academy

Introdução

Sobre o **Curso Oficial**

Sobre a **Formação**

Sobre a **Ementa Geral**

- ✓ Informação e segurança;
- ✓ Ameaças e riscos;
- ✓ Controles de segurança;
- ✓ Legislação, regulamentos e normas.

- **O EXIN ISFS atestará que você entende os princípios e conceitos de segurança da informação aplicados no ambiente de trabalho e saberá como mitigar riscos.**

Sobre o **Exame**

Examination type:	Multiple-choice questions
Number of questions:	40
Pass mark:	65% (26/40 questions)
Open book:	No
Notes:	No
Electronic equipment/aides permitted:	No
Exam duration:	60 minutes

Alteração No **Nome Da Norma**

- **A frase “código de prática” foi retirada do título do padrão ISO 27002**

De:

Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação

Para:

Segurança da Informação, Segurança Cibernética e Proteção à Privacidade — Controles de Segurança da Informação

Tamanho da **Norma**

- **Significativamente maior;**

De:

88 páginas

Para:

164 páginas

- **Os controles foram reordenados e atualizados;**
- **Alguns controles foram mesclados ou removidos;**
- **E alguns foram adicionados.**

Temas dos Controles

- **A ISO 27001/2:2022 lista 93 controles em vez dos 114 da ISO 27001/2:2013**

Esses controles são agrupados em 4 'temas' em vez de 14 cláusulas:

- ✓ Humanos (8 controles)
- ✓ Organizacionais (37 controles)
- ✓ Tecnológicos (34 controles)
- ✓ Físicos (14 controles)

Novos **Atributos de Controles**

- **Para facilitar a categorização:**
  - ✓ Tipo de controle (preventivo, detectivo, corretivo);
  - ✓ Propriedades de segurança da informação (confidencialidade, integridade, disponibilidade);
  - ✓ Conceitos de segurança cibernética (identificar, proteger, detectar, responder, recuperar);
  - ✓ Capacidades operacionais (governança, gestão de ativos, segurança física, continuidade etc.);
  - ✓ Domínios de segurança (governança e ecossistema, proteção, defesa, resiliência).

Exemplos dos Novos **Atributos de Controles**

Por controle

7.6 Working in secure areas				
Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security	#Protection

Matriz

Table A.1 – Matrix of controls and atribute values						
ISO/IEC 27001 control identifier	Control name	Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
5.1	Policies for information security	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Resilience
5.2	Information security roles and responsibilities	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem #Protection #Resilience
5.3	Segregation of duties	#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Governance #Identity_and_acess_management	#Governance_and_Ecosystem
5.4	Management responsibilitities	#Preventive	#Confidentiality #Integrity #Availability	#Identify	#Governance	#Governance_and_Ecosystem
5.5	Contact with authorities	#Preventive #Corrective	#Confidentiality #Integrity #Availability	#Identify #Protect #Respond #Recover	#Governance	#Defence #Resilience

Norma Significa **Qualidade?**

- **O que é Qualidade?**
  - ✓ "Conformidade com requisitos" - P.B. (Phil) Crosby (1926-2001);
  - ✓ "Aptidão para uso" - Joseph Juran (1904-2008);
  - ✓ "Totalidade das características de uma entidade que afetam sua capacidade de satisfazer necessidades declaradas e implícitas" - ISO 9001:2015;
  - ✓ Modelos de qualidade para negócios, incluindo o Prêmio Deming, o modelo de excelência EFQM e o Prêmio Baldrige.
- **Qual Objetivo de uma Norma?**
  - ✓ Evitar confusão

Normas **Relacionadas**

- **Ainda sobre Segurança da Informação:**
  - ✓ Família: ISO/IEC 27000 (mais de 50);
  - ✓ Cibersegurança: ISO/IEC 27103 (equivalente ao Framework NIST);
  - ✓ Computação em nuvem: ISO/IEC 27017;
  - ✓ Gestão de risco: ISO/IEC 31000;
  - ✓ Continuidade de negócios: ISO/IEC 27031 e ISO/IEC 27301.

Importância da **ISO/IEC 27001:2022**

- **Ei, você futuro Gestor de SI, veja a abrangência:**

✓ Compreender os requisitos de SI e estabelecer políticas;

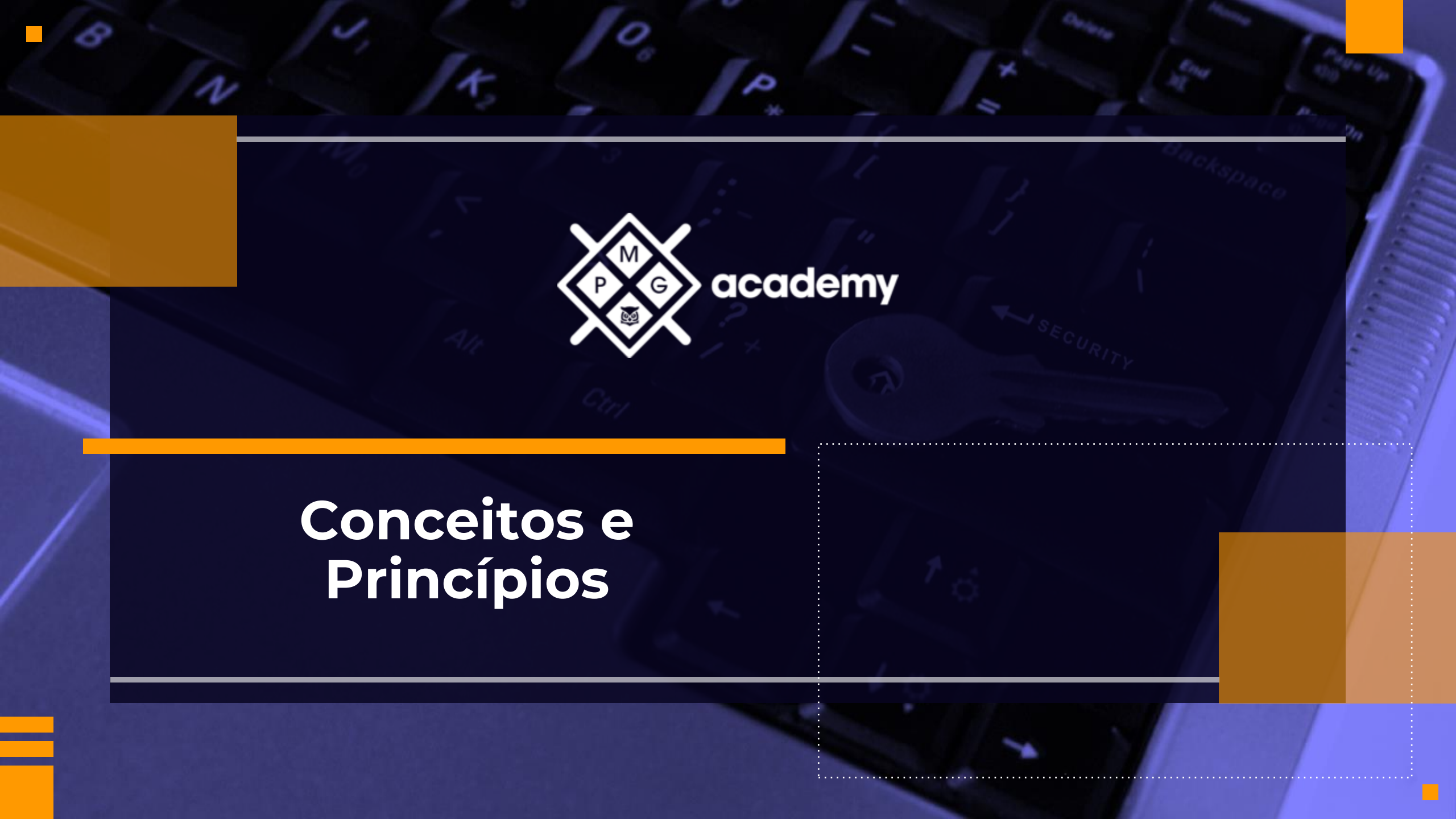
✓ Implementar e operar controles para gerenciar os riscos;

✓ Monitorar e revisar o desempenho SGSI;

✓ Melhoria contínua com base nas medições.

OBRIGADO

Introdução



Conceitos e Princípios

Como a Segurança **É Gerenciada**

Vulnerabilidade → **Ameaça** → **Exposição** → **Risco**

1 - O que e do que estamos protegendo;

2 - Priorize ações: Custos envolvidos, ativos, etc;

3 - Implemente os controles.

Para qualquer tipo de empresa:

- Lucratividade;
- Vantagem competitiva;
- Conformidade;
- Imagem comercial.

Começando do Começo

Antes de iniciar uma estratégia de segurança, precisamos:

- Saber o que queremos proteger;
- Do que ou de quem queremos proteger;
- Para isso, vamos iniciar uma análise de risco.

Ao analisar os riscos:

- Identificamos os requisitos;
- Os custos;
- Nos guiará e determinará as ações.

A análise (ou avaliação de risco) deve:

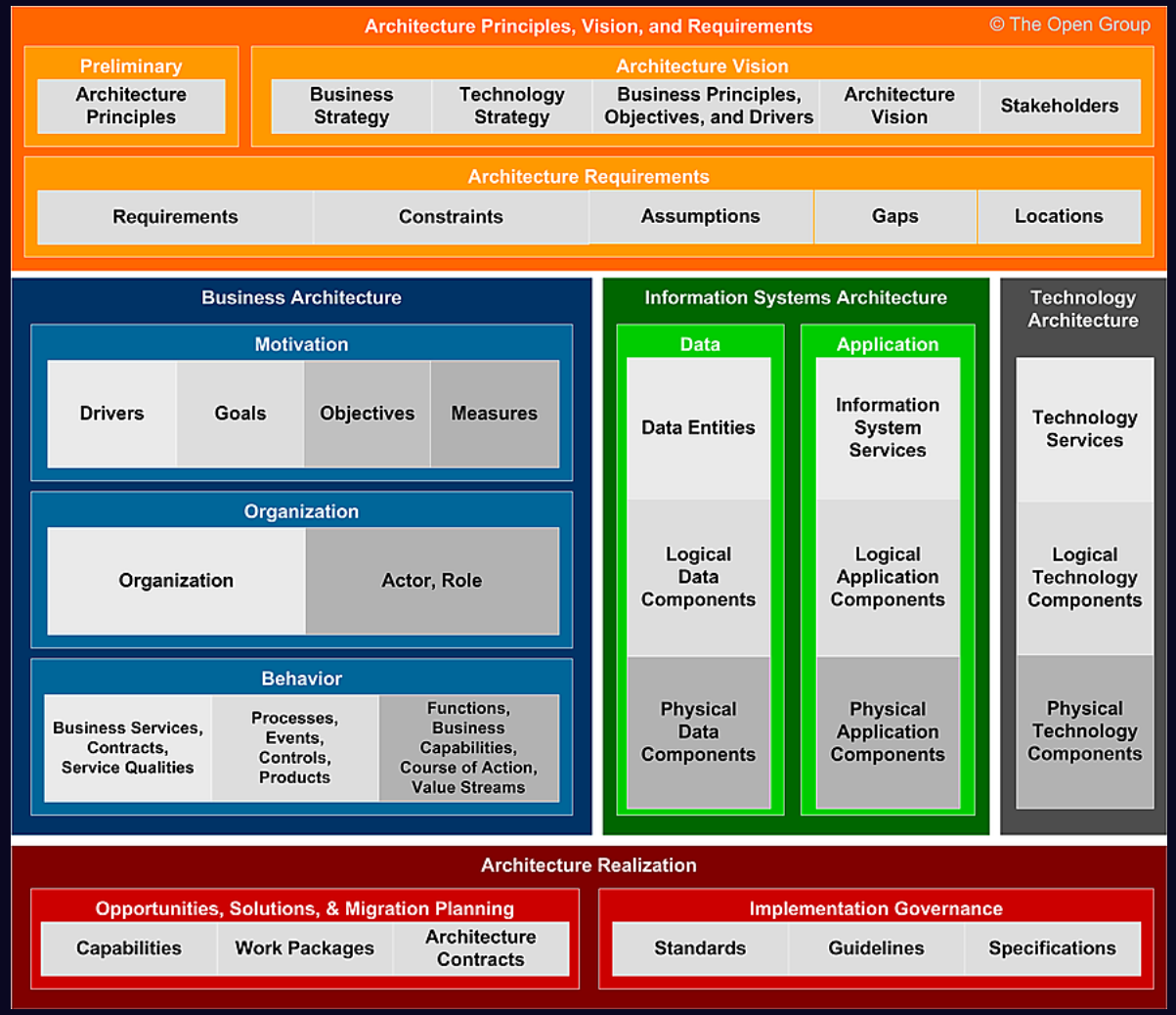
- Feita periodicamente;
- Lidar com as mudanças.

“A Segurança é alcançada por meio da aplicação de controles (contramedidas)”

Arquitetura da Informação

- É a arte de expressar um modelo ou conceito de informação;
- Expressados em atividades em sistemas complexos, como:
  - ✓ Sistemas de biblioteca;
  - ✓ Sistemas de gerenciamento de conteúdo;
  - ✓ Desenvolvimento web;
  - ✓ Interações com usuários;
  - ✓ Desenvolvimento de banco de dados;
  - ✓ Programação;
  - ✓ Redação técnica;
  - ✓ Projeto de softwares de sistemas críticos.
- As organizações reconhecem a importância ou correrão o risco de criar grandes conteúdos que ninguém nunca vai encontrar;
- O desafio é orientar as pessoas através da vasta quantidade de informações ofertadas a perceberam o seu valor.

TOGAF


Architecture Principles, Vision, and Requirements
© The Open Group
Preliminary
Architecture Principles
Architecture Vision
Business Strategy
Technology Strategy
Business Principles, Objectives, and Drivers
Architecture Vision
Stakeholders
Architecture Requirements
Requirements
Constraints
Assumptions
Gaps
Locations
Business Architecture
Motivation
Drivers
Goals
Objectives
Measures
Organization
Organization
Actor, Role
Behavior
Business Services, Contracts, Service Qualities
Processes, Events, Controls, Products
Functions, Business Capabilities, Course of Action, Value Streams
Information Systems Architecture
Data
Data Entities
Logical Data Components
Physical Data Components
Application
Information System Services
Logical Application Components
Physical Application Components
Technology Architecture
Technology Services
Logical Technology Components
Physical Technology Components
Architecture Realization
Opportunities, Solutions, & Migration Planning
Capabilities
Work Packages
Architecture Contracts
Implementation Governance
Standards
Guidelines
Specifications

Definições para Arquitetura da Informação

- A combinação de esquemas de organização, rotulagem e navegação dentro de um sistema de informação;
- O design estrutural de um espaço de informações para facilitar a conclusão de tarefas e acesso intuitivo ao conteúdo;
- A arte e ciência de estruturar e classificar sites e intranets para ajudar as pessoas a encontrar e gerenciar informações;
- É a “planta” que os desenvolvedores e designers usam para construir o sistema.

Visão Geral da Segurança da Informação

A segurança da informação é a disciplina que se concentra na qualidade (confiabilidade)

Baseado na tríade de requisitos

Disponibilidade;

Confidencialidade;

Integridade;

O truque para execução da SI é equilibrar estes aspectos:

- Os requisitos de qualidade que uma organização pode ter para a informação;
- Os riscos que estão associados a estes requisitos de qualidade;
- As controles necessárias para minimizar esses riscos.

Disponibilidade, Integridade e Confidencialidade

Propriedades da CIA:

- **Confidencialidade**: Informação que não é disponibilizada ou divulgada para pessoas, entidades ou processos não autorizados;
- **Disponibilidade**: Estar acessível e utilizável sob demanda por uma entidade autorizada;
- **Integridade**: Proteção da exatidão e a integridade dos ativos.

Confidencialidade, integridade e disponibilidade são princípios críticos de segurança!

- ✓ Devemos olhar para a CIA ao proteger o valor da informação;
- ✓ CIA são os requisitos de qualidade que a informação tem que satisfazer.
- ✓ A CIA garante que a informação é confiável.

Confidencialidade

- Também chamada de exclusividade;
- Diz respeito a quem pode obter que tipo de informação;
- Assegura que o nível necessário de sigilo seja aplicado;
- Impede a divulgação não autorizada;
- Prevalecer enquanto os dados residirem em sistemas, dispositivos na rede ou offline;
- Mantém enquanto as informações:
  - ✓ Forem transmitidas;
  - ✓ Até chegarem ao seu destino.
- Fornecida através:
  - ✓ Criptografia de dados no armazenamento e transmissão;
  - ✓ Controle de acesso;
  - ✓ Classificação dos dados;
  - ✓ Treinamento de pessoal nos procedimentos apropriados.

Ou seja, é o grau em que o acesso à informação é restrito a um grupo definido de pessoas autorizadas.

Visa proteger a Privacidade.

Exemplo De Medidas De Confidencialidade

- Controlar o acesso de um colaborador da área financeira ao histórico de conversas com clientes.
- Aplicar a política de mesa limpa para evitar que informações não caiam em mãos erradas, como documentos confidenciais que ficaram sobre a mesa na ausência do dono.
- Acesso a um usuário que não tem o direito de alterar as configurações de uma estação de trabalho.
- Segregação de funções para que um desenvolvedor de sistema não faça qualquer alteração nas informações de salários.
- Separação entre ambientes de desenvolvimento, teste, homologação e ambiente de produção.
- Segregação de rede, para que o departamento de RH tenha sua rede própria e que não seja acessível a outros departamentos.

- Controle de acesso aos computadores da rede com ID, biometria, senha, token, etc.
- Criptografar tráfego na rede para evitar a análise indevida do conteúdo transmitido.
- Usar o *traffic padding* com textos cifrados e confundir o atacante entre dados verdadeiros e preenchidos.

Integridade

- É o **grau** em que a informação está **atualizada** e sem **erros**;
- Se refere a ser correto e consistente com o estado ou a informação pretendida;
- É evitar modificação não autorizada de dados, deliberada ou acidental;
- É garantir que programas gravem as informações corretamente e não introduzam valores diferentes dos desejados;
- Significa que nada está faltando na informação, ela está completa. Significa que a informação é completa, perfeita e intacta (não necessariamente correta);
- A informação pode ser:
  - ✓Incorreta ou não autêntica, mas possuir integridade;
  - ✓Ou ser correta e autêntica, mas faltar integridade.
- A integridade é comprometida quando:
  - ✓Um atacante insere um vírus, uma *logic bomb* ou um *backdoor*;
  - ✓Um usuário insere ou modifica (maliciosamente ou não) os dados de um sistema.

Exemplo de Medidas de Integridade

- Um membro da equipe entra com um novo preço para um produto no site.
- Segregar função para o desenvolvimento de um novo produto que não pode ser realizada por apenas um pessoa.
- Assinatura digital (e/ou criptografia) que protegerá as informações contra alteração; e a confirmação da origem de um e-mail.
- Política de uso de termos para “cliente“, “consumidor” ou “usuário“ para evitar a inserção errada de cadastro em um banco de dados.
- Log das ações dos usuários de forma que possa ser determinado quem modificou uma informação.

Disponibilidade

- Disponibilidade é o grau em que a informação está disponível para o usuário e para o sistema de informação que está em operação no momento em que a organização a solicita.
- O que viola a disponibilidade:
  - ✓ Falta de acesso à informação provocada por uma falha de hardware;
  - ✓ Indisponibilidade devido ataques;
  - ✓ Atrasos que exceda o nível de serviço esperado para um sistema;
  - ✓ Um sistema que pode ser afetada pela falha de um software;
- Medidas:
  - ✓ Backup que devem ser utilizados para substituir rapidamente os sistemas críticos;
  - ✓ Funcionários qualificados e disponíveis para fazer os ajustes necessários para restaurar o sistema;
  - ✓ Lidar com questões ambientais como calor, frio, umidade, eletricidade estática e contaminantes;
  - ✓ Sistemas de detecção de intrusão (Intrusion Detection Systems – IDS) para evitar ataques de negação de serviço ou Denial-of-Service (DoS);
  - ✓ Liberar apenas os serviços e portas necessárias;
  - ✓ Monitorar o tráfego da rede e a atividade dos equipamentos;
  - ✓ Configurações adequadas de roteadores e firewalls.

Características da Disponibilidade

01

Oportunidade (Pontualidade)

Os sistemas de informação estão disponíveis quando necessários;

Continuidade

O pessoal pode continuar a trabalhar no caso de um fracasso ou indisponibilidade;

02

03

Robustez

Não há capacidade suficiente para permitir que todos os funcionários trabalhem nos sistemas de informação.

Exemplo de Medidas de Disponibilidade

- Gestão e o armazenamento de dados para evitar perder informações;
- Um dado que é armazenado em um disco de rede, e não no disco rígido do PC;
- Os procedimentos de backup são estabelecidos;
- Atender os requisitos legais de quanto tempo os dados devem ser armazenados.
- A localização do backup deve ser separada fisicamente do negócio.
- Criar procedimentos de emergência para garantir que as atividades possam ser recuperadas o mais breve possível após uma interrupção de grande escala.

Responsabilidade **E Auditabilidade**

Tudo começou com o SOX:

- Demonstra que a Governança está em ordem;
- Afeta como lidamos com o triângulo CIA.

Responsabilidade diz respeito a:

- Responsabilização;
- Culpabilidade;
- Prestação de contas.

Auditabilidade diz respeito a:

- Ao acesso ao tipo de informação para uma auditoria;
- Registros bem organizados, completos;
- Em conformidade com os padrões contábeis.

A auditoria envolve:

- Avaliação de controles de qualidade;
- Gerenciamento de riscos:
  - Sem acesso, os auditores emitem uma opinião qualificada sobre as finanças da empresa.

NIST **além da CIA**

Instituto Nacional de Padrões e Tecnologia dos Estados Unidos (NIST):

- Em 2013: Framework de Segurança Cibernética (CSF) ;
- Em 2018: Descrito na ISO/IEC TS 27103 (limitado).

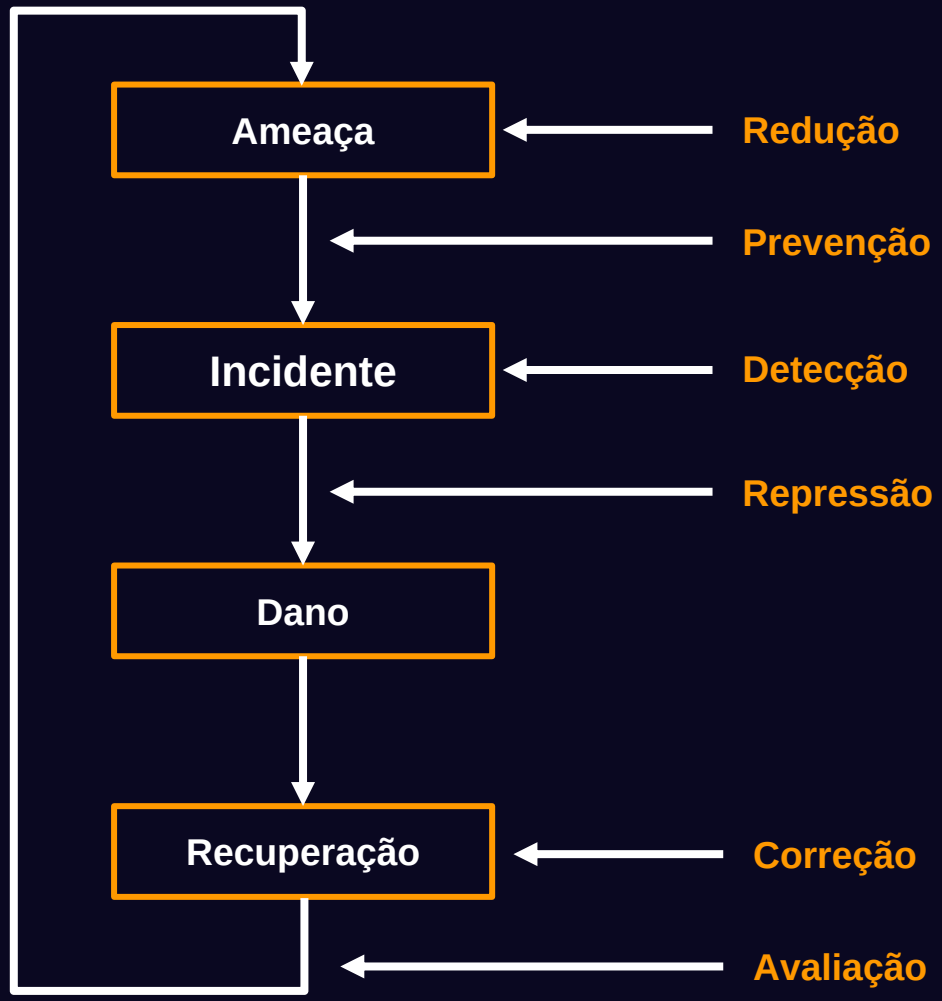
Aborda com base nos seguintes princípios:

- Identificar (mapear e analisar riscos);
- Proteger (tomar medidas de proteção);
- Detectar (medidas de reconhecimento de incidentes);
- Responder (estabelecer procedimentos);
- Recuperar (se algo der errado).

7.6 Working in secure areas				
Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security	#Protection

Medidas no **Ciclo de Vida do Incidente**

As medidas de segurança são focadas em um ponto específico do ciclo de incidente:



Atributos De **Controle**

Tipos de Controles

- Preventivas
- Detectivas
- Corretivas

Domínios de Segurança

- Governança e Ecossistema
- Proteção
- Defesa
- Resiliência

7.6 Working in secure areas				
Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security	#Protection

Atributos De **Controle**

Capacidades Operacionais

- Governança
- Gestão de ativos da empresa
- Proteção da informação
- Segurança pessoal
- Segurança física
- Segurança de sistema e rede
- Segurança de aplicativos
- Configuração segura
- Gerenciamento de identidade e acesso
- Gerenciamento de ameaças e vulnerabilidades
- Continuidade
- Segurança nos relacionamentos com fornecedores
- Legal e conformidade
- Gerenciamento de eventos de segurança da informação
- Garantia de segurança da informação

7.6 Working in secure areas

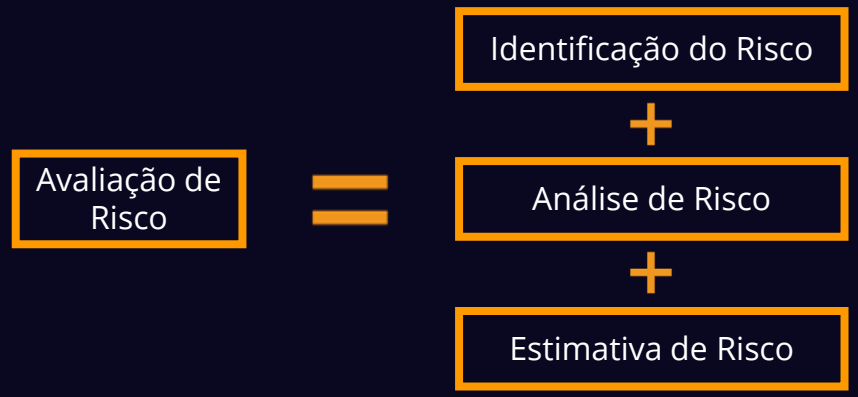
Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive	#Confidentiality #Integrity #Availability	#Protect	#Physical_security	#Protection

OBRIGADO

Conceitos e Princípios

Gerenciamento de Riscos

Matemática da Avaliação de Riscos



- Avaliação de Risco deve incluir:
  - ✓ Uma abordagem sistemática para estimar a magnitude dos Riscos (Análise de Risco);
  - ✓ Processo de comparar os riscos estimados em relação aos critérios de risco para determinar a significância dos Riscos (Estimativa de Risco).

Avaliação de Riscos

Identificação do risco

- É o processo de encontrar, reconhecer e descrever riscos;
- Envolve a identificação das suas fontes, eventos, causas e suas potenciais consequências;
- Pode envolver também os dados históricos, análise teórica, opiniões, pareceres fundamentados e de especialistas, e necessidades das partes interessadas.

Análise de riscos

- Um processo para compreender a natureza do risco;
- Tem a finalidade de determinar o nível de risco;
- Proporciona a base para a estimativa do risco;
- Base para as decisões sobre o tratamento do Risco;
- A análise de riscos inclui a estimativa do risco.

Estimativa do risco

- Atribuição de valores à probabilidade e consequências de um risco (quantitativa ou qualitativa);
- Atribuição de valores ao impacto que um risco pode ter e a probabilidade de sua ocorrência.

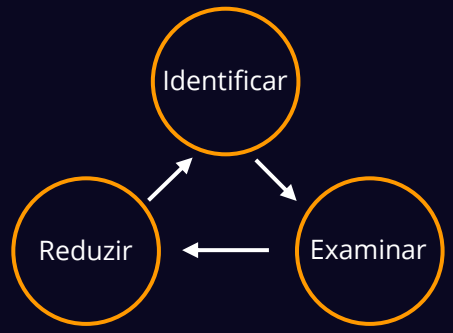
Gerenciamento de Riscos

Análise de Riscos: Ajuda saber contra o que nos proteger e identificar os riscos

Quando uma ameaça surge, inicia o processo de análise de RISCO
Ex: Novo vírus começa a circular e uma tempestade começa a se formar.

