armazenadas;

b) **ativos de *software***: aplicativos, sistemas, ferramentas de desenvolvimento e utilitários;

c) **ativos físicos**: equipamentos computacionais, equipamentos de comunicação, mídias removíveis e outros equipamentos;

d) **serviços**: serviços de computação e comunicações, utilidades gerais, por exemplo aquecimento, iluminação, eletricidade e refrigeração;

e) **pessoas e suas qualificações**, habilidades e experiências;

f) intangíveis, tais como a **reputação e a imagem da organização**.

Fonte: NBR ISO/IEC 27002:2005

Por que proteger-se?

"A arte da guerra ensina-nos a não confiar na probabilidade do inimigo não vir, mas sim na nossa prontidão para recebê-lo; não na chance dele não atacar, mas no fato de termos feito nossa posição não assediável."

Sun Tzu, A Arte da Guerra

Definição ISO/IEC

O que é Segurança da Informação?

Segurança da Informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio*.

Como a Segurança da Informação é alcançada?

A segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de *software* e *hardware***.

Fontes: *NBR ISO/IEC 27002:2005 e **NBR ISO/IEC 27002:2013

O que é um sistema seguro?

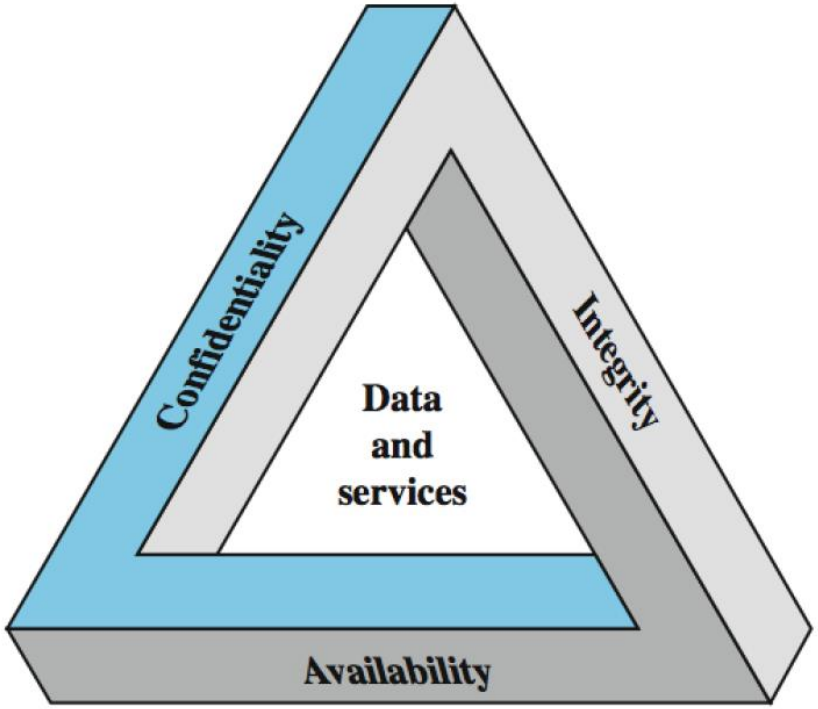
Sistema Seguro é todo sistema composto por pessoas, processos e tecnologia, que tem a capacidade de fornecer informações íntegras a todo usuário devidamente autenticado e autorizado no momento em que elas são solicitadas, sempre por meio de requisições válidas, identificadas e rastreáveis, impedindo que terceiros não autorizados interceptem, observem ou alterem estas mesmas informações.

Serviços básicos de segurança

NIST	ITU-T	Donn B. Parker
• Confidencialidade • Integridade • Disponibilidade	• Autenticação • Controle de acesso • Confidencialidade ou Privacidade • Integridade • Irretratabilidade (não repúdio)	• Confidencialidade • Integridade • Disponibilidade • Autenticidade • Posse ou Controle • Utilidade

Serviços básicos de segurança
NIST

De acordo com Stallings, o NIST (*National Institute of Standards and Technology*) define segurança da computação como uma tríade formada pela confidencialidade, integridade e disponibilidade, também conhecida como **Tríade da Segurança**.



Serviços básicos de segurança NIST

CONFIDENCIALIDADE

Garantir o acesso às informações somente a indivíduos, entidades ou processos autorizados.

INTEGRIDADE

Proteger contra modificação ou destruição inadequada das informações.

DISPONIBILIDADE

Garantir o acesso oportuno e confiável e o uso das informações.

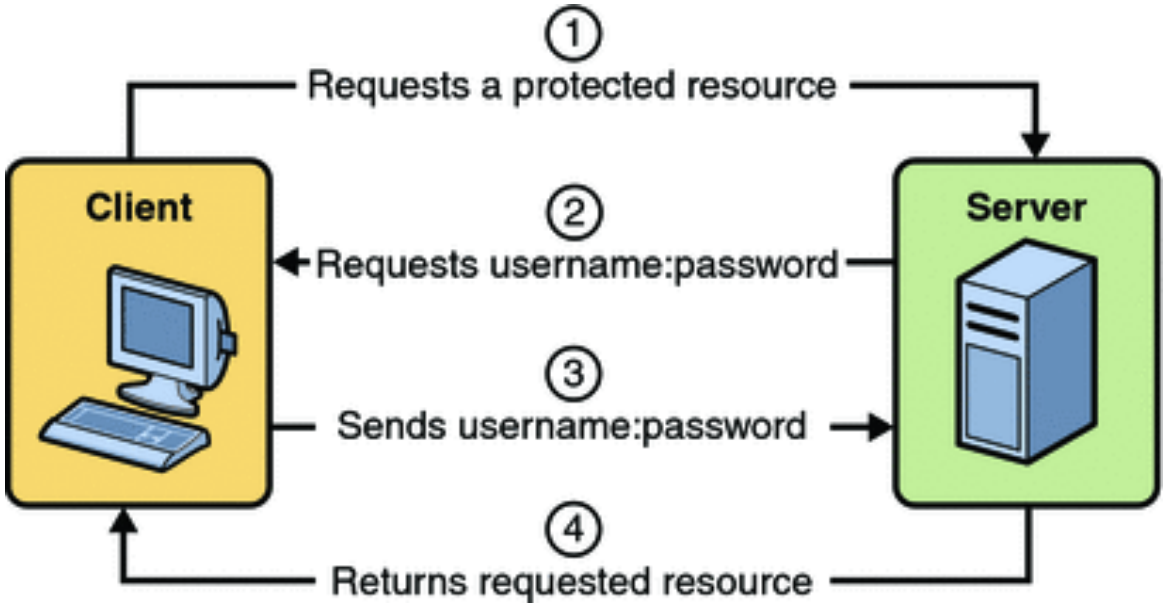
Serviços básicos de segurança ITU-T

De acordo com a Recomendação ITU-T X.800, que trata da Arquitetura de Segurança para Interconexão de Sistemas Abertos, os serviços básicos de segurança são os seguintes:

- Autenticação;
- Controle de acesso;
- Confidencialidade ou Privacidade;
- Integridade;
- Irretratabilidade (não repúdio).

Autenticação
ITU-T

A autenticação tem por objetivo garantir a identidade presumida de quem está acessando os recursos da rede.



Métodos de autenticação
ITU-T

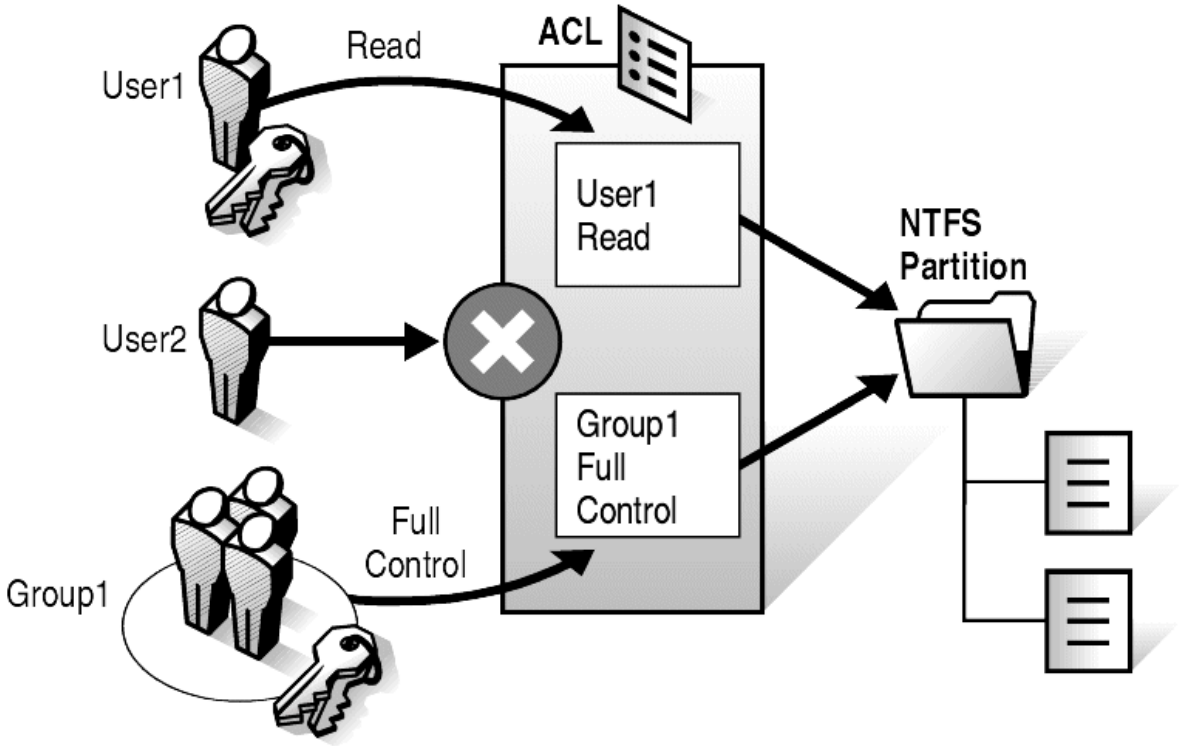
A autenticação pode ser baseada em um dos seguintes métodos:

- O que o usuário sabe (senha);
- O que o usuário tem (token);
- O que o usuário é (biometria).

A autenticação também pode ser baseada em uma combinação destes métodos.

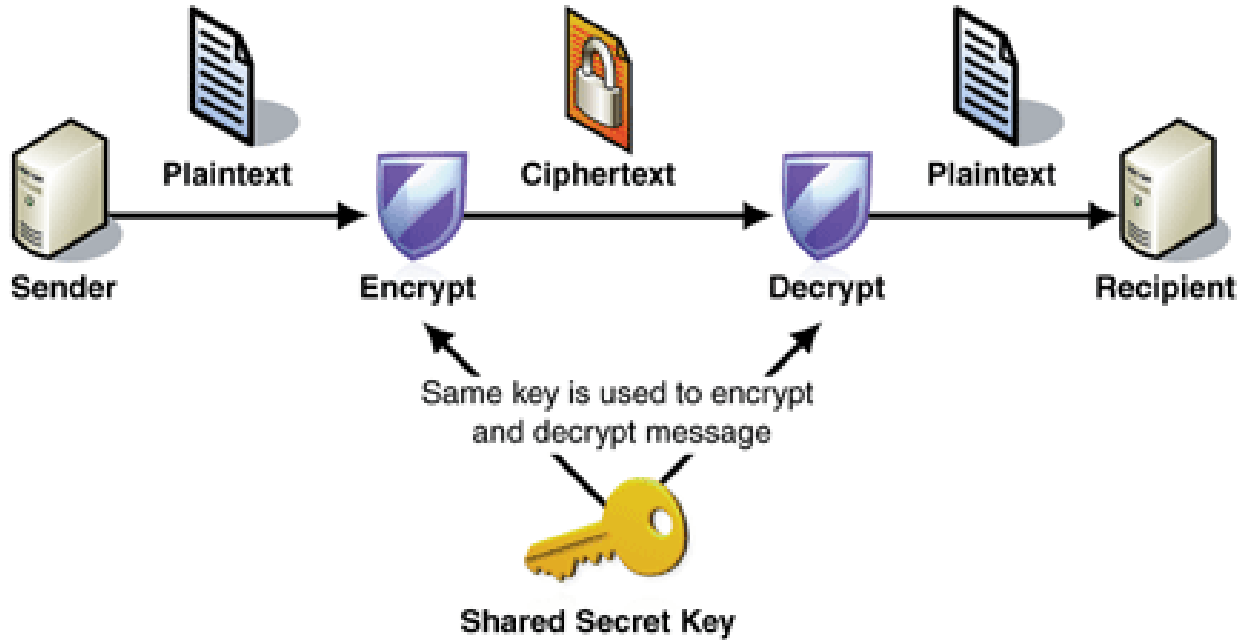
Controle de acesso
ITU-T

O controle de acesso é o mecanismo que limita o acesso a sistemas e aplicações somente a usuários autorizados.



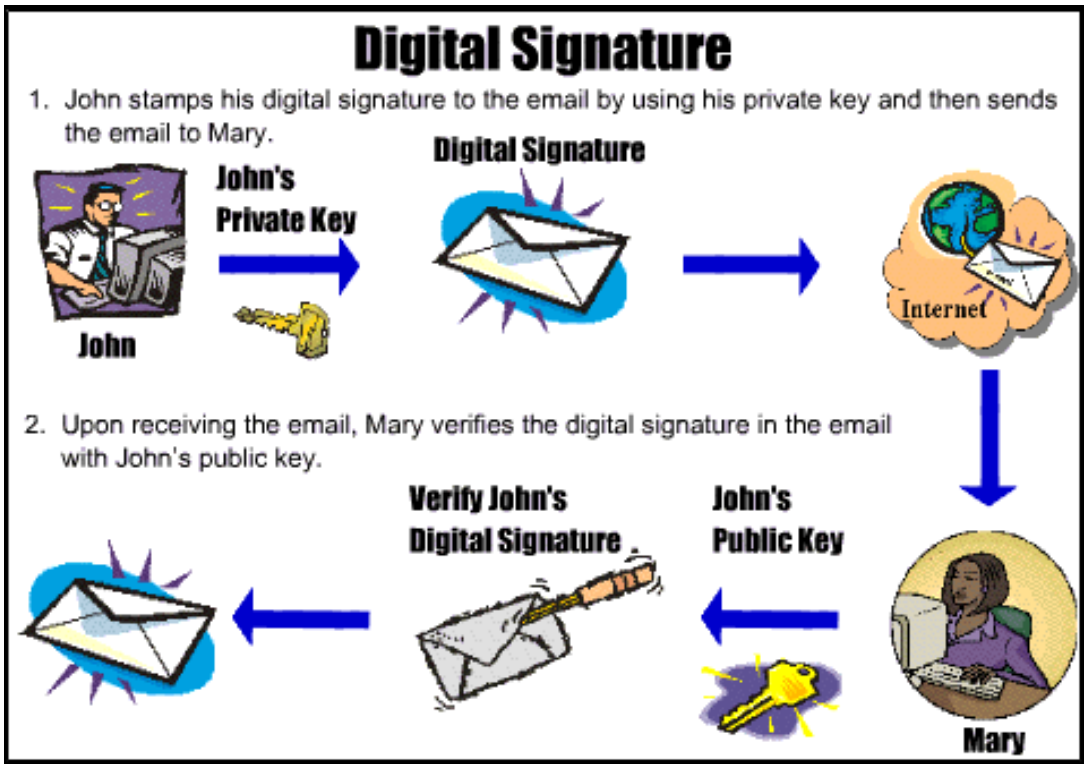
Confidencialidade
ITU-T

A confidencialidade garante que os dados ficarão protegidos contra divulgação não autorizada. Em outras palavras, impede que os dados sejam usados caso seja recuperado por terceiros.



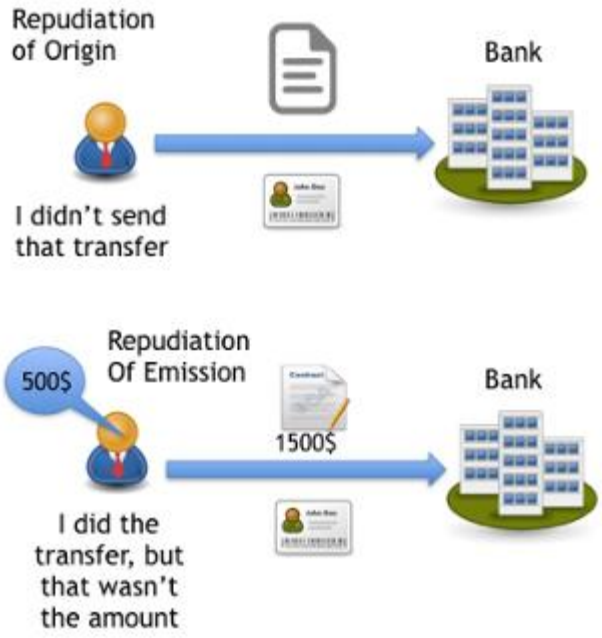
Integridade
ITU-T

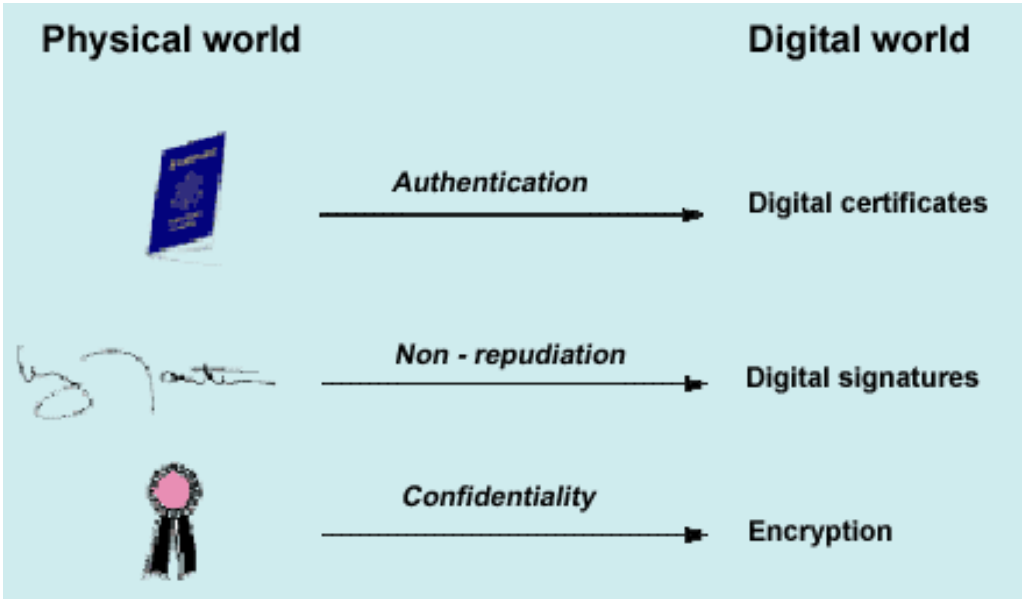
A integridade é uma garantia de que o dado ou informação não foi alterado por terceiros durante sua transmissão.



Irretratabilidade (não repúdio) ITU-T

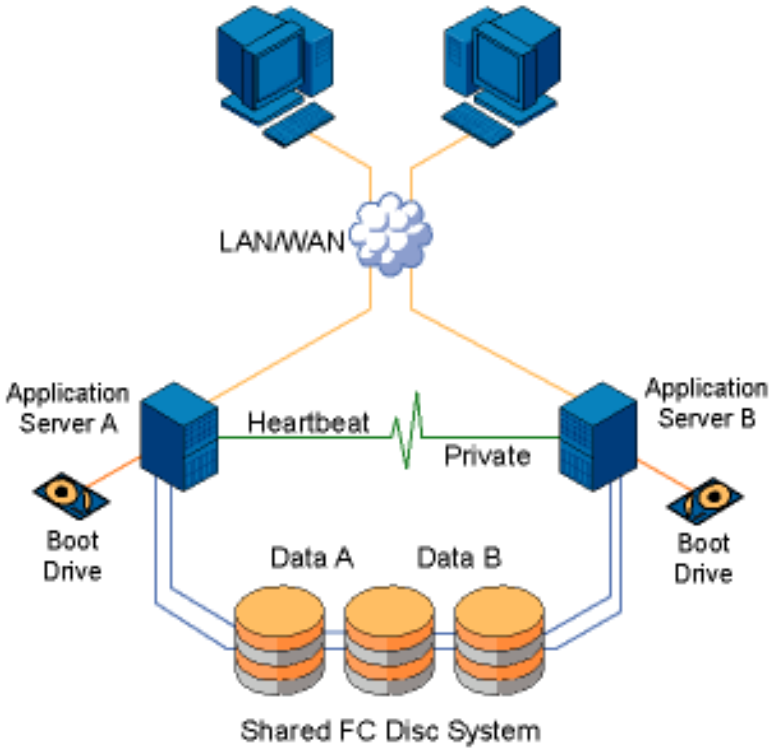
A irretratabilidade ou não repúdio impede que o emissor negue que enviou uma mensagem (irretratabilidade de origem) ou que o destinatário negue que a recebeu (irretratabilidade de destino).





Disponibilidade
ITU-T

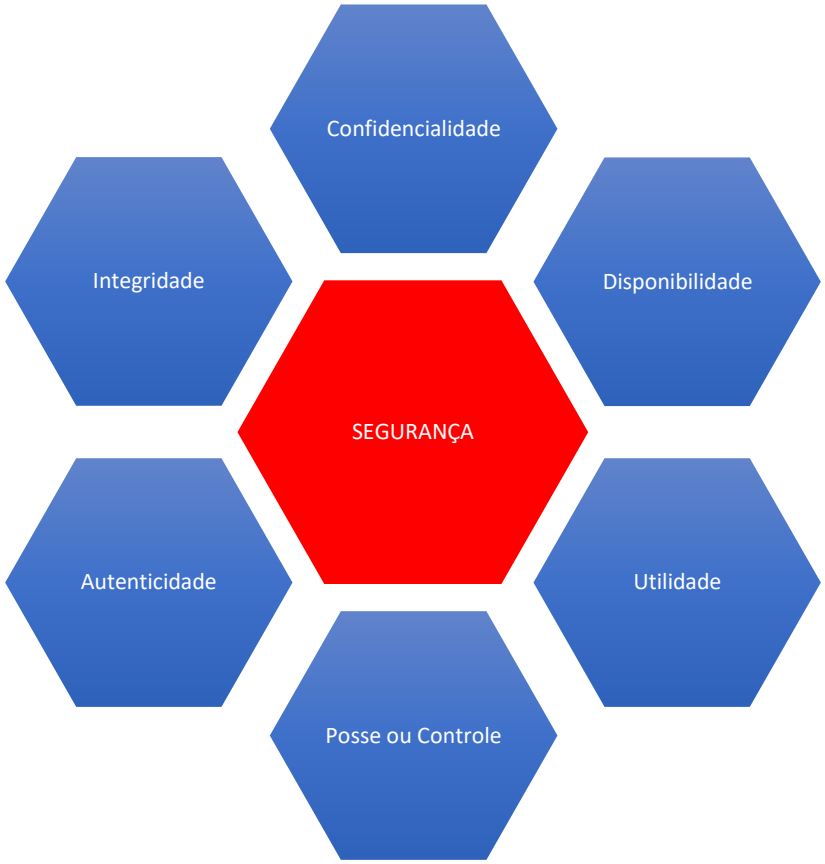
Tanto a X.800 como a RFC 2828 definem a disponibilidade como sendo a capacidade de um sistema ou recurso ser acessível a qualquer usuário autorizado a utilizá-lo.



Serviços Básicos de Segurança
Hexagrama Parkeriano

O Hexagrama Parkeriano (Parkerian Hexad) foi proposto por Donn B. Parker e visa expandir os atributos da Tríade de Segurança:

- Autenticidade – busca verificar a veracidade quanto à alegação de origem ou autoria de um dado documento ou informação, que poderia ser aferida com o uso de assinatura digital;
- Posse ou Controle – quando o dado, informação ou sistema esta na posse de quem o controle ou utiliza. Um cartão de banco roubado pode ser usado sem o consentimento de seu proprietário, que perdeu assim o controle e a posse sobre o cartão;
- Utilidade – diz respeito ao proveito que o usuário pode fazer de dados, informações ou sistemas. Um arquivo criptografado cuja chave foi perdida tem sua utilidade comprometida.



Para saber mais...

... leia o capítulo 1 do livro Segurança de Computadores, de William Stallings e Lawrie Brown.

Módulo 2

Visão geral de Segurança da Informação no Brasil

Introdução

Desde o advento da Lei Geral de Proteção de Dados Pessoais (LGPD) e com o início da pandemia de COVID-19, as organizações tiveram que se movimentar para implantar a digitalização de seus serviços e mudar a forma de trabalhar.

Com isso, consolidou-se um movimento de que a Segurança da Informação não deve ser somente uma preocupação apenas dos líderes de Tecnologia da Informação (TI), mas de todos os executivos dos mais altos escalões das organizações.

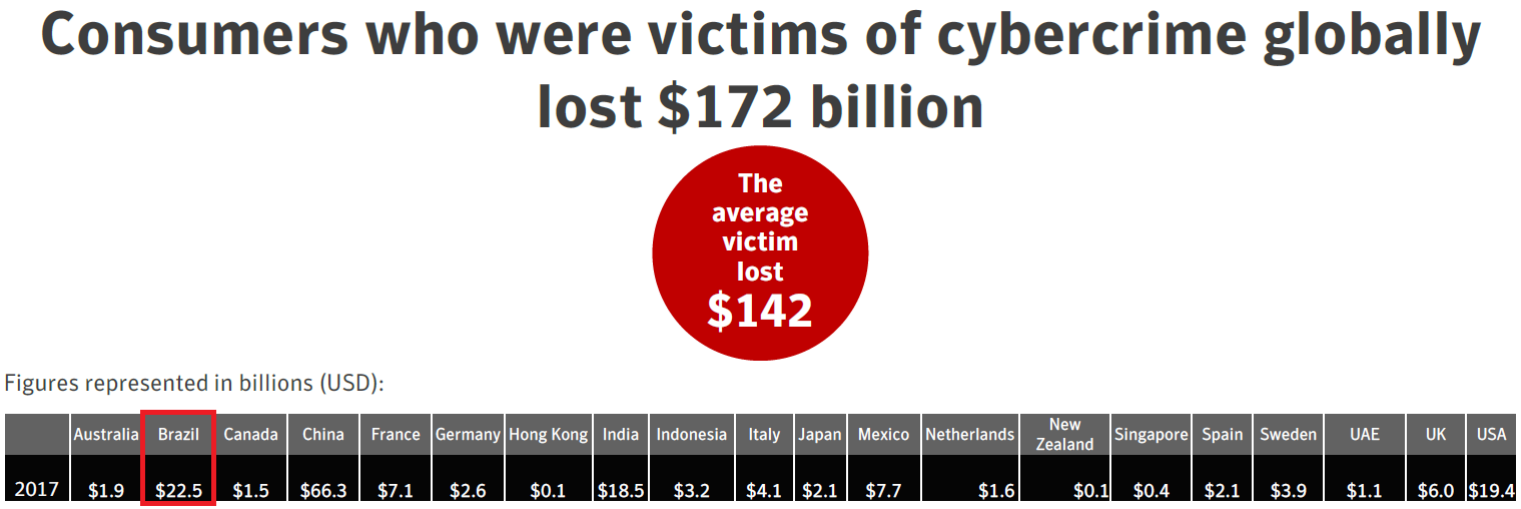
O envolvimento dos mais altos escalões nos assuntos referentes à Segurança da Informação nas organizações já era recomendado em guias de governança como COBIT e ITIL, entre outros.

Fonte: Guia definitivo de tendências de Segurança da Informação [2021], Jefferson Souza

Cenário atual

De acordo com dados levantados no Norton Cyber Security Report 2017, o Brasil é considerado o segundo país em que mais ocorrem casos de crimes cibernéticos no mundo.

A pesquisa mostrou que 34% das empresas entrevistadas já sofreram algum tipo de furto virtual, sendo que 29% paralisaram suas atividades e 27,8% tiveram um alto custo para reconstruir e restaurar todas as informações e sistemas perdidos.



	Australia	Brazil	Canada	China	France	Germany	Hong Kong	India	Indonesia	Italy	Japan	Mexico	Netherlands	New Zealand	Singapore	Spain	Sweden	UAE	UK	USA
2017	$1.9	$22.5	$1.5	$66.3	$7.1	$2.6	$0.1	$18.5	$3.2	$4.1	$2.1	$7.7	$1.6	$0.1	$0.4	$2.1	$3.9	$1.1	$6.0	$19.4

Fonte: O estado da segurança da informação no Brasil, Esdras Moreira

Desafios

Necessidade de contar com especialistas qualificados

Um dos principais desafios para as empresas é a necessidade de contar com o trabalho de especialistas qualificados para proteger as informações.

Embora muitas organizações façam uso de sistemas avançados de proteção de dados, ter um profissional com a função de prevenir o vazamento de dados sigilosos é fundamental nos dias de hoje.

Esse desafio é ainda maior para as empresas que não tem a segurança da informação como prioridade, por não a considerarem tão importante a ponto de envolvê-la no orçamento da organização.

Fonte: O estado da segurança da informação no Brasil, Esdras Moreira

Desafios

Falta de prioridade

A falta de prioridade por parte das organizações também é um dos grandes obstáculos que impedem o avanço da segurança de dados no Brasil, como mostra o levantamento feito no Relatório de 2019 do Cyber View.

De acordo com a pesquisa, 46,3% das empresas participantes da entrevista não consideravam a segurança cibernética como uma das principais prioridades, mesmo reconhecendo a sua importância. Além disso, 44,2% sequer tinham planos de investir na proteção contra ataques cibernéticos no futuro.

Considerando que, ainda segundo o levantamento, 55,4% das empresas são 100% dependentes de dados pessoais, a escolha de não colocar a segurança de dados como prioridade pode causar sérios prejuízos nos próximos anos.

Fonte: O estado da segurança da informação no Brasil, Esdras Moreira

Desafios

Adaptação à LGPD

Graças à sua extensa lista de novas obrigações a respeito da segurança de dados, muitos empresários consideram que a adaptação à LGPD é o maior desafio para a implementação de um sistema de proteção da informação eficaz no Brasil.

Empresas que não começarem a direcionar investimentos para essa área, de forma imediata, podem ser submetidas a punições severas, causando prejuízos financeiros, jurídicos e até mesmo para a sua imagem diante o mercado.

Para se adaptar é preciso a criação de um Relatório de Impacto à Proteção de Dados Pessoais, contendo a descrição dos tipos de dados coletados pela empresa, o motivo do armazenamento, os métodos utilizados para a captura de informações e a garantia de que as normas impostas pela LGPD estão sendo cumpridas.

Fonte: O estado da segurança da informação no Brasil, Esdras Moreira

Tendências

A TIVIT Labs, hub de inovação da TIVIT, multinacional brasileira de Tecnologia da Informação, é uma incubadora de ideias, soluções e produtos inovadores e tem como missão acelerar o desenvolvimento de novas soluções.

Em 2021 ela mapeou as quinze principais tendências de Segurança da Informação:

1. CIOs ganharão posição estratégica nas empresas
2. Aumento no investimento em Segurança da Informação com a LGPD
3. Maior atenção aos dados e privacidade dos colaboradores
4. Aumento dos vazamentos internos de dados nas empresas
5. Gestão de dispositivos móveis e BYOD
6. Uso de Inteligência Artificial para mapear e combater ameaças
7. Gestão de Cibersegurança em nuvem
8. Ascenção da Malha de Cibersegurança

(continua...)

Fonte: Guia definitivo de tendências de Segurança da Informação [2021], Jefferson Souza

Tendências

(... continuação)

9. Novas soluções de Cibersegurança fora do eixo EUA-Europa
10. Segurança da Informação para Internet das Coisas
11. Conformidade voltada para Cadeia de Suprimentos
12. Melhorias nos métodos de autenticação
13. Crescimento dos Cyber Seguros
14. Soluções de Extended Detection and Response (XDR)
15. Aumento dos ataques de Ransonware

Fonte: Guia definitivo de tendências de Segurança da Informação [2021], Jefferson Souza

CIOs ganharão posição estratégica nas empresas

Altas lideranças devem dialogar de forma mais frequente com os Chief Information Officers (CIOs), que reforçarão seu papel consultivo ao orientar diferentes departamentos sobre a gestão da informação.

O estudo “CIO Agenda Report 2021”, do Instituto Gartner, realizado em 2020 com 1,8 mil CIOs em 74 países, mostra que 66% dos CIOs estreitaram as relações com o Chief Executive Officers (CEOs) de suas empresas em função da pandemia de Covid-19.

Ainda, 70% disseram ter assumido a liderança de iniciativas de alto impacto, enquanto 80% atuaram na educação de CEOs e líderes sêniores sobre o valor da TI para a companhia.

Este movimento deve se intensificar com a consolidação de políticas de home office nas empresas. No Brasil, outro agravante é a necessidade de adequação de processos e sistemas à Lei Geral de Proteção de Dados (LGPD).

Fonte: Guia definitivo de tendências de Segurança da Informação [2021], Jefferson Souza

Aumento no investimento em Segurança da Informação com a LGPD

As empresas estão em uma corrida por serviços e soluções de segurança da informação que garantam a conformidade com a Lei Geral de Proteção de Dados (LGPD).

Embora a LGPD tenha entrado em vigor em setembro de 2020, apenas 41% das empresas tinham algum tipo de normativa sobre o tema. Além disso, apenas 12% possuíam medidas preventivas contra violações de dados pessoais, segundo um estudo da consultoria ICTS Protiviti.

De acordo com a pesquisa da Forrester Predictions 2021, 30% das empresas vão aumentar investimentos em nuvem, segurança, gestão de riscos e redes.

Fonte: Guia definitivo de tendências de Segurança da Informação [2021], Jefferson Souza

Maior atenção aos dados e privacidade dos colaboradores

Mudanças nos formatos de trabalho se consolidaram com a pandemia, o que também altera a forma como empresas coletam, analisam e compartilham dados pessoais dos funcionários.

Segundo o relatório de previsões Forrester Predictions 2021, o número de ações judiciais relacionadas a violações de privacidade de funcionários dobrará em 2021.

Diante de leis de proteção de dados pessoais, que se aplicam inclusive a dados de colaboradores, empresas deverão adotar uma abordagem “Privacy by Design” ao lidar com informações de colaboradores.

Isso significa identificar e seguir requisitos de privacidade, ética e comunicação com colaboradores para garantir a segurança da informação.

Privacy by Design pressupõe que todas as etapas do processo de desenvolvimento de um produto ou serviço devem ter a privacidade em primeiro lugar, ou seja, o conceito de privacidade deve estar totalmente embutido no projeto, e não se aplica à iniciativas onde a privacidade é discutida somente na fase final.

Fonte: Guia definitivo de tendências de Segurança da Informação [2021], Jefferson Souza

Aumento dos vazamentos internos de dados nas empresas

De acordo com a Forrester Predictions 2021, 33% dos vazamentos de dados serão causados por incidentes internos nas empresas – o percentual anterior era de 25%.

Os Chief Information Security Officers CISOs e CIOs deverão monitorar três fatores principais que produzirão um aumento nas ameaças internas:

- O rápido aumento de usuários internos com atividades remotas, incluindo alguns fora dos controles de segurança típicos das empresas;
- Maior facilidade de movimentação de dados roubados de empresas;
- Maior número de ameaças internas intencionais ou não intencionais, com a instalação e uso remoto de softwares e sistemas.

Na prática, líderes e CISOs terão que focar na defesa contra ameaças internas e conscientização de colaboradores.

Fonte: Guia definitivo de tendências de Segurança da Informação [2021], Jefferson Souza

Gestão de dispositivos móveis e BYOD

Uma das verdades sobre o “novo normal” é o fato de que colaboradores dependem cada vez mais de dispositivos móveis para a comunicação e acesso de arquivos em rede.

As empresas deverão intensificar o investimento em segurança da informação para dispositivos móveis e políticas BYOD (Bring Your Own Device).

De acordo com a Forrester Predictions 2021, 33% dos vazamentos de dados vão ser causados por incidentes internos nas empresas.

É indicado que companhias estabeleçam práticas de cibersegurança mais rigorosas, usando soluções de proteção endpoints de nova geração para varredura de dispositivos, articulação de firewalls, sistemas de proteção contra vazamento de dados ou Data Loss Prevention (DLP) e criptografia em comunicações.

