

Aula 5 - Classificação da informação/ Arquiteturas e Modelos de Segurança da Informação

A decorative graphic element consisting of several horizontal lines of varying lengths and colors (teal, light blue, and white) extending from the left side of the slide towards the right.

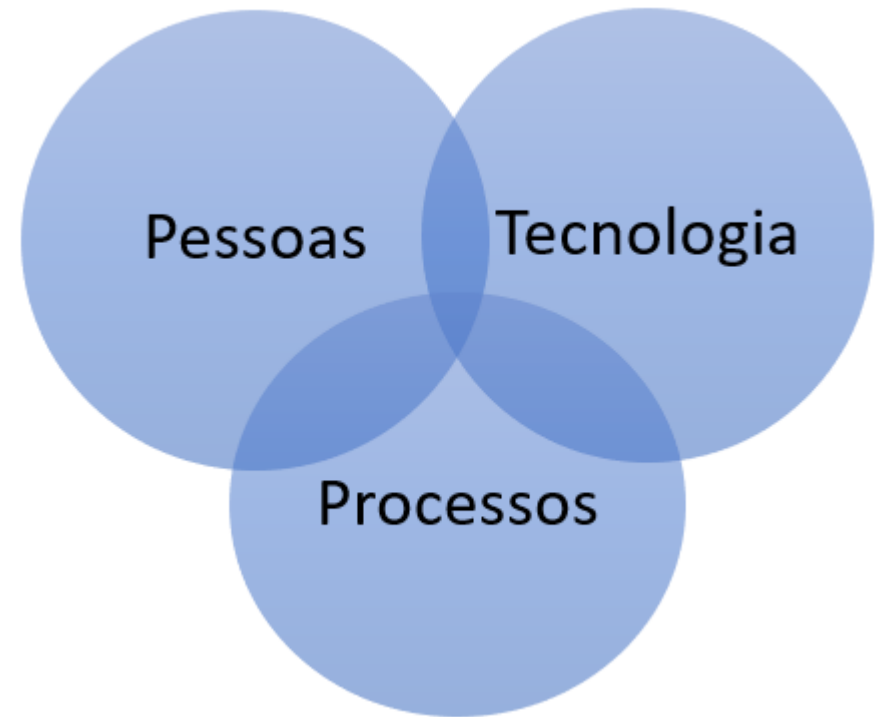
Classificação da informação

A series of horizontal lines in teal and light blue colors, with varying lengths and offsets, creating a modern, layered effect across the width of the slide.

- As empresas geram, diariamente, um montante de informações altamente elevado, e essas informações são primordiais para o negócio, devendo estar sempre a disposição.
- O processo de administrar essas informações é essencial, mas complexo, pois diversas variáveis incidem sobre a informação... Sua segurança e disponibilidade nem sempre depende apenas de nós.

- Temos que lidar com:

- Ameaças
- Vulnerabilidades
- Necessidade de classificação
- Local de armazenamento adequado
- Backup
- Direitos de acesso
- Continuidade, etc.



- Assim, a gestão da informação é altamente importante em uma empresa.

- A ideia da gestão da informação é fornecer apoio ao gestores de TI na tomada de decisões mediante todas as situações e variáveis que podem ocorrer.
- A informação alimenta os processos de diversas áreas da empresa, ela é manipulada pelos mais diversos tipos de usuário e cada um deles usa a mesma para realizar suas atividades dentro da empresa.
- Dentro de uma empresa, como vimos, temos a divisão das informações e atividades em 3 camadas: estratégica, tática e operacional.

• **Estratégica**

- Camada onde decisões são tomadas
- Define o futuro e rumo da organização
- Informações dessa camada possuem valor para o objetivo do negócio e ajudam a determinar as diretrizes operacionais
- São informações complexas



• Tática

- Informações que auxiliam os gestores em suas funções
- Essas informações auxiliam o processo de atingir os objetivos estratégicos
- São informações com grau de detalhamento intermediário



- **Operacional**

- Informações altamente detalhadas e necessárias para a execução das atividades diárias.





Estratégica

O que fazer

Tática

Como fazer

Operacional

Fazer

Gestor da Informação

- Pessoa que tem a função de liberar ou negar acessos de qualquer usuário a uma informação.
- Deve levar em consideração se o usuário precisar de fato ter aquele acesso (considerando as funções do usuário na empresa).
- O usuário não pode acessar todas as informações e recursos de TI por falta de conhecimento e preparação para tal!
- O gestor da informação é quem cuida desse processo de gerenciamento, e podemos dizer que o pessoal de segurança é o gestor dessa informação.