Quando uma ameaça se manifesta: torna-se um INCIDENTE
Ex: Hacker invadiu e houve uma falha de energia.

Processo Contínuo:



A tarefa de monitorar esse processo é conduzida por um especialista em segurança da informação, tal como um (Information Security Officer – ISO) ou Diretor (CISO).

Risco

- Efeito da incerteza sobre os objetivos;
- É a probabilidade de um evento (ameaça) se concretizar;
- Combinação da probabilidade de um evento e sua consequência:
  - ✓ Um efeito é um desvio do que é esperado;
  - ✓ Pode ser positivo e/ou negativo.
- Os objetivos podem ter diferentes aspectos, como:
  - ✓ Financeiro;
  - ✓ Saúde e segurança;
  - ✓ Segurança da informação;
  - ✓ Metas ambientais.
- Podem ser aplicados em diferentes níveis:
  - ✓ Estratégico;
  - ✓ Em toda a organização;
  - ✓ Projeto;
  - ✓ Produto;
  - ✓ Processo.

Exemplos de Riscos

- Firewall com portas abertas;
- Usuários sem treinamento nos processos e procedimentos;
- Ataque ao site;
- Engenharia social com os funcionários da TI;
- Vulnerabilidade no SO do servidor;
- Um incêndio ou enchente;
- Um funcionário que não trabalha no RH obtendo acesso a informações sensíveis ou privadas;
- Sua empresa é atingida por uma falha de energia;
- Um hacker consegue obter acesso à rede wireless de TI da empresa;
- Vazamento de informação confidencial de uma equipe de call center;
- Manter a porta do Datacenter aberta;
- Falta de atualização de software aplicativos;
- Equipamento emprestado para um parente de funcionário.

Ameaça

“A causa potencial de um incidente indesejado que pode resultar em danos a um sistema ou à organização.”

- Se algo resultar em dano, chamaremos de ameaça;
- Se o que temos é vulnerável, falho ou deficitário, abriremos brecha para o ataque;
- Aquele que aproveita a vulnerabilidade, é conhecido como agente de ameaça (ou agente ameaçador);

Um agente ameaçador pode ser:

- ✓ Um ladrão roubando seu patrimônio;
- ✓ Um invasor acessando a rede através de uma porta do firewall;
- ✓ Alguém acessando indevidamente os dados de terceiros;
- ✓ Um funcionário violando uma política de segurança;
- ✓ Ameaça de terrorismo e guerra a uma nação;
- ✓ Um tornado destruindo uma instalação;
- ✓ Um funcionário cometendo um erro não intencional expondo informações confidenciais.

No processo de Segurança da Informação:

- Ameaças (efeitos indesejáveis) são mapeadas na medida do possível;
- Verifica-se se algo pode ser feito para evitar essas ameaças;
- Determina-se quais medidas de segurança devem ser tomadas para evitar essas ameaças.

Vulnerabilidade

Vulnerabilidade: Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

- ✓ Uma vulnerabilidade é uma fraqueza;
- ✓ É a ausência ou a fraqueza de uma proteção que pode ser explorada.

Exemplo:

- ✓ Uma porta ou janela que não tranca direito;
- ✓ Um servidor de desenvolvimento rodando sem atualização;
- ✓ Aplicações ou sistemas operacionais desatualizados;
- ✓ Acesso irrestrito para um modem;
- ✓ Uma porta aberta no firewall;
- ✓ Uma segurança física fraca que permita a qualquer pessoa entrar no Datacenter;
- ✓ Controle de senha fraco que permite o fácil acesso à sistemas e ambientes.

DOWNLOAD

Exposição

- Exposição é ficar exposto às perdas;
- Um agente ameaçador aproveita essa exposição;
- Uma vulnerabilidade expõe uma organização a possíveis ameaças;

Exemplo:

- ✓ Portas abertas no firewall;
- ✓ Protocolos habilitados sem necessidade, facilitando um Sniffer capturar o tráfego em tempo real;
- ✓ Se a gestão de senhas for fraca e as regras não forem aplicadas, a empresa fica exposta;
- ✓ Se uma empresa não tem seu cabeamento inspecionado e não estabelece medidas proativas de prevenção contra incêndios.

Relação entre **Ameaça e Risco**

Medidas de Segurança

- Medida de segurança é colocada em prática para mitigar o risco em potencial;
- Significa: Controle, contramedida ou salvaguarda;
- Podendo ser:
  - ✓ Uma configuração de software;
  - ✓ Um dispositivo de hardware;
  - ✓ Um procedimento que elimine a vulnerabilidade;
  - ✓ Procedimento que reduza a probabilidade de um agente ameaçador ser capaz de explorar a vulnerabilidade.
- Exemplos de contramedidas incluem:
  - ✓ A gestão de senhas fortes;
  - ✓ Um guarda de segurança;
  - ✓ Mecanismos de controle de acesso em sistemas operacionais;
  - ✓ Implementação de senhas do basic input/output system (BIOS);
  - ✓ Treinamento de conscientização sobre segurança;
  - ✓ Software antivírus atualizado.

Análise de Risco

Análise de Risco é:

- ✓ O processo que define e analisa os perigos;
- ✓ Que ajuda a adquirir uma visão/compreensão dos riscos que a organização está enfrentando e que precisa se proteger;
- ✓ Fornece a base para as decisões de como lidar com o risco;
- ✓ Vai incluir a estimativas de risco.
- ✓ Relatório de análise de riscos pode ser usado para alinhar os objetivos da tecnologia com os do negócio;
- ✓ Análise de riscos pode ser quantitativo ou qualitativo.

Nota: os riscos possuem “donos” que também devem estar envolvidos na análise e avaliação de riscos.

Objetivos e Propósito da **Análise de Riscos**

Objetivos

1. Identificar Ativos e seus Valores;
2. Determinar Vulnerabilidades e Ameaças;
3. Determinar o Risco das Ameaças se tornarem realidade e interromperem o Processo Operacional;
4. Estabelecer o equilíbrio entre os custos de um incidente e os custos de uma Medida de Segurança.

Tem o propósito de ser usado:

- ✓ Como ferramenta para Gerenciamento de Riscos;
- ✓ Como ferramenta para determinar quais ameaças são relevantes para os processos operacionais;
- ✓ Para identificar os riscos associados aos processos operacionais;
- ✓ Para garantir que as medidas de segurança sejam implantadas;
- ✓ Para evitar gastos desnecessários em medidas de segurança por falta de conhecimento de segurança;
- ✓ Para avaliar os custo envolvidos em cada medida de segurança;
- ✓ Para ajudar no equilíbrio correto das medidas de segurança.

Tipos de **Análises de Riscos**

Exemplos de casos:

- ✓ Uma corretora de seguros e os detalhes das apólices dos assegurados tornam-se públicos.
- ✓ Dados pessoais de testemunhas em um processo penal são divulgados.
- ✓ Um funcionário perdeu um pendrive e o seu conteúdo cai nas mãos da imprensa que automaticamente é feito a publicação do assunto.

Que tipo de análise poderíamos fazer com estes 3 exemplos?

- ✓ Qual o impacto?
- ✓ Qual a chance de acontecer?
- ✓ Qual a consequência?

Análise Quantitativa de Risco:

- ✓ Objetivo de calcular um Valor do Risco com base no nível do prejuízo financeiro e na probabilidade de que uma Ameaça possa se tornar um Incidente de Segurança da Informação;

Análise Qualitativa de Risco:

- ✓ Baseia-se em cenários e situações e as chances de uma Ameaça se tornar realidade são analisadas com base em intuições.

Tipo de Análise de Riscos: **Quantitativo**

- ✓ **Baseados no impacto;**
- ✓ **Baseado na perda financeira;**
- ✓ **Baseado na probabilidade da ameaça tornar-se um incidente.**

- Neste tipo de análise, consideremos o valor de cada elemento compostos pelo custo:
  - ✓ Das medidas de segurança;
  - ✓ Bem como os ativos, como edifícios, hardware, software, informações e impacto dos negócios.
- É fornecida uma imagem clara do risco financeiro total;
- As medidas adequadas podem então ser determinadas;
- Uma parte importante disso é determinar quais riscos residuais são aceitáveis;
- Os custos das medidas não devem exceder o valor do objeto protegido e do risco;
- Uma análise de riscos puramente quantitativa é praticamente impossível;
- Uma análise quantitativa de risco tenta atribuir valores a todos os aspectos, mas isso nem sempre é possível;

- Pode ser atribuído um valor a um servidor com defeito: por exemplo, o valor de compra e depreciação, o valor do software, salários etc. Agora tente dar um valor ao dano causado a uma empresa;
- Pode ser possível determinar em algumas ocasiões, mas nem sempre.

Tipo de Análise de Riscos: **Qualitativo**

✓ **Baseado nos cenários;**
✓ **Baseado nas situações;**
✓ **Baseado nos sentimentos.**

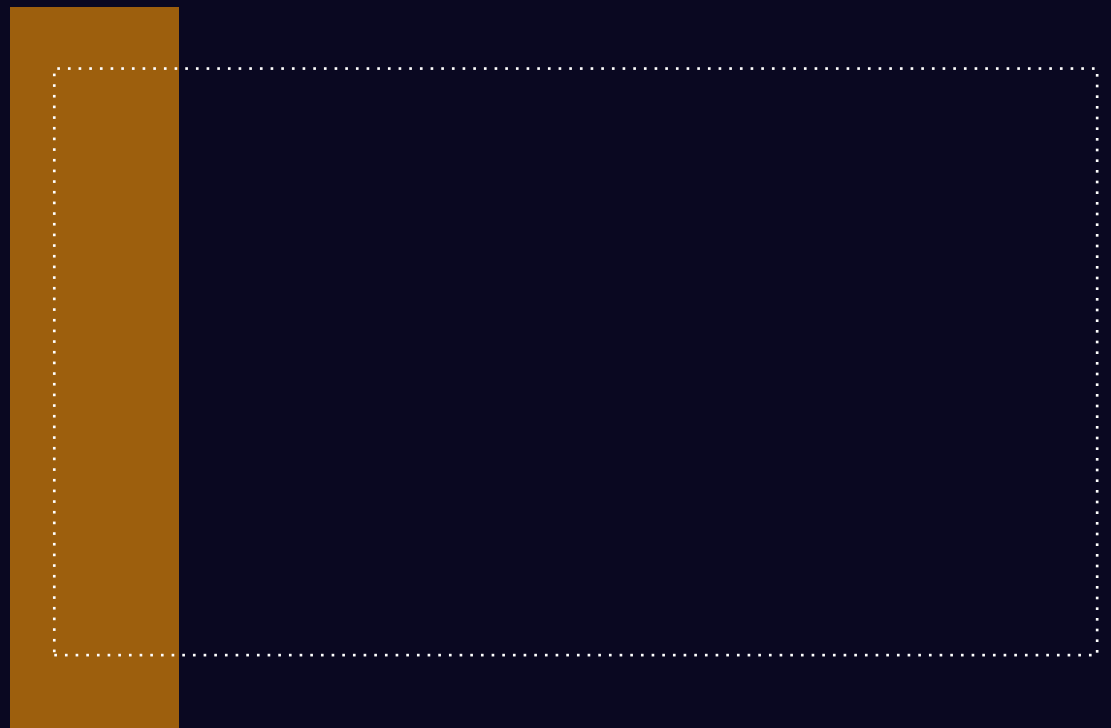
- Números e valores monetários não são atribuídos a componentes e perdas;
- Pode ser definido, por exemplo, como baixo, médio e alto, ou, provável, certo, possível, raro e improvável, etc.;
- Utilizam bom senso, melhores práticas, intuição e experiência;
- Exemplos de técnicas qualitativas são Delphi, brainstorming, esboços sequenciais (storyboarding), grupos de discussão, pesquisas, questionários, listas de verificação, reuniões entre duas pessoas e entrevistas;
- A equipe de análise de riscos considera a cultura da empresa e os indivíduos envolvidos na análise;
- É reunido pessoal com experiência e conhecimento das ameaças sob avaliação;
- A este grupo é apresentado um cenário que descreve as ameaças e as potenciais perdas, e cada membro então responde com sua intuição e experiência sobre a probabilidade da ameaça e a extensão do dano que pode resultar.

- As análises quantitativa e qualitativa do risco têm, cada uma, suas vantagens e desvantagens.
- A administração, em consulta com especialistas, determina qual método deve ser aplicado em cada situação particular.

Análise Combinada

Para evitar o ônus de uma avaliação abrangente de risco quantitativo:

- ✓ Inicia com uma avaliação qualitativa;
- ✓ Para os maiores riscos, realize:
  - ✓ Análise de custo-benefício;
- ✓ Como parte da análise quantitativa.

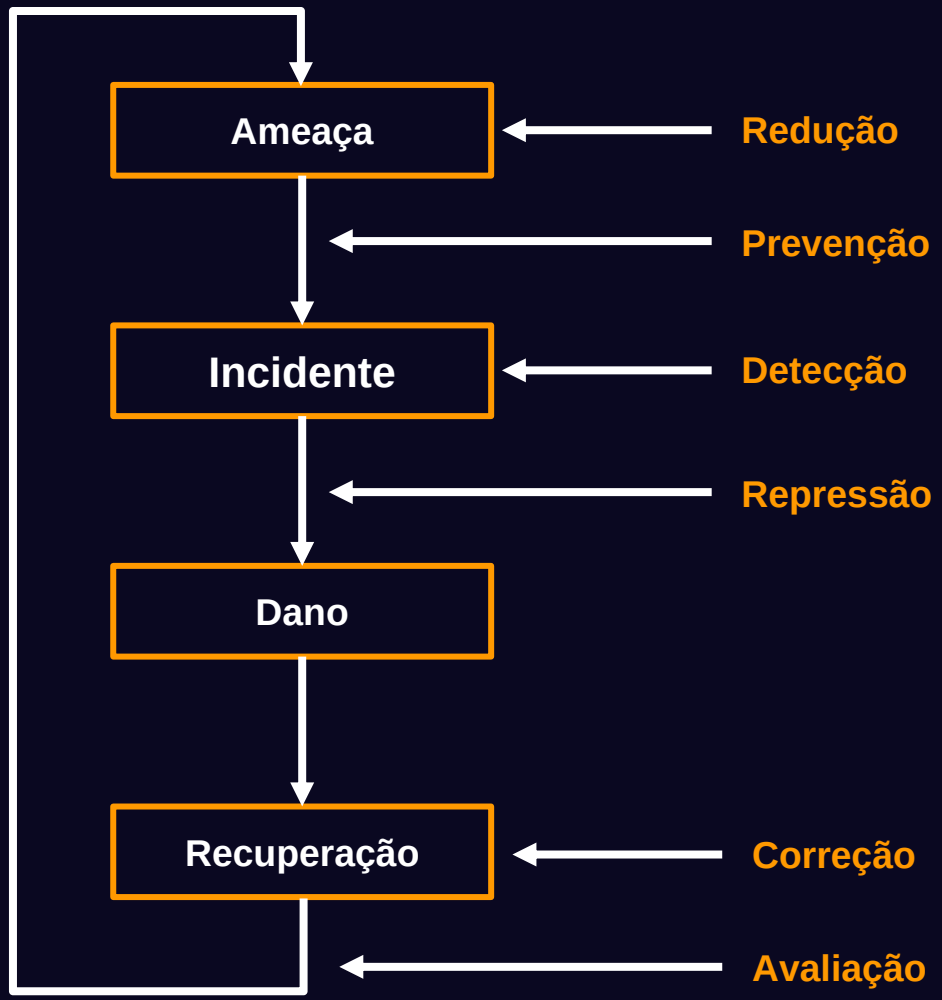


SLE, ALE, EF e ARO

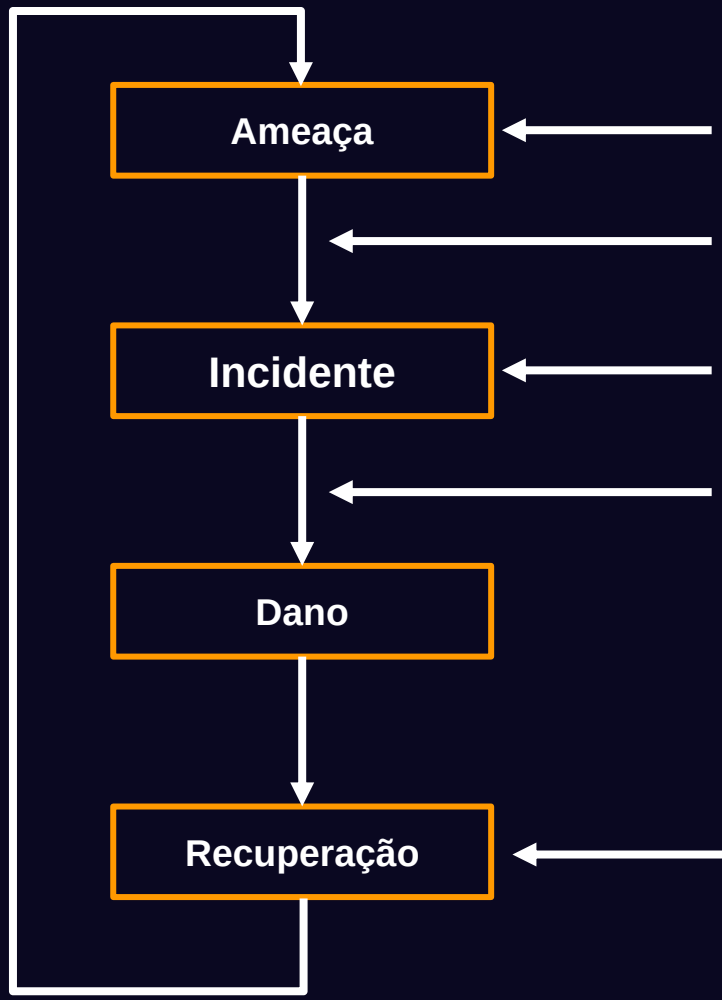
- Siglas:
  - ✓ SLE significa expectativa de perda única;
  - ✓ ALE significa expectativa de perda anualizada;
  - ✓ EF significa o valor de exposição;
  - ✓ ARO significa a taxa anual de ocorrência.

- Fórmulas
  - ✓ EF = % de perda em um ativo sob ameaça
  - ✓ SLE = Valor do Ativo x Fator de Exposição (EF)
  - ✓ ALE: SLE x ARO

Medidas no Ciclo de Vida do Incidente



Medidas para Reduzir Incidentes



Medidas reativas visam reduzir as ameaças

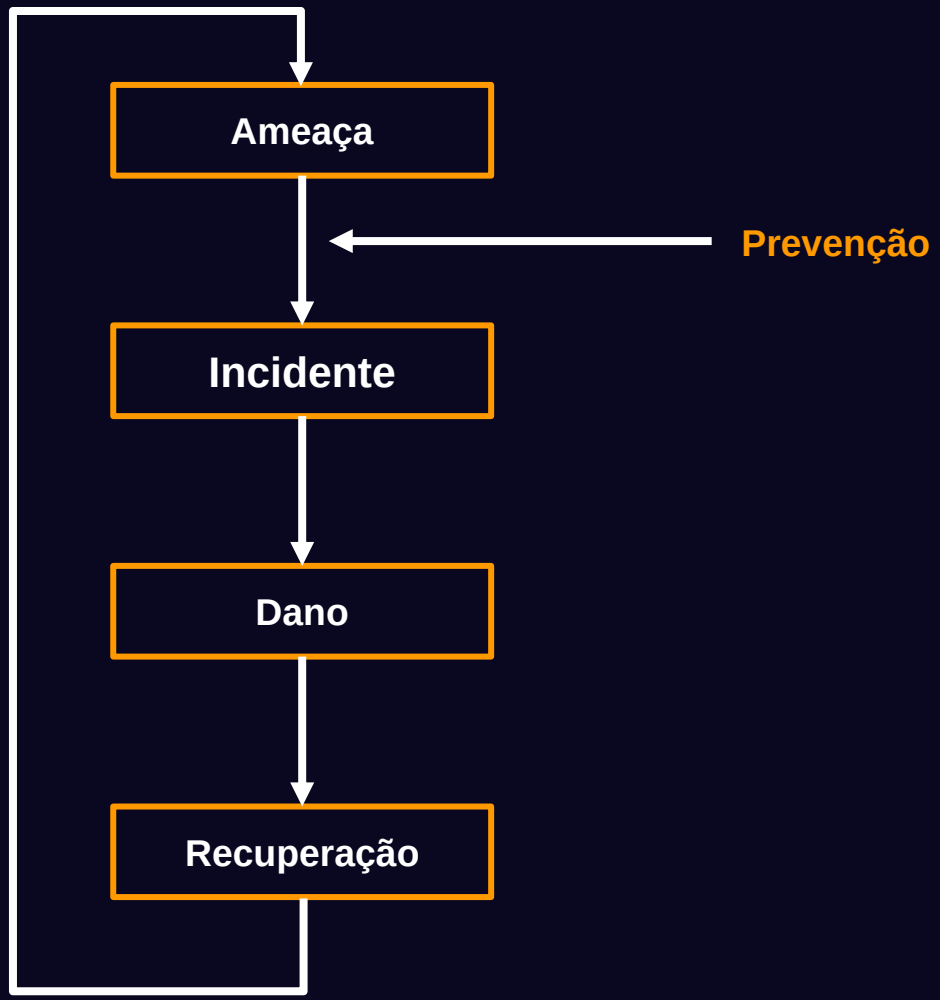
Medidas preventivas visam evitar incidentes

Medidas detectivas são projetadas para detectar incidentes

Medidas repressivas são projetadas para interromper as consequências de um incidente

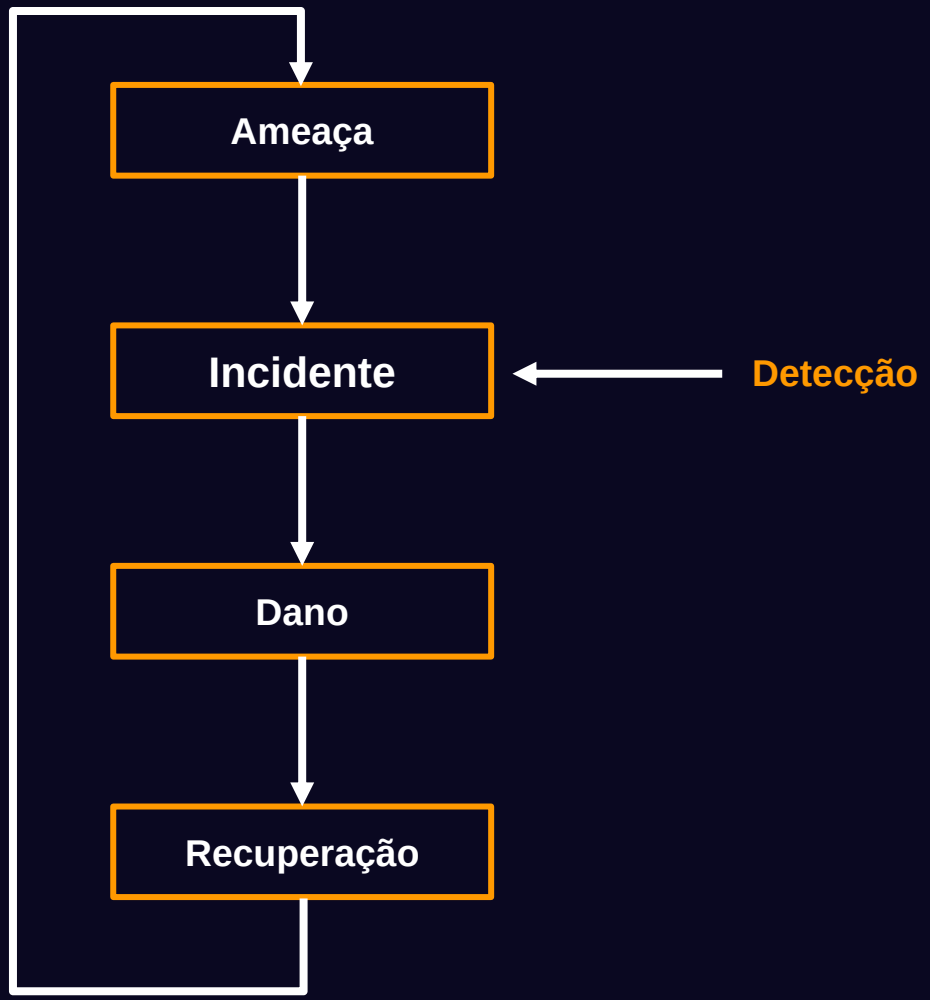
Medidas corretivas concentram-se em reparar os danos causados

Prevenção



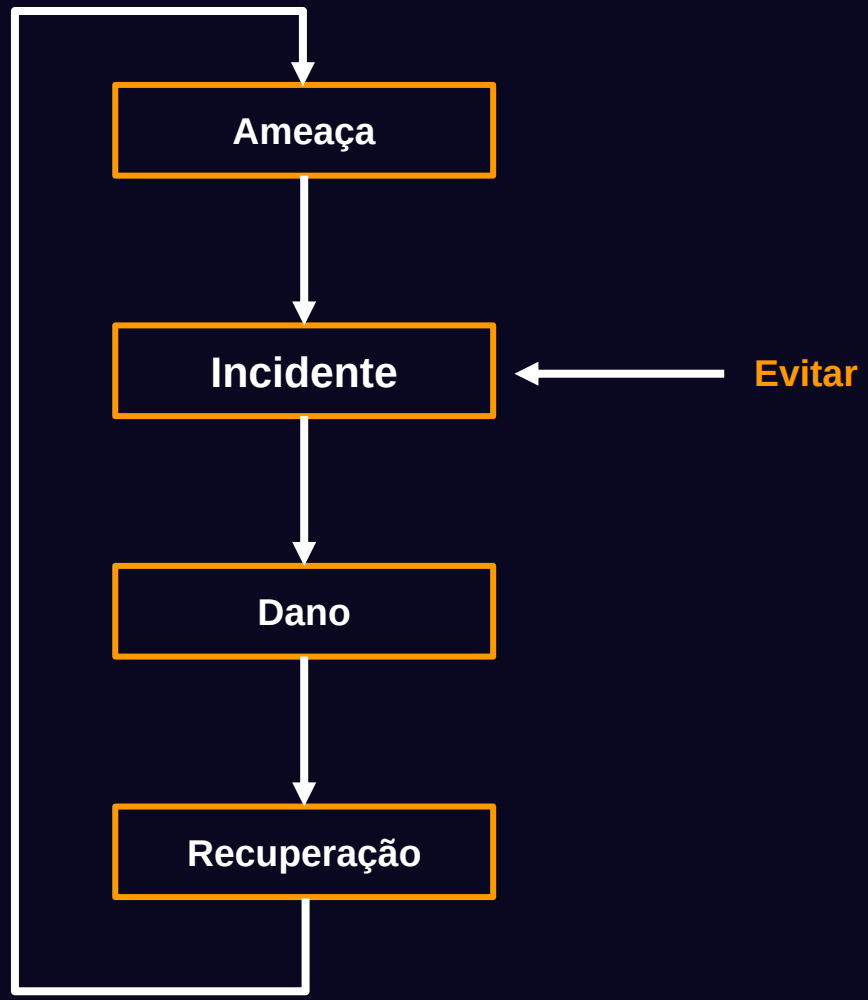
- ✓ A prevenção torna a ameaça impossível;
- ✓ Exemplo: Desconectar a Internet e bloquear portas;
- ✓ Pode ser impraticável;
- ✓ Mais prático: Colocar informações sensíveis em um cofre.