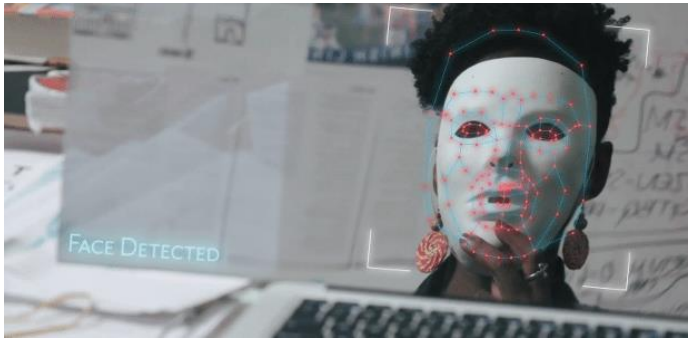
Fonte: Guia definitivo de tendências de Segurança da Informação [2021], Jefferson Souza

Uso de Inteligência Artificial para mapear e combater ameaças

A Inteligência Artificial (AI) será ainda mais usada a serviço da segurança da informação nas empresas.

Algoritmos de Deep Learning, Reinforcement Learning e sistemas de Managed Detection & Response (MDR) impulsionados por AI já são usados para testar redes e sistemas automaticamente em busca de vulnerabilidades e ameaças.

Entretanto, o uso da IA, bem como recursos de Machine Learning, dependerão de critérios e curadorias que possam assegurar o processamento autônomo ético e lícito, para evitar riscos de discriminação por parte desta tecnologia.



Documentário Coded Bias (2020)

Fonte: Guia definitivo de tendências de Segurança da Informação [2021], Jefferson Souza

Gestão de Cibersegurança em nuvem

A pandemia acabou com os limites físicos da gestão de cibersegurança, e por isso, as empresas precisam se atentar para a segurança da informação em nuvem, de forma a diminuir os riscos da descentralização de redes e dados.

Afinal, com o aumento da adoção de nuvens públicas e privadas, ambientes de nuvem também passam a ser alvos mais prováveis de ataques e do chamado Cloud Hijacking, quando um usuário usa um script de exploração para assumir o controle total de uma infraestrutura de nuvem.

Porém, é importante frisar os critérios e modelos de adoção de nuvem, seja privada ou pública.

É preciso que haja uma governança centralizada que assegure os controles e padrões utilizados pelos provedores, reduzindo possíveis custos e ajudando na conformidade com leis de tratamento de dados.

Fonte: Guia definitivo de tendências de Segurança da Informação [2021], Jefferson Souza

Ascenção da Malha de Cibersegurança

Em seu guia de tendências tecnológicas para 2021, o Instituto Gartner destaca o crescimento da Cybersecurity Mesh, ou malha de cibersegurança, entre as empresas.

Essa abordagem propõe uma arquitetura de cibersegurança escalonável e flexível, que centraliza a governança de segurança da informação, mas permite a distribuição e aplicação dessas políticas de forma modular, de acordo com cada área e necessidade da empresa.

Este modelo permite uma rápida adoção de práticas de segurança para diversas necessidades de integração, dando maior flexibilidade e agilidade, principalmente em empresas com soluções distribuídas de tecnologia.

Fonte: Guia definitivo de tendências de Segurança da Informação [2021], Jefferson Souza

Novas soluções de Cibersegurança fora do eixo EUA-Europa

O financiamento de empresas de cibersegurança fora dos Estados Unidos vai crescer cerca de 20%, de acordo com o relatório de previsões da Forrester para 2021.

Embora o país seja um polo de desenvolvimento de soluções de segurança da informação, há um processo de fortalecimento de empresas de tecnologia locais.

Esse movimento é impulsionado pela consolidação de leis de proteção de dados regionais específicas para o contexto de cada país.

Do ponto de vista dos negócios, isso significa que os líderes das empresas terão cada vez mais opções de fornecedores, e ao mesmo tempo precisarão harmonizar políticas consistentes de segurança da informação junto a múltiplos parceiros de negócio.

Fonte: Guia definitivo de tendências de Segurança da Informação [2021], Jefferson Souza

Segurança da Informação para Internet das Coisas

O número de aplicações de internet das coisas (IoT) cresce ano após ano, e empresas de diversos segmentos estão de olho em integrações de serviços com dispositivos domésticos, wearables (vestíveis) e outros objetos inteligentes.

Estes dispositivos podem ser um alvo fácil para invasões, tentativas de fraude direcionadas a sistemas de automação de processos, sensores e pontos de acesso.

Dentro da chamada 4ª Revolução Industrial, onde haverá cada vez mais a convergência de tecnologias digitais e físicas, decisões estratégicas sobre os usos de tecnologias de IoT tornar-se-ão cada vez mais relevantes do ponto de vista de segurança da informação.

Fonte: Guia definitivo de tendências de Segurança da Informação [2021], Jefferson Souza

Conformidade voltada para Cadeia de Suprimentos

A LGPD força executivos de diversas áreas a prestar mais atenção em toda a cadeia de suprimentos (Supply Chain) dos seus negócios.

No dia-a-dia de uma empresa, é muito comum o compartilhamento de informações e atividades com fornecedores, clientes, fabricantes e outros provedores de serviço.

Para evitar violações de dados por meio de terceiros, empresas devem se atentar para políticas de conformidade (Compliance).

Também devem exigir que subcontratados, fornecedores e parceiros críticos atendam padrões mínimos de segurança da informação.

Gestão de riscos de terceiros com práticas de diligência prévia (Due Diligence) e fiscalizações periódicas de seus parceiros deverão ser incorporados nas rotinas de organizações que terceirizam o tratamento de dados.

Fonte: Guia definitivo de tendências de Segurança da Informação [2021], Jefferson Souza

Melhorias nos métodos de autenticação

Empresas devem implementar métodos mais sofisticados de autenticação de identidade e acesso a sistemas internos.

A autenticação em dois fatores e via dados biométricos, por exemplo, devem ganhar mais adesão no mundo corporativo.

A autenticação de dois fatores cresceu 18% em 2020 e é usada por 82% das empresas, segundo o State of Data Security Report, da GetApp.

De acordo com o mesmo estudo, o uso de autenticação de dois fatores cresceu 18% em 2020 e tem sido usada por 82% das empresas.

Este estudo mostrou também que o uso de dados biométricos, como impressões digitais e reconhecimento facial, cresceu de 27% para 57% de 2019 para 2020.

Estes recursos têm se tornando cada vez mais comuns para reduzir fraudes e ataques de roubo de credenciais.

Fonte: Guia definitivo de tendências de Segurança da Informação [2021], Jefferson Souza

Crescimento dos Cyber Seguros

Um Cyber Seguro, ou seguro cibernético, é uma apólice que ajuda empresas a mitigar os riscos financeiros dos ataques cibernéticos e violações de dados, podendo cobrir custos de gerenciamento de crises, multas e sanções administrativas.

De acordo a consultoria PWC, muitas empresas norte-americanas já adquiriram algum tipo de seguro contra riscos cibernéticos, e espera-se que essa tendência ganhe força também no Brasil com a LGPD.

Quando uma empresa adota um Cyber Seguro, precisa adotar e comprovar medidas de segurança utilizadas para mitigar os riscos (para que as seguradoras possam precificar e comprar o risco).

Este tipo de seguro é uma maneira de reduzir possíveis impactos de prejuízos financeiros de uma violação de dados. Isto porque, mesmo que uma empresa tenha políticas de gestão de riscos, nunca estará 100% imunes a incidentes.

Fonte: Guia definitivo de tendências de Segurança da Informação [2021], Jefferson Souza

Soluções de Extended Detection and Response (XDR)

Uma das tendências mais quentes do mercado de segurança da informação são as soluções de Extended Detection & Response (XDR), ou Detecção e Resposta Estendidas.

XDR são plataformas unificadas de segurança e resposta a incidentes que coletam e correlacionam dados de várias origens.

A necessidade de se ter respostas rápida e times enxutos e focados em atividades mais nobres traz a necessidade de adotar ferramentas de automatização e correlacionamento de eventos.

A integração em XDR consolida vários serviços de segurança em um único produto, ajudando assim a alertar e indicar com maior facilidade possíveis comportamentos indesejáveis em sua estrutura tecnológica e que possam representar algum tipo de risco.

Fonte: Guia definitivo de tendências de Segurança da Informação [2021], Jefferson Souza

Aumento dos ataques de Ramsonware

De acordo com um estudo da empresa CheckPoint, o Brasil viu um aumento de 40% em ataques de ransomware apenas no primeiro trimestre de 2020, motivado pela pandemia.

Esse tipo de ataque só tende a crescer em 2021, tendo em vista a iminência do 5G e o aumento do número de dispositivos conectados em rede.

Fonte: Guia definitivo de tendências de Segurança da Informação [2021], Jefferson Souza

Para saber mais...

... leia o artigo Guia definitivo de tendências de Segurança da Informação [2021], de Jefferson Souza, disponível em https://labs.tivit.com/lgpd/tendencias-seguranca-da-informacao-2021/. Acesso em Fevereiro de 2022.

Módulo 3

Conceitos de vulnerabilidades e ameaças

Vulnerabilidades

Vulnerabilidade é uma **fraqueza** que um ativo possui ou apresenta e que poderia ser potencialmente explorada por uma ou mais ameaças. São os elementos que, uma vez expostos e explorados pelas ameaças, afetam a confidencialidade, a integridade e a disponibilidade dos ativos.

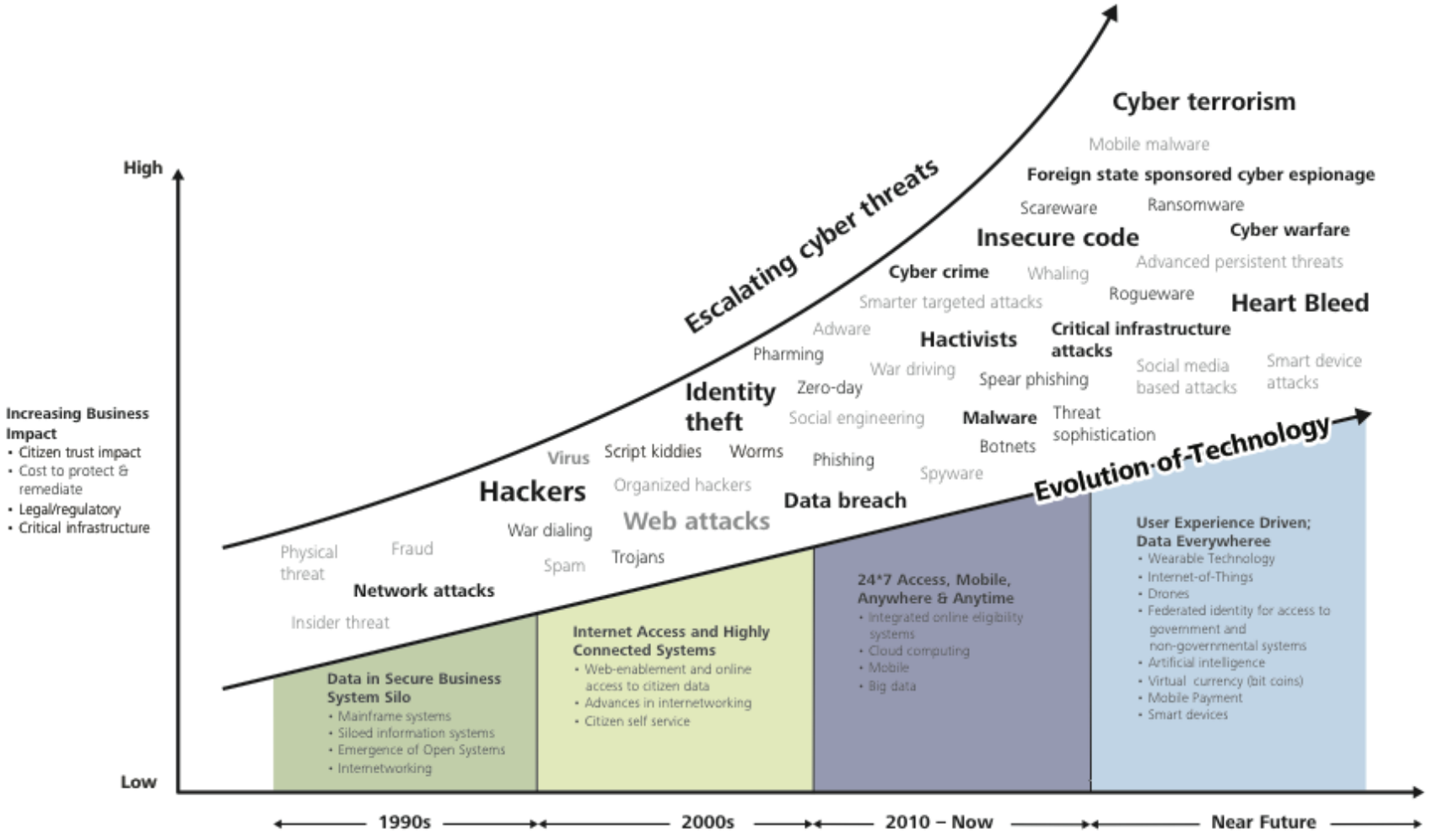
Ameaças

Ameaça é toda e qualquer **causa potencial** de um incidente indesejado que pode causar perdas e danos aos ativos da organização e afetar seus negócios.

Um sistema pode ser comprometido por ameaças do tipo:

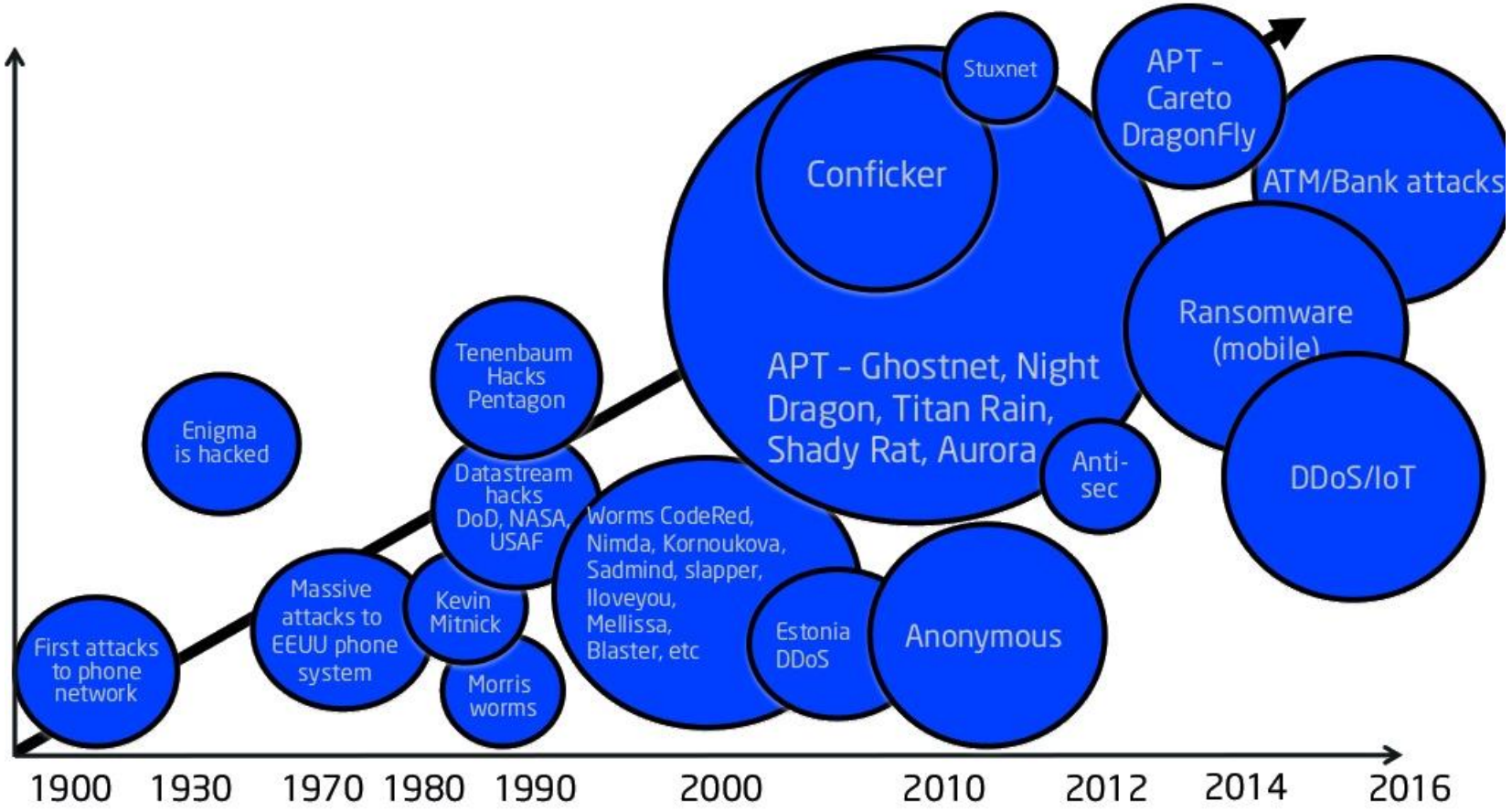
- Física;
- Lógica;
- Humana.

Escalada e evolução das ameaças cibernéticas



Fonte: Deloitte-NASCIO Cybersecurity Study, 2014

Escalada e evolução das ameaças cibernéticas



Fonte: Jorge Lopez Hernandez-Ardieta. **Cyber ranges: The (r)evolution in cybersecurity training**, 2016

Tipos de ataque

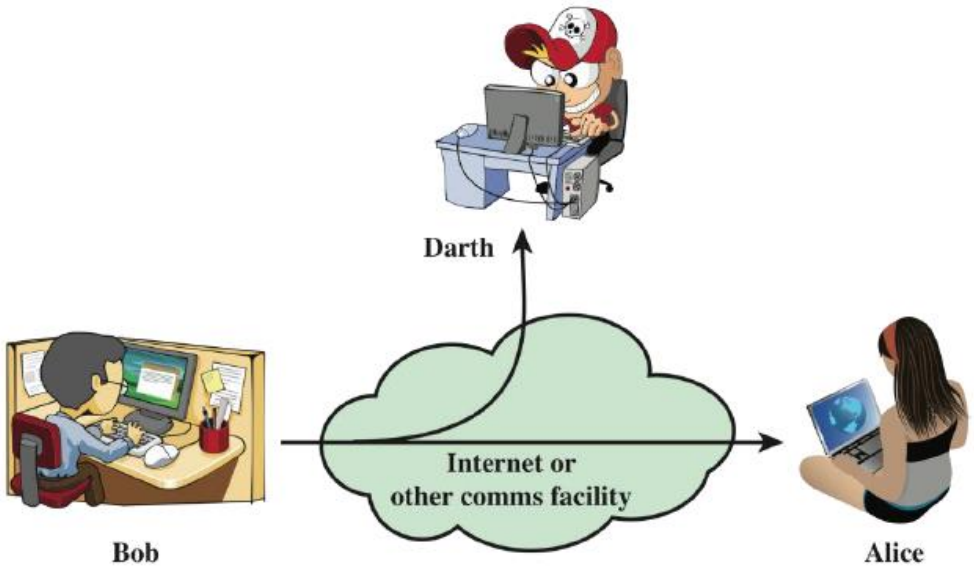
De acordo com Stallings, um meio de classificar ataques de segurança, usado tanto na X.800 quanto na RFC 4949, é em termos de ataques passivos e ataques ativos.

Um **ataque passivo** tenta aprender ou usar informações do sistema, mas não afeta os seus recursos, sendo assim mais difícil de se detectar.

Já um **ataque ativo** tenta alterar os recursos do sistema ou afetar a sua operação, sendo mais fácil de se detectar.

Ataque passivo

Os ataques passivos tem a natureza de espionagem ou de monitoramento de transmissões. O objetivo é obter informações que estão sendo transmitidas. Podem ser do tipo vazamento de conteúdo ou análise de tráfego.



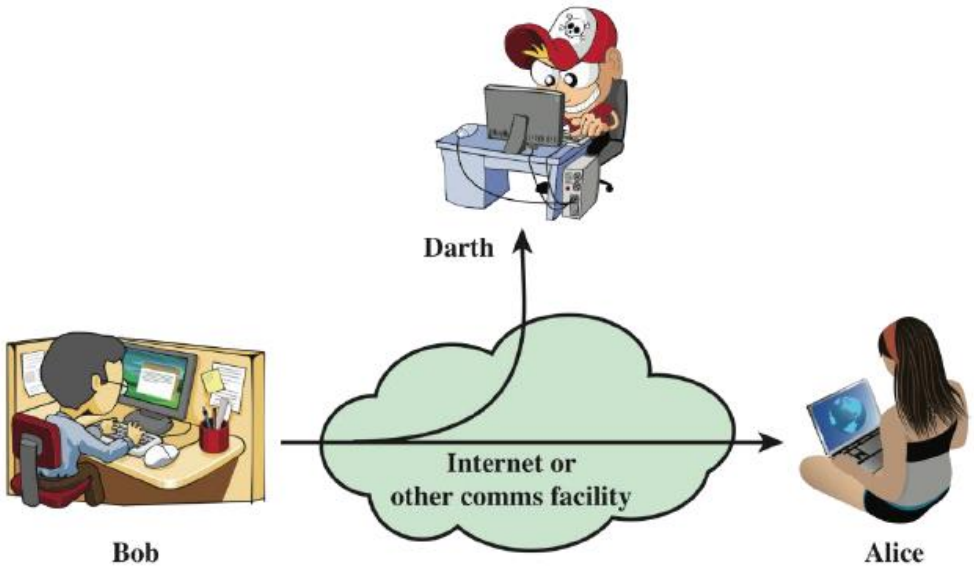
(a) Passive attacks

Fonte: Stallings

Ataque passivo – continuação

No vazamento de conteúdo o oponente procura obter informações sensíveis e confidenciais.

Na análise de tráfego o objetivo é obter o padrão de tráfego e determinar o local e a identidade dos interlocutores.

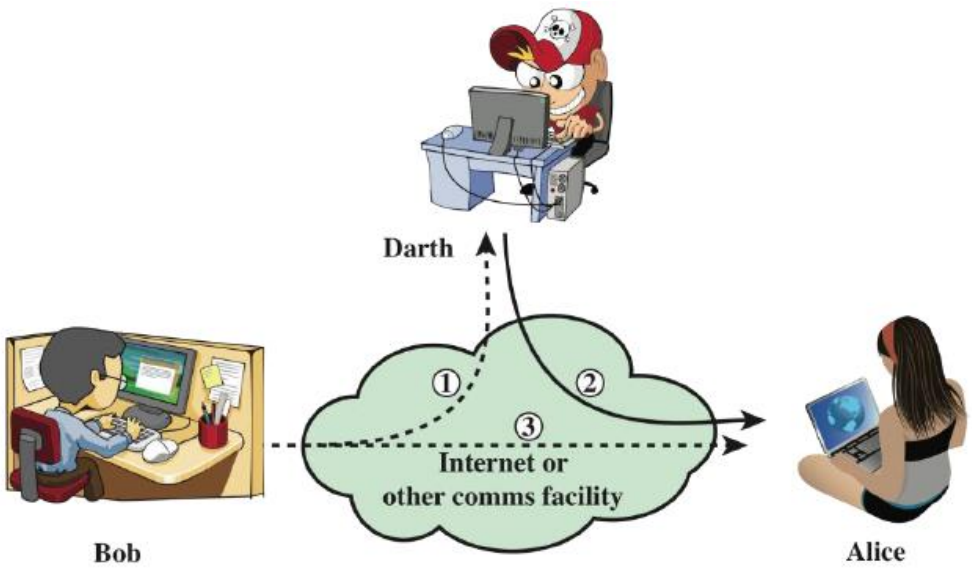


(a) Passive attacks

Fonte: Stallings

Ataque ativo

Os ataques ativos envolvem algum tipo de modificação do conteúdo ou do fluxo de dados ou a criação de um fluxo falso. Podem ser do tipo mascaramento ou disfarce (masquerade), repasse (replay), modificação de mensagens ou negação de serviço (denial of service).



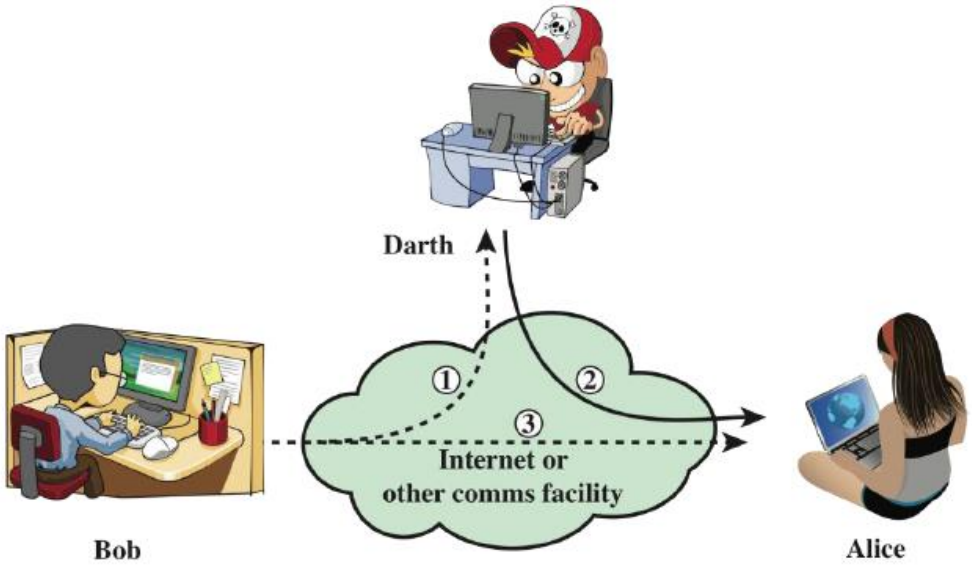
(b) Active attacks

Fonte: Stallings

Ataque ativo – continuação

O disfarce ocorre quando uma entidade finge ser outra diferente (2).

O repasse envolve a captura passiva de uma unidade de dados e sua subsequente retransmissão para produzir um efeito não autorizado (1, 2 e 3).

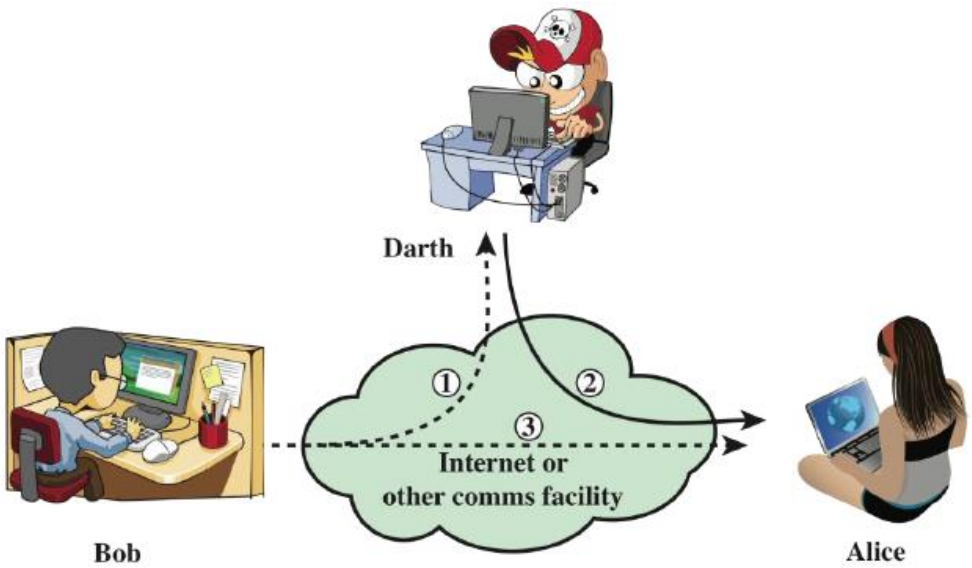


(b) Active attacks

Fonte: Stallings

Ataque ativo – continuação

A modificação de mensagens significa que parte de uma mensagem legítima é alterada, ou que as mensagens são atrasadas ou reordenadas, para produzir um efeito não autorizado (1 e 2).

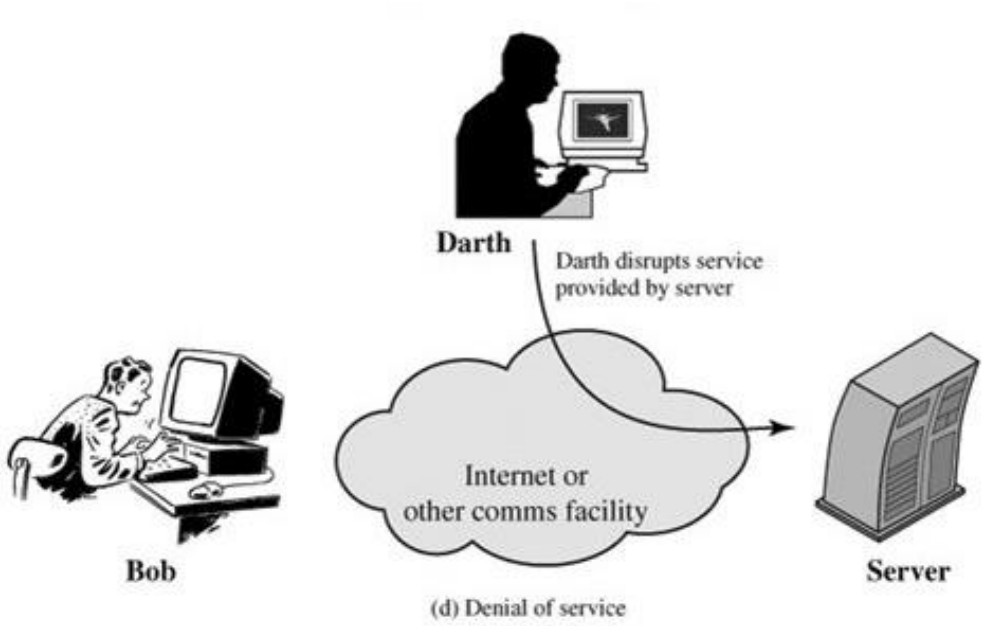


(b) Active attacks

Fonte: Stallings

Ataque ativo – continuação

A negação de serviço impede ou inibe o uso normal ou o gerenciamento das instalações de comunicações. Outra forma de negação de serviço é a interrupção de uma rede inteira, seja desativando a rede ou sobrecarregando-a com mensagens para degradar o desempenho.

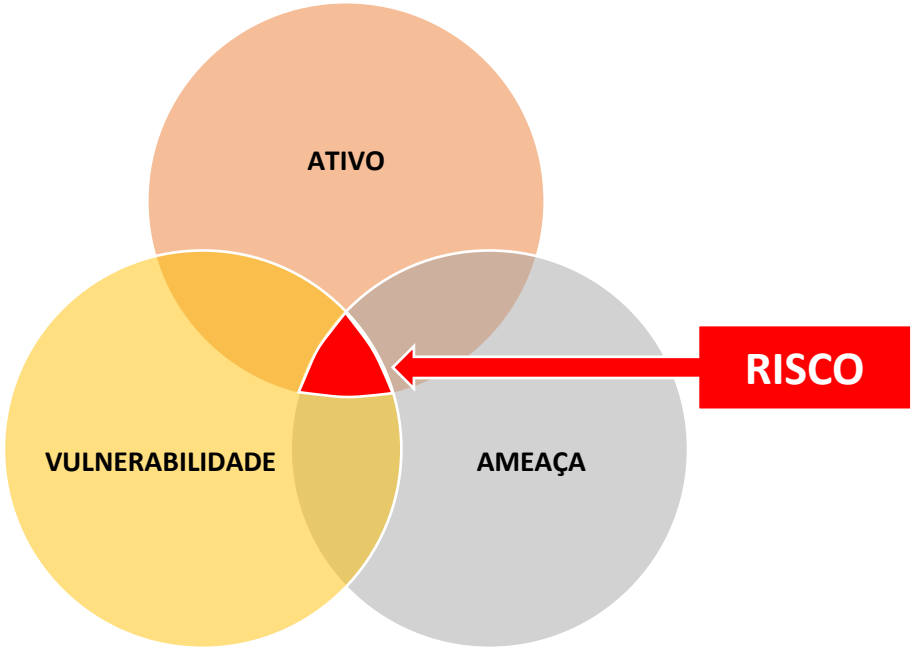


(d) Denial of service

Fonte: Stallings

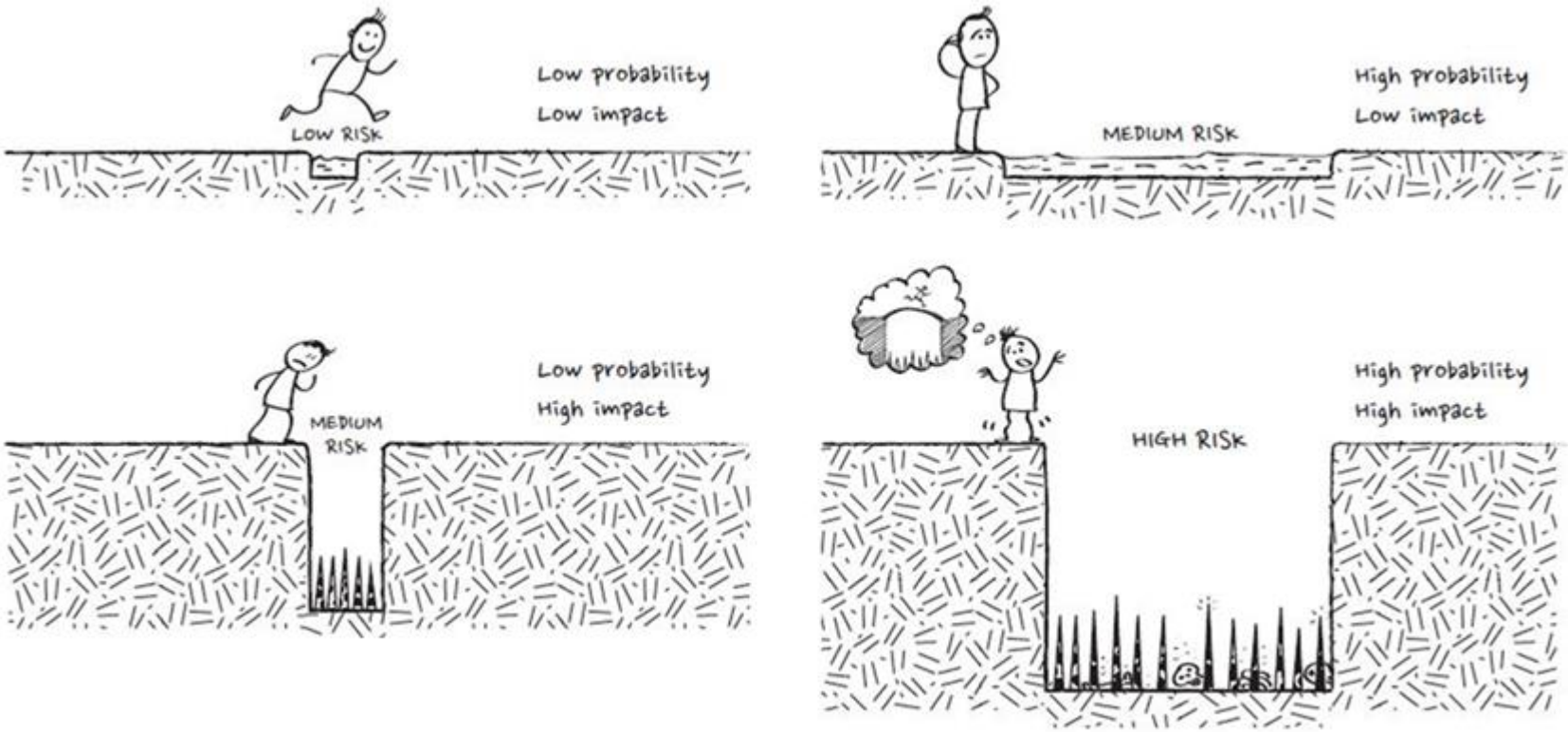
Riscos

Risco é a probabilidade de que as ameaças explorem as vulnerabilidades e comprometam os ativos.



OBS.: quando a exploração da vulnerabilidade é concretizada, temos um incidente.

