Introdução à segurança

Segurança ?

```
88b .d8888.  .d88b.   .o88b. d888888b d88888b d8888
   88'  YP .8P  Y8. d8P  Y8   `88'   88         88
   `8bo.   88    88 8P         88    88ooooo    88
     `Y8b. 88    88 8b         88    88         88
   db   8D `8b  d8' Y8b  d8   .88.   88.        88
   `8888Y'  `Y88P'   `Y88P' Y888888P Y88888P    YP


{1}--Venom
{2}--sqlmap
{3}--Shellnoob
  }--commix
   --FTP Auto Bypass
   --jboss-autopwn
     Blind SQL Automatic Injection And Exploit
     uteforce the Android Passcode given the hash
     mla SQL injection Scanner

     To Main Menu
```

Segurança Informática

Disciplina que se foca na previsibilidade de sistemas, processos, ambientes…

- **Envolve todos os aspetos do ciclo de vida:**
  - Planeamento
  - Desenvolvimento
  - Execução
  - Processos
  - Pessoas
  - Clientes e Fornecedores
  - Mecanismos
  - Normas
  - Propriedade intelectual, …

Segurança: planeamento

Desenho de uma solução que responda aos requisitos, num contexto normativo

- **Sem falhas**
  - Todos os estados de funcionamento são previstos
  - Não existem estados que fujam à lógica pretendida
    - Mesmo que se usem transições forçadas

- **Respondendo ao ambiente normativo**
  - Específico de cada atividade ou setor
  - Ex: ISO 27001, ISO 27007, ISO 37001

Segurança: desenvolvimento

Implementação uma solução que responda ao design, sem outros modos de funcionamento

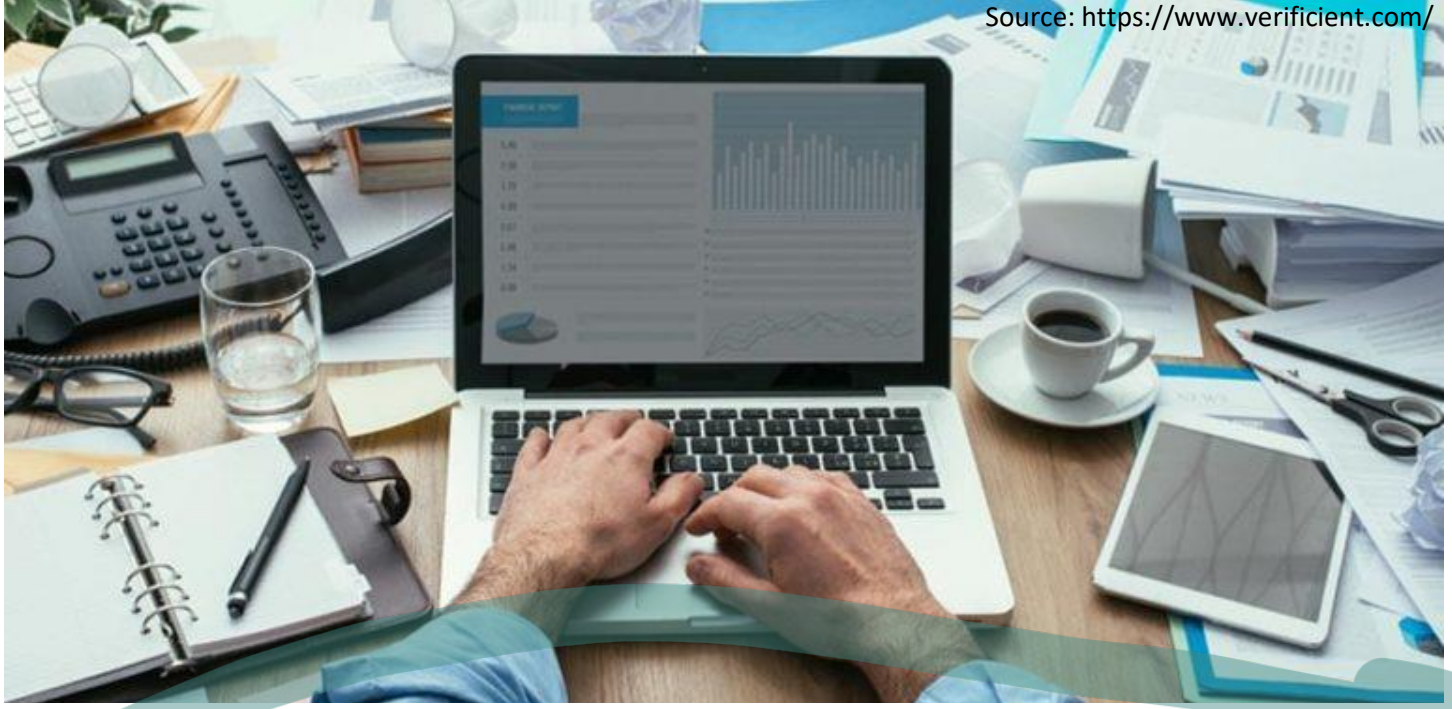
- **Sem erros (bugs) que comprometam a execução correta**
  - Sem "crashes"
  - Sem respostas inválidas ou inesperadas
  - Com tempo de execução correto
  - Com um consumo de recursos adequado
  - Sem fugas de informação
- **Software:**
  - Envolve uma implementação cuidada
  - Envolve testes de forma a se obter uma solução que faça o pretendido… e apenas o pretendido

Segurança: execução

Execução de um código tal como foi escrito e com todos os processos previstos

- **Ambiente controlado, não manipulável, não observável**
- **Sem a existência de comportamentos anómalos, introduzidos pelo ambiente onde executa**
  - Aspetos relevantes: velocidade dos discos, quantidade de RAM, comunicações fiáveis, …

Source: https://www.verificient.com/



ISO 27001 – Clean Desk Policy

Segurança: pessoas, parceiros

Comportamento dos sujeitos não possui um impacto negativo na solução

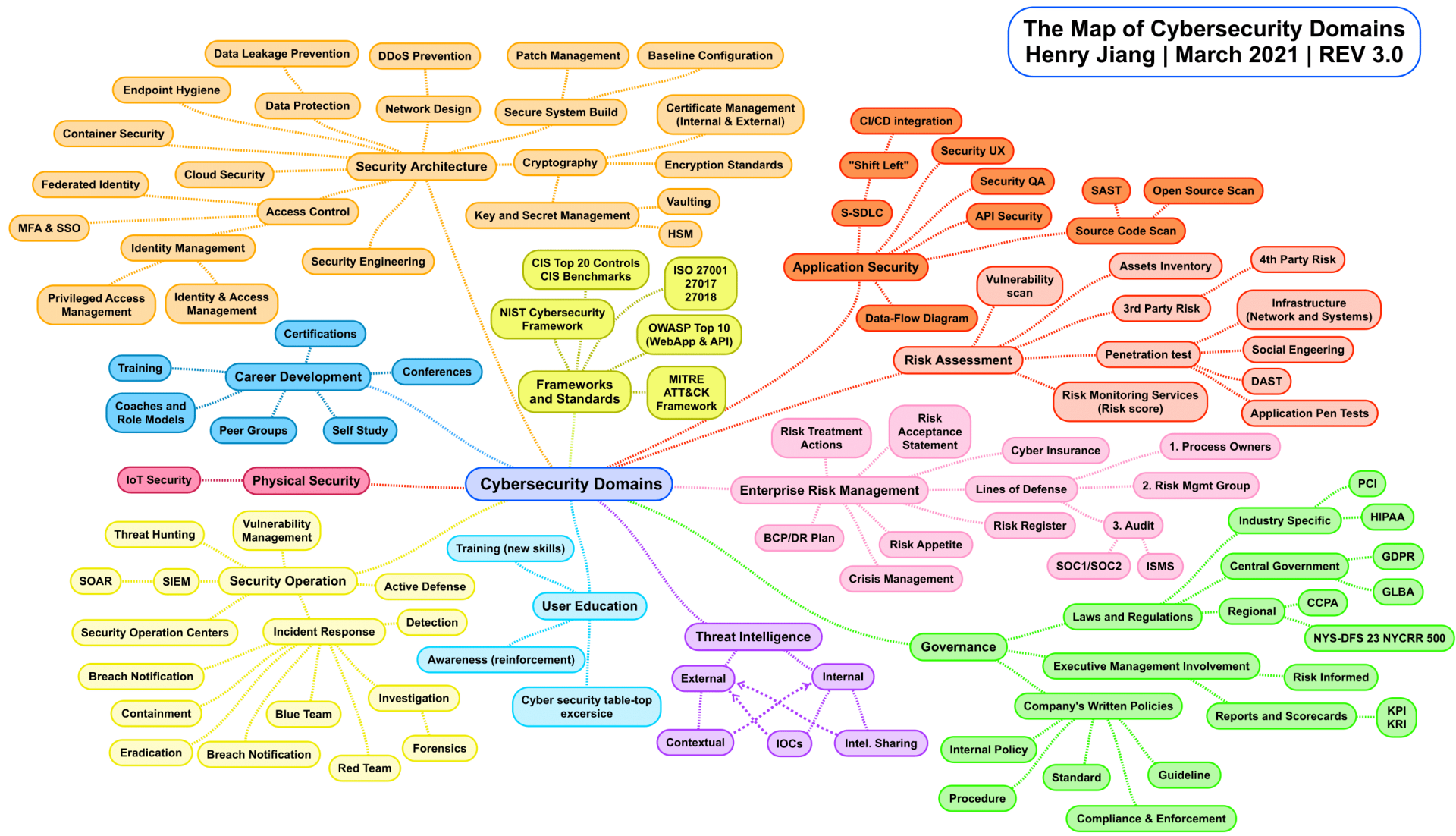
"evil maid" → attack from the inside, the attacker as acess to the physical to the system