Proprietário da Informação

- Órgão gerador da informação, que faz uso da mesma pela necessidade.
- É capaz de estimar quão crítica é uma informação, definindo, assim, a sua importância.
- É ele quem define os níveis de segurança que a informação demanda.
- É o proprietário que consegue classificar a informação, autorizar os acessos e divulgar a mesma.
- A empresa em si é a proprietária da informação, e o alto escalão da empresa também tem essa função, assim como aqueles por eles definidos.

Custodiante da Informação

- Função administrativa (cargo ou área) que mantém a guarda da informação.
- Quando a informação está armazenada nos servidores ou trafegando na rede, seu custodiante vai ser o pessoal de TI, que é responsável por seus processos e cuidados.
- Mas quando a informação está na máquina do usuário, sendo criada e manipulada por ele, ele é quem será o custodiante dessa informação.
- A função do custodiante é zelar pelo armazenamento e preservação de informações que não lhe pertence, mas que foram deixadas sob sua guarda.
- O custodiante NÃO pode repassar a custódia da informação para outro sem autorização do proprietário.

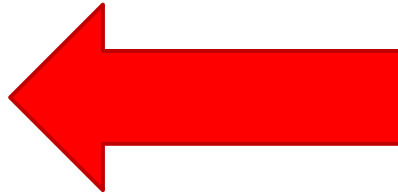
Responsabilidades do Custodiante

- Verificar e testar a eficácia dos controles usados na proteção da informação;
- Caso algum risco seja encontrado, informar proprietário dessas informações;
- Fazer a configuração dos equipamentos, ferramentas e sistemas com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos pela PSI.
- Aplicar, gerenciar e manter as trilhas de auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes;
- Promover proteção física;
- Fazer backup da informação.

• **O custodiante da informação deve:**

- Aplicar procedimentos de proteção do ativo
- Autorizar e cancelar autorização de acessos
- Executar serviços em nome do proprietário
- Determinação dos direitos que o usuário terá (leitura, gravação, alteração, exclusão, execução)

Enquete

- Como podemos considerar a pessoa que cria um arquivo que está armazenado na rede da empresa?
 - Usuário da informação 
 - Custodiante da informação
 - Proprietário da informação

Classificação da Informação

- O ato de classificar algo refere-se a organizar um ou mais itens de acordo com suas características comuns, colocando-os em ordem.
- Podemos classificar quase tudo, desde roupas em um armário, produtos em um supermercado, livros, DVDs, brinquedos, informações, etc..
- Classificar envolve escolher a melhor alternativa de se colocar algo em ordem.
- O primeiro passo da classificação é a determinação de um parâmetro de classificação e a definição dos rótulos de classificação.
- Devemos ter em mente que TODA a informação deve ser classificada.

- Por exemplo: podemos classificar filmes pelo parâmetro gênero, usando os seguintes rótulos:



- Precisamos classificar as informações pois as empresas possuem diversos tipos de informação, todas elas com necessidades de segurança diferentes. Mas esse é um processo complexo, devido ao volume de informação que as empresas possuem.
- Existem informações em uma empresa que necessitam de um alto nível de proteção, enquanto outras não.
- Quanto mais informatizado um ambiente for, e com mais pessoas acessando as informações, mais vulnerabilidades teremos.
- Classificando a informação podemos:
 - Identificar situações de risco
 - Adotar procedimentos de segurança adequados a cada tipo de informação

- Fazendo a classificação da informação adequada pode-se definir os procedimentos e tecnologias para garantir o CID; com a classificação da informação realizada, pode-se definir melhores regras de controle de acesso.
- Para se classificar a informação, é preciso criar um roteiro de como esse processo será feito, tendo o aval da alta administração e definindo, previamente, quais rótulos serão utilizados.
- A classificação da informação vai permitir identificar uma situação de risco mais facilmente e reagir em menor espaço de tempo.

- Além disso, a classificação da informação gera redução de custos e aumento da segurança.
- Classificando as informações de acordo com sua sensibilidade e controlando o acesso de acordo com essa classificação, a empresa poderá definir os modelos e as tecnologias que utilizará para preservar o CID.
- A classificação da informação deve ser abrangente para que seja eficiente, considerando todos os tipos de informação da empresa e todas as etapas de seu ciclo de vida.

