Olá, Professor!
Peço que realize a **avaliação do conteúdo** com o intuito de manter o nosso material sempre atualizado.

Avalie este conteúdo! 🚀 ✨

https://bit.ly/451BDqS

Introdução à segurança da informação

Princípios da segurança e o ciclo de vida da informação

Dado e informação

Dado é um valor sem contexto ou aplicação imediata.

Quando um dado é contextualizado em uma situação específica, ele se torna informação.

A informação tem valor e pode ser usada para tomada de decisões ou lucro, ao passo que dados sozinhos não têm esse potencial.

A contextualização dos dados é essencial para transformá-los em informações úteis.

Ciclo de vida da informação

A informação possui o seguinte ciclo de vida:

Criação **Transporte** **Manuseio** **Descarte**

Ciclo de vida da informação

Durante todas essas etapas, a informação deve ser protegida. Seu vazamento em quaisquer etapas pode provocar problemas em vários aspectos.

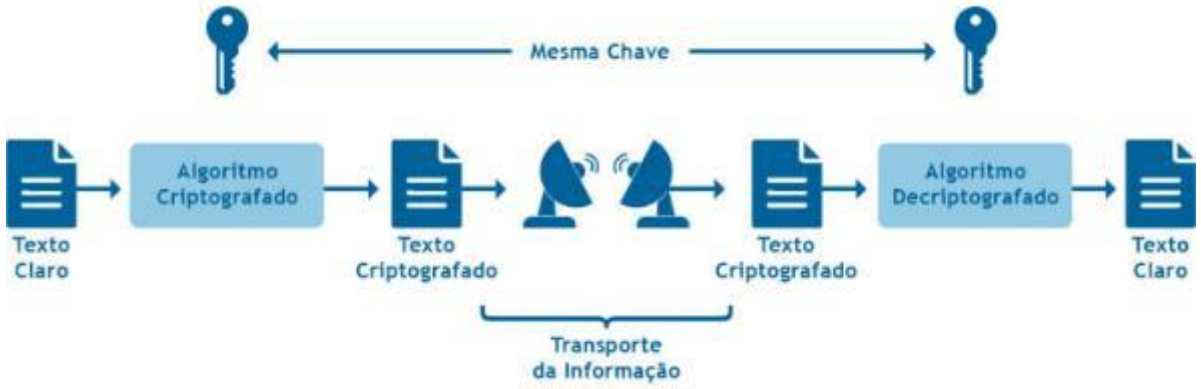
Transportadora com transporte inadequado de dados devido à falta de segurança.

Laptop desprotegido em manutenção, sujeito a roubo de dados sensíveis.

Roubo de laptop e disco rígido com dados sensíveis de veteranos devido a manuseio inadequado.

Ciclo de vida da informação

Quando a mesma chave é usada nas duas etapas, a criptografia é dita **simétrica**; quando são usadas chaves distintas, ela é **assimétrica**:



Ciclo de vida da informação

Para proteger as informações no pen drive, a prática recomendada é compactar arquivos com senha.

- Compactar com senha é eficaz, mas pode tornar o manuseio da informação mais demorado.
- Ferramentas como o 7-zip oferecem criptografia eficiente para a proteção de dados em pen drives.
- Ao descartar dispositivos como pen drives e discos rígidos, é importante usar **trituradores** adequados para evitar a recuperação de informações.

Aspectos da segurança da informação

O três principais aspectos da informação requerem cuidados especiais:

Confidencialidade

Capacidade do acesso à informação apenas para quem possui autorização.

Integridade

Possibilidade de alteração da informação por pessoas ou sistemas autorizados.

Disponibilidade

Faculdade de a informação poder ser acessada, em qualquer tempo, por pessoas ou sistemas autorizados para tal.

Aspectos da segurança da informação

Os aspectos seguintes, contudo, também são considerados importantes:

Autenticidade

Assegura que a informação foi gerada por pessoa ou sistema autorizado para isso.

Legalidade

Alinha informação e/ou dos processos com normas, portarias, leis e quaisquer outros documentos normativos, cada um na sua respectiva esfera de atribuição e abrangência.

Não repúdio

Relaciona-se ao fato de o emissor negar a autoria de uma informação divulgada. Também é conhecido como irretratabilidade.

Segurança física

Segurança física envolve a integridade e confidencialidade dos dados, dependendo da proteção das mídias e informações.

As normas ABNT ISO/IEC 27.000 dividem a segurança física em equipamentos e ambiente.

Controles físicos, como cancelas e catracas, são aplicados em camadas para proteção.

Proteção contra ameaças naturais, como incêndios, enchentes e ameaças humanas, requer monitoramento e prevenção, incluindo câmeras de segurança, extintores e redundância na rede e energia.

Segurança lógica

Medidas baseadas em software

- Segurança lógica envolve medidas baseadas em software, como senhas, listas de controle de acesso, criptografia e firewall.
- Controles biométricos, como leitura de digital e reconhecimento facial, protegem a confidencialidade da informação.
- Criptografia usa chaves e algoritmos matemáticos para embaralhar dados, incluindo algoritmos simétricos e assimétricos.

Segurança lógica

Criptografia simétrica

Algoritmos de criptografia simétrica usam uma única chave para criptografar e decriptografar, assegurando a confidencialidade."

Algoritmo	Tamanho da chave
AES (Rijnadel)	128, 192 e 256 bits
Twofish	128, 192 e 256 bits
Serpent	128, 192 e 256 bits
Blowfish	32 a 448-bits
RC4	40-128 bits
3DES (baseado no DES)	168 bits
IDEA	128 bits

Segurança lógica

Criptografia assimétrica

Criptografia Assimétrica: Usa duas chaves, pública e privada, permitindo confidencialidade e não repúdio.

Algoritmos: Diffie-Hellman, El Gamal, Curvas Elípticas.

Controles de rede: Firewalls, IDS e VPNs.

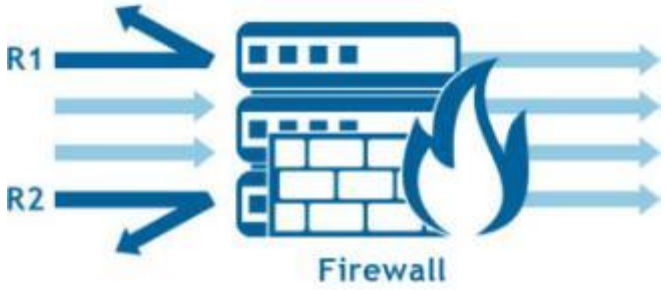
DMZ: Zona desmilitarizada para servidores web e de aplicação.

Segurança lógica

Criptografia assimétrica

As regras dos firewalls podem seguir duas políticas:

Negar por padrão



Aceitar por padrão

Ameaças e vulnerabilidades à Segurança da Informação

Ameaças e vulnerabilidades

- Informação Valiosa: Empresas dependem de informações valiosas, como patentes de vacinas, para seu valor de mercado.

- **Ativos Tangíveis e Intangíveis:** Ativos podem ser tangíveis (mensuráveis) ou intangíveis (difíceis de medir).

