Arquitetura corporativa e as questões de Segurança da Informação

Pilares do Togaf

Existem quatro domínios de arquitetura no TOGAF que oferecem especializações para empresas.

- **Arquitetura de negócios:** inclui informações sobre estratégia de negócios, governança, organização e como adaptar os processos existentes dentro da organização.

- **Arquitetura de aplicativos:** um projeto para estruturar e implantar sistemas de aplicativos e de acordo com as metas de negócios, outras estruturas organizacionais e todos os principais processos de negócios.

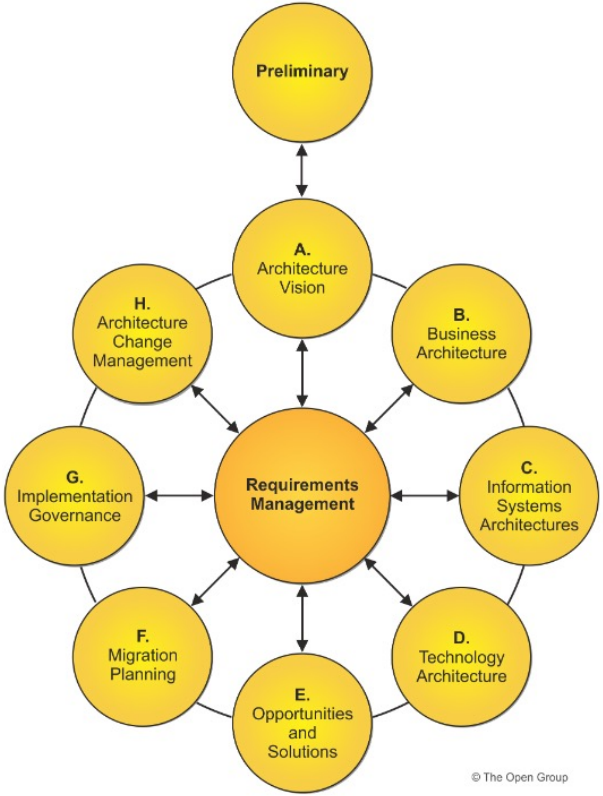
- **Arquitetura de dados:** definição do armazenamento, gerenciamento e manutenção de dados da organização, incluindo modelos de dados lógicos e físicos.

- **Arquitetura técnica:** também chamada de arquitetura de tecnologia. Descreve todo o hardware, software e infraestrutura de TI necessários para desenvolver e implantar aplicativos de negócios.