- **Existem normas que definem qual o comportamento correto**
- **Possuem formação para distinguir quais os comportamentos corretos e incorretos**
- **Possuem os incentivos para manter comportamentos**
- **Quando comprometidos ou desviantes, as ações têm um impacto limitado**

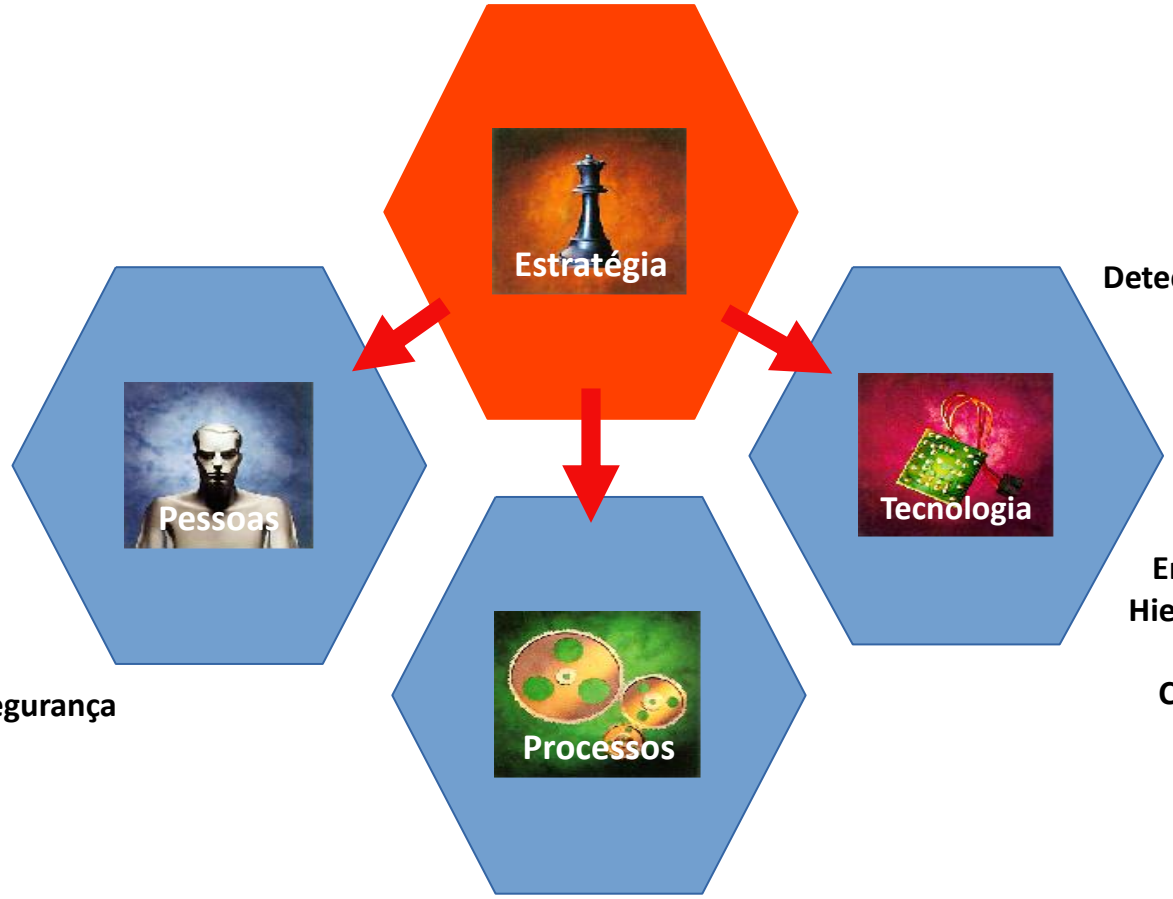
Segurança: análise e auditoria

Qual é o comportamento atual da solução?

- **Identificar aspetos desviantes**
  - Falhas, erros, comportamentos
- **Identificar o risco da solução ser desviada**
  - Exposição a possíveis atacantes
  - Incentivos para que seja desviada
  - Potenciais atores
- **Identificar o impacto dos desvios**
  - Perda total dos dados? Disrupção? Custo de Operação?


The Map of Cybersecurity Domains
Henry Jiang | March 2021 | REV 3.0
Cybersecurity Domains
Security Architecture
Data Leakage Prevention
DDoS Prevention
Patch Management
Baseline Configuration
Endpoint Hygiene
Data Protection
Network Design
Secure System Build
Certificate Management (Internal & External)
Container Security
Cloud Security
Cryptography
Encryption Standards
Federated Identity
Access Control
Vaulting
MFA & SSO
Key and Secret Management
HSM
Identity Management
Security Engineering
Privileged Access Management
Identity & Access Management
Application Security
CI/CD integration
Security UX
"Shift Left"
Security QA
S-SDLC
API Security
SAST
Open Source Scan
Source Code Scan
Frameworks and Standards
CIS Top 20 Controls
CIS Benchmarks
ISO 27001
27017
27018
NIST Cybersecurity Framework
OWASP Top 10 (WebApp & API)
MITRE ATT&CK Framework
Risk Assessment
Vulnerability scan
Assets Inventory
4th Party Risk
Data-Flow Diagram
3rd Party Risk
Infrastructure (Network and Systems)
Penetration test
Social Engeering
DAST
Risk Monitoring Services (Risk score)
Application Pen Tests
Career Development
Certifications
Training
Conferences
Coaches and Role Models
Peer Groups
Self Study
Enterprise Risk Management
Risk Treatment Actions
Risk Acceptance Statement
Cyber Insurance
1. Process Owners
Lines of Defense
2. Risk Mgmt Group
Risk Register
3. Audit
BCP/DR Plan
Risk Appetite
SOC1/SOC2
ISMS
Crisis Management
Physical Security
IoT Security
Security Operation
Threat Hunting
Vulnerability Management
SOAR
SIEM
Active Defense
Security Operation Centers
Incident Response
Detection
Breach Notification
Containment
Blue Team
Investigation
Eradication
Breach Notification
Red Team
Forensics
Training (new skills)
User Education
Awareness (reinforcement)
Cyber security table-top excersice
Threat Intelligence
External
Internal
Contextual
IOCs
Intel. Sharing
Governance
Laws and Regulations
Industry Specific
PCI
HIPAA
Central Government
GDPR
GLBA
Regional
CCPA
NYS-DFS 23 NYCRR 500
Executive Management Involvement
Risk Informed
Company's Written Policies
Reports and Scorecards
KPI
KRI
Internal Policy
Standard
Guideline
Procedure
Compliance & Enforcement

Dimensões a considerar



Seleção
Treino
Sensibilização
Organização da segurança

Deteção de Vulnerabilidades
Firewalls
Autenticação
Controlo de Acesso
Registos Auditáveis
Criptografia
Assinaturas Digitais
Entidades de Certificação
Hierarquias de Certificação
Deteção de ataques
Controlos de integridade