Detecção



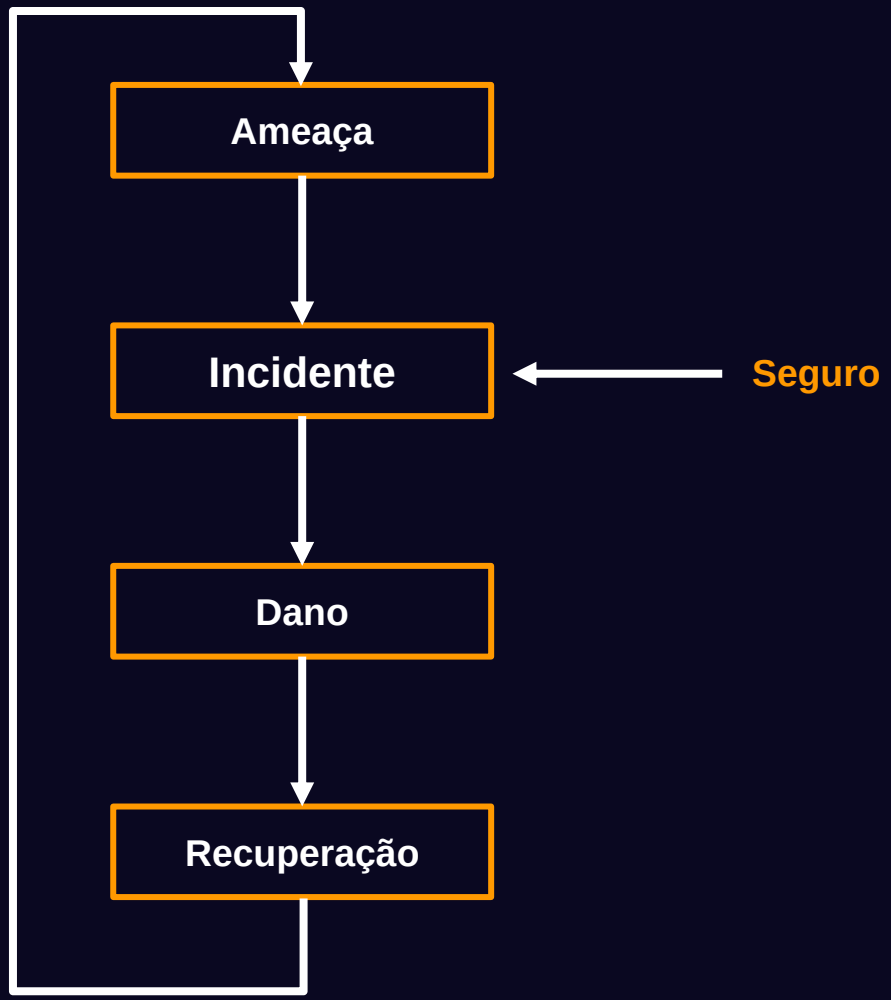
- ✓ Se os efeitos de um incidente não forem muito grandes;
- ✓ Se houver tempo para mitigar danos consequentes;
- ✓ Qualquer incidente seja detectado o mais rápido possível;
- ✓ Exemplo: vigilância por vídeo e com adesivos na janela;
- ✓ A notificação de que todo uso da Internet é registrado.

Evitar



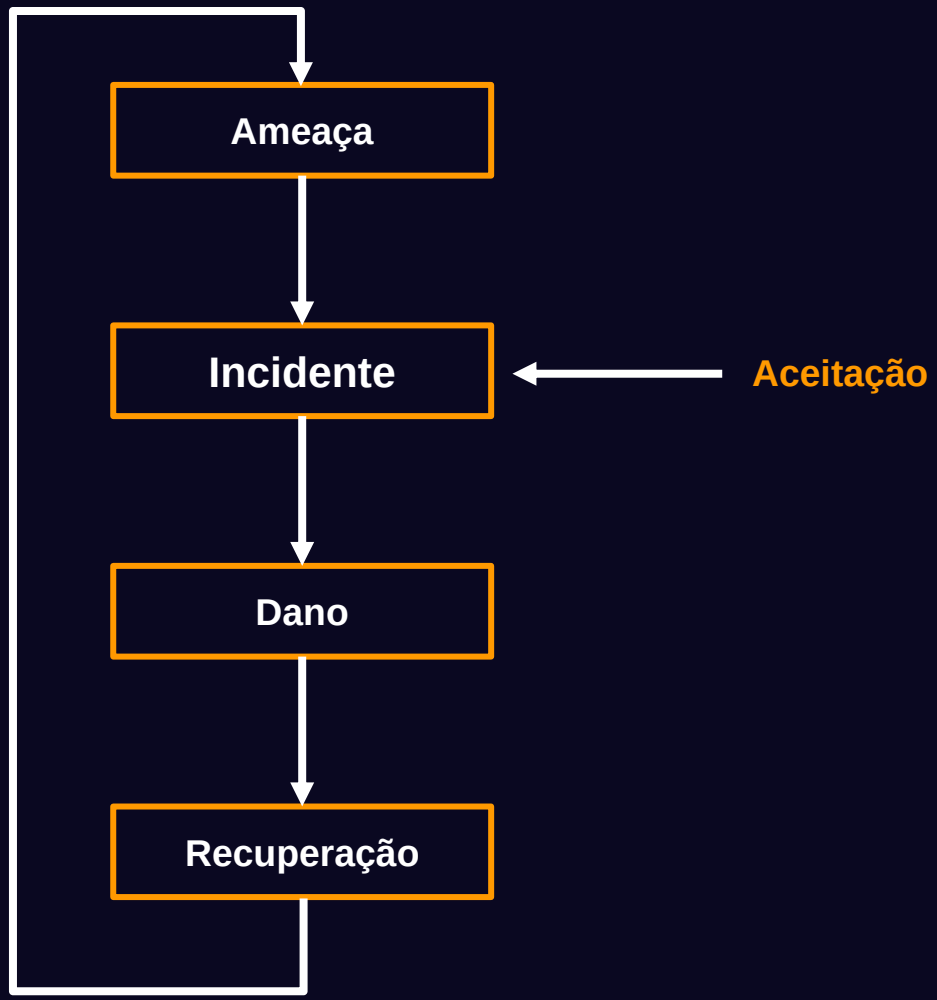
- ✓ Uma opção formal de risco;
- ✓ Significa que o risco é alto e não pode ser aceito, mitigado ou segurado (alta probabilidade e alto impacto).
- ✓ Significa que o processo de negócio deve ser abandonado, ou a atividade deve ser movida (fisicamente) para que o risco não seja mais aplicável.

Seguro



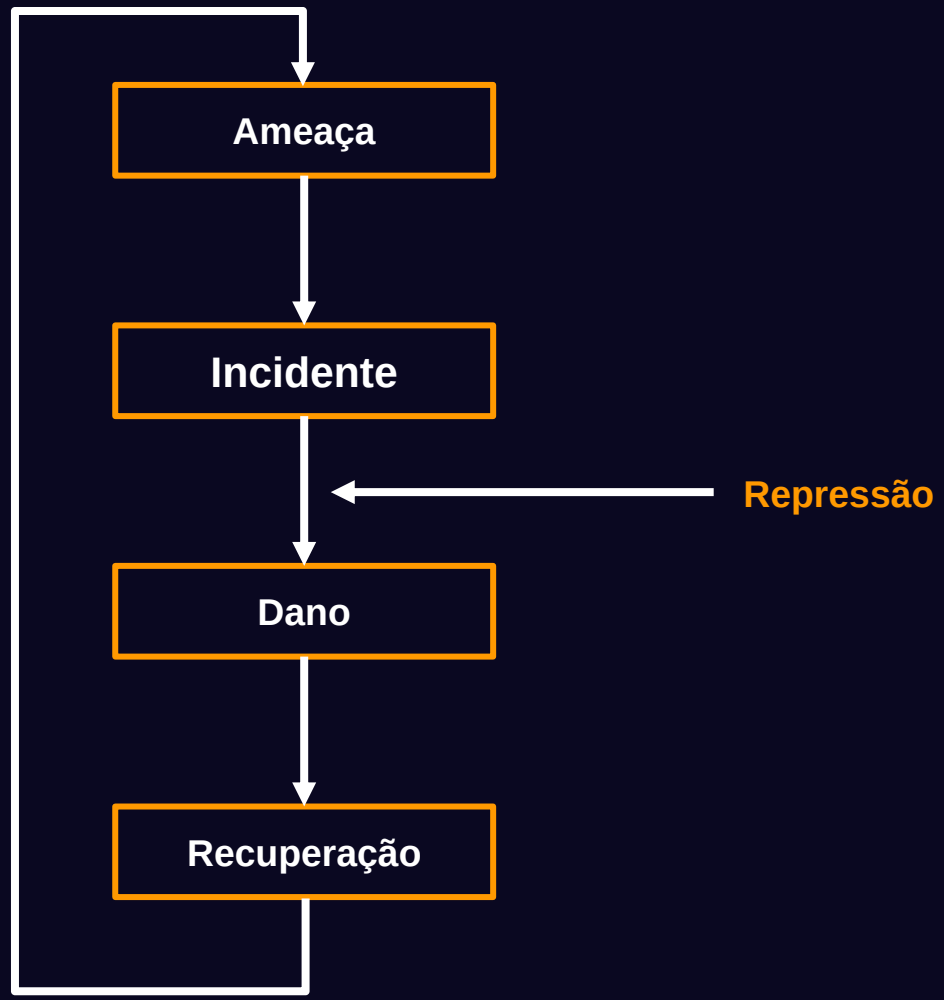
- ✓ Para eventos que não podem ser eliminados;
- ✓ Cujas consequências são inaceitáveis;
- ✓ Exemplo: Seguro contra incêndio e cópia diária de todos os dados importantes fora da organização;
- ✓ Nem sempre são baratas, mas geralmente justificadas.

Aceitação



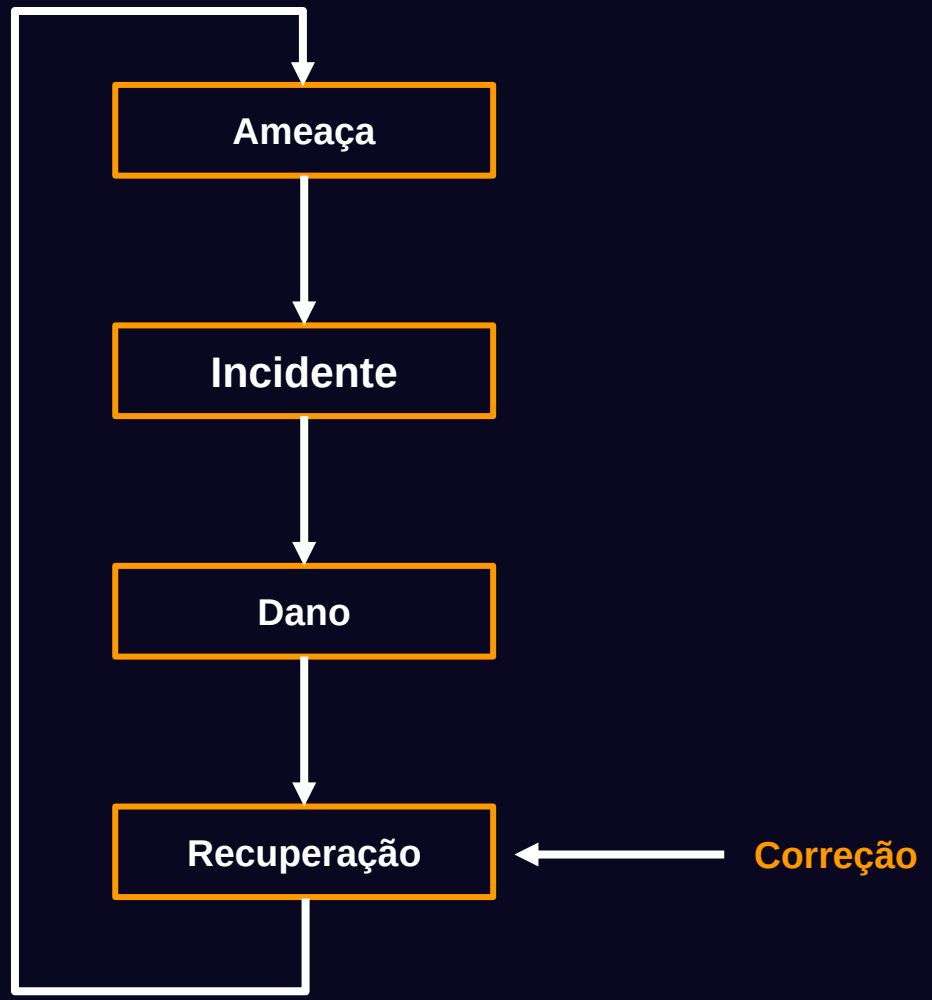
- ✓ Quando todas as medidas são conhecidas;
- ✓ Podemos decidir não implementar certas medidas;
- ✓ Quando o custo é desproporcional ao retorno;
- ✓ Ou não há medidas adequadas possíveis.

Repressão (Supressão)



- ✓ Limitar as consequências do incidente;
- ✓ Por exemplo, não adianta ter alarmes de incêndio se ninguém tomar a iniciativa de apagar um incêndio incipiente;
- ✓ Visam limitar ao máximo os danos causados;
- ✓ Fazer backup também é uma medida repressiva.

Correção



- ✓ Se um incidente ocorre, sempre há algo para ser reparado;
- ✓ Dependendo das medidas repressivas, os danos são limitados ou muito grandes.
- ✓ Exemplo: Funcionário criar acidentalmente um novo BD que sobrescreve o BD de produção.

Ameaças **Humanas**

Tipos:

Ameaça intencional:

- Existem ameaças com os próprios funcionários:
  - ✓ Destroem informações após demissão;
  - ✓ Se vingam da empresa, vendendo ativos para a concorrência por não terem recebido um aumento.

A engenharia social:

- Faz uso de pessoas;
- Induzindo-as ao fornecimento voluntário de informações sensíveis;
- O engenheiro social se aproveita das fraquezas das pessoas para realizar seus objetivos;

Ameaça não-intencional:

- Acidentalmente pressionar a tecla "delete“;
- Inserir um pen drive com um vírus em uma máquina e espalhar o vírus por toda a rede.

Ameaças **Não-Humanas**

- Ameaças não-humanas com influências externas, tais como:
  - ✓ Relâmpagos;
  - ✓ Incêndios;
  - ✓ Inundações;
  - ✓ Tempestades.
- Grande parte dos danos causados depende da localização do equipamento (por estarem vulneráveis):
  - ✓ Data Center localizado em local suscetível à vazamentos ou goteiras;
  - ✓ Localizado no subterrâneo, em uma área onde há água ou passível de inundação;
  - ✓ Salas que não têm janelas ou existem entradas e saídas de ar.
- Podemos subdividir as ameaças humanas e não-humanas em interrupções:
  - ✓ Na infraestrutura básica como equipamentos de informática, softwares ou banco de dados;
  - ✓ No ambiente físico, como edifícios, documentos físicos, instalações elétricas, abastecimento de água, aquecimento, ventilação e refrigeração.

Tipos de **Danos**

1 Direto

Exemplos:

- ✓ Roubo de um notebook;
- ✓ Incêndio;
- ✓ Site atacado por hackers.

2 Indireto

Exemplos:

- ✓ Tempo de recuperação dos dados;
- ✓ Água utilizada para apagar o fogo;
- ✓ Danos à imagem da empresa.

Tipos de Estratégia de **Riscos**

Assumir Riscos

- É aceitar o risco;
- Quando o custo excede o dano;
- Simplesmente decide-se não fazer nada;
- As medidas são normalmente repressivas.

Neutro em Relação a Riscos:

- Ações tomadas quando:
  - Até que as ameaças não se manifestem mais;
  - E se manifestar, os danos são minimizados.
- As medidas são normalmente preventivas, detectivas e repressivas.

Evitar Riscos:

- Ameaças sejam neutralizadas o máximo possível;
- A ameaça não leve a um incidente, exemplo:
  - Trocar um balde de ferro enferrujado por um de plástico;
  - Desativar um software antigo com problemas.

OBRIGADO

Gerenciamento de Riscos

academy

Contexto da Organização

Foco da Segurança da Informação

O objetivo geral da Segurança de TI é:

- ✓ "Segurança equilibrada com profundidade“;
- ✓ Implementar controles justificáveis;
- ✓ Assegurar que a Política de Segurança da Informação é aplicada;

? Normalmente, qual a melhor abordagem de uma segurança da informação?

Para muitas organizações, a abordagem é feita através de uma Política de Segurança da Informação (PSI).

? A PSI deve então ser o nosso foco?

Não! O processo de Gerenciamento da Segurança da Informação – GSI (SGSI) deve ser o ponto focal para todas as questões de Segurança de TI.

? Por que o SGSI? O que o SGSI garante?

Ela garante que uma PSI será criada, mantida e reforçada, cobrindo usos e abusos de todos os sistemas e serviços de TI.

A Organização da Segurança da Informação

- Sem uma Segurança da Informação aceita por todos, a empresa pode não sobreviver;
- Por isso a Alta Direção deve dar o exemplo;
- Apesar de todos estarem envolvidos, depende da natureza da empresa;
- Independente do porte, deve haver uma definição de responsabilidades dos envolvidos.

Contexto da Organização

Como funciona?

- ✓ Empresas tem Missão e Visão;
- ✓ A Segurança da Informação tem que estar alinhada aos objetivos;
- ✓ Proteção dos segredos comerciais;
- ✓ A continuidade faz parte da resiliência empresarial;
- ✓ Uma empresa nunca está “isolada”, dependem de outras partes.

? **Entenda as necessidades e expectativas das partes interessadas:**

Quem são e quais os seus requisitos?

Com essas informações, o gerente de segurança pode tomar decisões sobre a forma como a segurança da informação será estabelecida na organização.

Sistema de Gerenciamento de Segurança da Informação (SGSI)

- Qual utilizar?
  - ✓ ISO 27001.
- O que a organização deve fazer com um SGSI?
  - ✓ Estabelecer, implementar, manter e melhorar continuamente.
- O SGSI deve estar de acordo com quais requisitos?
  - ✓ Da ISO 27001, com suporte da 27002 e família 27000.
- Por quê estruturar um SGSI?
  - ✓ Ajuda a classificar tudo o que é importante em relação à SI.
- Como estruturar um SGSI?
  - ✓ Dividindo em domínios.

Domínios da ISO 27001

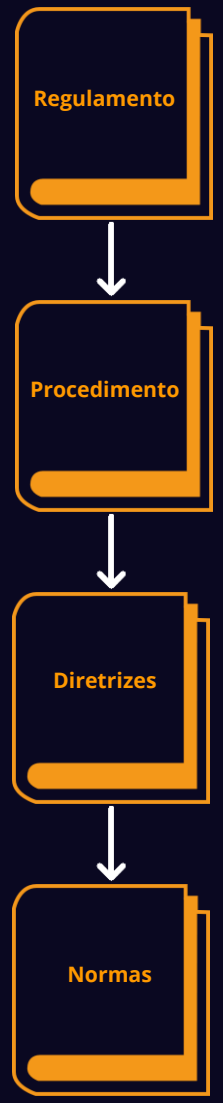
- Um “domínio” é um grupo de assuntos que estão logicamente conectados.

  ✓ 1. Medidas de controle organizacionais
  ✓ 2. Medidas de controle centradas no ser humano
  ✓ 3. Medidas de controle físico
  ✓ 4. Medidas de controle tecnológico

Política de Segurança da Informação

- Oferece suporte e direção;
- Elaborada com base (princípio orientador) nos processos de negócios;
- Deve ser aprovada pelo conselho administrativo e publicada a todos os interessados e envolvidos;
- As leis e regulamentos devem estar em conformidade com a PSI;
- Geralmente é distribuída uma versão resumida;
- Mantido a versão completa na Intranet, por exemplo;
- Ter uma Política é uma coisa, cumpri-la é outra;
- Manter uma campanha de conscientização.

Conteúdo Hierárquico de uma Política



Regulamento:

- Um regulamento é mais detalhado do que um documento de política.

Procedimento:

- Descreve a forma “como” certas medidas devem ser implementadas, e pode, às vezes, incluir instruções de trabalho.

Orientações (Manuais):

- Fornecer orientação:
  - ✓ Descreve quais aspectos precisam ser examinados através de aspectos de segurança específicos;
  - ✓ Não são obrigatórias, mas com natureza consultiva.

Normas:

- Descrevem as regras de como atingir os objetivos da organização.
- Por exemplo: Característica desejável de um software, visando a segurança, qualidade etc.

Avaliação da Política de Segurança da Informação

- O ciclo PDCA é uma forma de implementar uma PSI;
- A PSI contém além da política, os procedimentos e manuais;
- Juntos, esses documentos fazem parte importante do Sistema de Gerenciamento de Segurança da Informação (SGSI).

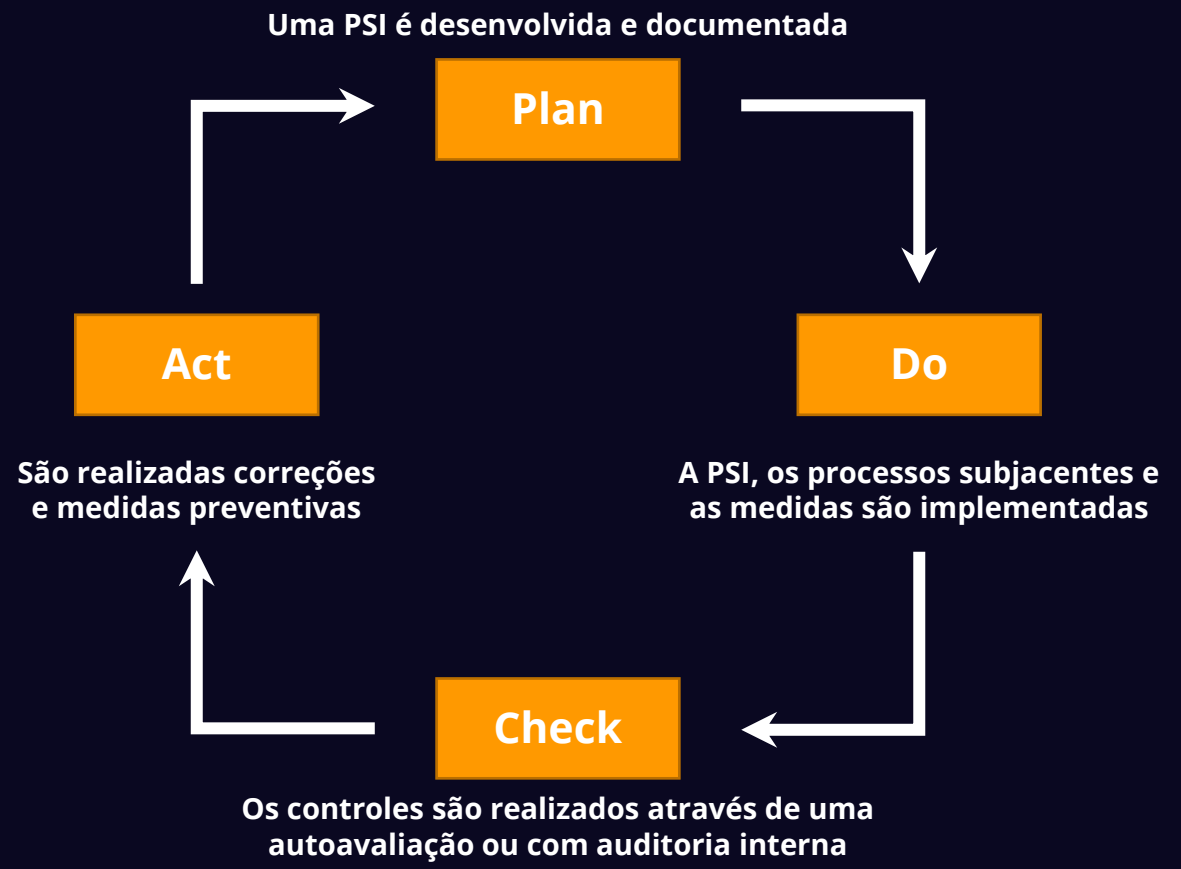
Modelo PDCA para o SGSI

- É a base para determinar, implementar, monitorar, controlar e manter o Sistema de Gestão de Segurança da Informação (SGSI);
- 27001:2022 deixa de obrigar este modelo, mas estabelece requisitos para o estabelecimento do SGSI;
- Muitas empresas possuem seu próprio ciclo de Planejamento e Controle.

PDCA para o SGSI

- Planejamento (projetar o SGSI):
- Execução (implementar o SGSI):
- Verificação (monitorar e verificar o SGSI):
- Ação (manter e ajustar o SGSI):

Ciclo do PDCA



Posse ou Controle

- Significa que existe uma informação e que ela deve estar sob a posse e controle de alguém;
- Lida com uma perda de controle ou posse de informações, mas não envolve a quebra de sigilo.

Exemplos:

- ✓ Um cartão de crédito que é roubado. O proprietário perde a posse e o controle, podendo o ladrão causar um dano.
- ✓ Um notebook com proteção de senha, biometria e criptografia que foi perdido. O dono perde o controle e a posse, mas não necessariamente a quebra de sigilo.

Autenticidade

- Busca verificar se a informação é autêntica, verdadeira;
- Autenticidade se refere à veracidade da alegação de origem ou a autoria das informações.

Por exemplo:

- ✓ Para verificar a autenticidade de um documento escrito à mão, compare com outro documento já escrito para validar a autoria;
- ✓ Uma assinatura digital pode ser usada para verificar a autoria de um documento digital usando criptografia de chave pública.

Utilidade

- Diz respeito ao proveito que se faz a um dado, informação ou sistema;
- Utilidade significa capacidade de uso.

Por exemplo:

- ✓ Perda da chave criptográfica de em um disco criptografado. Aquele que precisar acessar, não será útil, mesmo que os dados sejam confidenciais, controlados, íntegros, autênticos e disponíveis;
- ✓ Um dado armazenado no banco de dados que foi convertido de ASCII para UTF-8 e acabou ficando ilegível, ou seja, sem utilidade.

- Resolver um problema de utilidade pode levar muito tempo;
- A capacidade de uso, ou seja, utilidade é diferente do de disponibilidade!

Diligência e Cuidado Devido

Significado:

- ✓ Diligência X Negligência;
- ✓ Diligência devida é o grau de cuidado e cautela exigido pelas circunstâncias de uma pessoa;
- ✓ Se alguém usa o cuidado devido, então a parte prejudicada não pode provar negligência.

- A justiça responsabiliza parceiros pela falta de cuidado devido no caso de uma violação de segurança grave.
- Tanto violações de segurança quanto de privacidade.
- Diligência devida trata de entender as ameaças e riscos;
- Cuidado devido se preocupa em implementar controles;
- A empresa pode ser legalmente acusada de negligência.

Dados e Informação

- Dados podem ser processados pela TI, mas apenas se tornam informação após terem adquirido um certo significado;
- Informática é converter dados em informação;
- Informática é agregar dados que estão separados, gerando informação;
- Informação pode assumir a forma de texto, mas também da palavra falada e de imagens de vídeo.
- Uma informação é a compreensão das relações entre as partes dos dados.

Dados:	190477
Informações:	19/04/77 mm-dd-aa

Valor dos Dados e da Informação

Os dados podem ter grande importância, mesmo que não estejam no formato de 'informação’

- Tal importância da 'proteção de dados;
- O valor dos dados é determinado principalmente pelo usuário;
- O valor das informações é atribuído pelos donos.

Informação como um fator de produção:

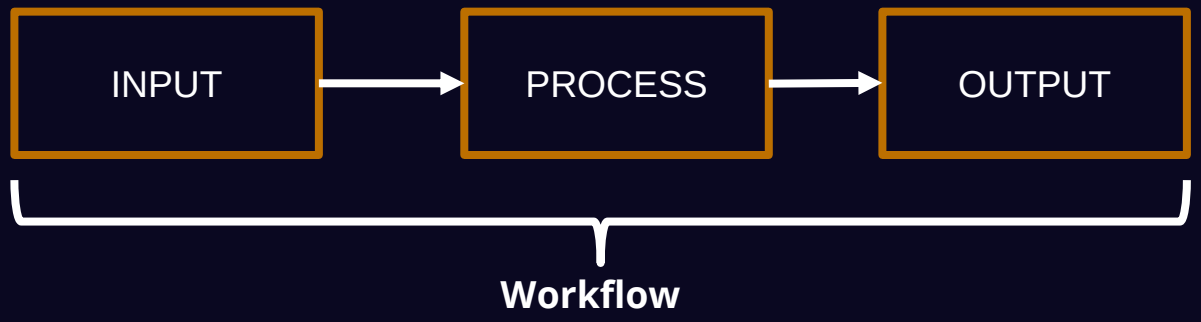
- Não são apenas o capital, a mão-de-obra e as matérias-primas;
- Os negócios não podem existir sem informação.

Análise da Informação

A análise da informação fornece uma imagem clara de como:

- Uma organização lida com informações;
- A informação “flui” na organização.

Baseado em um Fluxo:



Por exemplo:

- Um hóspede faz uma reserva em um hotel através de seu Website;
- Esta informação é passada para o departamento administrativo, que, em seguida, aloca um quarto;
- A recepção sabe que o hóspede chegará hoje;
- O departamento de limpeza sabe que o quarto deve estar limpo para a chegada do hóspede;

Sistema de Informação

- Não se refere apenas à TIC;
- Mas também na forma como as pessoas interagem com a tecnologia;
- Exemplo:
  - ✓ Arquivos em armários;
  - ✓ Arquivos de computador e bancos de dados;
  - ✓ Smartphones e impressoras;
  - ✓ Transporte de dados por meio de uma rede;
  - ✓ Servidores, compostos com sistema operacional e software.
- No contexto de SI:
  - ✓ É a combinação completa de meios, procedimentos, regras e pessoas que garantem o fornecimento de informações para um processo operacional.

Gestão da Informação

- A gestão da informação descreve o meio pelo qual uma organização trata a informação, como:
  - ✓ Planejamento;
  - ✓ Coleta;
  - ✓ Organização;
  - ✓ Utilização;
  - ✓ Controle;
  - ✓ Disseminação;
  - ✓ Descarte.

  - ✓ Seu foco é a informação como um recurso, independentemente da forma física em que ela ocorre.