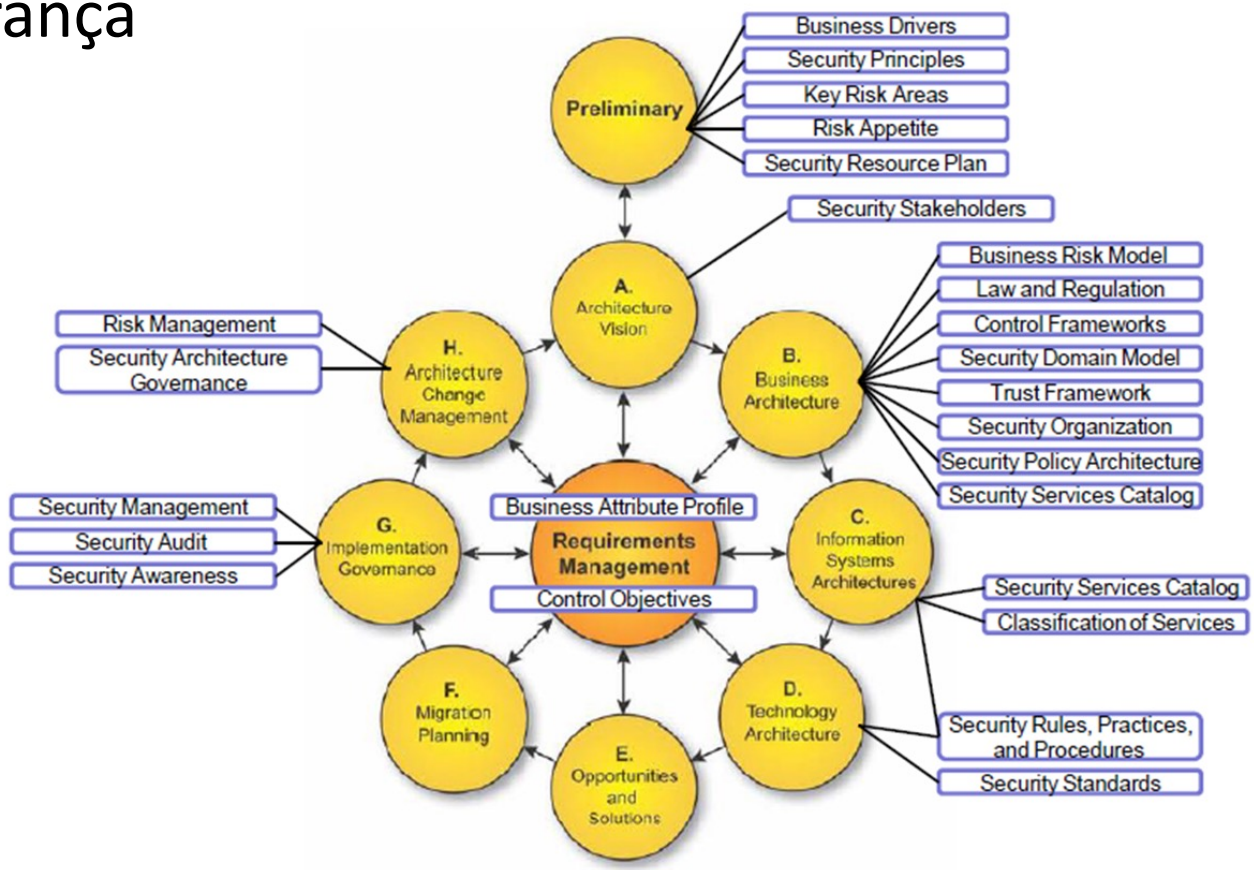
Togaf


Arquitetura de Negócios
Arquitetura Tecnológica
Arquitetura Corporativa
Arquitetura de Dados
Arquitetura de Aplicação

Togaf e Segurança



Togaf e Segurança



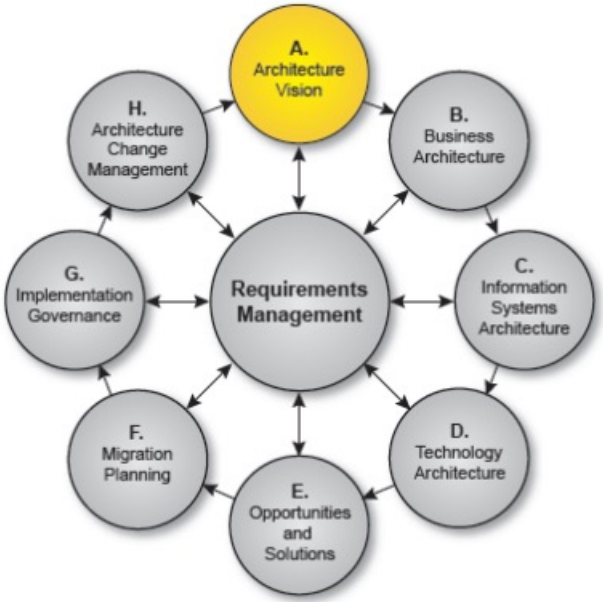
Mas o que isso tem a haver com Segurança