Ameaças e vulnerabilidades

Para compreender melhor esses conceitos:

Ativos intangíveis

São a imagem de uma organização ou um produto.

Ativos tangíveis

São aqueles que conseguimos medir.

Ameaças e vulnerabilidades

Explicação mais detalhada de cada ativo tangível:

Ativos tangíveis lógicos

São aqueles que envolvem a informação e sua representação em algoritmos.

Ativos tangíveis físicos

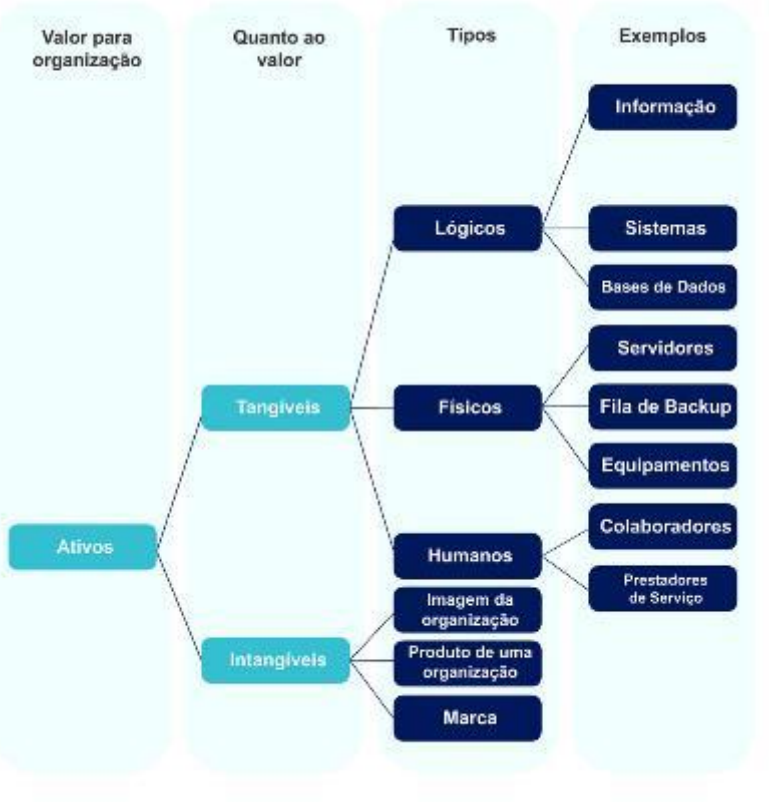
São aqueles que conseguimos tocar, como a usina hidrelétrica de Itaipu Cristo Redentor etc.

Ativos tangíveis físicos

São aqueles referentes aos colaboradores e prestadores de serviço.

Ameaças e vulnerabilidades

Os ativos tangíveis e intangíveis se posicionam e se desdobram desta maneira:



Fluxograma do posicionamento dos ativos tangíveis e intangíveis.

Ameaças e vulnerabilidades

Ativos Críticos: Perda ou dano a ativos valiosos pode causar grandes problemas financeiros.

Proteção por Controles: Controles de segurança são ferramentas e métodos para proteger ativos contra ameaças e vulnerabilidades.

Relação Ameaça-Vulnerabilidade: As ameaças podem explorar vulnerabilidades em ativos, e várias ameaças podem afetar um ativo.

Avaliação de Riscos: A avaliação considera a probabilidade de ameaças e custos de implementar controles para proteger ativos.

Tipos de ameaças e vulnerabilidades

A segurança da informação é fundamentada em três aspectos:

Diagrama dos três aspectos da segurança da informação.

Tipos de ameaças e vulnerabilidades

- **Ameaças ao WhatsApp:** Problemas de invasão no WhatsApp podem ser evitados com senhas e autenticação em duas etapas.
- **Perda de Confidencialidade e Integridade:** O armazenamento de documentos eletrônicos pode ser protegido com selos de autenticidade, como funções de hashes.

Tipos de ameaças e vulnerabilidades

Ameaças humanas originam-se de ações humanas, enquanto ameaças não humanas têm causas naturais ou de infraestrutura.

As ameaças provocadas por seres humanos podem ainda ser classificadas das duas formas a seguir:

Colaboradores

Ameaças humanas incluem ações maliciosas e incidentes causados por colaboradores mal-intencionados ou mal treinados.

Hackers

Hackers exploram vulnerabilidades por motivos diversos, como demonstração de habilidade, desafios ou ganhos financeiros.

Ataques cibernéticos

Definição

Ameaças cibernéticas são ataques maliciosos que exploram vulnerabilidades.

- Pessoas ou hackers podem realizar ataques por motivos variados.
- As ameaças visam danificar a informação, ferir a confidencialidade ou interromper sistemas.
- Além de ameaças humanas, eventos naturais ou acidentais podem causar indisponibilidade.

Ataques cibernéticos

Ataques de negação de serviço (DOS)

- Ataques de negação de serviço (DOS) visam tornar sistemas inacessíveis explorando vulnerabilidades.
- Exemplos incluem ataques como pod, syn flood, udp flood e tcp flood.
- Ataques distribuídos (DDOS) envolvem múltiplas fontes coordenando seus ataques, muitas vezes através de botnets.
- A coordenação é fundamental para sincronizar os ataques e amplificar seu impacto.

Ataques cibernéticos

Engenharia social

A engenharia social explora fraquezas humanas para obter informações, frequentemente visando a confidencialidade.

- O phishing é um exemplo comum de ataque de engenharia social, visando ganhos financeiros por meio de fraudes.
- Os ataques de phishing podem ocorrer por e-mail, SMS, redes sociais e até mesmo por dispositivos físicos, como os "chupa-cabras".
- Os fraudadores frequentemente utilizam sofisticação na criação desses dispositivos, tornando-os semelhantes aos usados pelos bancos.

Ataques cibernéticos

Pichação de site

A pichação de site envolve a alteração não autorizada de um site na internet, muitas vezes explorando vulnerabilidades.

Também conhecida como defacement, essa técnica visa adulterar o site sem consentimento, frequentemente gerando repercussão.

O ataque é comum em sistemas de gerenciamento de conteúdo (CMS), onde os proprietários personalizam seus sites.

O site Zone-H exibe conquistas de defacement, destacando a atividade nessa área.

Ataques cibernéticos

Botnets

Botnets são redes de dispositivos controlados por hackers após explorarem vulnerabilidades e instalarem software "bot".

Além dos dispositivos, as botnets incluem centros de comando e controle, permitindo ataques coordenados.

Os bots se assemelham a worms, mas respondem a ordens dos centros de controle.

Botnets são usados para ataques DDoS, envio de e-mails em massa e outras atividades maliciosas.

Outros tipos de ataques cibernéticos

Outras técnicas utilizadas em ataques cibernéticos:

Ip spoofing

Pharming ou dns cache poisoning

Ip session hijacking

Quebra de senhas

Hash

Trashing dumpster diving

Wardriving

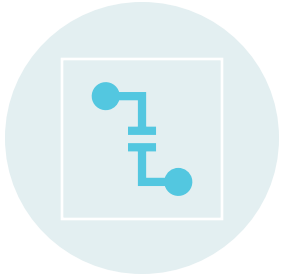
Outros tipos de ataques cibernéticos

Softwares maliciosos

Malwares são softwares maliciosos que visam infectar ativos de TI, incluindo vírus, cavalos de Troia e worms.

