Segurança e Gestão de Risco

2ºSem 2023/24

Tratamento dos Riscos

Controlos de Segurança

LUIS AMORIM

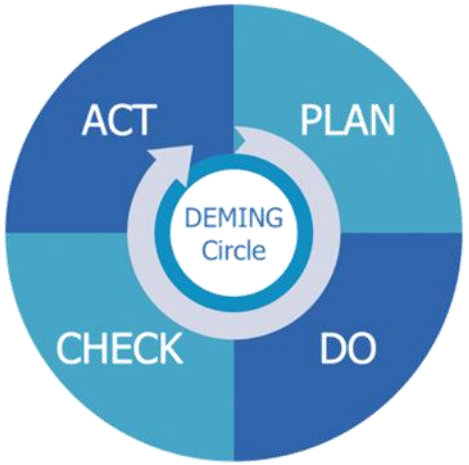
16 Mar 2024

Síntese da Aula Anterior

- Introdução à Segurança da Informação - ISO 27001
- Introdução à Gestão de Continuidade de Negócio
- A avaliação e gestão de riscos

Síntese da Aula Anterior

- Introdução à ISO 27001
  - Requisitos de um Sistema de Gestão
    - Requer Gestão de Risco
  - Controlos de Segurança
    - Para mitigação dos riscos



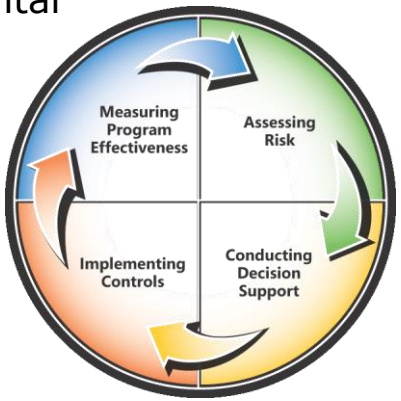
Síntese

- Introdução à Gestão de Continuidade de Negócio
  - Um processo de Business Continuity Management (BCM), deve fazer parte da Gestão de Risco de uma organização.
  - O processo de Gestão Continuidade de Negócio conduz à produção de planos e procedimentos que permitem responder a incidentes
  - O standard a seguir nesta área é a ISO 22301

Síntese

- A análise e gestão de riscos
  - Gestão de Risco como processo (não projeto) mais abrangente
  - A aplicação da Avaliação e Análise de Risco:
    - Sobre os processos e sistemas implementados
    - Sobre novos processos e sistemas (projet Impact Analysis)
  - Etapas da Avaliação de Riscos (NIST)
  - Formas de quantificar o Risco
    - Avaliação quantitativa, recorrendo a valores monetários
      - No seu cálculo inclui pode incluir o impacto no negócio
      que pode ser considerado na análise custo-benefício dos controlos a implementar
      - Mas pode tornar pouco clara a análise quantitativa
    - Avaliação qualitativa, através de níveis de valores
      - Utilizando categorias e níveis de risco
      - Permite observar facilmente a prioritização dos Riscos
      - Mostrando as áreas de melhoria imediata

	Matriz de Probabilidade x Impacto				
Probabilidade					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
Impacto	1	2	3	4	5



AGENDA

- **Tratamento dos Riscos**

- Controlos de segurança
  - Tecnológicos, Operacionais e de Gestão

- Modelo de segurança integrado
  - Controlos de segurança alinhados com as melhores práticas

Tratamento dos Riscos

- Opções de Tratamento de Risco (ISO27005/Segurança da Informação)
  - Assumir o Risco
    - Aceitar o Risco continuando com o sistema em operação
    - Podendo/devendo ir implementando controlos tendentes à redução do risco
  - Evitar o Risco
    - Eliminando a causa do risco ou as consequências (desactivar certas funcionalidades ou,mesmo, desligar o sistema)
  - Transferência de Risco
    - Utilizando opções que permitam cpmpensação em caso de perdas (p.e. seguros)
  - Aplicação de Controlos ou Mitigação dos Riscos
    - Controlos de segurança apropriados às ameaças e vulnerabilidades encontradas no sentido de reduzir o risco final

Tratamento dos Riscos

- Opções de Tratamento de Risco (ISO 31000)
  - "As opções para o tratamento do risco poderão envolver uma ou mais das seguintes opções:
    - evitar o risco ao decidir não iniciar ou continuar com a atividade que origina o risco;
    - aceitar ou aumentar o risco de modo a explorar uma oportunidade;
    - remover a fonte do risco;
    - alterar a verosimilhança;
    - alterar as consequências;
    - partilhar o risco (p.e. através de contratos, aquisição de seguros);
    - reter o risco mediante decisão informada.

Tratamento dos Riscos

- Opções de Tratamento dos Riscos (NIST)
  - Assumir o Risco
    - Aceitar o Risco continuando com o sistema em operação
    - Podendo/devendo ir implementando controlos tendentes à redução do risco
  - Evitar o Risco
    - Eliminando a causa do risco ou as consequências (desativar certas funcionalidades ou, mesmo, desligar o sistema)
  - Transferência de Risco
    - Utilizando opções que permitam compensação em caso de perdas (p.e. seguros)
  - Planeamento de Risco
    - Gerir o risco, desenvolvendo um plano de mitigação que prioriza, implementa e mantem os controlos
  - Limitar o Risco
    - Implementar os controlos capazes de minimizar o impacto de certas ameaças sobre alguma vulnerabilidade
    - Necessário implementar medidas de detecção, prevenção e suporte
    - (se for verificado um determinado incidente, desligar sistema, ou repor sistema…)
  - Reconhecimento e Desenvolvimento de controlos
    - De forma a baixar o risco, à medida que as vulnerabilidades são reconhecidas, é implementado um plano de desenvolvimento e implementação de controlos que permitam corrigir ou minimizar a vulnerabilidade

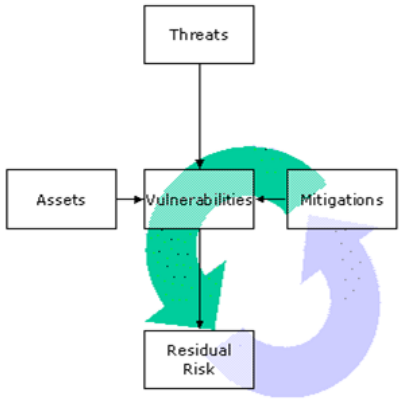
Tratamento dos Riscos - técnico e/ou administrativo

- Mitigação técnica ou administrativa ?
- Assumir o Risco
- Evitar o Risco
- Transferência de Risco
- Planeamento de Risco
- Limitar o Risco
- Reconhecimento e Desenvolvimento de controlos

Predominantemente técnicos

Tratamento dos Riscos

- Risk Mitigation Checklist (extraído do NIST)
  - Each proposed risk mitigation option should be examined from the following perspectives:
    - Effectiveness.
      - Will it reduce or eliminate the identified risks? To what extent do alternatives mitigate the risks? Effectiveness can be viewed as being somewhere along a continuum, as follows:
        - Level One (Engineering actions): The safety action eliminates the risk, for example, by providing interlocks to prevent thrust reverser activation in flight;
        - Level Two (Control actions): The safety action accepts the risk but adjusts the system to mitigate the risk by reducing it to a manageable level, for example, by imposing more restrictive operating conditions; and
        - Level Three (Personnel actions): The safety action taken accepts that the hazard can neither be eliminated (Level One) nor controlled (Level Two), so personnel must be taught how to cope with it, for example, by adding a warning, a revised checklist and extra training.

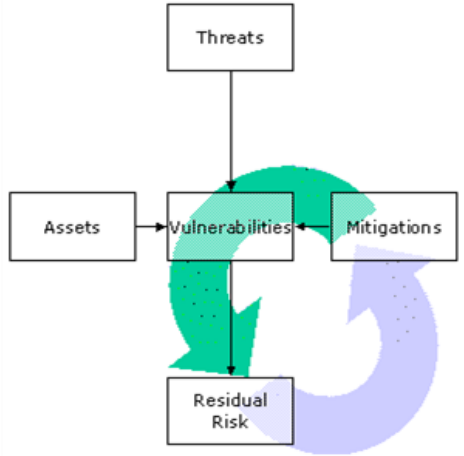


Tratamento dos Riscos

- Cost/benefit.
  - Do the perceived benefits of the option outweigh the costs? Will the potential gains be proportional to the impact of the change required?
- Practicality.
  - Is it doable and appropriate in terms of available technology, financial feasibility, administrative feasibility, governing legislation and regulations, political will, etc.?
- Challenge.
  - Can the risk mitigation measure withstand critical scrutiny from all stakeholders (employees, managers, stockholders/State administrations, etc.)?
- Acceptability to each stakeholder.
  - How much buy-in (or resistance) from stakeholders can be expected? (Discussions with stakeholders during the risk assessment phase may indicate their preferred risk mitigation option.)

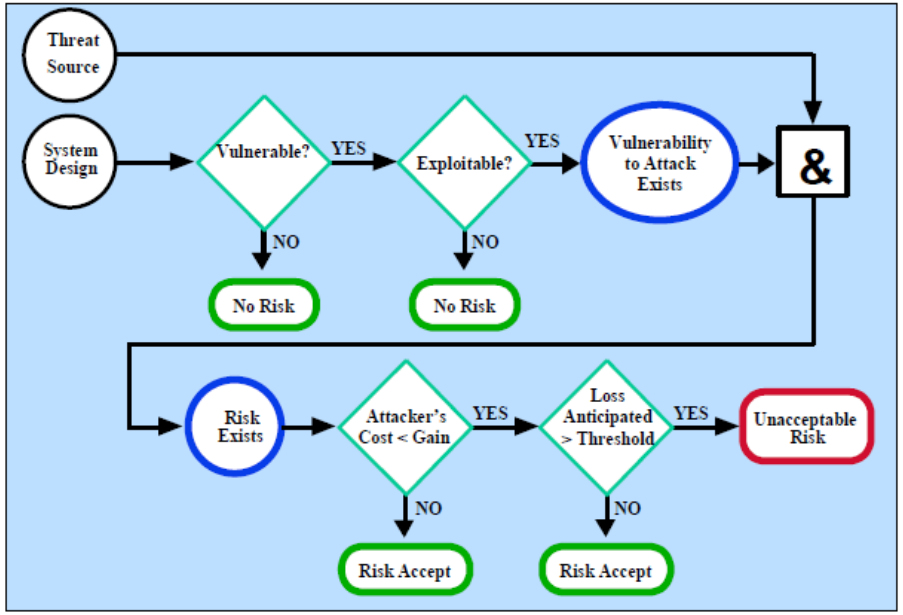
Tratamento dos Riscos

- Enforceability.
  - If new rules (SOPs, regulations, etc.) are implemented, are they enforceable?
- Durability.
  - Will the measure withstand the test of time? Will it be of temporary benefit or will it have long-term utility?
- Residual risks.
  - After the risk mitigation measure is implemented, what will be the residual risks relative to the original hazard? What is the ability to mitigate any residual risks?
- New problems.
  - What new problems or new (perhaps worse) risks will be introduced by the proposed change?



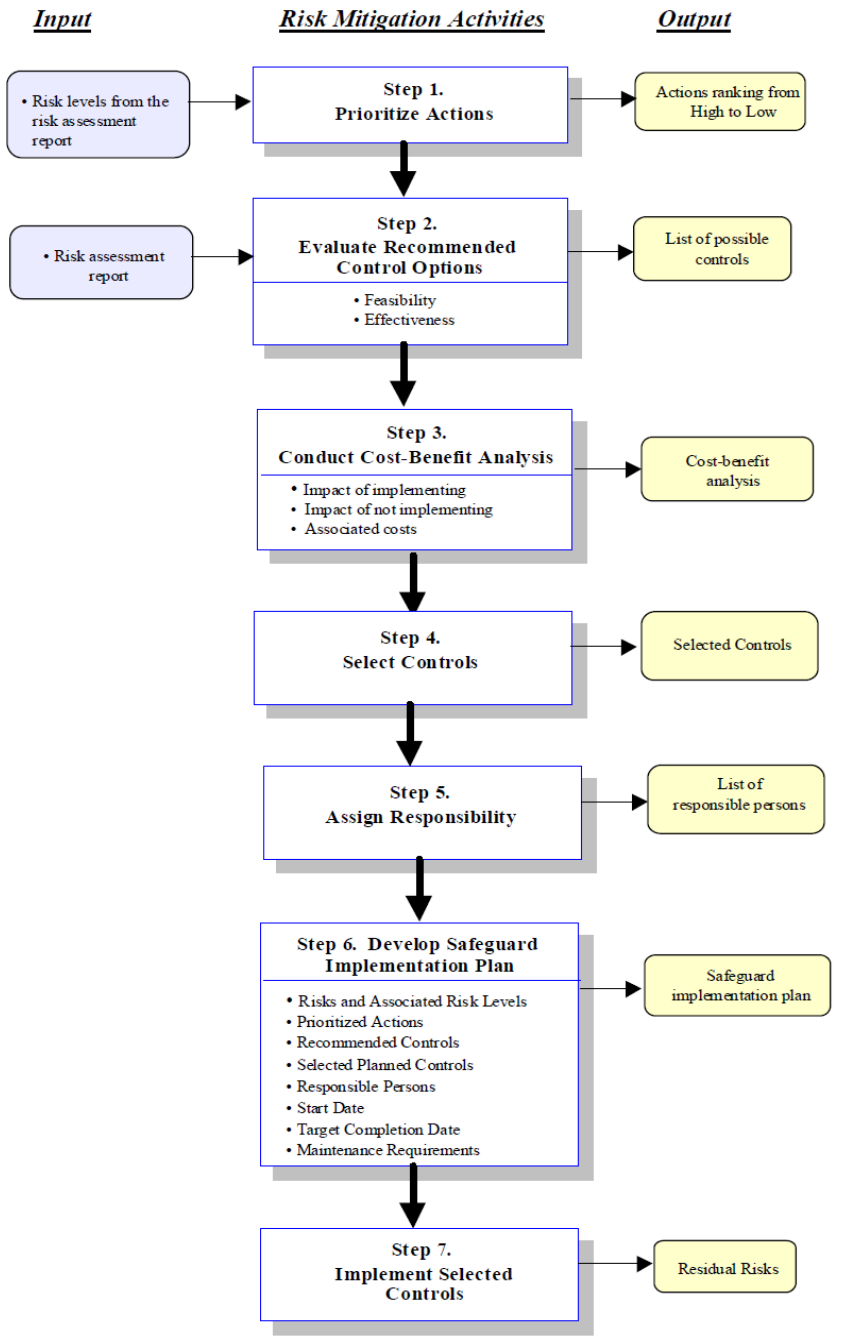
Tratamento dos Riscos

- Fluxo de aceitação de riscos
- Ou não aceitação e implementação de controlos



Tratamento dos Riscos

- 7 passos para a implementação de controlos
  - Step 1- Prioritize Actions
    - Output -Actions ranking from High to Low
  - Step 2- Evaluate Recommended Control Options
    - Output from - List of feasible controls
  - Step 3 - Conduct Cost-Benefit Analysis
    - Output - Cost-benefit analysis describing the cost and benefits of implementing or not implementing the controls
  - Step 4 - Select Control
    - Output from - Selected control(s)
  - Step 5 - Assign Responsibility
    - Output - List of responsible persons
  - Step 6 - Develop a Safeguard Implementation Plan
    - Output - Safeguard implementation plan
  - Step 7 - Implement Selected Control(s)
    - Output from - Residual risk



AGENDA

- Tratamento dos Riscos

- **Controlos de segurança**
  - **Tecnológicos, Operacionais e de Gestão**

- Modelo de segurança integrado
  - Controlos de segurança alinhados com as melhores práticas

Controlos de segurança

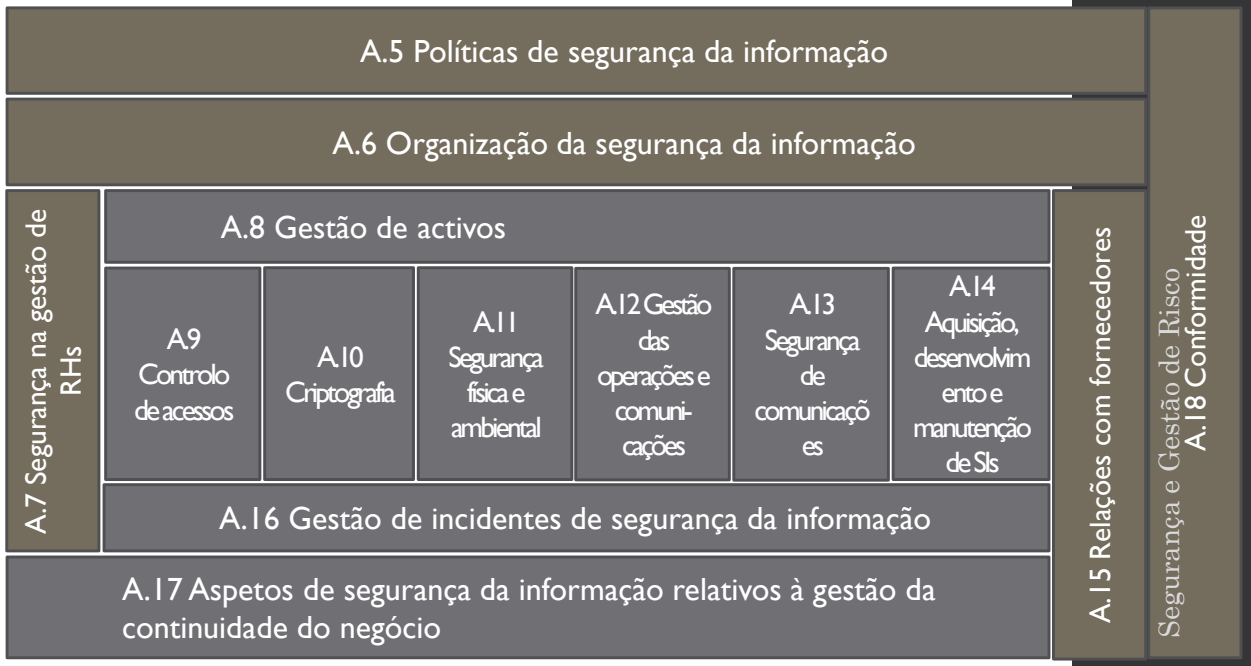
- Control (ISO 27001)
  - measure that is modifying risk (3.61)
    - Note 1 to entry: Controls include any process (3.54), policy (3.53), device, practice, or other actions which modify risk (3.61).
    - Note 2 to entry: It is possible that controls not always exert the intended or assumed modifying effect.

Controlos de segurança

- A implementação de controlos ou medidas de segurança
  - Deve resultar de um processo de avaliação de riscos
  - Opção de Tratamento Técnico ou Administrativo
    - Compromisso entre ambas
  - Carece de uma cuidada análise de custo-benefício

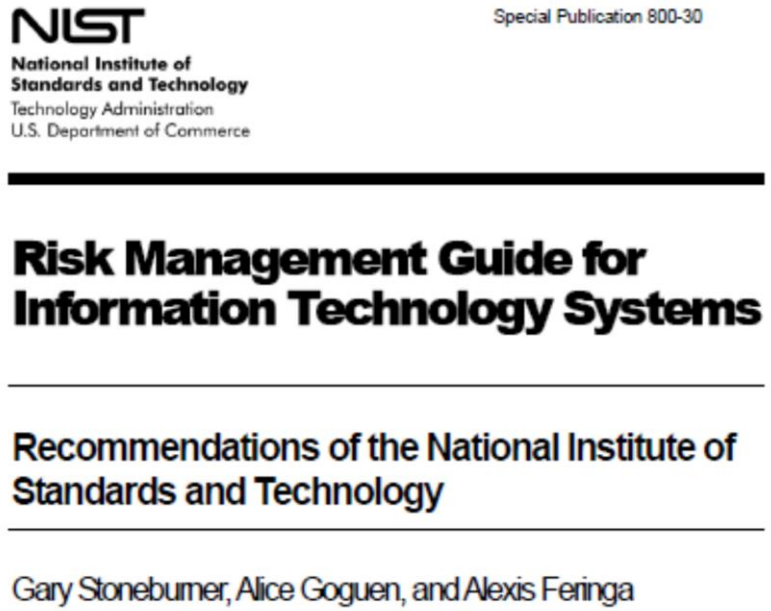
Controlos de segurança

- Na ISO/IEC 27001:2013 os controlos de segurança estão agrupados em 14 pontos, do Anexo A
  - Administrativos e de procedimento
  - tecnológicos



Controlos de segurança

- Os controlos a implementar podem ser agrupados em (NIST Special Publication 800-30)
  - Tecnológicos
  - Não tecnológicos: Gestão,
  - Operacionais e Organizacionais


NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-30

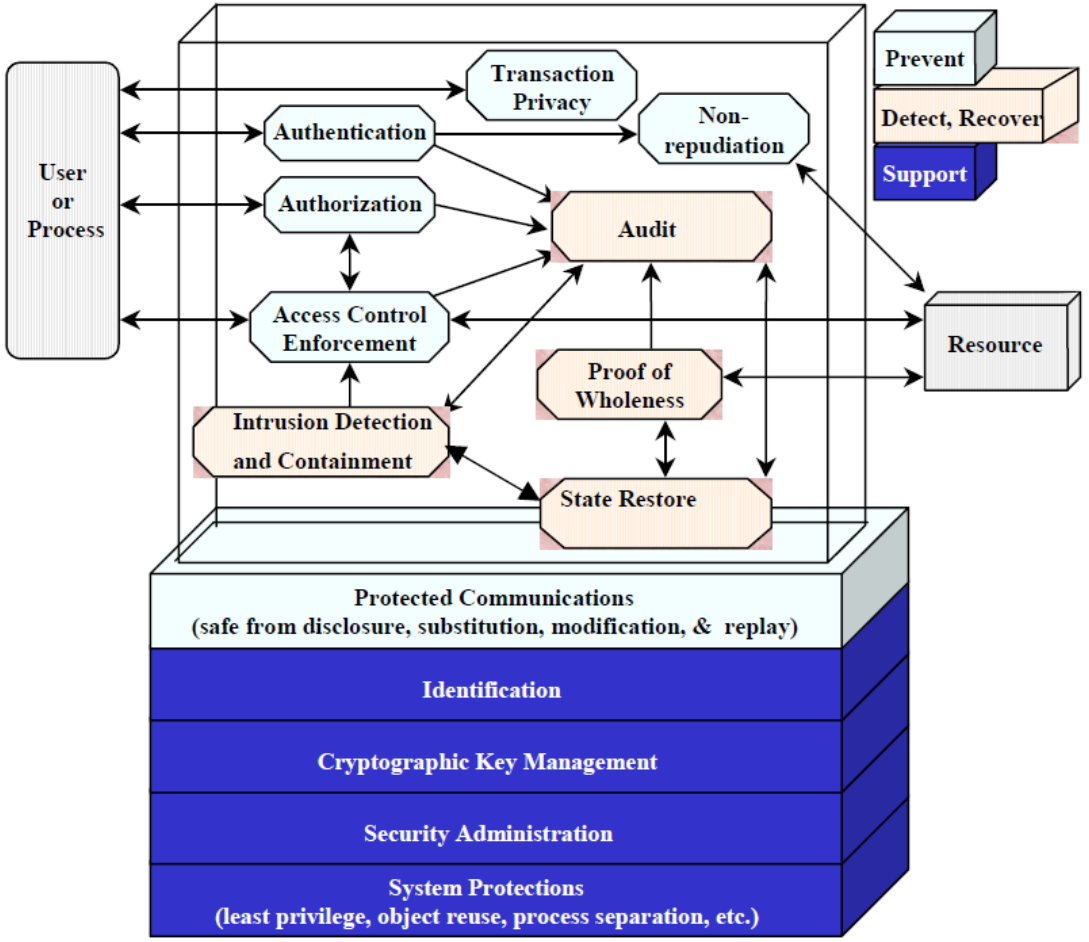
Risk Management Guide for Information Technology Systems

Recommendations of the National Institute of Standards and Technology

Gary Stoneburner, Alice Goguen, and Alexis Feringa

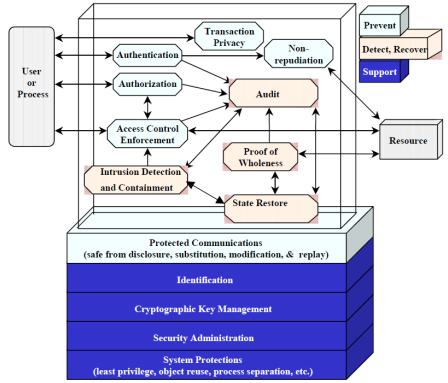
Controlos de segurança

- Controlos Tecnológicos
  - de Suporte
  - Preventivos
  - Para detecção e recuperação



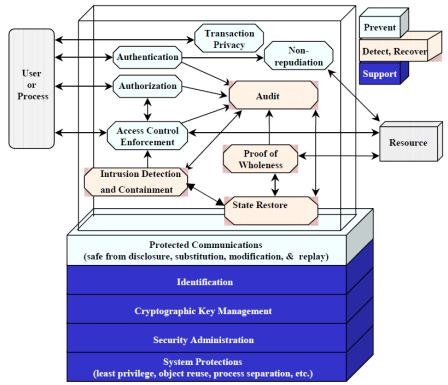
Controlos de segurança

- Controlos Técnicos de Suporte
  - São a base e estão interligados com outros controlos de segurança
  - Identificação
    - Permite a identificação de utilizadores, processos e recursos informacionais
  - Gestão de Chaves Criptográficas
    - Proporcionam uma gestão segura e eficiente
    - das chaves, utilizadas por outros controlos

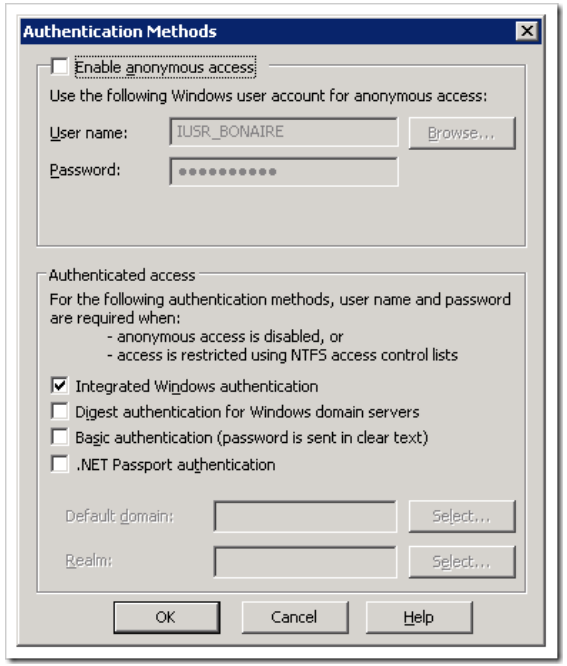


Controlos de segurança

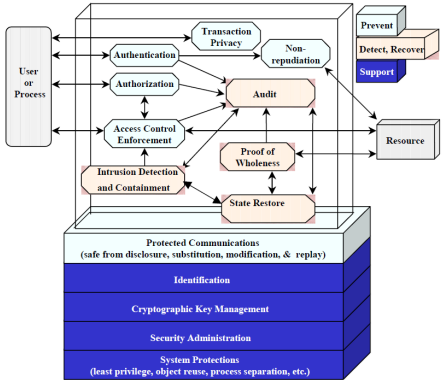
- Controlos Técnicos de Suporte (cont.)
  - Administração da Segurança
    - Configuração apropriada dos sistemas e aplicações tendo em conta as características de cada instalação
    - Ativação ou desativação de registos de auditoria
  - Proteção de Sistemas
    - Em que a segurança é atingida através de uma
    - implementação cuidada de cada sistema
      - Na sua conceção, desenvolvimento e instalação
        - Cuidados na proteção da informação residual (apagar se sensível)
        - A atenção à informação disponibilizada (respeitar a necessidade de conhecer)
        - Separação de processos
        - Modularidade
        - Desenvolvimento por camadas



Controlos de segurança

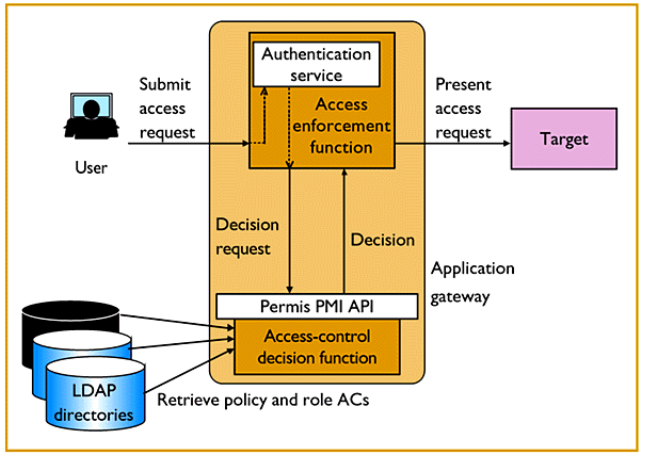


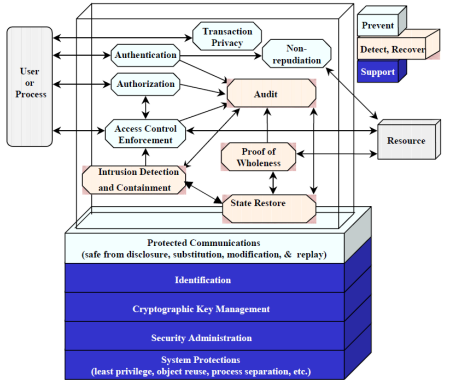
- Controlos Técnicos Preventivos
  - Autenticação
    - Assegura o processo de controlo de
    - identidade
    - Vários mecanismos:
      - User/Pass
      - PIN
      - Autenticação forte
      - Biometria
  - Autorização
    - Permite a especificação e posterior gestão das ações permitidas num determinado sistema
    - Quem ou que objetos podem criar ou apagar ficheiros
    - Quem pode executar determinada aplicação



Controlos de segurança

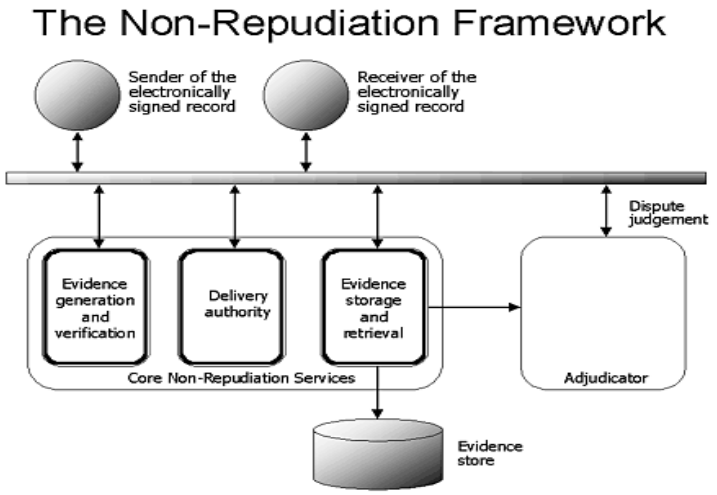
- Controlos Técnicos Preventivos
  - Controlo de Acessos
    - Visa conseguir a Integridade e confidencialidade da Informação,
    - respeitando a política de segurança
  - Algumas técnicas de Controlo de Acesso
    - Attribute-Based Access control (ABAC)
      - Controlo de acessos baseado nos atributos do utilizador
      - Por exemplo: a idade >18, uu local/morada
    - Discretionary Access Control (DAC)
      - Acesso controlado pelo utilizador ou criador do objecto
      - Ex: Permissões de Ficheiros, ACLs (access control lists)
    - Mandatory Access Control (MAC)
      - Controlado pelo sistema. Utilizado para implementar segurança a vários níveis, em informação sensível (tipicamente governo e militares)
      - Ex: sensitivity labels – todos os utilizadores e objectos têm uma label atribuída.
      - Utilizador só tem acesso a certo documento ou funcionalidade se a sua label estiver de acordo com a label do objecto.
    - Role Based Access Control (RBAC)
      - Controlado pelo sistema, mas baseado nas funções atribuídas a utilizadores ou grupos
      - Role assignment: Só pode executar uma transacção de tiver essa função atríbuida
      - Role authorization: dá utorização de determinados utilizadores utilizarem essa função
      - Transaction authorization: em conjunto com 1 e 2 assegura que a transacção só é realizada por utilizadores autorizados

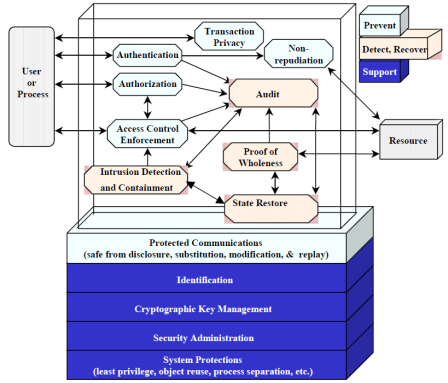




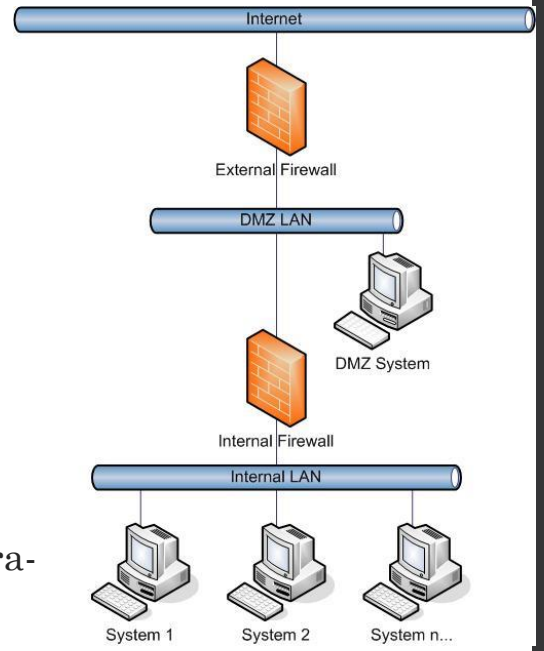
Controlos de segurança

- Controlos Técnicos Preventivos
  - Não repudio
    - Assegurar e garantir a responsabilidade de determinada ação
      - Envio ou receção de documento
      - Criar ou apagar dados
      - …
    - Ao assegurar a correta “accountability”
      - das transações relevantes
      - previne o não repúdio

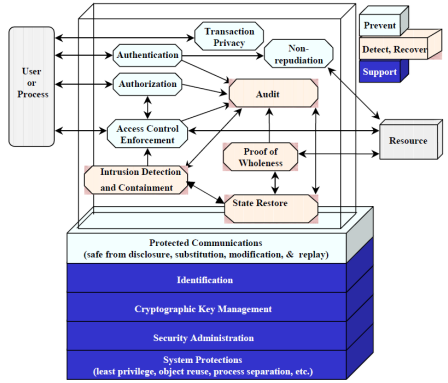




Controlos de segurança

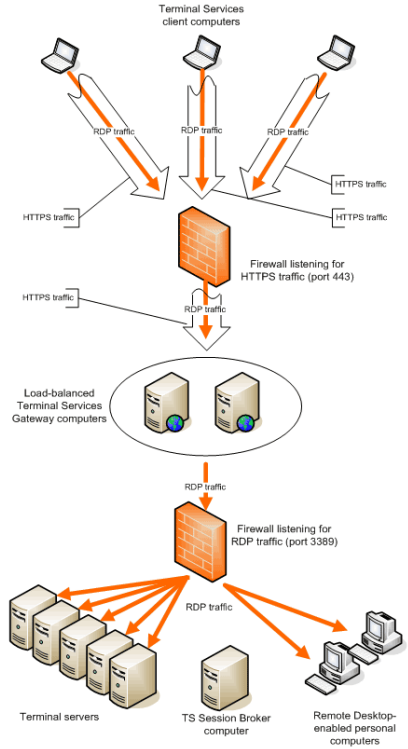


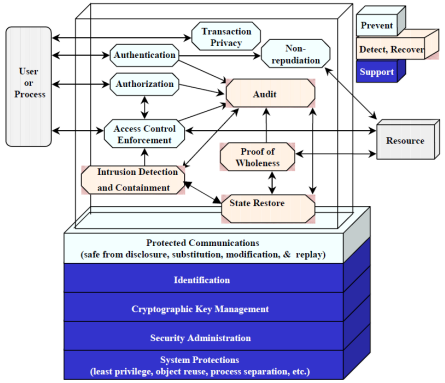
- Controlos Técnicos Preventivos
  - Proteção das comunicações
    - A segurança das comunicações é hoje um requisito para a generalidade das infra-estruturas
    - Assegura a confidencialidade, integridade e disponibilidade
      - Estabelecimento de VPNs, IPSEC, recorrendo a mecanismos criptográficos, para garantir a
      - integridade e confidencialidade
      - Implementação de segurança perimétrica, para manter a disponibilidade – Firewall, IPS(?)
    - Em certos cenários: necessário garantir segurança nas comunicações internas
    - Com especial atenção para a WLAN



Controlos de segurança

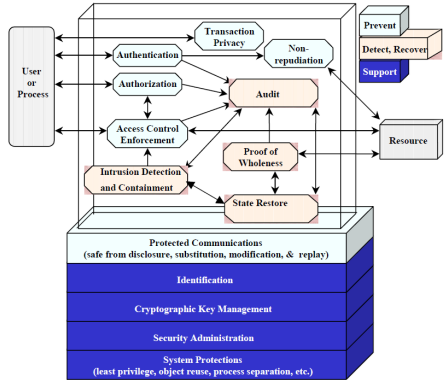
- Controlos Técnicos Preventivos
  - Privacidade das transações
    - Implementação de mecanismos que assegurem a privacidade de determinadas transações
    - Pode ser utilizado o SSL - Secure Sockets Layer
      - Para transferência segura de dados entre serviços como email ou HTTP (neste caso HTTPS)
    - Ou o SSH - Secure Shell
      - para interligação de dois sistemas, permitindo a execução de comandos remotos
    - Não esquecer que a privacidade da transação assegura apenas parte da privacidade de dados ou ações
      - Os dados gravados devem também ser acautelados através de formas de armazenamento dos dados e mecanismos de controlo de acessos





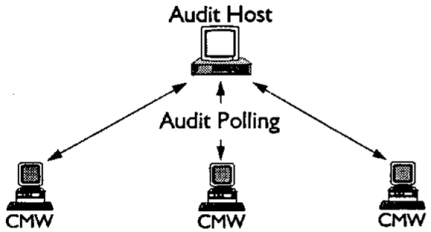
Controlos de segurança

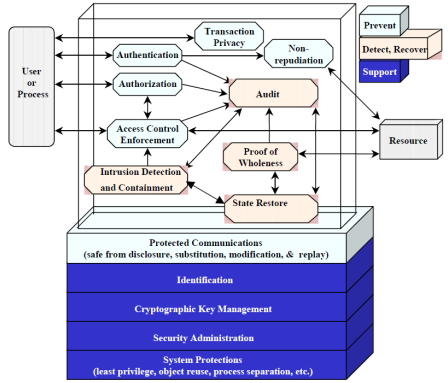
- Controlos Técnicos para deteção e recuperação
  - Controlos que permitem a deteção de violação ou tentativa de violação das regras de políticas
  - Funcionam como complemento à segurança das medidas de suporte e preventivas
  - Controlos:
    - Audit.
    - Intrusion Detection and Containment.
    - Restore Secure State.
    - Virus Detection and Eradication.



Controlos de segurança

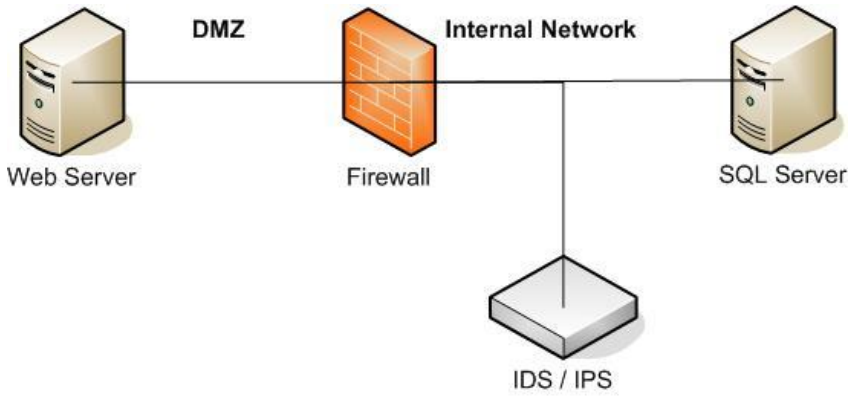
- Controlos Técnicos para deteção e recuperação
  - Audit
    - Análise de registos de auditoria/logs de sistema
    - Deteta eventos/acontecimentos à posteriori
    - Pode conduzir à recuperação de sistemas
    - Vantagem na centralização
      e utilização de aplicação específica

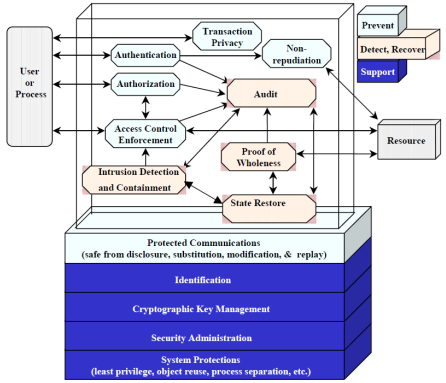




Controlos de segurança

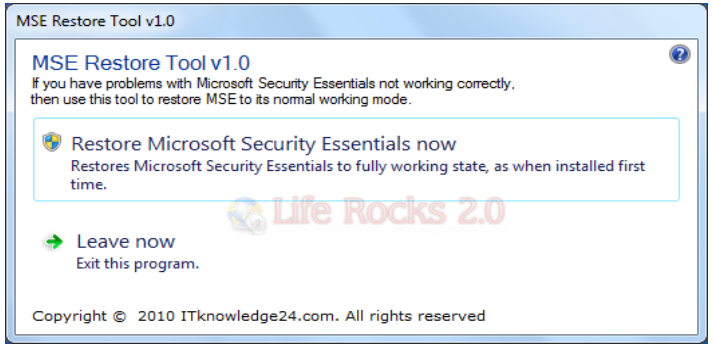
- Controlos Técnicos para deteção e recuperação
  - Intrusion Detection and Containment
    - Utilizado para detetar intrusões ou tentativas de intrusões
    - Pode atuar ativamente para conter a ameaça
    - Ou simplesmente lançar alertas
      - Uma tentativa de intrusão pode não ser concretizada, mas constituir prova
      - Requerer novos controlos
        - atualizações
        - ou configurações



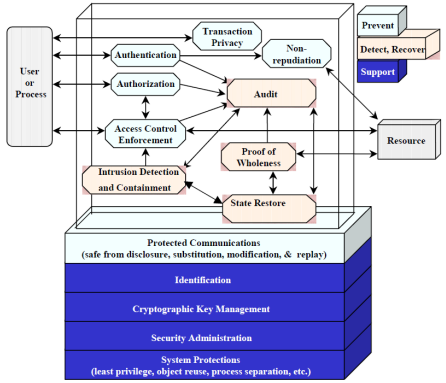


Controlos de segurança

- Controlos Técnicos para deteção e recuperação
  - Restore Secure State
    - Permite repor o sistema para um estado seguro
    - Sistemas já disponibilizam ferramentas



  - Virus Detection and Eradication
    - Deve ser instalado em servidores e postos de trabalho
      - Para detetar, identificar e remover virus



Controlos de segurança

- Controlos não tecnológicos
  - Devem ser implementados em conjunto com os controlos tecnológicos
  - Contribuindo para gerir e minorar o risco
  - Constituídos por:
    - Controlos de Gestão e Organizacionais
      - Focados na definição de políticas e normas de proteção da informação, realizadas através de procedimentos operacionais
      - Processos e procedimentos que definem como os elementos da organização devem atuar no sentido de colaborar na segurança
    - Controlos Operacionais
      - Conjunto de controlos e linhas orientadoras que assegurem procedimentos seguros de governação do IT, no sentido de cumprir os objetivos da organização

Controlos de segurança

- Controlos de Gestão da Segurança
  - Controlos Preventivos
    - Atribuir responsabilidades relativas à segurança dos sistemas críticos
    - Estabelecer e manter planos de segurança de suporte ao IT, que documentem
      - os controlos implementados
      - o plano de implementação de novos controlos
    - Implemente controlos de segurança pessoal
      - Separação de funções
      - Privilégios mínimos
      - Criação e desativação de contas de utilizadores e computadores
      - Registo de utilização
    - Estabeleça programas de formação e sensibilização dos utilizadores
      - Dando a conhecer os cuidados e regras de utilização dos sistemas
      - Responsabilidade de cada um na proteção da informação
    - Estabelecimento de procedimentos para acesso de terceiros
      - parceiros, fornecedores, clientes, prestadores de serviços

Controlos de segurança

- Controlos de Gestão da Segurança
  - De deteção
    - Implementar medidas de segurança de pessoal como
      - Credenciação de pessoal
        - analisando as competências e o passado (p.e. Registo Criminal e Referências)
      - Rotação de funções
    - Conduzir o processo de gestão de risco
    - Conduzir a revisão e atualização dos controlos de segurança
    - Realização de auditorias periódicas
    - Analise e subscreva a aceitação de riscos residuais
  - De recuperação
    - Providenciar o estabelecimento e gestão de um plano operacional de continuidade de negócio
    - Criar capacidade de resposta a incidentes
      - estabelecendo responsabilidades e papeis

Controlos de segurança

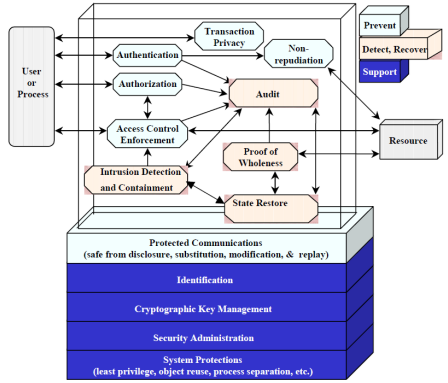
- Controlos Operacionais da Segurança
  - Preventivos
    - Controlar o acesso aos dados e à sua eliminação quando necessário
    - Controlar novos virus de software e a adequação dos controlos implementados (AV)
    - Manter em segurança os sistemas informáticos
      - Proteções de segurança dos equipamentos
      - Garantir os procedimentos definidos para as visitas
      - Manter os sistemas de controlo de acessos, por cartão ou biométricos
    - Manter em segurança os sistemas de rede e cablagem
    - Providenciar os mecanismos adequados de backup
      - Assegurando a salvaguarda de toda a informação necessária à recuperação
    - Estabelecer e controlar os procedimentos de segurança de armazenamento de dados for a da organização
    - Proteger os sistemas contra o fogo
      - Requer manter e conhecer os procedimentos de combate a incêndio
    - Providenciar e assegurar o funcionamento de geradores e UPSs
    - Controlo ambiental do Data Center (Ar condicionado)
      - E outros locais onde estejam equipamentos informáticos ou armazenados os dados

Controlos de segurança

- Controlos Operacionais da Segurança
  - De deteção
    - Providenciar a segurança física (deteção de intrusões, alarmes, CCTV)
    - Assegurar a segurança ambiental (detetores de incêndios, sensores de temperatura e humidade, e alarmes).

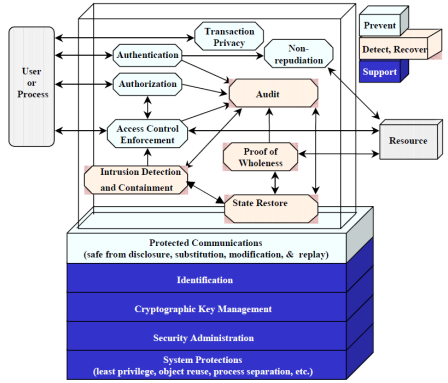
Controlos de segurança

- Exercício – Identificar controlos de segurança
  - Controlos não tecnológicos
    - Controlos de Gestão e Organizacionais
      - Preventivos
      - de Deteção
      - de Recuperação
    - Controlos Operacionais
      - Preventivos
      - de Deteção



Controlos de segurança

- Exercício – Identificar controlos de segurança
  - Controlos Técnicos de Suporte
    - Identificação
    - Gestão de Chaves Criptográficas
    - Administração da Segurança
    - Proteção de Sistemas
  - Controlos Técnicos Preventivos
    - Autenticação
    - Autorização
    - Controlo de Acessos
    - Não repudio
    - Proteção das comunicações
    - Privacidade das transações
  - Controlos Técnicos para deteção e recuperação
    - Audit.
    - Intrusion Detection and Containment.
    - Proof of Wholeness.
    - Restore Secure State.
    - Virus Detection and Eradication.



AGENDA

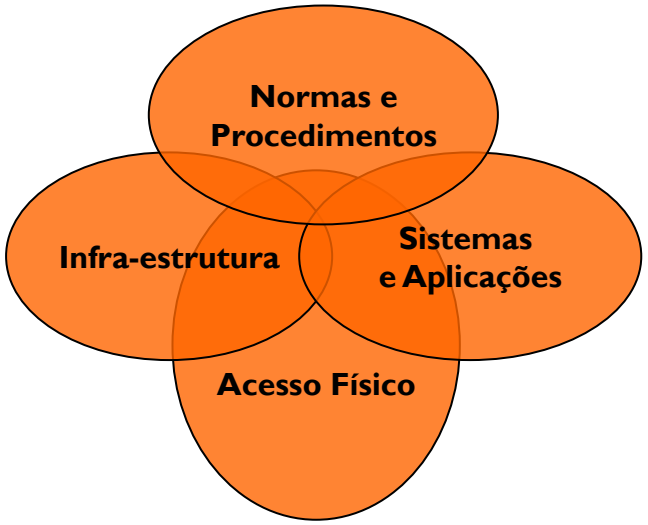
- Tratamento dos Riscos

- Controlos de segurança
  - Tecnológicos, Operacionais e de Gestão

- **Modelo de segurança integrado**
  - **Controlos de segurança alinhados com as melhores práticas**

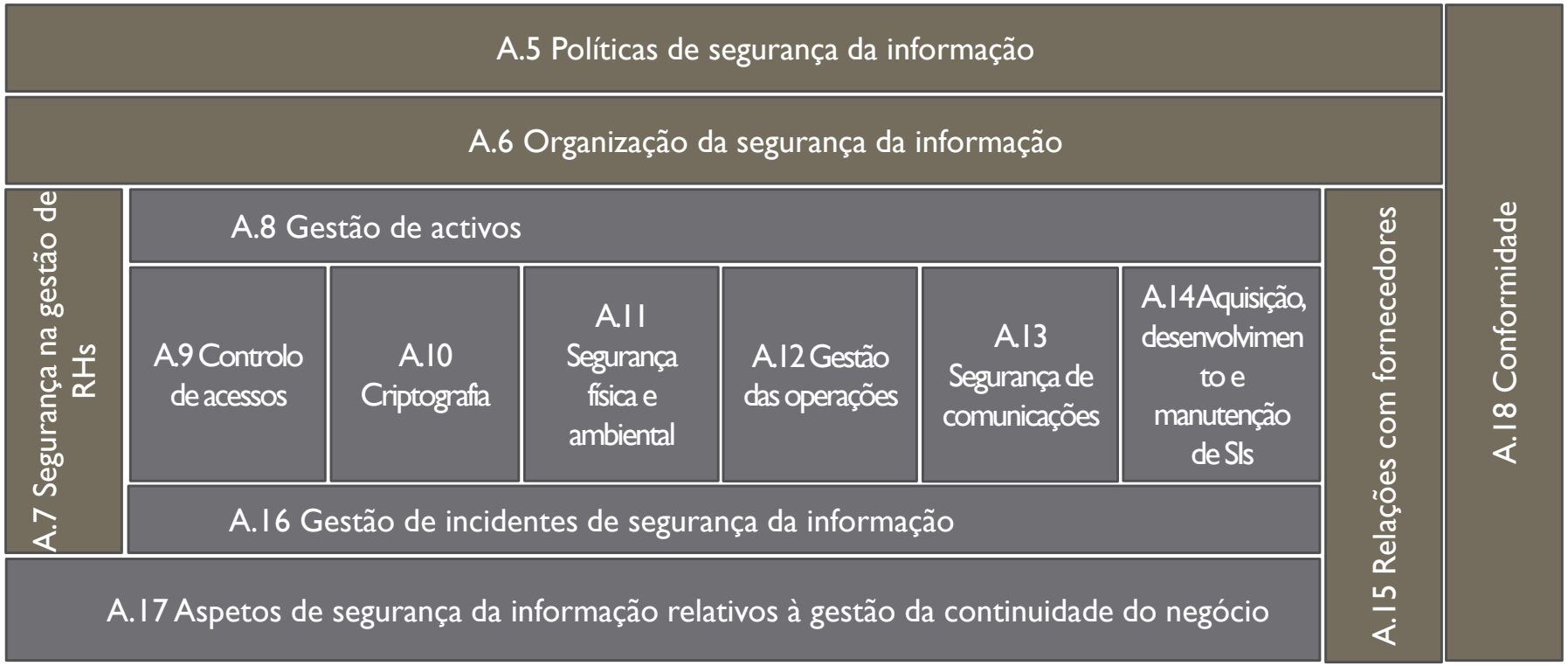
Abordagem Integrada à Segurança

- A Segurança de um Sistema de Informação só se consegue atingir considerando de forma integrada:
  - Normas e Procedimentos
    - Definição adequada de processos de negócio e fluxos de trabalho
    - **Definição de Políticas de Segurança**
    - Definição de Processo de Desenvolvimento de Software
    - Procedimentos de Operação definidos (operacionalização)
    - Programas de Sensibilização
  - Sistemas e Aplicações
    - Devidamente testados
    - Acompanhados ao longo do ciclo de vida
  - Infra-estrutura
    - Adequada aos Sistemas e Aplicações
    - Mecanismos de controlo (firewalls, ids ...)
    - Mecanismos de monitorização
  - Acesso Físico
    - Acesso ao(s) edifício(s)
    - Controlo de acesso a zonas
    - Monitorização



Modelo de segurança integrado

- Utilização da ISO 27002
  - Como suporte à gestão da segurança da informação



Controlos de segurança

- Na ISO/IEC 27001:2022 os controlos de segurança foram atualizados
  - De 114 Controlos na versão de 2013 passaram a 93
    - 35 permaneceram inalterados
    - fusão de 57 controlos, em 24
    - 23 Controlos renomeados
    - 11 novos controlos
    - 3 Controlos removidos
  - Agrupados em 4 áreas temáticas, face aos 14 domínios anteriores
    - A 5 – Controlos Organizacionais
    - A 6 – Controlos relacionados com as Pessoas
    - A 7 – Controlos físicos
    - A 8 – Controlos Tecnológicos

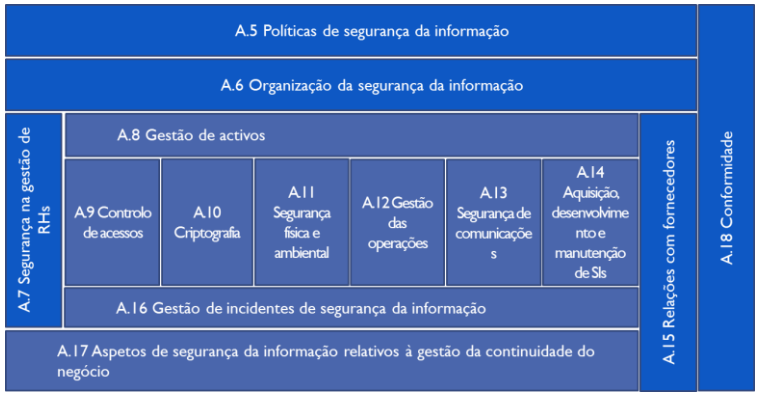
Controlos de segurança

- Na ISO/IEC 27001:2022 – exemplo novo controlos
  - Novo controlo
  - 5.07 Threatintelligence
    - Information relating to information security threats should be collected and analyzed to produce threat intelligence.

Control type	Information security properties	Cybersecurity concepts	Operational capabilities	Security domains
#Preventive #Detective #Corrective	#Confidentiality #Integrity #Availability	#Identify #Detect #Respond	#Threat_and_ vulnerability_ management	#Defence #Resilience

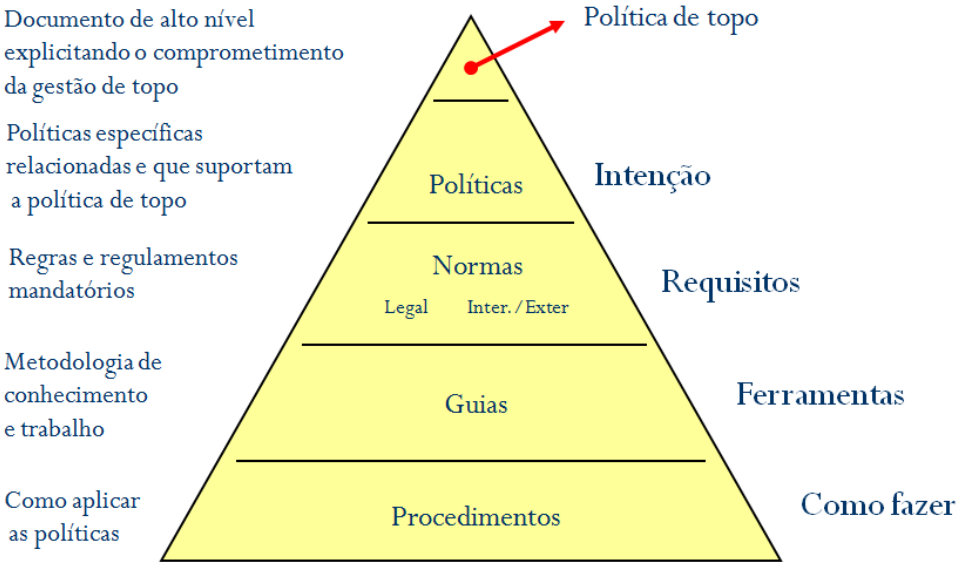
Modelo de segurança integrado

- Política de segurança
  - "Uma política de segurança deverá ser aprovada pela direção da organização, publicada e comunicada apropriadamente a todos os funcionários"
    - Para possuir a direção dos gestores de topo e o seu indiscutível suporte à segurança da informação;
    - Para fornecer elementos comuns de abordagem à Segurança da Informação;
    - Para responsabilização de todos os elementos da organização;
    - Sancionar quem não cumpre.



Modelo de segurança integrado

- Estruturação de políticas de segurança



- A política de segurança de alto nível (topo)
  - não pode deixar dúvidas quanto à necessidade de TODOS os funcionários a respeitarem na íntegra.
  - Simples e direta;
  - Os pontos principais deverão ocupar uma simples folha de papel A4;
  - O conteúdo completo da política deverá estar acessível a todos dentro da organização.

Modelo de segurança integrado

- As Políticas de segurança poderão conter:
  - Os requisitos para o plano de contingência da organização;
  - As necessidades de backup/restore;
  - A forma de seleção e gestão de ferramentas de eliminação de vírus;
  - As especificações de mecanismos para controlo de acessos a sistemas e dados;
  - Forma de comunicação de incidentes de segurança;
  - A descrição de ações disciplinares para atividades maliciosas ou de acesso/utilização inapropriado de recursos.
- Deverão ser revistas periodicamente

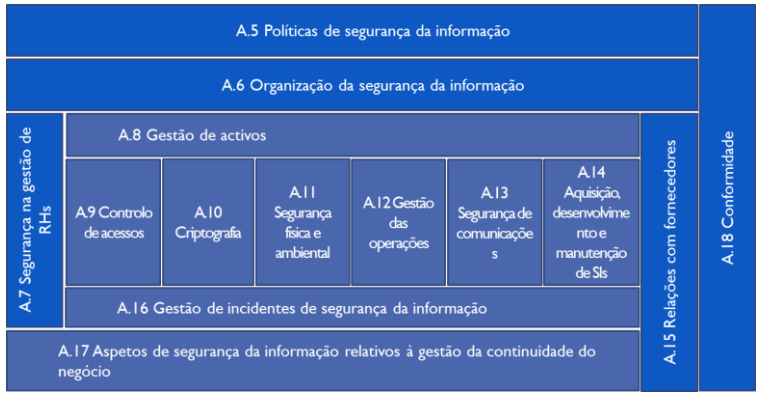
Modelo de segurança integrado

- Organização da Segurança

De forma a estabelecer um modelo de referência de gestão para iniciar e controlar a implementação e operação da segurança da informação dentro da organização.

- Papéis e responsabilidades de segurança da informação
- Segregação de funções
- Contacto com autoridades competentes
- Contacto com grupos de interesse especial
- Segurança da informação na gestão de projeto

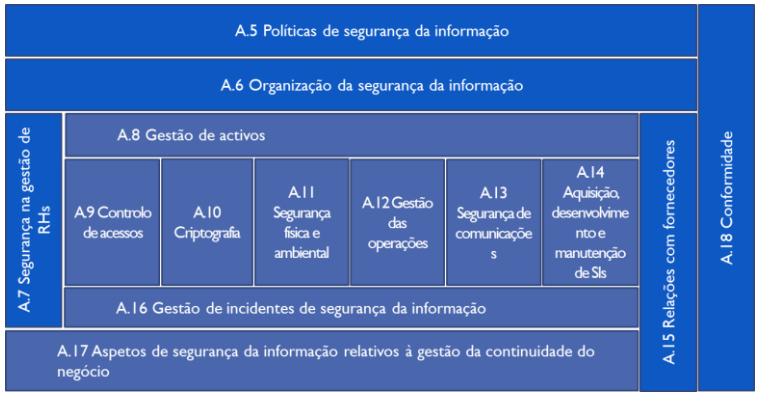
- Política de dispositivos móveis e Teletrabalho
  - De forma a assegurar a segurança no teletrabalho e na utilização de dispositivos móveis.



Modelo de segurança integrado

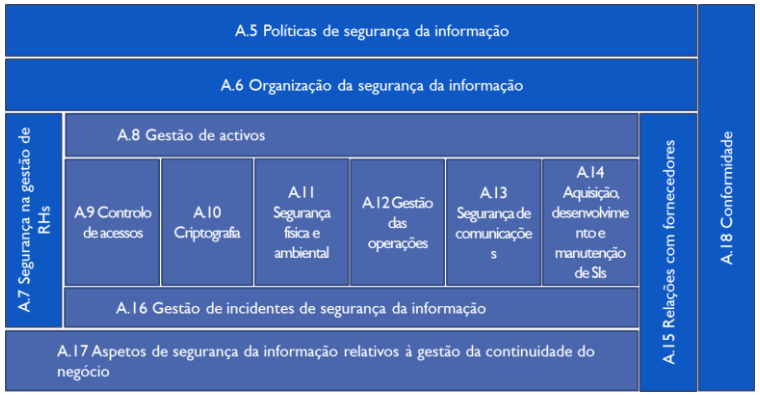
- Segurança na gestão de RHs

- Antes, durante a após a relação contratual
  - Verificação de credenciais
  - Acordos de confidencialidade
  - Termos e condições de trabalho
  - Responsabilidades
  - Resposta a incidentes de segurança
  - Educação e Treino
  - Ações disciplinares
  - Término das responsabilidades
  - Devolução de recursos
  - Remoção dos direitos de acesso



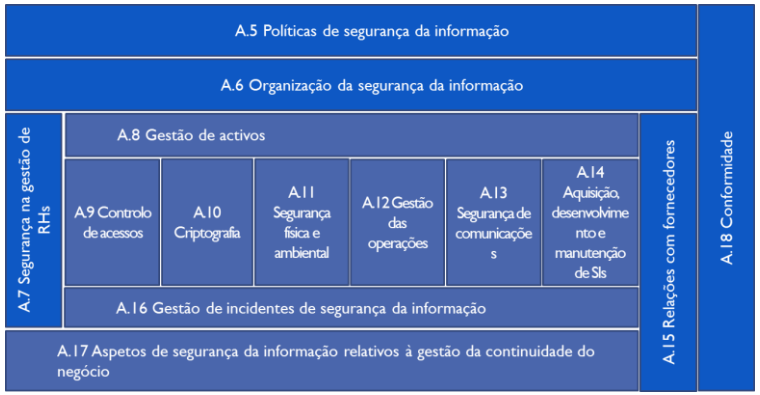
Modelo de segurança integrado

- Gestão de activos
  - Inventário de recursos
  - "Todos aqueles relevantes ao universo do Sistema de Gestão de Segurança da Informação."
  - Informação eletrónica, informação em papel, registos vídeo e sonoros, software aplicacional e de sistema, recursos físicos, elementos humanos, imagem e reputação e serviços contratados.
  - Responsabilidade pelos recursos
  - Classificação da Informação
    - Regras de classificação
    - Etiquetagem
    - Manuseamento



Modelo de segurança integrado

- Controlo de acessos à informação
  - Políticas de controlo de acessos
  - Regras de controlo
  - Responsabilidades dos utilizadores
  - Gestão de utilizadores
  - Controlo de acessos
    - Rede
    - Sistemas operativos
    - Aplicações
  - Monitorização de acessos e utilização
  - Clear Desk e Clear Screen



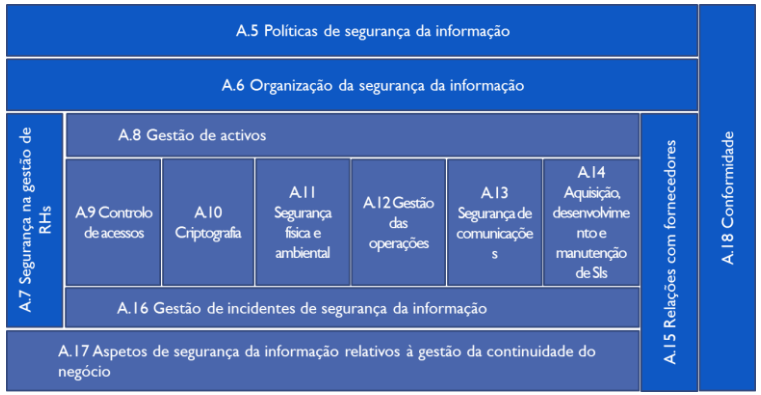
Modelo de segurança integrado

- Criptografia

De forma a assegurar a utilização adequada e eficaz de criptografia para proteger a confidencialidade, autenticidade e/ou integridade da informação

- Política sobre a utilização de controlos criptográficos
- Gestão de chaves
  - utilização, proteção e vida útil das chaves criptográficas

    ao longo de todo o seu ciclo de vida.



Exercício

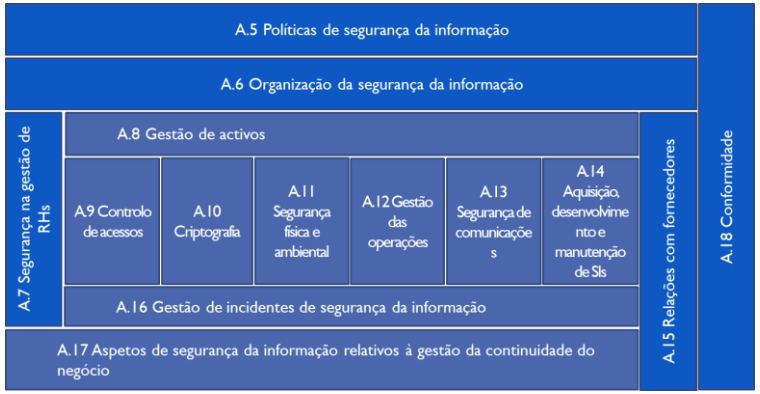
- Exemplos de controlos criptográficos?
  - Com vista à confidencialidade?
  - Com vista à integridade?
  - Disponibilidade?
  - Outras?

Controlos criptográficos

- (27002) Cryptographic controls can be used to achieve different information security objectives, e.g.:
  - a) confidentiality: using encryption of information to protect sensitive or critical information, either stored or transmitted;
  - b) integrity/authenticity: using digital signatures or message authentication codes to verify the authenticity or integrity of stored or transmitted sensitive or critical information;
  - c) non-repudiation: using cryptographic techniques to provide evidence of the occurrence or non-occurrence of an event or action;
  - d) authentication: using cryptographic techniques to authenticate users and other system entities requesting access to or transacting with system users, entities and resources.

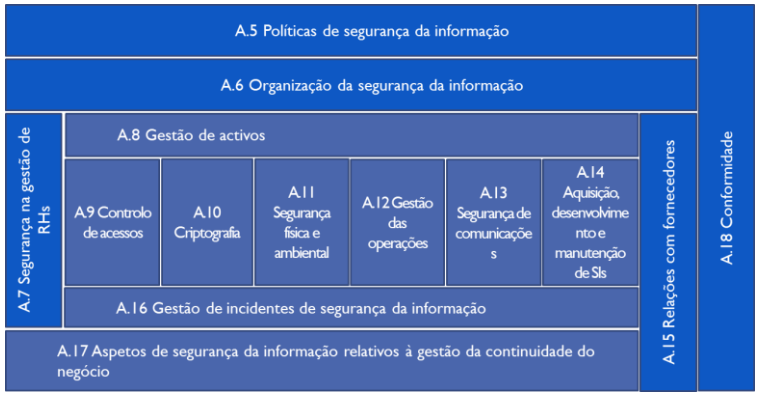
Modelo de segurança integrado

- Segurança física e ambiental
  - Perímetro de segurança física
  - Controlos de entrada física, permanência e saída
  - Segurança de escritórios, salas e instalações
  - Proteção contra ameaças externas e ambientais
  - Áreas de acesso público, de entrega e de carga
  - Proteção e acondicionamento do equipamento
  - Segurança da cablagem
  - Manutenção do equipamento
  - Segurança do equipamento fora das instalações da organização
  - Destruição e reutilização segura de equipamento



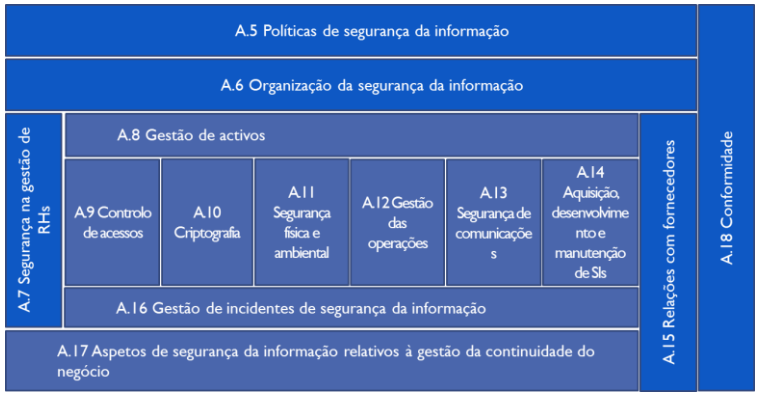
Modelo de segurança integrado

- Gestão de operações e comunicações
  - Procedimentos operacionais e responsabilidades
  - Segregação de funções
  - Gestão da capacidade e aceitação de sistemas
  - Proteções contra código malicioso e móvel
  - Monitorização e revisão dos serviços de terceiros
  - Gestão de rede
  - Salvaguarda da informação
  - Gestão de meios amovíveis
  - Políticas e procedimentos para troca/partilha de informação
  - Mensagens eletrónicas
  - Meios físicos em trânsito
  - Outras formas de partilha de informação



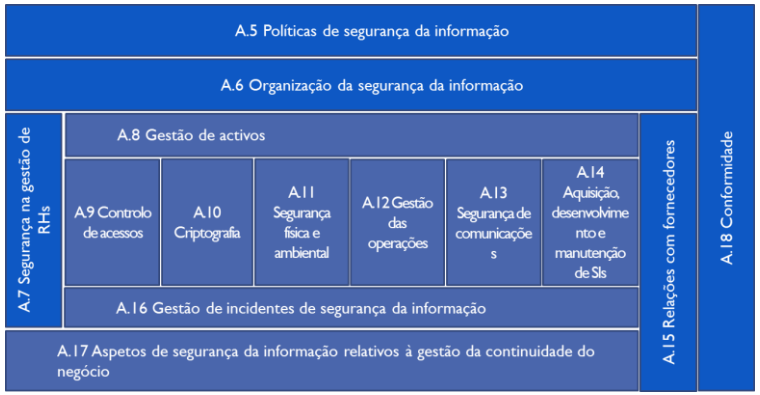
Modelo de segurança integrado

- Segurança de comunicações
  - Gestão da segurança da rede
    - Proteção da informação nas redes e nos seus recursos de processamento de informação.
    - Controlos da rede
    - Segurança de serviços de rede
      - mecanismos de segurança, níveis de serviço e requisitos de gestão para os serviços de rede devem ser identificados e incluídos nos acordos para serviços de rede,
    - Segregação das redes
  - Transferência da Informação
    - Mensagens eletrónicas
    - Acordos de transferência de informação



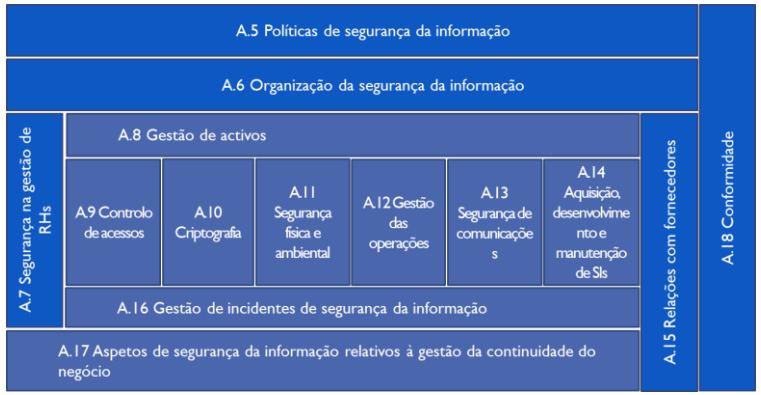
Modelo de segurança integrado

- Aquisição, desenvolvimento e manutenção de sistemas de informação
  - Análise e especificações de requisitos de segurança em sistemas de informação
  - Controlos criptográficos
  - Segurança de ficheiros de sistema
  - Restrições a alterações em pacotes de software
  - Desenvolvimento de software em outsourcing



Modelo de segurança integrado

- Gestão de incidentes de segurança da informação
  - Comunicação de eventos de segurança da informação
  - Comunicação de falhas de segurança
  - Responsabilidades e procedimentos
  - Aprendizagem com incidentes de segurança da informação
  - Coleção de evidências



Exercício de Grupo

- Idealizar um sistema de Gestão de Incidentes

Gestão de incidentes

A.16.1 Gestão de incidentes e melhorias de segurança da informação **Objetivo: Assegurar uma abordagem consistente e eficaz à gestão de incidentes de segurança da informação, incluindo a comunicação de eventos e pontos fracos de segurança.**		
A.16.1.1	**Responsabilidades e procedimentos**	Devem ser estabelecidos procedimentos e responsabilidades de gestão para assegurar uma resposta célere, eficaz e ordenada aos incidentes de segurança da informação.
A.16.1.2	**Reportar eventos de segurança da informação**	Os eventos de segurança da informação devem ser reportados através dos canais de gestão apropriados, o mais rapidamente possível.
A.16.1.3	**Reportar pontos fracos de segurança da informação**	Os colaboradores e os prestadores de serviço que utilizam os serviços e os sistemas de informação da organização devem ser instruídos a detetar e reportar qualquer ponto fraco de segurança da informação, observado ou suspeito, nos sistemas ou serviços.
A.16.1.4	**Avaliação e decisão sobre eventos de segurança da informação**	Os eventos de segurança da informação devem ser avaliados e deve ser decidido se os mesmos serão classificados como incidentes de segurança da informação.
A.16.1.5	**Resposta a incidentes de segurança da informação**	Os incidentes de segurança da informação devem ser tratados de acordo com os procedimentos documentados.
A.16.1.6	**Aprender com os incidentes de segurança da informação**	O conhecimento obtido através da análise e resolução de incidentes de segurança da informação deve ser empregue de forma a reduzir a probabilidade ou o impacto de futuros incidentes.
A.16.1.7	**Recolha de evidências**	A organização deve definir e aplicar procedimentos para a identificação, recolha, obtenção e preservação da informação, que possa servir como evidência.

Gestão de incidente

- O detalhe de "A.16.1.5 - Resposta a incidentes de segurança da informação"

16.1.5 Response to information security incidents

Control

Information security incidents should be responded to in accordance with the documented procedures.

Implementation guidance

Information security incidents should be responded to by a nominated point of contact and other relevant persons of the organization or external parties (see 16.1.1).

The response should include the following:

a) collecting evidence as soon as possible after the occurrence;

b) conducting information security forensics analysis, as required (see 16.1.7);

c) escalation, as required;

d) ensuring that all involved response activities are properly logged for later analysis;

e) communicating the existence of the information security incident or any relevant details thereof to other internal and external people or organizations with a need-to-know;

f) dealing with information security weakness(es) found to cause or contribute to the incident;

g) once the incident has been successfully dealt with, formally closing and recording it.

Post-incident analysis should take place, as necessary, to identify the source of the incident.

Other information

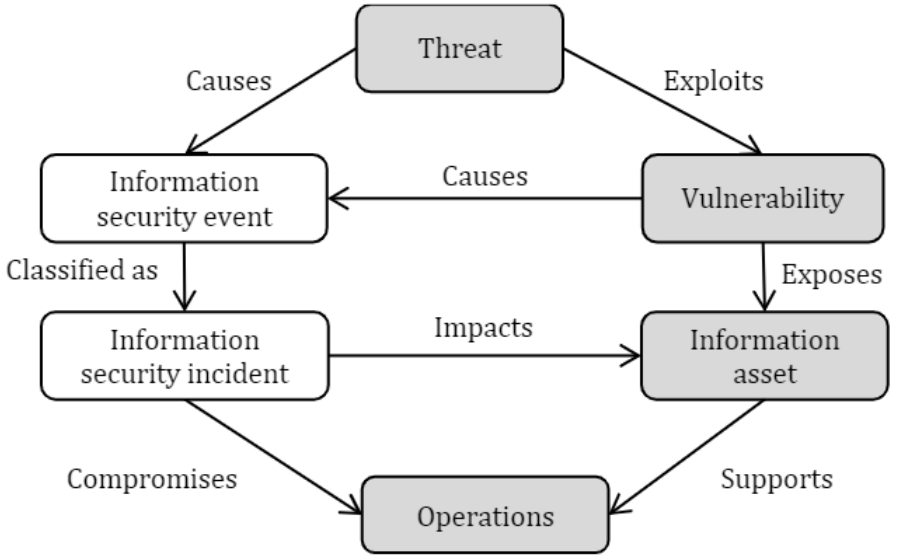
The first goal of incident response is to resume 'normal security level' and then initiate the necessary recovery.

Gestão de incidentes

- Com mais detalhe:
  - ISO/IEC 27035-1— Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management
  - ISO/IEC 27035-2:2016 — Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response
  - ISO/IEC 27035-3:2020 — Information technology — Information security incident management - Part 3: Guidelines for ICT incident response operations
  - ISO/IEC 27035-4 — Information technology — Information security incident management — Part 4: Coordination [DRAFT]
    - estabelece o conceito de Gestão Coordenada de Incidentes e sua aplicação em todo o ciclo de vida da Gestão de Incidentes - desde o planeamento da resposta até as lições aprendidas - por "comunidades" (supply chains ou redes relacionadas) com interesses comuns.

Gestão de incidentes

- Com mais detalhe:
  - ISO/IEC 27035-1:2022



NOTE The shaded objects are pre-existing, affected by the unshaded objects that result in an information security incident.

Figure 1 — Relationship of objects in an information security incident

Gestão de incidentes

- Com mais detalhe:
  - ISO/IEC 27035-1:2022

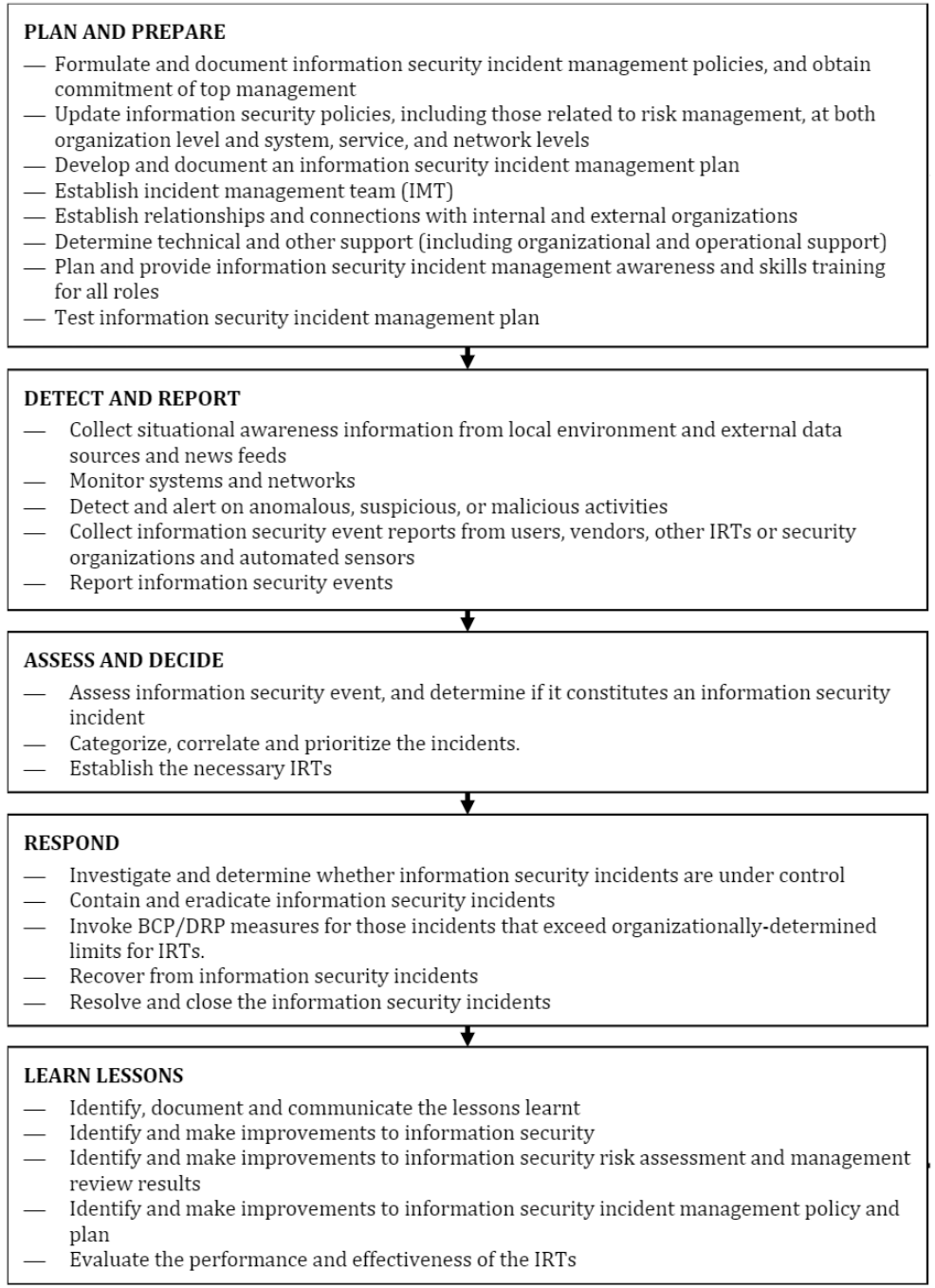


Figure 3 — Information security incident management phases

Gestão de incidentes

- Com mais detalhe:
  - ISO/IEC 27035-1:2022

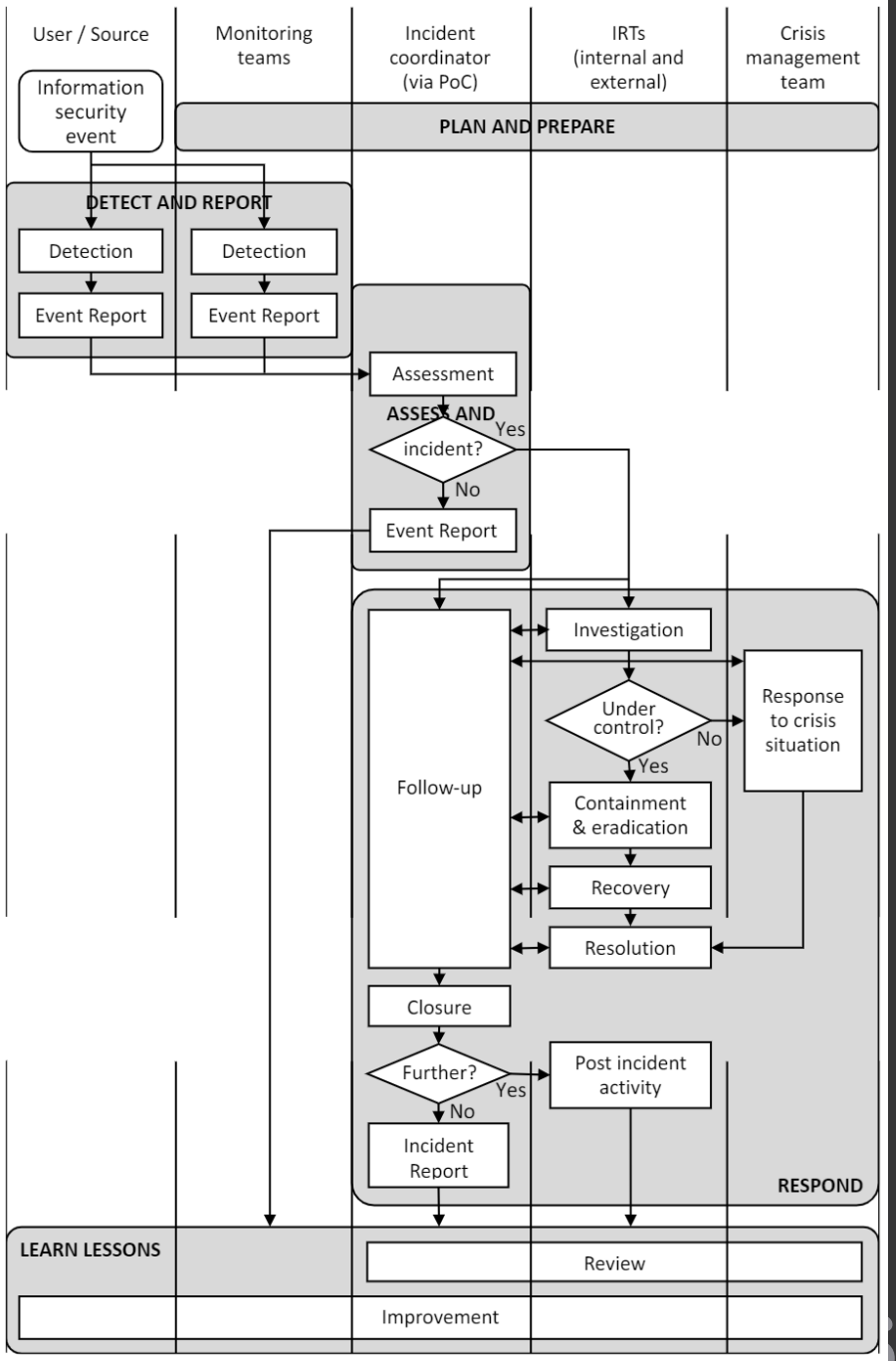
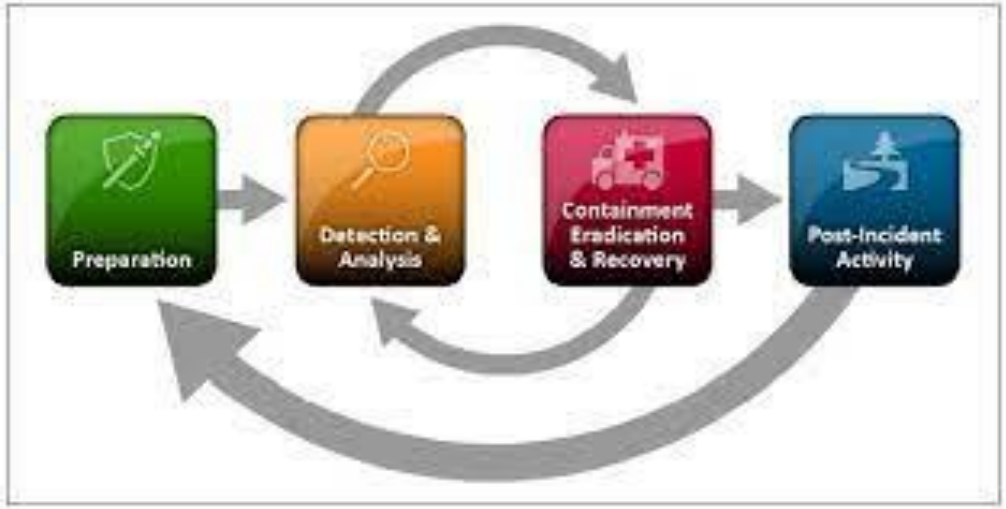


Figure 4 — Information security event and incident flow diagram

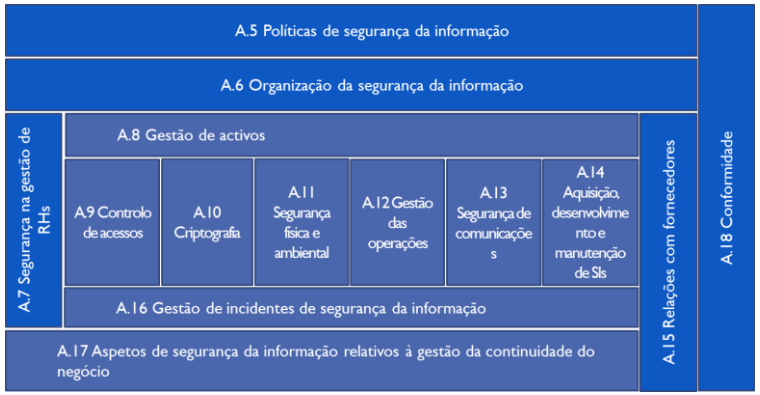
Gestão de incidentes

- Ou ainda (acesso livre)
  - NIST SP 800-61 incident response life cycle phases (https://doi.org/10.6028/NIST.SP.800-61r2)



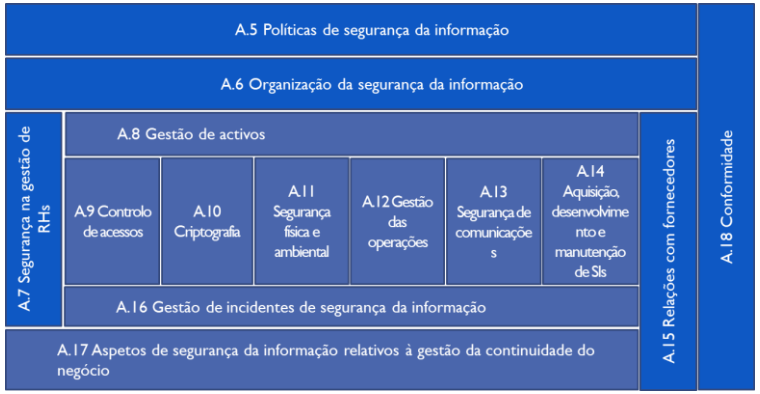
Modelo de segurança integrado

- Continuidade de negócio
  - Inclusão da segurança da informação no processo de gestão da continuidade do negócio
  - Análise de impacto no negócio e identificação de processos críticos
  - Estabelecimento das redundâncias necessárias à continuidade
  - Desenvolvimento e implantação de planos de continuidade, incluindo segurança da informação
  - Testes e exercícios
  - Reavaliação dos planos de continuidade do negócio



Modelo de segurança integrado

- Conformidades
  - Identificação de legislação aplicável
  - Direitos de propriedade intelectual
  - Proteção dos registos organizacionais
  - Proteção dos dados e privacidade de informação pessoal
  - Prevenção da utilização indevida das infraestruturas de processamento da informação
  - Conformidade com políticas e normas de segurança
  - Verificação da conformidade técnica
  - Controlos de auditoria a sistemas de informação



Modelo de segurança integrado

- Utilização da ISO 27002, define as melhores práticas para a gestão de segurança da informação
  - "Sem uma gestão formal da segurança da informação, a segurança será quebrada algures no tempo."
  - A segurança da informação é um processo de gestão, não um processo tecnológico.

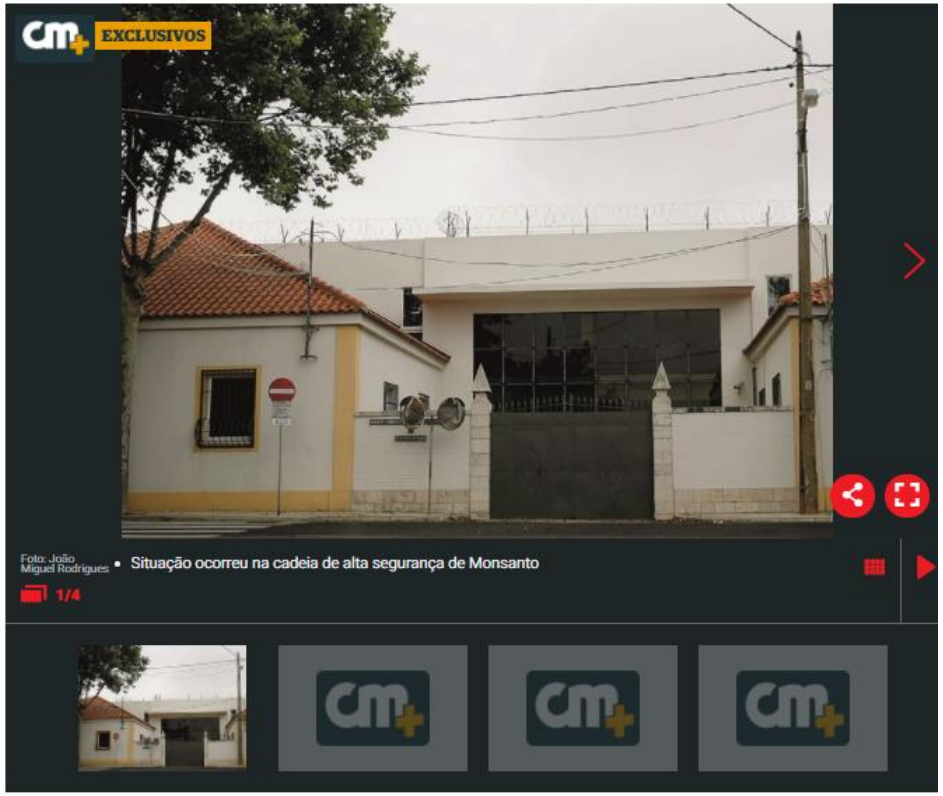
Exemplos de ameaças

- Coloquem-se no lugar do Responsável de Segurança da Prisão
  - O que falhou?
  - Ameaça?
  - Vulnerabilidades?
  - Que controlos implementarias?

Entra em prisão de alta segurança com emails

Mulher mostra alegada troca de correspondência com diretora-adjunta do estabelecimento prisional e consegue visitar um dos 21 refugiados marroquinos ali retidos.

Miguel Curado | 11 de Outubro de 2020 às 01:30



EXCLUSIVOS precisou apenas de mostrar alguns emails que disse ter trocado com a diretora-adjunta da cadeia de alta segurança de Monsanto, em Lisboa, para conseguir entrar na mesma e visitar um dos 21 refugiados marroquinos que ali se encontram há várias semanas, à espera de decisão do respetivo processo de extradição.

Exemplos de ameaças

- Coloquem-se no lugar do Responsável de Segurança da Elétrica
  - O que falhou?
  - Ameaça?
  - Vulnerabilidades?
  - Que controlos implementarias?

Como a energia elétrica se tornou o novo campo de batalha entre EUA e Rússia

Lioman Lima - @liomanlima
BBC News Mundo

19 junho 2019

Redes elétricas e outras estruturas vitais estão na mira das tensões entre a Rússia e os Estados Unidos

Em 23 de dezembro de 2015, uma parte da Ucrânia ficou às escuras.

Foi uma noite dentro da noite: ninguém sabia ao certo o que tinha acontecido.

As usinas não haviam registrado nenhuma falha, os geradores funcionavam normalmente, tudo parecia correr dentro dos parâmetros.

Até que cerca de 700 mil pessoas ficaram sem eletricidade.

Exercício de Grupo

- Conduzir uma Avaliação dos Riscos

Segurança e Gestão de Risco

2ºSem 2023/24

Information Security

and Applicable Standards

LUIS AMORIM

16 Mar 2024