Alguns conceitos de Segurança

Alguns dados sobre Segurança

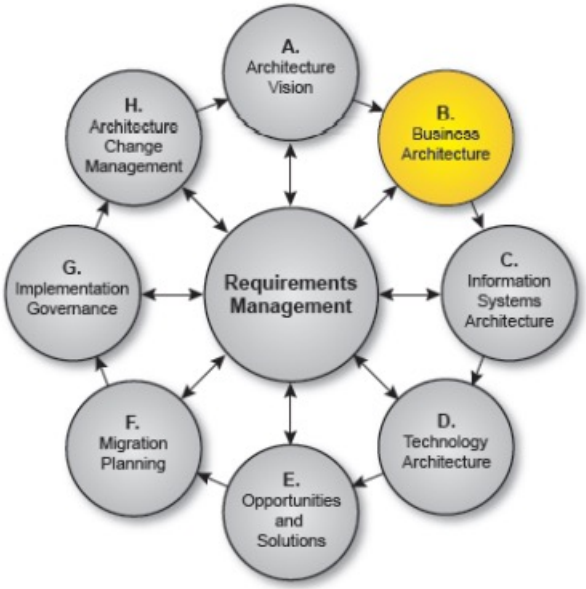
- Brasil foi 5º país com mais ataques cibernéticos em 2021
- 80% dos crimes cibernéticos poderiam ter sido prevenidos.
- Levantamento mostra que ataque cibernético no Brasil cresceu mais de 94% em 2022.

Togaf e Segurança



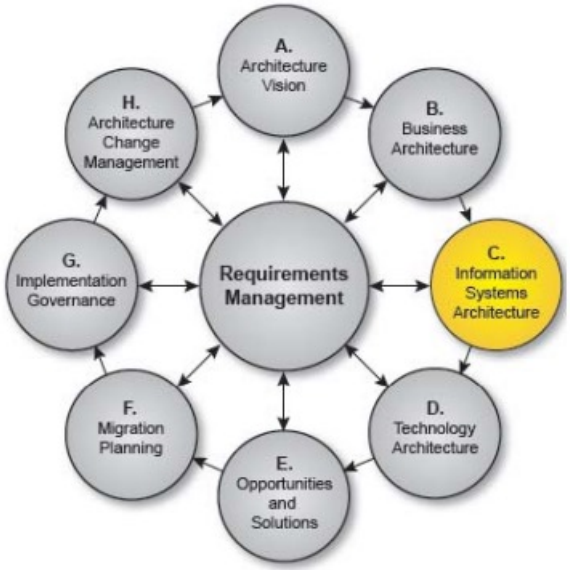
- Validar os princípios de negócios, objetivos de negócios e estratégias impulsionadores de negócios da organização.
- Definir o escopo e identificar e priorizar os componentes necessários para a arquitetura de SI.
- Definir as partes interessadas relevantes, e suas preocupações e necessidades com relação a SI.
- Definir os principais requisitos de negócios a serem abordados neste esforço de arquitetura e as restrições que devem ser tratadas

Togaf e Segurança



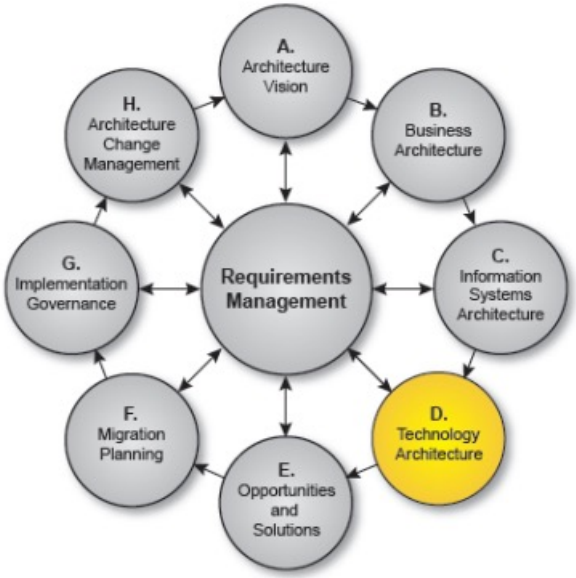
- Desenvolver uma Arquitetura alvo de SI, descrevendo o produto e/ou estratégia de serviço, e a organizacional, funcional, processo, informações, com base nos princípios de negócios, objetivos de negócios e impulsionadores estratégicos
- Selecionar a arquitetura de SI, que seja relevante para endereçar as questões de negócio e a preocupação das partes interessadas.
- Apoiar a seleção de ferramentas e técnicas relevantes a serem usadas para atender aos requisitos definidos.

Togaf e Segurança



- Desenvolver Arquitetura alvo cobrindo um ou ambos dos os domínios de SI definidos, compreendendo os sistemas necessários.
- Neste momento a arquitetura de SI deve interagir com a arquitetura de TI e olhar a completude do atendimento necessário.