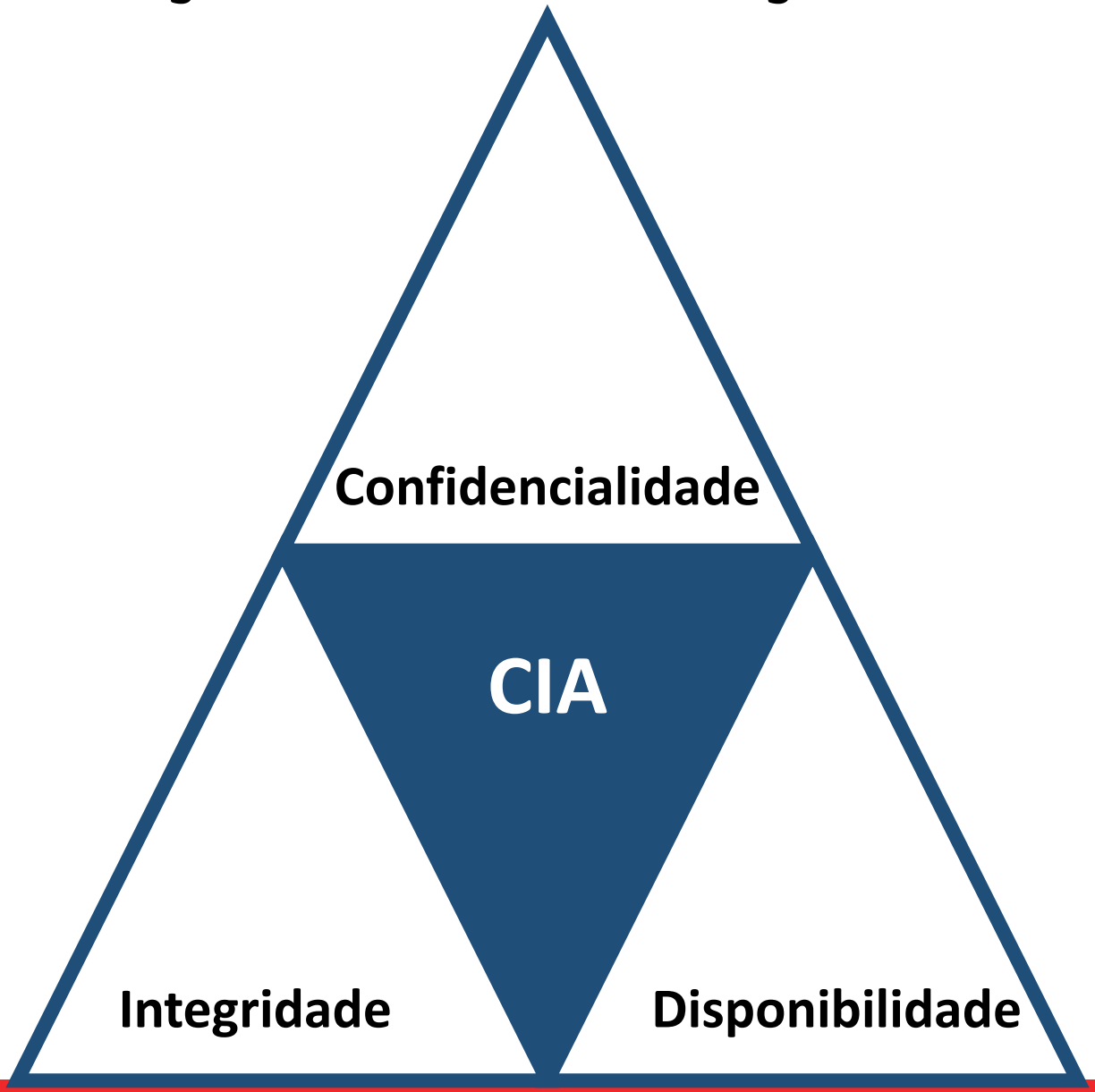
Políticas de segurança
Procedimentos administrativos de segurança
Procedimentos de auditoria e resposta a incidentes

Facetas

Facetas da segurança são interligadas e indissociáveis

- **Defensiva: foca-se na manutenção da previsibilidade**
- **Ofensiva: foca-se na violação da previsibilidade**
  - Pode ter intuito malicioso/criminoso
  - Pode ter intuito de validação da solução (Red Teams)
- **Outras:**
  - **Engenharia Reversa**: recuperação de design a partir do produto
  - **Forense**: identificar ações passadas e recuperar informação
  - **Recuperação de Desastres**: minimizar impacto
  - **Auditoria**: validar o cumprimento com certas premissas

Segurança da Informação



Segurança da Informação

- **Confidencialidade: Informação só pode ser acedida por um grupo restrito de sujeitos**

- **Medidas:**
  - Cifrar informação
  - Usar senhas de acesso (fortes)
  - Sistemas de Identificação e Autenticação
  - Firewalls, Grupos de segurança
  - Portas, Paredes robustas
  - Pessoal de Segurança
  - Formação das pessoas

Segurança da Informação

- **Integridade: Informação mantém-se inalterada**
  - Pode ser aplicada a comportamentos de dispositivos e serviços

- **Medidas:**
  - Controlos de integridade (sínteses)
  - Backups
  - Controlos de Acesso
  - Dispositivos de armazenamento robustos
  - Processos de verificação da informação

Segurança da Informação

- **Disponibilidade: Informação mantém-se disponível**
  - Pode ser aplicada a serviços e dispositivos
  - Inglês: **A**vailability

- **Medidas:**
  - Backups
  - Planos de recuperação de desastres
  - Redundância
  - Virtualização
  - Monitorização

Segurança da Informação - também

- **Privacidade: como é tratada a informação pessoal**
  - Recolha
  - Processamento
  - Armazenamento
  - Partilha de informação
  - Eliminação

- **Medidas:**
  - Controlos de acesso
  - Transparência dos processos
  - Cifras
  - Controlos de integridade e de autenticidade
  - Registos

Objetivos da Segurança (1/3)

- **Defesa contra catástrofes**
  - Fenómenos naturais
  - Temperatura anormal, relâmpagos, picos de energia, inundações, radiação…

- **Degradação dos sistemas informáticos físicos**
  - Setores degradados
  - Falha da fonte de alimentação
  - Erros em células da RAM ou SSD…

Objetivos da Segurança (2/3)

- **Defesa contra falhas e erros comuns**
  - Falhas de energia
  - Falhas internas aos sistemas operativos
    - Linux Kernel Panic, Windows Blue Screen, OSX panic
    - Bloqueios
    - Consumo anormal de recursos
  - Erros no Software / Erros nas Comunicações

Objetivos da Segurança (3/3)

- **Defesa contra atividades não autorizadas (adversários)**
  - Iniciados por alguém "de dentro", ou "de fora"

- **Tipos de atividades não autorizadas:**
  - Acesso a informação
  - Alteração de informação
  - Utilização de recursos
    - CPU, memória, impressão, rede…
  - Negação de serviço (DoS)
  - Vandalismo
    - Interferência do funcionamento normal, sem benefício direto para o atacante