Campo Interdisciplinar da Gestão da Informação

- Se baseia em, e combina habilidades e recursos de:
  - ✓ Biblioteconomia e ciência da informação;
  - ✓ Tecnologia da informação;
  - ✓ Gerenciamento de registros;
  - ✓ Arquivamento e administração geral.
- Alguns dos principais tópicos que os profissionais estão preocupados:
  - ✓ Classificação e codificação;
  - ✓ Indexação temática;
  - ✓ Construção e uso de tesauros e vocabulários;
  - ✓ Catalogação e indexação por nomes, lugares e eventos;
  - ✓ Design de banco de dados e estruturas de dados;
  - ✓ Armazenamento físico de livros e registros, em papel e eletrônico;
  - ✓ Armazenamento de imagens fotográficas e digitalizadas;
  - ✓ Auditorias de informação: avaliações dos recursos de informação de uma organização;
  - ✓ Documentação de objetos de museu, tanto para fins de gerenciamento quanto como recurso para pesquisa acadêmica.

Computação Distribuída

- Computação distribuída é qualquer computação que envolve:
  - ✓ Vários computadores distantes um do outro;
  - ✓ Onde cada um tem um papel no problema computacional ou no processamento da informação;
  - ✓ Passos dos processos de negócios são executados em locais mais eficientes.
- Usa o modelo de comunicação client/server, da seguinte forma:
  - ✓ O processamento da interface do usuário é feito em um PC local;
  - ✓ O processamento do negócio é feito em um computador remoto;
  - ✓ E o processamento e o acesso à base de dados são realizados em outro computador ou na nuvem.
- Acaba enfraquecendo a eficácia do controle centralizado e especializado;
- O Ambiente de Computação Distribuída ou Distributed Computing Environment (DCE), é um padrão industrial;
- Utiliza um serviço de diretório para pesquisa.

Tipo de Gestão

- Gestão de Nível Estratégico
  - ✓ **Determina objetivos de longo prazo;**
  - ✓ **Dá o direcionamento.**
- Gestão de Nível Operacional
  - ✓ **Preocupado com as operações diárias;**
  - ✓ **Garante a execução do chão de fábrica.**
- Gestão de Nível Tático
  - ✓ **Preocupada com o planejamento e controle (Mkt, RH etc.);**
  - ✓ **Objetivo de melhorar o desempenho a curto e médio prazo.**
- Gestão de Processos de Negócios
  - ✓ **Semelhante ao tático;**
  - ✓ **Produzem um serviço ou produto específico.**

Processos Operacionais e Informações

- Processo de Negócio é o processo que está no núcleo do negócio;
- Processos de Negócios:
  - ✓ **Começa com a necessidade do cliente;**
  - ✓ **Termina com o atendimento dessas necessidades;**
  - ✓ **Projetados para adicionar valor ao cliente;**
  - ✓ **Não devem incluir atividades desnecessárias.**
- Modelados por meio de variedade de métodos e técnica (BPMN);
- Organizações orientadas a processo evita silos;
- Um processo de negócio pode ser decomposto em vários subprocessos;
- Cada Processo de Negócio deve ter um gerente responsável designado;
- E também é responsável pelos **riscos relacionados** ao processo de negócio.

Processo de Segurança da Informação

Sem uma boa PSI, uma organização enfrentará riscos, e, no pior caso, pode impedir a continuidade dos processos de negócios.

A SI é um processo que envolve muitas pessoas.

- ✓ Sem apoio da administração, pode não ser efetivo;
- ✓ A forma de ser gerenciada depende do tamanho da organização;
- ✓ Depende das obrigações legais;
- ✓ Pode ser atribuída a uma ou algumas pessoas.

Se a SI estiver organizada, é possível **que todos os aspectos da SI sejam apoiados pelo conhecimento dos processos de negócio da organização.**

OBRIGADO

Contexto da Organização

Controles Organizacionais

Sobre **Política de Segurança da Informação**

- A Política de Segurança da Informação deve ser aprovada pelo conselho administrativo e publicada a todos os interessados e envolvidos;
- Deve ser revisada continuamente ou quando ocorrerem mudanças significativas;
- Mantido na Intranet, por exemplo;
- Pode ser incluída no processo de admissão de um funcionário;
- Ter uma Política é uma coisa, cumpri-la é outra;
- Uma Política contém: Procedimento, Política de Documento, Diretrizes, etc;
- Parte de um SGSI (Information Security Management System);
- Independente do tamanho da empresa.

Funções e Responsabilidades de Segurança da Informação

Primeiro:

- É necessário identificar ativos e processos de SI;
- Cada ativo tem um responsável;
- Cada processo tem um dono.

Como estes indivíduos devem ser?

- Competentes;
- Boa relação com fornecedores (identificados e documentados;
- Dependendo da organização, podem haver várias atribuições para um único indivíduo.

Funções

As funções de SI podem ter nomes diferentes, mas, em geral, se resumem às seguintes posições:

- O **Chief Information Security Officer - CISO** é o mais alto nível da gestão da organização e desenvolve a estratégia geral de segurança para todo o negócio;
- O **Diretor de Segurança da Informação (Information Security Officer – ISO)** desenvolve a política de segurança de uma unidade de negócios com base na política da empresa e garante que seja seguida;
- O **Gerente de Segurança da Informação – GSI (Information Security Manager – ISM)** desenvolve a política de segurança da informação dentro da organização de TI e garante que seja seguida;
- Além do **Information Security Policy Officer (ISPO)** ou um **Data Protection Officer (DPO).**

Segregação de Funções

Objetivo: Evitar a chance de alterações não autorizadas ou não intencionais, ou o uso indevido dos ativos.

Revisão deve ser realizada

Determine o acesso à informação
"necessidade de saber".

Desafios

- Aplique na medida do possível mesmo para empresas pequenas;
- Se não for possível, adote outras medidas de controle.

Exemplo

- Alguém planeja uma RDM e outro executa;
- Vendedores inserem pedidos. Coordenadores geram pedido de produção. Gerentes visualizam os lucros.

Responsabilidades da Gestão

Objetivo:

A gerência deve demonstrar apoio às políticas, procedimentos e controles de SI.

A gerência deve garantir que os funcionários:

- Sejam informados sobre seus papéis e responsabilidades de SI **antes** de receberem acesso às informações;
- Tenham acesso às diretrizes e expectativas de SI para o desempenho de suas funções;
- Cumpram com as políticas de Segurança da Informação;
- Obtenham um nível de conscientização em SI;
- Cumpram os termos e condições, contrato ou acordos;
- Mantenham as habilidades e qualificações adequadas em SI;
- Quando possível, tenham à disposição um canal confidencial para relatar violações ("denúncia");
- Tenham recursos adequados para implementar os processos e controles de segurança.

Contato com as Autoridades

Objetivo:

A organização deve estabelecer e manter contato com as autoridades relevantes.

Por que manter esses contatos?

- Melhorar o conhecimento;
- Obter acesso a conselhos especializados em segurança;
- Receber orientações e informações sobre patches de hardware e software, etc.

Inteligência de Ameaças

Objetivo:

A organização investiga ativamente se foram encontradas novas vulnerabilidades.

Tradicionalmente funciona assim:

1. A inteligência de ameaças faz parte da gestão de ameaças e vulnerabilidades;
2. Essa gestão garante que vulnerabilidades sejam descobertas e corrigidas em tempo hábil;
3. Então os patches de segurança são instalados assim que são conhecidos.

Mas, o que tem de diferente nessa “inteligência?

- A organização não espera por uma mensagem do fornecedor;
- A organização investiga ativamente:
  - Surgiram novas técnicas de ataque desconhecidas?
  - Que medidas você pode tomar para se proteger?
- A empresa aumenta sua resiliência com isso!

Segurança da Informação na Gestão de Projetos

Objetivo:

A segurança da informação deve ser integrada ao gerenciamento de projetos.

Por que isso é importante?

- Para que os riscos de SI sejam abordados durante todo o ciclo de vida do projeto;
- Uma avaliação de risco faz parte do projeto inicial;
- Seja incluído os requisitos de segurança da informação;
- Alinhado independente se é projeto em cascata ou ágil;
- Alinhado na programação segura;
- Alinhado com o DevSecOps.

OBRIGADO

Controles Organizacionais

academy

Informações e Ativos

Ativo de Informação

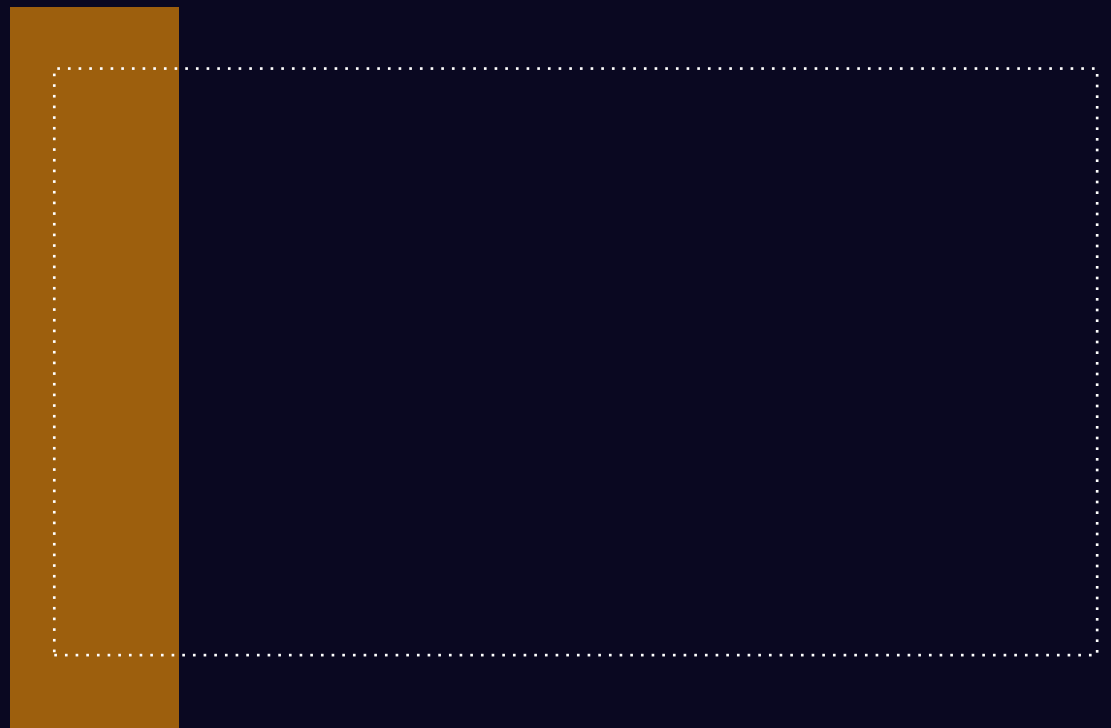
A definição de um ativo é ampla!

- ✓ Qualquer informação valiosa que a organização possui;
- ✓ Pode ter muitas formas diferentes:
  - ✓ Documento em papel;
  - ✓ Documento digital;
  - ✓ Banco de dados;
  - ✓ Senha ou chave criptográfica.
- ✓ Cada ativo é armazenado em algum suporte:
  - ✓ Papel;
  - ✓ Pen drive;
  - ✓ Disco rígido;
  - ✓ Laptop;
  - ✓ Servidor;
  - ✓ Nuvem;
  - ✓ Fita de backup.
- ✓ É importante reconhecer todos os tipos de ativos;
- ✓ Todo hardware e software devem ser documentados;
- ✓ Verifique sempre o CMDB quando novas vulnerabilidades se tornam conhecidas.

Inventário

No mínimo, um inventário deve conter:

- ✓ Nome e descrição;
- ✓ Proprietário de negócios (TI ou SI NÃO). Tipicamente um diretor ou gerente sênior fornece o orçamento para gerenciar ou melhorar o ativo;
- ✓ CIA: Qual desses três se aplica ao seu ativo?
- ✓ Dados pessoais: Na maioria dos países, os dados devem ter proteção adicional;
- ✓ Níveis de Acesso.



Inventário dos Ativos de Informação

Por que é importante?

- ✓ Ponta pé inicial para entendermos o que temos dentro de casa;
- ✓ É um dos primeiros passos para estabelecer um SGSI;
- ✓ Os ativos são a base para identificar os riscos;
- ✓ Ajudam a mitigar os riscos com medidas apropriadas.

O que eu posso usar para ajudar?

- ✓ CMDB (Configuration Management Database).

Uso Aceitável de Informações e Outros Ativos

Objetivo:

Garantir que as informações sejam adequadamente protegidas, usadas e manuseadas.

Quais as vantagens?

- Informações e ativos sejam tratados com cuidado;
- Informações devem estar corretas;
- Informações confidenciais não saia da sua organização, a menos que sejam aprovadas;
- Diretrizes elaboradas como parte da SI e da política de RH.

Devolução de Ativos

Objetivo:

Proteger os ativos da organização como parte do processo de mudança ou rescisão de emprego, contrato ou acordo.

O que acontece neste controle?

- Garantir a devolução dos ativos da organização em sua posse;
- Após a mudança ou rescisão, deve-se devolver todos os ativos da organização;
- Tem o objetivo de proteger os ativos da organização;
- Ao deixar a organização, todos os direitos sejam revogados;
- Faz parte do processo de mudança ou rescisão de trabalho, contrato ou acordo.

Classificação da Informação

Designar é forma especial de categorização (exemplo: de acordo com um determinado assunto da organização ou um grupo de pessoas autorizadas)

Dono (autoridade por um ativo de negócio)

Classificar é o ato de atribuir a classificação (como secreto, confidencial ou público)

Classificação é usada para definir diferentes níveis de sensibilidade na qual a informação deve ser estruturada

Classificação

Proprietário X Responsável

- O proprietário tem autoridade sobre um ativo;
- Responsável tem responsabilidade diária por ele;
- Eles não devem ser a mesma pessoa.

Como funciona?

- O proprietário atribui uma classificação de acordo com uma lista acordada de classificações;
- A classificação indica a forma de segurança necessária:
  - É determinado em parte pela sensibilidade, valor, requisitos legais e importância para a organização.
- O proprietário deve garantir que ele seja reclassificado, se necessário (diminuir ou conceder permissão).

Rotulagem

O que é?

- Após classificado, é hora do ativo ser “etiquetado” ou rotulado;
- Se um ativo tem uma classificação, é dada uma marca ou etiqueta a ele;
- Isto pode ser colocado de forma física e visível;

Todos os documentos que contêm informações classificadas devem:

- Ter um número de cópia ou versão;
- Numeração de páginas;
- Medidas rigorosas.

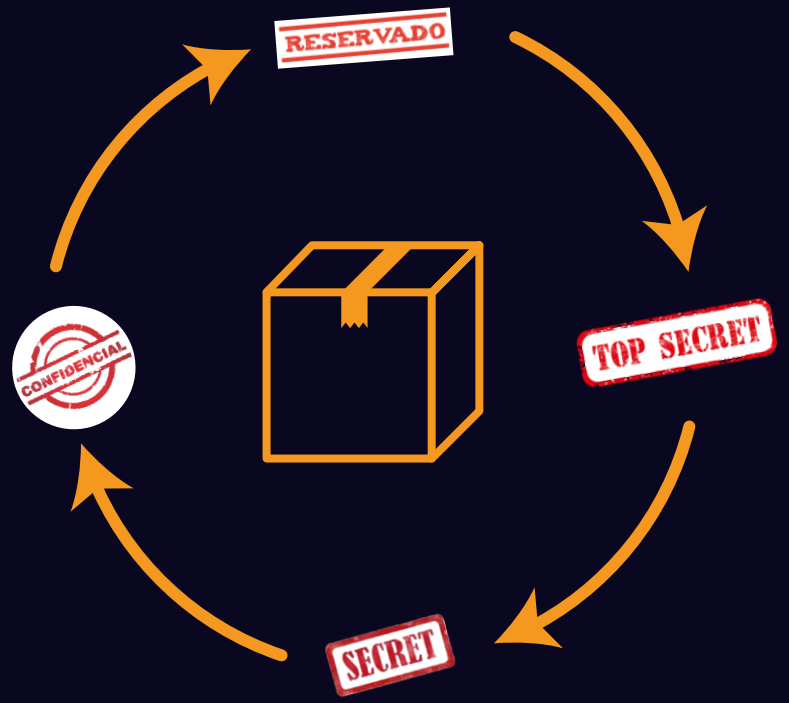
Desafios

- As pessoas precisam pensar cuidadosamente na classificação;
- Ao deixar de atribuir uma classificação, a informação pode se tornar pública;
- Na dúvida, coloque-as como classificação alta;
- Não conseguir acessar um novo ativo adquirido.

Exemplos de Classificação e Rótulos

- Etiquetas físicas são uma forma comum de rotulagem;
- No entanto, documentos eletrônicos requerem um meio eletrônico de rotulagem, como, por exemplo, uma mensagem de notificação na tela.

Atenção: A falta de um rótulo “CONFIDENCIAL” não faz do ativo um ativo “PÚBLICO”



Transferência de Informação

Objetivo:

Evitar que a informação acabe nas mãos de partes para as quais não é destinada.

Qual tipo de transferência?

- Para todos os tipos de transferências:
  - ✓ Verbal;
  - ✓ Eletrônica;
  - ✓ De mídia de armazenamento físico.

Como fazer?

- Aumente a conscientização;
- Evite que informações sejam trocadas entre pessoas de empresas diferentes (concorrentes).

OBRIGADO

Informações e Ativos

Controle de Acesso

Controle de Acesso

Como é feito a definição do controle de acesso?

- O proprietário é quem define os requisitos de acesso;
- O dono do negócio ou atividade é quem pode ter acesso aos ativos.

De onde vem os requisitos de acesso?

- Objetivos comerciais;
- Requisitos legais e regulamentares;
- Uma avaliação de riscos pode ser usada (o quão rigoroso serão os controles de acesso);
- Combinação de controles de acesso lógico e físico.

Precisa de uma política de controle de acesso?

- Sim, ela deve ser estabelecida, documentada e revisada com base nos requisitos de negócios e de segurança da informação.

Controle de Acesso Lógico

- Preveni o acesso indevido a qualquer coisa que tenha valor para a organização;
- As autorizações devem ser normalmente concedidas:
  - ✓ Pela pessoa responsável pelo ativo, geralmente um gerente;
  - ✓ Em certos casos, usuários individuais autorizem o acesso de outros usuários.
- Uma autorização consiste em um conjunto de permissões, como:
  - ✓ Muito simples: direito de ler um determinado arquivo;
  - ✓ Muito complexas: permissões para fazer pagamentos bancários.

Exemplos de tipos de acesso:

- ✓ Acesso a redes e serviços de rede;
- ✓ Acesso a aplicações de negócio;
- ✓ Acesso a equipamentos de TI;
- ✓ Acesso à informação.

Atividades no Gerenciamento de Acesso

Para prevenir que ativos sejam acessados por usuários não autorizados e garantir que estes sejam acessados somente por usuários autorizados é necessário as seguintes atividades:

- **Registro e cancelamento de registro de usuário;**
- **Provisionamento de acesso de usuário;**
- **Gestão de direitos de acesso privilegiado;**
- **Gestão de informações secretas de autenticação de usuários;**
- **Revisão dos direitos de acesso de usuário;**
- **Remoção ou ajuste dos direitos de acesso.**

Gerenciamento de Identidade

Conceder acesso envolve uma série de etapas que incluem:

- ✓ A identificação do usuário (Controle de Gerenciamento de Identidade);
- ✓ A autenticação deste usuário (Controle de Informação de Autenticação);
- ✓ Autorização do usuário para acessar um ativo (Controle de Direitos de Acesso).

Exemplo dos passos no processo de concessão de acesso:

1. Identificação de uma pessoa através de um token: número de conta ou nome de usuário;
2. O sistema então precisa determinar se o token é autêntico;
3. O sistema verifica se o nome de usuário existe dentro do sistema.
4. Se o nome de usuário existir, o usuário é solicitado a fornecer uma senha.
5. O sistema verifica se a senha está registrada com o nome de usuário fornecido.
6. Se ambos os testes forem válidos, o usuário é autenticado com base nas permissões atribuídas ao usuário autenticado.

Informações de Autenticação

Importante:

Ter processo, procedimento e ferramenta para orientar o pessoal sobre como criar e armazenar senhas seguras.

Cuidados:

- Senhas padrão de fábrica em sistemas devem ser desativadas;
- Usuário gere uma senha para o login pelo menos uma vez;
- Depois, pode ser atrelada a biometria, PIN, facial etc;
- Habilitar a autenticação em dois fatores;
- Uso de um um cartão inteligente (smart card).

Direitos de Acesso

- Deve haver um equilíbrio na restrição do direito de acesso:
  - ✓ Se muito, usuários são impedidos de desempenhar suas tarefas;
  - ✓ Se pouco, traz riscos de acesso não autorizado.
- O objetivo é ajudar o usuário a fazer login e não fornecer informação útil a um atacante;
- Medidas que podem ser tomadas, por exemplo, são:
  - ✓ Não mostrar um nome padrão de usuário;
  - ✓ Se o usuário ou senha estiverem incorretos, não informar qual;
  - ✓ Não mostrar muitas informações sobre o sistema no login;
  - ✓ Mostrar ao usuário (depois do login) uma mensagem que alguém tentou efetuar o login e não conseguiu (ou conseguiu).
- Use um bom sistema de gerenciamento de senhas;
- Limite o uso de utilitários com privilégios;
- Controles de acesso rigorosos ao código-fonte e documentação do projeto.

Tipo de Controle de Acesso

O tipo de controle de acesso que deve ser aplicado a um ativo precisa ser determinado pelo seu dono.

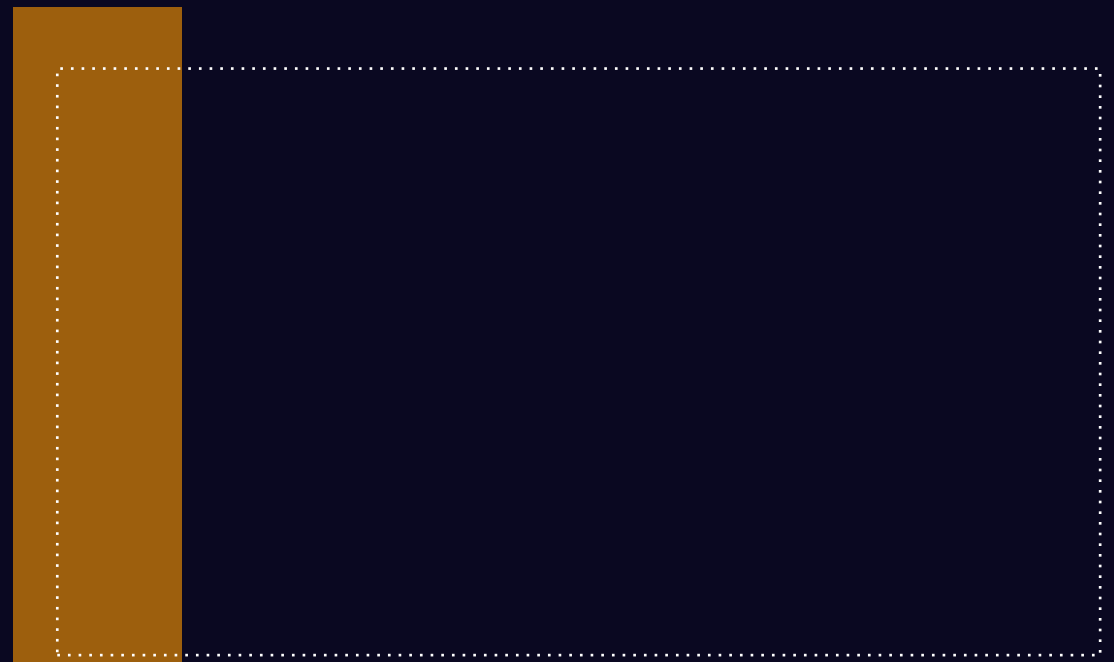
- **Controle de Acesso Discricionário (DAC).** A decisão de conceder o acesso à informação encontra-se com o próprio usuário e donos dos dados (diretório pessoal).
- **Controle de Acesso Mandatório (MAC).** Donos e usuários somente podem permitir acesso a outros dentro dos limites (classificação) declarado em uma política centralizada.
- **Controle de Acesso Baseado em Função (RBAC).** Decisões de acesso se baseiam na função dos sujeitos, normalmente pessoas.
- **Controle de Acesso Baseado em Reivindicações (CBAC).** As decisões são baseadas em conjunto de reivindicações necessárias antes de conceder o acesso (“o usuário trabalha para a organização X”). É a forma mais flexível de controle de acesso, pois não se limita a reivindicações relacionadas a um papel.

Segurança nos Pontos de Acesso

- A concessão de acesso é uma preocupação organizacional também;
- Importante monitorar também:
  - ✓ Quem tem acesso a quê;
  - ✓ Se há abuso dessa autorização.

Motivos para proteger pontos de acesso:

- Riscos de roubo de identidade;
- Roubo de dinheiro;
- Cumprimento de determinados requisitos legais;
- Regulamentos de privacidade.



OBRIGADO

Controle de Acesso

Segurança com Fornecedores

Relacionamento com Fornecedores

- Toda organização precisa de um fornecedor;
- Ao terceirizar parte ou a totalidade da TI, um contrato deve ser firmado;
- O contratante deve supervisionar o desenvolvimento que foi terceirizado;
- Lidar com a propriedade intelectual. Quem é dono do código-fonte?
- Garantir que os termos e condições de SI sejam cumpridos;
- Que incidentes e problemas sejam gerenciados;
- Opte por fornecedores com ISO 27001;
- Atenção às mudanças em serviços, levando a novos SLAs e reavaliação de riscos;
- Se houver subcontratados, estes devem ser contemplados.

Cadeias de Suprimentos de TIC

É essencial:

- Garantir, de forma segura e cuidadosa, o repasse dos dados e aplicações aos fornecedores externos;
- A organização que terceiriza seus dados continua sendo o responsável final;
- O contratante é e continua sendo a proprietário dos dados;
- Mas o contratado pode ser responsabilizado por um vazamento também;
- Por isso, registre os responsáveis no contrato;
- Registre os requisitos para as medidas de segurança do fornecedor;
- Busque saber se o fornecedor utiliza subcontratados "desconhecidos" e sem “consciência sobre segurança”.

Exemplos de Cadeias de Suprimentos de TIC

A. Provisionamento de Serviços em Nuvem:

- Desenvolvedores de software;
- Fornecedores de serviços de telecomunicações;
- Fornecedores de hardware.

B. IoT, onde o serviço envolve:

- Fabricantes de dispositivos;
- Provedores de serviços em nuvem (operadores de plataforma IoT);
- Desenvolvedores de aplicativos móveis;
- Desenvolvedores Web;
- Fornecedor de bibliotecas.

C. Serviços de hospedagem:

- Centrais de atendimento externas;
- Primeiro de atendimento;
- Equipe especializada segundo e terceiro nível de suporte.

Monitoramento, Revisão e Gerenciamento de Mudanças de Serviços de Fornecedores

Desafio: Grandes empresas normalmente não revelam suas medidas de segurança. Um órgão independente pode manter uma auditoria (normalmente aceita).

Considere na Auditoria:

- Gerenciamento de mudanças;
- Gerenciamento de incidentes;
- Gerenciamento de ameaças e vulnerabilidades;
- Gerenciamento de patches;
- Gerenciamento de identidade e acesso;
- Conscientização dos funcionários internos do fornecedor;
- Declarações de confidencialidade;
- Procedimentos de desenvolvimento e teste;
- Mudanças e aprimoramentos em redes;
- Uso de novas tecnologias;
- Adoção de novos produtos ou versões mais recentes;
- Novas ferramentas e ambientes de desenvolvimento;
- Mudanças na localização física das instalações de serviço;
- Mudanças de subfornecedores.