Spyware e adware monitoram o usuário para explorar comportamentos.

Ferramentas como sniffers e port scanners são usadas de forma mal-intencionada.



Classificações variam, mas malwares são geralmente executados em ambientes e exploram vulnerabilidades.

Outros tipos de ataques cibernéticos

Ransomware

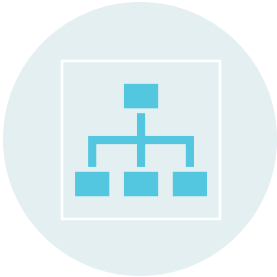
Ransomware é um malware que criptografa dados e exige resgate em troca da chave de descriptografia.

- Conhecido pelo ataque do WannaCry e sua alta proliferação nos últimos anos.
- O ataque é altamente lucrativo para criminosos e causa prejuízos significativos.
- Prevenção e backup seguro são essenciais para proteção contra ransomware.

Normas de Segurança da Informação

Conceito

Normas ISO e Segurança da Informação



ISO (International Organization for Standardization) cria padrões para várias áreas.

A norma ISO/IEC 27001 estabelece requisitos para um Sistema de Gestão da Segurança da Informação (SGSI).

O SGSI visa a proteção dos ativos de informações e a gestão de riscos de segurança.

Junto com a norma ISO/IEC 27002, é uma referência para tratar eficazmente a segurança da informação.

Requisitos

Estrutura geral da Norma ISO/IEC 27001

- A norma ISO/IEC 27001 estabelece requisitos para um Sistema de Gestão da Segurança da Informação (SGSI).
- Essa norma define o que uma organização deve fazer em relação à segurança da informação.
- A estrutura da norma inclui requisitos de avaliação e tratamento de riscos.
- A certificação ISO/IEC 27001 traz benefícios como melhor eficácia de segurança e conformidade global.

Certificados

O The ISO Survey of Certifications fornece uma visão geral dos certificados ISO em todo o mundo.

Um certificado é emitido por um organismo de certificação para atestar a conformidade com padrões.

A norma ABNT NBR ISO/IEC 27002:2013 é um código de prática para a gestão de segurança da informação.

A versão atual recomenda 114 tipos de controles básicos em comparação com a versão anterior.

Certificados

As descrições do controle estão estruturadas da seguinte forma:

Controle

Define a declaração específica do controle, para atender ao objetivo de controle.

Diretrizes para implementação

Apresenta informações mais detalhadas para apoiar a implementação do controle e alcançar o objetivo do controle.

Informações adicionais

Apresenta mais dados que podem ser considerados, como questões legais e referências normativas.

Tendências

- O estudo das normas técnicas não se limita apenas ao aprendizado dessas normas aqui apresentadas.
- Um caminho que pode ser seguido é analisar também outras normas de sistemas de gestão, tais como: qualidade, meio ambiente, conhecimento, ativos, educação etc.

Conceito

Benefícios da Norma ISO/IEC 27001

A Norma ISO/IEC 27001 ajuda a melhorar a segurança da informação.

Proporciona vantagens competitivas e satisfaz clientes.

Reduz responsabilidades, identifica fraquezas e envolve a gestão na segurança.

Aumenta a segurança para todas as partes interessadas e mede o sucesso do sistema.

Boas práticas em Segurança da Informação

Primeiros passos

Ações que ajudam a garantir a segurança da informação:

1. Nunca compartilhar senhas;
2. Sempre utilizar antivírus e mantê-lo atualizado;
3. Observar se os sites acessados são confiáveis;
4. Nunca abrir links ou fazer download de arquivos enviados por e-mails não confiáveis ou de remetentes desconhecidos;
5. Baixar programas apenas de fornecedores oficiais;
6. Fazer backup de arquivos regularmente;
7. Habilitar o firewall do sistema operacional;
8. Manter o sistema sempre atualizado.

Gerenciamento de senhas

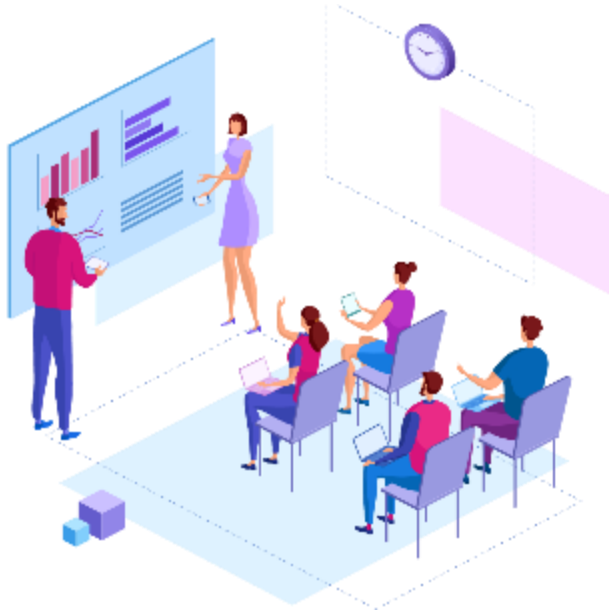
Senhas são essenciais para autenticar usuários em sistemas e devem ser seguras.

Senhas seguras têm pelo menos oito caracteres, incluem letras maiúsculas, minúsculas, números e caracteres especiais.

Senhas não devem ser compartilhadas, repetidas em várias contas ou baseadas em informações pessoais.

É crucial alterar senhas regularmente, especialmente após vazamentos de dados.

Treinamento



Treinamento em segurança é essencial para combater ameaças cibernéticas, como phishing.

- Conscientização contínua é crucial, pois os cibercriminosos estão em constante evolução.
- A ISO/IEC 27002 oferece diretrizes abrangentes para a segurança da informação.
- O treinamento aborda vários aspectos, incluindo políticas, organização, controle de acesso e continuidade do negócio.

Treinamento

Com o objetivo de apoiar as organizações a desenvolverem um programa eficaz de treinamento em conscientização de segurança, são sugeridas as seguintes recomendações baseadas na ISO/IEC 27002:

Obrigatoriedade do envolvimento da diretoria

Envolvimento de toda a organização

Criação de conteúdo para treinamento e conscientização de segurança

Diversidade de treinamento

Exercícios de simulação

Periodicidade na realização do treinamento de conscientização de seguraça

Mecanismos de Proteção

Trata-se do **conjunto de ações e recursos** que visa a **proteger um sistema ou uma organização**. Esses mecanismos são definidos considerando o ponto de vista da organização e dos sistemas:

Do ponto de vista da organização

Referem-se às restrições de comportamento de seus membros e de possíveis atacantes por meio de mecanismos como portas, fechaduras, chaves e paredes.

Do ponto de vista dos sistemas

A política de segurança aborda restrições de funções e de fluxo, entre elas, restrições de acesso por sistemas externos e adversários.