Conceitos Fundamentais

1. Domínios

2. Políticas

3. Mecanismos

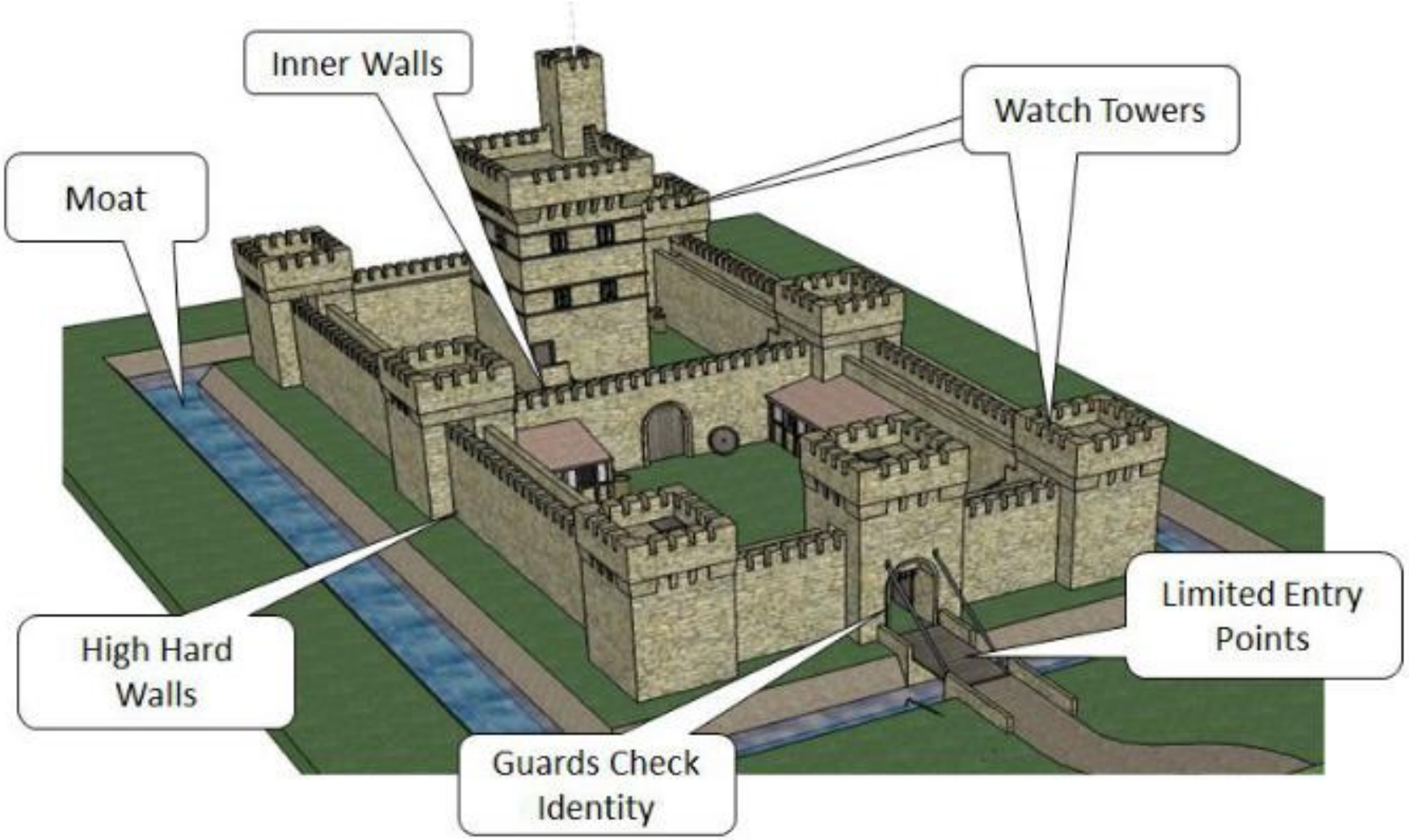
4. Controlos

Domínios de Segurança

Um conjunto de entidades que partilham atributos de segurança semelhantes

- **Servem para gerir a segurança de forma agregada**
  - Definem-se os atributos ao domínio
  - Englobam-se entidades no domínio
- **Comportamentos e interações são homogéneos dentro do domínio**
- **Domínios podem ser organizados de forma plana ou hierárquica**
- **Interações entre domínios são normalmente controladas**

Domínios de Segurança



Políticas de Segurança

Conjunto de orientações relativas à segurança que regem um domínio

- **Organização possui uma hierarquia de políticas**
  - Aplicáveis a cada domínio particular
  - Podem existir sobreposições (ex, hierarquias)
  - Podem possuir âmbitos e níveis de abstração distintos
- **Devem ser coerentes entre si**
- **Exemplo de políticas**
  - Só é possível aceder a serviços web
  - Pessoas têm de se identificar para entrar
  - Paredes devem ser robustas
  - Comunicações devem ser confidenciais

Políticas de Segurança

- **Definem o poder de cada sujeito**
  - princípio do privilégio mínimo: cada sujeito só tem acesso ao essencial para as suas funções
- **Definem os procedimentos de segurança**
  - quem faz o quê e quando
- **Definem requisitos mínimos de seg. dos sistemas**
  - Níveis de segurança,
  - Grupos de segurança
  - Autorizações e autenticação correspondentes (fraca/forte, simples/multifatorial, remota/presencial)

Políticas de Segurança

- **Definem a estratégias de defesa e de resposta**
  - Arquitetura defensiva
  - Monitoria de atividades críticas/deteção de sinais de ataques
  - Reação a ataques ou outras disrupções

- **Definem o que é correto e incorreto (legal/ilegal)**
  - Modelo baseado numa lista de negações
    - Proíbem-se algumas coisas
    - O resto é permitido
  - Modelo baseado numa lista de permissões
    - Proíbe-se tudo
    - Algumas coisas são permitidas

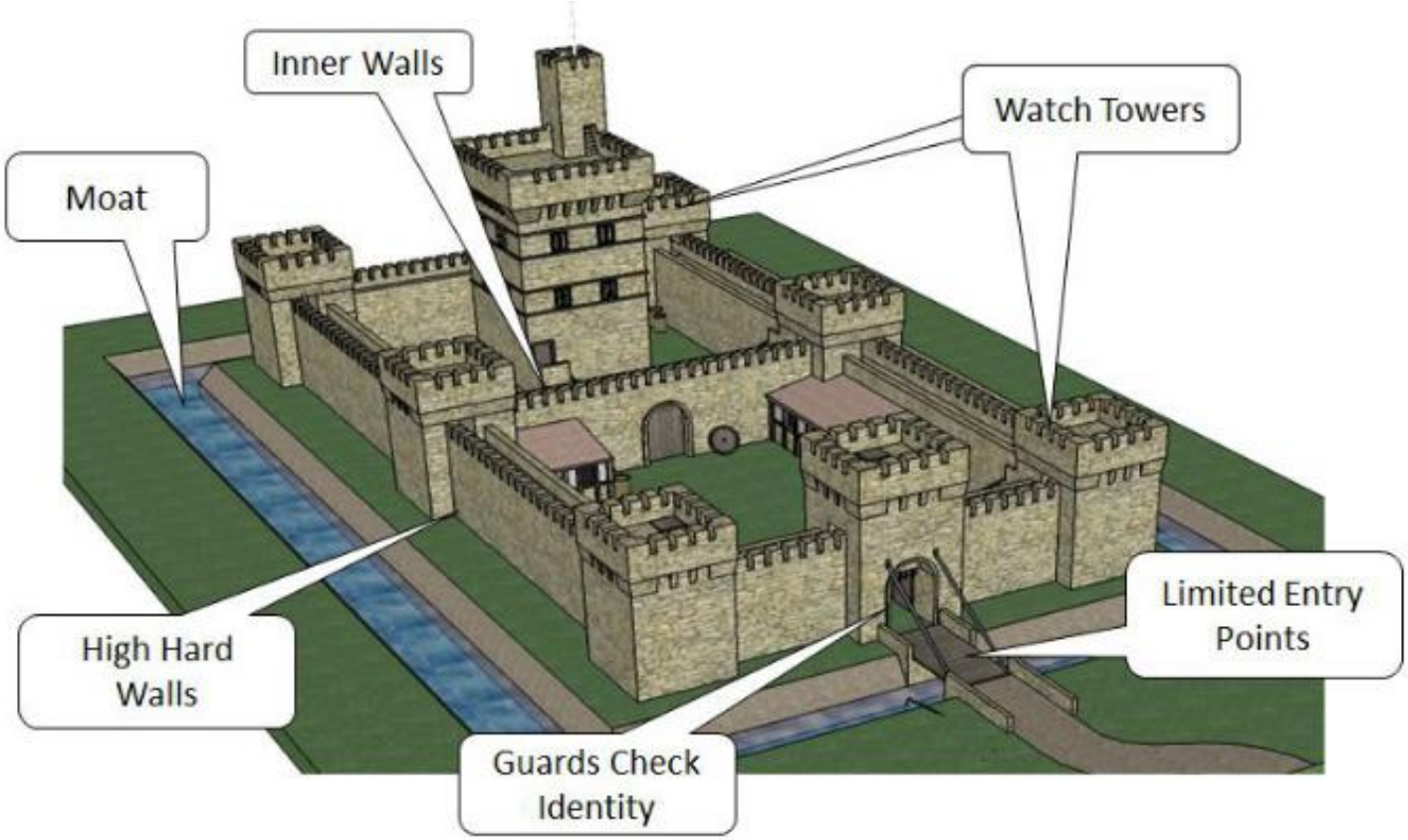
Mecanismos de Segurança

- **Mecanismos implementam as políticas no domínio**
  - Mecanismos tornam as políticas efetivas no context do domínio

- **Mecanismos de segurança genéricos:**
  - Confinamento
  - Autenticação
  - Controlo de acesso
  - Execução Privilegiada
  - Filtragem
  - Registo
  - Algoritmos e protocolos criptográficos
  - Auditorias
  - Cifras