Segurança da Informação para Uso de Serviços em Nuvem

A organização deve estabelecer e comunicar:

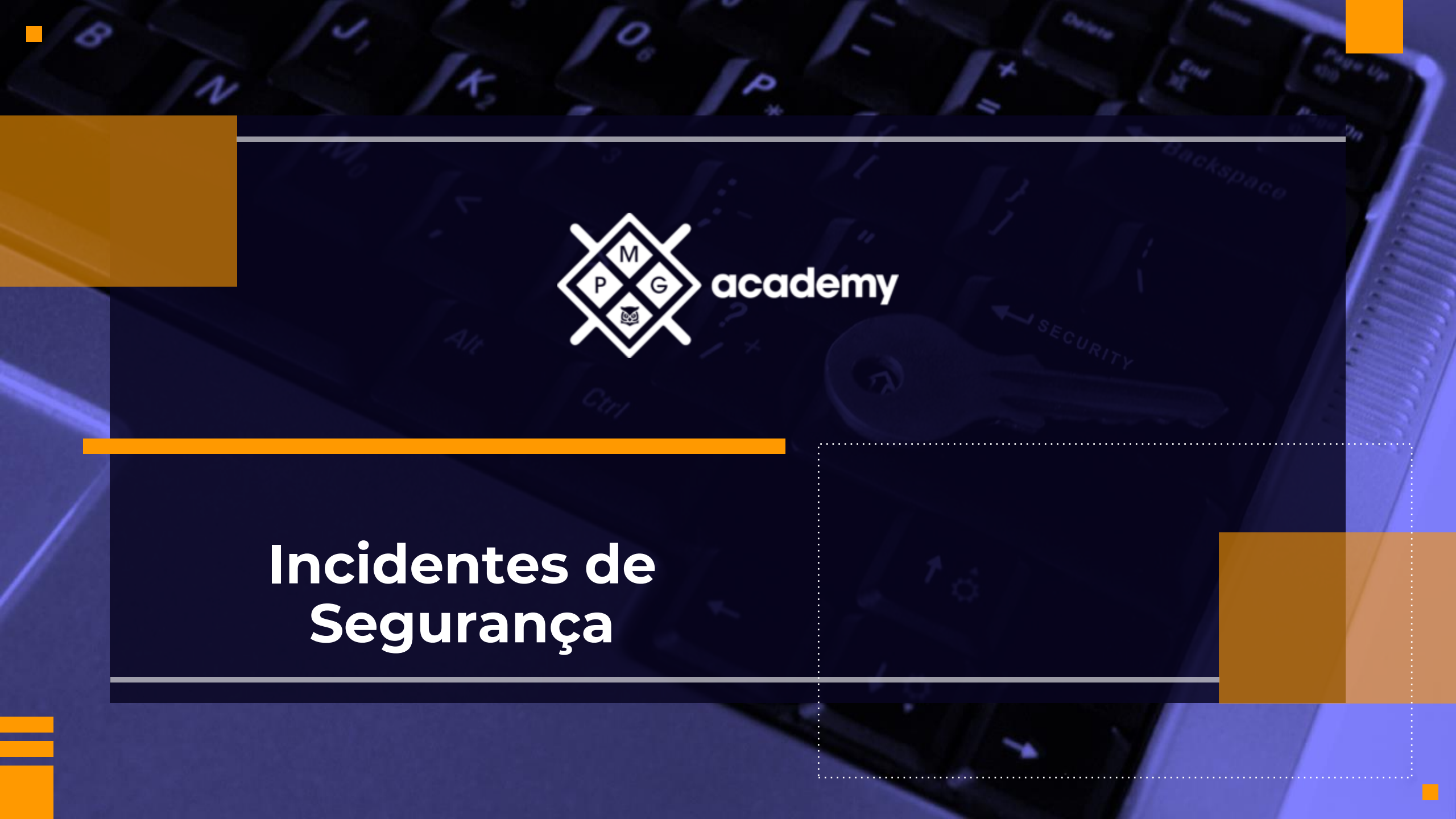
- Uma política sobre o uso de serviços em nuvem para todas as partes interessadas;
- Como pretende gerenciar os riscos de SI associados ao uso de serviços em nuvem.

Sobre a norma:

- Atualmente o ISO/IEC 27017 oferece orientações para a nuvem;
- Ainda não estão disponíveis na ISO/IEC 27001:2022;
- Mas, a 27002 é muito útil, pois separa as responsabilidades:
    - Do Provedor de Serviços em Nuvem;
    - Da parte que terceiriza.

OBRIGADO

Segurança com Fornecedores



Incidentes de Segurança

Planejamento e Preparação do Gerenciamento de Incidentes de Segurança da Informação

Incidente:

- Pode ser silencioso, furtivo e inesperado;
- Pode ser catastrófico;
- Se bem controlado, a empresa pode dar uma boa impressão na gestão de crise;
- Podem surgir de ações humanas (intencional ou não);
- Pode vir de dentro ou de fora da empresa;
- Podem ter uma causa técnica ou natural.

Proteção:

- Toda organização deve estar preparada para incidentes de SI;
- Visualize seu ambiente sob a ótica de um atacante;
- Pense em quem deve ser alertado e toma decisões;
- Investimento na contratação de especialistas externos;
- Medidas que permitam investigações forenses.

O mais importante é voltar ao funcionamento normal o mais rápido possível.

Avaliação e Decisão sobre Eventos de Segurança da Informação

Nem todo incidente é um incidente de SI

- O que é entendido por Incidente de SI?
- Como categorizar e priorizar Incidentes?
- Quais outros processos são ativados?

Objetivo do Gerenciamento de Incidentes

- Que os incidentes sejam conhecido;
- Que sejam tratados em tempo hábil;
- Que os procedimentos sejam seguidos;
- Que os incidentes e vulnerabilidades sejam relatados o mais rápido possível à CS.

Considerações na Avaliação e Decisão sobre Eventos de SI

Considerações

- Aprender para evitar a recorrência;
- Relatar não é sinal de punição (nem sempre);
- Sem medo da delação;
- Um formulário ajuda a minimizar o medo.

Formulário:

- Data e hora;
- Nome da pessoa que relata;
- Localização (onde ocorreu o incidente?);
- Qual é o problema? (vírus, roubo, invasão);
- Qual é o efeito do incidente?
- Como foi descoberto?
- Tipo de sistema (desktop, impressora);
- Quem mais foi informado?

Exemplo de Incidentes de SI

- Falta de manutenção dos equipamentos;
- O fornecimento de energia de emergência não foi testado;
- Um colega perde um laptop;
- Um colega não segue a política de mesa limpa;
- Um colega traz um visitante não autorizado;
- Um novo software é implementado sem ser testado;
- Um vírus conseguiu entrar na rede;
- Dados incompletos da empresa, os resultados de lucro são pouco confiáveis;
- Os direitos de acesso de um funcionário não são modificados após uma mudança de cargo;
- Um colega escreve sua senha em um papel que está embaixo do teclado.

Exemplo de Procedimento em caso de Incidentes de SI

Descreve quem faz o quê, incluindo:

- A análise da causa do incidente;
- Medidas para minimizar as consequências do incidente;
- Medidas corretivas para evitar a recorrência;
- Partes devem ser informadas em caso de um incidente;
- O que deve ser relatado sobre o incidente e para quem;
- Escalonamento caso a situação piore ou não seja resolvida de forma oportuna.

Todos os Incidentes deve ser relatados à Central de Serviços de TI ou diretamente ao escritório de segurança.

Todos os Incidentes receberão um Nível de Severidade.

Nível de Severidade

Crítico

- Causa problema no negócio;
- Impacto crítico nas operações e comercial;
- Não há solução alternativa aceitável para o problema.

Alto

- Perda significativa de serviço;
- Afeta negativamente o negócio, mas a operação pode continuar de forma restrita ou alternativa.

Médio

- Não está causando perda de serviço ou é muito pequena;
- Não impede a operação ou os negócios;
- Normalmente iniciados por e-mail.

Baixo

- Pergunta relacionada à operação de um produto;
- Sugestão de alteração em um produto.

Resposta a Incidentes de Segurança da Informação

Objetivo:

Necessário para que todos saibam o que fazer.

Documentar o processo de gerenciamento de incidentes e conscientizar a todos para agir o mais rápido possível

O que documentar?

- A quem informar o mais rápido possível;
- Quais medidas tomar;
- Para "incidentes frequentes", é possível desenvolver playbooks para lidar com o mesmo tipo de incidente.

Aprendendo com Incidentes de Segurança da Informação

Como aprender com Incidentes?

- O processo de incidente foi executado conforme o planejado?
- Avalie o incidente desde o início até o seu fechamento;
- Registre todas as ações;
- Registre quais decisões foram tomadas e por quem;
- A partir desta análise podem surgir melhorias;
- Identifique possíveis erros no processo;

Aprenda com o próprio Incidente

- Pode ser um sinal de que um risco não foi identificado;
- Sinal que o risco foi avaliado incorretamente;
- Sinal que talvez o risco tenha sido aceito indevidamente;
- Sinal de que uma medida de controle não estava funcionando.

Coleta de Evidências

Objetivo:

Assegurar uma gestão consistente e eficaz das provas relacionadas a incidentes de segurança da informação.

Essas evidências (legais) só terão valor se:

- Houver um equilíbrio entre retomar o mais rápido possível e, identificar o agente causador;
- Que seja possível levar o agente à justiça;
- Criminosos devem ser responsabilizados por suas ações e pelos custos de recuperação.

Segurança da Informação Durante a Interrupção

Como estar preparado para agir durante um incidente de segurança?

- Mantenha um alto nível de segurança durante um incidente ou uma situação de continuidade de negócios;
- Planos devem estar disponíveis, implementados e testados regularmente;
- Planos devem ser avaliados constantemente;
- Um Sistema de Gestão de Continuidade de Negócios deve ser implementado.

Princípios de Gestão da Continuidade de Negócios

O que faz parte da Governança Corporativa?

- A Gestão da Continuidade de Negócios (BCM);
- Gestão de Crises.

As atividades de BCM devem

- Concentrar-se e apoiar diretamente a estratégia de negócios e objetivos da organização;
- Deve fornecer resiliência organizacional;
- Otimizar a disponibilidade de produtos e serviços;
- Otimizar a eficiência de custos (por se basear em valores);
- Agregar valor e não apenas por conta da governança ou questões regulatórias;

Preparação da TIC para Continuidade de Negócios

Se prepare com um BCM que contemple:

- Recuperação de desastres;
- Gerenciamento de crise;
- Controle de gerenciamento de riscos;
- Um amplo espectro de negócios e disciplinas de gestão.

Um BCM têm dimensões estratégicas e operacionais!

Falácias:

1. Se aplica apenas a empresas do setor privado;
2. Trata-se apenas da Recuperação de Desastres de TI.

Envolve:

- Avaliações de Impacto nos Negócios (BIA) ;
- Objetivo de tempo de recuperação (RTO);
- Objetivos de ponto de recuperação (RPO);
- Resultado: Planos de continuidade de negócios prontos e testados e preparado quando ocorrer um desastre.

OBRIGADO

Incidentes de Segurança

academy

CONFORMIDADE

Requisitos Legais, Estatutários, Regulamentares e Contratuais

O que é conformidade?

- Pode ser descrita como obrigação, obediência, adequação etc.
- Tão desafiador quanto lidar com o cenário de ameaças;
- Leis e regulamentações podem variar dependendo do ramo da indústria, país, tipo de informação, entre outros aspectos.

Como podem ser apresentadas?

- Leis trabalhistas;
- Requisitos de segurança relacionados à TI;
- Direitos de propriedade intelectual e direitos autorais;
- Leis de Privacidade e proteção de dados.

A falta pode resultar:

- Multas pesadas ou penalidades dos órgãos reguladores;
- Ações judiciais por negligência e exposição na mídia;
- Negativamente a imagem, marca e o valor da empresa.

Direitos de Propriedade Intelectual

- Os Direitos de Propriedade Intelectual (IPR / DPI) devem ser considerados ao usar um software;

Considere ao proteger as propriedades intelectuais:

- Definir e comunicar a política de proteção de direitos de propriedade intelectual;
- Manter uma conscientização da política;
- Incluir na política de DPI as medidas disciplinares caso haja violação;
- Comprar programas apenas de fornecedores seguros;
- Se software de código aberto, respeite a respectiva licença;
- Manter um registro de ativos e identificar todos os requisitos;
- Compreenda os direitos de propriedade nas condições da licença.

Considerações sobre os Direitos de Propriedade Intelectual

Os direitos de propriedade intelectual incluem:


Direitos autorais de software;


Direitos autorais de documentos;


Direitos de design;


Marcas registradas;


Patentes;


Licenças de código-fonte.

Proteção de Registros

Objetivo:

Garantir que os registros sejam protegidos contra perda, destruição, falsificação, acesso não autorizado e liberação não autorizada.

Quais são os tipos de registros?

- Registros contábeis;
- Registros de base de dados;
- Registros de transações;
- Registros de auditoria e procedimentos operacionais.

Com qual detalhe?

- Período de retenção;
- Tipo de mídia de armazenamento, como, por exemplo:
  - ✓ Papel, microficha;
  - ✓ Meio magnético ou óptico.

Definição de Dados Pessoais

Um dado de qualquer informação relacionada a uma pessoa física identificada ou identificável, ou seja, de um "titular dos dados".

- Para que as informações sejam "dados pessoais", elas não precisam ser verdadeiras ou comprovadas;
- Mentiras ou dados incorretos sobre uma pessoa ainda são dados pessoais;
- O conceito de dados pessoais inclui informações disponíveis em qualquer forma:


Texto;


Figuras;


Gráficos;


Fotografias;


Vídeo;


Áudio ou qualquer outra forma possível.

Privacidade e Proteção de Dados Pessoais

- **PRIVACIDADE** é definida como o direito a respeitar a vida privada e familiar de uma pessoa, sua casa e correspondência.
- **PROTEÇÃO DE DADOS PESSOAIS** diz respeito à proteção de dados pessoais, não de todos os dados.

Escopo Territorial

Onde é aplicado a lei para qualquer pessoa que processe informações de identificação pessoal (PII)?

- Na União Europeia;
- Àqueles fora da Europa que oferecem bens ou serviços a cidadãos da EU.

Para uma multinacional, dependendo da localização europeia, a autoridade reguladora terá sua jurisdição.

- Então a pessoa terá uma variedade maior de ações contra a organização;
- Associações comerciais também serão autorizadas a entrar com ações coletivas em nome de seus membros;
- Os processadores de dados compartilharão a mesma responsabilidade das leis (aumentando os riscos para a TI).

Restrições no Uso de Dados

As organizações são impactadas no que diz respeito aos dados do cliente, independentemente se:

- B2C ou B2B;
- Tamanho da organização.

O processamento de dados pessoais deve estar em conformidade com a lei de proteção de dados por design ou por padrão.

Quais as características do regulamento da EU?

- O consentimento sempre deve ser obtido antecipadamente e de forma explícita;
- Dados do cliente podem ser transferidos eletronicamente para um concorrente mediante solicitação do respectivo cliente (Artigo 18);
- Os indivíduos terão o direito de transferir todas ou quaisquer informações para uma organização terceira (quem paga?);
- Do ponto de vista da relação entre segurança e privacidade, o Artigo 32, trata da segurança da informação para proteger os dados pessoais.

Deveres Adicionais para as Empresas

Existem mais obrigações, tais como:

- Obrigação adicional de transparência (Artigo 14);
- Direito ilimitado à informação (Artigo 15);
- Elaboração de diretrizes corporativas;
- Documentação complexa;
- Avaliação de impacto (Artigo 33);
- Possível consulta a autoridade de supervisão independente para obter aprovação para o processamento de dados;
- Demonstrar auditorias regulares (DPO);
- Avaliação de riscos;
- Encarregado capacitado para empresas acima de 250 funcionários e autoridade pública;
- Relatar violações de proteção de dados em até 24 horas.

Aumento das Multas

O regulamento da UE prevê penalidades pesadas para violações repetidas:

- Primeiras infrações, as autoridades de supervisão nacionais podem enviar uma carta de aviso;
- Violações graves (processamento de dados sensíveis sem o consentimento), as autoridades de supervisão imporão multas:
  - ✓ Até €1 milhão;
  - ✓ Até 2% do faturamento anual global de uma empresa.

Revisão da Segurança da Informação

Objetivo:

Avaliar periodicamente as medidas de segurança, processos e procedimentos.

Qual a utilidade?

- Testar se as medidas de segurança estão em conformidade;
- Avaliar se as medidas de segurança estão de acordo com requisitos específicos de segurança;
- Ajudar a verificar se essas medidas estão funcionando conforme especificado e esperado.

Elementos de um programa de revisão:

- ✓ Escopo das revisões;
- ✓ Critérios de revisão;
- ✓ Frequência;
- ✓ Metodologia de revisão.

Regras da Revisão da Segurança da Informação

Quais as regras da revisão?

- Regra de ouro: Um auditor nunca deve revisar seu próprio trabalho;
- Procedimento documentado com responsabilidades;
- Definir escopo para o planejamento e a condução das revisões;
- O gerente responsável deve garantir que quaisquer não conformidades identificadas sejam investigadas;
- Gerente deve garantir que as ações necessárias sejam tomadas e verificar os resultados dessas ações;
- O auditor interno e/ou externo deve verificar se a organização está em conformidade com as regulamentações;
- O auditor faz isso verificando:
  - ✓ A medida específica está em vigor?
  - ✓ Ela está incluída na política?
  - ✓ É observada na prática?
  - ✓ A medida funciona como deveria?

Conformidade com Políticas e Padrões de Segurança da Informação

Objetivo:

Garantir conformidade com as Políticas, Regras e Padrões após revisões.

Como saber se estamos em conformidade?

- Revisando os requisitos de SI definidos na política, regras, padrões e outros;
- Coletando o resultado de ferramentas automáticas de medição;
- Obtendo o resultado de relatório.

E se encontramos uma não conformidade? O que fazer?

- Identificar as causas da não conformidade;
- Avaliar a necessidade de ações corretivas para atingir a conformidade;
- Implementar ações corretivas apropriadas;
- Revisar as ações corretivas para verificar sua eficácia e identificar quaisquer deficiências ou fraquezas.

Considerações

- Os resultados das revisões e ações corretivas devem ser registrados;
- As ações corretivas devem ser concluídas em tempo hábil.

Organizações e Padrões Sobre Segurança da Informação

ISO

- Mais usada na Europa, é a federação mundial de organismos nacionais de normatização de cerca de 100 países.
- Promove a camada OSI (Interconexão de Sistemas Abertos)

NIST

- Promove publicações sobre ameaças e vulnerabilidades e para implementar medidas de segurança;
- Como a série NIST 800 é um conjunto de documentos que descreve políticas, procedimentos e diretrizes para a segurança de computadores;
- Em 2014 o NIST publicou um novo padrão de segurança cibernética.

ANSI

- Membro dos EUA na ISO;
- Estabeleceu alguns padrões, como o ASCII.

Organizações e Padrões Sobre Segurança da Informação

ITU-T

- Padrões cooperativos para equipamentos e sistemas de telecomunicações.

IEEE

- Padrões para protocolos mundialmente utilizados para a conexão de redes.

OWASP

- Projeto de segurança de aplicativos de código aberto. Trabalha de forma imparcial.

PCI

- Lida com cartões e processadores de pagamento.

Procedimentos Operacionais Documentados

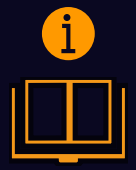
Objetivo:

Documentar e disponibilizar procedimentos operacionais associados à segurança da informação.

O que incluir em um procedimento?

- Como lidar com informações;
- Como, quando e quais backups são feitos;
- Pessoas de contato em caso de incidente;
- Gerenciamento de registros de auditoria e arquivos de log.

Qual objetivo final é garantir:



- Que não haja mal-entendidos em relação à forma como o equipamento deve ser operado;
- Armazenamento dos registros de auditoria, logs do sistema, eventos e ações no sistema e na rede;
- Em caso de problemas, esses arquivos podem ser cruciais para descobrir o que deu errado.

OBRIGADO

CONFORMIDADE

Controle de Pessoas

Controle de Pessoas

- Patrimônio da empresa;
- Habilidades e conhecimento tem valor;
- Todos são responsáveis pela Segurança da Informação;
- Responsabilidades descritas no contrato de trabalho;
- Os controles de pessoas geralmente são preventivos;
- Procedimentos na saída da organização ou mudança de cargo;
- Lembrar de alterar ou remover direitos e recolher equipamentos e cartões de acesso;
- Os direitos de acesso devem ser controlados pelo gerente;
- Se aplica também a qualquer equipe temporária contratada;
- Os acordos como uma recrutadora, devem incluir sanções em caso de violações.

Controle: Triagem

O que é feito antes da contratação?

- Verifica-se os antecedentes de todos os candidatos a se tornarem funcionários;
- Geralmente apresenta-se também um atestado de boa conduta;
- Em alguns países, é obrigatório o preenchimento de um 'certificado de boa conduta';
- Respeite as leis e regulamentos do país/estado.

As verificações de antecedentes devem incluir:

- Identidade do candidato;
- Referências;
- Integridade do currículo e das qualificações;
- Fontes abertas por conta própria, se permitido em seu país.

Termos e Condições de Emprego

Objetivo:

Registrar em políticas, procedimentos e nos contratos de trabalho, as regras de SI.

Essas obrigações devem mencionar:

- Acordo de confidencialidade (NDA) assinado;
- Processo disciplinar em caso de violação;
- Regras e regulamentos em relação ao tratamento de informações de terceiros;
- Respeito às leis e regulamentos, como leis de privacidade, leis de direitos autorais, etc.;
- Como lidar com os ativos, informações e equipamentos da organização;
- Obrigação de seguir o programa de conscientização da organização;

Mantenha a PSI atualizada, as leis sempre mudam!

Mantenha um código de conduta, ex: uso de e-mails pessoais. O gerente é responsável pela descrição.

Conscientização, Educação e Treinamento

Sensibilização

Documentação

Proteção contra Engenharia Social

Cursos (na integração e mudança de cargo)

Conscientes da Importância

Conscientização, Educação e Treinamento em Segurança da Informação

Considerações:

- O efeito da segurança da informação não dura para sempre;
- Use exemplos reais de incidentes que ocorreram na organização;
- Use diversos meios: panfletos, folhetos, mensagens nas telas dos computadores, mouse pads, boletins informativos, vídeos etc.;
- Desenvolva cursos separados para gerentes de sistemas, desenvolvedores, usuários e pessoal de segurança;
- A documentação de segurança e informações deve estar disponível para todos na organização e revisada periodicamente;
- Atividades sociais cotidianas e contatos, como aniversários, reuniões com amigos, conhecidos casuais, representam um risco;
- Em uma grande organização onde nem todos se conhecem, há uma boa chance de sucesso do ataque de engenharia social;
- Quando, por exemplo, ouvimos alguém falar usando a terminologia correta, assumimos que ele faz parte da organização.

Processo Disciplinar

Como usar um processo disciplinar?

- Um processo disciplinar é usado para quem viola a política de segurança da informação;
- Deve ser formalizado e comunicado com as partes interessadas relevantes;
- Garantir que entendam as consequências da violação da política de SI.

Considerações

- Processo disciplinar deve ser abordado durante a conscientização;
- Além de ser mencionado nos contratos de empregados;
- Procure maneiras de recompensar comportamentos positivos, caso o processo disciplinar não seja apropriado para a organização.

Responsabilidades Após Rescisão ou Mudança de Emprego

Pode ser necessário que, após o término do contrato ou mudança de cargo:

- Garantir a confidencialidade do conhecimento sobre a segurança ou outros segredos;
- Abordar nos acordos de confidencialidade;
- Abordar nos termos e contrato de trabalho;
- Abordar nos contratos com fornecedores e pessoal externo;
- Manter um processo quando alguém deixa a organização;
- Garantir que todos os seus direitos sejam revogados;
- Garantir a devolução dos ativos;
- Considerar após o término do trabalho do pessoal externo ou contratados.

Contratos de Confidencialidade ou Não Divulgação

Como aplicar?

- Envolve acordos após o término do contrato;
- O gerente é responsável por documentar as regras;
- Cargos que envolvem confidencialidade devem assinar um NDA;
- Pode ser muito caro a triagem. Alguns países, o governo mantém organizações para isso;
- Considere os prazos da confidencialidade;
- Considere sanções em caso de violação.

Recomenda-se envolver o departamento jurídico na elaboração de um NDA.

Trabalho Remoto

Emita uma política específica que contemple:

- Benefícios do teletrabalho sem aumentar indevidamente os riscos;
- Controles que estão ausentes no trabalho presencial;
- Aquela tentação de adotar um comportamento doméstico em vez de profissional;
- Equipamentos, tecnologia e software para tal;
- Avaliação de riscos individuais, pois dependem do local, cargo, nível de confidencialidade, criticidade, etc.

Elementos Considerados no Trabalho Remoto

- Autorização e autenticação, utilizando autenticação de vários fatores;
- Provisão de equipamentos e segurança dos equipamentos, antimalware, segurança de endpoint;
- Segurança da informação durante o teletrabalho;
- Aspectos de segurança física ao trabalhar em um local diferente;
- Como garantir a segurança das comunicações;
- Como usar tecnologias de acesso remoto, como desktops virtuais e VPN;
- As ameaças diferentes do trabalho no escritório;
- Como lidar com visitantes no local de trabalho remoto, incluindo familiares;
- Condições de rescisão e revogação de direitos.

Relatórios de Eventos de Segurança da Informação

Exemplo de eventos detectados:

- Alguém deixou um documento confidencial na impressora;
- Um arquivo com informações pessoais desapareceu;
- Odor incomum no datacenter;
- Uma porta que deveria estar trancada foi deixada aberta;
- Um colega está se comportando de forma errática;
- O computador está exibindo mensagens estranhas;
- O PC não está bloqueado ao deixar o escritório.

Processo para relatar:

- ✓ Incidente é relatado à CS;
- ✓ Se não houver conhecimento, escalar (horizontal e vertical).

OBRIGADO

Controle de Pessoas

academy

CONTROLES FÍSICOS DA SEGURANÇA DOS PERÍMETROS

Medidas de Segurança Física

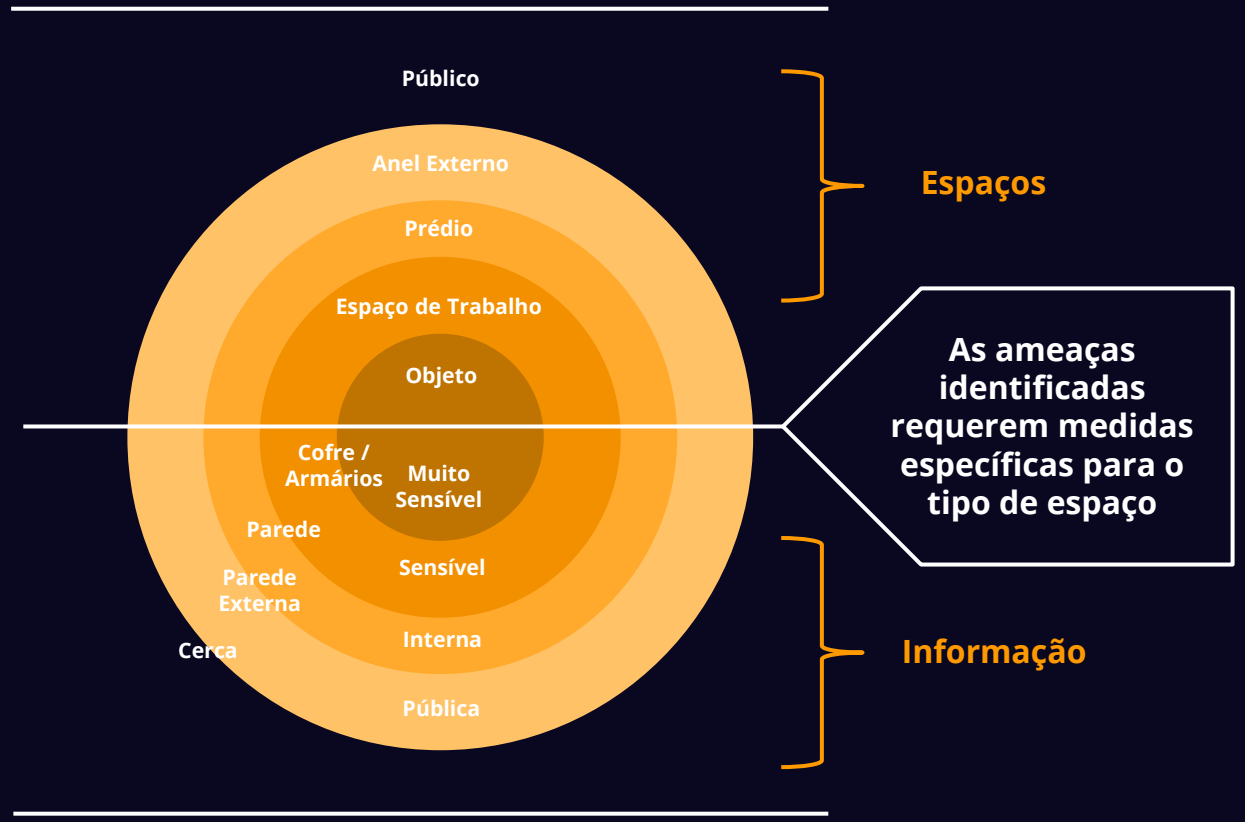
- As medidas físicas geralmente são implementadas em combinação com medidas técnicas e organizacionais.

Tudo depende do tipo de organização:

- Se pública, o acesso aos prédios e ao local será bastante irrestrito, como uma biblioteca pública;
- Organizações que fabricam produtos sob condições de segurança muito rigorosas, com uma indústria farmacêutica.