- Os rótulos mais comumente usados na classificação da informação são:
 - Secreta
 - Confidencial
 - Restrita
 - Interna
 - Pública

- **Secreta:** informação que é um diferencial competitivo, referente às estratégias de negócio. Trata-se da informação cuja perda ou acesso indevido pode ocasionar em grandes perdas financeiras e, por vezes, em encerramento das atividades da empresa. Ex: fórmula da coca-cola;



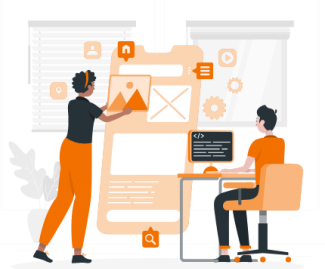
- **Confidencial:** informação restrita ao alto escalão da empresa e àqueles que eles determinarem (para a execução de suas tarefas). Em geral são informações estratégicas e administrativas. Ex: projeto para compra de um concorrente;

CONFIDENCIAL

- **Restrita:** informação de acesso apenas para os usuários que precisam fazer uso da mesma em suas tarefas. Ex: apenas o RH e o financeiro acessam a folha de pagamento;



- **Interna:** informação cujo uso é possível apenas dentro da empresa e deve ser liberado a todos que nela atuam. Geralmente trata-se de informações técnicas ou organizacionais. Ex: calendário de eventos e treinamentos;



- **Pública:** informações que podem estar disponíveis para qualquer um. Ex: relação de produtos a venda pela empresa.



Atividades (em grupo)

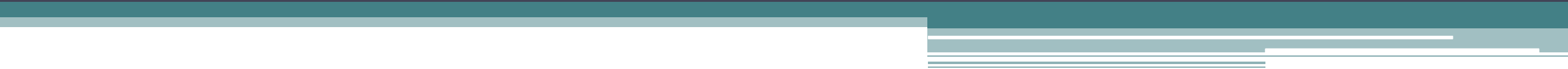
1. Antes de implantarmos a segurança na Empresa, precisamos saber o porquê e para que proteger as informações e os sistemas de computadores da mesma. Destaquem **5 motivos** para justificar a necessidade da implantação da Segurança da Informação em uma empresa.

2. Pensem em um tipo de informação de uma como fazer para garantir o CIDAL da mesma?

- INFORMAÇÃO:
- Confidencialidade:
- Integridade:
- Disponibilidade:
- Autenticidade:
- Legalidade:

3. Classificação da Informação.

Arquiteturas e Modelos de Segurança da Informação

A decorative graphic element consisting of several horizontal lines of varying lengths and colors (teal, light blue, and white) extending from the left side of the slide towards the right, positioned below the title.

Arquitetura de Segurança da Informação

- A arquitetura de segurança envolve a avaliação dos controles de segurança da informação e a implementação adequada de processos empresariais e ferramentas nos sistemas de tecnologia da informação.
- O objetivo é salvaguardar os dados utilizados e armazenados por uma organização. No entanto, a arquitetura de segurança é apenas o ponto de partida; a eficácia da segurança surge da implementação contínua e das operações consistentes.

- Quando a arquitetura de segurança não é estabelecida de maneira sólida, as equipes da organização muitas vezes se veem lutando para encontrar soluções que protejam de forma aleatória contra ameaças.
- A maioria das chamadas 'arquiteturas de segurança cibernética' é reativa e orientada por ameaças. No entanto, uma arquitetura de segurança robusta procura oferecer medidas preventivas para garantir a proteção empresarial.



O que é Arquitetura de Segurança?

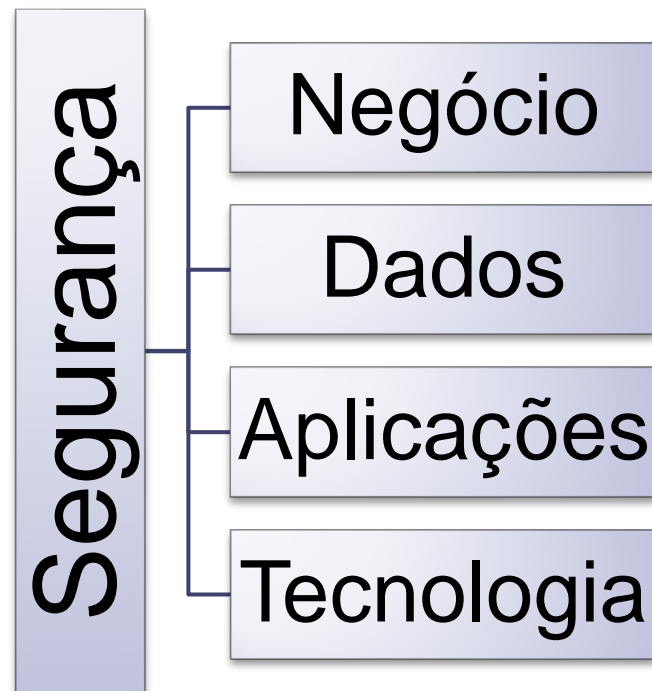
- Apesar das diversas interpretações do conceito de arquitetura de segurança, sua essência reside em ser uma coletânea de conceitos, processos e modelos de segurança que equilibram as oportunidades e as ameaças. Cada ação executada pela empresa cria um campo de possibilidades e riscos.
- A capacidade de tolerar riscos varia entre diferentes setores do negócio. Uma arquitetura de segurança eficiente se alinha aos objetivos de benefício e mitigação de riscos. Fundamentalmente, ela assegura que a empresa mantenha um nível de segurança suficiente para se proteger contra ataques cibernéticos.