Mecanismos de Segurança

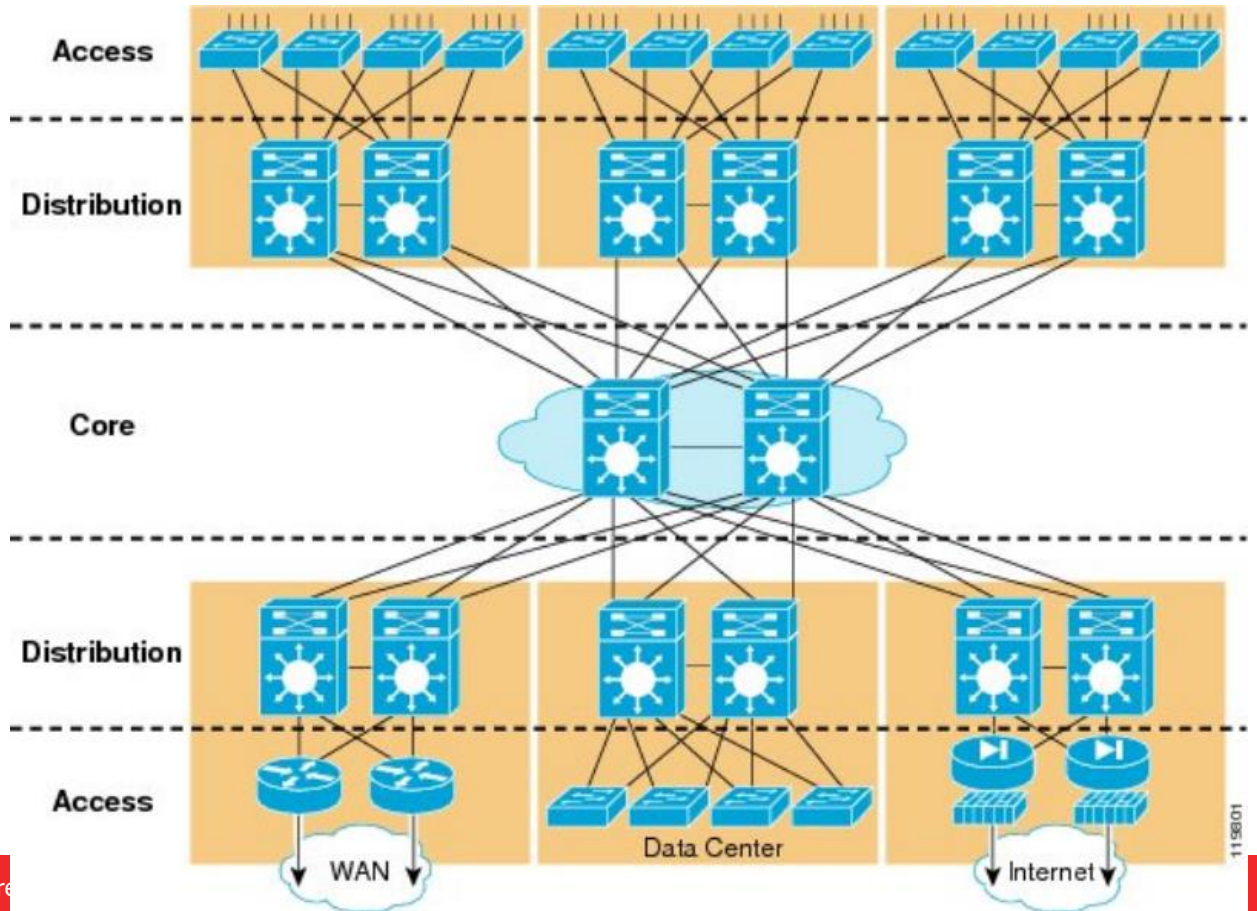
Política: Movimentos entre domínios devem ser restritos
Mecanismos: Portas, guardas, senhas, objetos/documentos



Mecanismos de Segurança

Política: Sistemas devem ser resilientes

Mecanismos: Equipamentos/ligações duplicadas, arquitetura



Controlos de Segurança

Controlos são todos e quaisquer aspetos que permitam evitar, detetar, neutralizar ou minimizar o risco

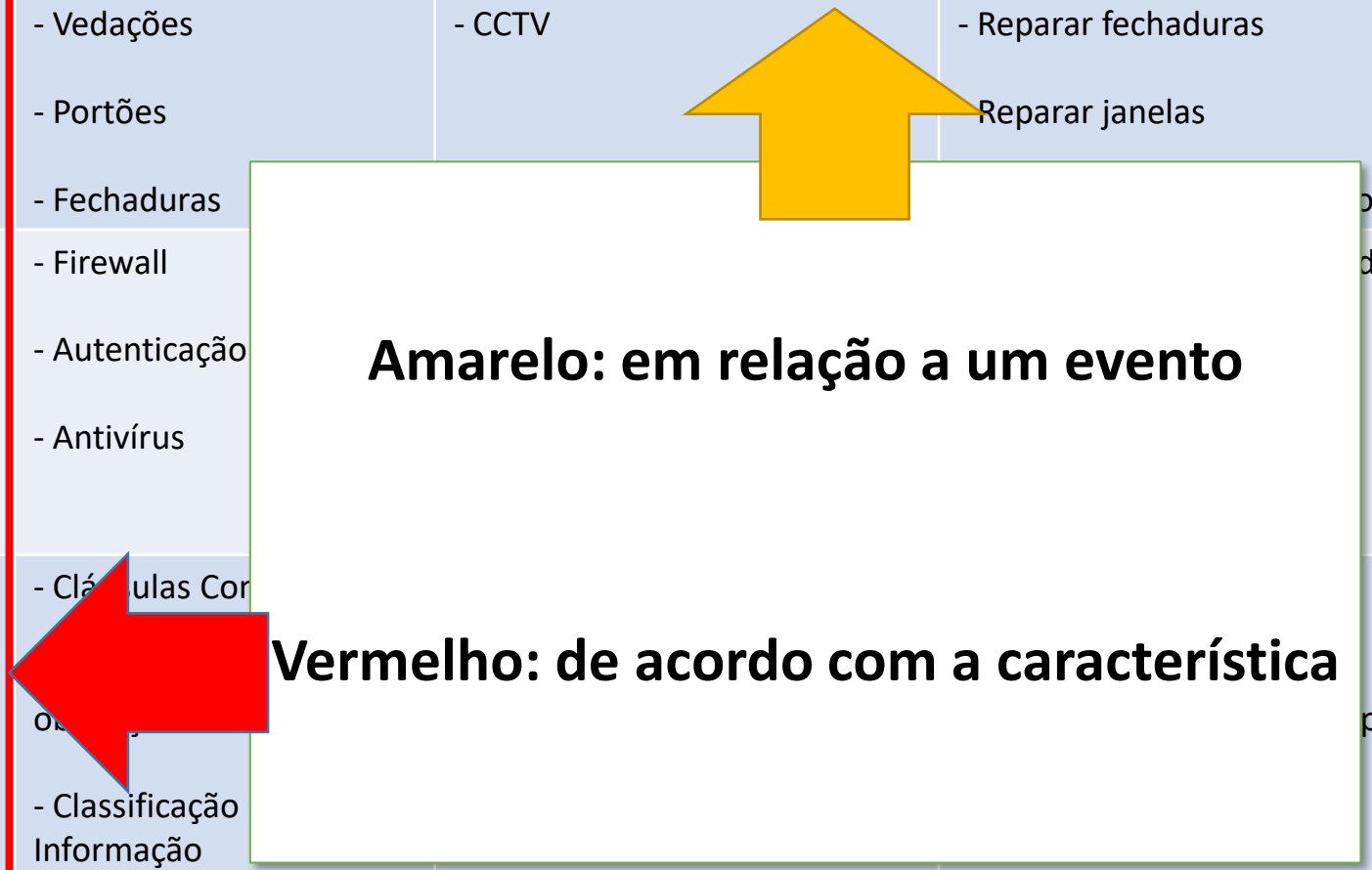
- **Controlos incluem políticas e mecanismos, mas também:**
  - Normas e Leis
  - Processos
  - Políticas
  - Mecanismos
  - Técnicas, etc…
- **Controlos são definidos de forma explícita e são verificáveis**
  - Exemplo: ISO 27001 define 114 controlos em 14 grupos
    - … Gestão de equipamentos, segurança física, gestão de incidentes…