Anéis de Proteção

Perímetros de Proteção



Anel Externo

Estacionamento

Riacho

Muros

Cerca Viva

Anel Externo

Arames Farpados

Prédio

Reconhecimento das mãos

Vidros Blindados

Biometria

Portões Resistentes

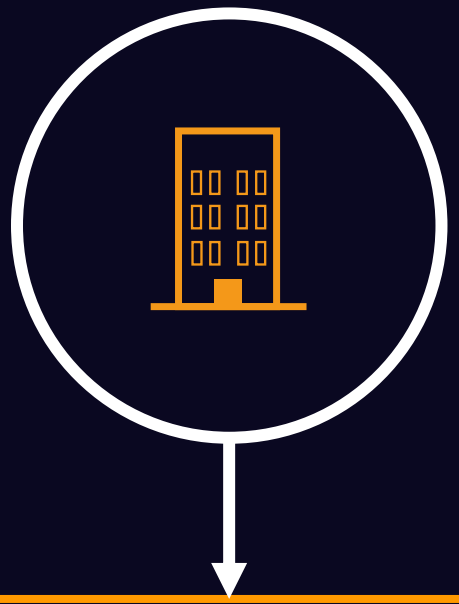
Construções

Impressão Digital

Cômodos e Quartos/Cofre

A entrada do prédio pode ser uma parte acessível ao público:

Recepção



Acompanhamento
- Na entrada
- Até a saída

Quarto Seguro / Cofre

Maior proteção
- Direitos especiais
- Datacenter (Salas especiais)

Os locais de trabalho não devem ser acessados sem orientação ou supervisão.

Perímetros de Segurança Física

A segurança física é mais antiga do que a segurança da informação!

- É utilizado métodos e técnicas particulares;
- Fornecida pelos gerentes de serviços gerais e técnicos;
- Integração importante entre segurança física e segurança da informação;
- Medidas físicas devem ser tomadas em relação às medidas de TI;
- Utilize uma avaliação de riscos para garantir que não haja lacuna entre as várias medidas de segurança;
- A entrada do perímetro deve ser guardada ou ter um recepcionista;
- Utilize as próximas medidas de segurança mencionadas.

Controles de Acesso Físico

Anel Interno. Onde fica?

Entre o anel externo e as instalações.

O que pode ser utilizado?

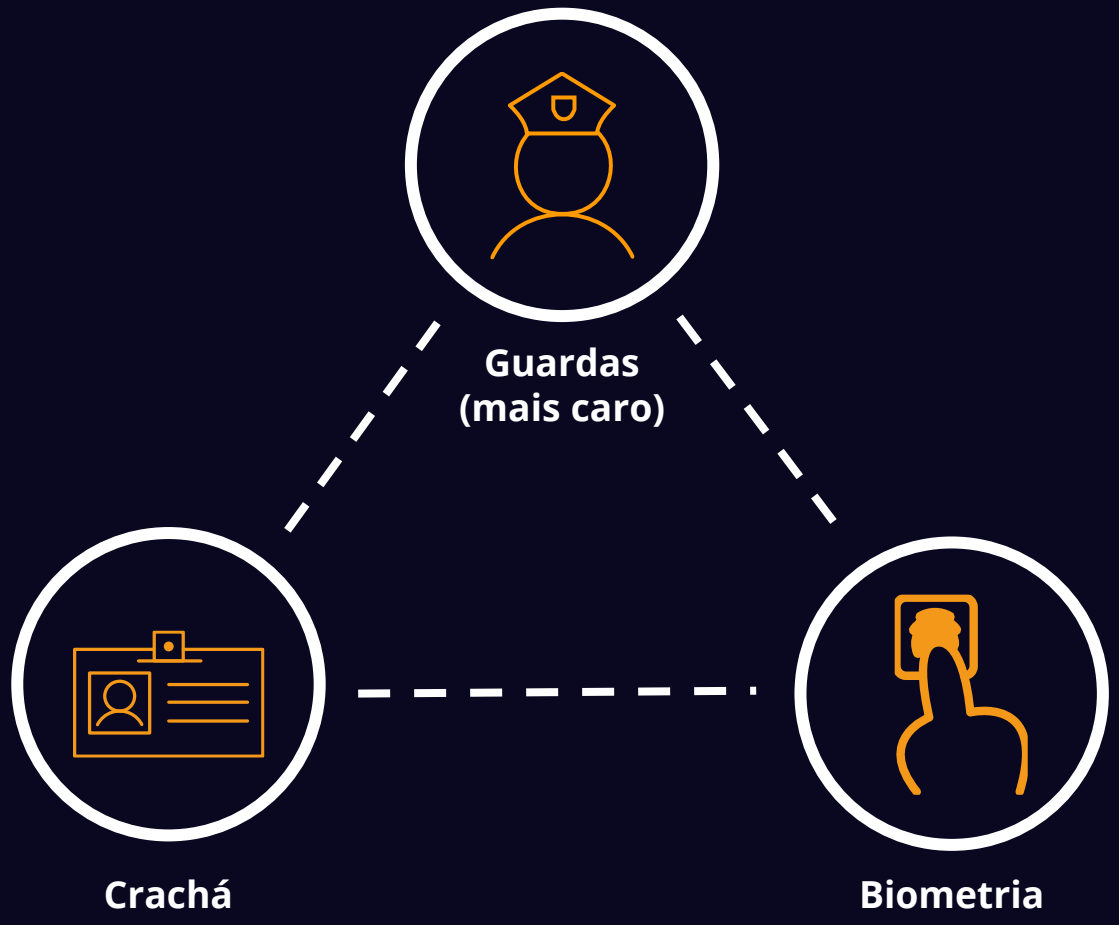
- Vigilância por um segurança e para serviços auxiliares;
- Por exemplo, estacionamento (preferencialmente isolada do prédio), mas com boa iluminação;
- Atenção ao telhado e às paredes;
- Câmeras de vigilância podem ajudar muito.

Opções para gerenciar o acesso às instalações?

- Guardas de segurança;
- Gerenciamento eletrônico de acesso.

Gestão de Acesso

Medidas Adicionais ao Guardas

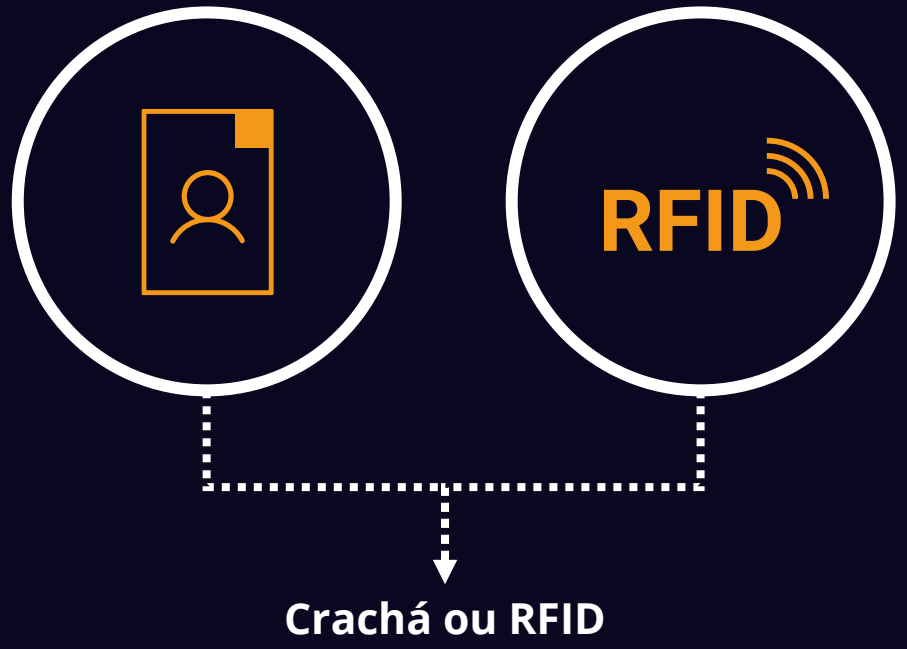


Gerenciamento Eletrônico de Acesso

Gerenciamento de acesso eletrônico

Recomendação

- Colocar uma foto no cartão;
- Não coloque o nome da empresa ou logotipo;
- Exija que funcionários e visitantes usem o crachá em um lugar visível;



- Algo que você saiba, por exemplo, um código ou uma senha.
- Algo que você possui, por exemplo, um cartão ou outro dispositivo;
- Algo que seja parte de você (biometria), tal como uma impressão digital ou uma varredura de íris.

Outras Medidas de Segurança Física

Para autenticação:

- Equipamentos biométricos (cuidado com a GDPR);
- Impressões digitais;
- Leitura das retinas e íris oculares;
- Padrões de voz, faciais e medidas da mão.

Características biométricas podem ser divididas:

- Fisiológicas: forma do corpo;
- Comportamentais: comportamento de uma pessoa.

Mais medidas:

- Inspecionar pertences pessoais, se necessário;
- Inspecionar na entrada e na saída;
- Registro de visitantes (onde, data e hora de entrada e saída).

Protegendo Escritórios, Salas e Instalações

Objetivo:

Manter pessoas não autorizadas longe dos locais onde os ativos estão localizados.

Não adianta só “esconder”!

- Adicione medidas adicionais (propósito de um local);
- Não seja possível ouvir do lado de fora;
- Proteção do telefone em salas seguras;
- Proteção de janelas para assuntos confidenciais;
- Sala contra qualquer radiação eletromagnética para informações processadas eletronicamente.

Monitoramento de Segurança Física

Objetivo:

Monitorar continuamente o acesso físico não autorizado, caso contrário, por exemplo, uma câmera seria inútil!

Sensores para detectar intrusões:

- Detecção passiva de infravermelho (temperatura);
- Câmeras que registram imagens e realizam verificações;
- Detecção de vibração;
- Sensores de quebra de vidro;
- Contatos magnéticos para porta ou janela abertas.

Importante:

- Acompanhar detecções para minimizar danos;
- Sensores conectados a um sistema de detecção com um bom monitoramento;
- Sistemas que podem entrar em contato com terceiros;
- Investigar a causa quando um alarme é acionado;
- Registro deve ser mantido de todos os alarmes;
- Câmeras causam um efeito dissuasor (preventivo).

Proteção Contra Ameaças Físicas e Ambientais

Objetivo:

Prevenir ou reduzir as consequências de eventos originados de ameaças físicas e ambientais.

Proteger do quê?

- Incêndios;
- Inundações;
- Surtos elétricos;
- Explosões, etc.;

Peça ajuda para especialistas com:

- Terreno (topografia local);
- Clima;
- Ameaças urbanas;
- Faça uso de uma avaliação de riscos para avaliar!!

Trabalhando em Áreas Seguras

Objetivo:

Criar áreas seguras, como: áreas especiais para fornecedores pegarem e entregarem mercadorias.

Outras medidas:

- Proibir equipamentos de gravação e eletrônicos;
- Revisar periodicamente áreas seguras desocupadas;
- Protegem muito bem a porta da frente e as áreas de carga;
- Evitar o trabalho não supervisionado em áreas seguras;
- Trancar fisicamente e inspecionar periodicamente as áreas seguras vazias.

OBRIGADO

CONTROLES FÍSICOS DA SEGURANÇA DOS PERÍMETROS

academy

CONTROLES FÍSICOS DE EQUIPAMENTOS

Mesa Limpa e Tela Limpa

Política de mesa limpa:

- Materiais sensíveis protegidos;
- Nenhuma informação deve ser deixada em uma mesa após o expediente de trabalho;
- Informações devem ser armazenadas em algo que possa ser trancado;
- Não deixar impressões na impressora (código PIN para liberar a impressão).

Política de tela limpa:

- Bloquear a tela ao sair do local de trabalho:
  - ✓ "Tecla do Windows + L“;
  - ✓ Ou bloqueio configurado automaticamente.
- Encerrar sessões ativas quando concluídas;
- Fazer logout de aplicativos ou serviços de rede quando não forem mais necessários;
- Bloqueio com proteção de tela com senha.

Localização e Proteção do Equipamento

inclui a proteção de equipamentos por meio:

- Controle climático (ar-condicionado, umidade do ar);
- Uso de extintores de incêndio especiais;
- Fornecimento de energia "limpa“ e filtrada.

Depende do tipo de sala:

- Tamanho, tipo de parede, altura, conteúdo.

Métodos mais comumente utilizados:

- Detecção passiva por infravermelho (Se o sistema de detecção de intrusos disparar um alarme, uma resposta imediata é necessária);
- Salas separadas podem ser usadas para armazenar materiais sensíveis;
- O acesso a salas especiais deve ser monitorado;
- Mídias como fitas de backup não devem ser armazenadas em salas de rede.

Salas Especiais

Entrega e retirada segura, evitando o acesso:

- À empresa;
- Às informações
- Aos funcionários da empresa.

Sala de armazenamento de materiais sensíveis:

- Informações;
- Medicamentos;
- Ou artigos caros.

Sala de Servidores:

- Equipamentos sensíveis;
- Vulneráveis à umidade e ao calor;
- Fonte de energia independentes;
- A sala do servidor não é um armazém;
- Fitas de backup NÃO!

Proteção de Salas Especiais

Sistema de Refrigeração:

- Desumidificado;
- Filtrado;
- Calor jogado para fora.

Energia de emergência:

- Baterias e UPS;
- Geradores.

Umidificador e Desumidificador:

- Cuidado com o uso da água para esfriar equipamentos.

Sistemas contra Incêndio:

- Detectores e alarmes contra fumaça;
- Tipos certos de extintores de incêndios;
- Nenhuma embalagem deve ser armazenada nessas salas;
- Cabos resistentes ao fogo.

Armários Resistentes ao Fogo e Armários de Segurança

Armários

X

Cofres

Armário não é particularmente resistente ao fogo e armários resistentes ao fogo não são cofres.

- Maneira mais simples de armazenar;
- De preferência à prova de fogo;
- Armazenar fitas de backup, documentos em papel e dinheiro;
- Trancados com chave;
- Podem ser facilmente arrombados.

Proteção Contra Umidade

Salas de impressoras, redes, etc. devem ser controladas e monitoradas.
Essas salas não devem conter umidade.

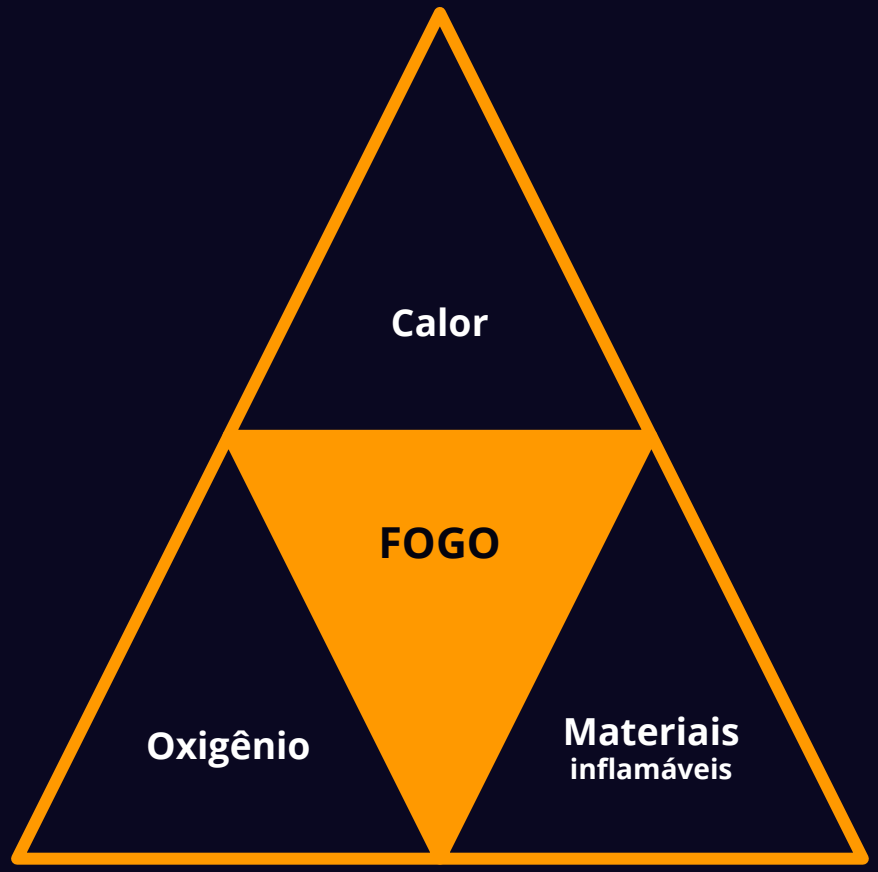
- Ações:
  - ✓ Ar deve ser desumidificado;
  - ✓ Atenção à tubulação de agua;
  - ✓ Vazão do ar-condicionado;
  - ✓ De refrigeração;
  - ✓ Atenção aos sistemas de resfriamento;
  - ✓ E os antigos mainframes?

Proteção Contra Incêndio

Existem requisitos obrigatórios.
Medidas devem ser tomadas o tempo todo. Ameaça de fogo pode ocorrer a qualquer momento.

- Incêndios podem começar com:
  - ✓ Curtos-circuitos;
  - ✓ Ação humana;
  - ✓ Equipamentos com defeito, etc.
- Ações em salas:
  - ✓ Manter nível baixo de oxigênio;
  - ✓ Claramente marcadas e, com instruções para trabalhar nelas.
- Danos causados por:
  - ✓ Queima do material, calor excessivo ou à fumaça;
  - ✓ Dano do material usado para extinguir o fogo.
- Medidas de Proteção:
  - ✓ Limitar o fumo;
  - ✓ Manter o mínimo de materiais inflamáveis, como papel.

Sinalização



Importante:

- Para sinalizar a presença de incêndio, geralmente são usados detectores de fumaça;
- Verificar regularmente os detectores de fumaça;
- Realizar regularmente treinamentos de incêndio e evacuação (familiarizar com o som).

Agentes Extintores de Incêndio

Os vários agentes extintores de fogo são:

Gases inertes (um gás que suprime o oxigênio), tais como: dióxido de carbono, argônio (gás nobre), INERGEN (nome comercial) e Argonite (nome comercial).

Espuma (à base de água, não é adequado para a eletricidade);

Pó (adequado para a eletricidade);

Água (não é adequado para a eletricidade);

Areia (apropriado para o petróleo e seus derivados).

Segurança de Ativos Fora das Instalações

O que entender sobre "ativos fora das instalações"?

- Usado fora da organização, por exemplo:
  - ✓ Dispositivo móvel usados em viagem;
  - ✓ BYOD, em home office ou ATMs.

Itens inclusos na PSI quanto equipamentos ou mídias:

- ✓ Orientações quando deixados sem vigilância (um laptop no carro);
- ✓ Orientações do fabricante sobre o manuseio;
- ✓ Manter um registro de quem possui quais equipamentos/ativos;
- ✓ Como lidar com os ativos, dependendo da localização física (casa, em trânsito, etc.);
- ✓ Controles de proteção física;
- ✓ Política para dados usados/armazenados por tipo de mídia (disco criptografado, telefone celular, pendrive);
- ✓ Uso aceitável, quanto ao comportamento do usuário final;
- ✓ Treinamento obrigatório de segurança para novos funcionários.

Mídias de Armazenamento

Objetivo:

Evitar que informações valiosas em mídias (papel, CDs, DVDs, pen drives, HD, fitas de backup, smartphone, etc.) caiam em mãos erradas.

O que poderia constar em uma política:

- Autorização e rastreamento de auditoria (quem possui o quê e por quê);
- Regras de armazenamento;
- Medidas criptográficas para proteger informações;
- Proteção contra perda de informações, ex: podem se perder com o tempo devido à degradação;
- Registro das mídias;
- Backup de informações em mídias;
- Bloqueio do uso de determinadas portas nos equipamentos de computador.

Descarte Seguro

Objetivo:

Evitar vazamento de informações do equipamento a ser descartado ou reutilizado.

A forma como as mídias devem ser tratadas:

- Geralmente está relacionada à classificação;
- Por meio de procedimentos documentados.

Consideração sobre o descarte:

- Após o término do prazo de armazenamento, as mídias são trituradas ou destruídas;
- Solicite ajuda a empresa certificada;
- Esvaziar pendrives usando uma ferramenta de "limpeza" que destrói os dados de forma segura;
- Mídias não podem simplesmente ser jogadas no lixo;
- Podem ser reciclados (com o disco rígido adequadamente limpo).

Descarte Seguro ou Reutilização de Equipamentos

Tipos de mídias:

- ✓ Smartphones;
- ✓ Pen drives, cartões de memória;
- ✓ Laptops;
- ✓ Impressoras podem armazenar informações.

Considerações:

- A exclusão de informações confidenciais de mídias quando uma pessoa deixa a organização;
- Funcionários que deixam a empresa, devolvem todos os equipamentos e excluem as informações;
- Procedimentos para equipamentos perdidos ou roubados;
- Criar processo de destruição e criptografia.

Transporte Seguro

As mídias que precisam ser transportadas precisam de proteção!

Considere o seguinte:

- Precisam de proteção de acordo com sua sensibilidade;
- Protegida com base nas informações contidas nelas;
- Utilize serviços de courier aprovados;
- Embale as mídias de forma inviolável;
- Embale de acordo com as propriedades físicas (por exemplo, fitas devem ser protegidas eletricamente e contra calor).

Energia de Emergência

Objetivo:

Evitar perda, dano, interrupção ou comprometimento de informações e outros ativos associados.

Medidas:

- Várias fontes de energia independentes;
- Pacotes de bateria (substituídas a cada 4 anos);
- Sistema de Alimentação Ininterrupta (UPS) que ajusta as flutuações e absorve quaisquer picos;
- Gerador de emergência (testado e abastecido).

Refrigeração

O ar precisa ser resfriado e o calor produzido pelos equipamentos deve ser dissipado.

- Esse ar também é desumidificado;
- Ele deve ser filtrado;
- Cuidado ao adicionar novos equipamentos;
- Atenção na capacidade de resfriamento das salas.

Segurança de Cabeamento

Objetivo:

Evitar perda, dano, roubo ou comprometimento de informações e outros ativos associados.

Medidas:

- Os cabos devem ser instalados separadamente para evitar interferência;
- Separar os cabos de rede da energia;

- Os efeitos muitas vezes não são visíveis ou audíveis (telefones celulares causam interferência em alto-falantes ou rádios);
- Os dutos de cabos devem ser protegidos;
- Usar fontes de alimentação separadas em salas de servidores;
- Usar duas fontes de alimentação, cada uma conectada a seu próprio grupo de energia.

Manutenção de Equipamentos

Objetivo:

Evitar perdas, danos, roubos ou comprometimento de informações e outros ativos associados por falta de manutenção.

Medidas:

- Manutenção deve ser realizada apenas por pessoal autorizado;
- Equipe com treinamento e que conheça as diretrizes do fabricante;
- Usar medidas antiestáticas, como uma pulseira aterrada e uma superfície aterrada;
- Estar ciente dos requisitos decorrentes das políticas da apólice de seguro;
- Inspecionar e testar os equipamentos antes de introduzi-los no ambiente operacional;
- Criar plano de teste deve ser elaborado e avaliado para ativos importantes.

OBRIGADO

CONTROLES FÍSICOS DE EQUIPAMENTOS

academy

Dispositivos Endpoint

Dispositivos Endpoints

O que é um endpoint de segurança?

- Uma extremidade de um canal de comunicação;
- Chamado também de dispositivo terminal;
- Pode ser um celular, laptop, notebook;
- É muito mais que um hardware, contêm software e dados.

Proteção de endpoint:

- Muitos incidentes ocorrem envolvendo o endpoint;
- Segurança redobrada quando usados fora das instalações ou no transporte;
- Notebooks são roubados de carros todos os dias;
- Nunca deixar dispositivos importantes sem supervisão;
- Evitar armazenar informações sensíveis;
- O ladrão sabe identificar uma bolsa de notebook;
- Difícil obter seguro contra esse tipo de perda;
- Se possível, deixe o endpoint na empresa.

Dispositivos Endpoint do Usuário

Medidas de Segurança:

- Adote uma política de segurança que descreva:
  - ✓ Tunelamento;
  - ✓ Proteção contra malware;
  - ✓ Controle de acesso;
  - ✓ Restrição de instalação de software;
  - ✓ Criptografia, backups e atualizações;
  - ✓ Treinamento do usuário e etc.
- Os usuários NÃO devem usar seus dispositivos móveis em locais públicos e desprotegidos;
- Se for permitido o trabalho remoto, é necessário ter uma política específica.

Considerações sobre Dispositivos Endpoint do Usuário

Considerações no uso remoto do Endpoint:

- Benefícios sejam alcançados sem aumentar o risco;
- Permita com base em uma avaliação dos riscos:
  - ✓ O riscos podem ser diferentes em cada caso;
  - ✓ Dependendo do local e da criticidade dos ativos;
  - ✓ Pode exigir uma avaliação de risco individualmente.
- Muitos dos controles em um ambiente físico estarão ausentes em um local de teletrabalho;
- Comportamento doméstico em vez de profissional;
- Providencie equipamentos na organização também;
- Software e o equipamento precisam ser licenciados;
- Meios para continuar a trabalhar em caso de falha;
- Garantir instalações no local de trabalho remoto;
- Incluir armazenamento seguro e trituradoras.

Política de Trabalho Remoto

O que considerar?

- Autorização;
- Fornecimento de equipamentos;
- Segurança das informações durante o trabalho remoto;
- Uso de equipamentos de trabalho remoto;
- Encerrar sessões ativas quando concluídas;
- Encerrar o acesso a aplicativos ou serviços de rede quando não forem mais necessários;
- Bloquear a tela/acesso por um mecanismo seguro, por exemplo, um protetor de tela protegido por senha.

Instalação de Software em Sistemas Operacionais

Como evitar a exploração de vulnerabilidades em SO?

- Manutenção do software operacional pelos usuários finais não deve ser permitida;
- Atualizações apenas por administradores treinados e com autorização;
- Instalação e atualização somente após testes extensivos e bem-sucedidos;
- Pensar em uma estratégia de reversão (rollback).

Programas Utilitários

Qual a finalidade?

- Ajuda na execução do S.O. e na manutenção geral do sistema;
- Executa uma tarefa específica com funções úteis, como formatação, compactação, digitalização, exploração etc.

Tarefas comuns realizadas por Programas Utilitários

Desfragmentação de disco;

Limpeza de disco;

Gerenciamento de arquivos;

Backup;

Depuradores.

Tarefas dos Programas Utilitários

Tarefas comuns realizadas por Programas Utilitários

Ferramenta de Diagnóstico;

Monitoramento de rede;

Compressão;

Gerenciamento de Disco;

Antivírus;

Firewall;

A maioria dos endpoints tem um ou mais programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações!

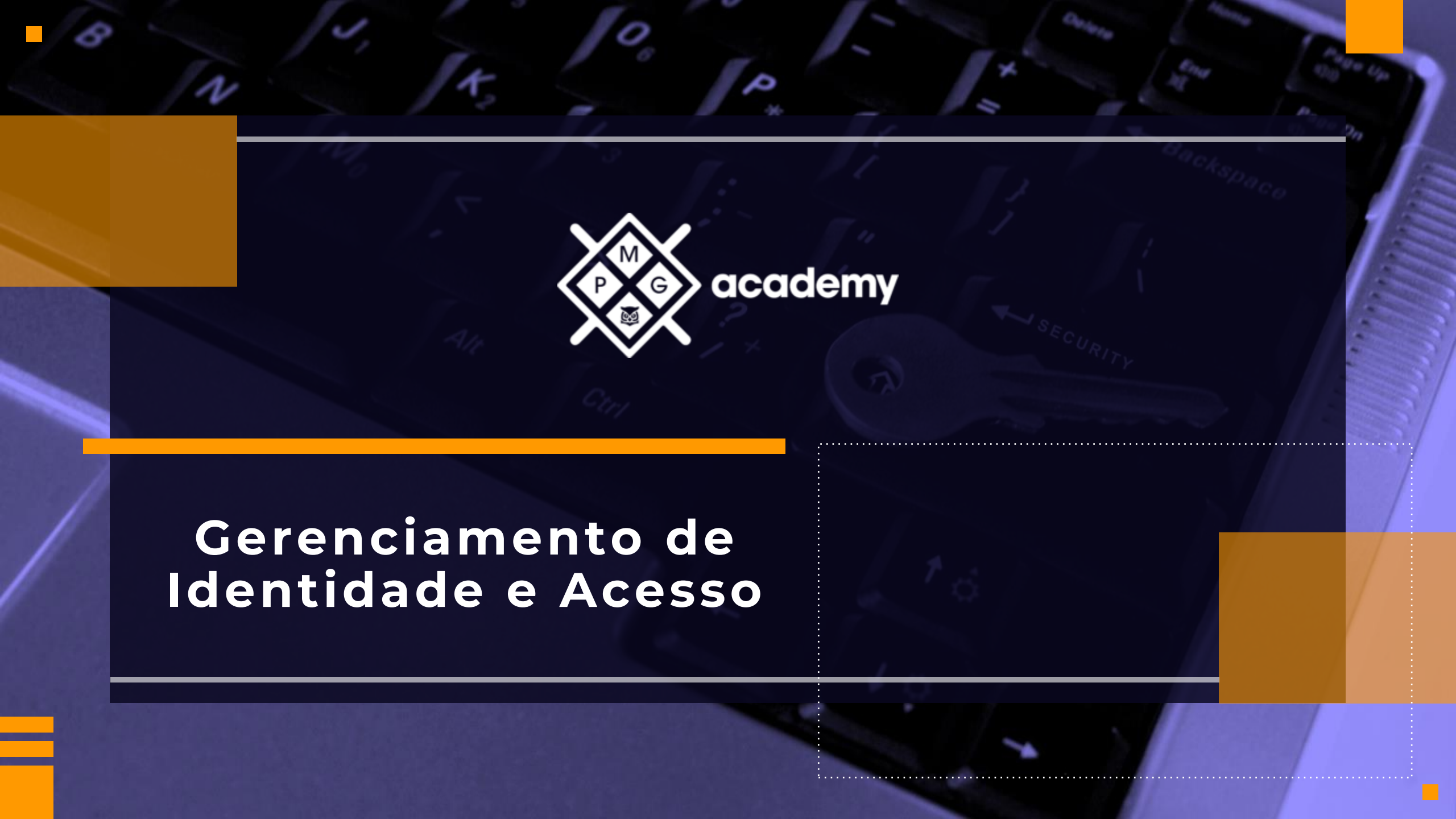
Uso de Programas Utilitários Privilegiados

Como evitar que os utilitários prejudiquem os sistemas e substituam os controles?