Mecanismos de Proteção

A seguir estão alguns exemplos de princípios que se aplicam aos mecanismos de proteção:

Economia de mecanismo

Padrões à prova de falhas

Mediação completa

Projeto aberto

Separação de privilégio

Privilégio mínimo

Compartilhamento mínimo

Aceitação psicológica

Controle de acesso

Controle de acesso limita a abordagem a sistemas ou recursos, como na computação em nuvem.

Os usuários precisam fornecer credenciais, como senhas ou identificação biométrica.

Isso garante que apenas pessoas autorizadas acessem sistemas ou informações.

É crucial para a segurança da informação e proteção de recursos.

Controle de acesso

Existem **três tipos de sistemas de controle de acesso**:

Controle de acesso discricionário ou discretionary acess control (DAC)

Controle de acesso obrigatório ou mandatory access control (MAC)

Controle de acesso baseado em função ou role-based acess control (RBAC)

Controle de acesso

Os objetivos dos controles de acesso são garantir:

- O acesso aos recursos apenas por usuários autorizados.
- A correspondência entre os recursos necessários e as atividades dos usuários.
- O monitoramento e a restrição do acesso a recursos críticos.
- Execução de transações compatíveis com as funções e responsabilidades dos usuários.

Controle de acesso

Controle de acesso envolve identificação e autenticação de usuários.

O logon requer um ID (login) e senha para garantir que o usuário seja legítimo.

Procedimentos de logon eficazes não devem divulgar informações desnecessárias.

Identificação única do usuário e autenticação adequada são essenciais para a segurança do sistema.

Política contra vírus

- Política contra vírus é essencial para proteger sistemas.
- Vírus são programas maliciosos que se replicam e danificam computadores.
- Existem diversas categorias de vírus com objetivos variados.
- A política visa prevenir, detectar e mitigar ameaças de vírus.

Política contra vírus

Principais tipos de vírus de computador:

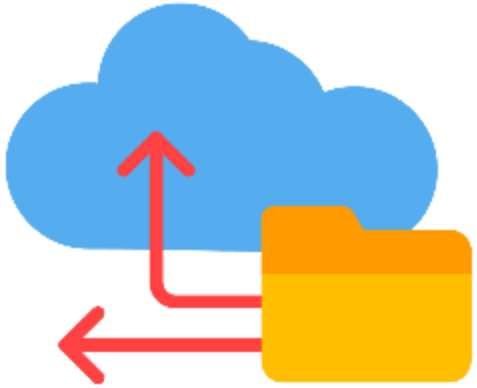
Vírus de arquivo	**Vírus de boot**	**Vírus de macro**	**Código-fonte vírus**
Mutante	**Polimórfico**	**Cavalo de Troia (trojan)**	**Vírus *multipartite***
Vírus *stealth*	**Vírus de encapsulamento**	**Vírus criptografado**	**Vírus blindado**

Política contra vírus

Orientações:

- Computadores na rede institucional precisam de antivírus atualizado e verificações regulares.
- Recomenda-se programar atualizações regulares dos servidores antivírus centralizados nos computadores da rede.
- É essencial verificar arquivos recebidos eletronicamente quanto a vírus imediatamente após o recebimento.
- Dispositivos de armazenamento, como pendrives e HDs externos, devem ser verificados quanto a vírus antes de serem usados.
- Não inicie computadores ou servidores a partir de dispositivos externos de fontes desconhecidas.
- Carregue software antivírus em todos os computadores e servidores para monitorar e prevenir ataques de vírus.

Sistemas de backup



Backup é a cópia de segurança de dados para evitar perdas.

- Deve haver uma política de backup com responsáveis, periodicidade e locais de armazenamento definidos.
- Testes regulares garantem a restauração eficaz dos dados.
- Uma boa política de backup minimiza problemas em caso de perda de dados.

Sistemas de backup

Existem alguns tipos de sistemas de backups:

Backup completo

Backup incremental

Backup diferencial

Criptografia

Criptografia consiste no ato de codificar dados para que apenas pessoas autorizadas consigam ter acesso às informações. Pode ser classificada em três tipos:

Criptografia de chave simétrica

Função Hash

Criptografia de chaves assimétricas

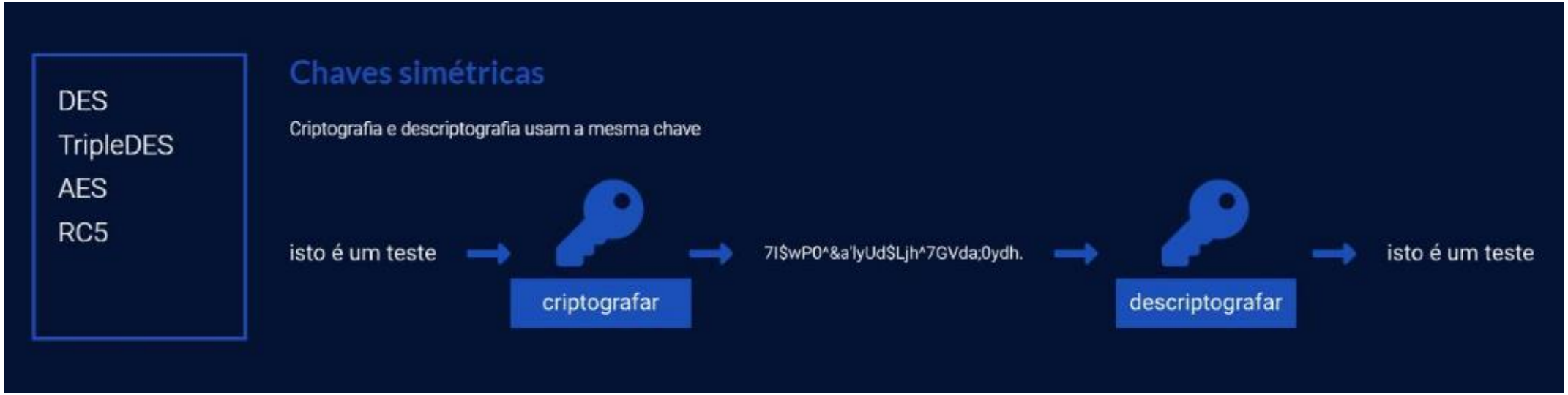
Criptografia

Criptografia de chave simétrica

- A criptografia de chave simétrica envolve uma única chave para criptografar e descriptografar mensagens.
- AES é um exemplo comum de algoritmo de criptografia de chave simétrica.
- Outros tipos incluem DES, RC2, IDEA, Blowfish e Stream cipher.

Criptografia

Criptografia de chave simétrica



Criptografia

Criptografia de chave assimétrica

- A criptografia de chave assimétrica envolve duas chaves: uma privada e uma pública.
- A chave pública é compartilhada, enquanto a chave privada é mantida em segredo.
- O RSA é um algoritmo comum usado nesse método.
- É mais seguro do que a criptografia de chave simétrica. Veja a ilustração fornecida.

Criptografia

Criptografia de chave assimétrica

Criptografia

Função Hash

A função hash usa uma função matemática para criar uma impressão digital irreversível dos dados.

Garante a integridade da mensagem, detectando alterações nos dados.

Exemplos de algoritmos de hash incluem MD5, SHA, Whirlpool e RIPEMD.

