

Segurança e Gestão de Risco

2ºSem 2023/24

Revisões

LUIS AMORIM

01 Jun 2024

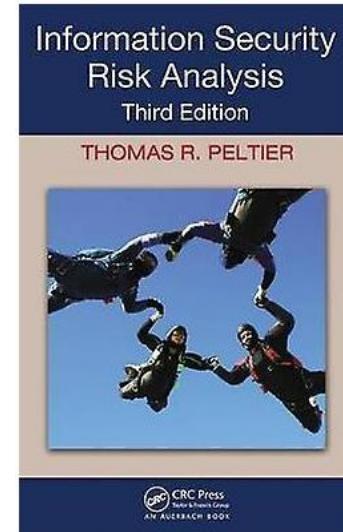
Revisões

Agenda/Objectivos

- Capacidades/Objectivos a adquirir
 - Compreender os princípios subjacentes à segurança nos SI
 - Compreender os conceitos de ameaça, a avaliação dos bens, os activos de informação, segurança física, operacional e da informação e como eles estão relacionados
 - Compreender a análise de risco e gestão de riscos
 - Compreender as abordagens de mitigação técnicas e administrativas
 - Compreender a necessidade de um modelo de segurança global e suas implicações para o gestor de segurança
 - Compreender as tecnologias de segurança
 - Compreender as noções básicas de criptografia, as considerações sobre a sua implementação e a gestão de chaves
 - Aprender a projetar e orientar o desenvolvimento de uma política de segurança na organização
 - Aprender a determinar estratégias adequadas para assegurar confidencialidade, integridade e disponibilidade da informação
 - Aprender a aplicar técnicas de gestão de risco de modo a melhor gerir riscos, reduzir vulnerabilidades, ameaças e aplicar garantias / controlos adequados

Informações sobre a cadeira

- Bibliografia principal:
 - Information Security Risk Analysis, 3rd Edition, Thomas R. Peltier, Auerbach Publications, 2010, ISBN-978-1-4398-3956-0
 - ISO 27001, 27005, 31000
 - NIST



Agenda/Objectivos

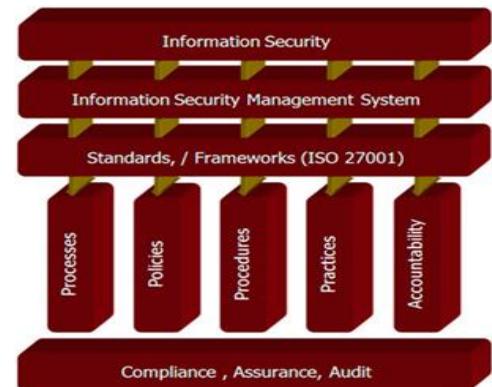
- Capacidades/Objectivos a adquirir
 - **Compreender os princípios subjacentes à segurança nos SI**
 - **Compreender os conceitos de ameaça, a avaliação dos bens, os activos de informação, segurança física, operacional e da informação e como eles estão relacionados**
 - Compreender a análise de risco e gestão de riscos
 - Compreender as abordagens de mitigação técnicas e administrativas
 - Compreender a necessidade de um modelo de segurança global e suas implicações para o gestor de segurança
 - Compreender as tecnologias de segurança
 - Compreender as noções básicas de criptografia, as considerações sobre a sua implementação e a gestão de chaves
 - Aprender a projetar e orientar o desenvolvimento de uma política de segurança na organização
 - Aprender a determinar estratégias adequadas para assegurar confidencialidade, integridade e disponibilidade da informação
 - Aprender a aplicar técnicas de gestão de risco de modo a melhor gerir riscos, reduzir vulnerabilidades, ameaças e aplicar garantias / controlos adequados

Síntese

- **Segurança da Informação**

- Segurança da Informação, mas os Sistemas são a base da Informação
- A informação (conjunto de dados devidamente ordenados) é considerada o activo mais importante nas Organizações
- Importante identificar os activos a “segurar”
- Atenção às várias formas de Informação (Visual, Áudio, Escrita, ..., Electrónica)
- Importante o Controlo de acesso à Informação (âmbito e classificação)
- Os 3 atributos essenciais para a segurança da informação: C-I-A
- A probabilidade de uma ameaça vir a usar uma vulnerabilidade para causar dano resulta num risco para a organização.
- A Segurança da informação deve ser um processo integrado, que abrange toda a organização

- **Abordagem integrada à Segurança**



Exemplificação

- Ameaça: Social Engineering

(<https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402>)

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <https://www.djreprints.com>.

<https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402>

PRO CYBER NEWS

Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case

Scams using artificial intelligence are a new challenge for companies



PHOTO: SIMON DAWSON/BLOOMBERG NEWS

By [Catherine Stupp](#)

Updated Aug. 30, 2019 12:52 pm ET

Criminals used artificial intelligence-based software to impersonate a chief executive's voice and demand a fraudulent transfer of €220,000 (\$243,000) in March in what cybercrime experts described as an unusual case of artificial intelligence being used in hacking.

The CEO of a U.K.-based energy firm thought he was speaking on the phone with his boss, the chief executive of the firm's German parent company, who asked him to send the funds to a Hungarian supplier. The caller said the request was urgent, directing the executive to pay within an hour, according to the company's insurance firm, Euler Hermes Group SA.

Exemplificação

- Ameaça: Social Engeneering

(<https://www.reuters.com/article/us-facc-cyber-arrest-china-idUSKCN1110PR>)

AEROSPACE AND DEFENSE AUGUST 26, 2016 / 9:16 AM / UPDATED 6 YEARS AGO

Chinese man arrested in Hong Kong over FACC cyber attack in Austria

By Reuters Staff

3 MIN READ



VIENNA (Reuters) - A Chinese citizen has been arrested in Hong Kong in connection with a cyber attack that cost Austrian aerospace parts maker FACC 42 million euros (\$47.39 million), Austrian police said on Friday.

FACC fired its chief executive and chief financial officer after the attack, which involved hoax emails asking an employee to transfer money for a fake acquisition project - a kind of scam known as a "fake president incident". FACC's customers include Airbus and Boeing.

A 32-year-old man, who was an authorized signatory of a Hong Kong-based firm that received around 4 million euros from FACC, was arrested on July 1 on suspicion of money laundering, a spokesman for Austria's Federal Office for Crime said.

Such attacks, also known as "business email compromise", involve thieves gaining access to legitimate email accounts inside a company – often those of top executives – to carry out unauthorized transfers of funds. The technique, which relies on simple trickery or more sophisticated computer intrusions, typically targets businesses working with international suppliers that regularly perform wire transfers.

A spokesman for FACC said the company was working on getting back 10 million euros which had been found and frozen on accounts in different countries around the world. These 10 million euros are not included in the 42 million euro hit the group has already booked.

In June, the U.S. Federal Bureau of Investigation (FBI) said identified losses from this scam totaled \$3.1 billion and had risen by 1,300 percent in the past 18 months.

Exemplificação

• Ameaça: Phishing

(<https://www.wsj.com/articles/beware-of-qr-code-scams-11647625020?page=1>)



JOURNAL REPORTS: TECHNOLOGY

Beware of QR Code Scams

It's so easy to click on a QR code. Criminals are counting on it.

By Heidi Mitchell

Updated March 19, 2022 8:00 am ET

During the Super Bowl in February, one ad grabbed a lot of attention: a mysterious bouncing QR code that enticed viewers to point their phones at their screens and click through to an unknown website. (Spoiler alert: It was for [Coinbase](#). [COIN -1.83% ▼](#)) Within seconds, more than 20 million people had done just that, crashing the cryptocurrency-exchange platform.

The incident illustrated just how willing people are to click on QR codes, but unfortunately for consumers, marketers aren't the only group that understands this. Two months before, in December, a much darker scenario involving QR codes unfolded when malicious actors placed QR-code stickers on parking meters [in major Texas cities](#), directing drivers to a fraudulent website where they supposedly could pay for parking.

“People were tricked into putting in their credit-card information,” says Eric Chien, security threat researcher at Symantec, part of Broadcom Software’s security technology and response division. “It was a really well-done attack.”