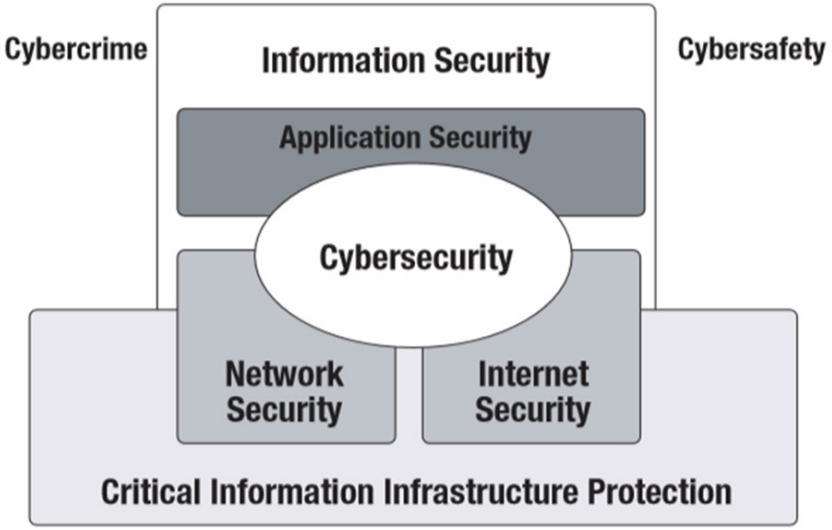
Togaf e Segurança



- Neste ponto começa a ser desenvolvida uma Arquitetura Tecnológica que será a base de todos os requisitos de SI.
- Para as questões de segurança, essa iteração é utilizada para refinar as especificações dos detalhes técnicos e dos requisitos necessários para atender as questões de segurança.

Segurança – uma visão global

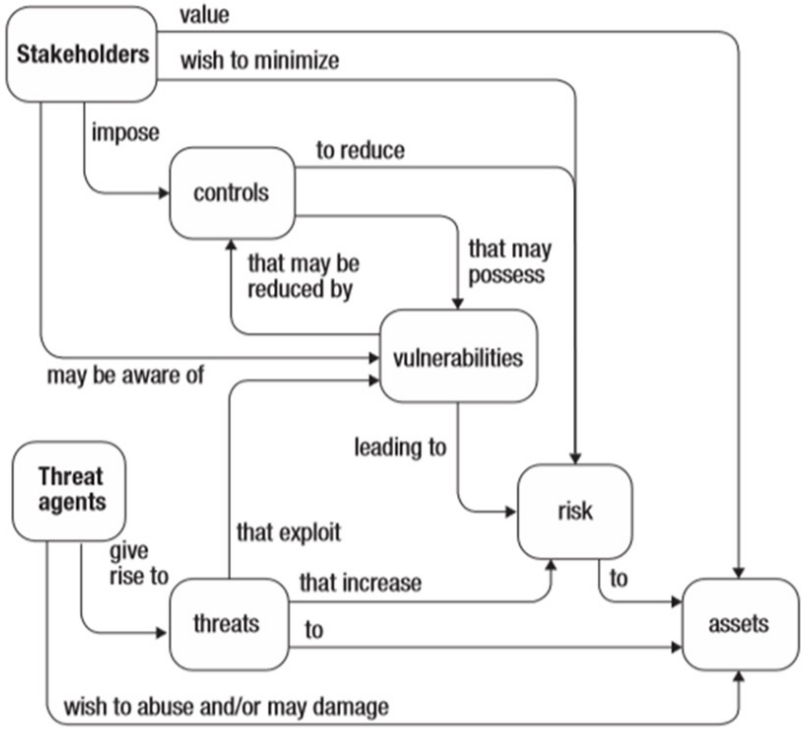
Figure 1.2—Relationship Among Cybersecurity and Other Security Domains



Source: International Organization for Standardization, *ISO/IEC 27032:2012: Information technology—Security techniques—Guidelines for cybersecurity*, Switzerland, 2012