Diferentes tipos de criptografia são otimizados para aplicações específicas, como privacidade, confidencialidade, integridade e troca de chaves.

Criptografia

Função Hash

Certificado digital

O **certificado digital** é um **documento eletrônico** que **identifica pessoas e instituições**, provando identidades e permitindo o acesso a serviços informatizados que garantam:

Autenticidade

Integridade

Não repúdio

Certificado digital

O certificado digital é usado para assinar documentos digitalmente.

Emitido por uma Autoridade Certificadora (AC) para indivíduos ou entidades.

Deve conter nome do sujeito, chave pública, número de série, data de validade, assinatura digital da AC e outras informações.

A cadeia de confiança verifica a autenticidade do certificado, ligando-o à AC confiável.

Certificado digital

Utilização de certificado digital:

Bancos

Os bancos possuem certificado para autenticar-se perante o cliente, assegurando que o acesso está realmente ocorrendo com o servidor deles (aqui cabe lembrar o nome dessa característica de segurança da informação: autenticidade).

Cliente

Em contrapartida, o cliente, ao solicitar um serviço, como, por exemplo, acesso ao extrato da conta corrente, pode utilizar o seu certificado para autenticar-se perante o banco.

Certificado digital

A figura a seguir mostra como os certificados digitais podem ser usados para validar a identidade de um provedor de conteúdo.

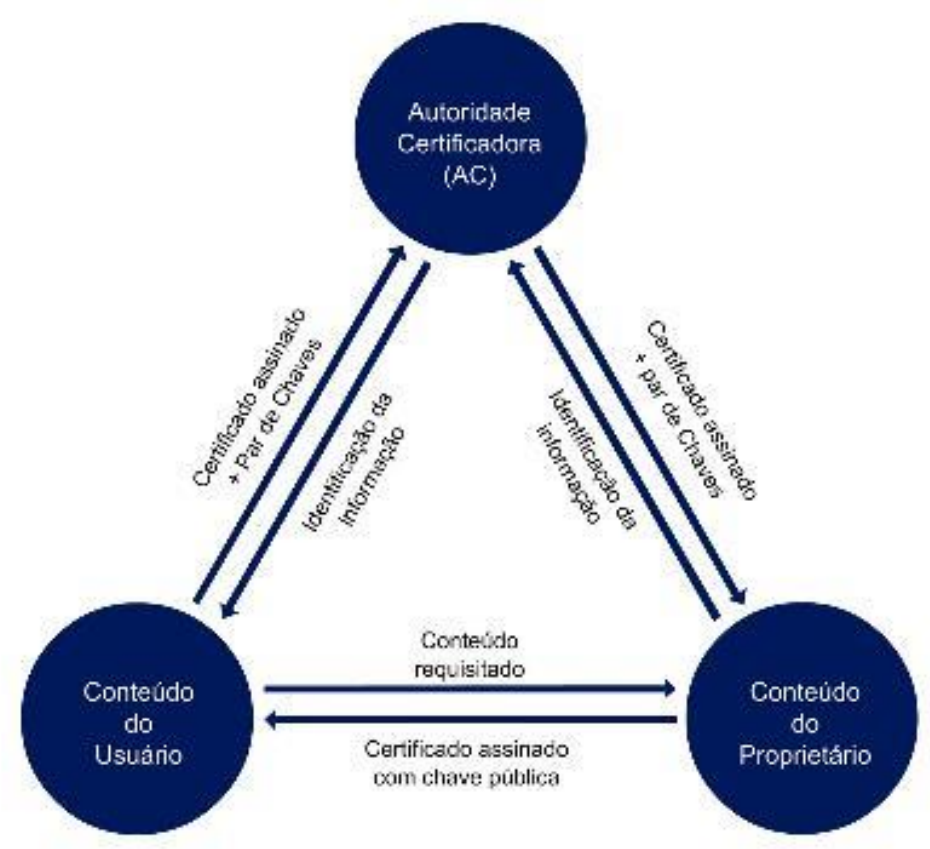


Diagrama do Certificado Digital.

Certificado digital

Os certificados são utilizados em diversas aplicações:

- Automatização da prestação de informações fiscais à Receita Federal do Brasil
- Nota fiscal eletrônica
- Informatização do Poder Judiciário
- Informatização de serviços cartoriais
- Informatização de processos para abertura de empresas
- Informatização de prontuários médico-odontológicos
- Compras governamentais por meio de pregão eletrônico

Certificado digital

Regulamentos da ICP-Brasil incluem a Medida Provisória 2.200-2, decretos e resoluções do Comitê Gestor.

A Medida Provisória 2.200-2 é o marco legal principal da ICP-Brasil, com força de lei.

Certificados digitais têm data de validade e podem ser cancelados ou revogados, com listas de certificados de revogação (CRL).

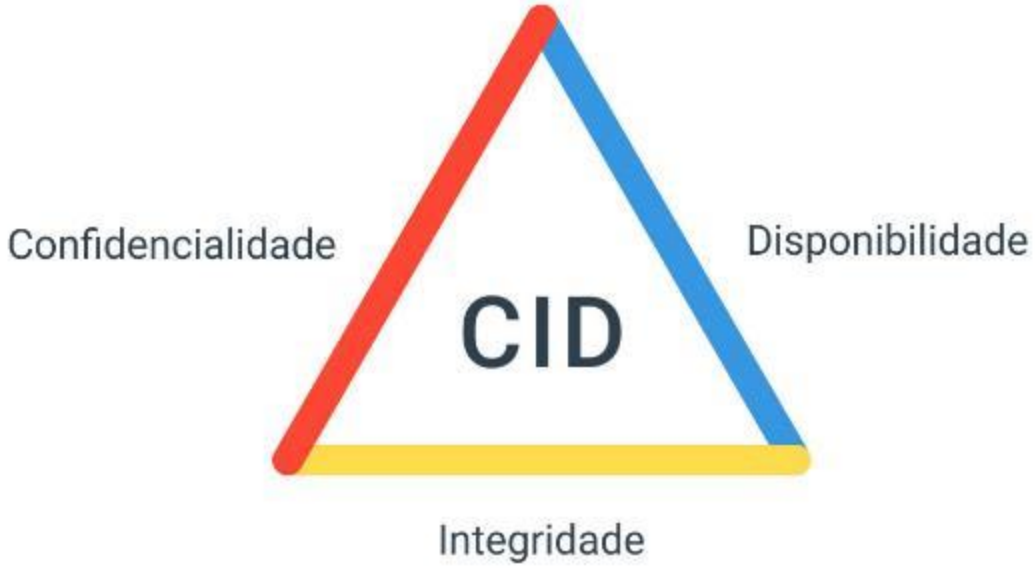
Transações com certificados digitais são mais seguras e o avanço da criptografia contribui para a segurança nas operações online.