Tipos de Controlos

	Prevenção	Deteção	Correção
Físicos	- Vedações - Portões - Fechaduras	- CCTV	- Reparar fechaduras - Reparar janelas - Reemitir cartões de acesso
Técnicos	- Firewall - Autenticação - Antivírus	- Deteção de intrusões - Alarmes - Honeypots	- Correção de vulnerabilidades - Reiniciar sistemas - Repor VMs - Remover Vírus
Administrativos	- Cláusulas Contratuais - Separação de obrigações - Classificação de Informação	- Revisão de matrizes de acesso - Auditorias	- Implementar planos de continuidade de negócio - Implementar plano de resposta a incidentes

Tipos de Controlos

	Prevenção	Deteção	Correção
Físicos	- Vedações - Portões - Fechaduras	- CCTV	- Reparar fechaduras Reparar janelas
Técnicos	- Firewall - Autenticação - Antivírus		
Administrativos	- Cl ulas Cor - Classificação Informação		



Aplicação da Segurança

Prevenção realista

- **Considerar que não existe segurança perfeita**
- **Focar nos eventos mais prováveis**
  - Poderá depender da localização física, enquadramento legal,…
- **Considerar custo e receitas**
  - Um grande número de controlos tem um custo baixo
  - Custo de uma estratégia de segurança não tem limite prático
- **Considerar todos os domínios e entidades**
  - Um ataque numa entidade pode comprometer outras lateralmente

Aplicação da Segurança

Prevenção realista

- **Considerar impacto**
  - À luz da CIA, ou outros aspetos relevantes (e.g Marca)
- **Considerar custo e tempo de recuperação**
  - Custo monetário, reputação, posição de mercado
- **Caracterizar os atacantes**
  - E criar controlos para esses atacantes
  - Existem sempre atacantes com mais conhecimento/recursos
- **Considerar que o sistema vai ser comprometido**
  - Ter planos de recuperação

Segurança nos Sistemas Computacionais: Problema Complexo

- **Computadores podem fazer muitos estragos num curto espaço de tempo**
  - Podem processar grandes quantidades de informação
  - Processam informação a grande velocidade

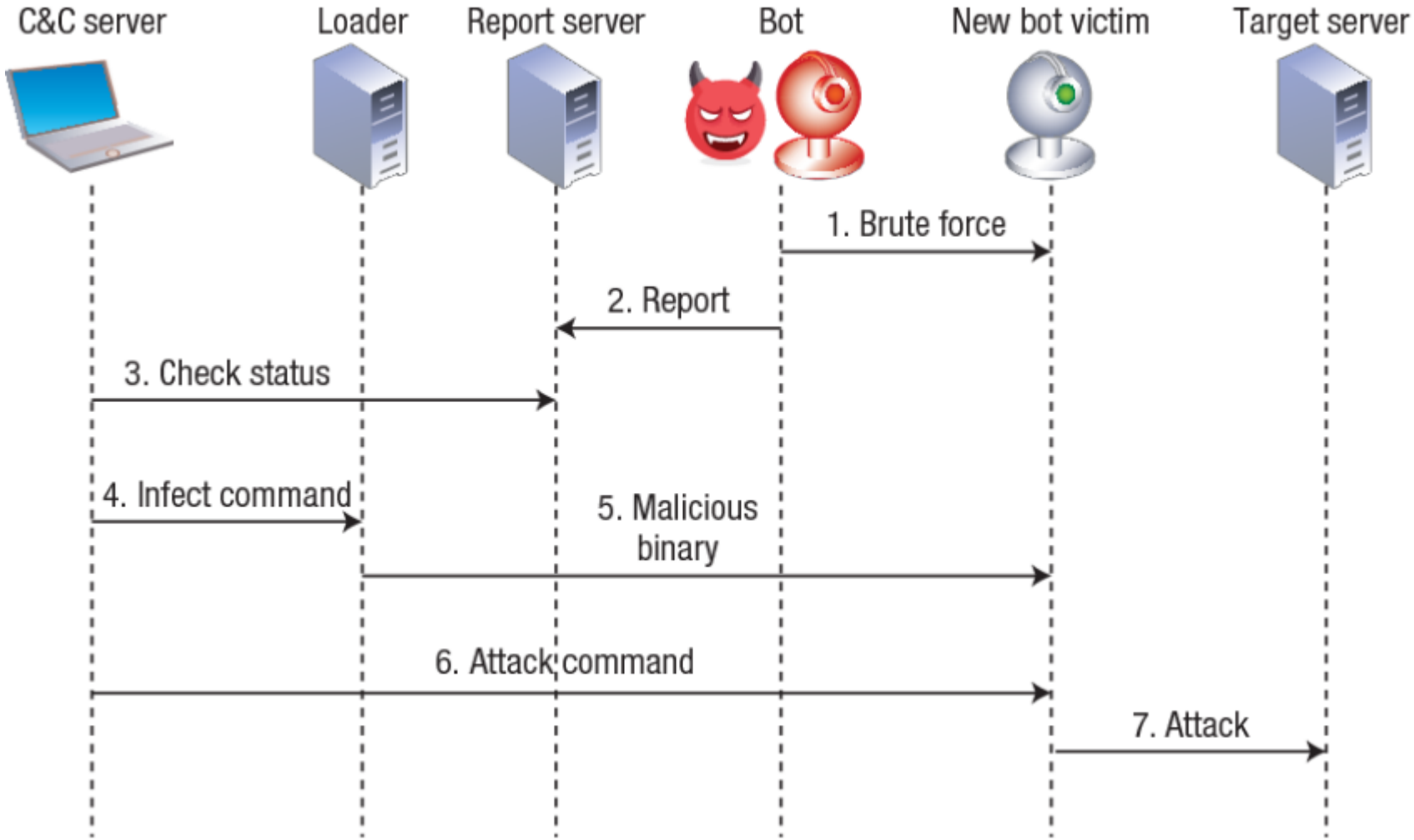
- **O número de vulnerabilidades aumenta sempre**
  - Complexidade incremental dos sistemas
  - Pressões de mercado (time to market, ou custo)

Segurança nos Sistemas Computacionais: Problema Complexo

- **Redes permitem novos mecanismos de ataque**
  - Ataques anónimos de qualquer ponto do planeta
  - Ataques distribuídos sobre várias geografias
  - Exploração de aplicações e sistemas inseguros

- **Atacantes podem construir cadeias de ataque complexas**
  - Primeira exploração
  - Movimento lateral
  - Exfiltração de informação
  - Etc…https://attack.mitre.org/matrices/enterprise/

Encadeamento de atividades



Operação e comunicação da botnet Mirai botnet.
Mirai causa uma negação de serviço distribuída (DDoS) a servidores, propagando-se constantemente para dispositivos IoT mal configurados

Fonte: Kolias, Constantinos et al. “DDoS in the IoT: Mirai and Other Botnets.” Computer 50, 2017: 80-84

Segurança nos Sistemas Computacionais: Problema Complexo

- **Usuários não possuem noção do risco**
  - Não conhecem o problema
    - ... o impacto
    - ... as boas práticas
    - … ou as soluções

- **Usuários são desleixados**
  - Tomam riscos
  - Não querem saber (não possuem/identificam responsabilidade)
  - Não estimam o risco de forma adequada

Principais fontes de Vulnerabilidades

- **Aplicações hostis ou erros em aplicações**
  - Root kits: Inserem elementos no Sistema Operativo
  - Worms: Programas controlados por um atacante
  - Vírus: Código executável p/ infetar ficheiros (ex, Macros)

- **Usuários**
  - Ignorantes e descuidados
    - ... telnet vs ssh, FTP vs FTPS, IMAP vs IMAPS, HTTP vs HTTPS
  - Falsa noção de segurança (ex: tenho um anti-vírus, estou protegido)
  - Hostis

- **Administração deficiente**
  - A configuração por omissão raramente é a mais segura
  - Restrições de Segurança vs Operações Flexíveis
  - Exceções a indivíduos

- **Comunicações sobre ligações não controladas/conhecidas**

Políticas de Segurança em Sistemas Distribuídos

Tem de englobar múltiplos sistemas e redes

- **Domínios de segurança**
  - Definição de um conjunto de sistemas e rede
  - Definição de um conjunto de usuários aceites/autorizados
  - Definição de um conjunto de atividades aceites/não aceites
- **Gateways de segurança**
  - Definição das interações de entrada e saída de um domínio
- **Conjunto de controlos para validação**