Probabilidade e impacto



Fonte: christianespinosa.com

Proteção

Para que os ativos possam ser protegidos, deve-se tomar as seguintes medidas:

- Identificar o que se quer proteger;
- Avaliar os riscos;
- Desenvolver medidas de segurança e/ou remediação.

Proteção

CONTROLE

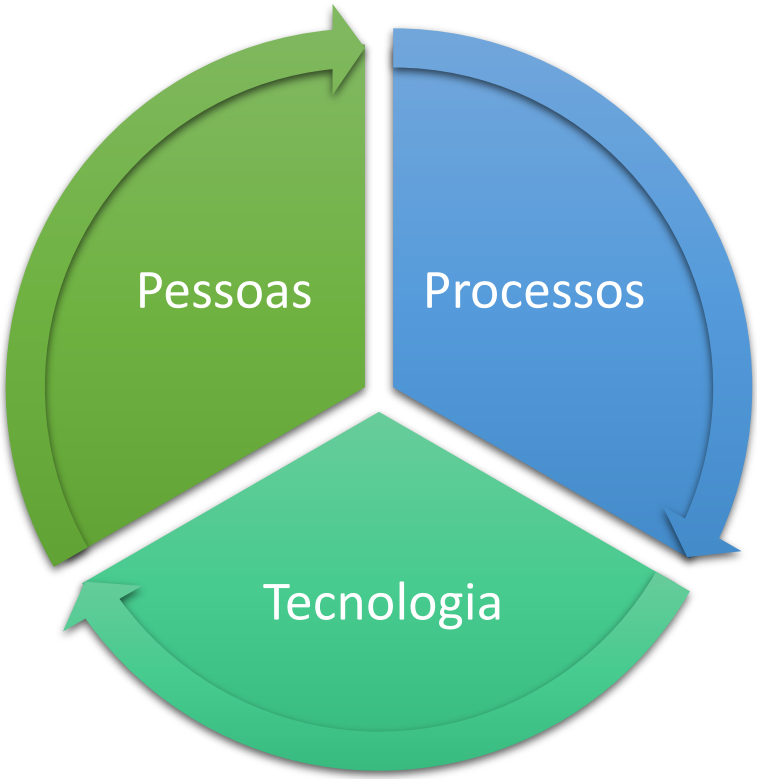
*A criptonita em si é uma ameaça. A vulnerabilidade do Superman é a sensibilidade ou “alergia” que ele tem da radiação emitida por ela.

Resposta aos riscos

Evitar, prevenir ou eliminar	• Elimina a causa raiz do problema a fim de evitar a exposição ao risco. **Pode afetar a utilidade do ativo.**
Transferir	• Não trata o risco, apenas transfere o ônus para um terceiro, de modo parcial ou total, como num seguro. **Há a necessidade de se pagar um prêmio para a parte que assume o risco.**
Mitigar	• Reduz a probabilidade de ocorrência de um incidente ou o seu impacto até um nível aceitável.
Aceitar	• Quando a probabilidade de ocorrência e o impacto são baixos ou quando não é possível aplicar nenhuma estratégia e decide-se arcar com as consequências.

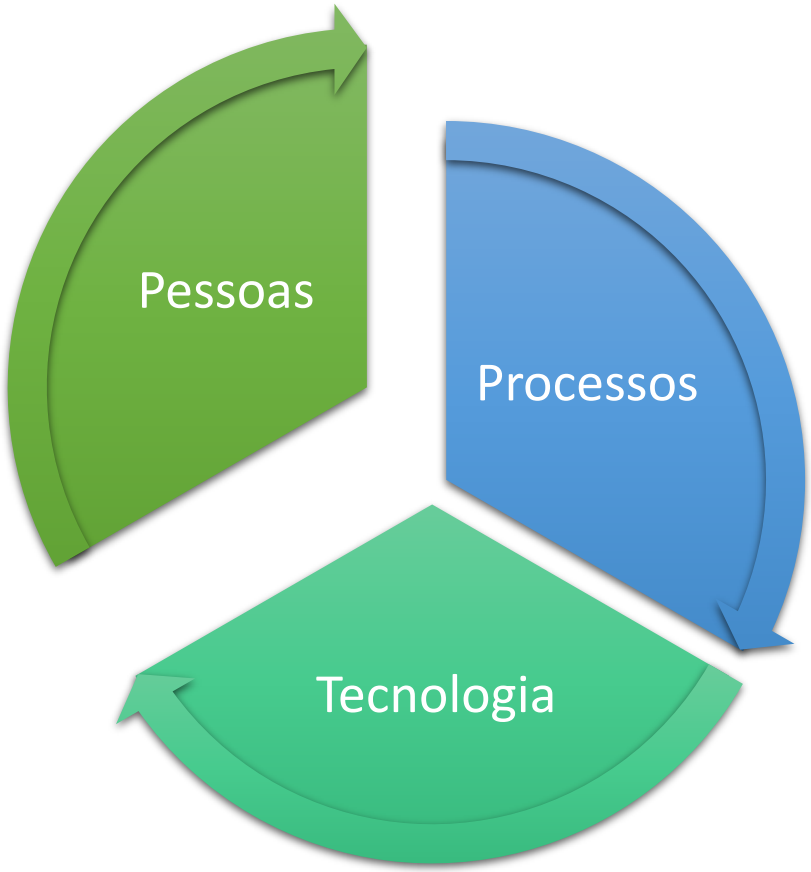
Pessoas, processos e tecnologia

O pilar de implementação de um sistema de gestão da segurança da informação (SGSI) é a tríade pessoas, processos e tecnologia. Não há como pensar a segurança da informação dentro das organizações sem levar em consideração estes três componentes.



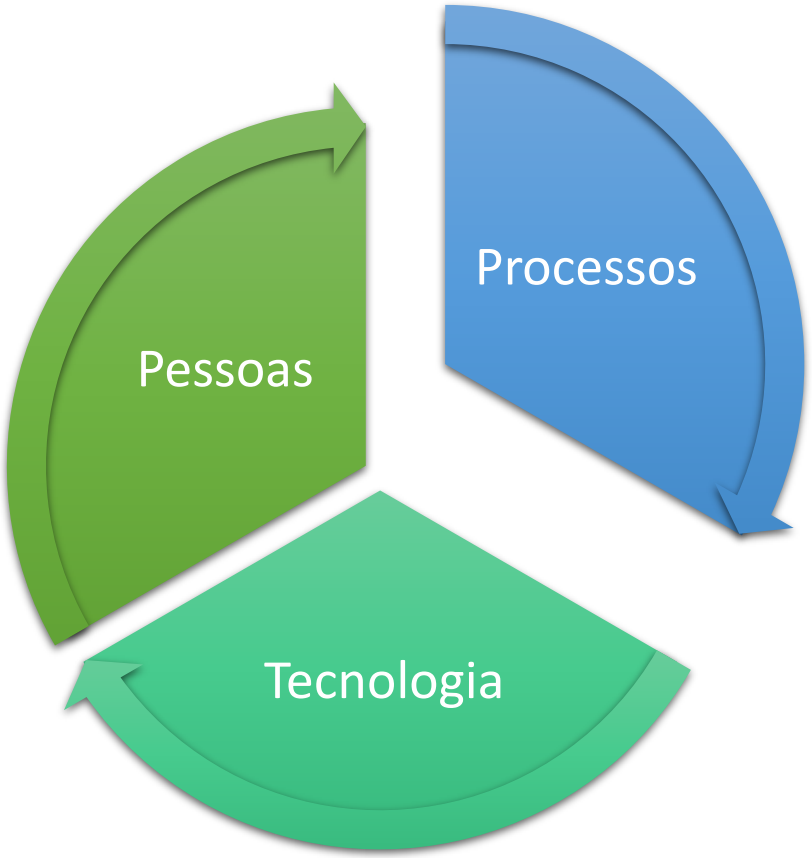
Pessoas, processos e tecnologia

- Pessoas – são ao mesmo tempo o elo mais fraco da cadeia de segurança (engenharia social) e ao mesmo tempo a essência da organizações, pois são elas que planejam, executam e suportam os processos de negócio e de segurança. São valorizados aspectos como conscientização (porque fazer), cultura (o que fazer) e capacitação (como fazer).



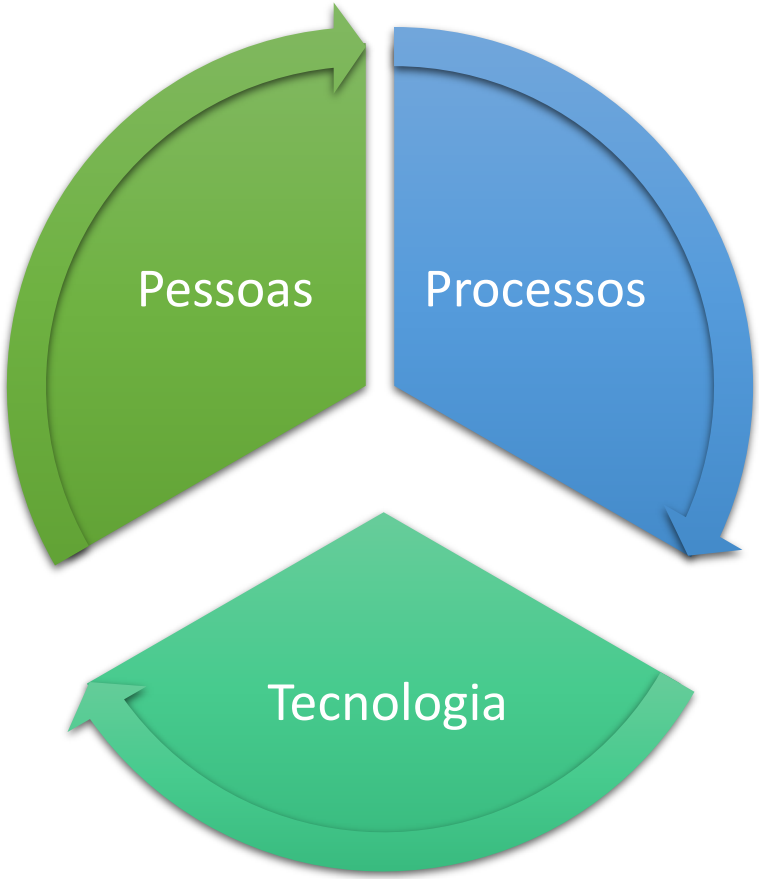
Pessoas, processos e tecnologia

- Processos – compreende o modelo de negócios e seus objetivos, a identificação dos ativos que se quer proteger e a estratégia de segurança para tal; a definição das políticas de segurança e sua implementação, as normas, os procedimentos e a metodologia adotados para manter e melhorar o SGSI. Inclui também as normas, documentações e padrões de conformidade. Os processos devem ser flexíveis tanto quanto possível, de tal modo que a organização não perca a sua dinâmica e agilidade para responder aos desafios diários.



Pessoas, processos e tecnologia

- Tecnologia – são as ferramentas e soluções de segurança adotadas para suportar a estratégia de segurança da informação dos ativos identificados. Devem estar de acordo com a Política de Segurança da Informação, as demais normas e processos definidos para o seu cumprimento.



Segurança física

De acordo com a norma NBR ISO/IEC 27002, o projeto de implantação de um *Datacenter* deve contemplar uma série de características únicas, de forma que sejam projetadas e aplicadas proteção física contra sinistros.

De forma geral, deve-se garantir proteção:

- contra acesso não autorizado por meio de dispositivos de segurança;
- contra incêndios e demais intempéries, por meio de implantação de salas cofre;
- equipamentos de contingência e mídias de backup devem ficar armazenadas em local diverso;
- etc.

Segurança lógica

A segurança lógica pode ser implementada com o uso de proteção nos seguintes níveis:

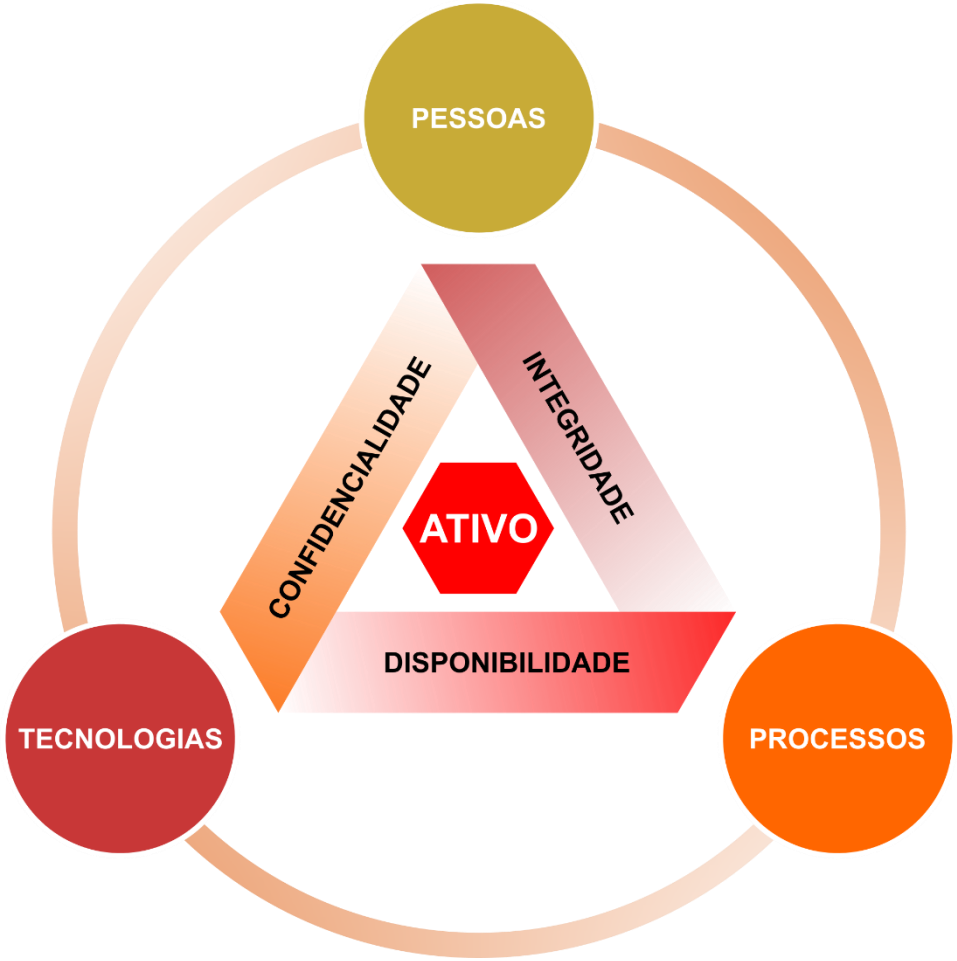
- na borda da rede – por meio do uso de firewall e snort;
- no interior da rede – por meio do uso de antivírus e antispam e outros mecanismos para controle de acesso;
- etc.

Segurança em recursos humanos

A segurança em recursos humanos pode ser implementada da seguinte forma:

- cuidados na contratação e dispensa de pessoal;
- documentação de procedimentos quanto ao uso de recursos;
- etc.

Segurança – resumo



Fonte: SANTANA, W. R.; et. al. Aplicação da norma NBR ISO/IEC 27002 para atendimento do Marco Civil da Internet e da LGPD. CONTECSI USP – 17th International Conference on Information Systems and Technology Management, São Paulo, 2020

Para saber mais...

... leia o capítulo 3 do livro Fundamentos de segurança da informação com base na ISO 27001 e na ISO 27002, de Jule Hintzbergen

... leia o capítulo 1 do livro Criptografia e segurança de redes: princípios e práticas, de William Stallings

Módulo 4

Tipos de malware e principais ataques

Introdução

Malware é um termo genérico para qualquer tipo de “**mal**icious soft**ware**” (“software malicioso”) projetado para se infiltrar em dispositivos sem o conhecimento do usuário.

Existem muitos tipos de malware, e cada um funciona de maneira diferente na busca de seus objetivos.

No entanto, todas as variantes de malware compartilham duas características fundamentais: são sorrateiras e trabalham ativamente contra os interesses dos usuários.

Fonte: avast.com

Tipos de malware

A grande maioria dos malwares, dependendo de seu funcionamento, se enquadra em uma das seguintes categorias básicas:

Fonte: avast.com

Tipos de malware – Ransomware

Ransomware é a versão malware da carta de resgate de um sequestrador.

Normalmente, ele bloqueia ou nega o acesso ao dispositivo e arquivos até que ele receba um resgate.

Pessoas ou grupos que armazenam informações vitais em seus dispositivos correm risco com a ameaça de ransomware.

Fonte: avast.com

Tipos de malware – Spyware

Spyware coleta informações sobre um dispositivo ou rede e transmite esses dados para o invasor.

Os cibercriminosos normalmente usam spyware para monitorar a atividade de uma pessoa na Internet e coletar dados pessoais, incluindo credenciais de login, números de cartão de crédito ou informações financeiras, para fins de fraude ou roubo de identidade.

Fonte: avast.com

Tipos de malware – Worms

Worms são projetados com um objetivo em mente: proliferação.

Um worm infecta um computador e se replica em seguida, espalhando-se para dispositivos adicionais enquanto permanece ativo em todas as máquinas infectadas.

Alguns worms atuam como agentes de entrega para instalação de malware adicional.

Outros tipos são projetados apenas para se espalhar, sem causar danos intencionais às máquinas host, mas eles sobrecarregam as redes com demandas de largura de banda.

Fonte: avast.com

Tipos de malware – Adware

O trabalho do adware é gerar receita para o desenvolvedor exibindo para a vítima anúncios indesejados.

Tipos comuns de adware incluem jogos gratuitos ou barras de ferramentas do navegador.

Eles coletam dados pessoais sobre a vítima para usá-los para personalizar os anúncios que exibem.

Embora a maioria dos adwares seja instalada legalmente, eles são tão irritantes quanto outros tipos de malware.

Fonte: avast.com

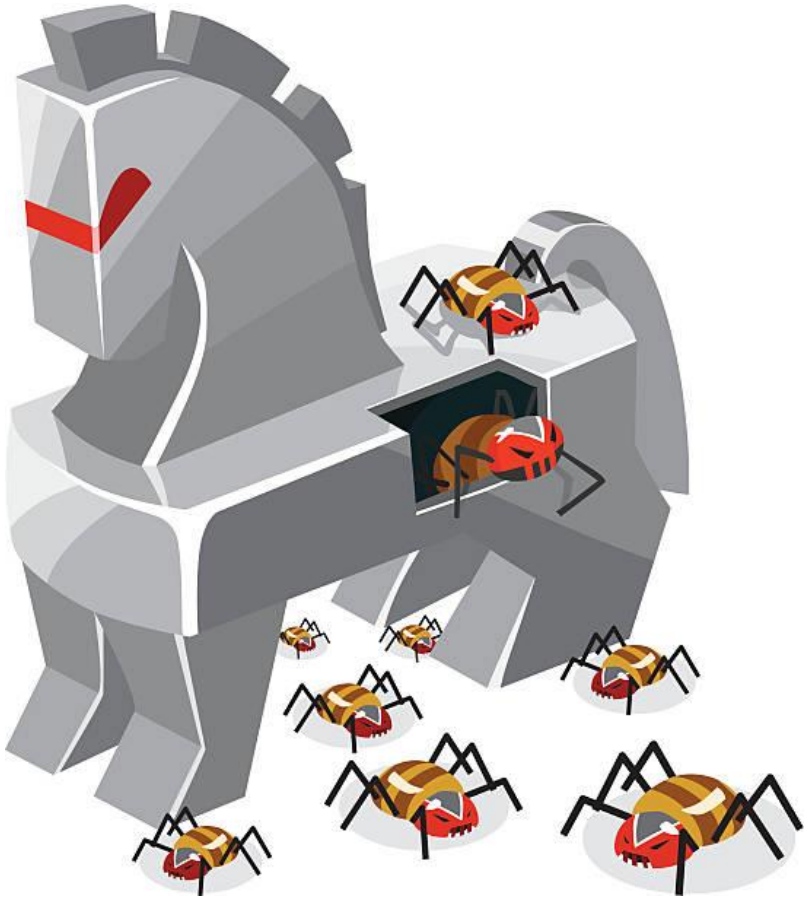
Tipos de malware – Cavalo de Tróia

Os poetas gregos antigos contavam que os guerreiros atenienses se esconderam dentro de um cavalo de madeira gigante e saíram depois que os troianos o puxaram para dentro das muralhas da cidade.

Um cavalo de Tróia é, portanto, um veículo para atacantes ocultos.

Cavalo do Troia é um malware que se infiltra no dispositivo da vítima apresentando-se como software legítimo.

Uma vez instalado, o cavalo do Troia é ativado e às vezes ele pode até mesmo baixar malware adicional.



Fonte: avast.com

Tipos de malware – Botnet

Um botnet não é um tipo de malware, mas uma rede de computadores ou código de computador que pode transmitir ou executar malware.

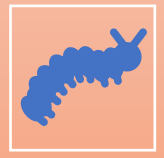
Os invasores infectam um grupo de computadores com software malicioso, conhecidos como “bots”, que pode receber comandos de seu controlador.

Esses computadores formam uma rede, fornecendo ao controlador acesso a um poder de processamento coletivo substancial, que pode ser usado para coordenar ataques, enviar spam, roubar dados e criar anúncios falsos no seu navegador.

Fonte: avast.com

Vírus vs Worms vs Cavalos de Tróia

Vírus é um programa de computador ou software que se conecta a outro software ou programa de computador para danificar o sistema do computador. Quando o programa de computador é executado anexado com vírus, ele executa alguma ação, como excluir um arquivo do sistema do computador. Vírus não pode ser controlado por controle remoto.



Worms também são um programa de computador como vírus, mas não modifica o programa. Ele se replica cada vez mais para causar lentidão no sistema do computador. Worms podem ser controlados por controle remoto.

Cavalos de Tróia não se replicam como vírus e worms. É um pedaço de código oculto que rouba as informações importantes do usuário. Por exemplo, o software Cavalo de Tróia observa o ID de e-mail e a senha ao entrar no navegador da Web para registro.

Fonte: geeksforgeeks.org

Principais tipos de ataque

Um ciberataque é um tipo de ação ofensiva que alveja os sistemas de informação dos computadores, a infraestrutura, as redes de computadores ou dispositivos pessoais, usando vários métodos para roubar, alterar ou destruir os dados e os sistemas de informação.

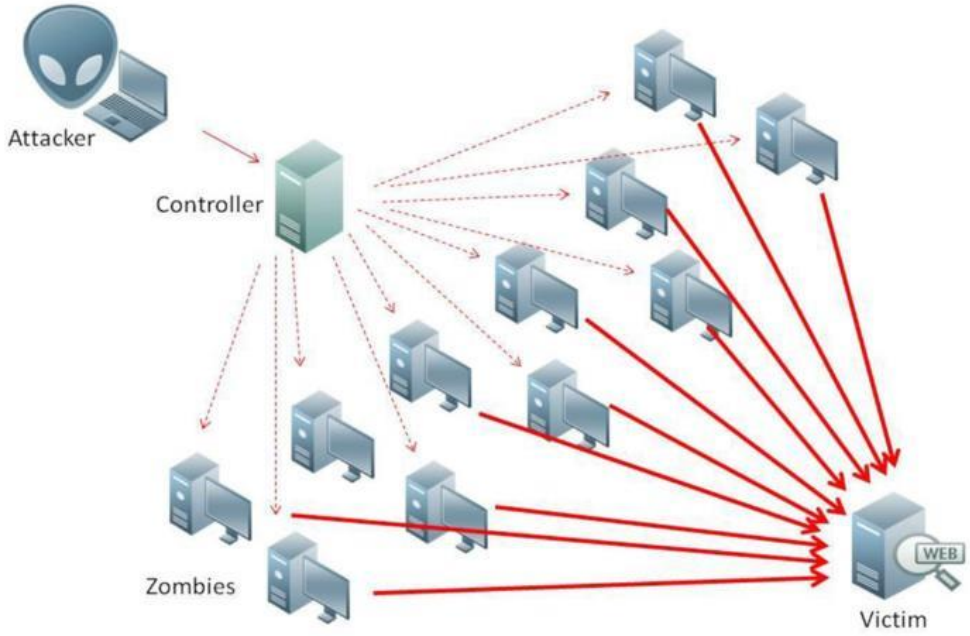
Segue abaixo uma lista de alguns tipos de ciberataques mais comuns:

- Denial-of-Service (DoS) e Distributed Denial-of-Service (DDoS);
- Ataque Adversary-in-the-Middle (AitM);
- Ataques de Phishing e Spear Phishing;
- Ataques de Drive-by;
- Ataques de senha;
- Ataque de injeção SQL;
- Ataque de Cross-site Scripting (XSS);
- Ataque de espionagem;
- Ataque de aniversário;
- Ataques de malware.

Fonte: Top 10 Most Common Types of Cyber Attacks, de Jeff Melnick, disponível em blog.netwrix.com

Denial-of-Service (DoS) e Distributed Denial-of-Service (DDoS) – continuação

Um ataque de Denial-of-Service sobrecarrega os recursos de um sistema para que ele não responda aos serviços solicitados. Um ataque de DDoS também ataca os recursos dos sistema, porém é lançado em um maior número de estações que estão infectadas com o software malicioso controlado pelo atacante.



Fonte: Top 10 Most Common Types of Cyber Attacks, de Jeff Melnick, disponível em blog.netwrix.com

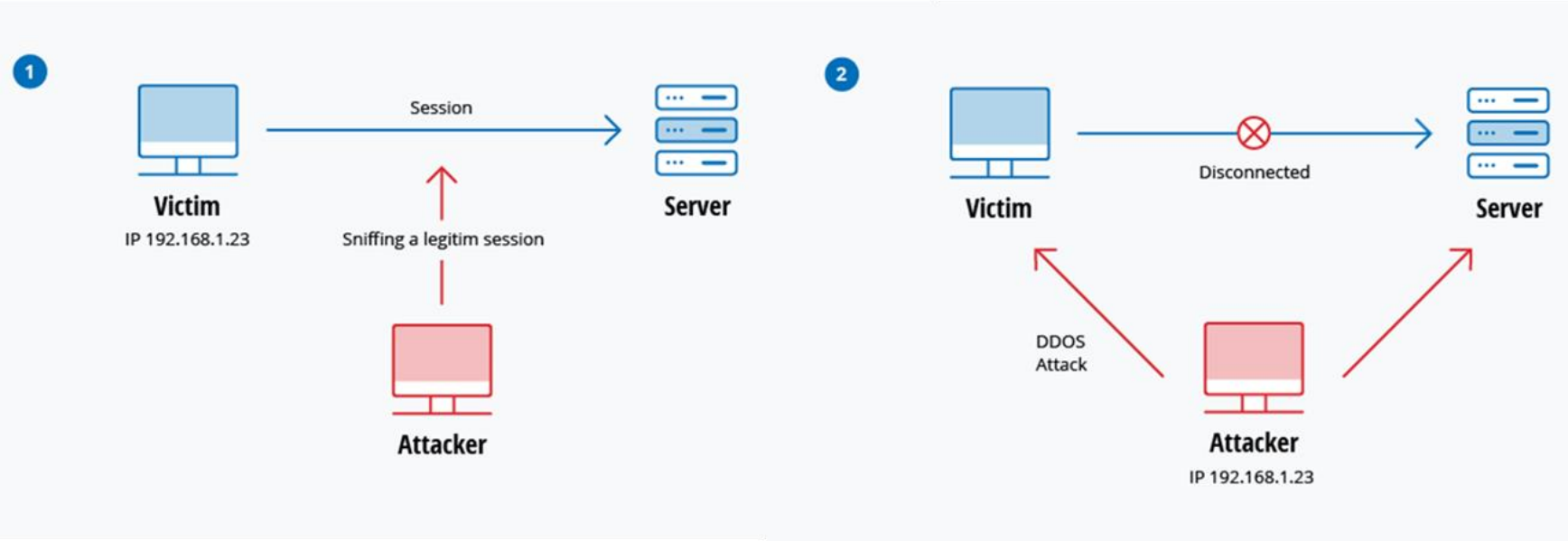
Denial-of-Service (DoS) e Distributed Denial-of-Service (DDoS) – continuação

Ao contrário de ataques que são feitos para habilitar que o atacante ganhe ou aumente seu acesso em um ambiente, o Denial-of-Service não oferece benefícios diretos aos atacantes. Para alguns deles, a satisfação de ter o serviço negado é suficiente. Entretanto, se o recurso atacado pertence ao competidor do negócio, então o benefício do atacante pode ser real. Outro propósito do ataque de DoS é para deixar um sistema offline para que um ataque diferente seja lançado. Um exemplo comum é usurpar uma sessão.

Fonte: Top 10 Most Common Types of Cyber Attacks, de Jeff Melnick, disponível em blog.netwrix.com

Adversary-in-the-Middle (AitM)

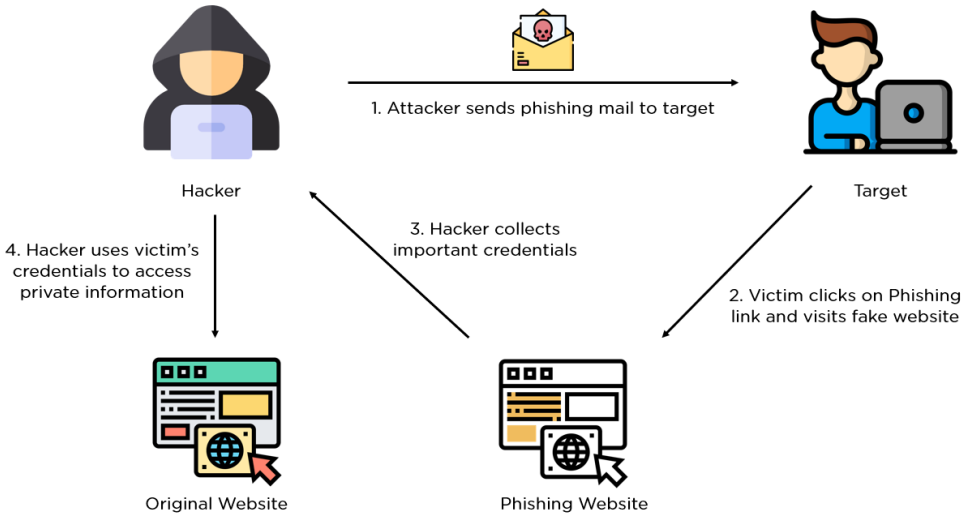
Um ataque AitM ocorre quando um hacker se insere entre os meios de comunicação de um cliente e um servidor.



Fonte: Top 10 Most Common Types of Cyber Attacks, de Jeff Melnick, disponível em blog.netwrix.com

Phishing e Spear Phishing

Ataque de phishing é uma prática de enviar e-mails que parecem ser de fontes confiáveis com o objetivo de ganhar acesso a informação pessoal ou influenciar os usuários a fazer algo. Utiliza-se bastante a engenharia social neste tipo de ataque. Pode haver um anexo no e-mail que carrega um malware para o seu computador. Ele também pode ser um link para um site ilegítimo que pode te enganar a baixar um malware ou te fazer entregar sua informação pessoal.



Fonte: Top 10 Most Common Types of Cyber Attacks, de Jeff Melnick, disponível em blog.netwrix.com

Phishing e Spear Phishing – continuação

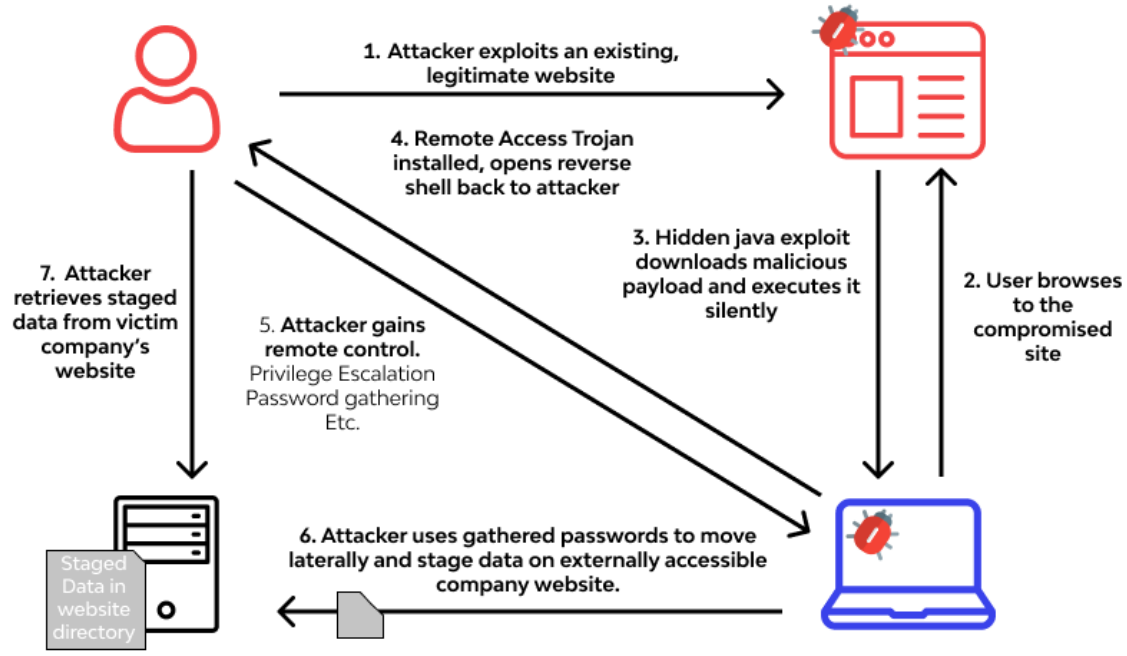
Spear phishing é um tipo de ataque de atividade de phishing bem direcionada. Os atacantes levam bastante tempo para conduzir uma pesquisa nos alvos e criar mensagens que pareçam pessoais e relevantes. Por isso, o spear phishing pode ser bem difícil de se identificar e até de se defender.

Fonte: Top 10 Most Common Types of Cyber Attacks, de Jeff Melnick, disponível em blog.netwrix.com

Drive-by

Ataques de download Drive-By são comuns no método de espalhar malware.

Os hackers procuram sites inseguros e plantam um script malicioso no código HTTP ou PHP em uma das páginas.



Fonte: Top 10 Most Common Types of Cyber Attacks, de Jeff Melnick, disponível em blog.netwrix.com

Drive-by – continuação

Esse script pode instalar um malware diretamente no computador de alguém que visita o site, ou pode redirecionar a vítima a um site controlado por hackers.

Downloads Drive-by podem acontecer quando visitar um website, abrir uma mensagem de e-mail ou em uma janela de pop-up.

Ao contrário de outros tipos de ciberataques, um drive-by não requer que um usuário faça algo para habilitar o ataque.

Um download drive-by pode tomar vantagem de um aplicativo, sistema operacional ou navegador que contenha falhas de segurança devido a atualizações mal sucedidas ou falta de atualizações.

Fonte: Top 10 Most Common Types of Cyber Attacks, de Jeff Melnick, disponível em blog.netwrix.com

Ataques de senha

Por conta das senhas serem o mecanismo mais comum de autenticar usuários a um sistema de informação, obter senhas é uma forma de ataque comum e efetiva. Acesso a senha de uma pessoa pode ser obtida olhando na mesa de uma pessoa, realizando um "sniffing" na rede para conseguir senhas não criptografadas, usando engenharia social, ganhando acesso ao banco de dados de senhas ou até adivinhando. A última forma pode ser feita de forma manual ou sistemática:

- Adivinhação através de **força bruta** significa que você está usando um método aleatório tentando senhas diferentes na esperança de que alguma lógica seja aplicada tentando senhas relacionadas ao nome da pessoa, cargo, hobbies ou coisas similares;
- Em um **ataque de dicionário**, um dicionário de senhas comuns é usado para tentar ganhar acesso ao computador e rede de um usuário. Um dos métodos envolve copiar um arquivo criptografado que contenha a senha, aplicar a mesma criptografia em uma das senhas comuns do dicionário e comparar o resultado.

