Prime

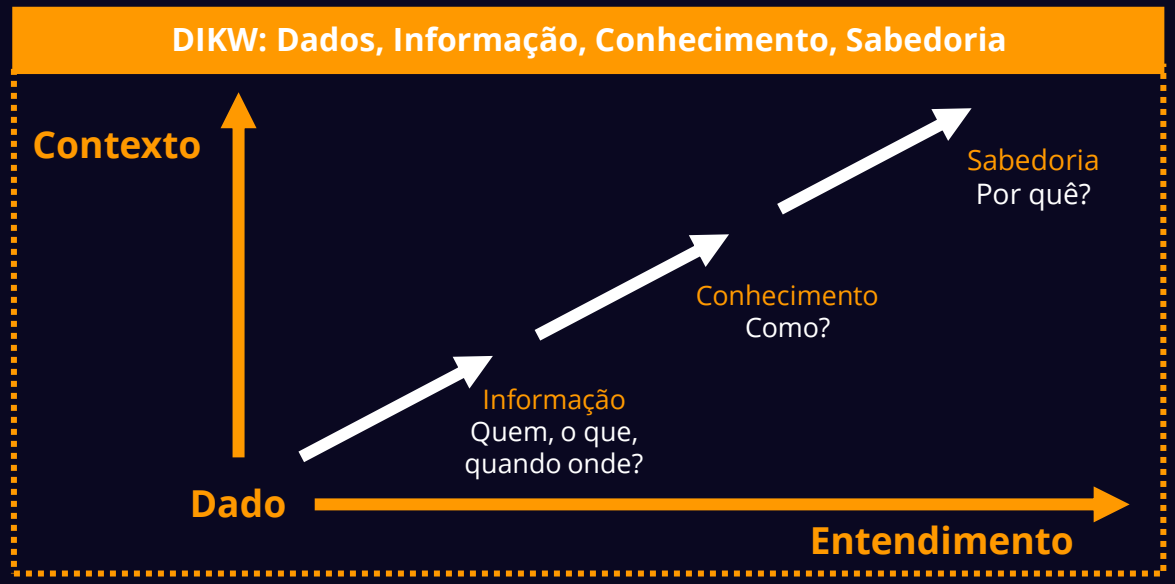
ISF – PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

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.

- Um dado se transforma em informação quando é possível responder essas questões:
  - ✓ Quem?
  - ✓ O que?
  - ✓ Quando?
  - ✓ Onde?

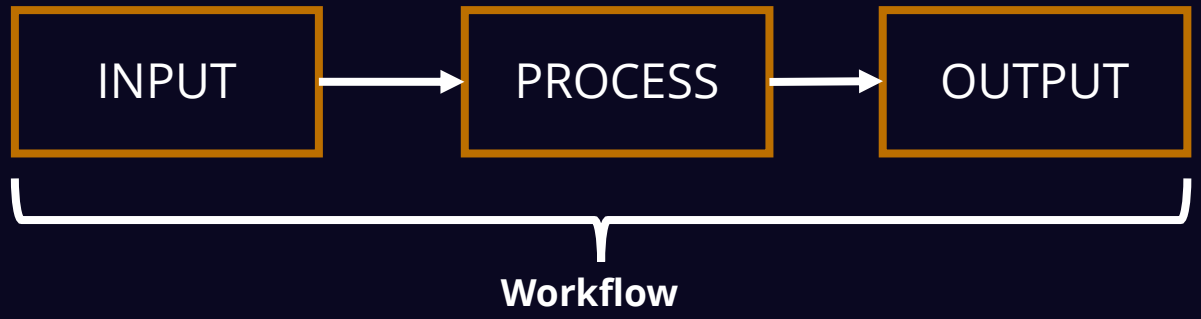
Dados:	190477
Informações:	19/04/77 mm-dd-aa



Análise da Informação

- A análise da informação fornece uma imagem clara de como a informação “flui” na organização;
- Em todos esses passos, o mais importante é que a informação seja confiável;
- Os resultados de uma Análise da Informação podem ser usados para desenvolver um Sistema de Informação.