- Um arquiteto de segurança trabalhará na empresa por um período para descobrir o que torna sua organização única. Ele falará com os executivos, funcionários para aprender sobre os objetivos da sua empresa, requisitos do sistema, desejos do consumidor e outros aspectos essenciais. Ele pode então criar uma estratégia e aconselhamento adaptados aos objetivos da empresa e que atendam ao seu risco de segurança cibernética.



Os Quatro Elementos Críticos da Arquitetura de Segurança

- Para compreender a natureza da arquitetura de segurança, é necessário observá-la sob quatro contextos críticos.



- Não existe uma arquitetura de segurança isolada. Por exemplo, ao considerar o contexto da empresa e analisar o software empresarial, é perceptível que ele contém um componente de segurança que por sua vez, integra-se à arquitetura de segurança e operações correspondentes.

Modelos de Arquitetura de Segurança

- **ISO/IEC 27001:** Embora seja um padrão mais abrangente para gestão de segurança da informação, a ISO/IEC 27001 também incorpora aspectos de arquitetura de segurança, fornecendo diretrizes para estabelecer, implementar, manter e melhorar sistemas de gestão de segurança da informação.
- **Zero Trust Architecture (Arquitetura de Confiança Zero):** Esta abordagem baseia-se na premissa de que nenhuma parte da rede ou usuário deve ser automaticamente confiável. A autenticação e a autorização ocorrem constantemente, independentemente da localização do usuário ou dispositivo.

- **ABAC (Attribute-Based Access Control):** Este modelo utiliza atributos específicos do usuário, contexto e recursos para tomar decisões de acesso. Ele permite políticas de acesso mais detalhadas e flexíveis do que os modelos tradicionais de controle de acesso baseados em funções.
- **NIST Cybersecurity Framework (Estrutura de Cibersegurança do NIST):** Desenvolvido pelo Instituto Nacional de Padrões e Tecnologia dos EUA (NIST), este framework oferece orientações para ajudar as organizações a gerenciar e reduzir riscos de cibersegurança. Ele enfatiza a identificação, proteção, detecção, resposta e recuperação.

- Um framework é como um conjunto de ferramentas organizadas que ajudam a resolver um tipo específico de problema.
- É como ter peças de LEGO prontas para montar um modelo.
- Um framework fornece diretrizes, estruturas e partes reutilizáveis que facilitam a criação de algo, como um site, um aplicativo ou um plano de segurança.
- Utilizar um framework o economiza tempo e esforço, permitindo se concentrar mais em construir e menos em começar do zero.

- **PbD (Privacy by Design - Privacidade desde o Design):** Enquanto não é estritamente um modelo de arquitetura de segurança, o PbD é uma abordagem que promove a incorporação da privacidade no design de sistemas desde o início. Isso assegura que as preocupações com a privacidade sejam abordadas desde a concepção.
- **CCM (Cloud Controls Matrix):** Especialmente voltado para a segurança em ambientes de nuvem, o CCM fornece um conjunto de controles de segurança que ajudam as organizações a avaliar os riscos e a implementar práticas de segurança adequadas na nuvem.

- **TOGAF (The Open Group Architecture Framework):** Embora não seja focado exclusivamente em segurança, o TOGAF é um framework de arquitetura empresarial que também inclui considerações de segurança em sua metodologia de desenvolvimento.
- **SBSA (Security By Design, Security By Default, Security By Deployment, Security By Operation):** é um modelo de arquitetura de segurança que enfatiza a integração da segurança em todos os estágios do ciclo de vida de um sistema ou aplicativo.

SBSA

- **Security By Design:** Isso significa que a segurança é incorporada desde o início do desenvolvimento. Em vez de adicionar medidas de segurança após o fato, elas são planejadas e implementadas durante a criação do sistema. Isso inclui considerar as ameaças possíveis e projetar defesas apropriadas.
- **Security By Default:** Aqui, a ideia é que as configurações padrão de um sistema sejam seguras por natureza. Isso evita que usuários ou administradores tenham que fazer ajustes extensivos para proteger o sistema. A segurança é a premissa inicial.