Fonte: Top 10 Most Common Types of Cyber Attacks, de Jeff Melnick, disponível em blog.netwrix.com

Ataques de senha

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

HIVE SYSTEMS

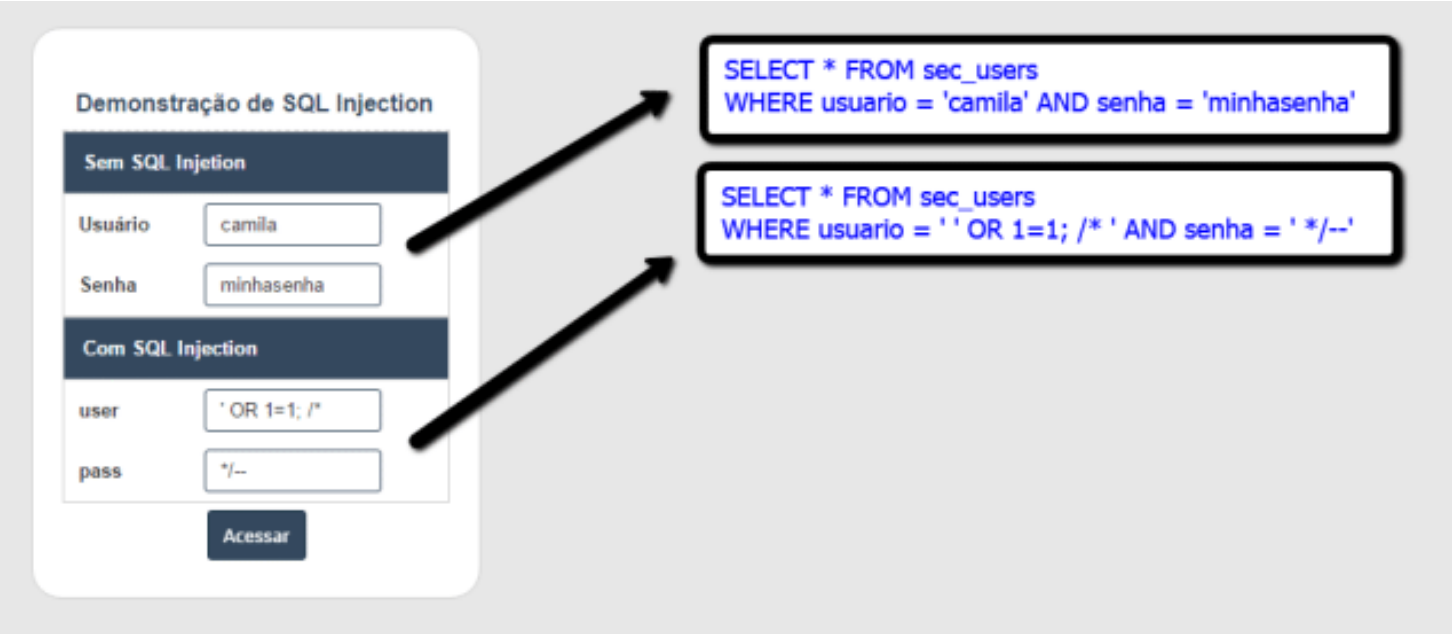
› Learn about our methodology at hivesystems.io/password

Fonte: Hive Systems

SQL injection

A injeção de SQL ocorre quando um malfeitor executa uma consulta de SQL no banco de dados através dos dados de entrada do cliente pra o servidor.

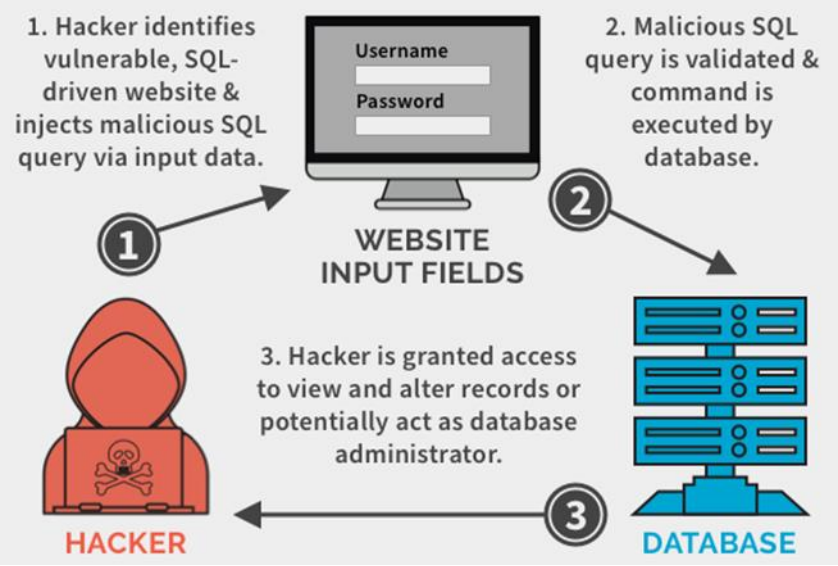
Comandos de SQL são inseridos na entrada do plano de dados (por exemplo, ao invés de um login ou senha) para executar os comandos predefinidos no SQL.



Fonte: Top 10 Most Common Types of Cyber Attacks, de Jeff Melnick, disponível em blog.netwrix.com

SQL injection – continuação

Uma injeção de SQL bem sucedida pode causar uma vulnerabilidade capaz de ler dados sensíveis do banco de dados, modificar (inserir, atualizar ou apagar) a base de dados, executar operações de administração (como desligamento) de um banco de dados, recuperar conteúdo de um determinado arquivo e, em alguns casos, enviar comandos para o sistema operacional.



Fonte: Top 10 Most Common Types of Cyber Attacks, de Jeff Melnick, disponível em blog.netwrix.com

Cross-site scripting (XSS)

Ataques de XSS usam recursos web de terceiros para executar scripts no navegador ou na aplicação da vítima.

Especificamente, o atacante injeta uma carga com um Javascript malicioso em um banco de dados de um site.

Quando a vítima requisita uma página do site, o site transmite a página com a carga do atacante como parte do corpo HTML para o navegador da vítima, que executa o script malicioso.

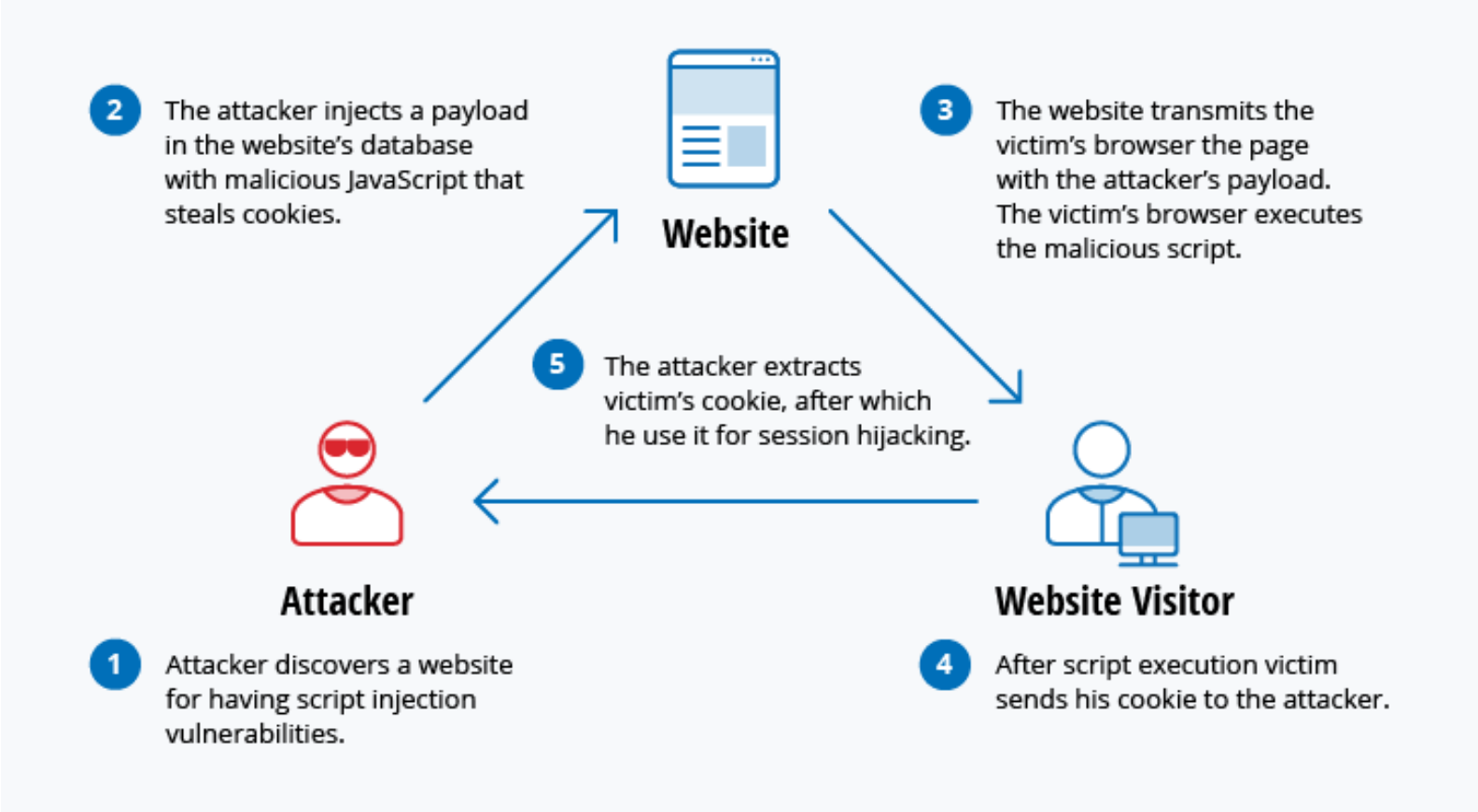
Ele pode por exemplo enviar o cookie da vítima para o servidor atacante, e então ele pode extraí-lo e usar para usurpar a sessão.

As consequências mais perigosas ocorrem quando o XSS é usado para explorar vulnerabilidades adicionais.

Essas vulnerabilidades podem habilitar o atacante a roubar não apenas cookies, mas também chaves de logs, capturar a tela, descobrir e coletar informação da rede e acessar e controlar remotamente a máquina da vítima.

Fonte: Top 10 Most Common Types of Cyber Attacks, de Jeff Melnick, disponível em blog.netwrix.com

Cross-site scripting (XSS) – continuação



Fonte: Top 10 Most Common Types of Cyber Attacks, de Jeff Melnick, disponível em blog.netwrix.com

Espionagem

Ciberataques de espionagem ocorrem através da interceptação do tráfego de rede. Por espionagem, um atacante pode obter senhas, números de cartão de crédito e outras informações confidenciais que um usuário pode estar mandando através da rede. A espionagem pode ser passiva ou ativa:

- Espionagem passiva – Um hacker detecta a informação ouvindo a transmissão da mensagem na rede;
- Espionagem ativa – Um hacker pega ativamente a informação se disfarçando como uma unidade amigável e enviando consultas aos transmissores. Isso é chamado de sondagem, digitalização ou adulteração.

Detectar ciberataques de espionagem passivas é mais importante do que encontrar ativos, já que ativos requerem que o atacante tenha conhecimento de unidades amigáveis conduzindo espionagem passiva antes.

A criptografia de dados é a melhor forma de prevenção contra espionagem.

Fonte: Top 10 Most Common Types of Cyber Attacks, de Jeff Melnick, disponível em blog.netwrix.com

Ataque de aniversário

Cibertaques de aniversário são feitos contra os algoritmos de hash que são usados para verificar a integridade da mensagem, software ou assinatura digital.

A mensagem processada por uma função de hash produz um digesto de mensagem ou message digest (MD) de largura fixa, independente da largura da mensagem de entrada, e esse MD único caracteriza a mensagem.

O ataque de aniversário se refere a probabilidade de encontrar essas duas mensagens aleatórias que geraram o mesmo MD quando processada pela função de hash.

Se um atacante calcular o mesmo MD para suas mensagens que o usuário tem, ele pode substituir seguramente a mensagem do usuário com a dele e o destinatário não será capaz de detectar a substituição mesmo comparando os MDs.

Para saber mais, faça uma pesquisa sobre o paradoxo do aniversário.

Fonte: Top 10 Most Common Types of Cyber Attacks, de Jeff Melnick, disponível em blog.netwrix.com

Ataques de malware

Softwares maliciosos podem ser definidos como softwares indesejados que são instalados no seu sistema sem o seu consentimento. Ele pode se anexar em um código legitimo e se propagar, ele pode se esconder em aplicações uteis e se replicar através da internet.

Segue abaixo alguns dos tipos mais comuns de malware:

- Vírus de Macro – infectam aplicações como o Word e o Excel. Os vírus de macro são anexados na sequência de inicialização da aplicação. Quando a aplicação é aberta, o vírus executa instruções para transferir o controle da aplicação. O vírus se replica e se anexa outro código no sistema do computador;

Fonte: Top 10 Most Common Types of Cyber Attacks, de Jeff Melnick, disponível em blog.netwrix.com

Ataques de malware – continuação

- Infectador de arquivos – se anexam ao código executável como arquivos .exe. O vírus então é instalado quando o código é carregado. Outra versão de um infectador de arquivos é um arquivo contendo um vírus com o mesmo nome, mas com a extensão. exe. Logo, quando o arquivo é aberto, o código do vírus é executado;
- Infectadores de sistema ou registros de inicialização – se anexa ao registro de inicialização mestre nos discos rígidos. Quando o sistema é iniciado, ele olhará o setor de inicialização e carregará o vírus na memória, onde ele se propagará a outros discos e computadores;

Fonte: Top 10 Most Common Types of Cyber Attacks, de Jeff Melnick, disponível em blog.netwrix.com

Ataques de malware – continuação

- Vírus polimórficos – se escondem através de vários ciclos de criptografia e descriptografia. O vírus criptografado e um motor de mutação associado são incialmente descriptografados por um programa de descriptografia. O vírus então procede a infectar a área do código. O motor de mutação então desenvolve uma nova rotina de descriptografia e copia o vírus com um algoritmo corresponde a nova rotina de descriptografia. O pacote criptografado é difícil de detectar e tem um auto nível de entropia por conta das várias modificações no seu código origem. Softwares de antivírus e ferramentas grátis como o Process Hacker usam esse recurso para detectá-los;
- Vírus invisíveis – tomam conta das funções do sistema para se esconder. Eles fazem isso comprometendo o software de detecção de malware para que o software reporte uma área que esteja infectada como segura. Esses vírus escondem qualquer aumento no tamanho de um arquivo infectado ou alterações a data e hora da última modificação.

Fonte: Top 10 Most Common Types of Cyber Attacks, de Jeff Melnick, disponível em blog.netwrix.com

Para saber mais...

... leia o artigo Top 10 Most Common Types of Cyber Attacks, de Jeff Melnick, disponível em https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/. Acesso em Março de 2022. [Versão em Inglês]

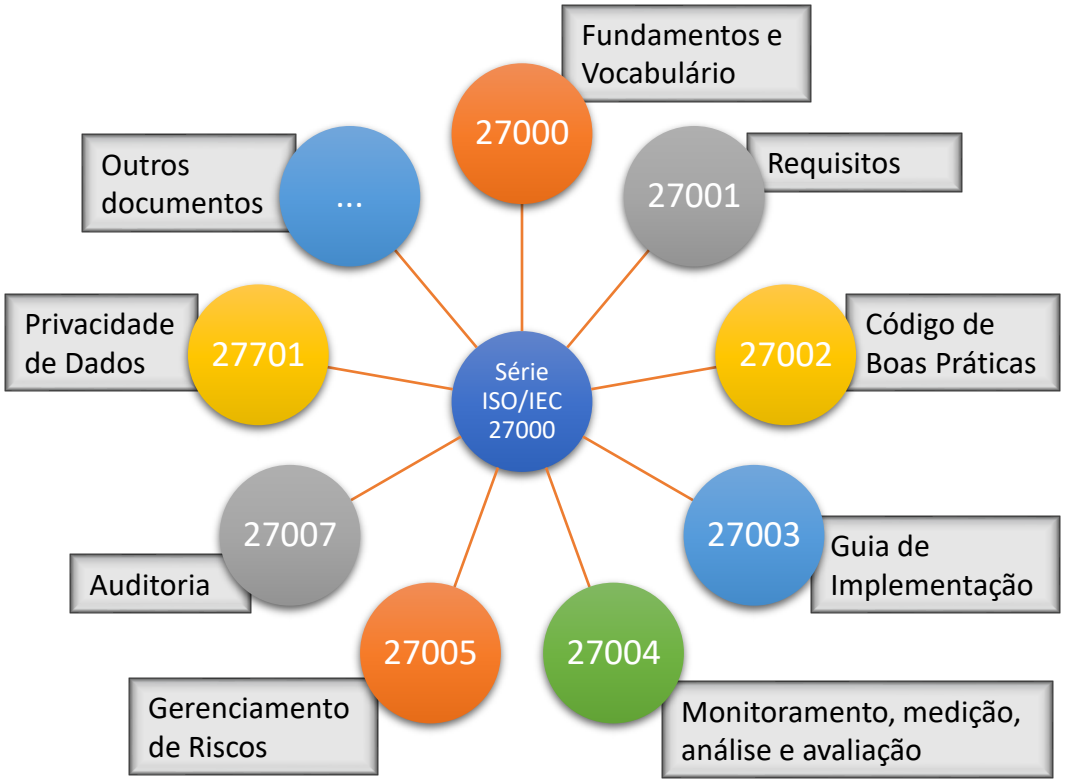
... leia o artigo TOP 10 – Os mais comuns ciber ataques, de Jeff Melnick, disponível em https://aiqon.com.br/blog/top-10-os-mais-comuns-ciber-ataques/. Acesso em Março de 2022. [Versão em Português]

Módulo 5

Norma ISO/IEC série 27000

ISO/IEC 27000 – série

A família ISO/IEC 27000 é uma série abrangente de normas para o gerenciamento da segurança da informação, dos riscos e dos controles. A série possui ao todo 47 documentos.



ISO/IEC 27000 – série

- ISO/IEC 27001 – guia para certificação de sistemas de gestão de segurança da informação;
- ISO/IEC 27002 (antiga ISO/IEC 17799) – código de boas práticas;
- ISO/IEC 27005 – gestão de riscos.

ISO/IEC 27001 – introdução

A ISO/IEC 27001:2013 foi preparada para prover requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação (SGSI). A sua adoção deve ser uma decisão estratégica da organização. O estabelecimento e a implementação do SGSI de uma organização são influenciados por:

a) suas necessidades e objetivos;

b) requisitos de segurança;

c) processos organizacionais; e

d) tamanho e estrutura da organização.

O SGSI preserva a confiabilidade (confidencialidade, integridade e disponibilidade) da informação por meio da aplicação de um processo de gestão de riscos, fornecendo a garantia necessária para as partes interessadas de que os riscos são adequadamente gerenciados.

É importante que o SGSI esteja integrado aos processos da organização!

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – processos

Processo é um conjunto de atividades que faz uso de recursos (humanos, materiais, financeiros, etc.) e que são gerenciados de forma a se obter um resultado.

De acordo com a ISO/IEC 27001:2006, a aplicação de um sistema de processos dentro de uma organização, junto com a identificação e interações destes processos, e a sua gestão podem ser consideradas como "abordagem de processo".

Fonte: NBR ISO/IEC 27001:2006

ISO/IEC 27001 – abordagem

Atualização da versão

A ISO/IEC 27001:2006 indicava claramente que o modelo “Plan-Do-Check-Act” (PDCA) era o que deveria ser aplicado por padrão para estruturar todos os processos do SGSI.

Já a nova versão da ISO/IEC 27001:2013 não especifica nenhum modelo de processo em particular. Ela exige apenas que seja utilizado um processo de melhoria contínua, a critério da organização.

Implicações para a transição

Para organizações com um SGSI já existente não há a necessidade de mudança, pois o modelo PDCA ainda é válido.

Já as organizações que estejam iniciando um SGSI baseado na ISO/IEC 27001:2013, devem identificar o melhor processo de melhoria contínua para o seu negócio.

ISO/IEC 27001 – abordagem

A abordagem de processo para a gestão da segurança da informação descrito na ISO/IEC 27001:2006 encoraja que seus usuários enfatizem a importância dos seguintes aspectos:

a) entendimento dos requisitos de segurança da informação de uma organização e da necessidade de estabelecer uma política e objetivos para a segurança de informação;

b) implementação e operação de controles para gerenciar os riscos de segurança da informação de uma organização no contexto dos riscos de negócio globais da organização;

c) monitoração e análise crítica do desempenho e eficácia do SGSI;

d) melhoria contínua baseada em medições objetivas.

Fonte: NBR ISO/IEC 27001:2006

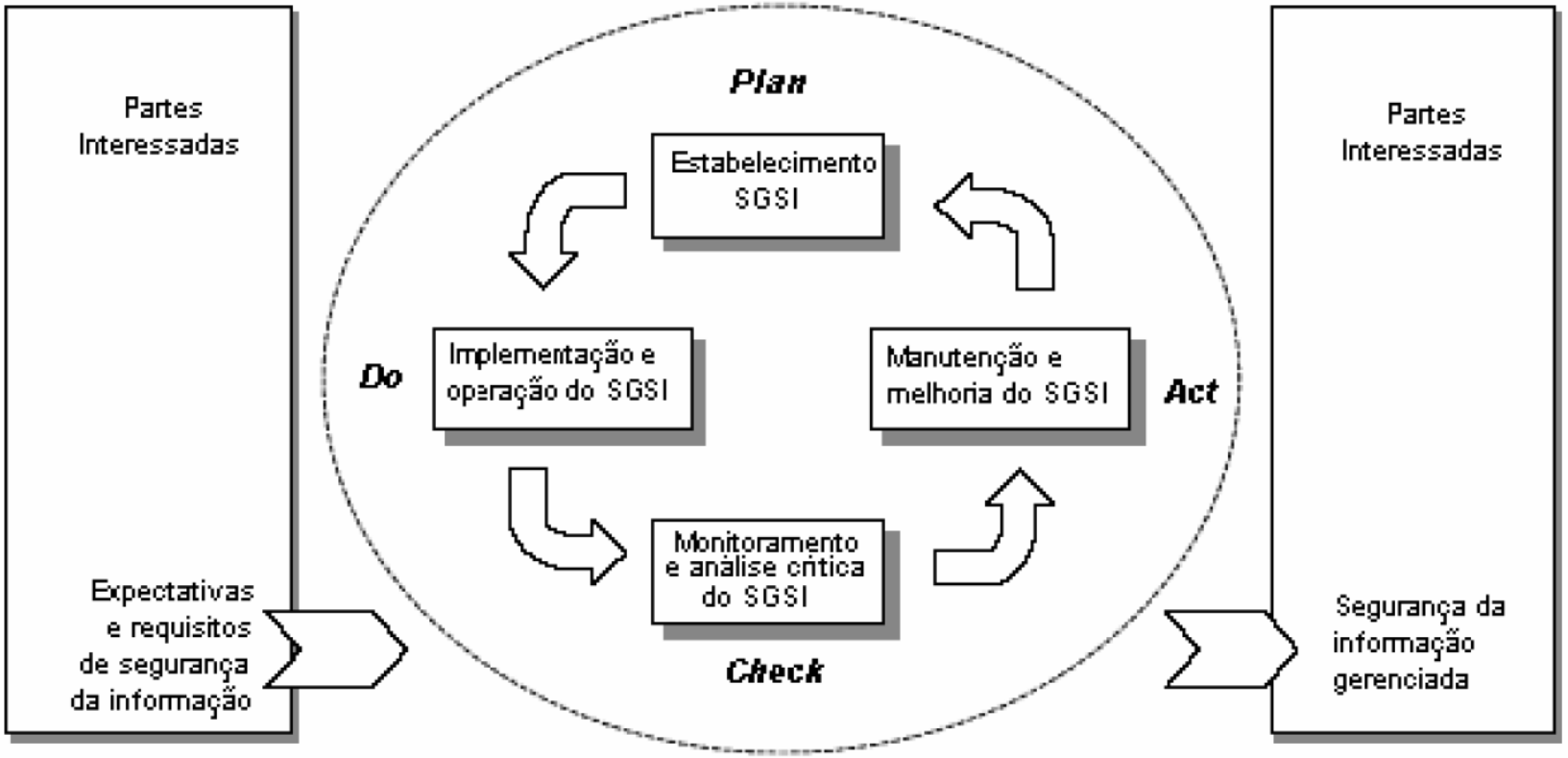
ISO/IEC 27001 – abordagem

A ISO/IEC 27001:2006 adota o modelo “Plan-Do-Check-Act” (PDCA), que é aplicado para estruturar todos os processos do SGSI.

A próxima figura ilustra como um SGSI considera as entradas de requisitos de segurança de informação e as expectativas das partes interessadas, e como as ações necessárias e processos de segurança da informação produzidos resultam no atendimento a estes requisitos e expectativas.

Fonte: NBR ISO/IEC 27001:2006

ISO/IEC 27001 – abordagem

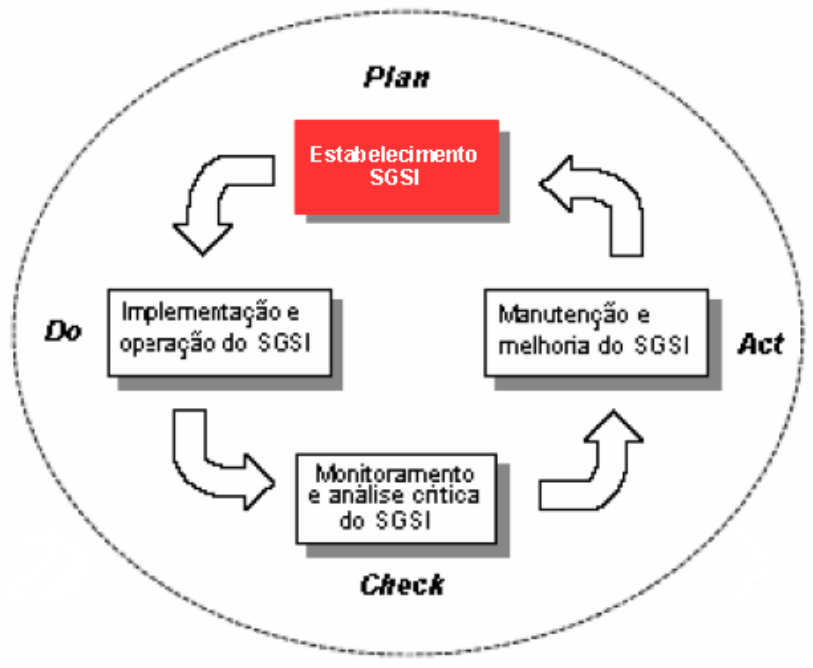


Modelo PDCA aplicado aos processos do SGSI

Fonte: NBR ISO/IEC 27001:2006

ISO/IEC 27001 – abordagem

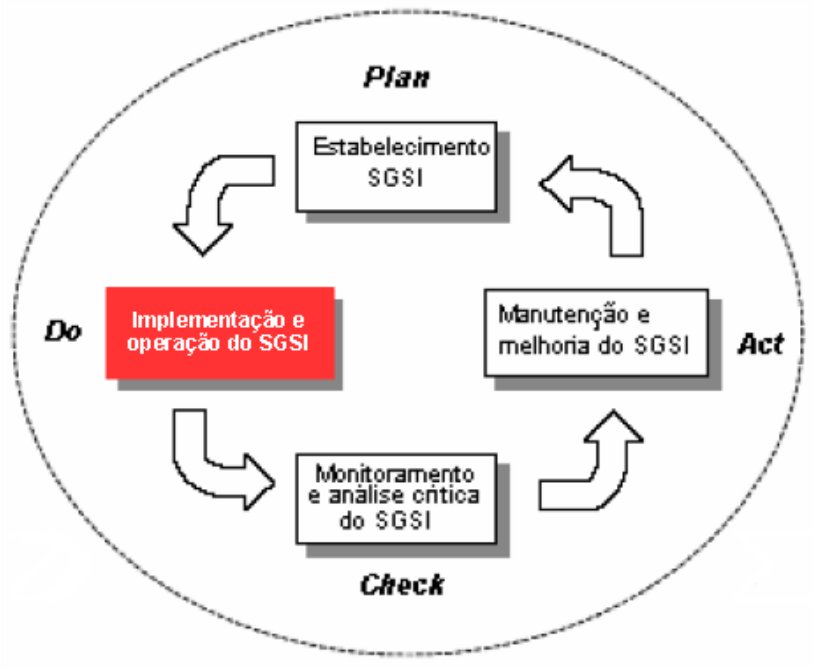
Plan – Estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.



Fonte: NBR ISO/IEC 27001:2006

ISO/IEC 27001 – abordagem

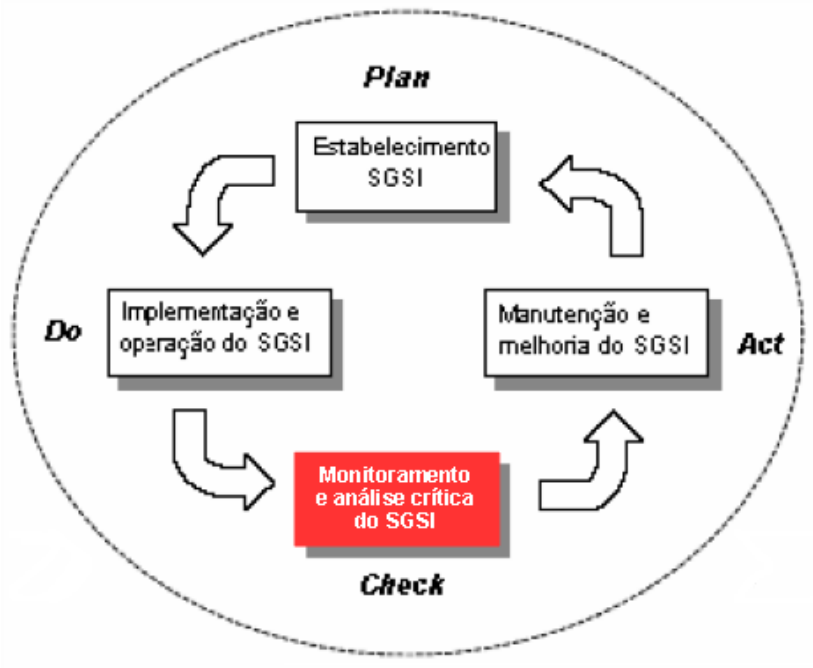
Do – Implementar e operar a política, controles, processos e procedimentos do SGSI.



Fonte: NBR ISO/IEC 27001:2006

ISO/IEC 27001 – abordagem

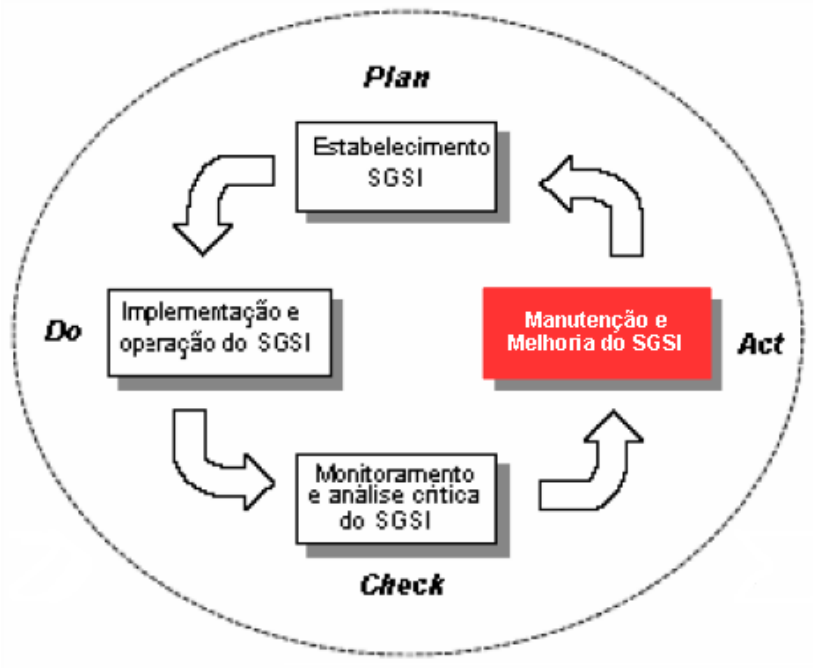
Check – Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção.



Fonte: NBR ISO/IEC 27001:2006

ISO/IEC 27001 – abordagem

Act – Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.



Fonte: NBR ISO/IEC 27001:2006

ISO/IEC 27001 – liderança

Liderança e comprometimento

A alta direção da organização deve demonstrar sua liderança e comprometimento em relação ao SGSI pelos seguintes meios:

a) assegurando que a política de segurança da informação e seus objetivos estão estabelecidos e são compatíveis com a estratégia da organização;

b) garantindo a integração dos requisitos do SGSI dentro dos processos da organização;

c) assegurando que os recursos necessários para o SGSI estão disponíveis;

d) comunicando a importância de uma gestão eficaz da segurança da informação e da conformidade com os requisitos do SGSI;

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – liderança

Liderança e comprometimento – continuação...

e) assegurando que o SGSI alcança seus resultados pretendidos;

f) orientando e apoiando pessoas que contribuam para eficácia do SGSI;

g) promovendo a melhoria contínua; e

h) apoiando outros papéis relevantes da gestão para demonstrar como sua liderança se aplica às áreas sob sua responsabilidade

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – liderança

Política

A alta direção deve estabelecer uma política de segurança da informação que:

a) seja apropriada ao propósito da organização;

b) inclua os objetivos de segurança da informação ou forneça a estrutura para estabelecer os objetivos de segurança da informação;

c) inclua o comprometimento em satisfazer os requisitos aplicáveis, relacionados com a segurança da informação;

d) inclua o comprometimento com a melhoria contínua do sistema de gestão da segurança da informação.

A política de segurança da informação deve ainda estar disponível como informação documentada, ser comunicada dentro da organização e estar disponível para as partes interessadas.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – liderança

Autoridades, responsabilidades e papéis organizacionais

A alta direção deve assegurar que as responsabilidades e autoridades dos papéis relevantes para a segurança da informação sejam atribuídos e comunicados.

A atribuição de responsabilidades e autoridade devem:

a) assegurar que o SGSI está em conformidade com os requisitos desta norma;

b) relatar sobre o desempenho do SGSI para a alta direção.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – planejamento

Ações para contemplar riscos e oportunidades – Tratamento de riscos

A organização deve definir e aplicar um processo de tratamento dos riscos de segurança da informação para:

a) selecionar, de forma apropriada, as opções de tratamento dos riscos de segurança da informação, levando em consideração os resultados da avaliação do risco;

b) determinar todos os controles que são necessários para implementar as opções escolhidas do tratamento do risco da segurança da informação;

c) comparar os controles necessários para implementar as opções de tratamento dos riscos de segurança da informação com aqueles constantes da Tabela de Referência aos Controles e Objetivos de Controle e verificar se algum controle necessário foi omitido;

d) elaborar uma declaração de aplicabilidade que contenha os controles necessários e a justificativa para inclusões, sejam eles implementados ou não, bem como a justificativa para a exclusão dos controles da Tabela de Referência aos Controles e Objetivos de Controle;

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – planejamento

Ações para contemplar riscos e oportunidades – Tratamento de riscos – cont....

e) preparar um plano para tratamento dos riscos de segurança da informação; e

f) obter a aprovação dos responsáveis pelos riscos do plano de tratamento dos riscos de segurança da informação e a aceitação dos riscos residuais de segurança da informação.

O processo de tratamento dos riscos de segurança da informação deve ser documentado.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – apoio

Recursos

A organização deve determinar e prover recursos necessários para o estabelecimento, implementação, manutenção e melhoria contínua do SGSI.

Competência

A organização deve:

a) determinar a competência necessária das pessoas que realizam trabalho sob o seu controle e que afeta o desempenho da segurança da informação;

b) assegurar que essas pessoas são competentes, com base na educação, treinamento ou experiência apropriados;

c) onde aplicável, tomar ações para adquirir a competência necessária e avaliar a eficácia das ações tomadas; e

d) reter informação documentada apropriada como evidência da competência.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – apoio

Conscientização

Pessoas que realizam trabalho sob o controle da organização devem estar cientes da:

a) política de segurança da informação;

b) suas contribuições para a eficácia do sistema de gestão da segurança da informação, incluindo os benefícios da melhoria do desempenho da segurança da informação; e

c) implicações da não conformidade com os requisitos do sistema de gestão da segurança da informação.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – apoio

Comunicação

A organização deve determinar as comunicações internas e externas relevantes para o sistema de gestão da segurança da informação incluindo:

a) o que comunicar;

b) quando comunicar;

c) quem comunicar;

d) quem será comunicado; e

e) o processo pelo qual a comunicação será realizada.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27001 – avaliação de desempenho

Monitoramento, medição, análise e avaliação

A organização deve avaliar o desempenho da segurança da informação e a eficácia do SGSI. Ela deve determinar:

a) o que precisa ser monitorado e medido;

b) os métodos para monitoramento, medição, análise e avaliação, conforme aplicável, para assegurar resultados válidos;

c) quando o monitoramento e a medição devem ser realizados;

d) o que deve ser monitorado e medido;

e) quando os resultados do monitoramento e da medição devem ser analisados e avaliados e por quem.