Defesa em Perímetro

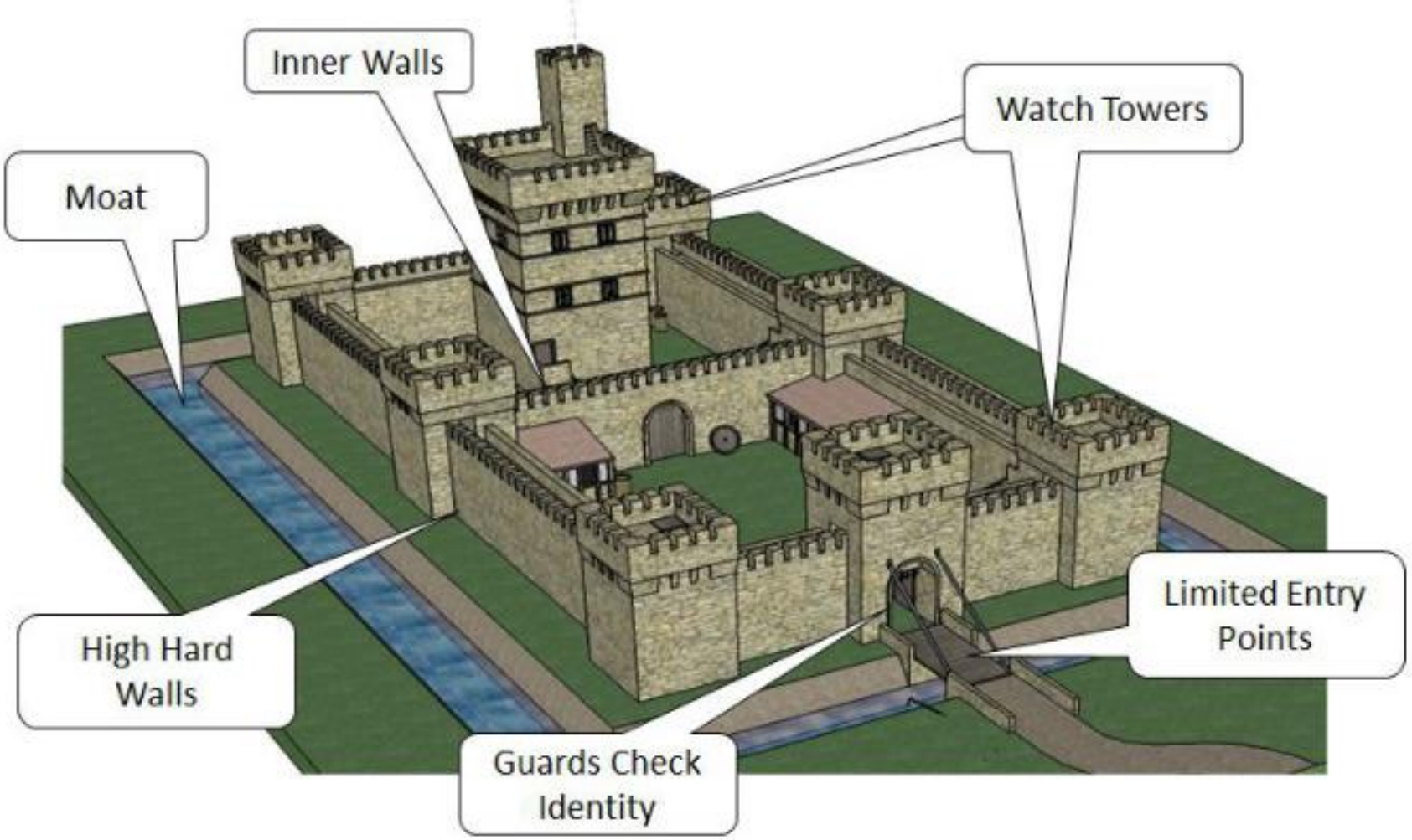
(mínimo aconselhado, **mas insuficiente**)

Defesa em Perímetro

- **Proteção contra atacantes externos**
  - Internet
  - Outros utilizadores
  - Outra organização
- **Assume que utilizadores internos são confiáveis e partilham políticas**
  - Amigos, família, colaboradores
- **Utilização doméstica ou em pequenas organizações**
- **Limitações**
  - Não protege contra atacantes internos
    - Utilizadores de confiança
    - Atacantes que adquiram acesso interno

Defesa em profundidade

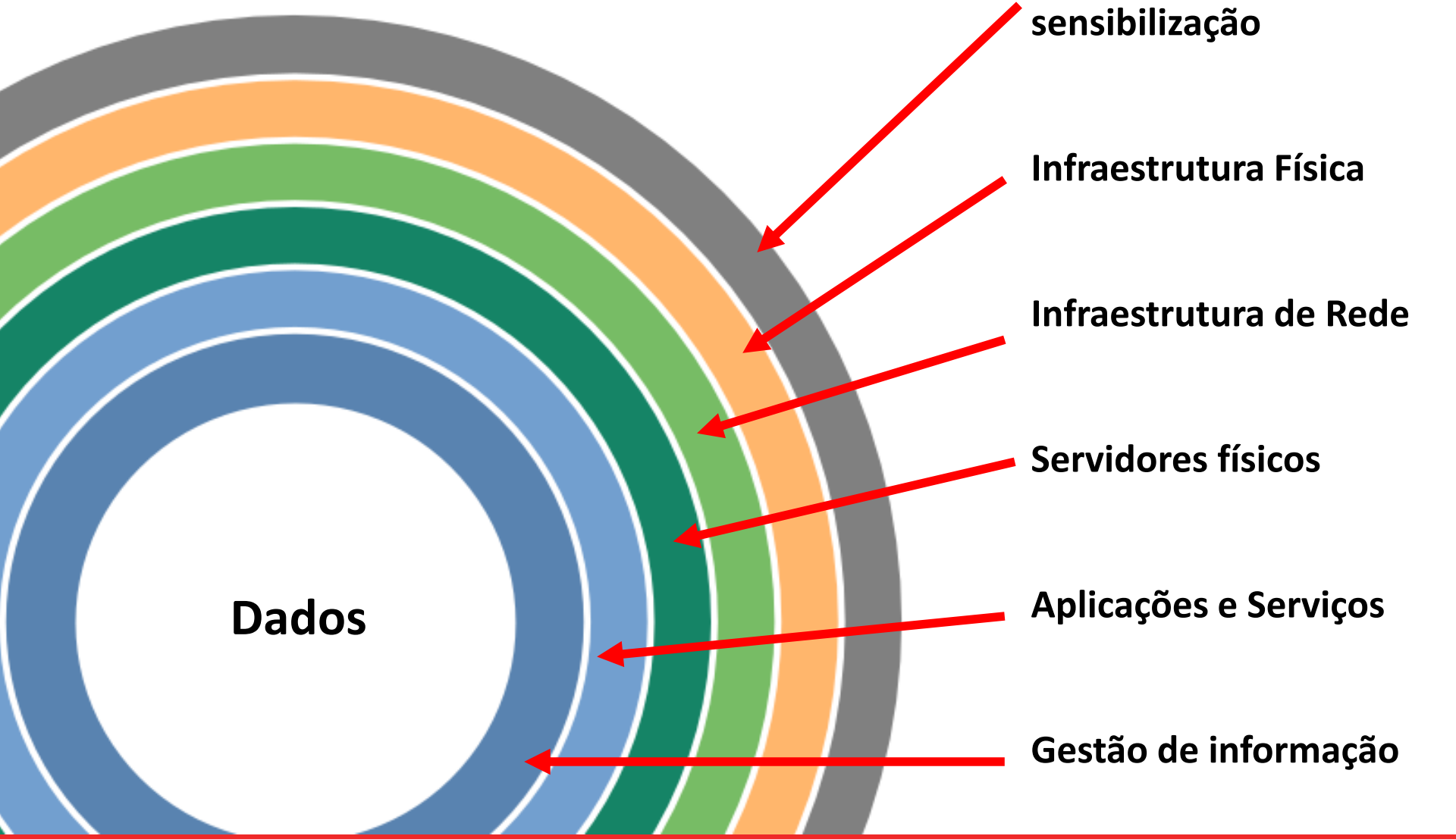
(mais adequado, mas também falível)



Defesa em Profundidade

- **Proteção contra atacantes externos e internos**
  - Internet
  - Qualquer utilizador
  - Outra organização
- **Assume domínios bem definidos sobre todos os aspetos**
  - Paredes, Portas blindadas, autenticação, vigilantes, cifras, redes seguras…
- **Limitações**
  - Necessária uma coordenação entre controlos
    - Possível acumulação de controlos, com sobreposição de funções mas também buracos na defesa
  - Custo
  - Necessidade de Treino, alteração de processos e auditorias frequentes