Exemplos

- Ameaça: Roubo de documentos

Expresso

Roubados documentos dos submarinos

Vários documentos foram "cirurgicamente" roubados de um carro ontem em Lisboa.

10:01 | Quarta feira, 3

O contrato entre o Estado e a empresa alemã Ferrostaal sobre as contrapartidas pela venda a Portugal de dois submarinos foi ontem roubado, segundo revela hoje o "Correio da Manhã".

Os documentos foram roubados do carro quando Christoph Mollenbeck, representante da Ferrostaal, jantava com um amigo em Lisboa, perto da Cinemateca.

Segundo o mesmo diário, o Audi A6 foi "cirurgicamente assaltado" e não tinha quaisquer "sinais de arrombamento". Só quando Mollenbeck e o amigo e compatriota Kai Jusec chegaram a casa é que deram pela falta da pasta e do portátil.

Às autoridades, Christoph Mollenbeck disse que as contrapartidas foram ontem renegociadas entre a empresa e o Estado. Do carro também desapareceu o memorando de entendimento entre a Ferrostaal e o Laboratório de Tecnologias de Informação.

O caso está a ser investigado pelo DIAP de Lisboa, liderado por Maria José Morgado.

Exemplificação

- Ameaça: Inundação



(<http://www.youtube.com/watch?v=ttcQy3bCiiU>)

Exemplificação

- Ameaça: Malware

(<http://www.christiantoday.com/article/google.hacked.no.internal.systems.breached.nearly.five.million.gmail.accounts.infected.computers.leaked/4>)

Gmail hacked: Five million accounts from malware-infected computers leaked

Monday, September 15, 2014, 13:58 (BST)



Almost five million usernames and passwords that were [reportedly](#) taken from Google's Gmail accounts had been leaked online last Tuesday on a Russian Bitcoin security forum.

Several data breaches were said to be the main cause of such inconvenient occurrence, and majority of the leaked passwords had been identified as three years old or more.

Despite the hacking incident having leaked mostly outdated information, it has been strongly suggested by security experts that users should update their passwords in a regular manner, especially when data breaches occur.

It has also been recommended that Gmail users should not overlook the two-step authentication process that provides increased information security.

With Google becoming associated with hacking incidents more than a few times in the past months, the company has released a statement regarding the latest hack attack and the security of their users' information.

"The security of our users' information is a top priority for us," a Google spokesperson commented. "We have no evidence that our systems have been compromised, but whenever we become aware that accounts may have been, we take steps to help those users [secure](#) their accounts."

Moreover, Google claimed that the adverse impact of the hacking incident was strongly exaggerated.

Síntese

- Normas e legislação aplicável
 - Standards relacionados com a segurança
 - ISO/IEC 2700x, ISO22301 (Business Continuity), e ISO 15408 (Common Criteria), ISO 18028 (IT network security), ISO 24760 - A Framework for Identity Management
 - Mas também: IT Governance (ITIL, COBIT), Legislação, Regras específicas de sector de negócio, Qualidade, Segurança física



Legislação Consolidada

Lei do Cibercrime

Lei n.º 109/2009 - Diário da República n.º 179/2009, Série I de 2009-09-15

Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa

Lei n.º 109/2009
de 15 de Setembro

Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa.
A Assembleia da República decreta, nos termos da alínea c) do artigo 161.º da Constituição, o seguinte:

Capítulo I
Objecto e definições

Síntese

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

Cap. 0 a 3

- Introdução
- Âmbito
- Referências normativas
- Termos e Definições

Cap. 4 a 10

- Cláusulas 4 a 10
 - Contexto da organização
 - Liderança
 - Planeamento
 - Suporte
 - Operação
 - Avaliação de desempenho
 - Melhoria

Anexos

- Anexos
 - Anexo A (normativo) Objetivos de controlo e controlos
 - Anexo B (informativo) Correspondência entre os termos em inglês e em português

Síntese

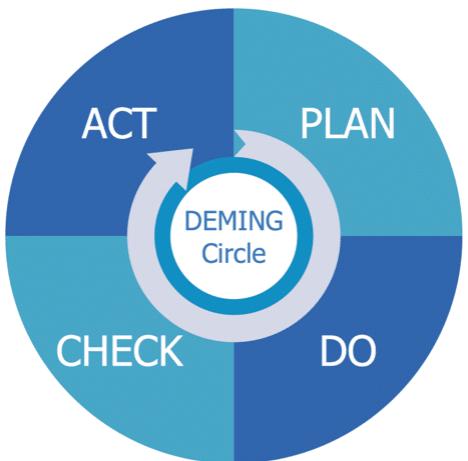
Introdução à ISO 27001:2022

- **Anexo A - Controlos A5 a A8**

- 114 Controlos na versão de 2013 > 93 Controlos em 2022
 - Fusão de 56 controlos, em 24
 - 23 Controlos renomeados
 - 3 Controlos removidos
 - 11 novos controlos
- 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

Síntese

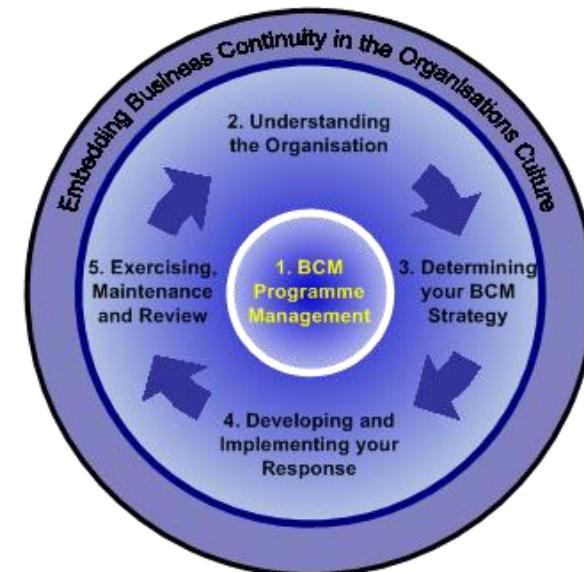
- Modelo PDCA aplicado ao ISMS
 - Plan (establish the ISMS)
 - Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.
 - Do (implement and operate the ISMS)
 - Implement and operate the ISMS policy, controls, processes and procedures.
 - Check (monitor and review the ISMS)
 - Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.
 - Act (maintain and improve the ISMS)
 - Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.