A evidência do monitoramento e dos resultados da medição devem ser documentados.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27002 – introdução

Como estabelecer requisitos de segurança da informação?

É essencial que uma organização identifique os seus requisitos de segurança da informação. Existem três fontes principais de requisitos de segurança da informação:

1. A avaliação de riscos para a organização, levando-se em conta os objetivos e as estratégias globais de negócio da organização. Por meio da avaliação de riscos, são identificadas as ameaças aos ativos e as vulnerabilidades destes, e realizada uma estimativa da probabilidade de ocorrência das ameaças e do impacto potencial ao negócio.
2. A legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que a organização, seus parceiros comerciais, contratados e provedores de serviço têm que atender, além do seu ambiente sociocultural.
3. Os conjuntos particulares de princípios, objetivos e os requisitos do negócio para o manuseio, processamento, armazenamento, comunicação e arquivo da informação, que uma organização tem que desenvolver para apoiar suas operações.

A ABNT NBR ISO/IEC 27005 fornece diretrizes sobre gestão de riscos de segurança da informação, incluindo orientações sobre avaliação de riscos, tratamentos de riscos, aceitação de riscos, comunicação de riscos, monitoramento e análise crítica dos riscos.

Fonte: NBR ISO/IEC 27002:2013

ISO/IEC 27002 – análise de riscos

Analisando/avaliando os riscos de segurança da informação

As análises/avaliações de riscos devem:

- Identificar, quantificar e priorizar os riscos com base em critérios para aceitação dos mesmos, para orientar e determinar as ações de gestão apropriadas e as prioridades para o gerenciamento dos riscos de segurança da informação;
- Incluir um enfoque sistemático para estimar a magnitude do risco (análise de riscos) e o processo de comparar os riscos estimados contra os critérios de risco para determinar a significância do risco (avaliação do risco);
- Ser realizadas periodicamente para contemplar as mudanças nos requisitos de segurança da informação e na situação de risco. Essas análises/avaliações de riscos devem ser realizadas de forma metódica, capaz de gerar resultados comparáveis e reproduzíveis.
- Ter um escopo claramente definido para ser eficaz e incluir os relacionamentos com as análises/avaliações de riscos em outras áreas, se necessário.

Fonte: NBR ISO/IEC 27002:2005

ISO/IEC 27002 – controles

Seleção de controles

Controles podem ser selecionados desta norma ou de outros conjuntos de controles, ou novos controles podem ser projetados para atender às necessidades específicas, conforme apropriado.

A seleção de controles de segurança da informação depende das decisões da organização, baseadas nos critérios para aceitação de risco, nas opções para tratamento do risco e no enfoque geral da gestão de risco aplicado à organização, e convém que a seleção destes controles também esteja sujeita a todas as legislações e regulamentações nacionais e internacionais relevantes. A seleção de controles também depende da maneira pela qual os controles interagem para prover uma proteção segura.

Fonte: NBR ISO/IEC 27002:2013

ISO/IEC 27002 – estrutura

Estrutura da norma

Contém 14 seções de controles de segurança da informação, que juntas totalizam 35 categorias principais de segurança ou objetivos de controle, 114 controles e uma seção introdutória . Cada seção contém um número de categorias principais de segurança da informação, conforme listadas abaixo:

a) Políticas de Segurança da Informação (1 categoria e/ou objetivo de controle e 2 controles);

b) Organização da Segurança da Informação (2 categorias e/ou objetivos de controle e 7 controles);

c) Segurança em Recursos Humanos (3 categorias e/ou objetivos de controle e 6 controles);

d) Gestão de Ativos (3 categorias e/ou objetivos de controle e 10 controles);

e) Controle de Acessos (4 categorias e/ou objetivos de controle e 14 controles);

f) Criptografia (1 categoria e/ou objetivo de controle e 2 controles);

g) Segurança Física e do Ambiente (2 categorias e/ou objetivos de controle e 15 controles);

Fonte: NBR ISO/IEC 27002:2013

ISO/IEC 27002 – estrutura

Estrutura da norma – continuação...

h) Segurança nas Operações (7 categorias e/ou objetivos de controle e 14 controles);

i) Segurança nas Comunicações (2 categorias e/ou objetivos de controle e 7 controles);

j) Aquisição, Desenvolvimento e Manutenção de Sistemas (3 categorias e/ou objetivos de controle e 13 controles);

k) Relacionamento na Cadeia de Suprimento (2 categorias e/ou objetivos de controle e 5 controles);

l) Gestão de Incidentes de Segurança da Informação (1 categoria e/ou objetivo de controle e 7 controles);

m) Aspectos da Segurança da Informação e Gestão da Continuidade do Negócio (2 categorias e/ou objetivos de controle e 4 controles);

n) Conformidade (2 categorias e/ou objetivos de controle e 8 controles).

Fonte: NBR ISO/IEC 27002:2013

ISO/IEC 27002 – estrutura

Estrutura da norma – continuação...

Cada seção principal contém:

- Um objetivo de controle declarando o que se espera que seja alcançado; e
- Um ou mais controles que podem ser aplicados para se alcançar o objetivo do controle.
  a) Controle – define a declaração específica do controle, para atender ao objetivo de controle.
  b) Diretrizes para implementação – apresenta informações mais detalhadas para apoiar a implementação do controle e alcançar o objetivo do controle. As diretrizes podem não ser totalmente adequadas ou suficientes em todas as situações e podem, portanto, não atender completamente aos requisitos de controle específicos da organização.
  c) Informações adicionais – apresenta mais dados que podem ser considerados, como por exemplo, questões legais e referências normativas. Se não existirem informações adicionais, esta parte não é mostrada no controle.

Fonte: NBR ISO/IEC 27002:2013

ISO/IEC 27002 – exemplos

A.5 Políticas de segurança da informação		
A.5.1 Orientação da Direção para segurança da informação		
Objetivo: Prover orientação da Direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.		
A.5.1.1	Políticas para segurança da informação	*Controle* Um conjunto de políticas de segurança da informação deve ser definido, aprovado pela Direção, publicado e comunicado para os funcionários e partes externas relevantes.
A.5.1.2	Análise crítica das políticas para segurança da informação	*Controle* As políticas de segurança da informação devem ser analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27002 – exemplos

A.8 Gestão de ativos		
A.8.1. Responsabilidade pelos ativos		
Objetivo: Identificar os ativos da organização e definir as devidas responsabilidades pela proteção dos ativos.		
A.8.1.1	Inventário dos ativos	*Controle* Os ativos associados com informação e com os recursos e processamento da informação devem ser identificados, e um inventário destes ativos deve ser estruturado e mantido.
A.8.1.2	Proprietário dos ativos	*Controle* Os ativos mantidos no inventário devem ter um proprietário.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27002 – exemplos

A.11 Segurança física e do ambiente		
A.11.1 Áreas seguras		
Objetivo: Prevenir o acesso físico não autorizado, danos e interferências nos recursos de processamento das informações e nas informações da organização.		
A.11.1.1	Perímetro de segurança física	*Controle* Perímetros de segurança devem ser definidos e usados para proteger tanto as instalações de processamento da informação como as áreas que contenham informações críticas ou sensíveis.
A.11.1.2	Controles de entrada física	*Controle* As áreas seguras devem ser protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso permitido.

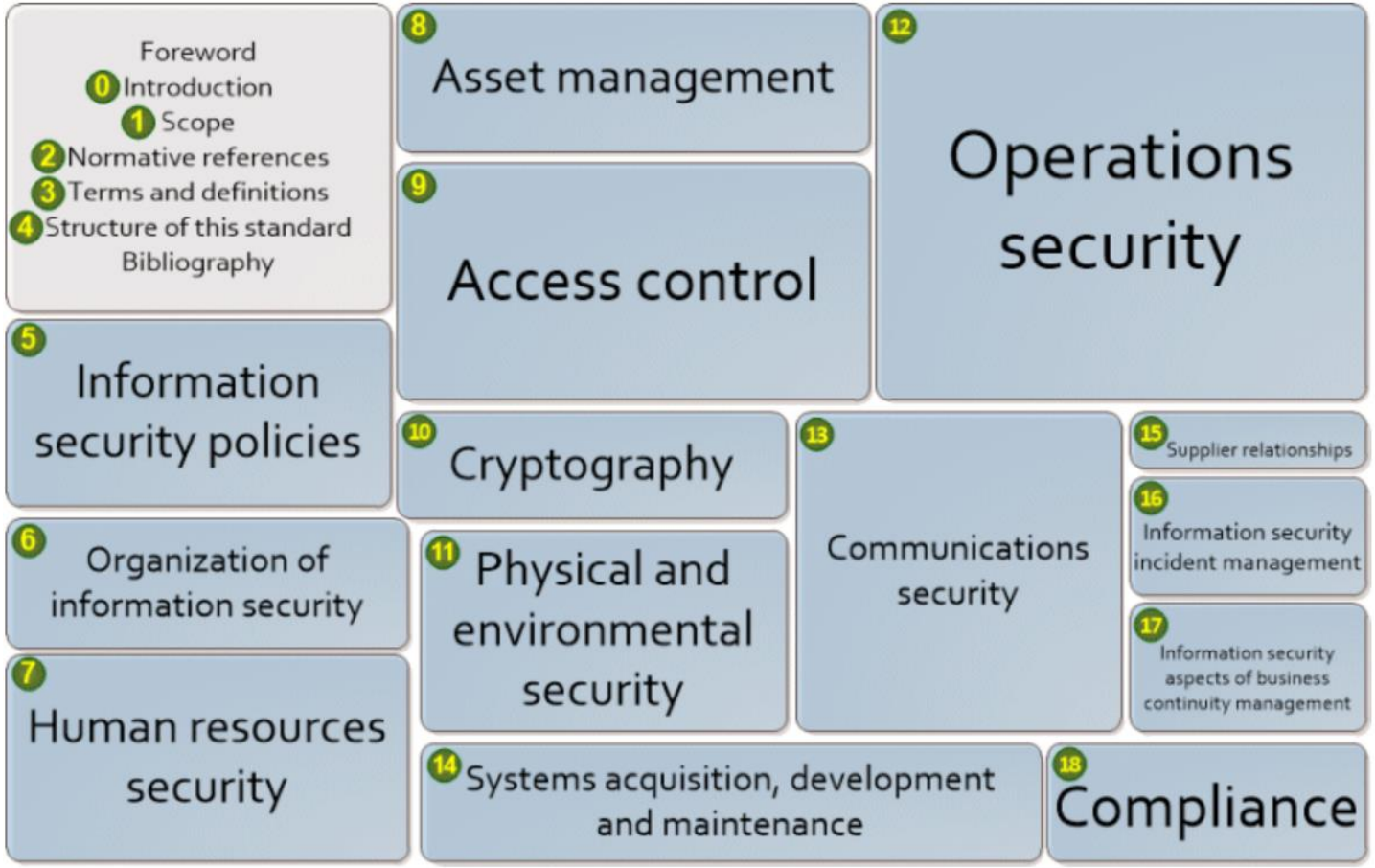
Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27002 – exemplos

A.12.3 Cópias de segurança		
Objetivo: Proteger contra a perda de dados.		
A.12.3.1	Cópias de segurança das informações	*Controle* Cópias de segurança das informações, *softwares* e das imagens do sistema devem ser efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida.

Fonte: NBR ISO/IEC 27001:2013

ISO/IEC 27002 – resumo



Fonte: NBR ISO/IEC 27002:2013

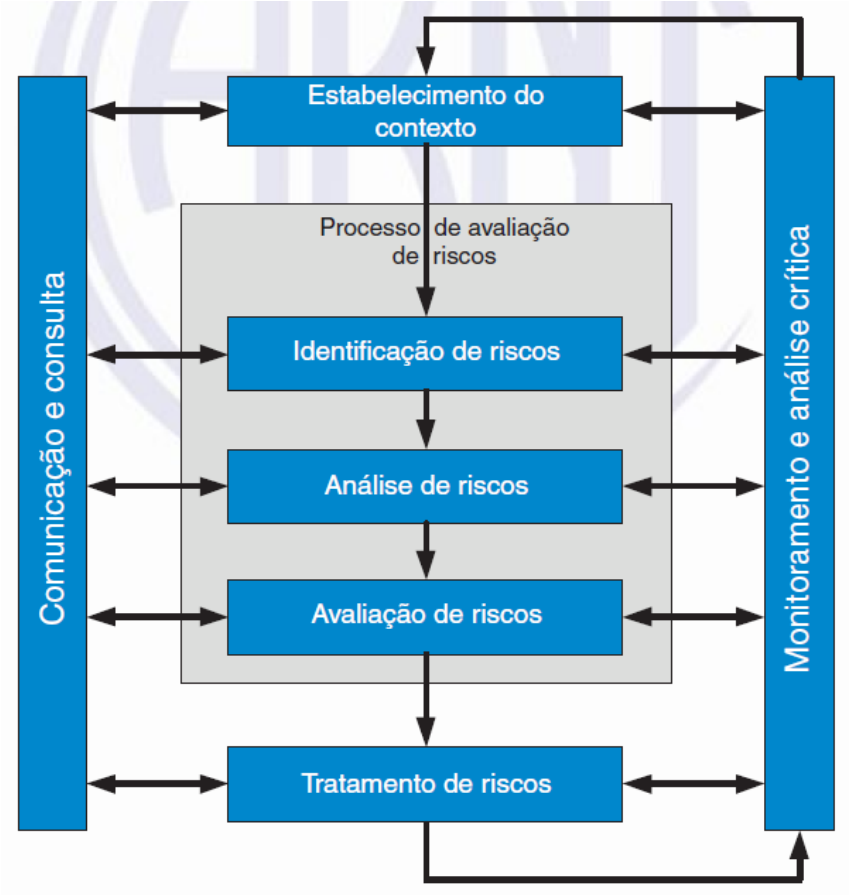
ISO/IEC 27005 – introdução

As análises/avaliações de riscos devem:

- Identificar, quantificar e priorizar os riscos com base em critérios para aceitação dos mesmos, para orientar e determinar as ações de gestão apropriadas e as prioridades para o gerenciamento dos riscos de segurança da informação;
- Incluir um enfoque sistemático para estimar a magnitude do risco (análise de riscos) e o processo de comparar os riscos estimados contra os critérios de risco para determinar a significância do risco (avaliação do risco);
- Ser realizadas periodicamente para contemplar as mudanças nos requisitos de segurança da informação e na situação de risco. Essas análises/avaliações de riscos devem ser realizadas de forma metódica, capaz de gerar resultados comparáveis e reproduzíveis.
- Ter um escopo claramente definido para ser eficaz e incluir os relacionamentos com as análises/avaliações de riscos em outras áreas, se necessário.

Fonte: NBR ISO/IEC 27002:2005

ISO/IEC 27005 – gestão de riscos



Processo de Gestão de Riscos

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – gestão de riscos

Processo do SGSI	Processo de gestão de riscos de segurança da informação
Planejar	Definição do contexto Processo de avaliação de riscos Definição do plano de tratamento do risco Aceitação do risco
Executar	Implementação do plano de tratamento do risco
Verificar	Monitoramento contínuo e análise crítica de riscos
Agir	Manter e melhorar o processo de Gestão de Riscos de Segurança da Informação

Alinhamento do processo do SGSI e do processo de Gestão de Riscos

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – definição do contexto

O contexto externo e interno para gestão de riscos de segurança da informação deve ser estabelecido, o que envolve a definição dos critérios básicos necessários para a gestão de riscos, a definição do escopo e dos limites e o estabelecimento de uma organização apropriada para operar a gestão de riscos.

É essencial determinar o propósito da gestão de riscos de segurança da informação, pois ele afeta o processo em geral e a definição do contexto em particular. Esse propósito pode ser:

- Suporte a um SGSI;
- Conformidade legal;
- Preparação de um plano de continuidade de negócios;
- Preparação de um plano de resposta a incidentes;
- Descrição dos requisitos de segurança da informação para um produto, um serviço ou um mecanismo.

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – critérios básicos

Abordagem da gestão de riscos

- Executar o processo de avaliação de riscos e estabelecer um plano de tratamento de riscos;
- Definir e implementar políticas e procedimentos, incluindo implementação dos controles selecionados;
- Monitorar controles;
- Monitorar o processo de gestão de riscos de segurança da informação.

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – critérios básicos

Critérios para avaliação de riscos

- O valor estratégico do processo que trata as informações de negócio;
- A criticidade dos ativos de informação envolvidos;
- Requisitos legais e regulatórios, bem como as obrigações contratuais;
- Importância, do ponto de vista operacional e dos negócios, da disponibilidade, da confidencialidade e da integridade;
- Expectativas e percepções das partes interessadas e consequências negativas para o valor de mercado (em especial, no que se refere aos fatores intangíveis desse valor), a imagem e a reputação.

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – critérios básicos

Critérios de impacto

- Nível de classificação do ativo de informação afetado;
- Ocorrências de violação da segurança da informação (por exemplo, perda da disponibilidade, da confidencialidade e/ou da integridade);
- Operações comprometidas (internas ou de terceiros);
- Perda de oportunidades de negócio e de valor financeiro;
- Interrupção de planos e o não cumprimento de prazos;
- Dano à reputação;
- Violações de requisitos legais, regulatórios ou contratuais.

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – critérios básicos

Critérios para aceitação de riscos

- Critérios para a aceitação do risco podem incluir mais de um limite, representando um nível desejável de risco, porém precauções podem ser tomadas por gestores seniores para aceitar riscos acima desse nível desde que sob circunstâncias definidas;
- Critérios para a aceitação do risco podem ser expressos como a razão entre o lucro estimado (ou outro benefício ao negócio) e o risco estimado
- Diferentes critérios para a aceitação do risco podem ser aplicados a diferentes classes de risco, por exemplo, riscos que podem resultar em não conformidade com regulamentações ou leis podem não ser aceitos, enquanto riscos de alto impacto podem ser aceitos se isto for especificado como um requisito contratual;
- Critérios para a aceitação do risco podem incluir requisitos para um tratamento adicional futuro, por exemplo, um risco pode ser aceito se for aprovado e houver o compromisso de que ações para reduzi-lo a um nível aceitável serão tomadas dentro de um determinado período de tempo.

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – processo de avaliação de riscos

Descrição geral do processo de avaliação de riscos de segurança da informação

O processo de avaliação de riscos determina o valor dos ativos de informação, identifica as ameaças e vulnerabilidades aplicáveis existentes (ou que poderiam existir), identifica os controles existentes e seus efeitos no risco identificado, determina as consequências possíveis e, finalmente, prioriza os riscos derivados e ordena-os de acordo com os critérios de avaliação de riscos estabelecidos na definição do contexto.

O processo de avaliação de riscos consiste nas seguintes atividades:

- Identificação de riscos;
- Análise de riscos;
- Avaliação de riscos.

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – processo de avaliação de riscos

Identificação de riscos

O propósito da identificação de riscos é determinar eventos que possam causar uma perda potencial e deixar claro como, onde e por que a perda pode acontecer.

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – processo de avaliação de riscos

Identificação das vulnerabilidades

Vulnerabilidades podem ser identificadas nas seguintes áreas:

- Organização;
- Processos e procedimentos;
- Rotinas de gestão;
- Recursos humanos;
- Ambiente físico;
- Configuração do sistema de informação;
- *Hardware*, *software* ou equipamentos de comunicação;
- Dependência de entidades externas.

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – processo de avaliação de riscos

Identificação das consequências

As organizações devem identificar as consequências operacionais de cenários de incidentes em função de (mas não limitado a):

- Investigação e tempo de reparo;
- Tempo (de trabalho) perdido;
- Oportunidade perdida;
- Saúde e segurança;
- Custo financeiro das competências específicas necessárias para reparar o prejuízo;
- Imagem, reputação e valor de mercado.

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – análise de riscos

Avaliação da probabilidade dos incidentes

Depois de identificar os cenários de incidentes, é necessário avaliar a probabilidade de cada cenário e do impacto correspondente, usando técnicas de análise qualitativas ou quantitativas.

- a experiência passada e estatísticas aplicáveis referentes à probabilidade da ameaça;
- para fontes de ameaças intencionais: a motivação e as competências, que mudam ao longo do tempo, os recursos disponíveis para possíveis atacantes, bem como a percepção da vulnerabilidade e o poder da atração dos ativos para um possível atacante;
- para fontes de ameaças acidentais: fatores geográficos (como por exemplo, proximidade a fábricas e refinarias de produtos químicos e petróleo), a possibilidade de eventos climáticos extremos e fatores que poderiam acarretar erros humanos e o mau funcionamento de equipamentos;
- vulnerabilidades, tanto individualmente como em conjunto;
- os controles existentes e a eficácia com que eles reduzem as vulnerabilidades.

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – análise de riscos

Determinação do nível de risco

A análise de riscos designa valores para a probabilidade e para as consequências de um risco. Esses valores podem ser de natureza quantitativa ou qualitativa. A análise de riscos é baseada nas consequências e na probabilidade estimadas. Além disso, ela pode considerar o custo-benefício, as preocupações das partes interessadas e outras variáveis, conforme apropriado para a avaliação de riscos. O risco estimado é uma combinação da probabilidade de um cenário de incidente e suas consequências.

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – análise de riscos

Exemplo – Matriz com valores pré-definidos

Para cada ativo, as vulnerabilidades relevantes e respectivas ameaças são consideradas. Se houver uma vulnerabilidade sem uma ameaça correspondente, ou uma ameaça sem uma vulnerabilidade correspondente, então não há risco nesse momento (mas convém que cuidados sejam tomados no caso dessas situações mudarem).

	Probabilidade de ocorrência (Ameaça)	BAIXA			MÉDIA			ALTA		
	Facilidade de exploração (Vulnerabilidade)	B	M	A	B	M	A	B	M	A
VALOR DO ATIVO	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – análise de riscos

Exemplo – Matriz com valores pré-definidos

Por exemplo, se o ativo tiver o valor **3**, a ameaça é "**alta**" e a vulnerabilidade é "**baixa**", a medida do risco é **5** (**A**). Supondo que um ativo tenha o valor **2**, o nível de ameaça é "**baixo**" e a facilidade de exploração é "**alta**", logo, a medida de risco é **4** (**B**).

	Probabilidade de ocorrência (Ameaça)	BAIXA			MÉDIA			ALTA		
	Facilidade de exploração (Vulnerabilidade)	B	M	A	B	M	A	B	M	A
VALOR DO ATIVO	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Fonte: NBR ISO/IEC 27005:2011

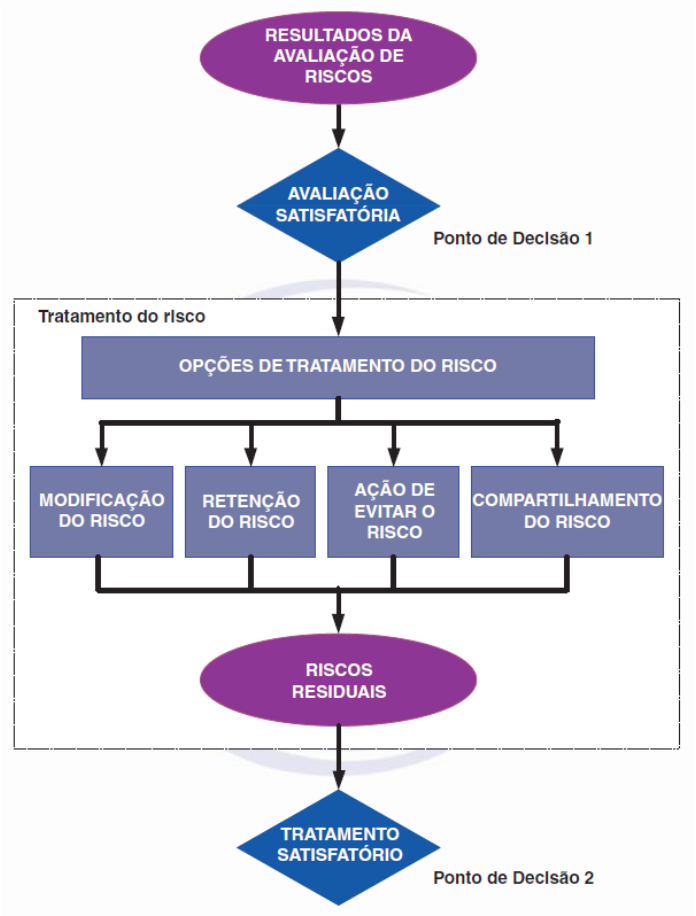
ISO/IEC 27005 – tratamento dos riscos

As opções de tratamento dos riscos devem ser selecionadas com base no resultado do processo de avaliação de riscos, no custo esperado para implementação dessas opções e nos benefícios previstos.

Quando uma grande modificação do risco pode ser obtida com uma despesa relativamente pequena, convém que essas opções sejam implementadas. Outras opções para melhorias podem ser muito dispendiosas e uma análise precisa ser feita para verificar suas justificativas.

Fonte: NBR ISO/IEC 27005:2011

ISO/IEC 27005 – tratamento dos riscos



Atividade de Tratamento de Risco

Fonte: NBR ISO/IEC 27005:2011

Resposta aos riscos

Evitar, prevenir ou eliminar	• Elimina a causa raiz do problema a fim de evitar a exposição ao risco. Pode afetar a utilidade do ativo.
Transferir	• Não trata o risco, apenas transfere o ônus para um terceiro, de modo parcial ou total, como num seguro. Há a necessidade de se pagar um prêmio para a parte que assume o risco.
Mitigar	• Reduz a probabilidade de ocorrência de um incidente ou o seu impacto até um nível aceitável.
Aceitar	• Quando a probabilidade de ocorrência e o impacto são baixos ou quando não é possível aplicar nenhuma estratégia e decide-se arcar com as consequências.

Resposta aos riscos *vs* tratamento dos riscos

Evitar, prevenir ou eliminar	• Ação de evitar o risco
Transferir	• Compartilhamento do risco
Mitigar	• Modificação do risco
Aceitar	• Retenção do risco

Para saber mais...

… veja os Objetivos de Controle e Controles da ABNT NBR ISO/IEC 27001:2013.

Módulo 6

Políticas e procedimentos de Segurança da Informação

Introdução

"Política de Segurança é composta por um **conjunto de regras e padrões** sobre o que deve ser feito para assegurar que as informações e serviços importantes para a empresa recebam a proteção conveniente, de modo a garantir a sua confidencialidade, integridade e disponibilidade"

Scott Barman apud Fernando Nicolau Freitas Ferreira

Fonte: FERREIRA, F. N. F.; ARAÚJO, M. T. D. **Política de Segurança da Informação**. 2ª. ed. Rio de Janeiro: Editora Ciência Moderna, 2008.

Premissas

Estabelecer o conceito de que as informações são um ativo importante para a organização

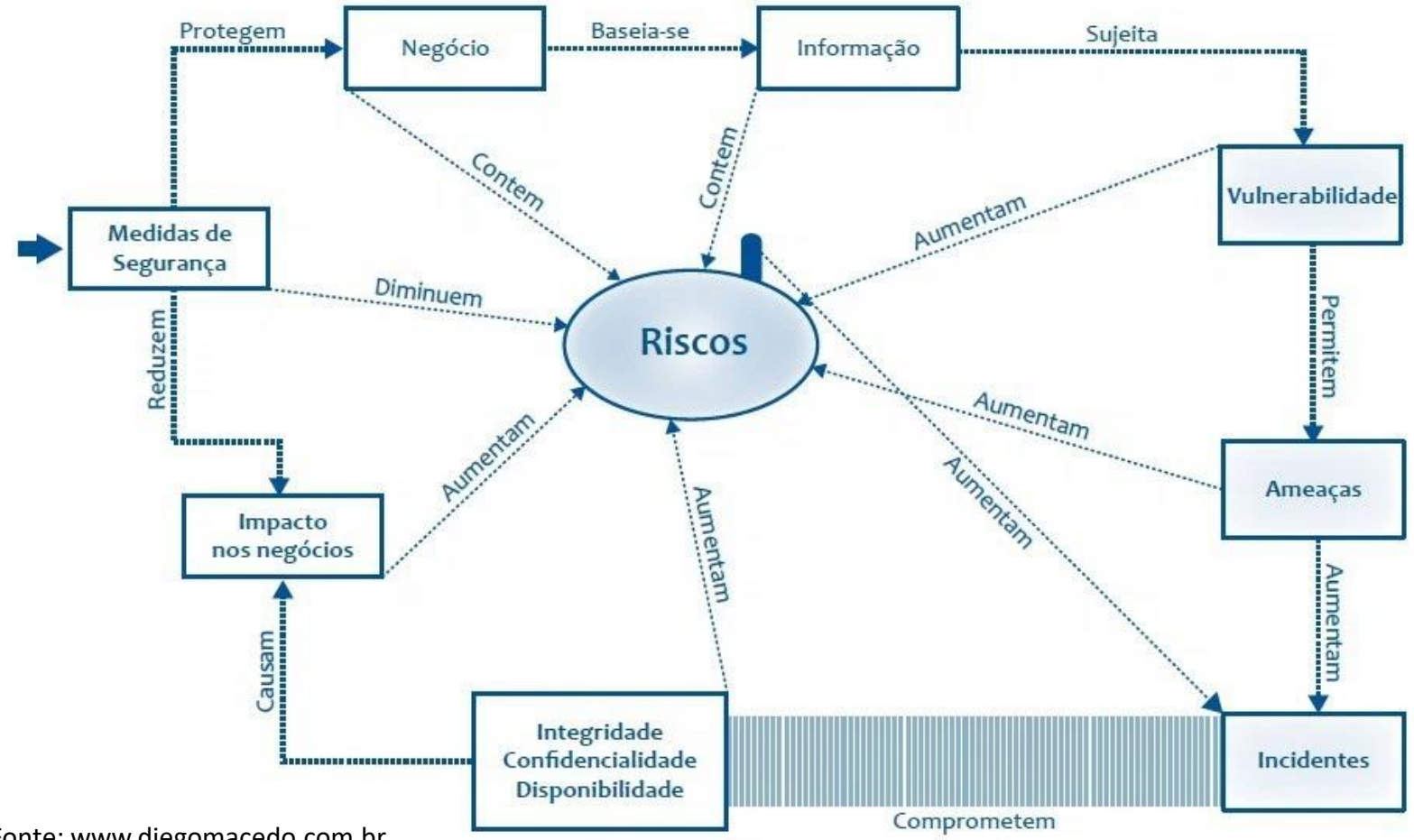
Envolver a alta administração da organização

Responsabilizar formalmente os colaboradores sobre a salvaguarda dos recursos da informação, definindo o conceito de irrevogabilidade

Estabelecer padrões para a manutenção da Segurança da Informação

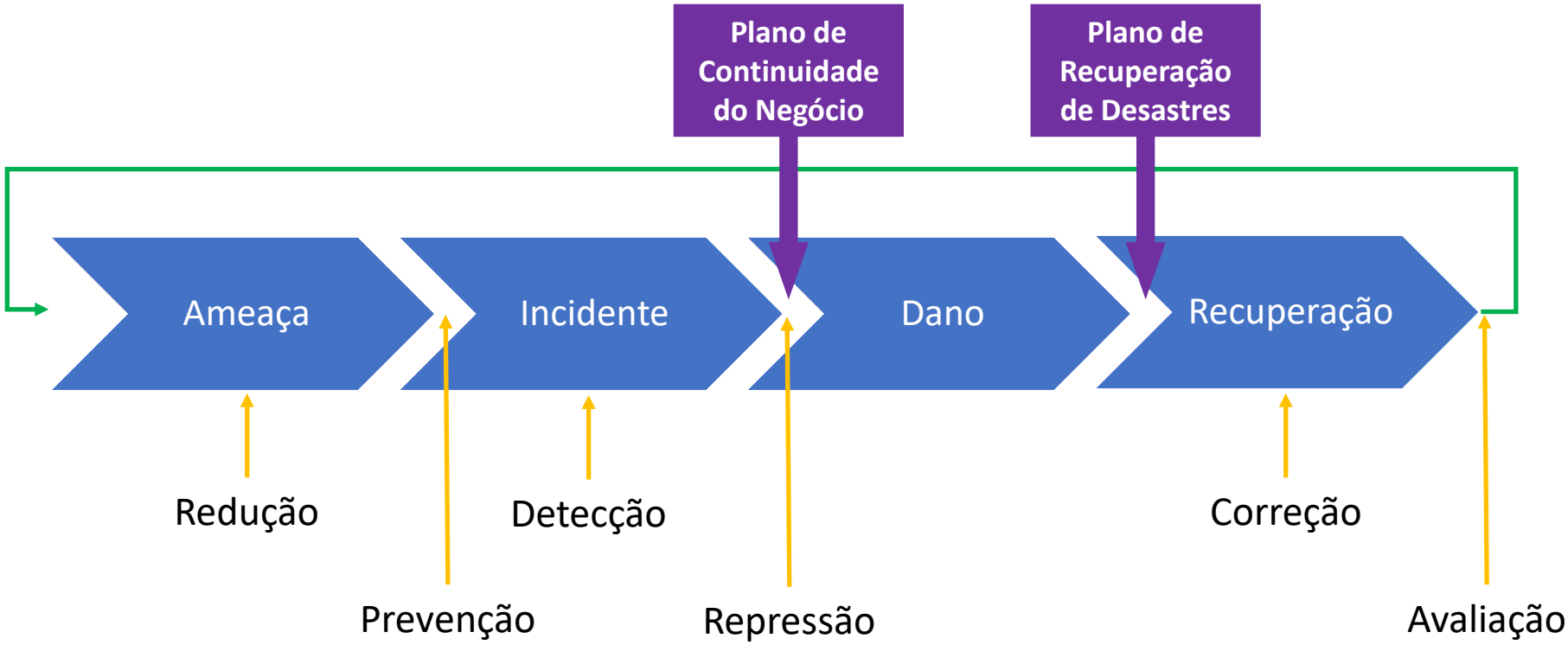
Fonte: FERREIRA, F. N. F.; ARAÚJO, M. T. D. **Política de Segurança da Informação**. 2ª. ed. Rio de Janeiro: Editora Ciência Moderna, 2008.