Sistema baseado no seu 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;

Processos Operacionais e Informações

- A Gestão está dividida em Estratégica, Tática e Operacional;
- Um Processo Operacional é o processo que está no núcleo do negócio;
- Em um processo operacional, as pessoas trabalham em um produto ou serviço para um cliente;
- Um processo operacional tem os seguintes componentes principais: Entrada, Atividades e Saída;
- Existem vários tipos de Processos Operacionais:
  - ✓ **Processo Primário**

    Ex.: Fabricar uma guitarra.
  - ✓ **Processo Orientador ou Gerenciamento**

    Ex.: Planejar a estratégia dos processos da empresa, como gestão financeira, governança, melhoria contínua, performance.
  - ✓ **Processo de Apoio ou Suporte**

    Ex.: Processos de fabricação, processo de vendas, de RH para contratar recursos.
- Informação se tornou um importante fator de produção na realização dos Processos Operacionais;
- Um dos métodos para determinar o valor da informação é verificar o papel da informação nos vários Processos Operacionais;
- Cada Processo Operacional define requisitos específicos para o fornecimento de informações;
- Há processos que são muito dependentes da disponibilidade de informações.

  Ex.: site da empresa.
- Outros processos são mais dependentes da precisão das informações.

  Ex.: preços dos produtos

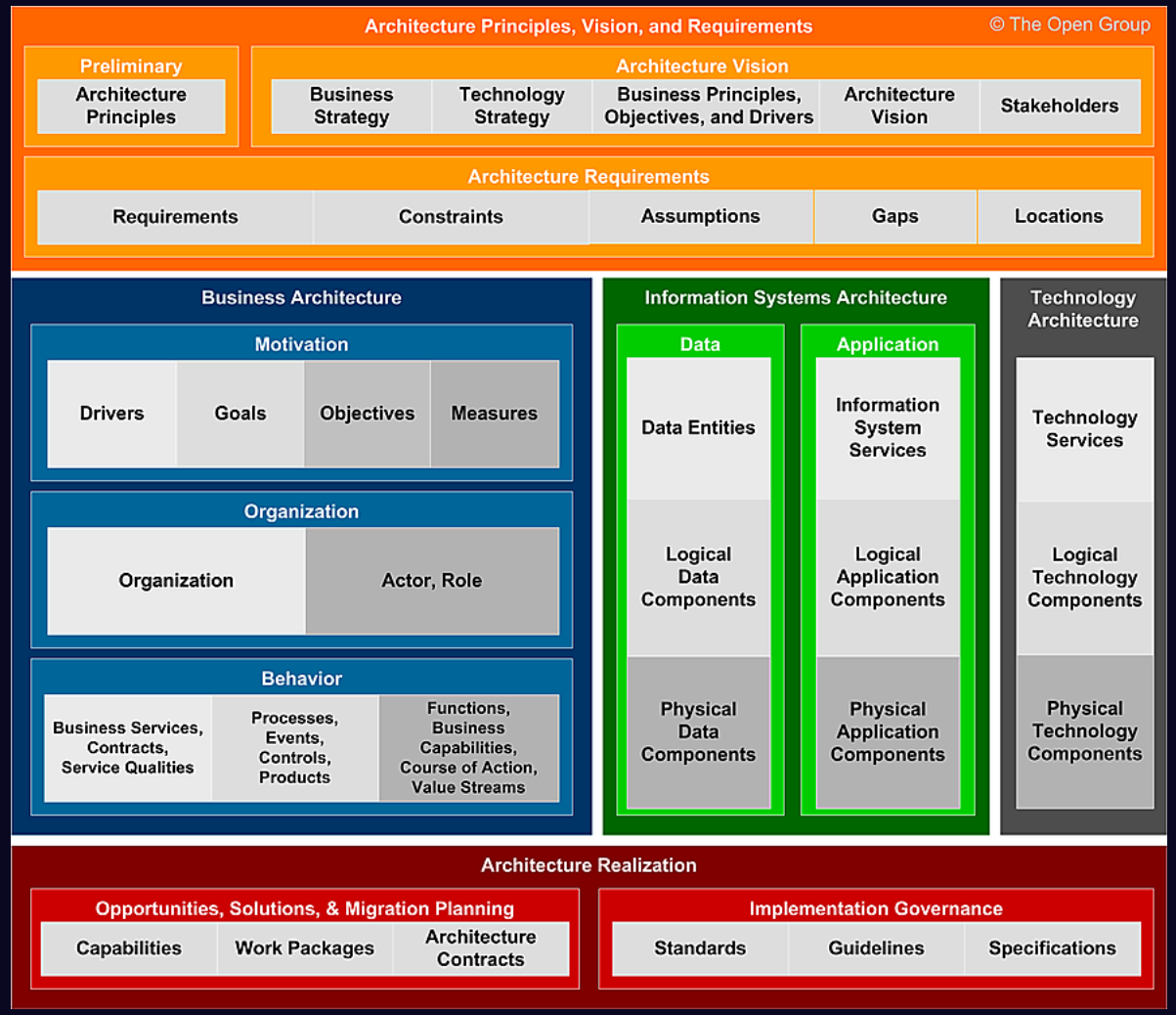
Arquitetura da Informação

- 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 devem reconhecer a importância da arquitetura da informação ou então elas correm o risco de criar grandes conteúdos e funcionalidades que ninguém nunca vai encontrar;
- O desafio é orientar as pessoas através da vasta quantidade de informações ofertadas a perceberam o seu valor.