Segurança – o que atender

Figure 1.3—Security Concepts and Relationships



Source: International Organization for Standardization, *ISO/IEC 27032:2012: Information technology—Security techniques—Guidelines for cybersecurity*, Switzerland, 2012

Segurança – exemplo de requesitos

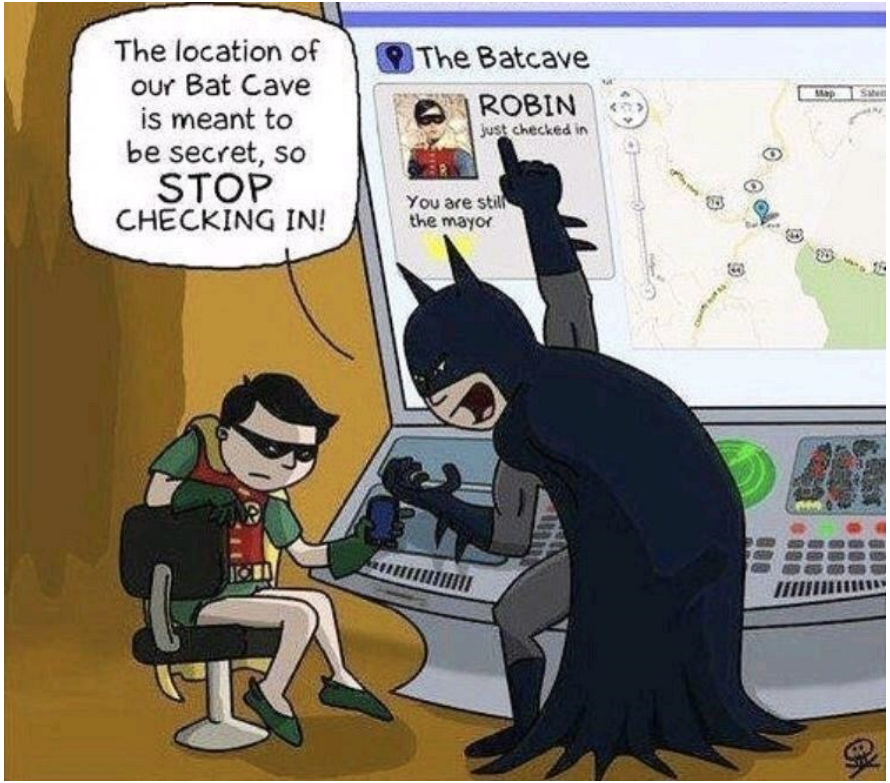
Figure 1.6—Confidentiality, Integrity and Availability Model and Related Impacts

Requirement	Impact and Potential Consequences	Methods of Control
Confidentiality: The protection of information from unauthorized disclosure	Loss of confidentiality can result in the following consequences: • Disclosure of information protected by privacy laws • Loss of public confidence • Loss of competitive advantage • Legal action against the enterprise • Interference with national security • Loss of compliance	Confidentiality can be preserved using the following methods: • Access controls • File permissions • Encryption
Integrity: The accuracy and completeness of information in accordance with business values and expectations	Loss of integrity can result in the following consequences: • Inaccuracy • Erroneous decisions • Fraud • Failure of hardware • Loss of compliance	Integrity can be preserved using the following methods: • Access controls • Logging • Digital signatures • Hashes • Backups • Encryption
Availability: The ability to access information and resources required by the business process	Loss of availability can result in the following consequences: • Loss of functionality and operational effectiveness • Loss of productive time • Fines from regulators or a lawsuit • Interference with enterprise's objectives • Loss of compliance	Availability can be preserved using the following methods: • Redundancy of network, system, data • Highly available system architectures • Data replication • Backups • Access controls • A well-designed disaster recovery plan or business continuity plan

Principais tipos de ataque em 2022

- DDoS Attack
- Phishing
- Ransomware
- Malware

Segurança – Mas quem acredita



As questões de segurança começam por um treinamento constante, onde os conceitos devem ser repetidos a treinados com todos os colaboradores da organização.

OBRIGADO

Carlos Guerra

55-11-9-7599-0071

carlos.guerra@gsoconsulting.com.br

GSOCONSULTING.COM.BR