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

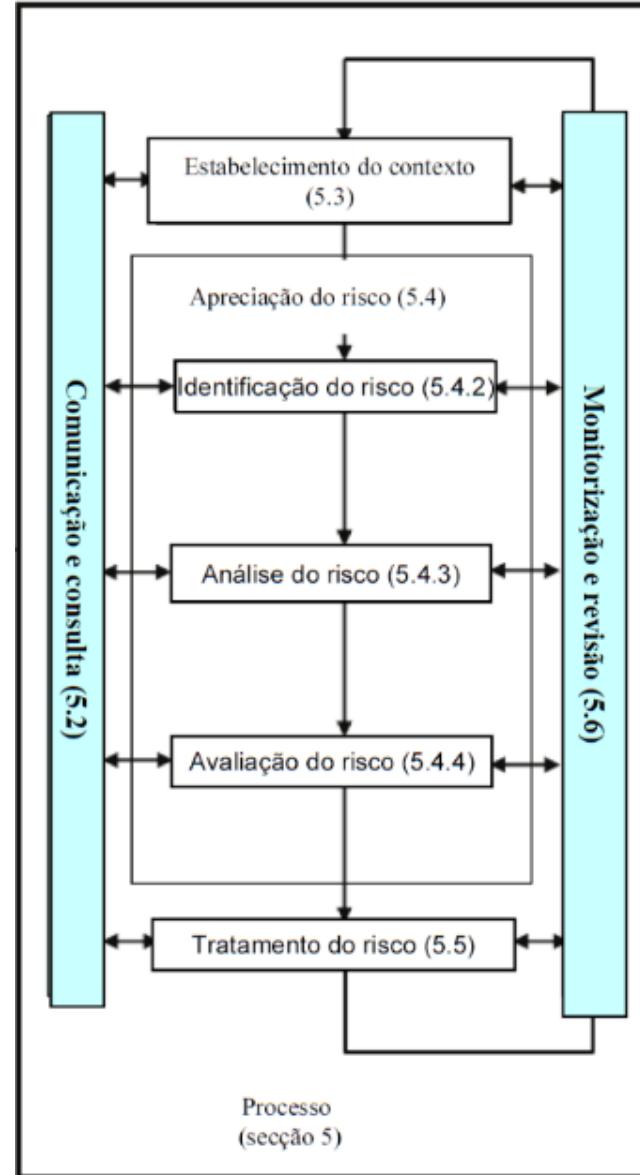


Agenda/Objectivos

- Capacidades/Objectivos a adquirir
 - Compreender os princípios subjacentes à segurança nos SI
 - Compreender os conceitos de ameaça, a avaliação dos bens, os activos de informação, segurança física, operacional e da informação e como eles estão relacionados
 - **Compreender a análise de risco e gestão de riscos**
 - Compreender as abordagens de mitigação técnicas e administrativas
 - Compreender a necessidade de um modelo de segurança global e suas implicações para o gestor de segurança
 - Compreender as tecnologias de segurança
 - Compreender as noções básicas de criptografia, as considerações sobre a sua implementação e a gestão de chaves
 - Aprender a projectar e orientar o desenvolvimento de uma política de segurança na organização
 - Aprender a determinar estratégias adequadas para assegurar confidencialidade, integridade e disponibilidade da informação
 - Aprender a aplicar técnicas de gestão de risco de modo a melhor gerir riscos, reduzir vulnerabilidades, ameaças e aplicar garantias / controlos adequados

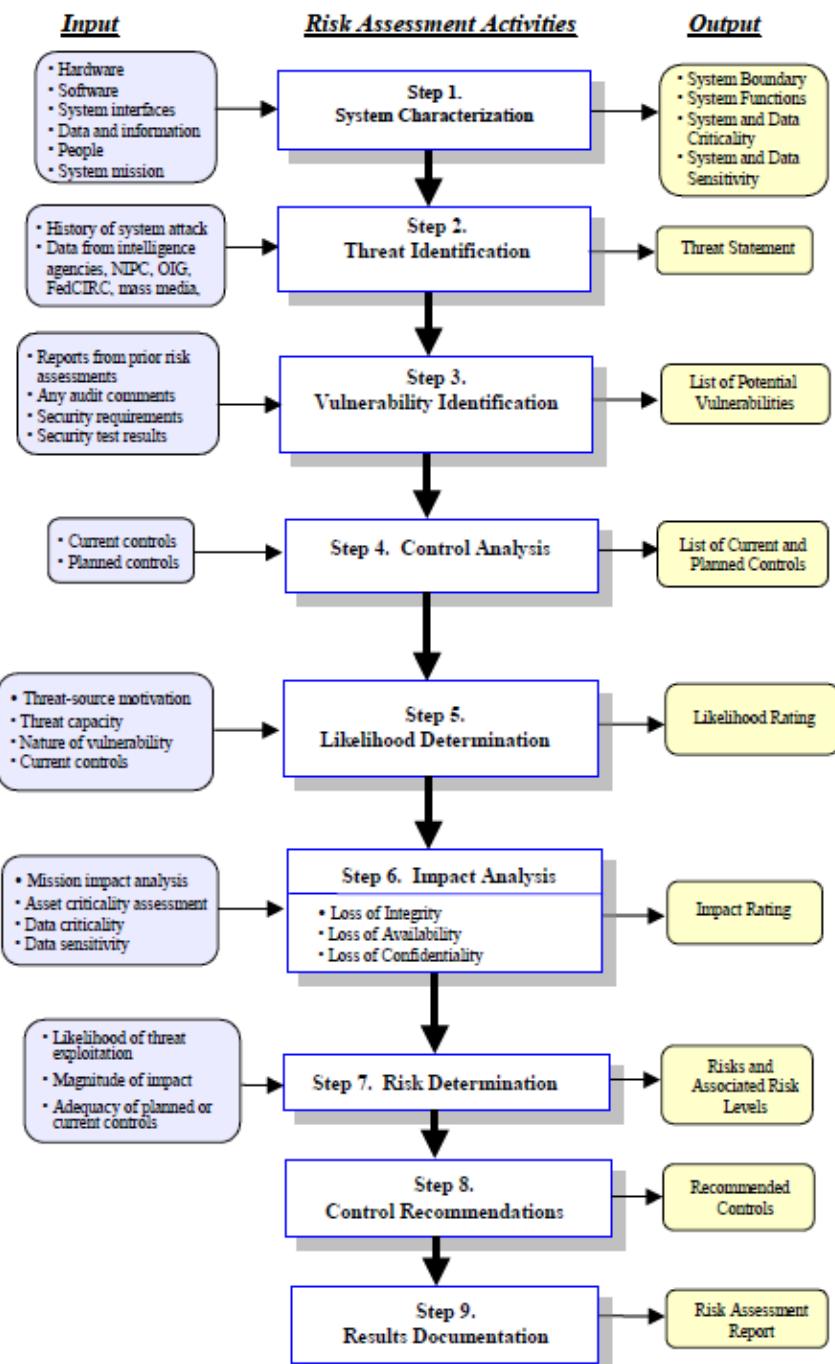
Síntese

- Introdução à Gestão de Risco
 - Risco é a probabilidade de algo mau vir a acontecer e causar danos a um ativo de informação
 - Existem várias formas de calcular o risco, em função da metodologia adotada e do tipo de organização
 - Após cada avaliação dos Riscos, estes devem ser tratados de acordo com o seu valor e as prioridades para o negócio
 - O standard a seguir é a ISO 27005 ou a ISO 31000



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 (projeto Impact Analysis)
 - Etapas da Avaliação de Riscos (NIST)



A Avaliação e gestão dos riscos

- Avaliação de risco

- Existem várias formas de calcular o risco

- Em função da metodologia adoptada
 - No entanto, tem que ser sistemática e repetível

- Alguns exemplos de fórmulas de cálculo de risco:

- Risco = Probabilidade x Consequência x Severidade
 - Risco = Valor_Ativo x Probabilidade x Impacto
 - Risco = Probabilidade x Impacto

- Preferencialmente, devem ser utilizados valores quantitativos (1, 2, 3, 4, 5) em vez de qualitativos (alto, médio, baixo)

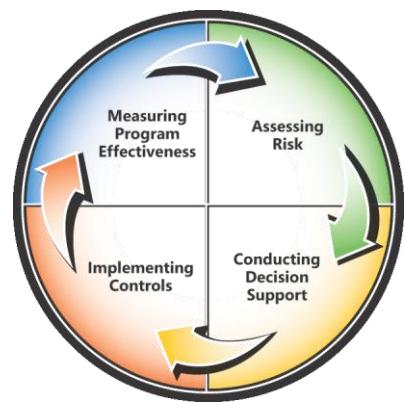
- A ISO27005 refere:

- “Qualitative risk analysis may be used:

- As an initial screening activity to identify risks that require more detailed analysis
 - Where this kind of analysis is appropriate for decisions
 - Where the numerical data or resources are inadequate for a quantitative risk analysis”

Síntese

- Formas de quantificar o Risco
 - Avaliação quantitativa
 - recorrendo a valores numéricos
 - Avaliação quantitativa, recorrendo a valores monetários
 - No seu cálculo pode incluir o valor do ativo
 - Ou 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 risco
 - Utilizando categorias e níveis de risco
 - Permite observar facilmente a priorização dos Riscos
 - Mostrando as áreas de melhoria imediata

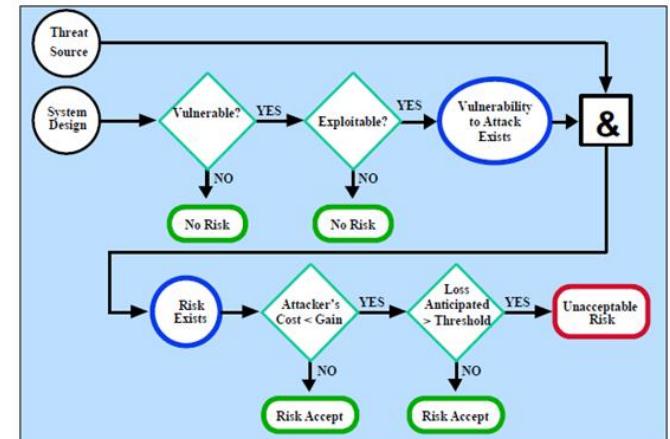
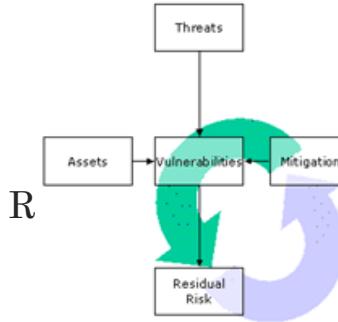


Agenda/Objectivos

- Capacidades/Objectivos a adquirir
 - Compreender os princípios subjacentes à segurança nos SI
 - Compreender os conceitos de ameaça, a avaliação dos bens, os activos de informação, segurança física, operacional e da informação e como eles estão relacionados
 - Compreender a análise de risco e gestão de riscos
 - **Compreender as abordagens de mitigação técnicas e administrativas**
 - **Compreender a necessidade de um modelo de segurança global e suas implicações para o gestor de segurança**
 - Compreender as tecnologias de segurança
 - Compreender as noções básicas de criptografia, as considerações sobre a sua implementação e a gestão de chaves
 - Aprender a projectar e orientar o desenvolvimento de uma política de segurança na organização
 - Aprender a determinar estratégias adequadas para assegurar confidencialidade, integridade e disponibilidade da informação
 - Aprender a aplicar técnicas de gestão de risco de modo a melhor gerir riscos, reduzir vulnerabilidades, ameaças e aplicar garantias / controlos adequados

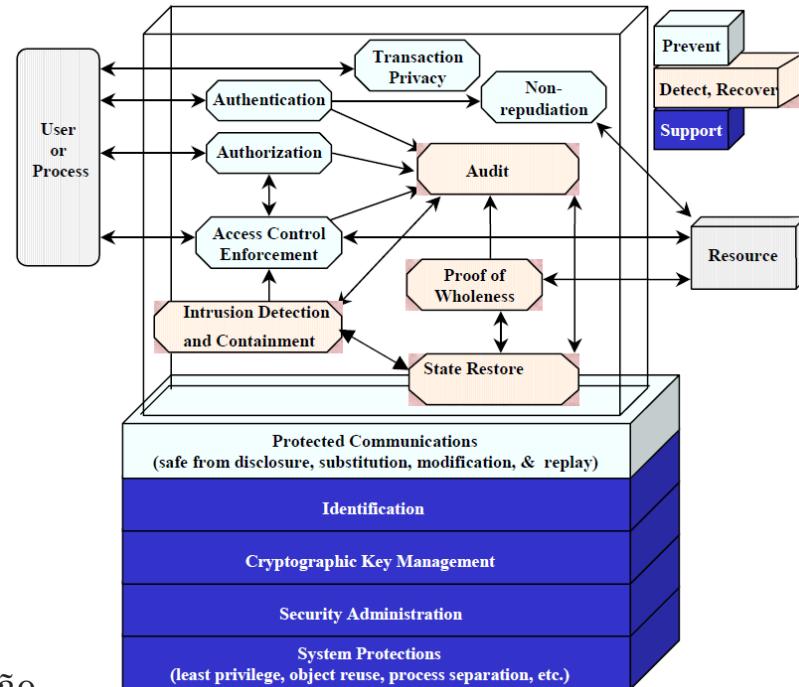
Síntese

- Tratamento dos Riscos
 - Opções de Mitigação de Risco
 - Administrativas
 - Assumir o Risco, Evitar o Risco, Transferência de Risco, Planeamento de Risco
 - Predominantemente técnicas:
 - Limitar o Risco, Reconhecimento e Desenvolvimento de controlos
 - Fluxo de aceitação de riscos Ou não aceitação e implementação de controlos
 - Análise de opções de mitigação utilizando o Risk Mitigation Checklist (estraído do NIST)
 - Passos para a implementação de controlos
 - Ter em atenção que a implementação de controlos pode gerar novas vulnerabilidades



Síntese

- Controlos de segurança
 - Tecnológicos
 - de Suporte
 - Preventivos
 - Para detecção e recuperação
 - Não tecnológicos:
 - Controlos de Gestão e Organizacionais
 - definição de políticas e normas de protecção da informação
 - definem como os elementos da organização devem actuar
 - Controlos Operacionais
 - controlos e linhas orientadoras que assegurem procedimentos seguros
 - considerando as políticas e normas definidas na gestão



Síntese

- **Modelo de segurança integrado**
 - A Segurança da Informação só se consegue atingir considerando de forma integrada os sistemas e processos da organização
 - A abordagem integrada da segurança pode seguir as melhores práticas para a gestão de segurança da informação descritas na ISO 27002
 - Política de segurança
 - Organização da Segurança
 - Recursos Humanos
 - Segurança física e ambiental
 - Gestão de operações e comunicações
 - Controlo de acessos à informação
 - Aquisição, desenvolvimento e manutenção de sistemas de informação
 - Gestão de incidentes de segurança da informação
 - Continuidade de negócio
 - Conformidades
 - A segurança da informação é um processo de gestão, não um processo tecnológico
- Controlos de segurança

A.7 Segurança na gestão de RHs	A.8 Gestão de activos						A.15 Relações com fornecedores	
	A.9 Controlo de acessos	A.10 Criptografia	A.11 Segurança física e ambiental	A.12 Gestão das operações e comunicações	A.13 Segurança de comunicações	A.14 Aquisição, desenvolvimento e manutenção de SIs		
A.16 Gestão de incidentes de segurança da informação						A.17 Aspetos de segurança da informação relativos à gestão da continuidade do negócio		
A.18 Conformidade								

Síntese

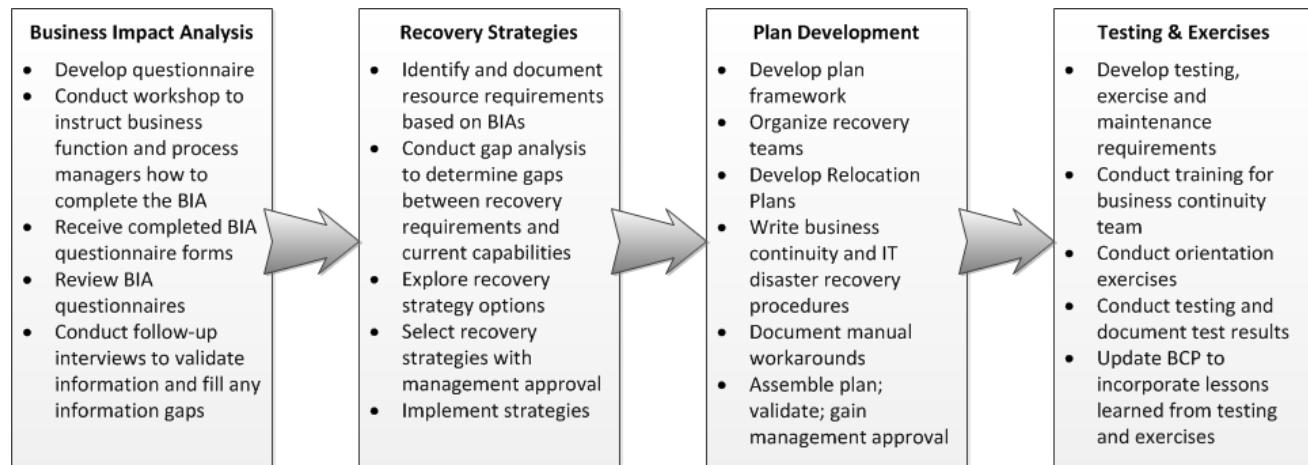
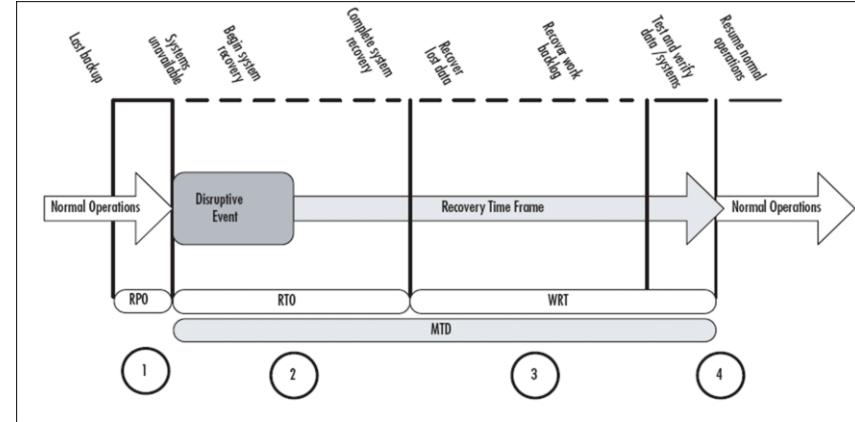
- Business Impact Analysis (BIA)

- Um processo de Business Impact Analysis pretende determinar os impactos que um incidente disruptivo tem na operação e na viabilidade dos processos core de negócio
- Implica antes
 - Determinar os processos core
 - Determinar quais são os principais recursos utilizados por esses processos
 - Aplicações; Sistemas; Processos; Funções; Pessoas
- Depois
 - Classificar esses recursos (em termos de importância e prioridade)
 - Caracterizar os requisitos de recuperação

Síntese

- Business Impact Analysis (BIA)

- Caracterizar os requisitos de recuperação
 - R P O = Recovery Point Objective R T O = Recovery Time Objective
 - W R T = Work Recovery Time
 - M T D = Maximum Tolerable Downtime
- Aplicar os resultados do BIA
 - Para estabelecer estratégias de recuperação



Síntese

- GAP Analysis

- GAP Analysis consiste na comparação entre o estado presente e o estado desejado (futuro)

- Para tal é preciso resposta para:
 - Qual o estado pretendido
 - Ou estado “compliant”,
 - quando numa auditoria/certificação
 - Qual o estado actual
 - O que é preciso ser feito

1 SCOPE		Comments
This international standard establishes guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organization.		
2 TERMS DEFINITIONS		
For better understanding, ISO 27002 identifies and defines key information security terms.		
3 STRUCTURE OF THIS STANDARD		
This standard contains eleven (11) chapters containing 38 control areas.		
4 RISK ASSESSMENT AND TREATMENT		
The information security risk assessment should have a clearly defined scope.		
5 SECURITY POLICY		
Note: ISO17799 Sections 1, 2 and 3 are non-action items, and are not included as checklist items.		
5.1 Information Security Policy	Management direction and support for information security must be clearly established.	
5.1.1 Information Security Policy Document	Has an information security policy been approved by management? <input type="checkbox"/> Y _____ <input type="checkbox"/> N _____	
	Has an information security policy been implemented? <input type="checkbox"/> Y _____ <input type="checkbox"/> N _____	
	Has an information security policy been communicated to all employees? <input type="checkbox"/> Y _____ <input type="checkbox"/> N _____	
5.1.2 Review of the Information Security Policy	Has the Information Security Policy been assigned an Owner? <input type="checkbox"/> Y _____ <input type="checkbox"/> N _____	
	Has a policy review process been established? <input type="checkbox"/> Y _____ <input type="checkbox"/> N _____	

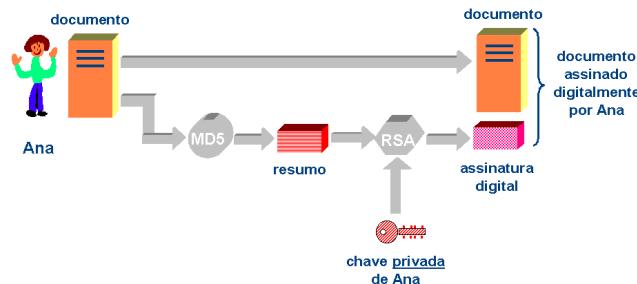
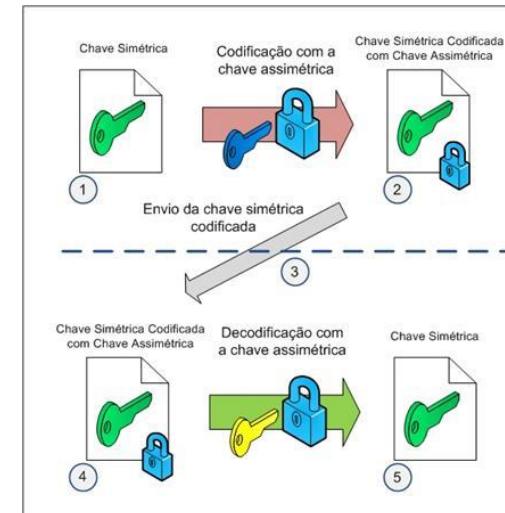
Agenda/Objectivos

- Capacidades/Objectivos a adquirir
 - Compreender os princípios subjacentes à segurança nos SI
 - Compreender os conceitos de ameaça, a avaliação dos bens, os activos de informação, segurança física, operacional e da informação e como eles estão relacionados
 - Compreender a análise de risco e gestão de riscos
 - Compreender as abordagens de mitigação técnicas e administrativas
 - Compreender a necessidade de um modelo de segurança global e suas implicações para o gestor de segurança
 - Compreender as tecnologias de segurança**
 - Compreender as noções básicas de criptografia, as considerações sobre a sua implementação e a gestão de chaves**
 - Aprender a projectar e orientar o desenvolvimento de uma política de segurança na organização
 - Aprender a determinar estratégias adequadas para assegurar confidencialidade, integridade e disponibilidade da informação
 - Aprender a aplicar técnicas de gestão de risco de modo a melhor gerir riscos, reduzir vulnerabilidades, ameaças e aplicar garantias / controlos adequados

Síntese

- Noções de criptografia

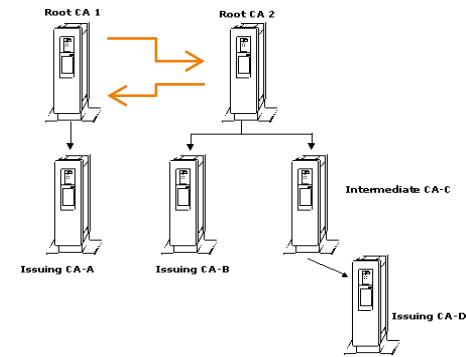
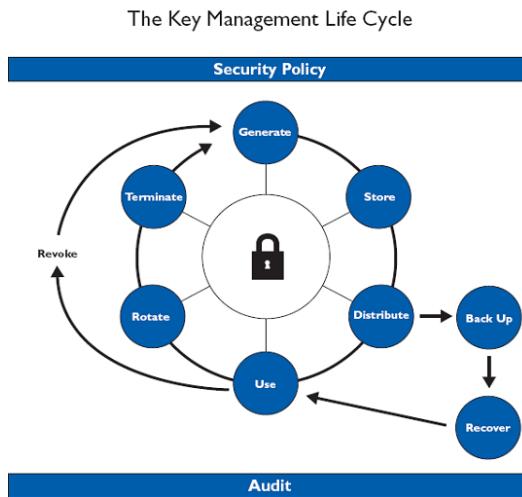
- Processos básicos de criptografia (Cifra e Decifra)
- Sistemas criptográficos simétricos
 - processamento mais rápido
- Sistemas criptográficos assimétricos
 - mais lento, mas mais seguro
- PKI – Public Key Infrastructure
- A Assinatura Digital



Síntese

- Noções de criptografia

- Gestão de chaves
 - técnicas e procedimentos relacionados com o ciclo de vida das chaves criptográficas
- Relações de confiança entre CAs



Agenda/Objectivos

- Capacidades/Objectivos a adquirir
 - Compreender os princípios subjacentes à segurança nos SI
 - Compreender os conceitos de ameaça, a avaliação dos bens, os activos de informação, segurança física, operacional e da informação e como eles estão relacionados
 - Compreender a análise de risco e gestão de riscos
 - Compreender as abordagens de mitigação técnicas e administrativas
 - Compreender a necessidade de um modelo de segurança global e suas implicações para o gestor de segurança
 - Compreender as tecnologias de segurança
 - Compreender as noções básicas de criptografia, as considerações sobre a sua implementação e a gestão de chaves
 - **Aprender a projectar e orientar o desenvolvimento de uma política de segurança na organização**
 - Aprender a determinar estratégias adequadas para assegurar confidencialidade, integridade e disponibilidade da informação
 - Aprender a aplicar técnicas de gestão de risco de modo a melhor gerir riscos, reduzir vulnerabilidades, ameaças e aplicar garantias / controlos adequados

Síntese

- Desenvolvimento da Política de Segurança
 - Organização
 - A Política de Segurança deverá ser desdobrada em documentos auxiliares que apresentam princípios e orientações mais específicas e dirigidas a grupos de funcionários ou a funções determinadas (por exemplo, orientações sobre reportar incidentes de segurança deverão ser dirigidas a todos os funcionários, políticas específicas relativamente à administração de sistemas destinam-se apenas aos técnicos da Informática).
 - Exemplos de Políticas
 - Política de Classificação de Informação
 - Política de Uso aceitável
 - Política de Controlo de Acessos
 - Política de Backups
 - Política de Teletrabalho e de Acesso Remoto
 - Política de controlos criptográficos
 - Política de Fornecedores



Síntese

- Exemplo de
Política de Backups

1. Política de Backup

1. Realização dos backups

Para salvaguardar a informação contida no servidor e respetivos projetos, existe uma política de backups definida, que passa por realizar backup a todas as máquinas virtuais onde estão inseridos todos os dados relativos aos projetos. Desta forma, garante-se que quando da necessidade de aceder a um dos backups todos os dados estão com o formato desejado.

Assim, são realizados backups incrementais

Para salvaguardar a informação relativa aos projetos de desenvolvimento seguro e do Sistema de Gestão de Segurança da Informação, deverão ser realizados os seguintes backups:

- Backup ao servidor principal onde é executado o ambiente de virtualização;
- Backup de cada uma das máquinas virtuais (projetos) existentes no ambiente de virtualização;

Cada um dos backups anteriores deve ser realizado de acordo com o seguinte ciclo:

- Full Backups todas as 2as feiras;
- Backups incrementais entre 3^a e 6^a feira

Estes backups devem ser realizados no final do dia de trabalho, ao final do dia.

Caso se verifique um erro na realização de uma tarefa de backup, este deve ser analisado pelo Gestor de Projeto e decidida qual a melhor forma de o realizar, nomeadamente na próxima pausa, por exemplo hora de almoço.

Síntese

- Exemplo de
Procedimento de Backups

1. Procedimento de Backups

A realização dos backups será executada através da ferramenta “*BackUp Maker*”, que deve estar configurada de forma a satisfazer a política de realização de backups.

É responsabilidade da Equipa de Operação IT garantir a sua realização, através da configuração e monitorização da ferramenta.

1.1. Validação dos Backups

De modo a validar-se a execução dos backups deve-se aceder ao servidor e validar-se através do relatório da aplicação “*BackUp Maker*” se os backups foram realizados com sucesso.

Caso os mesmos tenham sido realizados com sucesso deve-se continuar a execução das tarefas conforme o previsto. Em caso de erro deve-se tentar executar os mesmos de forma manual e verificar se o problema volta a ocorrer. Se o erro voltar a acontecer, deve-se proceder à reconfiguração dos backups de modo a garantir o normal funcionamento dos mesmos.

O diagrama seguinte ilustra o que foi descrito nos parágrafos anteriores.

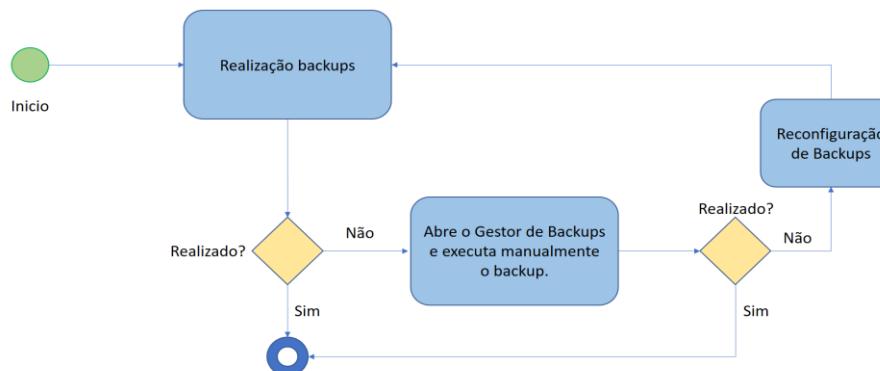


Figura 1 - Workflow de validação dos Backups

Agenda/Objectivos

- Capacidades/Objectivos a adquirir
 - Compreender os princípios subjacentes à segurança nos SI
 - Compreender os conceitos de ameaça, a avaliação dos bens, os activos de informação, segurança física, operacional e da informação e como eles estão relacionados
 - Compreender a análise de risco e gestão de riscos
 - Compreender as abordagens de mitigação técnicas e administrativas
 - Compreender a necessidade de um modelo de segurança global e suas implicações para o gestor de segurança
 - Compreender as tecnologias de segurança
 - Compreender as noções básicas de criptografia, as considerações sobre a sua implementação e a gestão de chaves
 - Aprender a projectar e orientar o desenvolvimento de uma política de segurança na organização
 - Aprender a determinar estratégias adequadas para assegurar confidencialidade, integridade e disponibilidade da informação**
 - Aprender a aplicar técnicas de gestão de risco de modo a melhor gerir riscos, reduzir vulnerabilidades, ameaças e aplicar garantias / controlos adequados

Síntese

- A Cibersegurança – ISO/IEC 27032
 - Cybercrime - criminal activity where services or applications in the Cyberspace are used for or are the target of a crime, or where the Cyberspace is the source, tool, target, or place of a crime
 - Cybersafety - condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or other types or consequences of failure, damage, error, accidents, harm or any other event in the Cyberspace which could be considered non-desirable
 - Cybersecurity = Cyberspace security - preservation of confidentiality, integrity and availability of information in the Cyberspace
 - Cyberspace - complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form

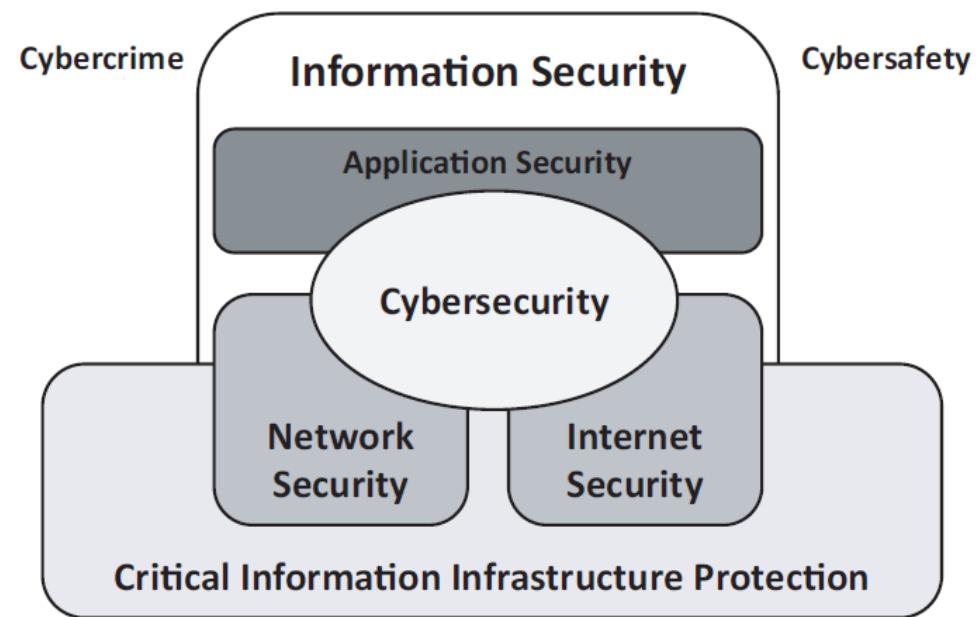


Figure 1 — Relationship between Cybersecurity and other security domains

Privacidade

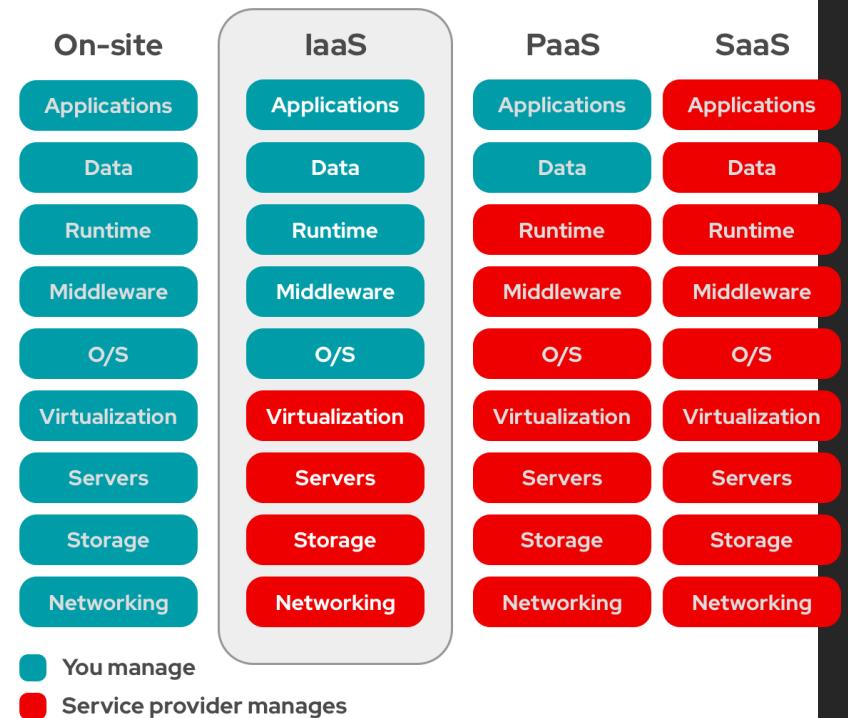
- Definidos requisitos em
 - Regulamento Geral de Proteção de Dados
 - Lei n.º 58/2019 - Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados
 - ISO/IEC 27701 - Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
 - PII - personally identifiable information

Segurança de serviços na cloud

- Segurança de serviços na cloud
 - ISO/IEC 27017 - Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
 - 3.1.4 **cloud computing** - paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with on-demand self-service provisioning and administration
 - NOTE – Examples or resources include servers, operating systems, networking, software, and storage equipment
 - 3.1.5 **cloud service** - one or more capabilities (3.1.2) offered via cloud computing (3.1.4) invoked using a declared interface
 - 3.1.6 **cloud service category** - group of cloud services (3.1.5) that possess some qualities in common with each other
 - 3.1.7 **cloud service customer** - party (3.1.13) which is in a business relationship for the purpose of using cloud services (3.1.5)
 - 3.1.8 **cloud service provider** - party (3.1.13) which makes cloud services (3.1.5) available
 - 3.1.9 **cloud service user** - person associated with a cloud service customer (3.1.7) that uses cloud services (3.1.5)

Segurança de serviços na cloud

- Definições
 - 3.1.10 IaaS (Infrastructure as a Service)** - cloud service category (3.1.6) in which the cloud capabilities type (3.1.3) provided to the cloud service customer (3.1.7) is an infrastructure capabilities type (3.1.11)
 - 3.1.12 PaaS (Platform as a Service)** - cloud service category (3.1.6) in which the cloud capabilities type (3.1.3) provided to the cloud service customer (3.1.7) is a platform capabilities type (3.1.14)
 - 3.1.15 SaaS (Software as a Service)** - cloud service category (3.1.6) in which the cloud capabilities type (3.1.3) provided to the cloud service customer (3.1.7) is an application capabilities type (3.1.1)



Segurança de serviços na cloud

- Interpretação da norma
 - Para determinados controlos do Anexo A da ISO 27001

A.6.1.3	Contact with authorities	<i>Control</i> Appropriate contacts with relevant authorities shall be maintained.
---------	--------------------------	---

- Apresenta requisitos acrescidos, na ótica do
 - cloud service customer
 - cloud service provider

6.1.3 Contact with authorities

Control 6.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

Implementation guidance for cloud services

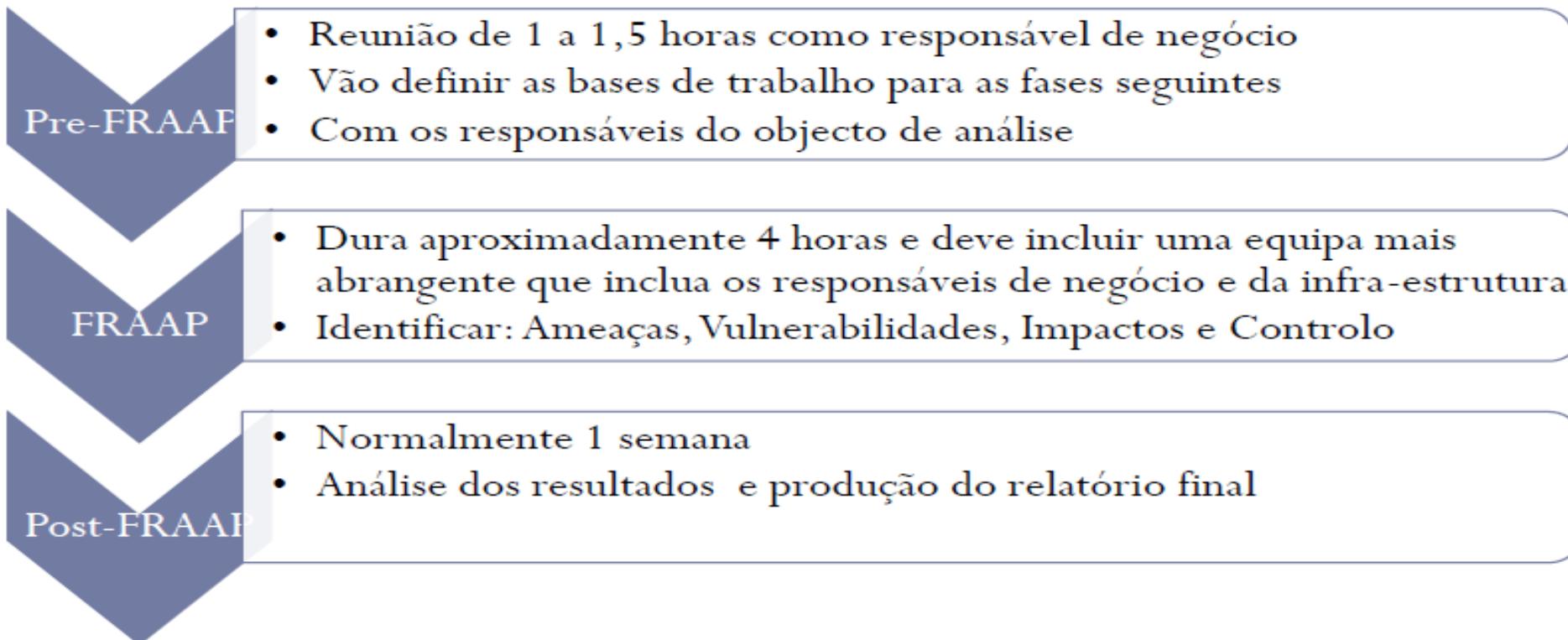
Cloud service customer	Cloud service provider
The cloud service customer should identify the authorities relevant to the combined operation of the cloud service customer and the cloud service provider.	The cloud service provider should inform the cloud service customer of the geographical locations of the cloud service provider's organization and the countries where the cloud service provider can store the cloud service customer data.