Arquitetura da Informação e **Segurança da Informação**

- A SI está intimamente relacionada à Arquitetura da Informação;
- A arquitetura da informação é o processo que foca no COMO será feito a prestação de informação dentro da empresa;
- A SI pode ajudar a garantir que o conjunto de requisitos dessa prestação seja feita através da Arquitetura da Informação;
- A Arquitetura da Informação se concentra em atender a necessidade de informação de uma organização;
- A Arquitetura da Informação está preocupada com a maneira pela qual a informação pode ser organizado;
- A SI pode apoiar este processo, garantindo confidencialidade, integridade e disponibilidade da informação.

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

Gestão da Informação

- A Gestão da Informação executa a Política relativa ao fornecimento de informação de uma organização;
- Um Gerente de Informação pode fazer uso da Arquitetura da Informação e de uma Análise da Informação;
- A Gestão da Informação envolve muito mais do que o processamento automatizado de informações;
- Em muitos casos, faz parte a estratégia de comunicação externa e a forma de mídia usada;
- A gestão da informação descreve o meio pelo qual uma organização trata a informação, como:
  - ✓ Planejamento;
  - ✓ Coleta;
  - ✓ Organização;
  - ✓ Utilização;
  - ✓ Controle;
  - ✓ Disseminação;
  - ✓ Descarte.

- Se baseia em, e combina habilidades e recursos de:
  - ✓ Biblioteconomia e ciência da informação;
  - ✓ Tecnologia da informação;
  - ✓ Gerenciamento de registros;
  - ✓ Arquivamento e administração geral.

Atividades da **Gestão da Informação**

- O foco das atividades de gestão da informação é usar a informação como um recurso, independentemente da forma física em que ela ocorre.
- Principais atividades:
  - ✓ Classificação e codificação;
  - ✓ Indexação de assunto;
  - ✓ Construção e uso de dicionários e vocabulários controlados;
  - ✓ Catalogação e indexação por nomes, lugares e eventos;
  - ✓ Projeto de banco de dados e estruturas de dados;
  - ✓ Armazenamento físico de livros e registros, em papel e em formato eletrônico;
  - ✓ Armazenamento de imagens fotográficas e digitalizadas;
  - ✓ Auditorias de informação: revisão dos recursos de informação de uma organização;
  - ✓ Documentação de objetos de museu, tanto para fins de administração quanto como um recurso para estudos.

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;
- A Internet Web3 é semelhante ao Peer-to-Peer. (Web3 Foundation)

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, quer deliberada ou acidental;
- É evitar 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* em um sistema;
  - ✓ Um usuário que 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 adequeadas de roteadores e firewalls.

Características da **Disponibilidade**

01

Oportunidade (Pontualidade)

Os sistemas de informação estão disponíveis quando necessários;

02

Continuidade

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

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.

Hexagrama **Parkeriano**

- Conjunto de seis elementos da segurança da informação proposto por Donn B. Parker;
- Soma mais três atributos aos três atributos clássicos de segurança do triângulo CIA;

1. **Confidencialidade;**
2. **Posse ou controle;**
3. **Integridade;**
4. **Autenticidade;**
5. **Disponibilidade;**
6. **Utilidade.**