Ciclo de segurança da informação



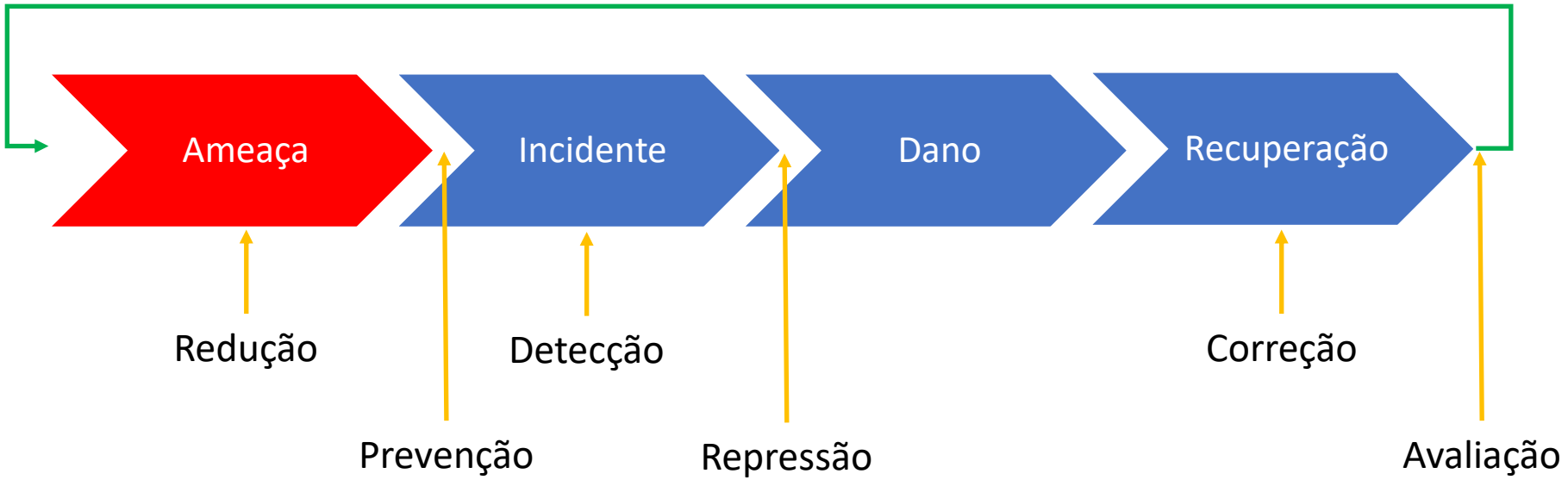
Fonte: www.diegomacedo.com.br

Ciclo de vida de um incidente de segurança



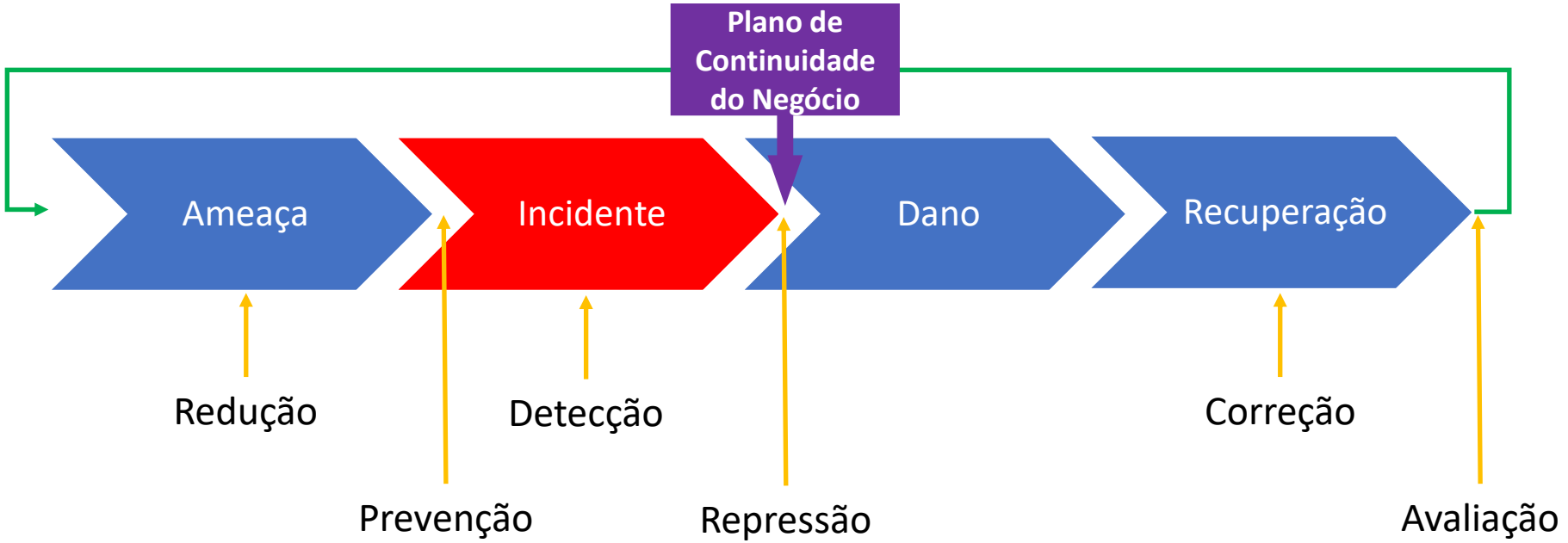
Ciclo de vida de um incidente de segurança

- Ameaça – todo ativo alvo da segurança da informação possui vulnerabilidades e está sujeito a ameaças que as explorem. O gerenciamento de riscos permite que se conheçam tais vulnerabilidades e ameaças e que medidas de redução e de prevenção das ameaças possam ser adotadas.



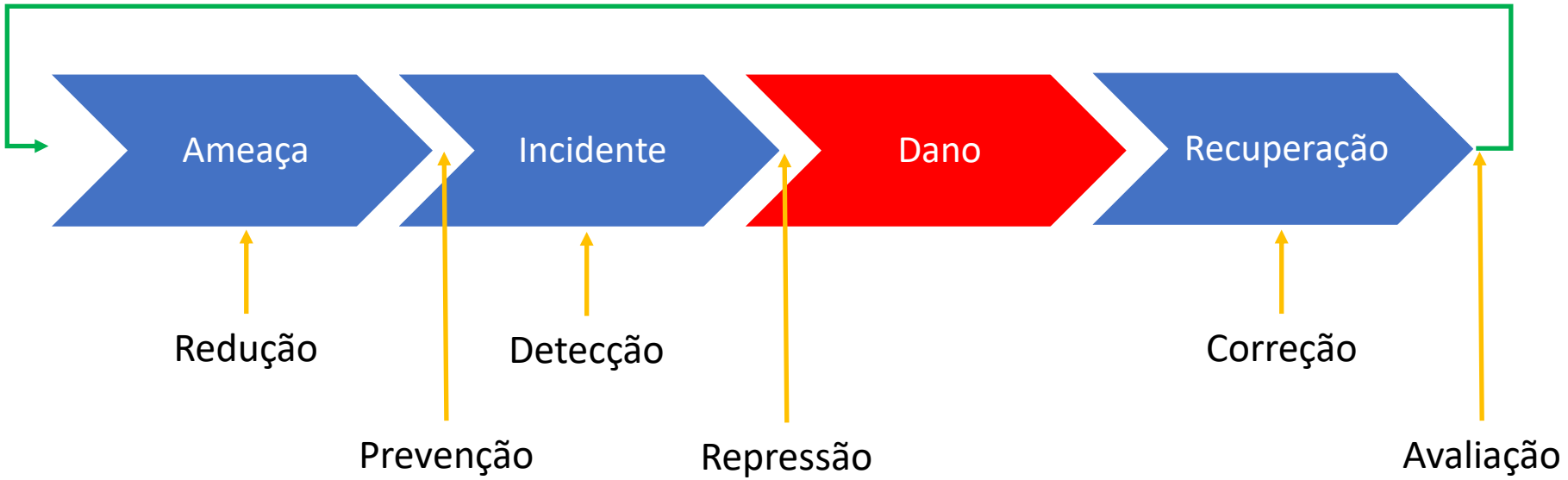
Ciclo de vida de um incidente de segurança

- Incidente – ainda que as medidas de redução e prevenção de ameaças sejam adotadas, um incidente pode ocorrer. Neste caso é importante que o mesmo seja detectado o quanto antes de modo a causar o menor dano possível. As medidas repressivas, como um Plano de Continuidade do Negócio, podem ser acionadas para reprimir o dano a sua menor intensidade possível.



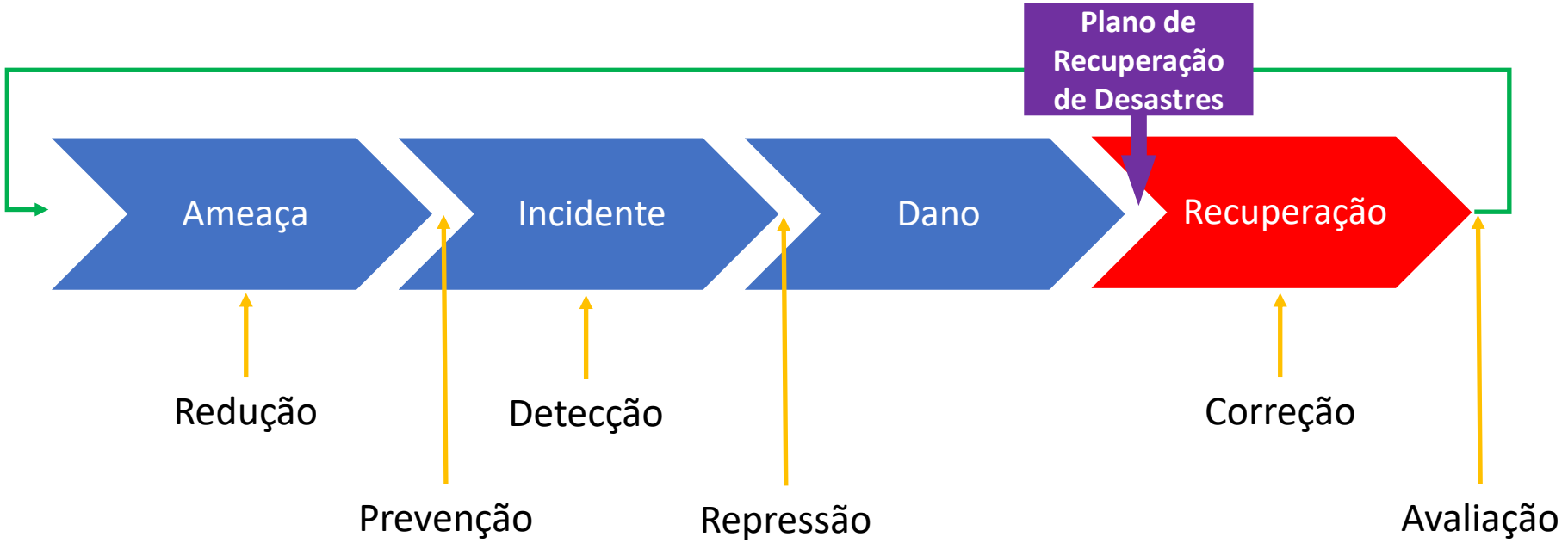
Ciclo de vida de um incidente de segurança

- Dano – nesta etapa a organização deve avaliar os danos causados pelo incidente e confrontá-los com a análise de impacto realizada no gerenciamento de riscos. O objetivo aqui é avaliar se os controles de segurança adotados eram adequados ou não e se devem ser refinados.



Ciclo de vida de um incidente de segurança

- Recuperação – durante a etapa de recuperação, a partir do Plano de Recuperação de Desastres e quando há o retorno à operação normal, medidas corretivas e avaliativas devem ser adotadas para evitar que incidentes como o que provocou a descontinuidade da operação não voltem a ocorrer. As medidas avaliativas são extremamente importantes no processo de melhoria contínua.



Para saber mais...

... leia o capítulo 3 do livro Fundamentos de segurança da informação com base na ISO 27001 e na ISO 27002, de Jule Hintzbergen

... leia o capítulo 1 do livro Criptografia e segurança de redes: princípios e práticas, de William Stallings

... leia os capítulos 1 e 2 do livro Governança de segurança da informação, de Sergio da Silva Manoel

Módulo 7

Plano de continuidade do negócio

Introdução

Continuidade do Negócio, ou Business Continuity, é o processo que prepara para uma paralisação do sistema que pode afetar de modo adverso as operações de negócios, responde a essa paralisação e recupera as operações.

- O processo de Continuidade do Negócio permite a disponibilidade contínua das informações e dos serviços em caso de não atendimento do SLA requerido;
- Continuidade do Negócio envolve várias contramedidas proativas e reativas;
- É importante automatizar o processo de Continuidade do Negócio para reduzir a intervenção manual;
- O objetivo da Continuidade do Negócio é garantir a disponibilidade das informações.

Fonte: EMC Information Storage and Management v3

Plano

O Plano de Continuidade de Negócios, ou Business Continuity Plan, é o desenvolvimento preventivo de um conjunto de estratégias e planos de ação de maneira a garantir que os serviços essenciais sejam devidamente identificados e preservados após a ocorrência de um desastre, e até o retorno à situação normal de funcionamento da empresa dentro do contexto do negócio do qual faz parte.

O Plano de Continuidade de Negócios é constituído pelos seguintes planos:

- Plano de Contingência (Emergência);
- Plano de Administração de Crises (PAC);
- Plano de Recuperação de Desastres (PRD);
- Plano de Continuidade Operacional (PCO).

Fonte: NBR 15999-1:2007

Estrutura

Plano de Contingência (Emergência): deve ser utilizado em último caso, quando todas as prevenções tiverem falhado. Define as necessidades e ações mais imediatas.

Plano de Administração ou Gerenciamento de Crises (PAC): define funções e responsabilidades das equipes envolvidas com o acionamento das ações de contingência, antes durante e após a ocorrência.

Plano de Recuperação de Desastres (PRD): determina o planejamento para que, uma vez controlada a contingência e passada a crise, a empresa retome seus níveis originais de operação.

Plano de Continuidade Operacional (PCO): seu objetivo é reestabelecer o funcionamento dos principais ativos que suportam as operações de uma empresa, reduzindo o tempo de queda e os impactos provocados por um eventual incidente. Um exemplo simples é a queda de conexão à internet.

Fonte: www.venki.com.br

Disponibilidade das informações

Disponibilidade das informações é a capacidade de uma infraestrutura de TI funcionar de acordo com os requisitos dos negócios e com as expectativas do cliente durante seu tempo de operação especificado, e pode ser definida em termos de:

Acessibilidade	• As informações devem estar acessíveis para o usuário certo quando necessário
Confiabilidade	• As informações devem ser confiáveis e corretas em todos os aspectos
Agilidade	• Define a janela de tempo durante a qual as informações devem estar acessíveis

Fonte: EMC Information Storage and Management v3

Causas da indisponibilidade

- Falha de aplicativo
  - Por exemplo, devido a exceções catastróficas causadas por uma lógica ruim
- Perda de dados
- Falha de componentes da infraestrutura
- Datacenter ou local inativo
  - Devido a falta de energia ou desastre
- Atualização da infraestrutura de TI

Fonte: EMC Information Storage and Management v3

Impacto da indisponibilidade das informações

Perda de produtividade

- Número de funcionários afetados x horas de inatividade x custo por hora

Saiba o custo do tempo de inatividade (por hora, dia, dois dias e assim por diante).

Receita perdida

- Perda direta
- Pagamentos compensatórios
- Perda de receita futura
- Perda de faturamento
- Perda de investimentos

Reputação prejudicada

- Clientes
- Fornecedores
- Mercados financeiros
- Bancos
- Parceiros de negócios

Desempenho financeiro

- Reconhecimento de receita
- Fluxo de caixa
- Perda de descontos
- Garantias de pagamentos
- Classificação de crédito
- Preços de ações

Outras despesas

- Funcionários temporários, locação de equipamentos, custos de horas extras, custos extras de remessas, despesas de viagens, etc.

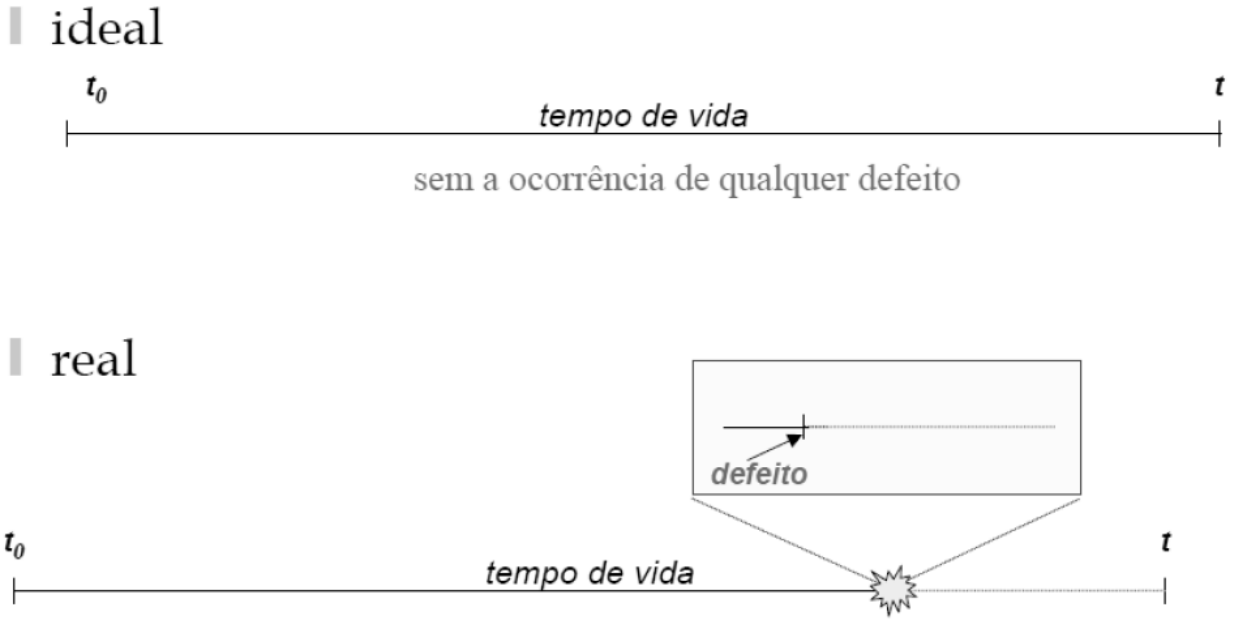
Fonte: EMC Information Storage and Management v3

Confiabilidade e disponibilidade

Confiabilidade é a habilidade de um sistema ou equipamento exercer sua função sob uma determinada condição durante um período específico de tempo.

Disponibilidade é o quanto um sistema ou equipamento está operacional e acessível quando solicitado.

Falhas em equipamentos



Comportamento ideal e real de um componente

Falhas em equipamentos

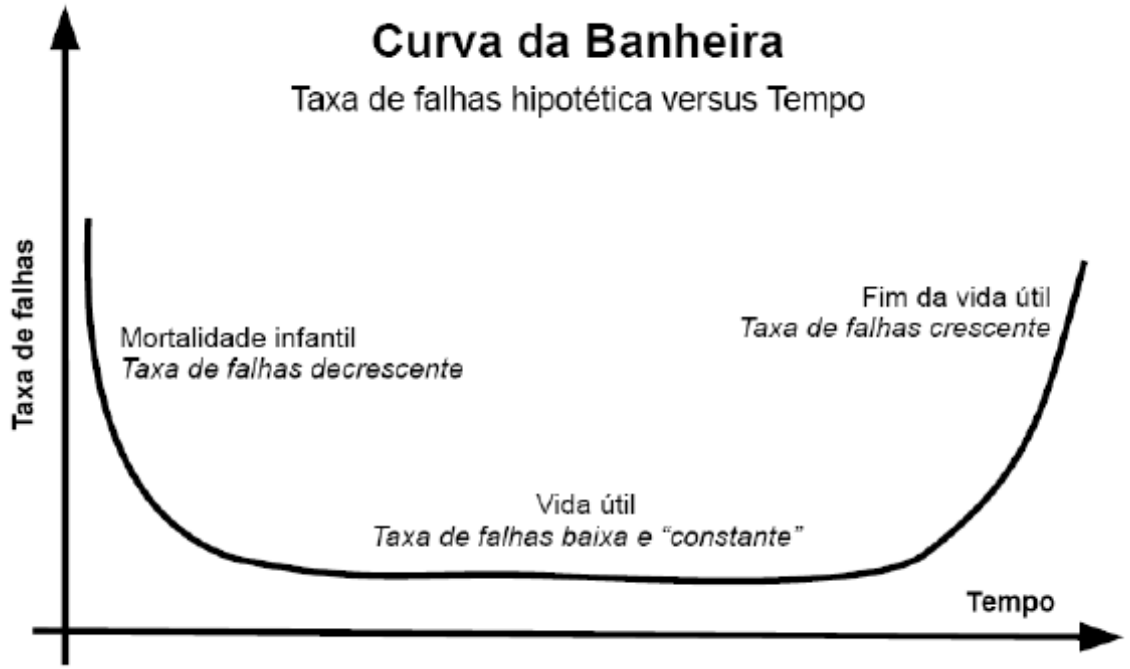
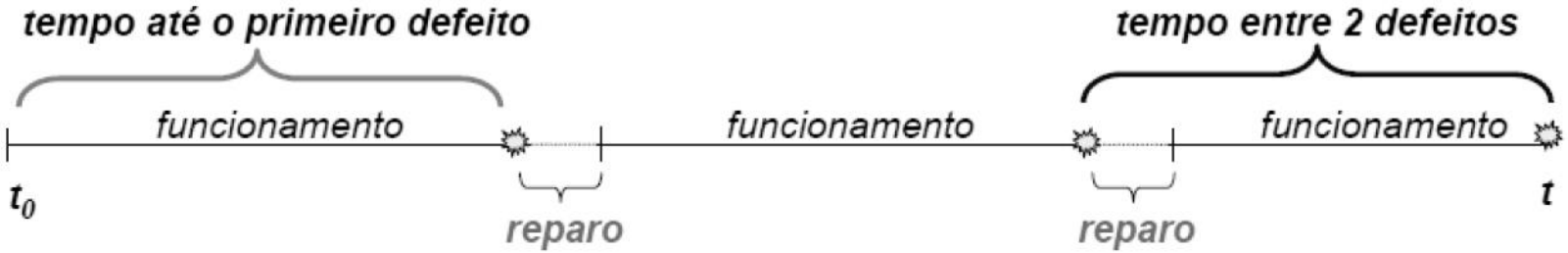


Gráfico da Curva da banheira

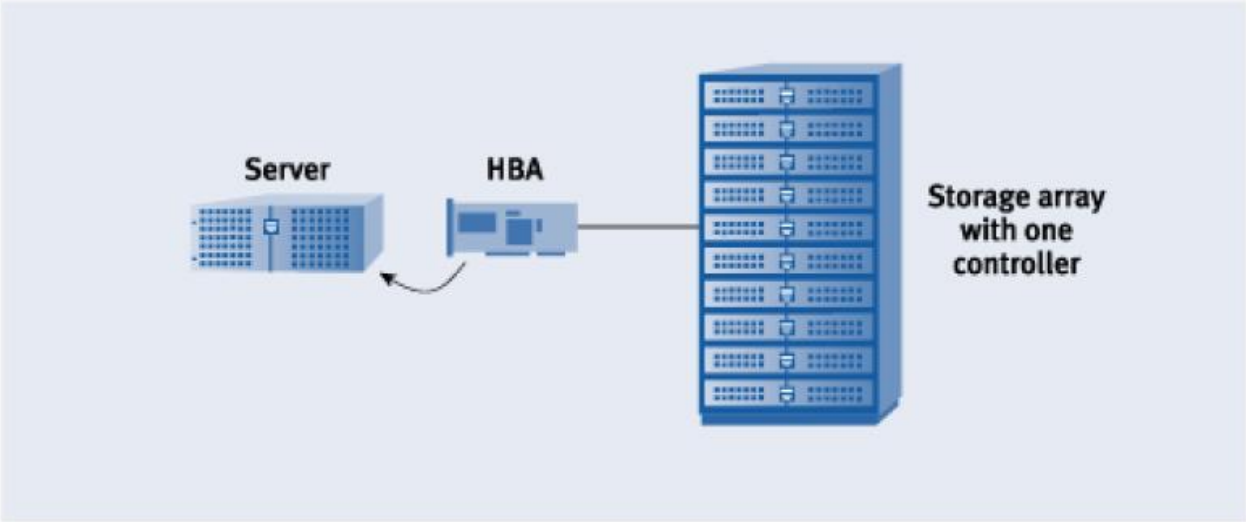
Medindo a disponibilidade

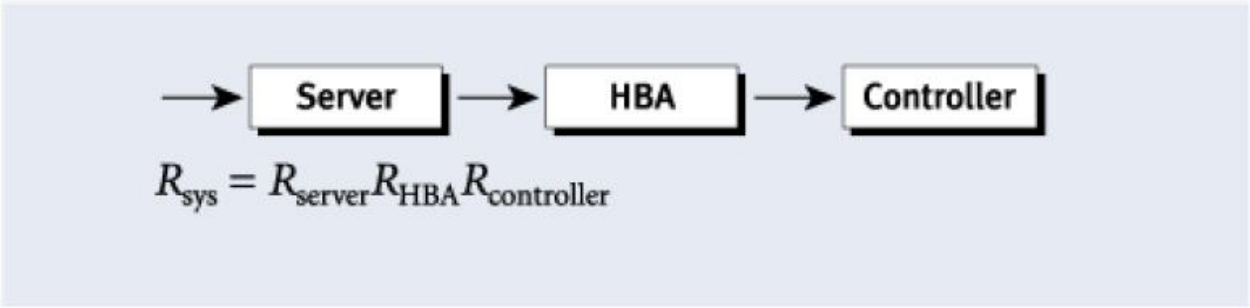
O tempo para ocorrer o primeiro defeito durante a vida útil de um equipamento ou produto é chamado de MTTF (*Mean Time to Failure*). O tempo de reparo (ou troca) deste equipamento é conhecido como MTTR (*Mean Time to Repair*), que inclui o tempo necessário para a notificação da falha, o tempo gasto com o deslocamento do técnico de campo, o tempo gasto com o transporte da nova peça do almoxarifado até o local de instalação e o tempo gasto no reparo ou troca propriamente dito. No MTTR devemos considerar também as paradas planejadas para manutenção. O intervalo entre as falhas do equipamento é chamado MTBF (*Mean Time Between Failures*).



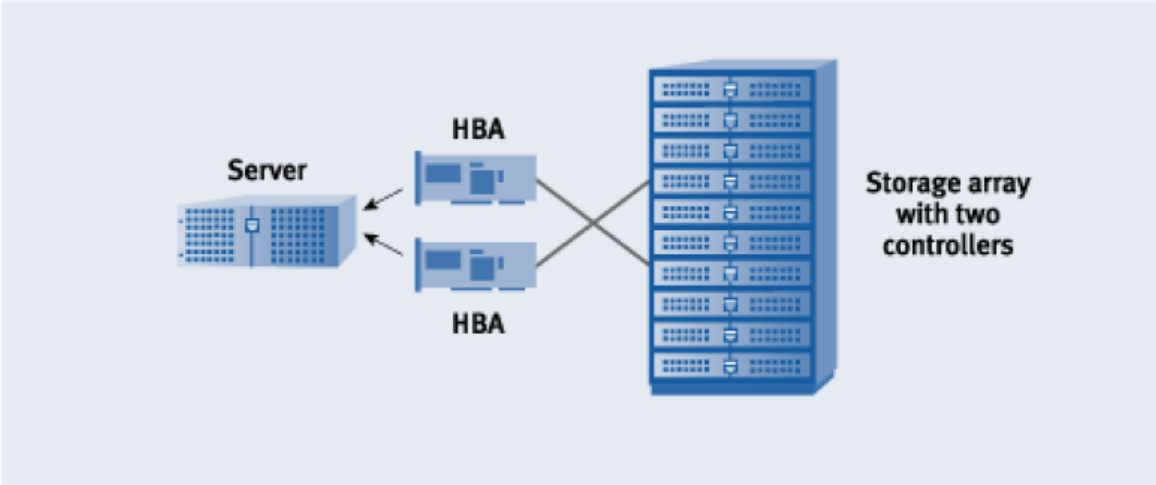
Linha do tempo para falhas de um equipamento

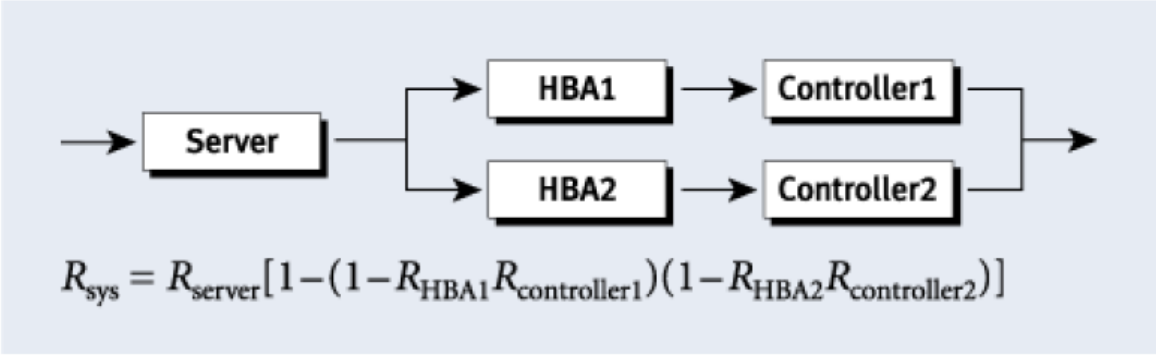
Associação de elementos em série





Associação de elementos em paralelo



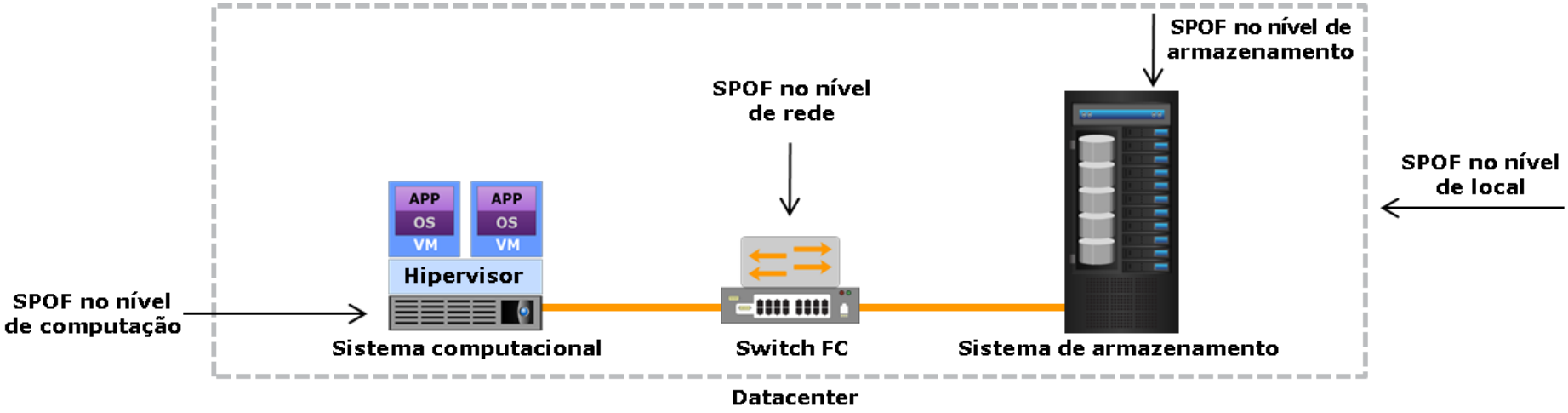


Disponibilidades típicas

Disponibilidade	Tempo de parada
90%	36,5 dias/ano
99%	3,65 dias/ano
99,9%	8,76 horas/ano
99,99%	52 minutos/ano
99,999%	5 minutos/ano
99,9999%	31 segundos/ano

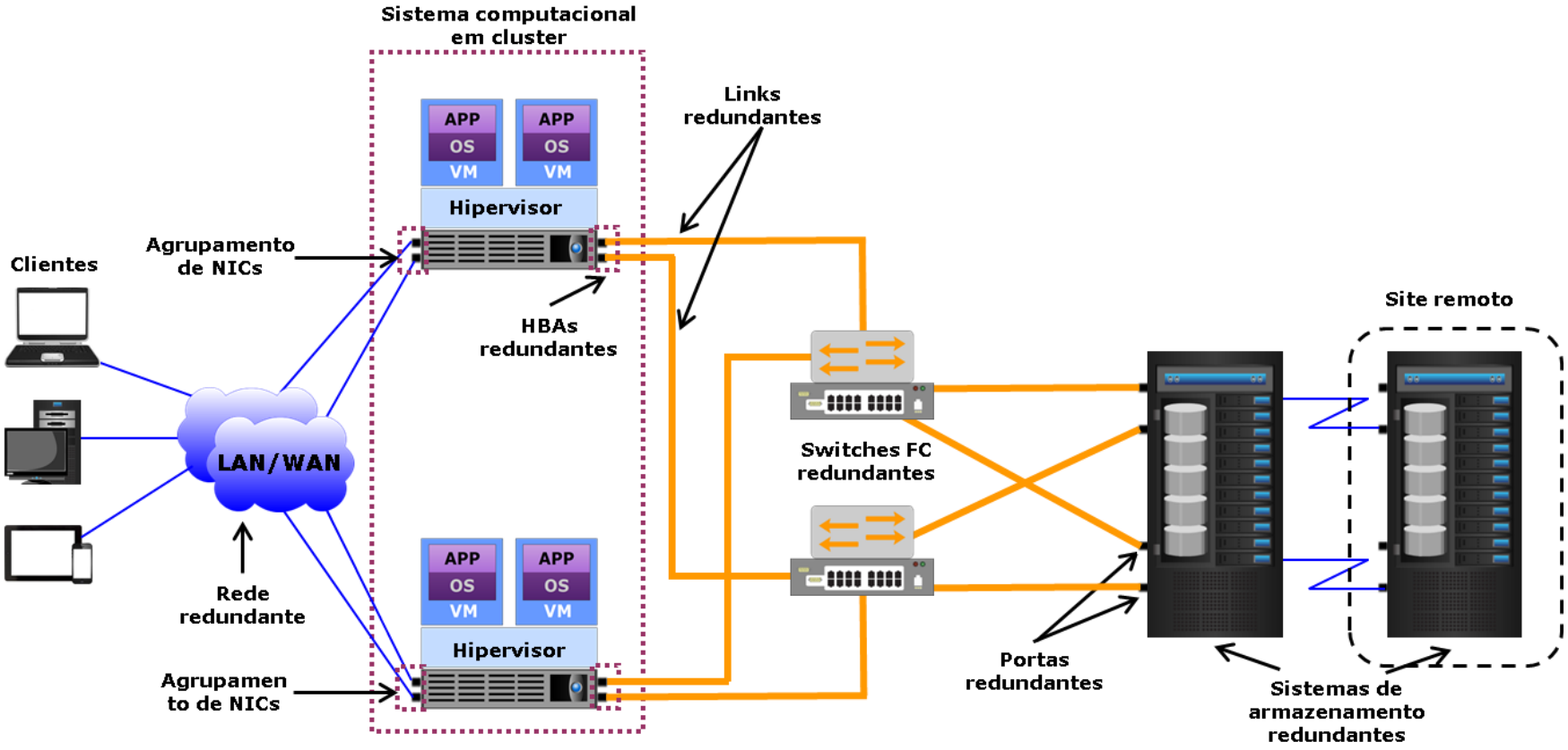
Ponto único de falha

Ponto único de falha, ou single point of failure (SPOF), refere-se a qualquer componente individual ou aspecto de uma infraestrutura cuja falha pode tornar todo o sistema ou serviço indisponível.