Gestão de risco

Segurança da informação

Pilares

Pilares da segurança da informação:



Segurança da informação

Pilares

No CID, minimiza-se o risco da ocorrência de incidentes que:

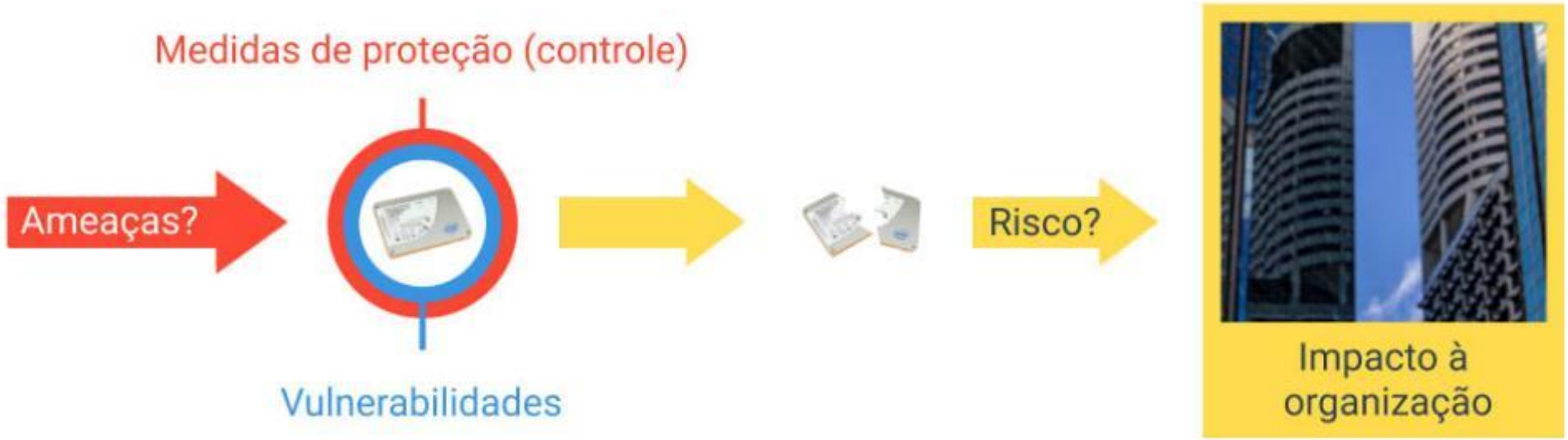
Disponibilizem uma informação para pessoas, entidades ou processos não autorizados (confidencialidade).

Afetem a exatidão e a integralidade de ativos (integridade).

Tornem os recursos inacessíveis e inutilizáveis sob demanda (disponibilidade).

Segurança da informação

Pilares



Segurança da informação

Ativos

- **Ativos de informação:** Dados, arquivos, contratos e acordos.
- **Ativos de software:** Aplicativos e sistemas.
- **Ativos físicos:** Equipamentos de TI e comunicação.
- **Intangíveis:** Reputação e imagem da organização.

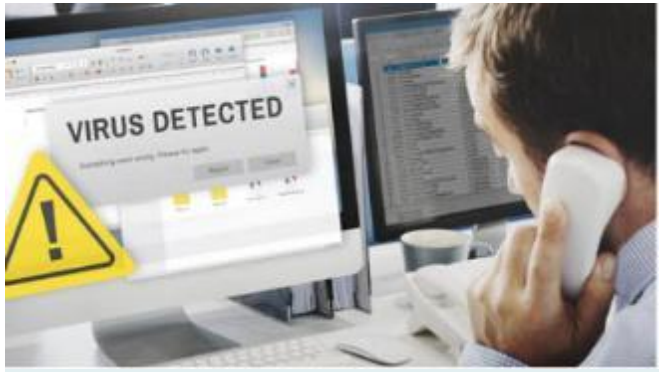
Segurança da informação

Ameaças

Os ativos estão sujeitos a ameaças de várias naturezas. Elas podem ser:

Físicas

Falhas de equipamentos e instalações, como relâmpagos, terremotos, ataques a bombas etc.



Lógicas

Vulnerabilidades em softwares, como bugs, vírus, malwares etc.

Segurança da informação

Medidas de proteção (controle)

- Medidas de proteção reduzem riscos.
- Controles podem ser políticas, práticas ou dispositivos.
- **Objetivo:** modificar ameaças e vulnerabilidades.
- Norma ISO/IEC 27000:2018 define controle.

Segurança da informação

Vulnerabilidades

- Vulnerabilidade: fragilidade que ameaças podem explorar.
- Identificação não é trivial.
- Análise de vulnerabilidades detecta falhas.
- Avaliação associa ameaças à probabilidade de ocorrência.

Segurança da informação

Vulnerabilidades

Alguns exemplos de ameaças, vulnerabilidades e medidas de controle cabíveis:

Ameaças	Vulnerabilidades	Medidas de controle
Lógicas	• Problemas no sistema operacional; • Falhas em aplicativos; • Sites perigosos da web.	• Instalação de antivírus; • Firewall; • Lista de controle de acesso; • Atualização do sistema operacional.
Físicas	• Falta de identificação de visitantes na empresa; • Fios soltos; • Sala do datacenter acessível para qualquer pessoa.	• Instalação de câmeras de segurança; • Acesso à sala por controle biométrico; • Piso elevado contra enchentes; • Para-raios; • Nobreaks.

Segurança da informação

Incidente

Incidente de segurança ocorre quando ameaças exploram vulnerabilidades.

Exemplos incluem malware, roubo de senhas e cópia não autorizada de dados.

Definido pela ISO/IEC 27000:2018 como evento que compromete operações ou ameaça segurança da informação.

Segurança da informação

Evento

- **Evento de segurança:** Indica possíveis falhas de política ou salvaguardas.
- **Exemplos:** Travamento inesperado de aplicação, desconexão acidental.
- **Impacto:** Mudança indesejável nos objetivos de negócios.
- **Risco:** Combina consequências e probabilidade de eventos.

Sistemas de gestão

Sistemas de gestão de riscos (SGR)

- SGR: Sistemas de gestão de riscos.
- Práticas e procedimentos para gerenciar riscos.
- Minimiza ocorrência e impacto de incidentes de segurança.
- Importante para reduzir danos e prejuízos.

Sistemas de gestão

Sistema de Gestão de Segurança da Informação (SGSI)

- **Controle:** Medida que modifica riscos.
- **Ameaça:** Potencial causa de incidentes de segurança.
- **Vulnerabilidade:** Fragilidade explorável que compromete segurança.
- **Evento de segurança:** Ocorrência indicando falha na segurança.
- **Incidente de segurança:** Evento que compromete operações ou segurança.
- **Risco:** Combina consequências e probabilidade de evento.
- **Impacto:** Mudança indesejável nos objetivos de negócios.

Risco à segurança da informação

Gestão de Riscos na Segurança da Informação é fundamental para proteger ativos como servidores e bancos de dados.

Exemplo: XPTO enfrenta risco extremo devido ao malware "No pain, no gain" devido a vulnerabilidades não tratadas.

O plano de tratamento para mitigar o risco envolve atualizações preventivas e monitoramento contínuo.

Percepção de risco varia entre organizações, influenciada pela infraestrutura e contexto. Critério de risco define o que é tolerável.

Gestão de riscos

Normas relevantes para a Gestão de Riscos incluem ABNT NBR ISO/IEC 27005 e ABNT NBR ISO/IEC 31000.