SBSA

- **Security By Deployment:** Isso se refere à garantia de que as medidas de segurança sejam mantidas durante a implantação do sistema em diferentes ambientes, como servidores ou redes. Isso evita brechas de segurança causadas por diferenças entre ambientes.
- **Security By Operation:** Esse aspecto envolve a manutenção da segurança durante a operação contínua do sistema. Isso inclui monitoramento, atualizações regulares de segurança e resposta a incidentes.

- O **SBSA** promove a abordagem proativa, em que a segurança é tratada como parte integrante de todos os aspectos de um sistema, em vez de ser uma reflexão tardia. Isso ajuda a reduzir riscos e vulnerabilidades, tornando os sistemas mais resilientes contra ameaças cibernéticas.



Gerenciamento de Riscos

- A arquitetura de segurança basicamente é o gerenciamento de riscos.
- Risco é a consequência da incerteza que afeta a realização de todos os objetivos empresariais.
- Essa incerteza advém tanto da perda de oportunidades quanto da exposição a possíveis ameaças.
- A arquitetura de segurança, por si só, não assegura a proteção contra ameaças. É essencial incluir um componente de gestão de riscos para abordar efetivamente essas situações.

- A prática de gerenciar os riscos associados ao uso da tecnologia da informação é denominada gerenciamento de riscos de segurança da informação.
- Envolve reconhecer, analisar e responder às ameaças que podem afetar a confidencialidade, integridade e disponibilidade dos recursos de uma organização.
- O propósito último do gerenciamento de riscos lidar com os riscos de acordo com a postura de risco da empresa.
- Ao invés de buscar eliminar todos os riscos possíveis, as empresas devem procurar estabelecer e aceitar um nível geral de risco aceitável.

Arquitetura de segurança X Arquitetura Corporativa

- A construção da Arquitetura de Segurança deve ser integrada ao desenvolvimento de uma estrutura corporativa.
- Em muitas empresas, implementar a segurança pode parecer uma tarefa quase impossível.
- Em vez de estabelecer uma arquitetura de segurança integrada, esforços aleatórios são empregados para proteger partes isoladas do negócio, frequentemente deixando outras áreas vulneráveis à invasão ou violação.
- Garantir um ambiente seguro exige uma combinação de medidas preventivas, investigativas e corretivas.

Importância da Arquitetura de Segurança

- A principal (e mais óbvia) vantagem do reforço da segurança é a diminuição das violações de segurança. Muitos invasores utilizam estratégias de ataque simples que miram vulnerabilidades comuns na cibersegurança, as quais são compartilhadas por empresas que não priorizam o desenvolvimento de uma base sólida de arquitetura de segurança.

- Diversos padrões e regulamentações relacionados à segurança da informação e proteção de dados estão surgindo.
- Muitos desses padrões e regulamentos exigem que as empresas mantenham uma arquitetura de segurança robusta e bem administrada, além de implementar uma série de procedimentos de segurança específicos.
- Um planejamento sólido de arquitetura de segurança uma visão clara da arquitetura da rede e das medidas de segurança integradas, em particular, simplifica determinar se a empresa corre o risco de violar alguma legislação importante.

Principais objetivos da Arquitetura de Segurança

- Identificar e avaliar os riscos de negócios associados à informação e tecnologia da informação.
- Identificar as principais preocupações de segurança da informação de confidencialidade, integridade e disponibilidade.
- Identificar os recursos encontrados em arquiteturas típicas de sistemas de informação, incluindo redes, sistemas operacionais e aplicativos.
- Integrar as metodologias de arquitetura de segurança e desenvolvimento de sistemas.

- Identificar, incrementar e implementar controles de segurança.
- Integrar segurança e privacidade dos sistemas de informação
- Definir garantia e compreender o papel da garantia na segurança dos sistemas de informação.
- Identificar as salvaguardas que podem ser implementadas no sistema de informação para garantir sua segurança.

Principais salvaguardas que podem ser implementadas em um sistema de informação:

- Firewalls;
- Antivírus/Antimalware;
- Autenticação Multifator (MFA);
- Criptografia;
- Controle de Acesso;
- Monitoramento de Segurança;
- Patches e Atualizações;
- Backup e Recuperação de Dados;
- Segregação de Redes;
- Políticas de Senha Forte;
- Gestão de Incidentes;
- Treinamento e Conscientização;
- Controles de Auditoria;
- Restrições de Software;
- Monitoramento de Terceiros.