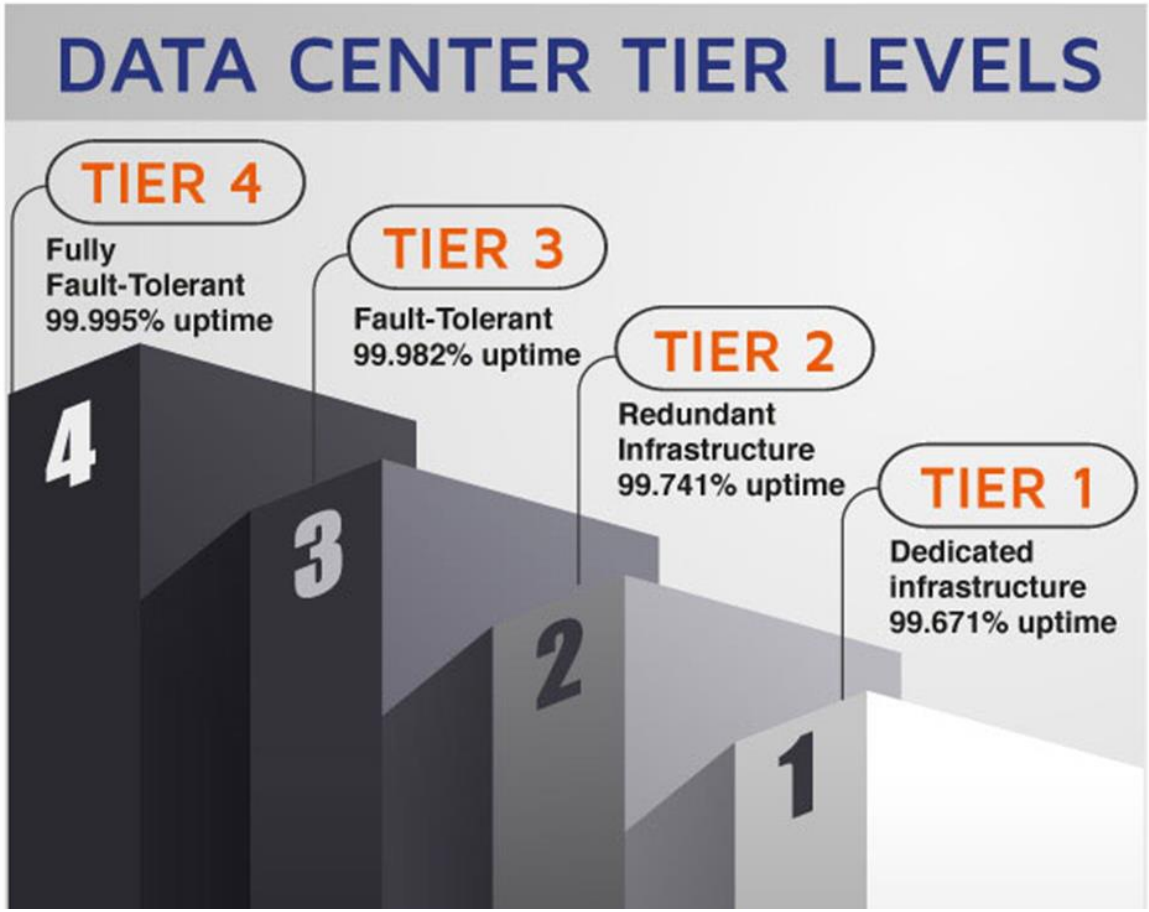
Fonte: EMC Information Storage and Management v3

Implementando redundância



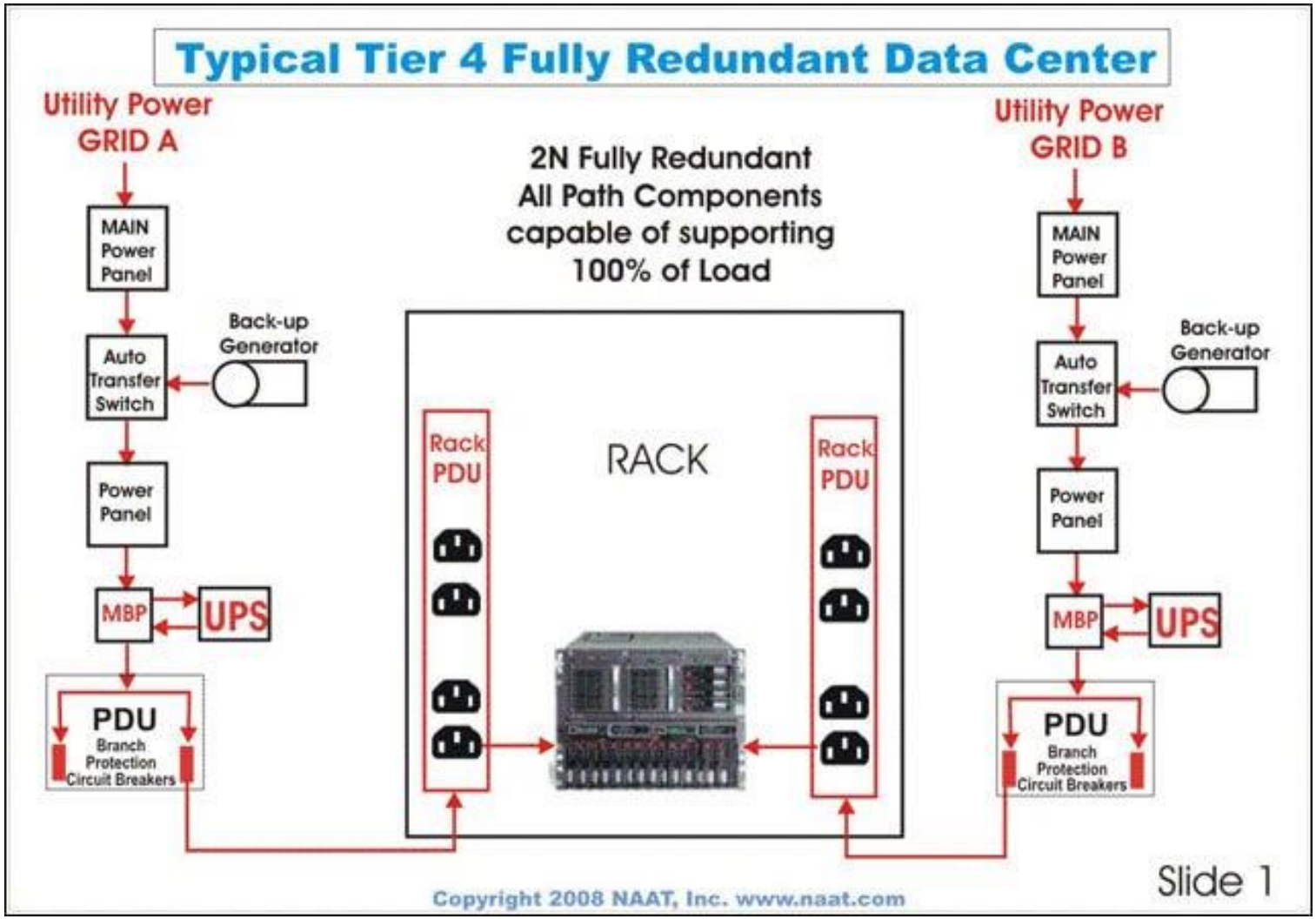
Fonte: EMC Information Storage and Management v3

Datacenter – Tier



Fonte: telehouse.com

Datacenter – Tier 4

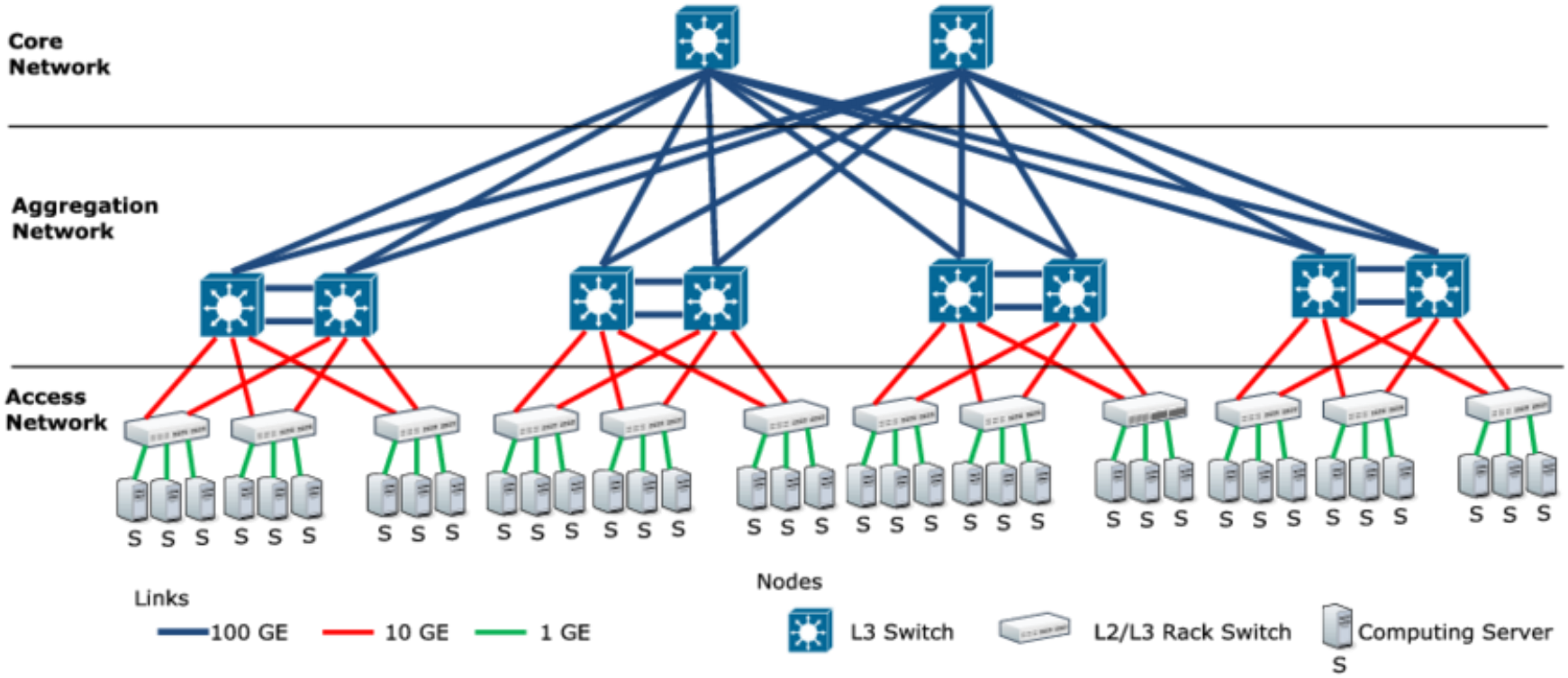


Datacenter – Tier 4

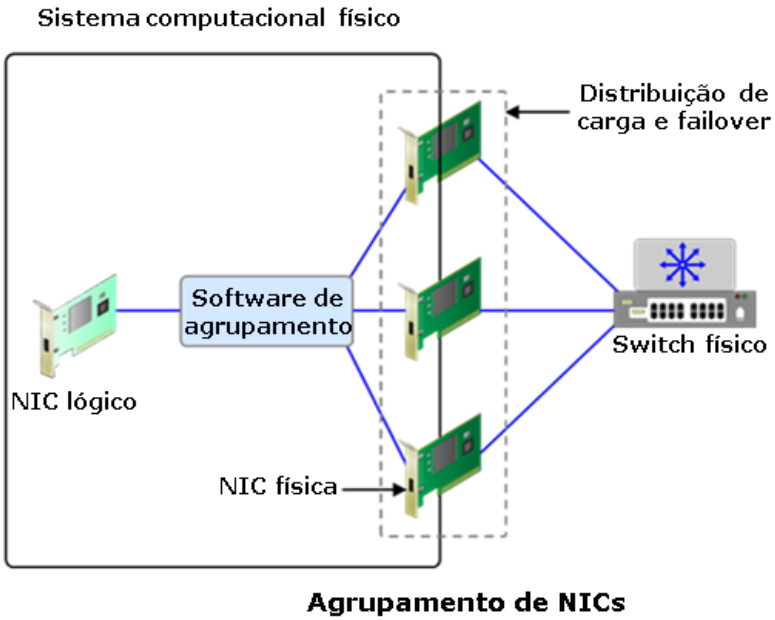
- 99,995% de tempo de atividade por ano
- 2N+1, ou seja, infraestrutura totalmente redundante
- Proteção contra queda de energia de 96 horas
- Sistemas de refrigeração que estão continuamente disponíveis 24x7x365
- Infraestrutura de local tolerante a falhas com instalações de armazenamento e distribuição de energia elétrica
- Caminhos de distribuição são fisicamente isolados uns dos outros e são frequentemente referidos como caminhos de distribuição "compartimentalizados", evitando danos de um único evento que pode ocorrer no local
- 12 horas no local de armazenamento de combustível

Fonte: Tier Classification Define Site Infrastructure Performance. W. Pitt Turner IV et al.

Redundância de rede

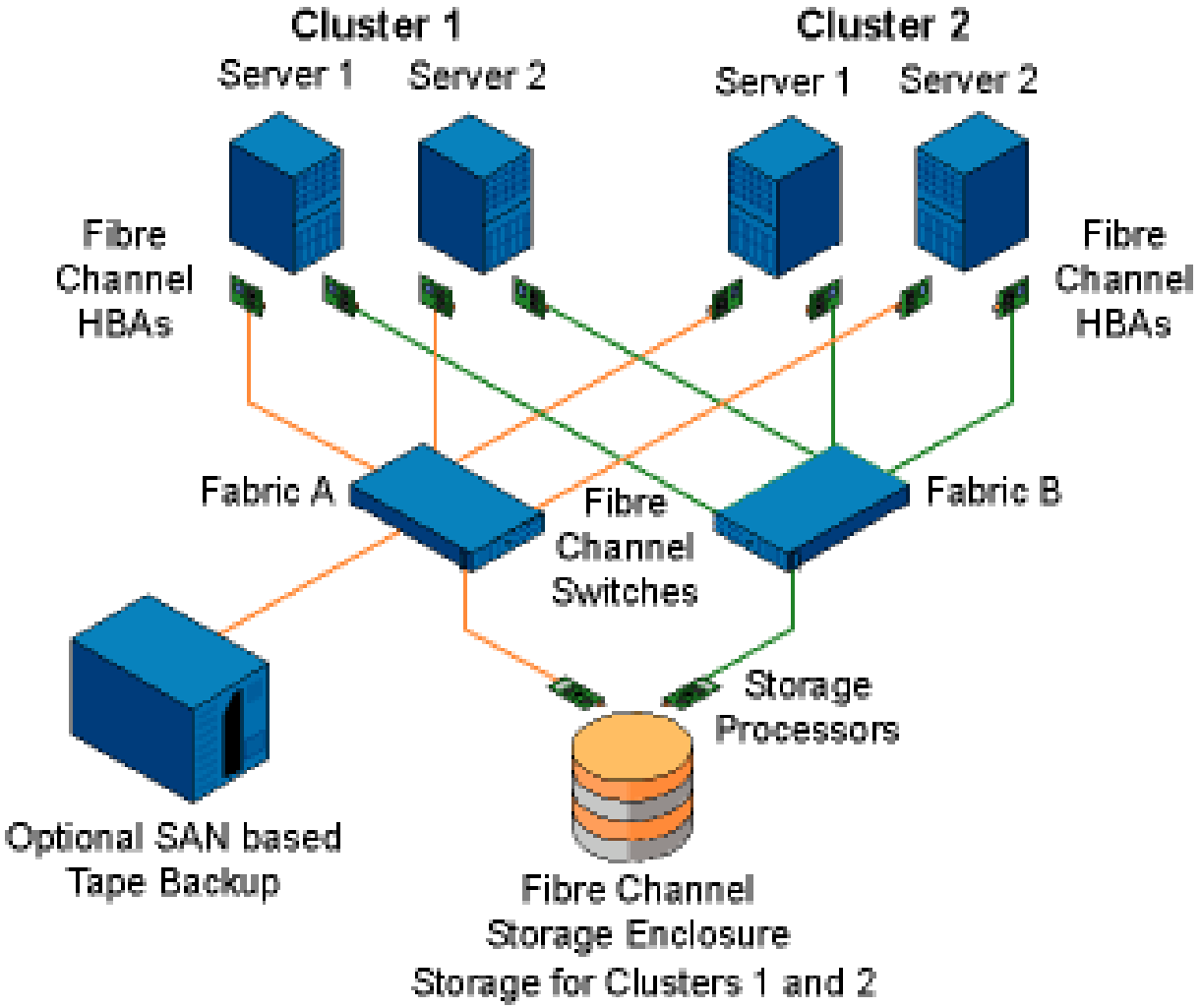


Agregação de enlaces

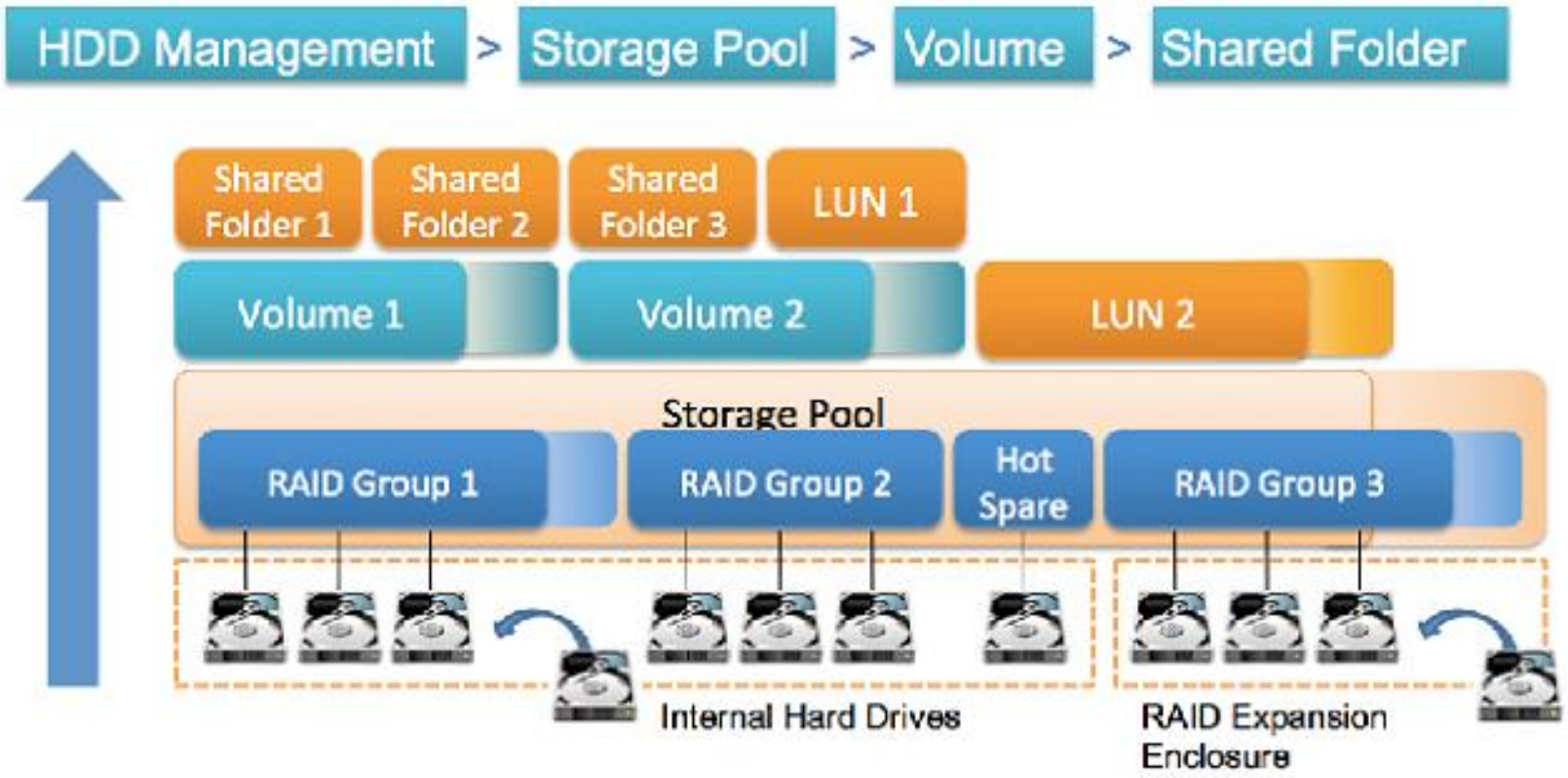


Fonte: EMC Information Storage and Management v3

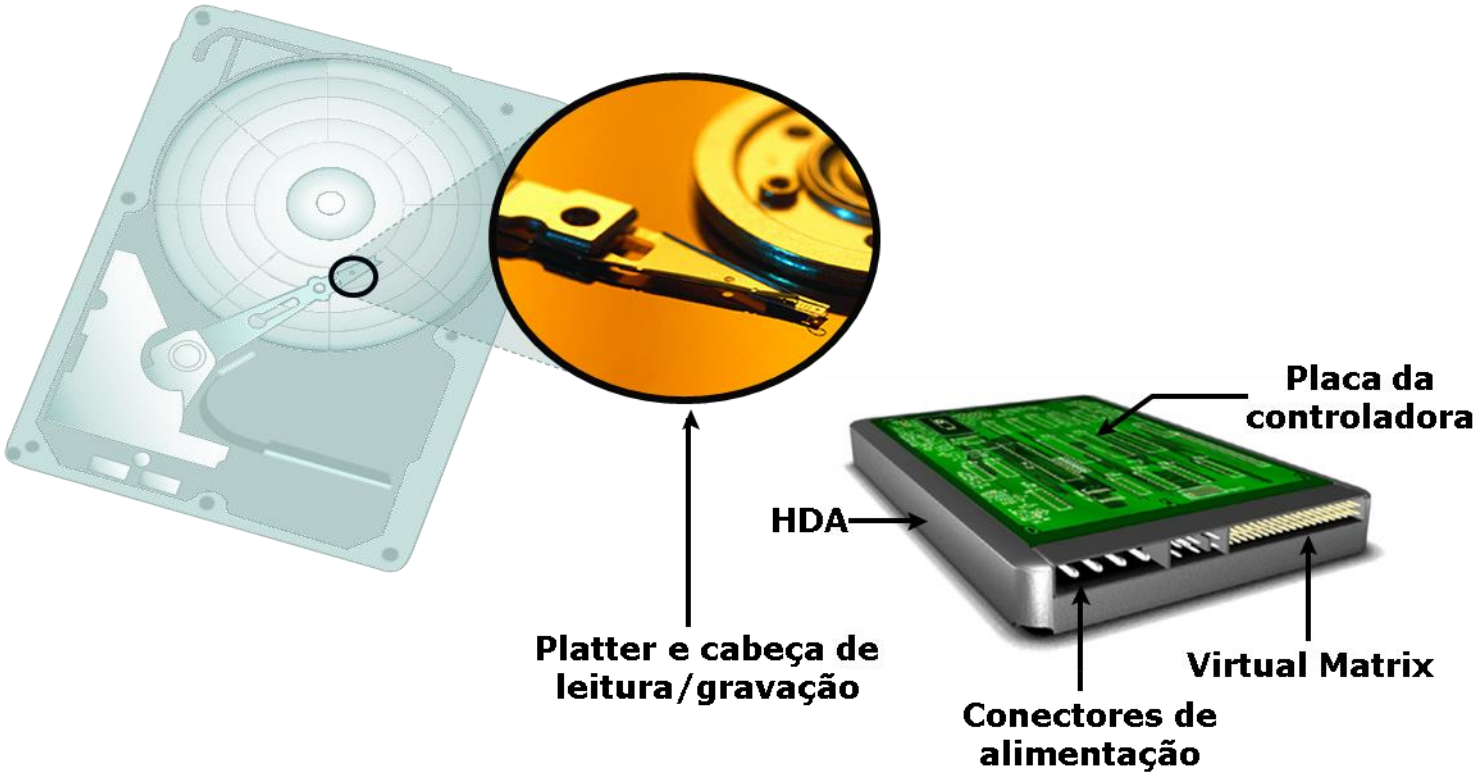
Cluster


Cluster 1
Server 1
Server 2
Cluster 2
Server 1
Server 2
Fibre Channel HBAs
Fibre Channel HBAs
Fabric A
Fabric B
Fibre Channel Switches
Storage Processors
Optional SAN based Tape Backup
Fibre Channel Storage Enclosure
Storage for Clusters 1 and 2

Array de discos

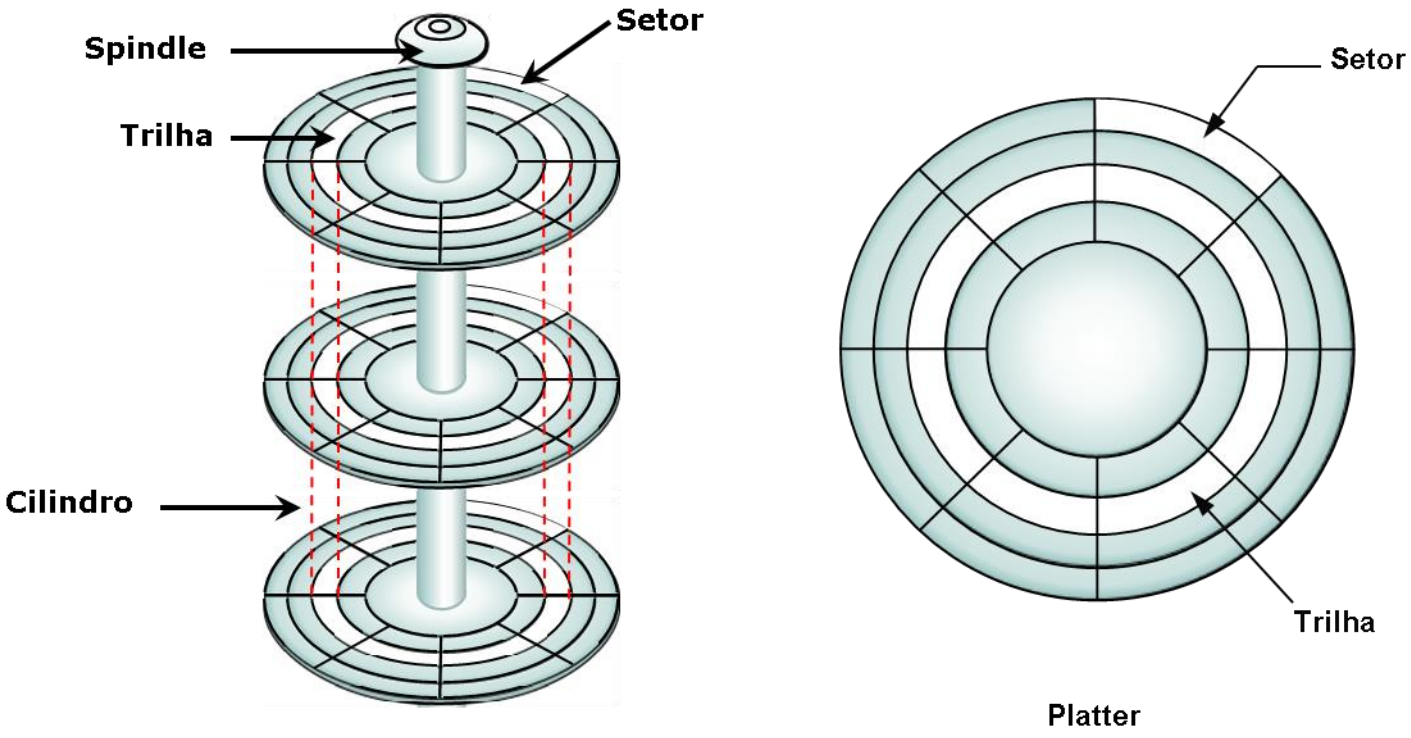


Componentes de disco



Fonte: EMC Information Storage and Management v3

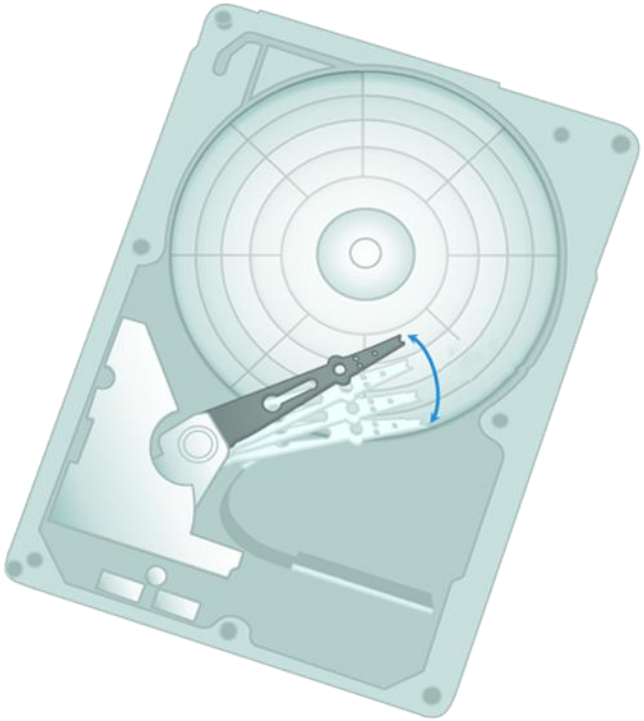
Estrutura do disco



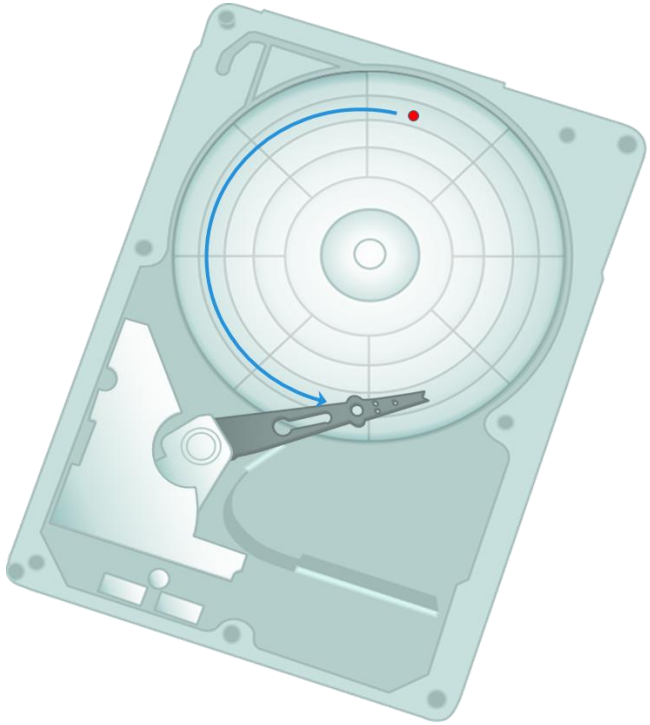
Fonte: EMC Information Storage and Management v3

Estrutura do disco

- Tempo de busca



- Latência rotacional



Fonte: EMC Information Storage and Management v3

Array de discos

O termo RAID (redundant array of independent disks)* refere-se a uma técnica que combina múltiplos discos em uma unidade lógica (conjunto de RAIDs) e fornece proteção, desempenho ou ambos.

Os níveis de RAID comumente usados são:

- RAID 0: Conjunto fracionado sem tolerância para falhas;
- RAID 1: Espelhamento do disco;
- RAID 1+0: RAID aninhado;
- RAID 3: Conjunto fracionado com acesso paralelo e disco de paridade dedicado;
- RAID 5: Conjunto fracionado com acesso independente ao disco e uma paridade distribuída;
- RAID 6: Conjunto fracionado com acesso independente ao disco e dupla paridade distribuída.

*no passado RAID significava *redundant array of inexpensive disks*.

Fonte: EMC Information Storage and Management v3

Níveis de RAID

Fonte: ufsexplorer.com

Servidor rack – visão frontal

Fonte: Dell Server Demo Installer

Servidor rack – visão frontal

Fonte: Dell Server Demo Installer

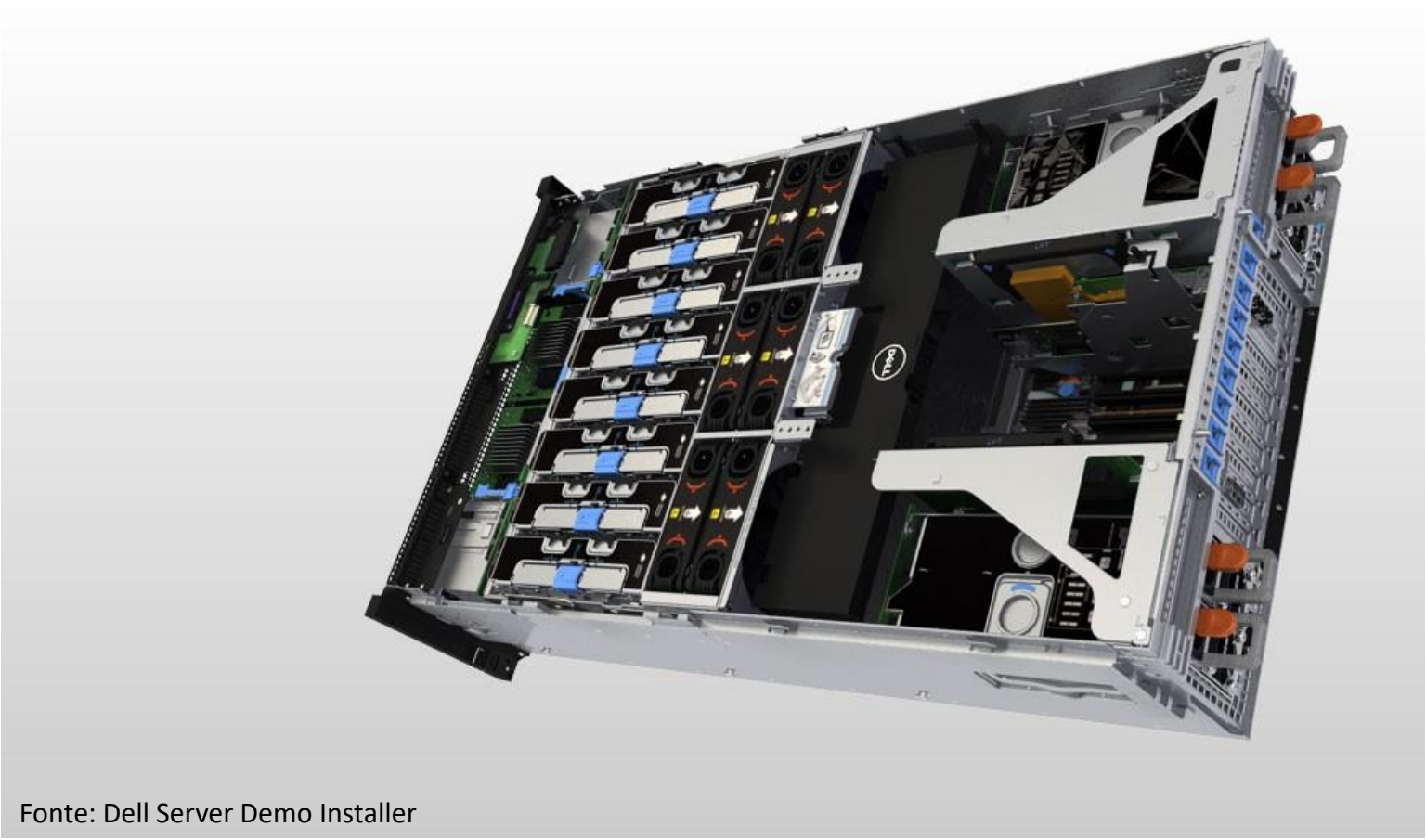
Discos hot-plug

Fonte: Dell Server Demo Installer

Servidor rack – visão superior

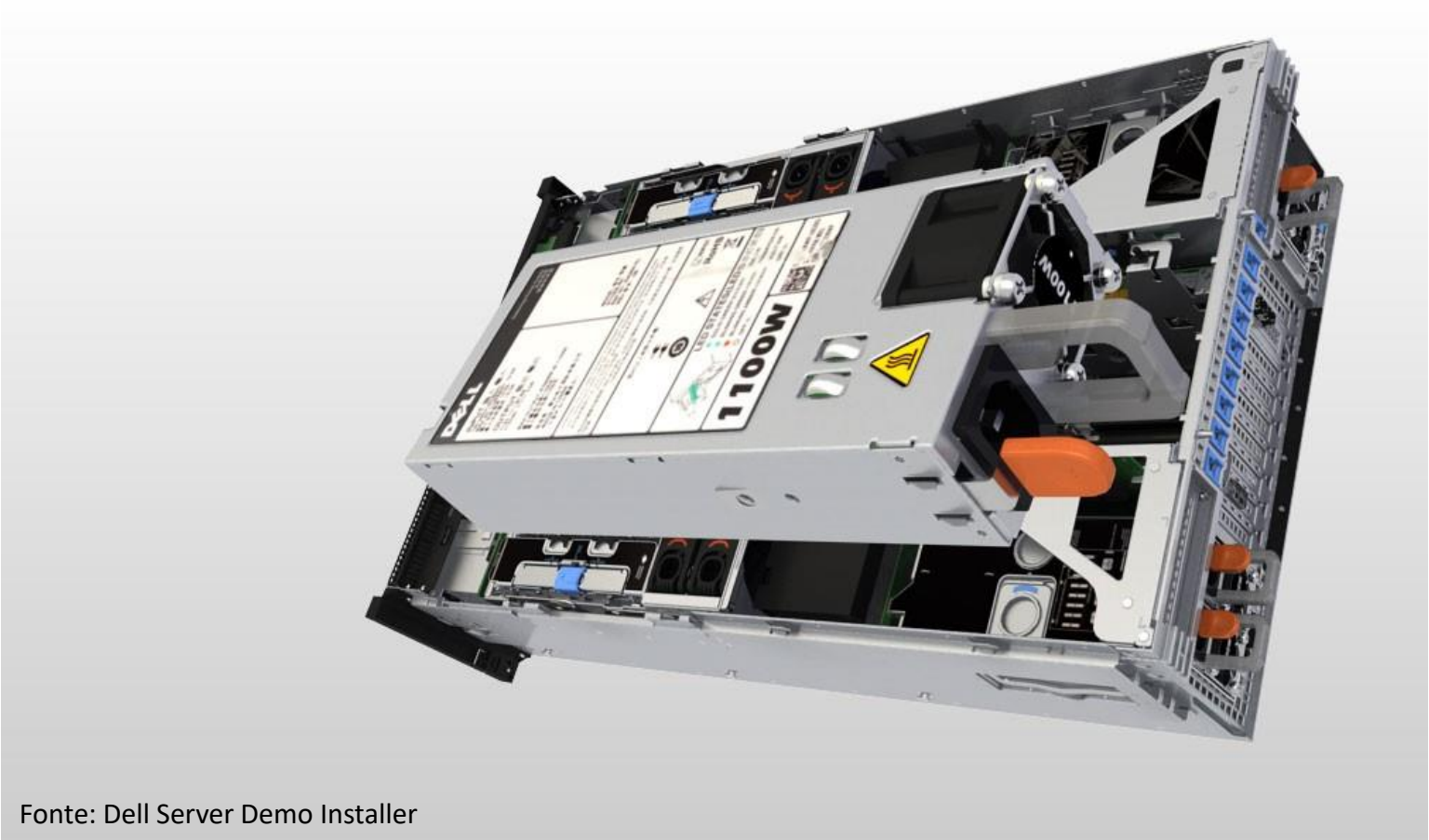
Fonte: Dell Server Demo Installer

Servidor rack – visão superior



Fonte: Dell Server Demo Installer

Fonte redundante

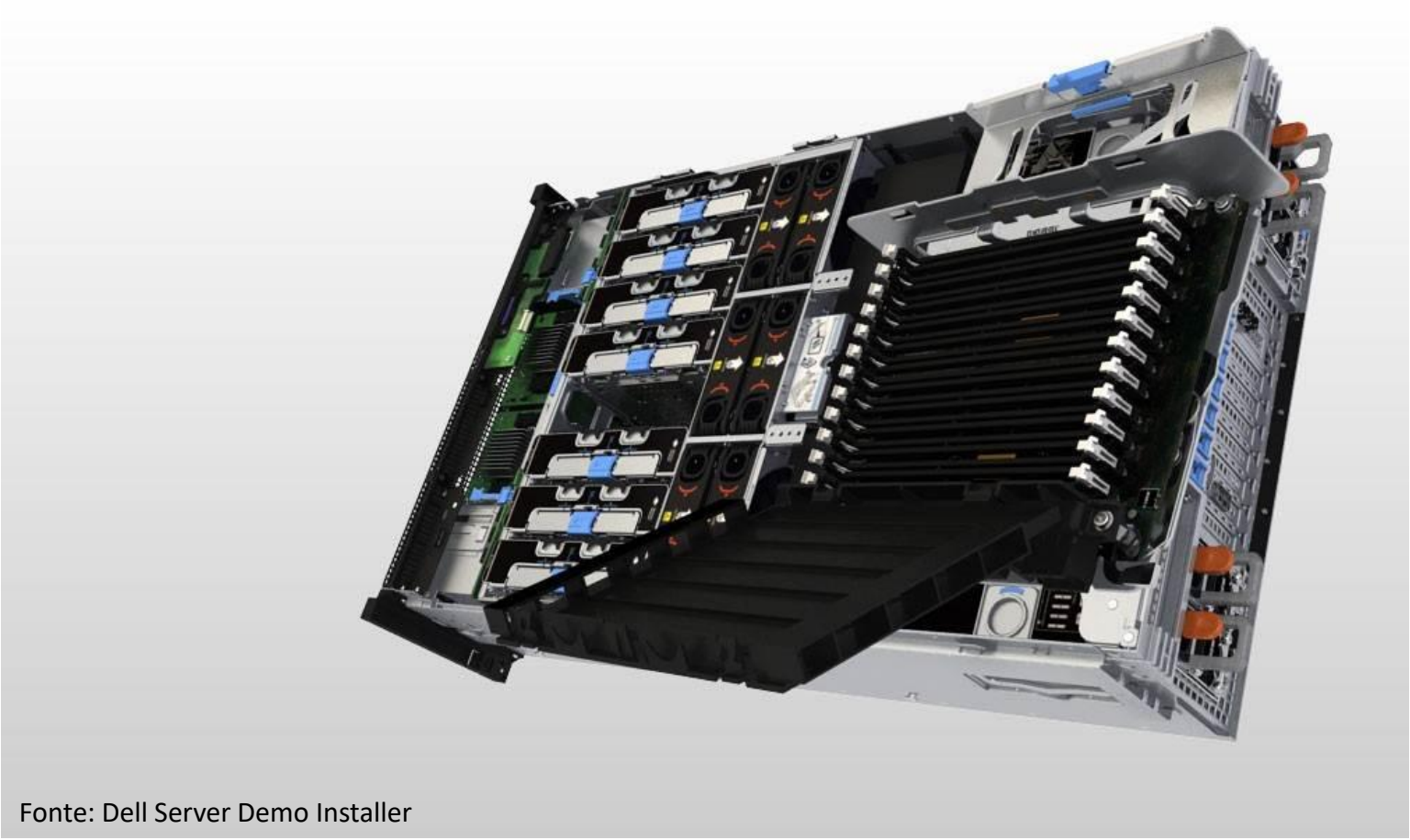


Fonte: Dell Server Demo Installer

Ventilador hot-plug

Fonte: Dell Server Demo Installer

Banco de memória



Fonte: Dell Server Demo Installer

Para saber mais...