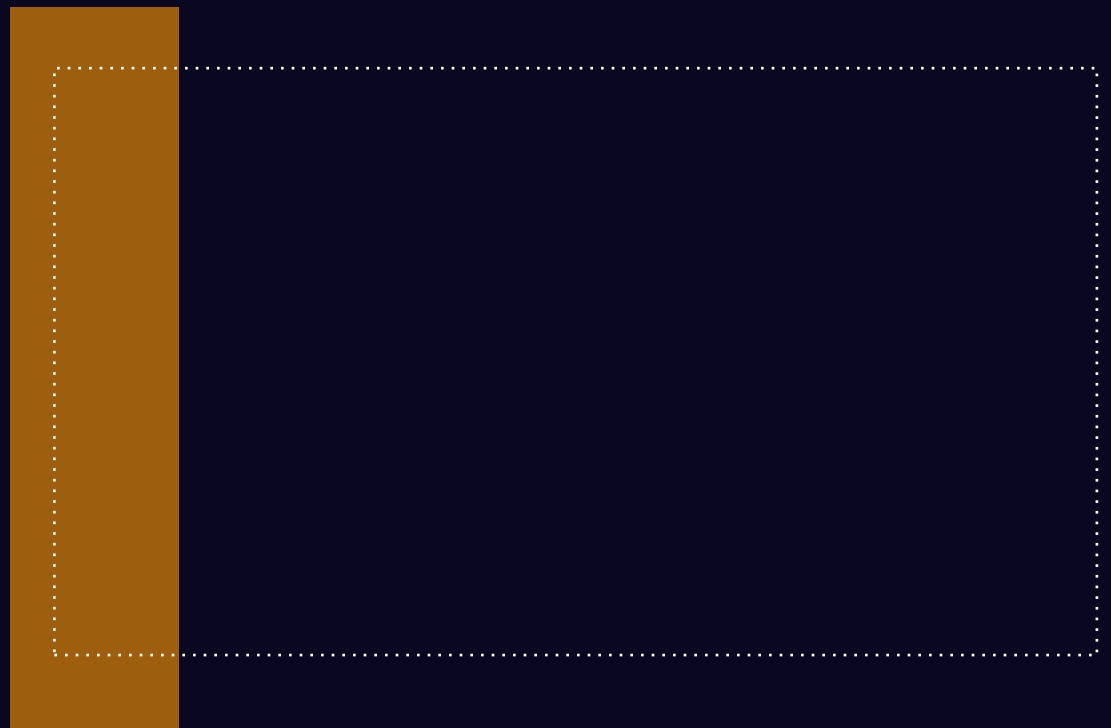
- ✓ Estes elementos são únicos, ou seja, não são divididos;
- ✓ Não se sobrepõem, pois referem-se a aspectos únicos da informação;
- ✓ Uma violação pode ser afetado por ou mais elementos.

Posse ou Controle

- Um dos elementos específicos do Hexagrama Parkeriano;
- 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.

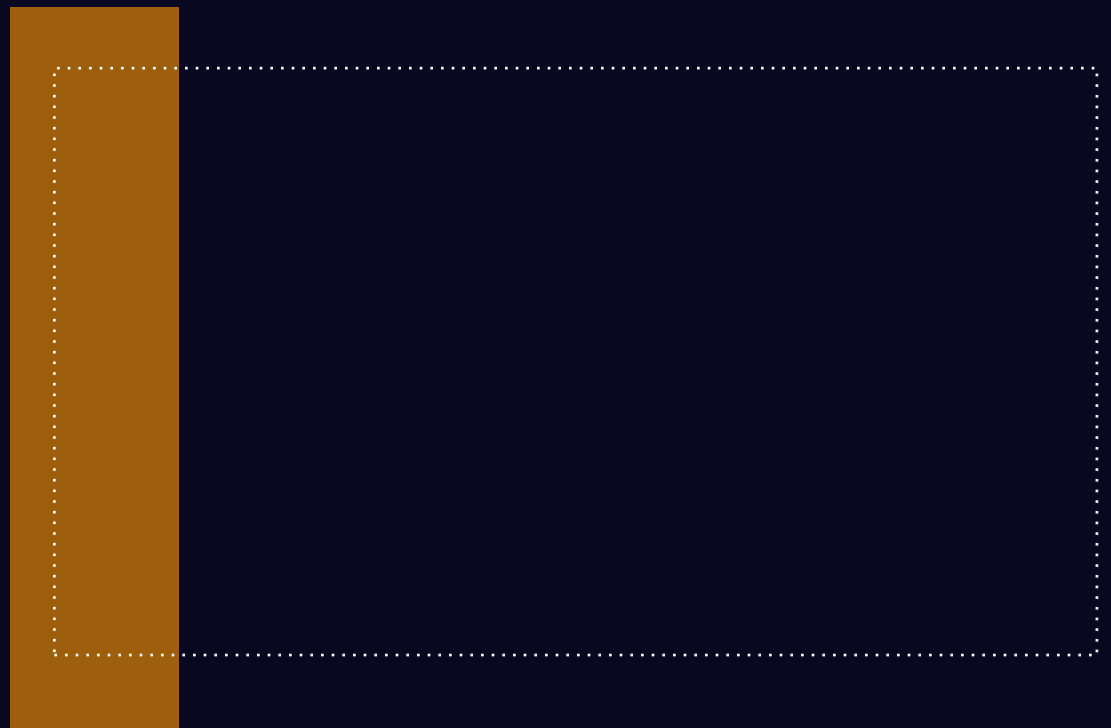


Autenticidade

- Um dos elementos específicos do Hexagrama Parkeriano;
- Busca verificar 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

- Um dos elementos específicos do Hexagrama Parkeriano;
- 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!

OBRIGADO

ISF – PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO