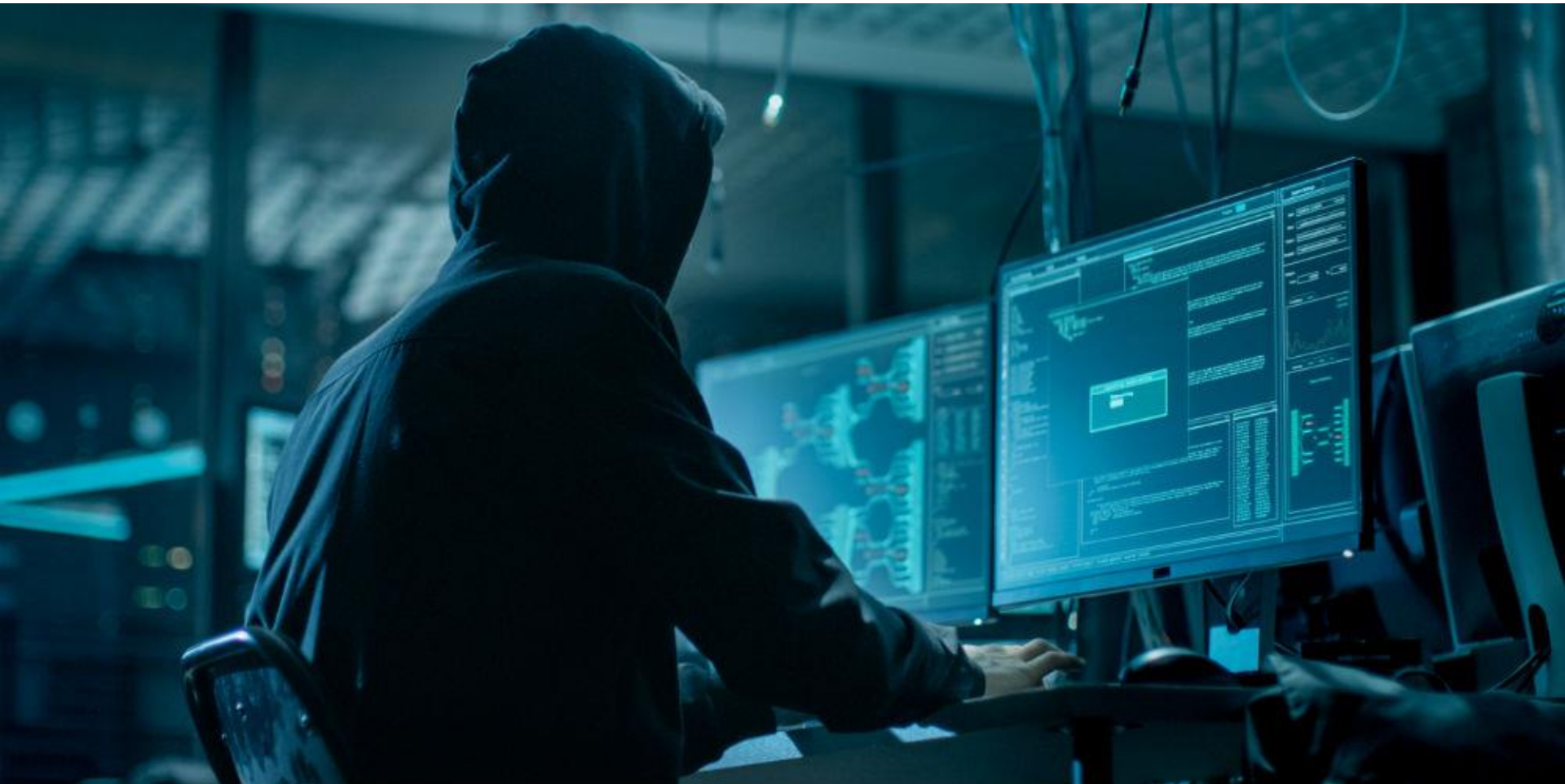




Introdução à segurança

Segurança



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 a existência de erros (bugs) que comprometam a execução correta**
 - Sem crashes
 - Sem resultados/respostas inválidos ou inesperados
 - Com tempos de execução correto
 - Com um consumo de recursos adequado
 - Com o devido controlo de acesso a recursos
 - 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, ...

Segurança: pessoas, parceiros

Comportamento dos sujeitos não possui um impacto negativo na solução

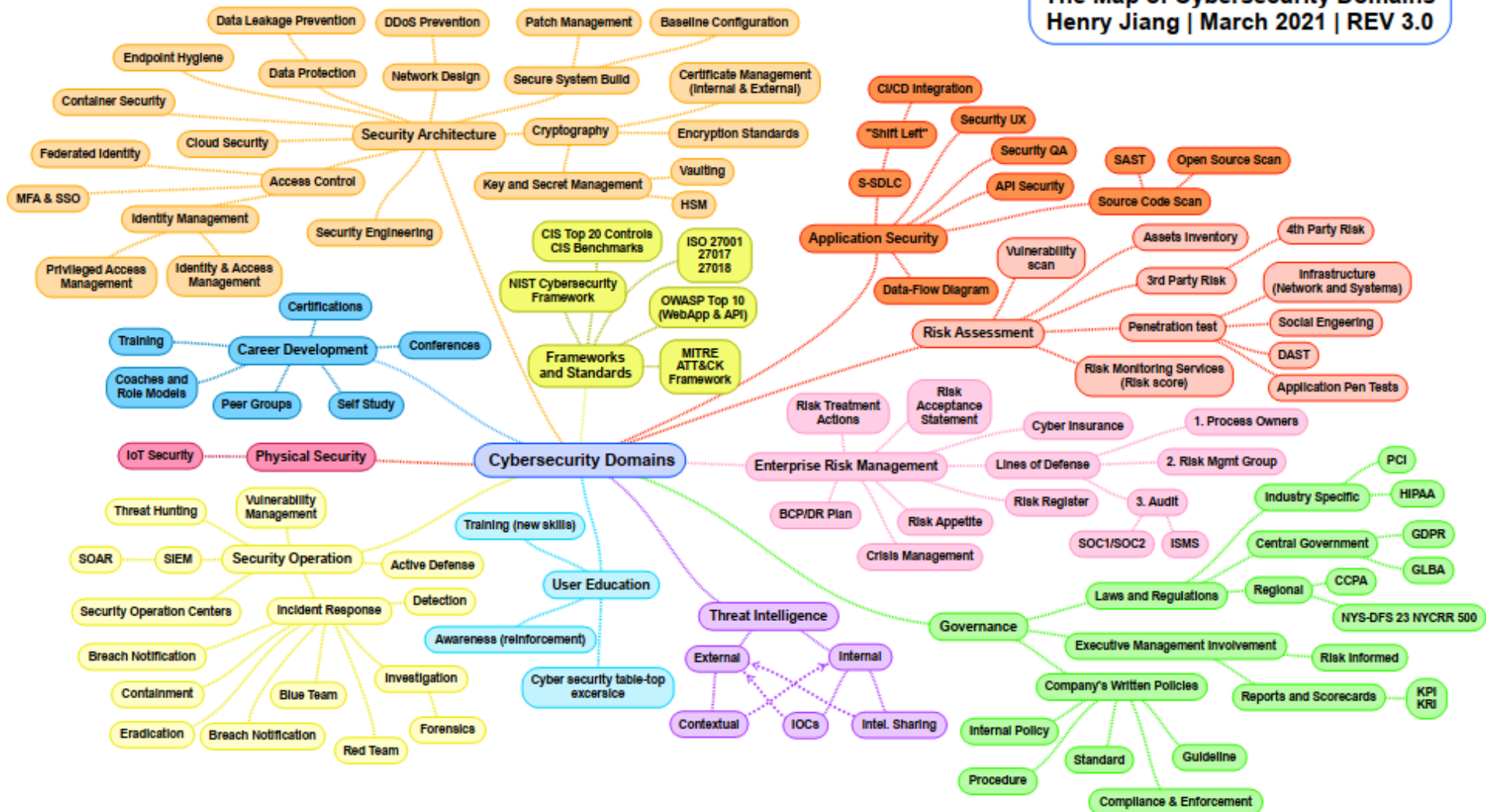
- **Existem normas que definem qual o comportamento correto**
- **Possuem formação para distinguir quais os comportamentos corretos e incorretos**
- **Possuem os incentivos para manter comportamentos**
- **Quando comprometidos ou desviantes, as ações têm um impacto limitado**

Segurança: análise e auditoria

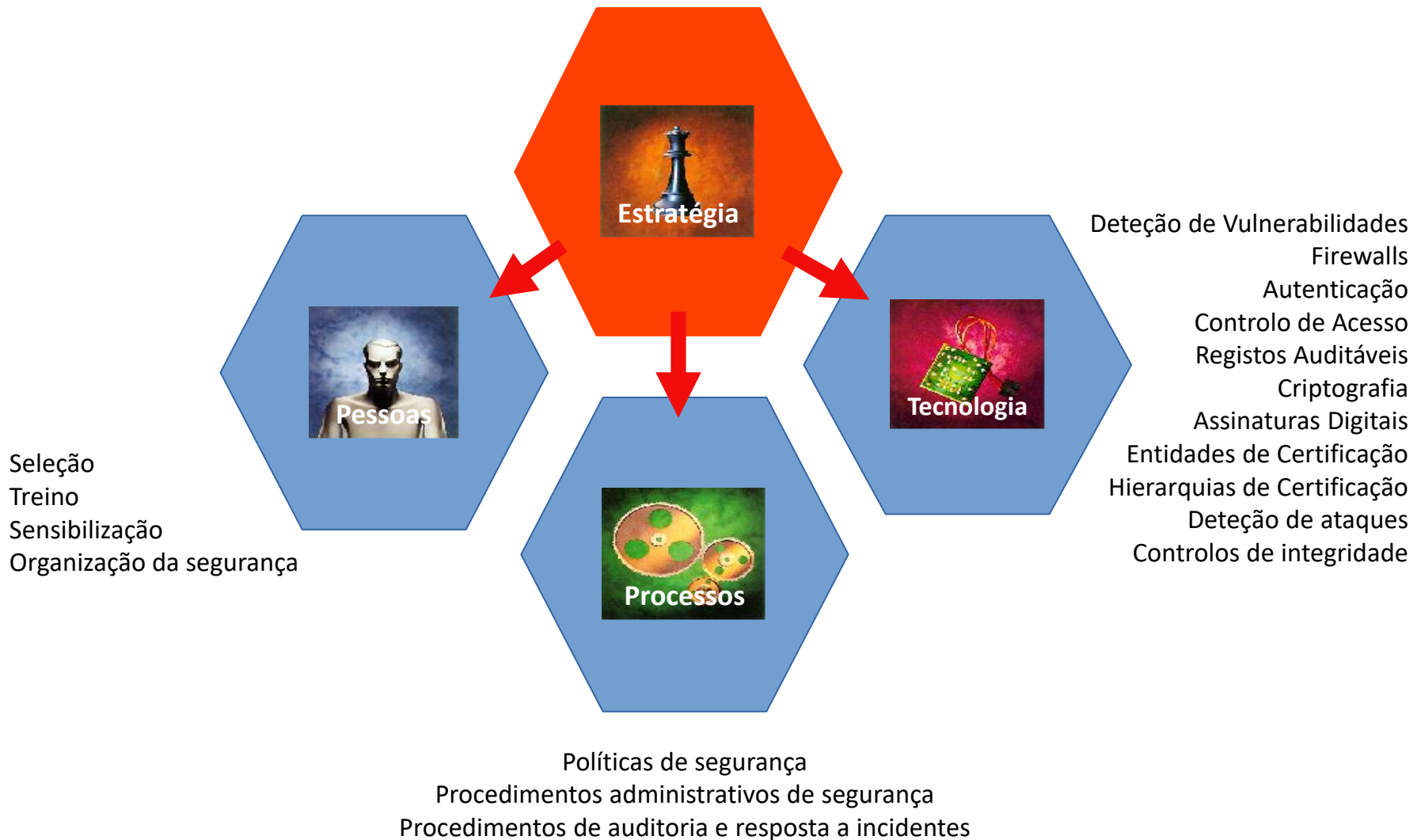
Qual é o comportamento atual da solução?

- **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



Dimensões a considerar



Facetas

- **Facetas da segurança são interligadas e indissociáveis**
- **Defensiva: foca-se na manutenção da previsibilidade**
- **Ofensiva: foca-se na violação da previsibilidade**
 - Com intuito malicioso/criminoso
 - Com 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

Objetos da Segurança da Informação

CIA: Confidentiality, Integrity, Availability

- **Confidencialidade**: Informação só pode ser acedida por um grupo restrito de sujeitos
- **Integridade**: Informação mantém-se inalterada
 - Pode ser aplicada a comportamentos de dispositivos e serviços
- **Disponibilidade**: Informação mantém-se disponível
 - Pode ser aplicada a serviços e dispositivos

Objetos da Segurança - Outros

- **Privacidade**

- Recolha não autorizada de informação pessoal
- Armazenamento (ou distribuição) desta informação
- Relacionado com pessoas

- **Impersonificação**

- Exploração não autorizada de perfis de identidade
- Relacionado com pessoas, serviços, entidades



Conceitos Fundamentais

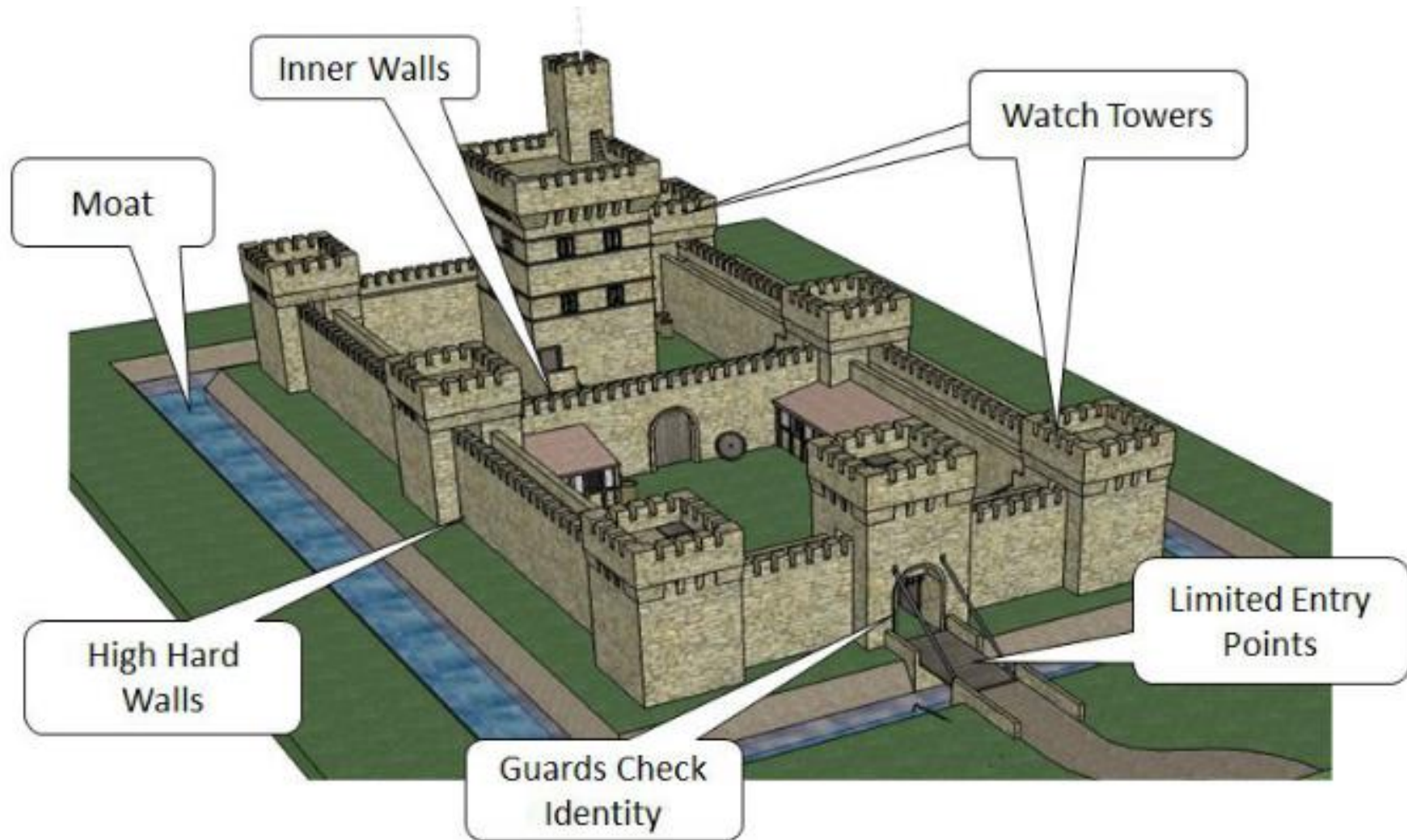
- **Domínios**
- **Políticas**
- **Mecanismos**
- **Controlos**

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, 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 são de betão
 - Comunicações são cifradas

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)