- Limitar o uso desses programas somente a usuários autorizados;
- Usar procedimentos de identificação, autenticação e autorização;
- Definição e documentação dos níveis de autorização;
- Remover ou desabilitar todos os programas utilitários desnecessários;
- Segregação de funções.

OBRIGADO

Dispositivos
Endpoint



Gerenciamento de Identidade e Acesso

Privilégios de Acesso Especiais

Para evitar que ativos sejam acessados por usuários não autorizados:

- Registro e remoção de usuários;
- Provisão de acesso de usuários;
- Gerenciamento de privilégios de acesso especiais;
- Gerenciamento das informações de autenticação secreta dos usuários;
- Revisão dos direitos de acesso dos usuários;
- Remoção ou ajuste dos direitos de acesso;
- Registro deve estar em vigor.

Os direitos de acesso privilegiados são direitos de acesso concedidos a uma conta que um usuário comum não pode e não deve realizar!

- Para conceder acesso a usuários autorizados (privilegiados): Identificação / Autenticação / Autorização.

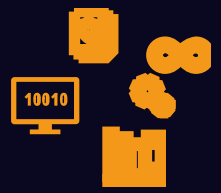
Restrição de Acesso à Informação

Considerações:

- Equilibrar: Restringir X Liberar;
- No login, não fornecer informações para o atacante:
  - ✓ Nome de usuário;
  - ✓ Sobre o sistema ou aplicativo;
  - ✓ O que deu errado no login.

- Mensagem pode ser exibida após o login bem-sucedido:
  - ✓ Informando o último login;
  - ✓ Tentativas mal sucedidas.
- Usar um sistema de gerenciamento de senhas;
- Limitar o uso de programas utilitários privilegiados (nas mãos de um usuário sem habilidades pode ser perigoso).

Acesso ao Código Fonte



O que proteger?

- Projetos de alto nível;
- Requisitos;
- Especificações;
- Planos de teste;
- Propriedade intelectual.

Considerações:

- O acesso ao código-fonte deve ser baseado apenas em necessidades;
- O registro de auditoria deve estar em vigor;
- Monitorar todas as alterações no código-fonte.

Autenticação Segura

Objetivo:

Garantir que um usuário ou uma entidade seja autenticado com segurança quando o acesso a sistemas, aplicativos e serviços é concedido.

Como manter seguro a autenticação?

- Nenhuma parte da informação deve ser revelada (usuário e senha);
- Usar asteriscos na senha e criptografar;
- Autenticações devem ser acompanhadas por autenticação multifator:

O que você sabe;

O que você tem;

O que você é.

Dicas de Senhas Seguras

- Pelo menos doze caracteres. Quanto mais longa, melhor;
- Use uma combinação de letras maiúsculas, minúsculas, números e caracteres especiais (@, #, &, ?, !, +, -, €, %, etc.);
- Frase de acesso (em vez de uma senha), que consiste em quatro ou mais palavras escritas juntas;
- Não use informações pessoais na senha;
- Não use palavras óbvias, muito menos palavras que possam ser associadas a você (como hobbies);
- Verifique se a senha aparece em listas de senhas invadidas;
- Use uma senha diferente para cada serviço.

Gerenciador de Senhas

Se você usa uma senha única para cada serviço, é difícil lembrar todas essas senhas!

O que fazer então?

- Escrever em um papel e guardar em um local seguro (?);
- Usar um sistema de “cofre” (Gerenciar de Senhas) como plugin no navegador, smartphone etc.;
- Muitos gerenciadores de senhas alertam quando sua senha aparece em uma lista de senhas invadidas ou fracas.

OBRIGADO

Gerenciamento de Identidade e Acesso

Proteção Contra Malware

Malware:
Um Software Malicioso

- Malware é uma combinação das palavras Malicioso e Software;
- Trata-se de um software indesejado, como vírus, worms, Cavalos de Troia e spywares;
- A solução padrão contra malwares é fazer varreduras com um antivírus e usar um firewall;
- As ações humanas (abertura de e-mails suspeitos ou de remetentes desconhecidos) podem ativar um Malware;
- Medidas adicionais:
  - ✓ Gerenciamento técnico de vulnerabilidades;
  - ✓ Medidas protetivas para arquivos e software de redes;
  - ✓ Validação automatizada de software e dados;
  - ✓ Verificação antes do uso e antes de abrir páginas da web.
- Cada usuário deve ser treinado para reconhecer comportamentos estranhos.

Phishing

- Phishing é uma forma de fraude na internet;
- Pode levar à instalação de um malware (cuidado com links);
- Disfarçado como uma entidade confiável para atrair;
- Típico exemplo de técnica de engenharia social;
- Geralmente a vítima recebe um e-mail pedindo para verificar ou confirmar dados bancários.

Às vezes mensagens SMS são usadas.

Até mesmo contato telefônico é utilizado.

Proteção
Contra Phishing

Desafio:

Como saber se a mensagem é real ou phishing?

Medidas:

- Verifique o remetente do e-mail (passe o mouse sobre o nome do remetente);
- Muitas vezes, a linguagem ou o layout da mensagem também fornecem uma indicação;
- Se houver muitos erros de ortografia ou gramática, ou se o e-mail parecer desleixado;
- Considere se o meio usado é uma escolha lógica para o remetente suspeito (Receita Federal);
- Entre em contato com o remetente suspeito por outro meio (telefone ou pelas redes sociais).

Ransomware

Definição:

- Sequestro de informação (criptografados) e liberação mediante pagamento de resgate;
- Impactos gigantescos na imagem da empresa;
- A ideia de exigir um resgate é bastante antiga;
- Nos dias atuais ficou mais comum por conta do Bitcoin (anonimato).

Medidas:

- Antes de clicar em um link, verifique a fonte;
- Realize varreduras regulares de vulnerabilidade para limitar a superfície de ataque;
- Realizar backups é a melhor opção;
- Denuncie às autoridades policiais federais por meio do IC3 ou a uma delegacia de polícia local;
- Mantenha a calma e atualize regularmente o software e o S.O.;
- Os atacantes frequentemente exploram vulnerabilidades conhecidas do software.

Exemplo: Clop Ransomware

- “Clop" é uma das ameaças de ransomware mais recentes e perigosas;
- Frequentemente mira usuários do MS Windows;
- Antes de iniciar o processo de criptografia, ele bloqueia mais de 600 processos do MS Windows;
- Desativa várias aplicações do MS Windows 10;
- Desativa o Microsoft Windows Defender e o Microsoft Security Essentials;
- Atualmente mira redes inteiras;
- Caso: Universidade de Maastricht, na Holanda, teve quase todos os dispositivos MS Windows da rede criptografados e forçados a pagar um resgate.

Exemplo: Ransomware Oculto

- É oculto porque trata-se de falsas atualizações do MS Windows;
- Os hackers enviam emails solicitando a instalação de atualizações urgentes do MS Windows;
- Na verdade são arquivos executáveis de ransomware disfarçados;
- O ransomware contido nesses emails é conhecido como "Cyborg“;
- Ele criptografa todos os arquivos e programas e exige pagamento de resgate para descriptografar;
- Infelizmente, muitos provedores de serviços de email e software antivírus básico não são capazes de detectar e bloquear esses emails;
- Use um antivírus que forneça segurança adequada na internet.

Exemplo: Zeus Gameover

- Faz parte da família de malware e vírus "Zeus“ (Trojan) - um malware disfarçado de algo legítimo;
- Acessa os detalhes sensíveis da sua conta bancária e rouba todos os fundos;
- Não requer um servidor centralizado de "Comando e Controle" para concluir transações;
- Criar servidores independentes da qual não se consegue rastrear seus dados roubados.

Exemplo: Notícias

- Utilizam notícias atuais e eventos globais para direcionar pessoas com malware;
- Exemplo: hackers utilizando a onda do surto de COVID-19 (Coronavírus);
- Os hackers enviam e-mails disfarçados de informações legítimas sobre o surto;
- Os leitores são induzidos a clicar em um link para obter mais informações;
- O link contém malware que copia os arquivos em seu dispositivo e rouba suas informações pessoais.

Exemplo: Dispositivos IoT

Razões pelas quais os hackers escolhem direcionar dispositivos IoT:

- A maioria não possui armazenamento suficiente para instalar medidas de segurança adequadas;
- Contêm dados de fácil acesso, como senhas e nomes de usuários;
- Podem usar câmeras e microfones na Internet para espionar e se comunicar com pessoas (babás eletrônicas inteligentes);
- Esses dispositivos também podem ser pontos fracos na rede de uma empresa;
- Por meio de dispositivos IoT desprotegidos – espalha-se malware para outros dispositivos na rede.

Spam

- Spam é nome para o coletivo de mensagens indesejadas;
- O termo é normalmente utilizado para e-mails indesejados;
- Gera um custo enorme para o destinatário;
- Nem sempre é falso, como no Phishing;
- Um filtro de spam pode diminuir esse problema;
- Relate, bloqueie e exclua mensagens de spam;
- Use e-mails temporários em fóruns, por exemplo.

Nunca responda uma mensagem de spam, até mesmo para cancelar a inscrição;

Criar uma lista de permissões de e-mail;.

Vírus

Definição:

- Pequeno programa que se multiplica propositalmente, às vezes em formas alteradas;
- Para que o vírus se espalhe é necessário um programa que contenha um código executável.

Explicação:

- Assim que o programa é executado, o vírus procura novos programas para tentar infectá-los;
- Um vírus só se espalhar se um usuário transferir arquivos infectado para um novo sistema;

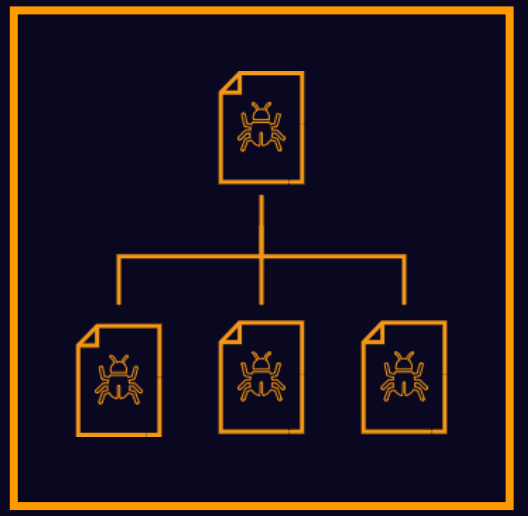
- Os hóspedes dos vírus eram apenas programas, mas atualmente podem ser documentos (macros, VBScript ou ActiveX);
- Exemplos: O vírus Brain (1986) / Chernobyl (1998) / ZEUS (2014~) / Cryptolocker (2014) / Locky (2016) / WannaCry (2017) / Petya (2017).

Medidas contra Vírus

Medidas:

- Atualizações do S.O. e programas do usuário final;
- Endurecimento do computador removendo software e funções não utilizados;
- Scanner de vírus no servidor de e-mail e nos computadores individuais;
- Scanner de vírus com definições atualizadas;
- Inclua o assunto de vírus em uma campanha de conscientização sobre segurança;
- Inclua esse assunto na política de segurança da informação da organização;
- Maneiras eficazes de relatar incidentes e que haja bons procedimentos de acompanhamento.

WORM



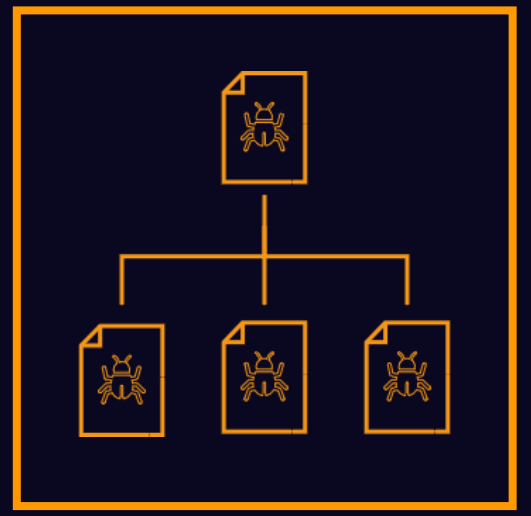
Definição:

- Pequeno programa que se multiplica intencionalmente;
- O resultado da multiplicação são cópias do original;
- Se espalham por outros sistemas, fazendo uso dos recursos de rede do seu hospedeiro.

Explicação:

- As diferenças entre vírus e worms estão se tornando cada vez mais tênues;
- Um vírus depende da ativação do usuário, o worm não;
- O worm se espalha e é ativado automaticamente em um curto período de tempo;
- Ambos dependem de um código executável;
- Exemplos: Blaster (2003) / Storm Worm (2007) / Stuxnet (2010) / Mirai (2016).

Medidas contra Worm



Medidas:

- Tenha um scanner (de vírus) no servidor de e-mail e nos computadores individuais;
- Tenha o scanner de vírus com definições atualizadas;
- Garanta que as últimas atualizações para o computador e equipamentos de rede estejam instaladas;
- Ferramenta de monitoramento de rede;
- Inclua o assunto em uma campanha de conscientização sobre segurança e na PSI;
- Maneiras eficazes de relatar incidentes e bons procedimentos de acompanhamento.

Cavalo de Troia

Definição:

- Programa que executa atividades secundárias sem que o usuário do computador perceba;
- Pode prejudicar a integridade do sistema infectado.

Explicação:

- À primeira vista, se apresenta como algo útil, mas, quando é ativado, realiza atividades indesejadas;
- Muitas vezes instala uma "backdoor", para ter acesso não autorizado ao sistema infectado;
- Pode enviar informações confidenciais para outro local onde serão recolhidas e analisadas;
- Diferente do vírus e Worms, o Cavalo de Troia não pode se replicar, por isso permanece despercebido por um longo período de tempo;
- Exemplo: BackOrrifice (2000) / Netbus (1998) / Sub7 (1999) / Storm Worm (2007) / Emotet (2018).

Medidas contra Cavalo de Troia

Medidas:

- Scanner de trojans e/ou vírus no servidor de e-mail e nos computadores individuais;
- Scanner de vírus está atualizado regularmente;
- Últimas atualizações para o S.O. e programas utilizados pelos usuários estejam instaladas;
- Considere a otimização do computador removendo software e funções não utilizadas;
- Inclua o assunto de cavalos de Troia em uma campanha de conscientização sobre segurança;
- Inclua esse assunto na PSI;
- Ferramentas de monitoramento de rede;
- Firewall pessoal no próprio local de trabalho para detectar tráfego de rede suspeito;
- Formas eficazes de relatar incidentes e que haja bons procedimentos de acompanhamento.

HOAX

Definição:

- Uma hoax (em tradução literal, “boato”, “embuste” ou “mentira ardilosa”);
- Uma forma de engenharia social;
- Mensagem que tenta convencer o destinatário de sua veracidade;
- Em seguida, levar o leitor a realizar uma determinada ação;
- A disseminação depende dos leitores enviarem deliberadamente a mensagem para outras vítimas.

Explicação:

- A carga de uma hoax não é de natureza técnica, mas, sim, psicológica;
- Ao jogar com as emoções das pessoas, a hoax tenta convencer o leitor a compartilhá-la com outros);
- Exemplo: Good times (1994) / Pen Pal (Greetings) (2000) / Olympic Torch (2006) /Relacionados ao coronavírus (2020).

Medidas contra Hoax

Medidas:

- Scanner de vírus no local de trabalho e uma solução anti-spam para o servidor de e-mail;
- Um hoax frequentemente contém textos que podem ser reconhecidos por esses scanners;
- Assunto de boatos em uma campanha de conscientização sobre segurança;
- Inclua esse assunto na PSI;
- Formas eficazes de relatar incidentes e que haja bons procedimentos de acompanhamento.

Bomba Lógica

Definição:

- Pedaço de código que é construído em um sistema;
- Este código irá, em seguida, executar uma função quando reunir condições específicas.

Explicação:

- Os gatilhos detonam depois que uma condição é atendida;
- Ou os gatilhos lançam uma bomba lógica quando uma condição não for atendida;
- Bombas lógicas, muitas vezes, contêm malwares, que normalmente demoram algum tempo para serem “detonadas”, ou seja, para que se propague.

Medidas:

- Para softwares desenvolvidos por funcionários da empresa ou sob contrato com terceiros, realize uma análise minuciosa do código por outra parte.

Spyware

Definição:

- Programa que recolhe informações sobre o usuário e as encaminha para terceiros, com fins lucrativos;
- Não prejudica o computador e/ou o software instalado, mas, viola a privacidade do usuário.

Explicação:

- Um Spyware pode ser reconhecido através de diversas maneiras, por exemplo:
  - ✓ O computador está mais lento do que de costume;
  - ✓ Programas estão sendo executados sem terem sido iniciados ou vistos antes;
  - ✓ Há uma nova barra de ferramentas no seu navegador e você não consegue removê-la;
  - ✓ Vários tipos de pop-ups aparecem sem mais nem menos.

Medidas contra Spyware

Medidas:

- Varreduras dos registros do Windows por chaves suspeitas de registros;
- Muitos programas antivírus também detectam spywares;
- Use um firewall para detectar o tráfego da rede de um computador sem nenhum motivo aparente;
- O assunto sobre spywares está incluído nas campanhas de conscientização e PSI;
- Formas eficazes de relatar incidentes e bons procedimentos de follow-up.

Botnet

Definição:

- Combinação das palavras robot e network, com uma conotação negativa ou maliciosa;
- Programas conectados a outros similares, via internet, a fim de realizar tarefas no computador de alguma pessoa.

Explicação:

- Esses programas se comunicam por vários canais para enviar e-mails de spam ou DDoS;
- É possível se tornar parte de um botnet clicando em um link em um e-mail, página da web ou anexo;
- Muitas vezes podem ser baixados sem qualquer noção do usuário;
- Quando um computador se torna um bot, ele se torna uma espécie de “zumbi”, recebendo ordens;
- Quando o computador se torna uma botnet, é mantida uma conexão com um servidor de comando e controle.

Medidas contra Botnet

Medidas:

- Software no local de trabalho esteja regularmente atualizado;
- Scanners que verificam o Registro do Windows em busca de chaves de registro suspeitas;
- Às vezes, programas antivírus também podem detectar atividade de worms;
- Firewall pessoal para detectar tráfego de rede suspeito;
- Ferramentas de monitoramento de rede;
- Assunto incluso em uma campanha de conscientização sobre segurança;
- Assunto na incluso na PSI;
- Formas eficazes de relatar incidentes e que haja bons procedimentos de acompanhamento.

Rootkit

Definição:

- Conjunto de ferramentas de software que são usadas por um terceiro (normalmente um hacker);
- Usado após ter obtido acesso a um sistema (computador);
- O rootkit se esconde com profundidade no S.O., fazendo com que este se torne instável;
- É quase impossível remover um rootkit sem danificar o sistema operacional;
- O propósito é criar e esconder arquivos, conexões de rede, endereços de memória e entradas de índice.

Rootkit

Explicação:

- Rootkits podem trabalhar em dois níveis: nível do kernel e nível do usuário;
  - ✓ Kernel: pode fazer quase qualquer coisa no sistema. O objetivo é ler, alterar ou influenciar os processos em execução, dados ou arquivos do sistema;
  - ✓ No nível do usuário são limitados a segmentos específicos da memória.
- Um rootkit ajuda o intruso a obter acesso ao sistema sem a consciência do usuário;
- Existem rootkits para quase todos os sistemas operacionais.

Medidas contra Rootkit

Medidas:

- Garantir que os softwares sejam atualizados regularmente, assim com o antivírus;
- Scanners que inspecionem o registro do Windows;
- Usar programas que podem detectá-los na memória;
- Assunto incluso em uma campanha de conscientização sobre segurança;
- Assunto na incluso na PSI;
- Formas eficazes de relatar incidentes e que haja bons procedimentos de acompanhamento.

OBRIGADO

Proteção Contra Malware

SEGURANÇA EM REDES E COMUNICAÇÕES

Segurança de Redes

Importante:

- A rede é a espinha dorsal da maioria, se não de todos, os sistemas de informação;
- Ter acesso a uma rede não é a mesma coisa em ter acesso aos sistemas;
- Impressoras na rede contém HD;
- Responsabilidades e procedimentos no gerenciamento de equipamentos de rede devem ser estabelecidos;
- Aplicativos protegidos individualmente podem conter vulnerabilidades se acessos via rede;
- Limitar o acesso dos sistemas à rede para o mínimo necessário;
- Realizar verificações regulares para identificar quais sistemas estão conectados e por quê;
- Desabilitar protocolos de rede vulneráveis.

Controles
Segurança de Redes

O que considerar ao proteger as informações em redes?

- Medidas para proteger a confidencialidade e integridade dos dados transmitidos;
- Controles ao se conectar a uma rede sem fio e/ou pública;
- Redes sem fio podem não ser capazes de transmitir informações se houver interferência elétrica;
- Monitoramento das redes é importante;
- Detecção de violações de segurança;
- Gerenciamento de incidentes e causa raiz;
- Estreita coordenação entre diferentes redes e serviços de rede de terceiros.

Serviços de Rede

O que é incluído nestes Serviços de Rede?

- Fornecimento de conexões (Gateway, DNS, DHCP, Proxy etc.);
- Serviços de rede sem fio;
- Soluções gerenciadas de segurança de rede, como:

Firewalls;

VPNs;

Sistemas de detecção de intrusão.

Segurança dos Serviços de Rede

Considerações:

- Impedir que usuários não autorizados acessem uma rede;
- Verificar as credenciais;
- Usar certificados digitais;
- Métodos de autenticação do usuário, firewalls;
- Usar sistemas de criptografia;
- Usar protocolos como IPSec.

Segregação de Redes

Propósito:

Dividir a rede em segmentos menores para que o tráfego entre eles sejam mais seguros.

O que é segregar uma rede?

- É dividir em domínios com base em níveis de confiança, criticidade e sensibilidade:
  - ✓ Domínio de acesso público;
  - ✓ Domínio de desktop;
  - ✓ Domínio de servidor;
  - ✓ Sistemas de baixo e alto risco;
  - ✓ De unidades organizacionais, como RH, finanças, marketing;
  - ✓ Ou alguma outra combinação.
- Segmentação de rede seja aplicada com base em políticas para evitar interrupções.

Tipos de Redes

Intranet

- Rede privada (colaboração);
- Por meio de uma rede pública (Internet), é possível conectar as partes separadas da intranet;
- Medidas adicionais como criptografia.

Extranet

- Parte da Intranet se torna pública;
- Requer o uso de medidas de proteção e privacidade.

Rede Local

- Barreira construída em torno dos componentes internos;
- O maior perigo é um invasor (hacker) ter a liberdade para agir se conseguir penetrar na rede interna.

Filtragem da Web

Objetivo:

Proteger os sistemas de serem comprometidos por malware e impedir o acesso a sites e recursos não autorizados.

Que tipo de site a organização deve evitar que seu pessoal acesse?

- Que contenham informações ilegais;
- Que contenham vírus;
- Sites maliciosos com conteúdo de phishing ou malware;
- Sites com função de upload de informações;

Como bloquear esses acessos?

- Bloqueando o endereço IP;
- Bloqueando domínio do(s) site(s) em questão;
- Alguns navegadores e tecnologias antimalware fazem isso automaticamente;
- Treinamento ao pessoal sobre o uso seguro e apropriado de recursos online.

OBRIGADO

SEGURANÇA EM REDE E COMUNICAÇÕES

Criptografia

Criptografia

O que é?

- combinação das palavras "kryptós", que significa "oculto", e "gráphein", que significa "escrever“;
- A pesquisa em algoritmos criptográficos também é chamada de criptoanálise;
- Criptografia remontam a tempos antigos;
- A criptoanálise avançou especialmente durante e após a Segunda Guerra Mundial.

Uso de Criptografia

Qual o objetivo da Criptografia?

Confidencialidade:

- ✓ Proteger informações confidenciais ou críticas;
- ✓ Informações armazenadas;
- ✓ Informações transmitidas.

Integridade ou autenticidade:

- ✓ Assinaturas digitais ou códigos de autenticação de mensagens;
- ✓ Para fins de verificação de integridade de arquivos.

Não repúdio:

- ✓ Para evidenciar a ocorrência (ou não) de um evento ou ação.

Autenticação:

- ✓ Ao solicitar acesso;
- ✓ Para realizar transações com usuários, entidades e recursos do sistema.

Política de Criptografia

O uso da criptografia deve ser cuidadosamente considerado e definido em uma política;

Conteúdo de uma Política de Criptografia:

- Limitações legais para a troca de informações entre países;
- Onde a organização deve usar a criptografia;
- Quais tipos de criptografia a organização usa e em quais aplicativos (incompatibilidade);
- Controle e gerenciamento de chaves;
- Cópia de segurança das chaves;
- Controle das chaves, principalmente as públicas;
- Uso indevido de criptografia.

Gerenciamento de Chaves

Criptografia: Gerenciamento de Chaves

- As chaves criptográficas devem ser protegidas contra alteração, perda e destruição;
- Chaves secretas e pessoais precisam ser protegidas contra a divulgação não autorizada;
- Registro dos pares de chaves: quais pares foram emitidos a quem e quando;
- Quando uma chave irá expirar?
- O que deve ser feito quando uma chave for comprometida?
- Evite usar a mesma chave em sistemas diferentes (por exemplo, notebooks);
- A segurança da chave é tão importante quanto a segurança da fechadura.

Exemplos de Sistemas Criptográficos

Simétrico de deslocamento alfabético:

- Cada letra é representada por 1 número
- “ADRIANO” é 1-4-17-9-1-13-14
- A chave secreta é 5, ficando: 6-9-22-14-5-18-19
- “ADRIANO” é a mensagem, “5” é a chave

Características do sistema simétrico:

- A mesma chave é usada tanto pelo receptor quanto pelo remetente;
- A chave secreta deve ser trocada antes da comunicação;
- Isso torna o sistema vulnerável.

Criptografia Simétrica

Simétrico

Como você está?

Criptografia

%RT$@<SW?S<MG_(*

Descriptografia

Como você está?

A mesma chave secreta foi compartilhada

Sistema Assimétrico

Características:

- Resolve a vulnerabilidade envolvida no compartilhamento de uma chave secreta;
- Chaves diferentes são usadas para criptografar e descriptografar;
- O algoritmo funciona com pares de chaves, chamados de chave privada e chave pública.

Usado de 2 formas:

- Assinar uma mensagem com a chave privada; A chave pública certifica o remetente;
- Criptografar mensagens enviadas com a chave pública e lida com a chave privada;
- A chave pública pode ser enviada pelo destinatário ao remetente usando o mesmo canal de comunicação;
- Isso torna o sistema mais seguro.

Criptografia Assimétrica

Simétrico

Como você está?

Criptografia

Chave pública

%RT$@<SW?S<MG_(*

Descriptografia

Chave privada

Como você está?

Diferentes chaves são usadas para criptografar e descriptopgrafar

Infraestrutura de Chave Pública (PKI)

- Não é a mesma coisa que criptografia de chave pública;
- Baseada em chave pública e inclui muito mais do que somente a criptografia;
- Muitas vezes é gerenciada por uma autoridade independente e confiável;
- Fornece garantias referentes a quais pessoas ou sistemas pertencem a uma chave pública específica;
- A força de uma PKI depende em grande parte de aspectos não técnicos:
  - ✓ A forma como um usuário obtém sua chave privada;
  - ✓ Pessoalmente é mais confiável do que por e-mail.

Componentes de Soluções PKI

- Componentes de uma solução PKI:
  - ✓ Autoridade Certificadora (CA) – Emite o certificado;
  - ✓ Autoridade Registradora (RA) – Verifica as credenciais.