Defesa em profundidade



Defesa em profundidade

- **Sistemas Operativos Confiáveis**
  - Níveis de segurança, certificação
  - Ambientes de execução segura
  - Sandboxes / Máquinas Virtuais
- **Firewalls e Sistemas de segurança**
  - Controlo de tráfego entre redes
  - Monitorização (carga de tráfego, comportamento…)
- **Comunicações Seguras / VPNs**
  - Canais seguros sobre redes públicas / inseguras
  - Extensão segura das redes da organização

Defesa em profundidade

- **Autenticação**
  - Local
  - Remota (sobre a rede)
  - Single Sign-On
  - Segredos, Tokens, biometria, dispositivos, localização
- **Entidades de Certificação /PKI**
  - Gestão de chaves públicas e certificados
- **Cifra de ficheiros e dados em sessões**
  - Privacidade/confidencialidade de dados transmitidos
  - Privacidade/confidencialidade de dados armazenados

Defesa em profundidade

- **Deteção de intrusões**
  - Deteção de atividades proibidas ou anómalas
  - Baseado na rede / baseado nos sistemas
- **Inventariação de vulnerabilidades**
  - Pesquisa para resolução de problemas ou exploração
  - Baseado na rede / baseado no sistemas
- **Testes de Penetração**
  - Avaliação das vulnerabilidades
  - Demonstração de tentativas de penetração
  - Teste de mecanismos de segurança instalados
  - Determinação da existência de políticas de segurança mal aplicadas

Defesa em profundidade

- **Monitorização de conteúdos**
  - Deteção de vírus, Worms e outras ciber-pragas
- **Administração da segurança**
  - Desenvolvimento de políticas de segurança
  - Aplicação das políticas de forma distribuída
  - Co-administração / contratação de equipas externas
- **Resposta a Incidentes / Seguimento em Tempo Real**
  - Capacidade para detetar e reagir a incidentes em tempo real
  - Meios para resposta rápida e efetiva a incidentes

Zero Trust

- **Modelo de defesa sem perímetros específicos**
  - Não existe confiança intrínsica por entidades serem internas
    - Aliás, pode não existir definição de interno ou externo

- **Modelo recomendado para novos sistemas**
  - Sistemas tradicionais deverão migrar para este modelo
  - Implica o desenho de sistemas/serviços para este modelo
  - Sistemas legados requerem a instalação de níveis adicionais de proteção
    - Firewalls, filtros, adaptadores, plugins,…

Zero Trust – Princípios (NCSC)

1. **Conhecer a arquitetura**
   - serviços, dispositivos, pessoas

1. **Conhecer as identidades**
   - pessoas, serviços e saúde dos dispositivos

2. **Validar comportamentos e saúde de dispositivos e serviços**

3. **Usar políticas para autorizar pedidos**

Zero Trust – Princípios (NCSC)

5. **Autenticar e autorizar todas as interações**
   - Nada de APIs abertas, ou restritas por endereço IP

6. **Monitorizar utilizadores, dispositivos e serviços**

7. **Não confiar em nenhuma rede, nem mesmo a própria**
   - Atacantes internos deverão ter o mesmo acesso que os externos

8. **Usar serviços desenvolvidos para Zero Trust**
   5. Serviços legados

Atualidade – Utilizadores comuns

- **Usam os mesmos dispositivos para todas as suas interações**
  - Contactar outros
  - Aceder a serviços de lazer
  - Aceder a serviços críticos (ex., Bancos)
  - Trabalho (?)

- **Utilização de sistemas e serviços com base no objetivo final**
  - Comprar, aceder, ver, ouvir, comunicar

- **Sem formação e incautos**
  - Maus a calcular risco das suas ações
  - Consideram que os problemas só acontecem a grandes empresas/outros
    - Consideram que não são importantes
  - Com ideias pré-concebidas erradas
    - "algoritmos" para gerar senhas, reutilização de senhas
  - Sem investimento em segurança (exceto o eventual antivírus)
    - Consideram que o antivírus fornece proteção total
  - Sem processos de recuperação de incidentes

Atualidade - Empresas

- **Focadas no objeto do negócio**
  - Produto que fornecem
  - Aspetos financeiros
  - Recursos Humanos

- **Seguras na medida do estritamente necessário**
  - Devem cumprir regras e ambientes normativos
    - RGPD, regulação específica dos setores
  - Podem ter estratégias de segurança
    - Desde nada até serem focadas em "security driven culture"
  - Podem fornecer treino e investir em segurança
  - Podem ter auditorias frequentes
  - Podem ter um CISO: Chief Information Security Oficer

Category	Basic Organizations	Progressing Organizations	Advanced Organizations
Philosophy	Cybersecurity is a "necessary evil."	Cybersecurity must be more integrated into the business	Cybersecurity is part of the culture.
People	CISO reports to IT. Small security team with minimal skills. High burnout rate and turnover.	CISO reports to COO or other non-IT manager. Larger security team with some autonomy from IT. Remain overworked, understaffed, and under-skilled.	CISO reports to CEO and is active with the board. CISO considered a business executive. Large, well-organized staff with good work environment. Skills and staff problems persist due to the global cybersecurity skills shortage.
Process	Informal and ad-hoc. Subservient to IT.	Better coordination with IT but processes remain informal, manual, and dependent upon individual contributors.	Documented and formal with an eye toward more scale and automation.
Technology	Elementary security technologies with simple configurations. De-centralized security organization with limited coordination across functions. Focus on prevention and regulatory compliance.	More advanced use of security technologies and adoption of new tools for incident detection and security analytics.	Building an enterprise security technology architecture. Focus on incident prevention, detection, and response. Adding elements of identity management and data security to deal with cloud and mobile computing security.

Source: Enterprise Strategy Group, 2014.

Atualidade - Nações

- **Focadas na soberania política, económica, cultural**
  - Agindo de forma independente ou concertada (ex., NATO)
- **Possuem entidades dedicadas à cibersegurança**
  - Ciber defesa
    - Parte integrante das forças armadas
    - Entidades ad-hoc contratadas ou não declaradas
  - Ciber resiliência das entidades da nação
    - Universidades, utilities, empresas, cidadãos
    - Entidades específicas: Centro Nacional de Cibersegurança
  - Investigação criminal
    - Polícias
- **Podem realizar ações ofensivas contra outras entidades**
  - Empresas, indivíduos, grupos, nações
  - Guerra fria, governos totalitários, soberania

Atualidade – Grupos ofensivos

- **Realizam ataques contra qualquer um**
  - De forma esporádica ou concertada
  - Podem possuir grandes fundos disponíveis
    - Financiamento por grupos económicos ou nações
  - Podem agir como um coletivo sem organização estrita

- **Por vezes considerados Advanced Persistent Threats (APT)**
  - Realizam ataques ao longo de meses/anos
  - Podem manter-se numa entidade de forma silenciosa

- **Variadas motivações**
  - Hacktivismo: Lulzsec, Anonymous, AntiSec, (4chan?)
  - Concorrência económica
  - Interesses nacionais: Advanced Persistent Threats (APTs)
  - Crime: APTs, grupos variados de ransomware
  - Ciberguerra

Atualidade – Grupos Criminosos

- **Frequentemente operam como empresas**
  - Modelo de negócio explícito
  - Empregados e outros colaboradores
  - "Linha de suporte" (para ajudar vítimas a pagar resgates)
  - Por vezes com presença publica e publicidade

- **Operam segundo vários modelos**
  - Podem operar de países que os "ignoram"
    - E não atacam sistemas nesses países
  - Operações por contrato (outras empresas, nações, …)
  - Dirigidos a uma base de utilizadores larga ou outras companhias
  - Foco em áreas de negócio específicas (infraestruturas críticas, saúde, banca…)

- **Ambiente de software rico e dinâmico**
  - Software especificamente desenvolvido para estas atividades
    - Explorando vulnerabilidades em sistemas
    - Vulnerabilidades são comercializadas e são ferramentas para incluir nos ataques a sistemas
  - Podem fazer uso de ferramentas automáticas ou software dirigido

Fatores Limitantes

- **Cibersegurança é limitada por aspetos económicos, operacionais e logísticos**
  - Todas as entidades possuem recursos limitados
- **Cibersegurança resume-se a construir e aplicar uma estratégia, com um orçamento e num contexto operacional e legal**

http://targetedattacks.trendmicro.com/cyoa/en/