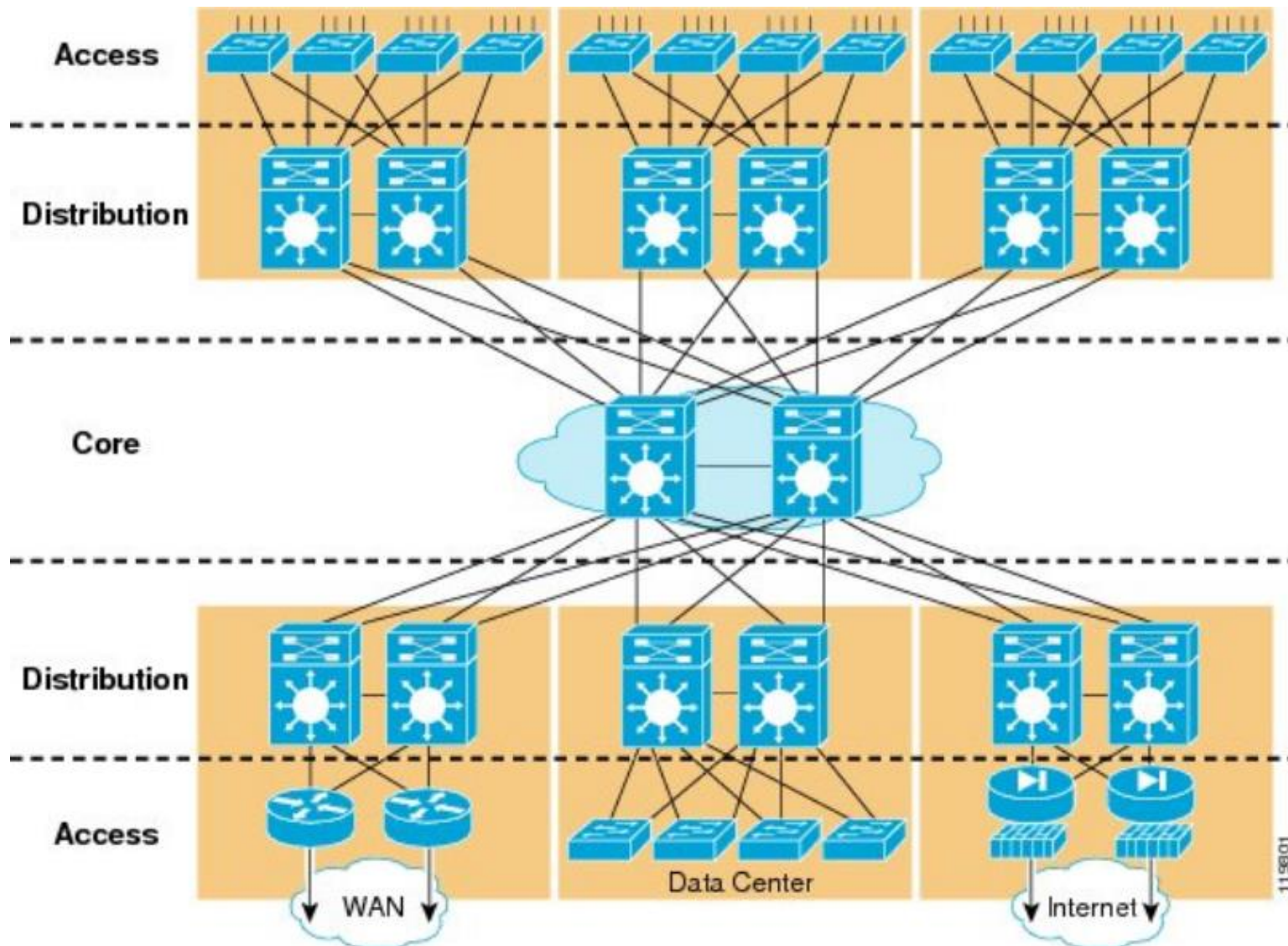
Políticas de Segurança

- **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 de lista de negações
 - Proíbem-se algumas coisas
 - O resto é permitido
 - Modelo de 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

Redundância de Sistemas



Redundância de Subsistemas



Fonte: DELL

Controlos de Segurança

**Controlos são todos e quaisquer aspetos que permitam
minimizar risco
(proteger as propriedades CIA)**

- **Controlos incluem políticas e mecanismos, mas também:**
 - Normas
 - Processos
 - Leis
 - Regulamentos
- **Controlos são definidos de forma explícita e são auditáveis**
 - Agem como pontos de controlo da solução

Tipos de Controlos

	Prevenção	Deteção	Correção
Físicos	<ul style="list-style-type: none">- Vedações- Portões- Fechaduras	<ul style="list-style-type: none">- CCTV	<ul style="list-style-type: none">- Reparar fechaduras- Reparar janelas- Reemitir cartões de acesso
Técnicos	<ul style="list-style-type: none">- Firewall- Autenticação- Antivírus	<ul style="list-style-type: none">- Deteção de intrusões- Alarmes- Honeypots	<ul style="list-style-type: none">- Correção de vulnerabilidades- Reiniciar sistemas- Repor VMs- Remover Vírus
Administrativos	<ul style="list-style-type: none">- Cláusulas Contratuais- Separação de obrigações- Classificação de Informação	<ul style="list-style-type: none">- Revisão de matrizes de acesso- Auditorias	<ul style="list-style-type: none">- Implementar planos de continuidade de negócio- Implementar plano de resposta a incidentes