O papel da GR é identificar e tratar riscos de forma sistemática e contínua, um componente crucial da Gestão de Segurança da Informação (GSI).

A GR deve ser permanente, detectando novas vulnerabilidades e ameaças que afetam confidencialidade, integridade e disponibilidade.

Para uma GR eficaz, é essencial criar uma estrutura organizacional adequada e desenvolver uma cultura de GR para manter riscos em níveis aceitáveis.

Etapas da gestão de riscos

Definição do contexto

Listagem dos objetivos organizacionais é fundamental para o gerenciamento de riscos.

Levantamento de informações relevantes sobre o ambiente onde a análise de riscos ocorrerá.

Compreensão das atividades da organização e seus propósitos na Governança de Segurança da Informação (GSI).

Propósitos incluem suporte ao SGSI, conformidade legal e planos de continuidade de negócios e resposta a incidentes.

Etapas da gestão de riscos

Definição do contexto

Itens que devem constar nessa análise da organização:

Propósito principal da organização	Negócio	Missão	Visão de futuro
Valores	Estrutura organizacional	Organograma	Estratégias
Produtos	Parceiros	Terceiros	Instalações
	Funcionários		

Etapas da gestão de riscos

Processo de análise/avaliação de riscos de segurança da informação

Esta etapa se divide em:

Etapas da gestão de riscos

Processo de análise/avaliação de riscos de segurança da informação

Análise de riscos compreende identificação, estimativa e avaliação de riscos.

Identificação mapeia eventos de risco e suas causas e consequências.

Estimativa calcula o nível de risco, considerando probabilidade e impacto.

Avaliação define medidas de tratamento com base no nível de risco residual e apetite a risco.

Etapas da gestão de riscos

Processo de análise/avaliação de riscos de segurança da informação

Probabilidade	Termo	Definição
71 a 90%	Alta	Chance de a ameaça se concretizar em um ano
31 a 70%	Média	Possibilidade de a ameaça se concretizar no próximo ano
1 a 30%	Baixa	Dificilmente a ameaça ocorrerá no próximo ano

Medição qualitativa da probabilidade – exemplificação. Probabilidade: chance de um evento acontecer.

Etapas da gestão de riscos

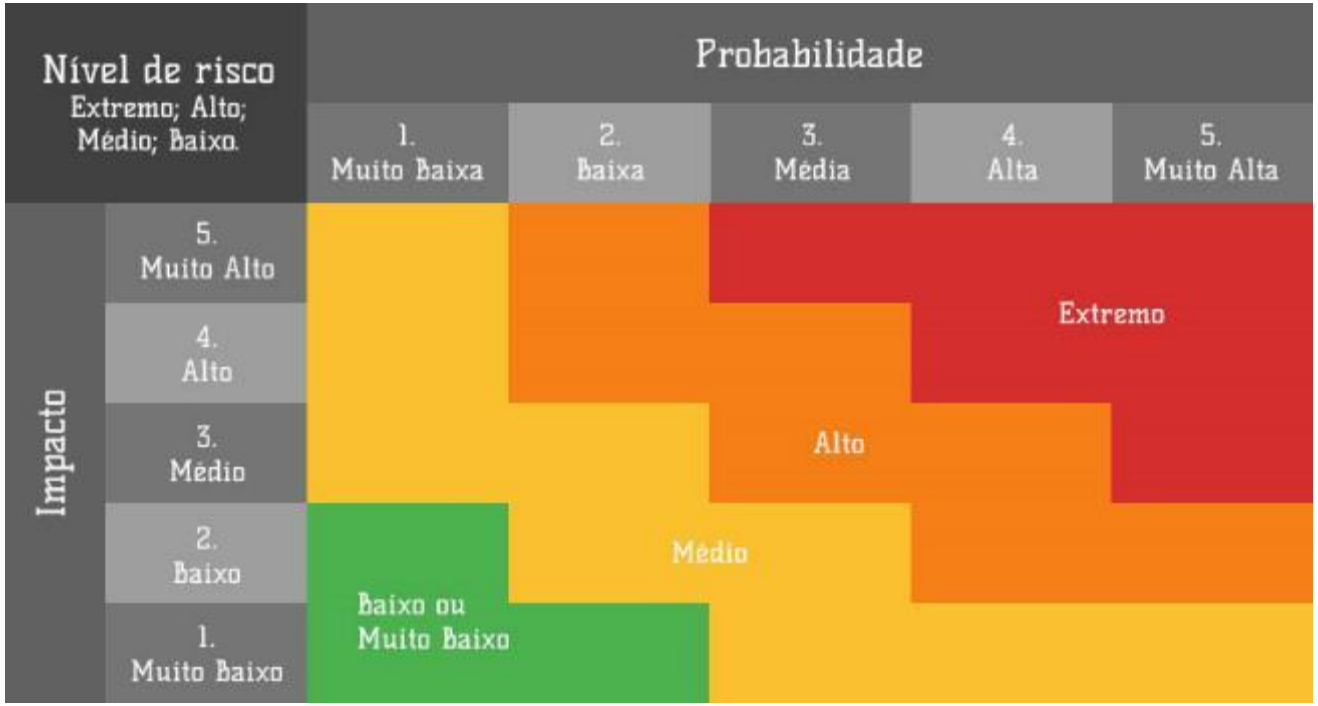
Processo de análise/avaliação de riscos de segurança da informação

Impacto	
Termo	Definição
Alto	Grave comprometimento da missão da organização
Médio	As perdas são restritivas a um segmento dela
Baixo	Sem muita relevância para seus negócios

Medição qualitativa da probabilidade – exemplificação. Impacto: medida para avaliar a magnitude de uma eventual perda.

Etapas da gestão de riscos

Processo de análise/avaliação de riscos de segurança da informação



Matriz de riscos.

Etapas da gestão de riscos

Processo de análise/avaliação de riscos de segurança da informação

Etapas da gestão de riscos

Tratamento do risco de segurança da informação

O tratamento do risco envolve a implementação de medidas específicas.

Cada medida de tratamento deve indicar responsáveis, prazos e ações.

O plano de tratamento do risco é estabelecido para reduzir riscos identificados.

Medidas de proteção, como criptografia e senhas robustas, devem ser definidas para ameaças específicas.

Etapas da gestão de riscos

Medidas de controle ou proteção

- **Preventiva**: Evita que incidentes ocorram.
- **Desencorajadora**: Desencoraja a prática de ações.
- **Monitoradora**: Monitora o estado e o funcionamento.
- **Corretiva**: Corrige falhas existentes.
- **Recuperadora**: Repara danos causados por incidentes.
- **Reativa**: Reage a determinados incidentes.
- **Limitadora**: Diminui os danos causados.

Etapas da gestão de riscos

Aceitação do risco de segurança da informação

A decisão de aceitar os riscos residuais não basta: é necessário se responsabilizar por ela. Afinal, é responsabilidade da política de gestão de riscos oferecer suporte a essa tomada de decisão.

Etapas da gestão de riscos

Comunicação do risco de segurança da informação

Recomenda-se que as informações sobre riscos sejam trocadas ou compartilhadas entre o tomador de decisão e as outras partes interessadas para haver um consenso sobre como eles devem ser administrados.