... leia o Guia de Boas Práticas para Planos de Continuidade de Negócios, da Associação Brasileira das Entidades Fechadas de Previdência Complementar

… leia o artigo Tier Classifications Define Site Infrastructure Performance, de W. Pitt Turner IV et al.

Módulo 8

Plano de recuperação de desastres

Introdução

À medida que mais aplicativos críticos são virtualizados e os datacenters se movem em direção ao enfoque definido por software, é importante que as organizações saibam que nem todos os aplicativos têm os mesmos requisitos de recuperação.

Ao projetar uma estratégia de continuidade de negócios, as empresas devem considerar os dois parâmetros importantes que estão intimamente associados com a recuperação. São eles o RPO (Recovery Point Objective, ou Objetivo de Ponto de Recuperação) e o RTO (Recovery Time Objective, ou Objetivo de Tempo de Recuperação).

O RPO e o RTO são contados em minutos, horas ou dias, e estão diretamente relacionados com a criticidade dos serviços de TI e dos dados.

Quanto menor for o número de RTO e RPO, maior será o custo de uma solução de recuperação de desastres.

Fonte: EMC Information Storage and Management v3

Recovery Point Objective

- **RPO (Recovery Point Objective, ou Objetivo de Ponto de Recuperação):** Este é um point-in-time em que os sistemas devem estar recuperados depois de uma paralisação. Ele define o volume de dados perdidos a que uma empresa pode resistir. Com base no RPO, as organizações planejam a frequência com que deve ser feito um backup ou réplica. Uma organização pode planejar uma solução tecnológica de continuidade de negócios apropriada com base no RPO que ela define. Por exemplo, se o RPO de um aplicativo de negócios particular for 24 horas, os backups são criados todos os dias à meia-noite. A estratégia de recuperação correspondente é restaurar os dados do conjunto do último backup.

Fonte: EMC Information Storage and Management v3

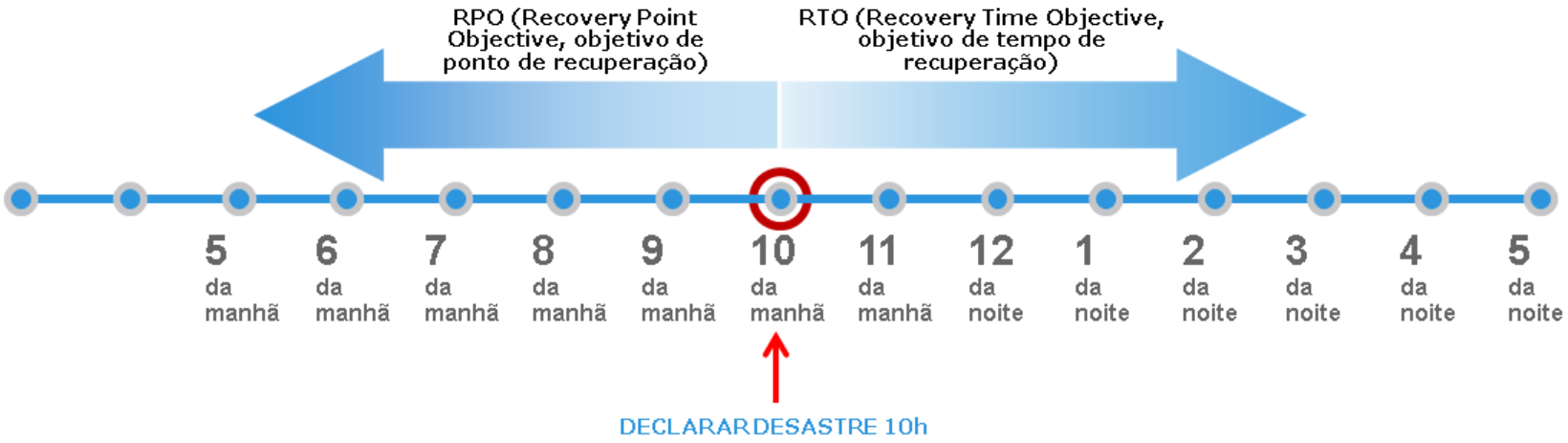
Recovery Time Objective

- **RTO (Recovery Time Objective, ou Objetivo de Tempo de Recuperação):** Esse é o tempo em que os sistemas e aplicativos devem estar recuperados depois de uma paralisação. Ele define a quantidade de tempo de inatividade que um negócio pode resistir e sobreviver. Por exemplo, se o RTO for de alguns segundos, então a implementação de clustering global ajudaria a atingir o RTO necessário. Quanto mais essencial o aplicativo, menor deve ser o RTO.

Fonte: EMC Information Storage and Management v3

Resumo

RPO (Recovery Point Objective, objetivo de ponto de recuperação)	RTO (Recovery Time Objective, objetivo de tempo de recuperação)
Point-in-time em que os sistemas devem estar recuperados depois de uma paralisação	Tempo em que os sistemas e aplicativos devem estar recuperados depois de uma paralisação
Volume de dados perdidos a que uma empresa pode resistir	Tempo de inatividade a que um negócio pode resistir e sobreviver



Fonte: EMC Information Storage and Management v3

Backup

Backup ou Cópia de Segurança é uma cópia adicional dos dados de produção, criada e retida com o objetivo exclusivo de recuperar dados perdidos ou corrompidos.

Tipicamente, tanto os dados do aplicativo quanto as configurações do servidor são incluídos em backups para restaurar dados e servidores em caso de paralisação.

As empresas também implementam soluções de backup para armazenamento de longo prazo, com o objetivo de preservar registros necessários para atender a requisitos regulamentares.

Fonte: EMC Information Storage and Management v3

Restore

A operação de recuperação de uma cópia de segurança (restore) procura atender aos seguintes objetivos:

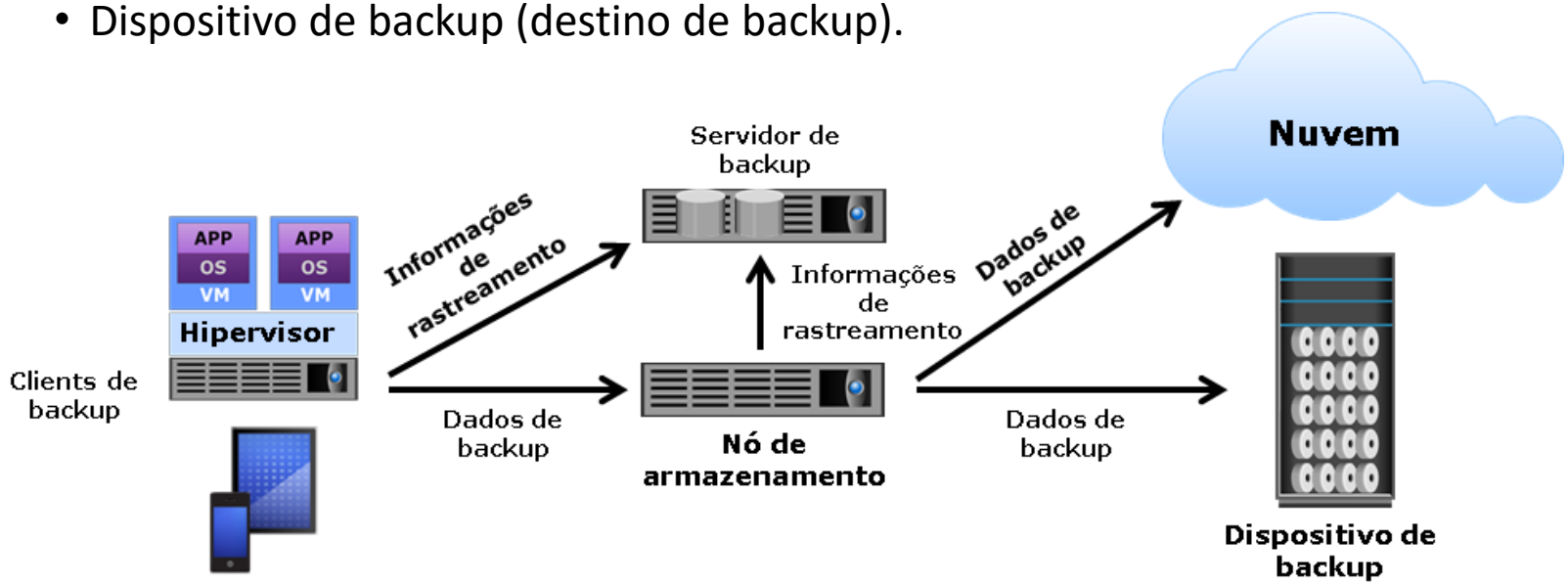
- Recuperação de desastres
  - Faz a restauração para o estado operacional após um desastre
- Restaurações operacionais
  - Permitem a recuperação em caso de perda ou corrupção lógica dos dados

Toda cópia de segurança (backup) deve ser submetida a uma operação de recuperação (restore) para verificação da mídia quanto a sua integridade.

Fonte: EMC Information Storage and Management v3

Arquitetura de backup

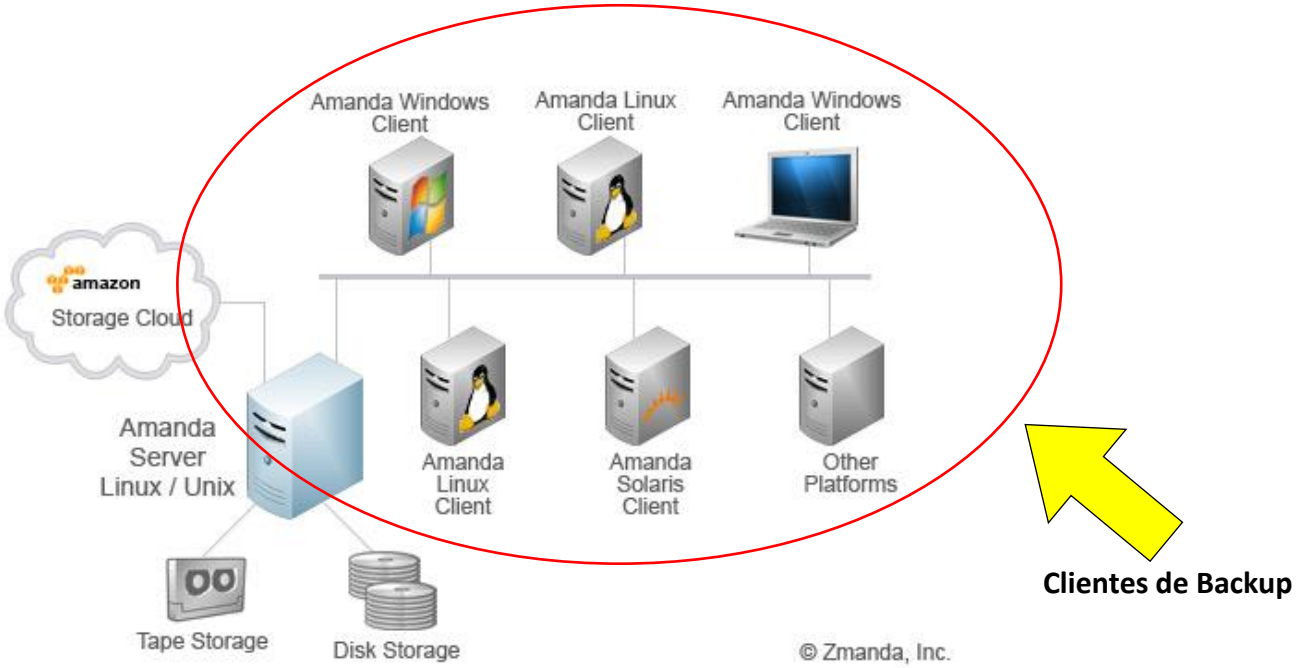
- Componentes principais do backup
  - Cliente de backup;
  - Servidor de backup;
  - Nó de armazenamento;
  - Dispositivo de backup (destino de backup).



Fonte: EMC Information Storage and Management v3

Arquitetura de backup

A função de um cliente de backup é coletar os dados a serem incluídos no backup e enviá-los ao nó de armazenamento. O cliente de backup pode ser instalado nos servidores de aplicativos, clientes móveis e desktops. Ele também envia informações de monitoramento para o servidor de backup.



Fonte: EMC Information Storage and Management v3

Arquitetura de backup

O servidor de backup gerencia as operações de backup e mantém o catálogo de backup, que contém informações sobre a configuração e os metadados do backup. A configuração do backup contém informações sobre quando os backups devem ser feitos, quais dados do cliente devem ser incluídos e assim por diante. Os metadados do backup contêm informações sobre os dados incluídos no backup.

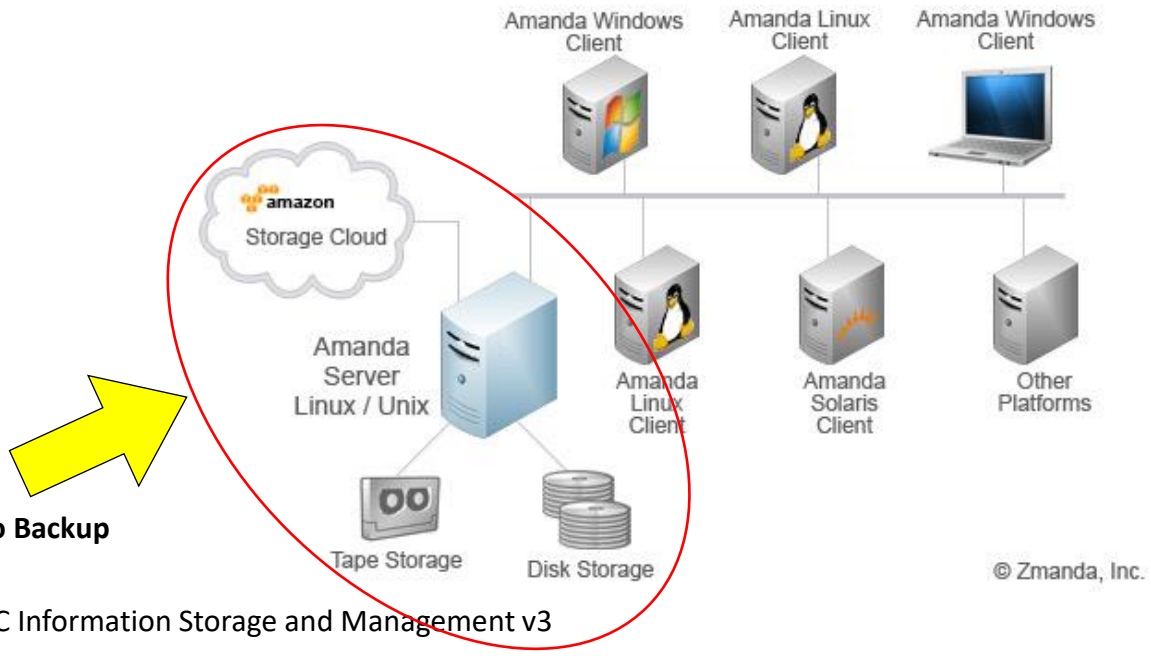
O nó de armazenamento é responsável por organizar os dados do cliente e gravá-los em um dispositivo de backup. O nó de armazenamento controla um ou mais dispositivos de backup. Os dispositivos de backup podem ser conectados diretamente ao nó de armazenamento ou através de uma rede. O nó de armazenamento envia ao servidor de backup as informações de monitoramento sobre os dados gravados no dispositivo de backup. Tipicamente, essas informações são usadas em recuperações.

Na maioria das implementações, o nó de armazenamento e o servidor de backup são executados no mesmo sistema.

Fonte: EMC Information Storage and Management v3

Arquitetura de backup

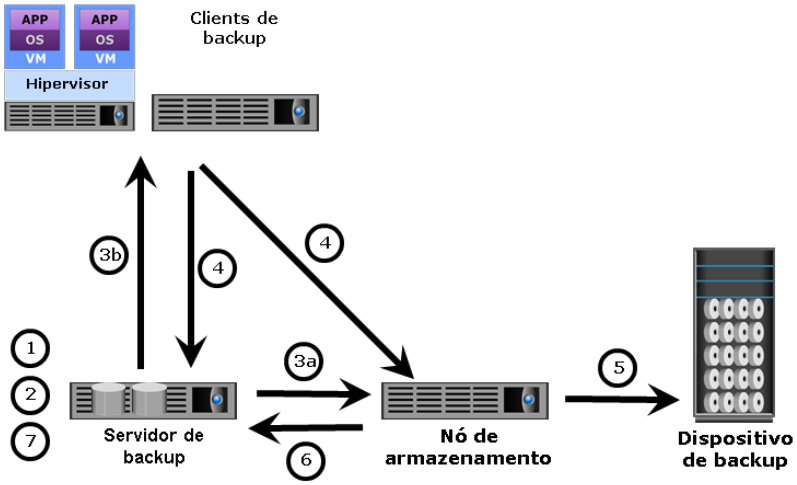
Uma ampla variedade de destinos de backup está disponível atualmente, como fita, disco e biblioteca de fitas virtuais (Virtual Tape Library ou VTL). Agora, a organização também pode fazer backup de seus dados no armazenamento em nuvem. Muitos prestadores de serviços oferecem backup como serviço, o que permite às organizações reduzir a sobrecarga de gerenciamento de backups.



Destino do Backup

Fonte: EMC Information Storage and Management v3

Operação de backup



1 - O servidor de backup inicia o processo de backup agendado.

2 - O servidor de backup obtém informações relacionadas ao backup do catálogo de backup.

3a - O servidor de backup instrui o nó de armazenamento para carregar a mídia de backup no dispositivo de backup.

3b - O servidor de backup instrui os clientes de backup a enviar dados ao nó de armazenamento incluído no backup.

4 - Os clientes de backup enviam dados ao nó de armazenamento e atualizam o catálogo de backup no servidor de backup.

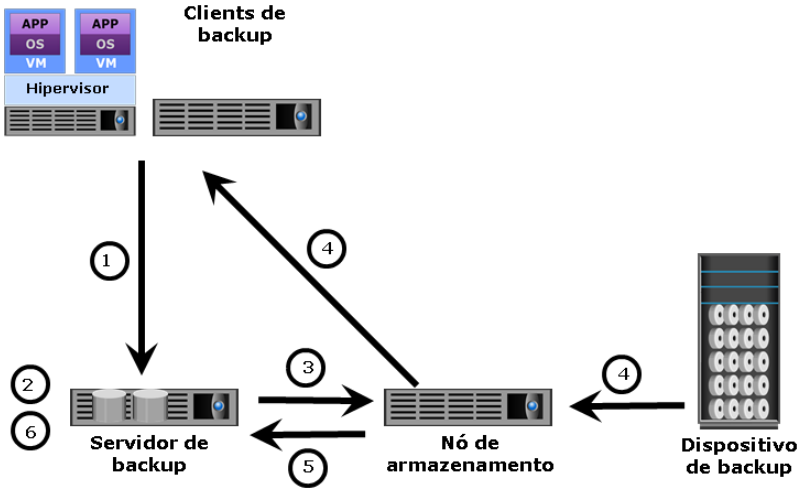
5 - O nó de armazenamento envia dados ao dispositivo de backup.

6 - O nó de armazenamento envia metadados e informações de mídia ao servidor de backup.

7 - O servidor de backup atualiza o catálogo de backup.

Fonte: EMC Information Storage and Management v3

Operação de restore



1 - O cliente de backup solicita a restauração de dados ao servidor de backup.

2 - O servidor de backup examina o catálogo de backup para identificar dados a serem restaurados e o cliente que receberá os dados.

3 - O servidor de backup instrui o nó de armazenamento a carregar a mídia de backup no dispositivo de backup.

4 - Os dados são lidos e enviados ao cliente de backup.

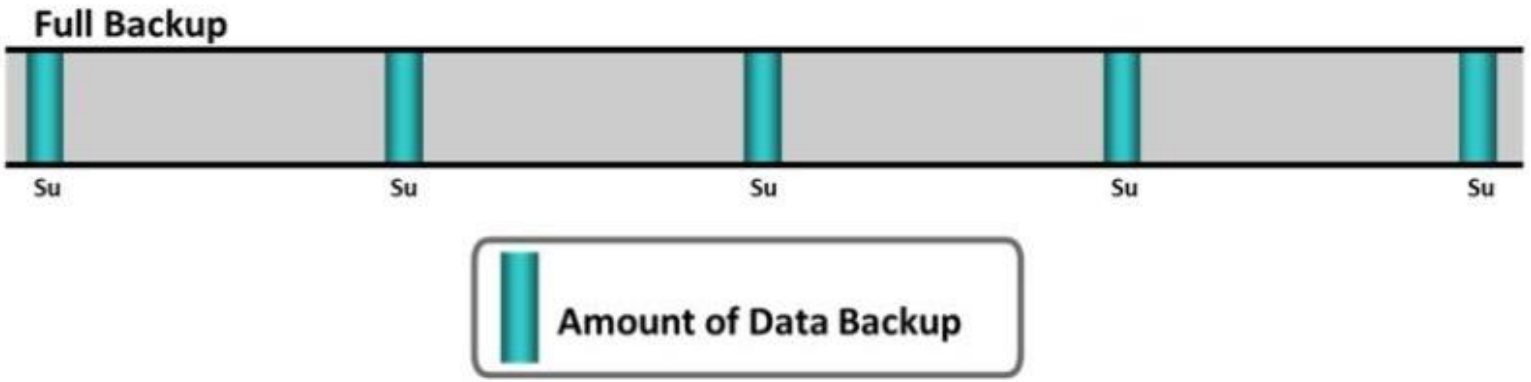
5 - O nó de armazenamento envia metadados de restauração ao servidor de backup.

6 - O servidor de backup atualiza o catálogo de backup.

Fonte: EMC Information Storage and Management v3

Granularidade

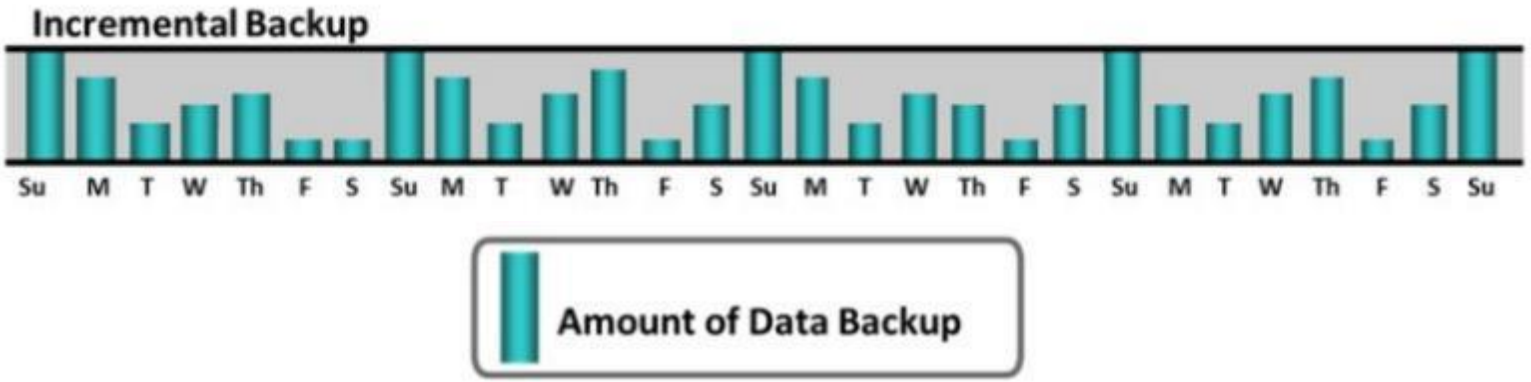
- **Backup completo:** como o nome indica, trata-se de uma cópia completa de todo o conjunto de dados. Tipicamente, as organizações usam o backup completo periodicamente, pois ele exige mais espaço de armazenamento e também demora mais para ser concluído. O backup completo oferece recuperação rápida dos dados.



Fonte: EMC Information Storage and Management v3

Granularidade

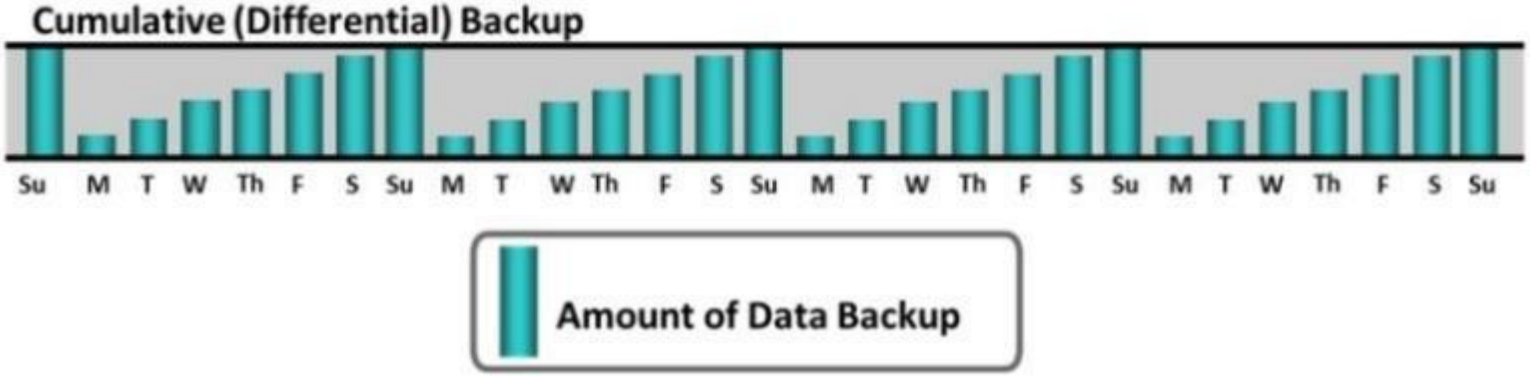
- **Backup incremental:** ele copia os dados que foram alterados desde o último backup. Por exemplo, um backup completo é criado para a segunda-feira, e backups incrementais são criados para o restante da semana. O backup de terça-feira conterá apenas os dados alterados desde segunda-feira. O backup de quarta-feira conterá apenas os dados alterados desde terça-feira. A desvantagem principal dos backups incrementais é o fato de que a restauração deles pode ser demorada. Imagine que um administrador queira restaurar o backup de quarta-feira. Para isso, ele deve primeiro restaurar o backup completo de segunda-feira. Depois, o administrador deve restaurar a cópia de terça-feira, seguida pela de quarta-feira.



Fonte: EMC Information Storage and Management v3

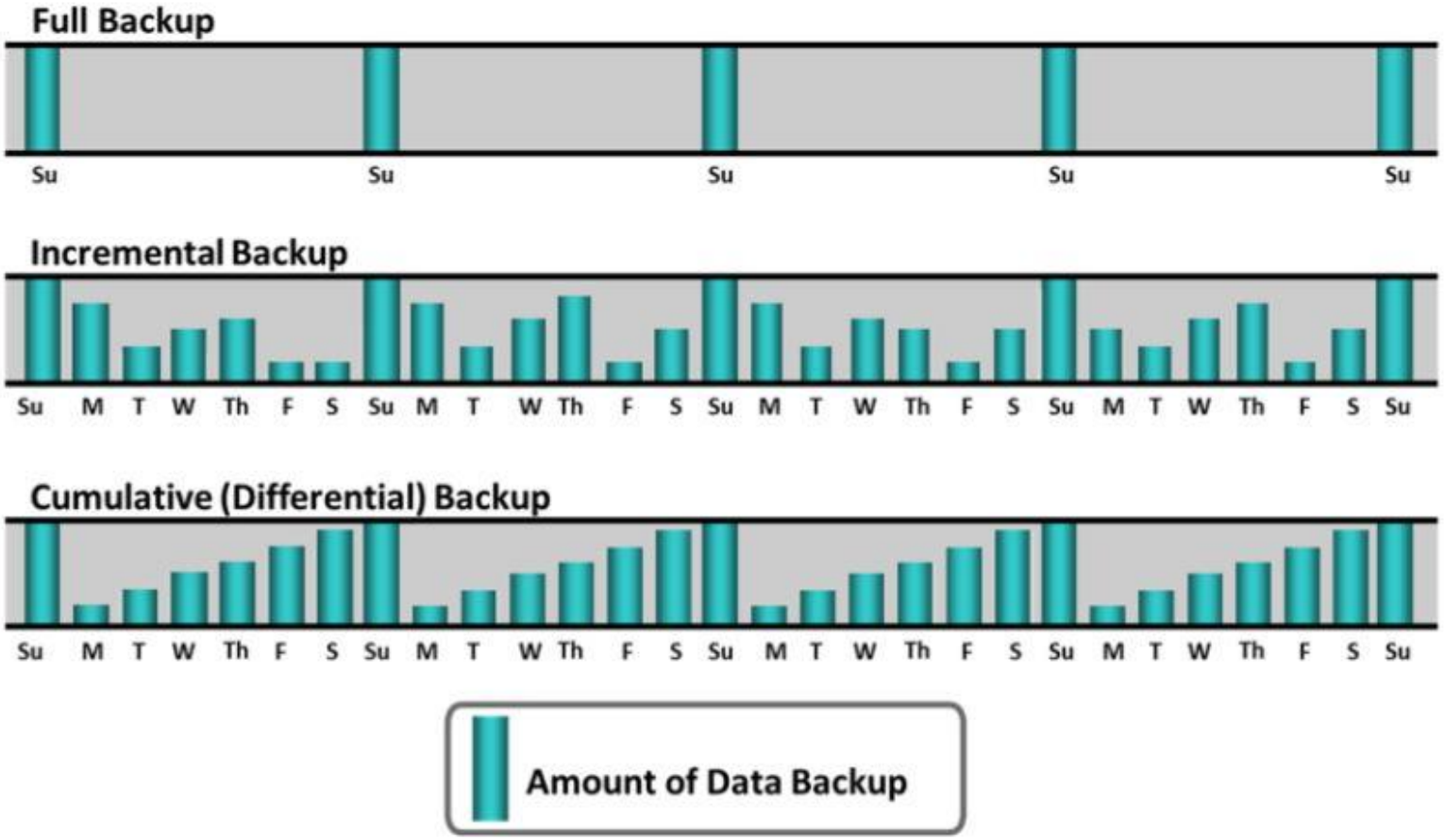
Granularidade

- **Backup cumulativo (diferencial):** ele copia os dados que foram alterados desde o último backup completo. Imagine, por exemplo, que o administrador queira criar um backup completo na segunda-feira e backups diferenciais para o restante da semana. O backup de terça-feira conterá todos os dados alterados desde segunda-feira. Neste ponto, ele seria idêntico a um backup incremental. No entanto, na quarta-feira, o backup diferencial incluirá todos os dados que foram alterados desde segunda-feira (backup completo). A vantagem dos backups diferenciais sobre os incrementais consiste nos tempos de restauração mais curtos. A restauração de um backup diferencial nunca exige mais do que duas cópias. Obviamente, a desvantagem é que, ao longo do tempo, o backup diferencial pode crescer e conter muito mais dados que o backup incremental.



Fonte: EMC Information Storage and Management v3

Granularidade - resumo



Fonte: EMC Information Storage and Management v3

Para saber mais...

… consulte o livro Armazenamento e Gerenciamento de Informações - Como Armazenar, Gerenciar e Proteger Informações, da EMC Education Services.

FIM