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

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



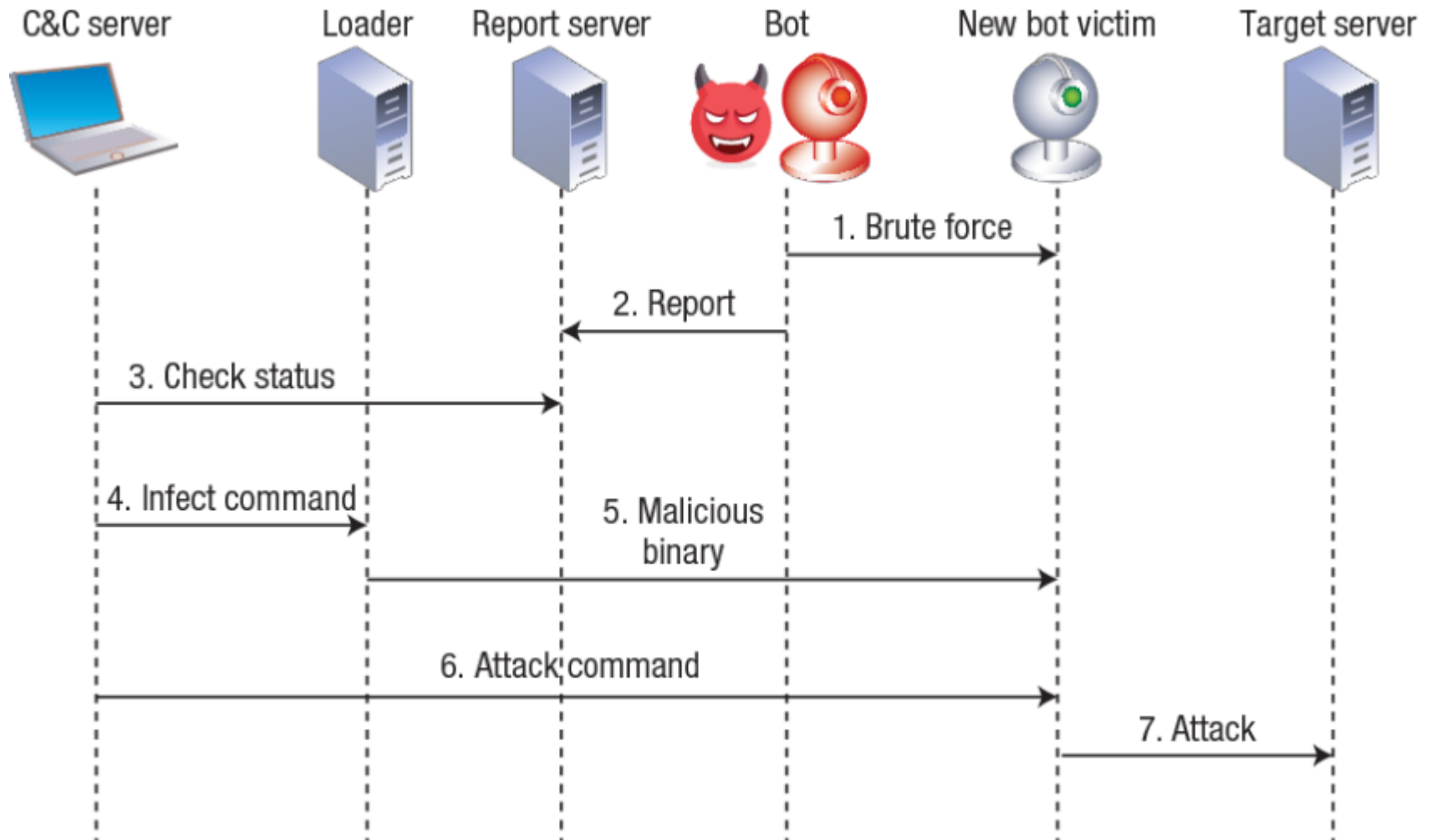
Segurança nos Sistemas Computacionais: Problema Complexo

- **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**

Níveis de Segurança

- **Definido por**
 - Políticas de segurança existentes
 - Correção e efetividade da sua especificação/ implementação
- **Critério de Avaliação (NCSC TCSEC, Orange Book)**
 - Classes: D, C (1, 2), B (1, 2, 3) e A (1)
 - D: Inseguro
 - A1: mais seguro
 - Políticas de proteção existentes e dispendiosas
 - Procedimentos formais de validação da especificação
 - Controlo rigoroso da implementação
- **Critério de Avaliação ITSEC**
 - Níveis E1 até E6
 - Nível de especificação formal e correção da implementação

NCSC TCSEC Nível C

- **C1 – Discretionary Security Protection**

- Identificação e Autenticação
- Separação de utilizadores e dados
- Controlo de acesso discricionário (DAC), capaz de aplicar limites de acesso por utilizador
- Necessário existir documentação do sistema e manuais

- **C2 – Controlled Access Protection**


- DAC com mais detalhe
- Rastreio individual das ações através de mecanismos de login
- Registos para auditorias
- Limpeza de objetos ao serem re-usados (Object Reuse)
- Isolamento de recursos

NCSC TCSEC Nível C

- **Política de Object Reuse**

- All authorizations to the information contained within a storage object shall be revoked prior to initial assignment, allocation or reallocation to a subject from the TCB's pool of unused storage objects.
- No information, including encrypted representations of information, produced by a prior subject's actions is to be available to any subject that obtains access to an object that has been released back to the system."

- **Storage object:** An object that supports both read and write accesses.



Políticas de Segurança em Sistemas Distribuídos (SD)

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)

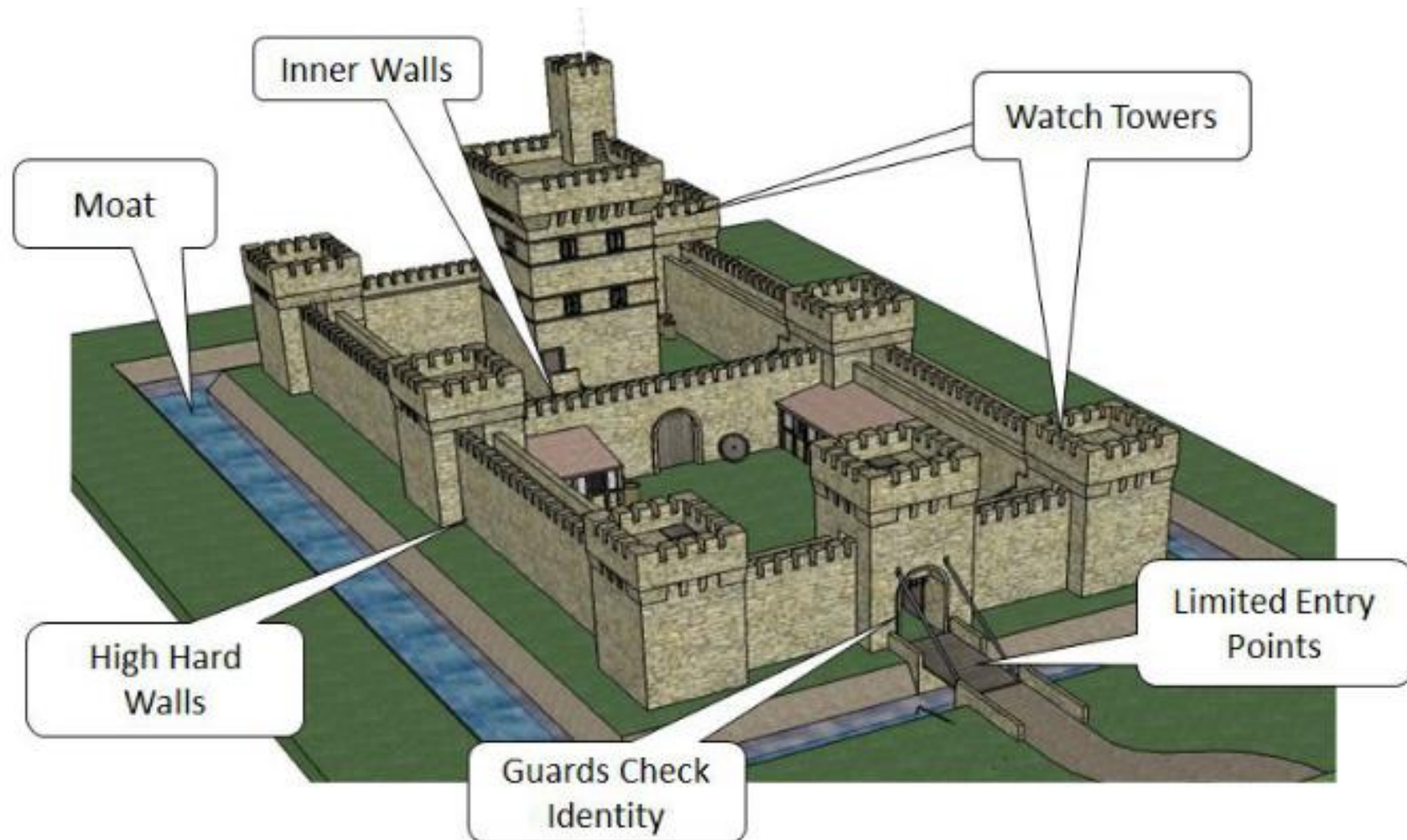


Defesa em Perímetro

- **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

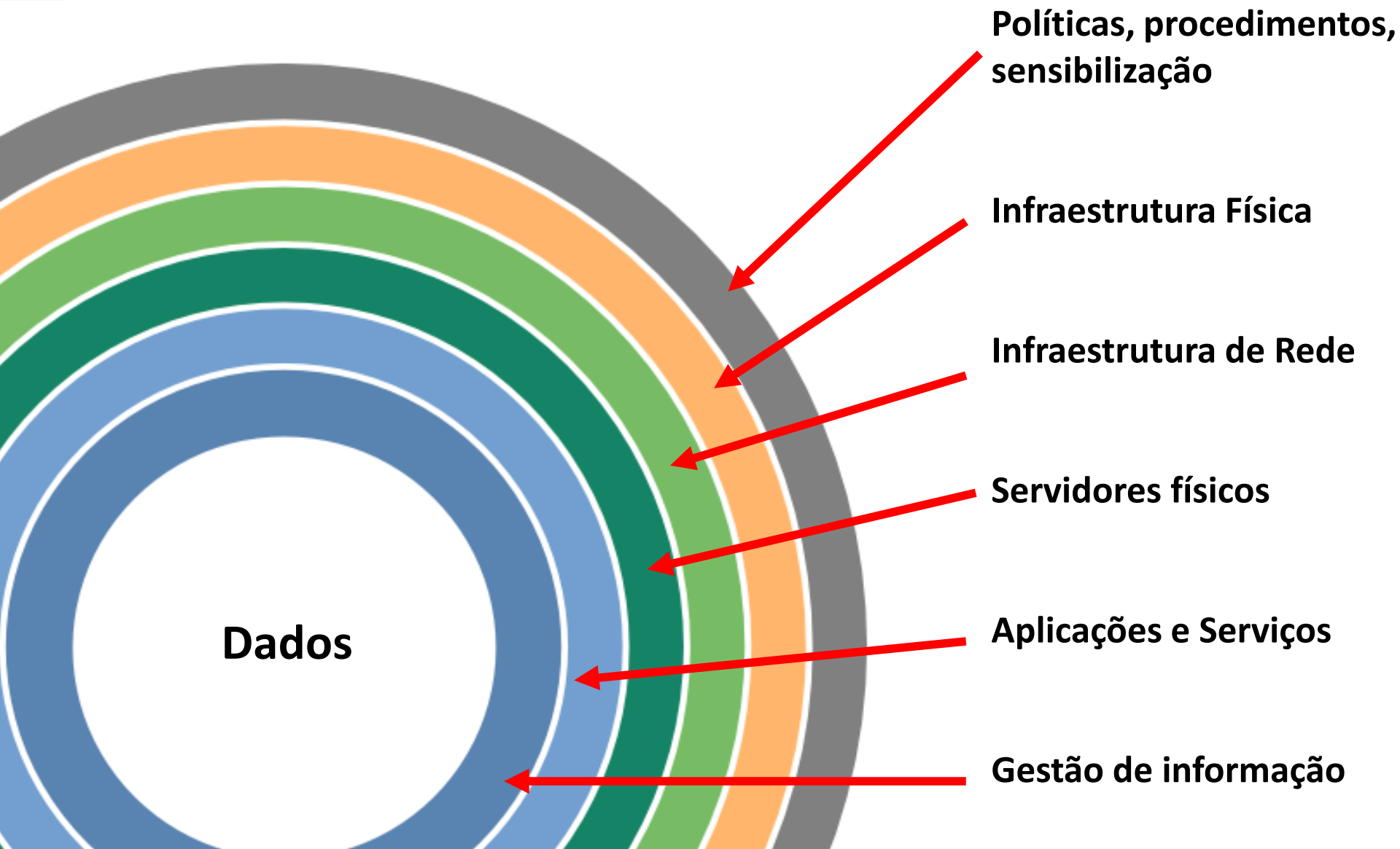
(o mais adequado, mas também falível)



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...
- **Utilização em qualquer organização**
- **Limitações**
 - Necessária uma coordenação entre controlos
 - Possível acumulação de controlos, com sobreposição de funções mas também buracos na defesa
 - Custo
 - Necessidade de Treino e Auditorias

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**
 - Detecção 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

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
- **Interagem com segurança na medida do estritamente necessário**
 - Cumprimento de 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 Officer

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. Decentralized 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 (e.x, 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
 - Investigação criminal
- **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**
 - 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