Etapas da gestão de riscos

Monitoramento e análise crítica de riscos de segurança da informação

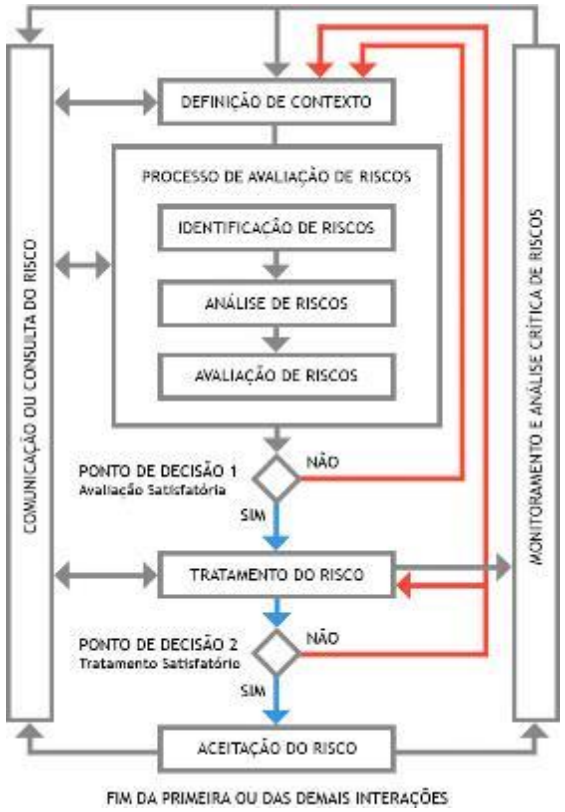
Nesta etapa, é avaliado se tudo o que foi feito saiu de acordo com o planejado. Além disso, são averiguados, dentre outros, os seguintes casos:

- Necessidade de atualizações.
- Listagem correta dos objetivos.
- Impossibilidade de um risco ser visto como esperado pelas atividades de controle.
- Cálculo correto dos níveis de risco.

Etapas da gestão de riscos

Monitoramento e análise crítica de riscos de segurança da informação

Visão do processo de gestão de risco (GR) segundo a norma ABNT NBR ISO/IEC 27005:



Governança, risco e *compliance*

Governança corporativa

Cuida para que o controle da gestão seja tão importante quanto ela própria.

Gestão de riscos

Gerencia o efeito da incerteza nos objetivos.

Compliance

Adere aos padrões da legislação (regulamentos oficiais vigentes, políticas empresariais e normas internas de procedimentos).

Gestão de continuidade do negócio

Conceitos

PCN (ABNT NBR 15999 Parte 1): Estratégias e planos para garantir recuperação e continuidade após desastres.

Os desastres podem ser ocasionados por diversos motivos:

Causas naturais

Falhas de segurança

Acidentes

Falhas de equipamentos

Ações propositais

Conceitos

O Plano de Continuidade de Negócios (PCN) visa preservar operações críticas e minimizar impactos.

Define diretrizes e responsabilidades no Sistema de Gestão de Continuidade de Negócios.

Identifica operações críticas, riscos, medidas de mitigação e ação em emergências.

Deve ser revisado regularmente para considerar mudanças e garantir recuperação eficaz em crises.

Termos e definições

Risco	Serviço	Disponibilidade	Desastre
Prática de gerenciamento de continuidade de serviço	Planos de recuperação de desastre	Análise de impacto no negócio	Garantia
	Avaliação de risco	Prática de gerenciamento de risco	

Ciclo PDCA

O **PDCA** é um modelo de processo de melhoria contínua composto de 4 passos:

P (*Plan*)

Planejar

Do (*Do*)

Fazer

C (*Check*)

Checar/verificar

C (*Check*)

Agir

Ciclo PDCA

PDCA pode ser aplicado ao PCN:

1. **1 - Mapeamento de negócios**
2. **2 - Análise de impacto de negócios**
3. **3 - Definições de melhores estratégias**
4. **4 - Documentação de planos**
5. **5 - Testes e simulações**

Ciclo PDCA

O PCN pode precisar de ajustes. Alguns dos motivos para que isso ocorra são:

- A avaliação e o teste das estratégias podem revelar sua ineficácia ou ineficiência.
- Pode haver deficiências nas estratégias.
- Algumas funções e responsabilidades são vagas e precisam de esclarecimentos.
- Mudança das funções e dos membros da equipe de continuidade de negócios.
- Introdução ou ocorrência de fatores ou de circunstâncias.

Política de Gestão de Continuidade de Negócios (PGCN)

A Política de Gestão de Continuidade de Negócios (PGCN) visa garantir resistência e gerenciar riscos.

Fortalece a confiança nos negócios e capacidade de gestão em cenários adversos.

Prepara a organização para ações previamente definidas na concretização de desastres.

Benefícios incluem identificação de impactos, redução de perdas financeiras e cumprimento de obrigações legais.

Política de Gestão de Continuidade de Negócios (PGCN)

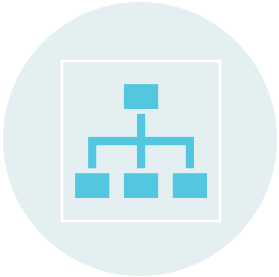
Os processos da biblioteca ITIL estão incluídos em cinco publicações separadas:

- Estratégia de serviço
- Design de serviço
- Transição de serviço
- Operação de serviço
- Melhoria contínua de serviço

Continuidade de Serviços de Tecnologia da Informação (GCSTI)

Objetivo do GCSTI é gerenciar riscos que afetam os serviços de TI.

Mantém a capacidade de recuperação de serviços de TI para atender necessidades de negócios.



Garante níveis mínimos de qualidade e utiliza Análise de Impacto nos Negócios e Gerenciamento de Riscos.

O plano de continuidade de serviços de TI faz parte do Plano Geral de Continuidade de Negócios.

Continuidade de Serviços de Tecnologia da Informação (GCSTI)

Benefícios

Em caso de acidente ou desastre, os serviços de Tecnologia da Informação e Comunicação (TIC) podem voltar a operar considerando sua ordem de importância.

- Apoio de reação mais rápido, auxiliando na recuperação de um acidente ou desastre.
- Atua na prevenção de acidentes, pois faz projeção de cenários de desastre com antecedência.

Continuidade de Serviços de Tecnologia da Informação (GCSTI)

Implementação

Para implementá-lo, a organização precisa aplicar algumas etapas:

Identificação dos serviços e dos ativos.

Identificação dos riscos e das ameaças.

Desenvolvimento de planos de contingência.

Documentação do plano de recuperação.

Continuidade de Serviços de Tecnologia da Informação (GCSTI)

Desafios

Desafios incluem criar planos de gerenciamento de continuidade de serviços de TI quando não há processos ou planos gerais de continuidade de negócios.

Alinhamento entre TI e área de negócios é crucial para o sucesso.

É fundamental o comprometimento da área de negócios em fornecer informações sobre os planos e estratégias futuras.

GCSTI fornece consultoria, assistência e mantém planos para apoiar a continuidade de negócios e minimizar incertezas em desastres.