Passos:

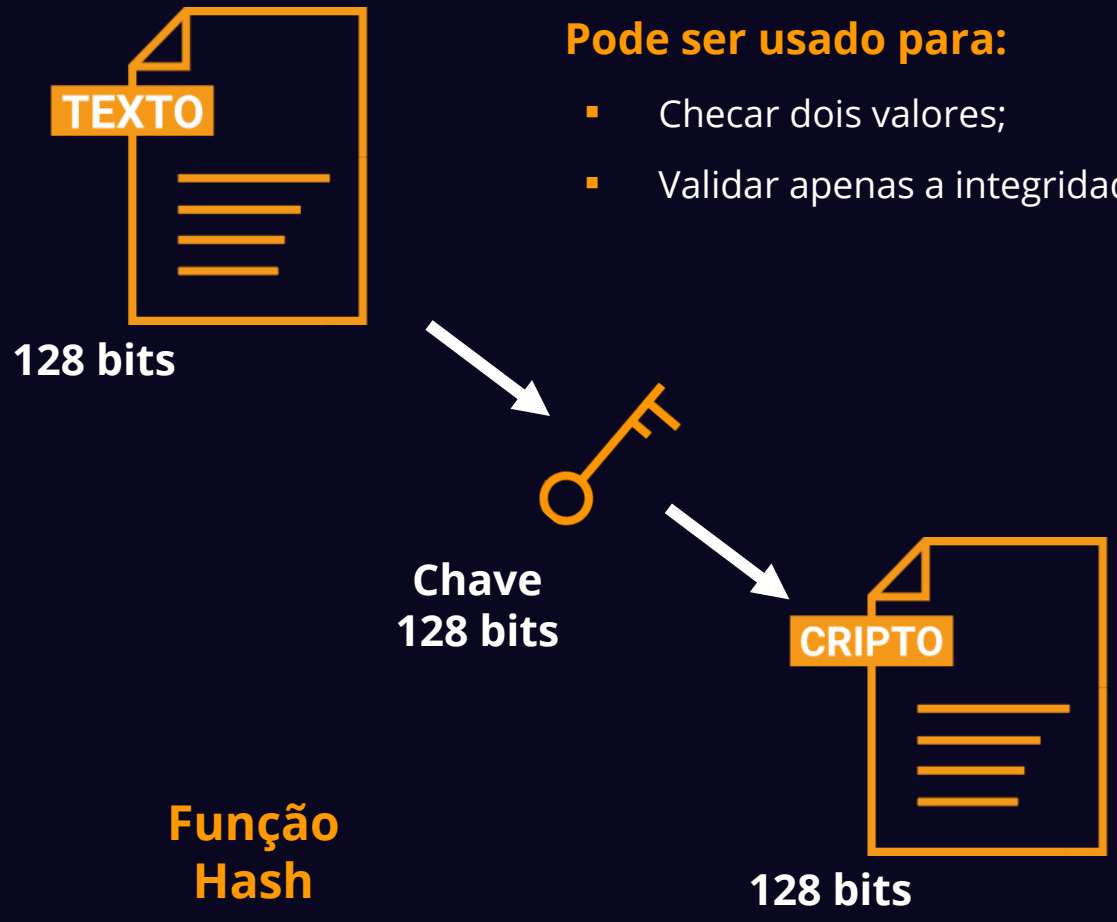
- Um usuário se registra em uma Autoridade de Registro (RA);
- Com base em credenciais (por exemplo, um passaporte), um pedido é enviado pela RA à Autoridade Certificadora (CA);
- A CA emite um certificado;
- O par de chaves que será usado pelo usuário pode ser gerado de diferentes maneiras;
- Em algumas PKIs, o usuário pode gerar essas chaves, enquanto em outras é usada uma instalação segura para gerá-las;
- CA emite um certificado que afirma que a chave pública pertence ao usuário a quem o certificado é emitido.

Assinaturas Digitais

Não-repúdio

- Repudiar significa negar;
- É a garantia de que alguém não pode negar algo;
- Carta registrada e testemunhas;
- A ISO define não-repúdio como a **capacidade de provar a ocorrência de um evento ou ação reivindicada e as entidades envolvidas**, a fim de resolver disputas sobre a ocorrência ou não ocorrência do evento ou ação e o envolvimento das entidades no evento;
- Assinaturas digitais para resolver essa questão;
- Quando o usuário assina, por exemplo, um contrato com uma assinatura digital:
  - ✓ A parte receptora pode verificar se a assinatura digital realmente pertence ao usuário;
  - ✓ O receptor valida por meio de uma Autoridade de Validação que tem acesso à Autoridade de Certificação.

Criptografia One-Way (Hash)



Pode ser usado para:

- Checar dois valores;
- Validar apenas a integridade.

OBRIGADO

Criptografia

academy

LIDANDO COM DADOS E INFORMAÇÕES

Exclusão de Informações

Quando excluir?

- Quando não forem mais necessárias, conforme período definido na política;
- Para evitar o uso ou processamento inadvertido;
- Evitar a divulgação acidental.

Considerações

- Algumas informações podem não ser removidas devido, por exemplo, à legislação;
- Pode ser necessário gerar um relatório comprovando a exclusão;
- Se for provedor em nuvem, deve constar contratualmente.

Mascaramento (Ocultação) de Dados

Quando usar?

Se dados sensíveis precisarem ser protegidos contra divulgação não autorizada ou se esses dados consistirem, por exemplo, em dados pessoais sensíveis.

O que seria mascaramento?

- Técnica de proteção de dados confidenciais (por exemplo, PII);
- Ocultação de dados usando asterisco;
- Técnicas de pseudonimização ou anonimização;
- A ocultação de dados deve ser usada de acordo com a política da organização.

Técnicas de Mascaramento de Dados

Quais as técnicas adicionais para mascaramento de dados?

Criptografia (exige que usuários autorizados tenham uma chave);

P*G
PR**E

Anulação ou exclusão de caracteres que impeça que pessoas não autorizadas vejam mensagens completas;

26/4
6/10

Variar números e datas;

Substituição (troca de um valor por outro para ocultar dados sensíveis);

Substituir valores por seu hash.

Anonimização ou Pseudonimização

Anonimização

- É irreversível;
- A PII não pode mais ser identificada direta ou indiretamente;
- As funções de hash podem ser usadas para anonimizar;
- Anonimização vai além de pseudonimização.

Pseudonimização

- Substitui as informações de identificação por um alias;
- Permite pelo menos alguma forma de identificação do principal PII;
- Essas “informações adicionais” devem, portanto, ser mantidas separadas e protegidas;
- Proteção mais fraca do que a anonimização.

Prevenção de Vazamento de Dados

Objetivo:

Detectar e impedir a divulgação e extração não autorizadas de informações por indivíduos ou sistemas.

O que fazer para reduzir o risco de vazamento de dados?

- Identificar e classificar informações para proteger contra vazamentos;
- Monitorar canais como e-mail, transferências de arquivos, dispositivos móveis e de armazenamento;
- Evitar o vazamento de informações, como e-mails contendo informações confidenciais.

Vazamento de Dados

Onde pode ocorrer:

- Encaminhados por e-mail;
- Armazenados em smartphones, pen drives;
- Armazenados em unidades de rede.

Vazamentos de dados são inevitáveis!!

- Pode ocorrer vazamento no armazenamento e transmissão;
- Se for necessário mover dados, considere a aprovação do gerente;
- Construa políticas, implementa-as e monitore-as.

Prevenindo o Vazamento de Dados

Para reduzir o risco de violação de dados, deve-se considerar o seguinte:

- Identificar e classificar todos os dados sensíveis;
- Avaliar o risco de partes externas;
- Monitorar todo o tráfego de rede;
- Monitorar todos os dados;
- Usar ferramentas para evitar a cópia, transferência ou upload de dados;
- Proteção de endpoints;
- Senhas fortes;
- Criptografia de dados em repouso e em trânsito;
- Configurar e manter controle de acesso lógico;
- Educação e treinamento do usuário.

Usuários ainda podem tirar fotos do que é visto na tela!

OBRIGADO

LIDANDO COM DADOS E INFORMAÇÕES

REGISTRO E MONITORAMENTO

Registro

- Com o aumento de ataques e mau comportamento, intencional ou não, é necessário ter a capacidade de registrar eventos e produzir evidências.
- Para esse propósito, é essencial ter um bom registro (logging).
- Registre e monitore, principalmente as evidências;
- Registre os eventos (log) de:

Atividades de sistema;

Atividades de usuários;

Exceções;

Falhas;

Eventos de segurança da informação.

- Um registro descreve o que acontece nos sistemas.

Uso do Registro

LOG

O bom registro pode ser usado para:

- Gestão de capacidade (status dos sistemas);
- Apoiar a descoberta de erros em software e hardware;
- Descobrir erros humanos e intrusos em sistemas;
- Detectar dados corrompidos ou notificações de vírus;
- Apoiar a investigação forense de sistemas;
- Apoiar investigações após um incidente;
- Base para a implementação de sistemas de Gerenc. de Eventos e Incidentes de Segurança (SIEM);
- Monitoramento de conformidade com SLA;
- Fornecer informações para uma auditoria;
- Fornecer informações para investigar a conformidade com políticas (ex: dispositivos estranhos conectados).
- Fornecer informações para demonstrar que uma determinada mensagem foi enviada ou não;
- Relatórios de uso do sistema e incidentes para o proprietário do sistema e o CISO.

Conteúdo dos Registros

Porque a criação de registros é um dos tópicos menos valorizados?

- Falta de recursos;
- Falta de tempo para ler um registro;
- Há registros em excesso ou insuficientes.

Um registro deve exibir o seguinte, os chamados cinco W's:

- O que aconteceu?
- Quando isso aconteceu?
- Onde isso aconteceu?
- Quem esteve envolvido?
- De onde isso veio?

Considerações dos Registros

Lembre-se:

- Os registros devem ser mantidos em um local seguro;
- Devem ser protegidos contra alterações ou exclusão;
- Antes de iniciar o registro, pense sobre o que registrar;
- Pense por quanto tempo manter os registros;
- Quem deve ter acesso às informações;
- Relógios do sistema devem estar sincronizados com uma única fonte de tempo de referência;
- Arquivos de registro com dados pessoais devem ser protegidos de acordo com as leis de privacidade.

Monitoramento de Atividades

Dependência:

Se não houver registro, o monitoramento não pode ocorrer. O registro e o monitoramento caminham juntos.

Exemplos de objetos para monitoramento:

- Ações dos administradores;
- Processos e sistemas críticos e arquivos de configuração;
- Acesso a servidores, bancos de dados, redes e aplicativos;
- Tráfego de entrada e saída;
- Registro de ferramentas de segurança;
- Utilização de recursos;
- Registro.

Monitorando

O que é registrado?

- Erros;
- Desvios das políticas;
- Ações não autorizadas e coisas do tipo.

Considerações

- É muito trabalhoso, portanto, use ferramentas;
- Valores de limite podem ser definidos dentro delas;
- Diferentes registros podem ser correlacionados entre si para criar informações significativas;
- A partir de incidentes, os chamados IOC's (indicadores de comprometimento) podem ser compartilhados entre Equipes de Resposta a Incidentes de Computador (CERTs);
- Possível monitorar (ou pesquisar nos registros) se um ataque (bem-sucedido) já ocorreu na infraestrutura da organização.

Sincronização do Relógio

Qual a importância de sincronizar relógio?

- Garante precisão dos logs de eventos;
- Necessários para investigações ou como prova em casos legais e disciplinares;
- Essenciais para registros de auditoria, pois evita prejudicar a credibilidade;
- Um tempo de referência padrão para uso dentro da organização deve ser definido;
- Um relógio atômico ou sistema de posicionamento global (GPS) deve ser usado;
- Usar NTP (Network Time Protocol) and PTP (Precision Time Protocol);
- Diferenças devem ser registradas para mitigar riscos decorrentes de discrepâncias.

OBRIGADO

REGISTRO E MONITORAMENTO

academy

BACKUP E REDUNDÂNCIA

Backup de Informações

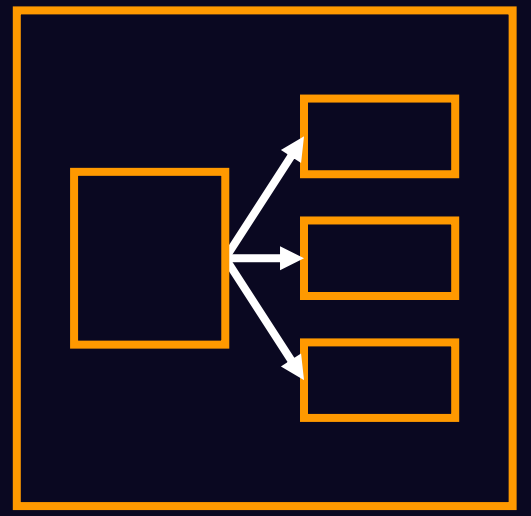
Objetivo de fazer backups, ou cópias de reserva:

- Manter a integridade;
- Manter a disponibilidade das informações e dos recursos de computação.

Dicas?

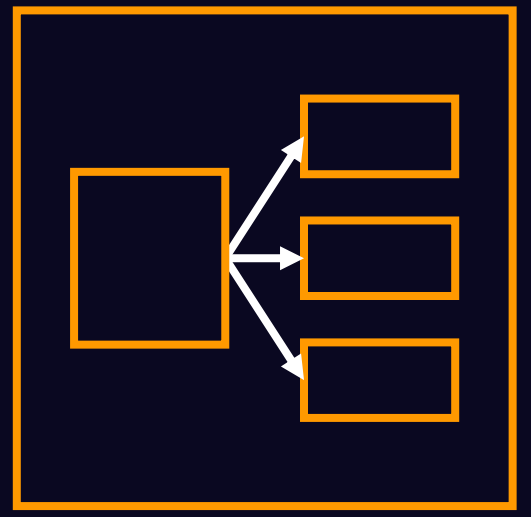
- Quanto mais antigo o backup, menores as consequências da perda de informação;
- Mais importante que o backup é o teste do Restore;
- Considere o intervalo em que os backups são feitos;
- É importante que o backup seja testado regularmente.
- Cuidado ao manejar os backups. São trancados? Onde são armazenados?

Redundâncias



- Redundância é a duplicação de instalações em parte ou em sua totalidade;
- Pode ser com componentes sobressalentes ou duplicando tudo;
- As redundâncias são sempre ativadas em caso de emergência;
- Ativadas automaticamente ou manualmente;
- A redundância deve garantir o mesmo nível de segurança que os primários;
- Devem existir mecanismos para alertar sobre qualquer falha nas instalações.

Tipos de Redundâncias



Existem alguns tipos de redundância para locais:

Cold Site: Funcionalidades básicas. Pode levar semanas para ativar e restaurar backups;

Hot Site: Espelha todos os equipamentos. Prontamente utilizado;

Warm Site: Intermediário ao Cold e Hot. Há constante atualização. Pode levar horas;

Mobile Site: Trailers ou caminhões. Mantém o essencial. Normalmente configurado como Cold ou Warm.

Site Redundante

Quando é adequado?

- Uma boa alternativa para uma empresa com muitas filiais;
- Mas apenas um único centro de computação central, é um site redundante;
- O site redundante contém uma cópia do centro de computação;
- Todos os dados que entram no site principal também são inseridos no sistema do site redundante;
- Se um desses dois locais apresentar uma falha, o outro local assumirá automaticamente;
- Quando isso é feito de forma suave, o usuário não perceberá nada.

Site de Emergência Sob Demanda

Características

- Solução de site móvel de emergência;
- Contém um ou mais caminhões com todo o equipamento necessário para funcionar como um centro de computação temporário;
- Em caso de desastre, os caminhões são usados por um curto período de tempo, normalmente algumas horas;
- São levados para um local pré-determinado e o equipamento é conectado;
- As possibilidades são limitadas;
- É uma maneira de colocar os processos mais cruciais em operação novamente o mais rápido possível.

Medidas de Pessoal

Características

- Um desastre pode resultar em problemas de pessoal;
- Se as pessoas que suportam o processo principal não estiverem mais disponíveis;
- Planos devem incluir formas de substituir essas pessoas chave;
- No caso de um problema grave que afeta a localidade, os funcionários podem ser incapazes de viajar, especialmente para um local remoto.

OBRIGADO

BACKUP E REDUNDÂNCIA

academy

PROCESSOS DE GERENCIAMENTO

Gerenciamento de Capacidade

Há duas formas de gerenciar a capacidade:

- Aumentando a Capacidade;
- Reduzindo a Demanda.

Como a Capacidade ajuda as empresa?

- Maximiza a eficiência de produção devido à demanda geral por um produto ou serviço no mercado;
- Identifica e elimina gargalos no processo de fabricação;
- Aumenta a velocidade de produção;
- Otimiza os recursos disponíveis;
- Remove restrições de tempo e capacidade;
- Superar desafios no atendimento à demanda dos clientes a curto e médio prazo;
- Gerencia operações da cadeia de suprimentos e setores como manufatura, varejo, serviços e TI;
- Gerencia a capacidade necessária das:
  - Informações;
  - Recursos humanos;
  - Instalações.

Vulnerabilidade

O que é?

- Uma fraqueza em um ativo ou grupo de ativos;
- Que pode ser explorada por uma ou mais ameaças;
- Ausência ou a fraqueza de uma salvaguarda que poderia ser explorada;
- Pode ser um serviço em execução em um servidor;
- Aplicativos ou software do S.O. não corrigidos;
- Acesso não restrito através de modem, uma porta aberta em um firewall;
- Segurança física fraca que permite que qualquer pessoa entre em uma sala de servidores;
- Gerenciamento de senhas não aplicado em servidores e estações de trabalho.

Gerenciamento de Vulnerabilidades Técnicas

Características:

- Vulnerabilidade permite que um atacante ataque o sistema vulnerável;
- Muitas vulnerabilidades que são descobertas por hackers éticos ou por coincidência;
- Todo sistema de computador possui vulnerabilidades.

Assim que uma vulnerabilidade for conhecida:

- Medidas apropriadas sejam tomadas para evitar a exploração;
- Para vulnerabilidades desconhecidas, é necessário um processo de gerenciamento de incidentes;
- Para vulnerabilidades conhecidas, os fornecedores provavelmente fornecerão atualizações ou correções;
- Se não houver uma correção disponível, o risco deve ser minimizado por meio de:
  - ✓ Isolamento do sistema;
  - ✓ Adaptação de firewalls e aumento da monitoração;
  - ✓ Uso de scanners;
  - ✓ Consultar a lista de CVE da Mitre cve.mitre.org

Configuração

Diz respeito às configurações de:

- Hardware;
- Software;
- Serviços;
- Redes.

As configurações devem ser registradas;

Um log deve ser mantido e mudanças devem ser registras e armazenadas em:

- Bancos de dados de configuração;
- Modelos de configuração.

Gerenciando a Configuração

As mudanças devem seguir o processo de gerenciamento de mudanças;

Características do processo:

- Fornece uma visão geral dos sistemas/programas existentes e da versão;
- Também das configurações de segurança e das configurações de rede;
- As configurações devem ser documentadas, gerenciadas e reavaliadas regularmente;
- Usados para fornecer entrada aos outros processos;
- Os Itens de Configuração (CI's) devem ser identificados e registrados;
- A falta de CI's atualizados afetam a disponibilidade, integridade, confidencialidade e verificabilidade dos serviços de TIC;
- Periodicamente, os itens de configuração devem ser comparados e atualizados.

Gerenciamento de Configuração

Máxima:

Se você não sabe o que tem, não pode proteger ou usar corretamente.

O que é definido neste processo?

- Registro: Registrar novos itens de configuração;
- Administração: Administração do banco de dados de gerenciamento de configuração (CMDB);
- Monitoramento de status: Monitoramento de status dos itens de configuração;
- Verificação: a) Deve ser adicionado ao CMDB ou b) Deve ser removido do ambiente.

CMDB atualizado: Encontrar vulnerabilidades para vulnerabilidade de dia zero.

Gerenciamento de Mudança

- Implementar ou não uma mudança, implica em risco;
- Se forem feitas, elas devem ser cuidadosamente consideradas antecipadamente e realizadas de maneira controlada;
- Mudanças devem ser planejadas com antecedência;
- Envolvem a CS para atuar com as novas versões;
- Lidar com diferentes tamanhos de mudanças.

IMPORTANTE:

- Segregar funções;
- Toda mudança deve ser aprovada antes de ir para produção;
- Deve haver procedimento de fallback;
- Deve ser atualizado o CMDB.

Proteção de Sistemas de Informação Durante Testes de Auditoria

Válido para auditoria e teste de penetração	Auditorias em sistemas sejam realizadas apenas em modo leitura
É necessário planejar e coordenar cuidadosamente as atividades	Ferramentas utilizadas para auditoria devem ser mantidas separadas da produção
Acordo: O testador de penetração não é responsável por erros	Se terceiro estiver envolvido, use um NDA

“Não importa o quão bem uma organização tenha planejado sua segurança, a segurança é tão forte quanto o elo mais fraco”

OBRIGADO

PROCESSOS DE GERENCIAMENTO

academy

DESENVOLVIMENTO SEGURO

Ciclo de Vida de Desenvolvimento Seguro

Quais aspectos a serem considerados no desenvolvimento seguro?

- Segregação de ambientes de desenvolvimento, teste e produção;
- Segurança no ciclo de vida e metodologia de desenvolvimento de software;
- Segurança na programação segura de cada linguagem;
- Especificar requisitos de segurança na fase inicial do projeto;
- Definir pontos de verificação de segurança nos projetos;
- Fazer Pentest, teste de varredura e teste de regressão (testar mudanças);
- Validar através de auditoria do desenvolvedor do sistema por uma terceira parte;
- Estar em conformidade com os requisitos de sua própria organização.

Ciclo de Vida do Desenvolvimento de Sistemas (SDLC)

Características:

- Adoção de um método SDLC (Ciclo de Vida do Desenvolvimento de Sistemas);
- SDLC que atendam às especificações, dentro dos prazos e custos estimados;
- Balancear segurança versus custo e desempenho de negócio;
- Muitas vezes os custos têm prioridade sobre a segurança;
- Muitas organizações ainda concentra-se apenas em aplicar segurança na fase de implantação;
- Tentam incorporar a segurança apenas no design final.

RESULTADO: Aplicação ineficaz da segurança!

Segurança por Design (SBD)

- **Como proteger**: Integrando a segurança em cada etapa do SDLC;
- **Em que momento**: Desde o início até o desenvolvimento, implantação e descarte eventual do sistema;
- **O que é Segurança por Design**: Abordagem de desenvolvimento de software e hardware que:
  - ✓ Minimiza as vulnerabilidades;
  - ✓ Reduz a superfície de ataque;
  - ✓ Avaliação contínua de segurança em cada estágio;
  - ✓ Aderência às melhores práticas.
- **Para quais atividades de Segurança (e Privacidade)?**
  - ✓ Desing, Análise e Planejamento;
  - ✓ Manutenção;
  - ✓ Aposentadoria;
  - ✓ Integração e Desenvolvimento;
  - ✓ Testes.

Benefícios na Integração da Segurança ao SDLC

- Identificação e mitigação precoce de vulnerabilidades;
- Redução de custos;
- Melhora as atitudes de segurança por meio de melhores práticas e técnicas;
- Facilitar decisões por meio de uma gestão abrangente de riscos;
- Documentação das principais decisões de segurança ao longo do ciclo de vida do sistema;
- Garantia que a segurança tenha sido totalmente considerada em todas as etapas;
- Melhoria da operacionalidade do sistema;
- Adiciona um design de segurança para as capacidades de identificação / proteção / detecção / resposta / remediação.

Requisitos de Segurança de Aplicações

Que requisitos devemos considerar ao desenvolver ou comprar um aplicativo?

- É mais caro incluir requisitos de segurança em estágios posteriores ao design inicial;
- Algumas vezes nem é possível por falhas estruturais;
- Projetar sistemas de informações seguros não é fácil,;
- Envolvem S.Os., infraestrutura, processos operacionais, produtos prontos, serviços e aplicativos;
- Normalmente é mais barato implementar, testar e manter medidas de segurança durante a fase de design;
- Requisitos de segurança devem ser considerados no "caso de negócio“;
- Se comprar, teste formalmente antes da aquisição;
- Deve constar no contrato os requisitos de segurança.

Serviços para Comércio Eletrônico

Lidar com:

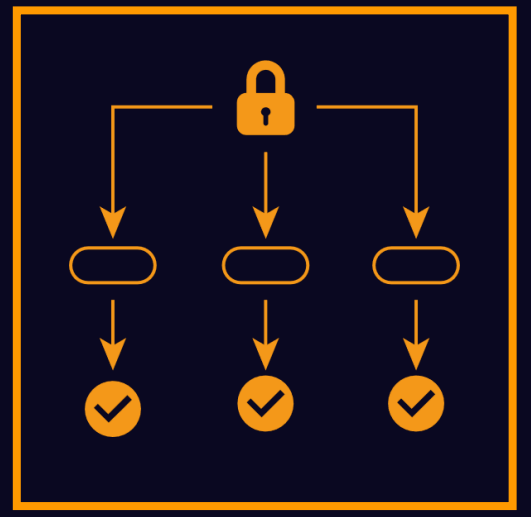
- Uma loja online gera riscos novos em relação ao uso da Internet apenas para buscar informações;
- Os serviços para comércio eletrônico e seu uso devem ser protegidos de forma eficaz;
- Considere, por exemplo, transações de pagamento seguras (por exemplo, Visa, MasterCard, PayPal);
- Proteção das informações contra fraudes;
- Contratos e acordos digitais;
- Lidar com o não repúdio e acordo com os preços;
- Confidencialidade e a integridade:
  - ✓ Transações de pedidos;
  - ✓ Informações de pagamento;
  - ✓ Detalhes do endereço do destinatário.

Informações
Publicamente Disponíveis

Lidar com Informações em uma página:

- São públicas, mas devem estar corretas e não ser manipuladas;
- Informações errôneas prejudicarão a reputação;
- Atendam aos requisitos legais e regulatórios em que o sistema está localizado;
- Importante que o “backend” atenda aos requisitos de segurança e do usuário.

Arquitetura de Segurança



A segurança deve ser projetada em todas as camadas da arquitetura:

- Negócios;
- Dados;
- Aplicativos;
- Tecnologia.

Os princípios de engenharia segura nos sistemas fornecem orientação sobre:

- Técnicas de autenticação do usuário;
- Controle de sessão segura;
- Validação de dados;
- Higienização de dados.

Princípios de Arquitetura e Engenharia de Sistemas Seguros

Realidade:

- Muitos sistemas de informação não foram projetados para serem seguros;
- Os meios técnicos são limitados e precisam ser apoiados por uma gestão;
- Identificar quais controles devem ser implementados requer um planejamento cuidadoso e atenção;
- A participação de todos os funcionários da organização é exigida;
- Pode exigir de acionistas, fornecedores, terceiros, clientes, especialistas ou outras partes externas;
- Nenhum sistema está “isolado”;
- Gestão de risco se torna primordial;
- Exige-se o CID, políticas, todos os controles, padrões, procedimentos, soluções, pessoas, ativos etc.

Programação Segura

Fato:

O software sempre contém erros; é impossível escrever software sem erros!

Mecanismos para garantir a codificação segura:

- Definir princípios e políticas para o desenvolvimento de software interno e externo;
- Aprender com erros do passado e não permitir que eles ocorram novamente;
- Utilizar padrões comprovados e software e ferramentas de desenvolvimento que sejam regularmente atualizados;
- Trabalhar com uma arquitetura adequada;
- Trabalhar com o princípio do menor privilégio e da confiança zero;
- Bibliotecas de terceiros podem conter riscos;
- Blocos de códigos-fontes podem conter vulnerabilidades.

Testes de Segurança no Desenvolvimento e Aceitação

O que é ambiente de aceitação?

- Ambiente no qual os usuários finais podem verificar se o produto atende às suas especificações.
- Configurações seguras no ambiente de dev, como:

Sistemas operacionais;

Firewalls;

Outros componentes de segurança.

Antes de colocar em produção:

- Após a aceitação, siga os procedimentos estabelecidos;
- Desenvolva um plano de contingência para casos de um problema grave.

Desenvolvimento Terceirizado

Quais pontos considerar em toda a cadeia?

- Fornecimento de relatórios com evidências com níveis aceitáveis de:

Segurança;

Privacidade;

Presença de conteúdo malicioso (intencional e não intencional);

Vulnerabilidades conhecidas.

- Acordos de garantias para o código-fonte caso o fornecedor falir;
- Monitorar a qualidade do código a ser entregue;
- Requisitos de segurança para o ambiente de desenvolvimento;
- Avaliar e monitorar os entregáveis;
- Manter um relacionamento maduro e saudável.

Separação dos Ambientes de Desenvolvimento, Teste e Produção

Objetivo:

Garantir que as alterações não sejam implementadas de forma descontrolada.

O que é necessário?

- Procedimentos para mover o software de um ambiente para outro;
- Em organizações menores, os diferentes ambientes podem ser combinados (desenvolvimento, teste e aceitação);
- Para a fase de desenvolvimento, aplicam-se requisitos de segurança específicos;
- No ambiente de desenvolvimento, os devs podem criar novos softwares ou trabalhar em alterações nos existentes;
- O controle de versão é muito importante.

Informações de Teste

Objetivo:

Garantir a relevância dos testes e a proteção das informações operacionais utilizadas para os testes.

Como garantir a confiabilidade nos testes?

- Aplicar os mesmos controles de acesso nos ambientes de desenvolvimento e operação;
- Autorização cada vez que uma informação é copiada para o ambiente de teste;
- Proteger informações confidenciais com remoção ou mascaramento;
- Excluir informações de um ambiente de teste imediatamente após o teste.

OBRIGADO

DESENVOLVIMENTO SEGURO