Agenda/Objectivos

- Capacidades/Objectivos a adquirir
 - Compreender os princípios subjacentes à segurança nos SI
 - Compreender os conceitos de ameaça, a avaliação dos bens, os activos de informação, segurança física, operacional e da informação e como eles estão relacionados
 - Compreender a análise de risco e gestão de riscos
 - Compreender as abordagens de mitigação técnicas e administrativas
 - Compreender a necessidade de um modelo de segurança global e suas implicações para o gestor de segurança
 - Compreender as tecnologias de segurança
 - Compreender as noções básicas de criptografia, as considerações sobre a sua implementação e a gestão de chaves
 - Aprender a projectar e orientar o desenvolvimento de uma política de segurança na organização
 - Aprender a determinar estratégias adequadas para assegurar confidencialidade, integridade e disponibilidade da informação
 - **Aprender a aplicar técnicas de gestão de risco de modo a melhor gerir riscos, reduzir vulnerabilidades, ameaças e aplicar garantias / controlos adequados**

Síntese

- Facilitated Risk Analysis and Assessment Process
 - Este processo envolve a análise de 1 sistema processo, plataforma, processo de negócio definido de cada vez



Síntese

- Pre-FRAAP
 - Resultados esperados
 - Pré-triagem dos resultados esperados
 - Definição do âmbito
 - Diagrama com a descrição/detalhe do sistema ou processo a avaliar
 - Identificação dos intervenientes/equipa a incluir no processo
 - Requisitos para a reunião FRAAP (planeamento, sala, materiais)
 - Acordar definições de princípio
 - Mini-Brainstorming (identificar ameaças para introdução na reunião FRAAP)

ISSUE	PRIOR TO THE MEETING	DURING THE MEETING
1. Date of Pre-FRAAP Meeting <i>Record when and where the meeting is scheduled</i>		
2. Project Executive Sponsor or Owner <i>Identify the owner or sponsor who has executive responsibility for the project</i>		
3. Project Leader <i>Identify the individual who is the primary point of contact for the project or asset under review</i>		
4. Pre-FRAAP Meeting Objective <i>Identify what you hope to gain from the meeting – typically the seven deliverables will be discussed</i>		
5. Project Overview <i>Prepare a project overview for presentation to the pre-FRAAP members during the meeting</i>		<ul style="list-style-type: none"> • Applications/Systems • Business Processes • Business Functions • People and Organizations • Locations/Facilities
6. Assumptions <i>Identify assumptions used in developing the approach to performing the FRAAP project</i>		
7. Pre-screening Results <i>Record the results of the pre-screening process</i>		
	8. Business Strategy, Goals and Objectives <i>Identify what the owner's objectives are and how they relate to larger company objectives</i>	
	9. Project Scope <i>Define specifically the scope of the project and document it during the meeting so that all participating will know and agree</i>	
	10. Time Dependencies <i>Identify time limitations and considerations the client may have</i>	
	11. Risks/Constraints <i>Identify risks and/or constraints that could affect the successful conclusion of the project</i>	
	12. Budget <i>Identify any open budget/funding issues</i>	
	13. FRAAP Participants <i>Identify by name and position the individuals whose participation in the FRAAP session is required</i>	
	14. Administrative Requirements <i>Identify facility and/or equipment needs to perform the FRAAP session</i>	
	15. Documentation <i>Identify what documentation is required to prepare for the FRAAP session (provide the FRAAP Document Checklist)</i>	

Síntese

- FRAAP
 - Não deve durar mais que quatro horas
 - Envolver os elementos da equipa que
 - Deve ter a seguinte agenda
 - Introdução, preparada no Pre-FRAAP
 - Identificação de Ameaças e Vulnerabilidades
 - Identificação Controlos Existentes
 - Avaliar os níveis de risco (inerentes)
 - Identificar Riscos Residuais
 - Apresentação do Sumário da Reunião
 - Resultados esperados
 - Identificação das Ameaças
 - Identificação das Vulnerabilidades
 - Identificação dos Controlos Existentes
 - Caracterização dos Riscos Residuais



Sessão FRAAP

- Agenda

FRAP Session Agenda	Responsibility
• Introduction	
• Explain the FRAP process and cover definitions	• Owner + Facilitator
• Review scope statement	• Owner
• Review Visual Diagram	• Technical support
• Discuss definitions	• Facilitator
• Review Objectives <ul style="list-style-type: none"> • Identify Threats • Establish Risk Levels • Identify possible safeguards 	
• Identify roles and introduction	• Team
• Review session agreements	
• Brainstorm for threats	• Team
• Establish risk levels (probability and impact)	• Team
• Prioritize threats	• Team
• Identify possible safeguards	• Team
• Create Management Summary Report	• Facilitator

Sessão FRAAP

- Estabelecimento do nível de risco

Definição de níveis e matriz de avaliação de risco

Avaliação das ameaças com os controlos já implementados

Identificar novos controlos para Riscos maiores

Avaliar novo nível de risco

Priorizar e planear implementação de controlos

Sessão FRAAP

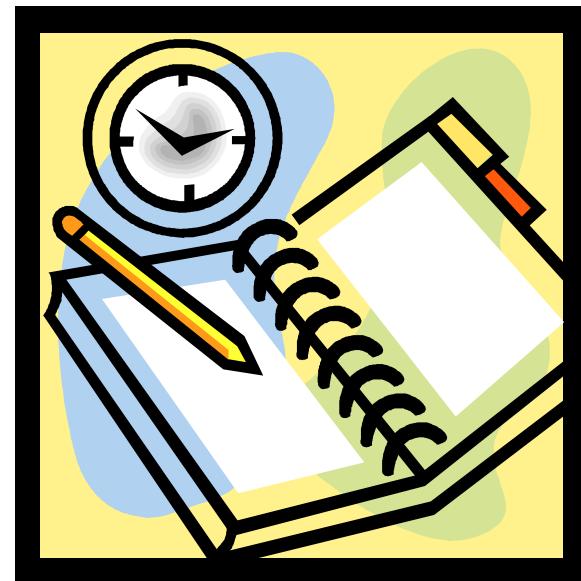


- Estabelecimento do nível de risco
 - Caracterizar novos níveis de risco

<i>Threat</i>	<i>Existing Control</i>	<i>Probability</i> 1 = Low 2 = Medium 3 = High	<i>Impact</i> 1 = Low 2 = Medium 3 = High	<i>Risk Level</i>	<i>New or Enhanced Selected Control</i>	<i>New Risk Level</i>
Confidentiality						
Insecure e-mail could contain confidential information		3	3	High	Information classification policy and handling standards are being implemented	Medium
Internal theft of information	Employee code of conduct and conflicts of interest addresses proprietary rights of the company and sanctions to be taken for breaches	1	2	Low		
Employee is not able to verify the identity of a client (e.g., phone masquerading)		1	1	Low		

Sessão FRAAP

- Estabelecimento do nível de risco
 - Prioritizar implementação de controlos
 - Planear essa implementação



Síntese

- Post-FRAAP
 - Realizado pela equipa de consultores (alunos)
 - Análise dos resultados da reunião
 - Pode ser necessário contactar alguns elementos da equipa
 - Através do gestor de projecto
 - Para algum esclarecimento adicional
 - Ou informação complementar
 - Resultados esperados
 - Relatório final
 - com sumário executivo
 - Resumo da reunião de equipa
 - Identificação de controlos complementares
 - Análise do processo
 - Apresentação das conclusões ao Gestor de Negócio



Trabalhos de Grupo

- Os Trabalhos são: (AR - Análise de riscos, AV - Análise de vulnerabilidades)
- Grupos constituídos
 - Grupo A – TICE (AV)
 - Ana Raquel Paradinha - 102491
 - João Miguel Matos – 103341
 - Diogo Almeida
 - Fábio Ferreira
 - Grupo B – *Inw* (AR)
 - Bruna Simões - 103453
 - Daniel Ferreira - 102442
 - Tiago Carvalho – 104142
 - Grupo C – *MetaTissue* (AR)
 - José João Alexandre - 118373
 - Rafael Oliveira – 117240
 - Gonçalo Marques
 - Grupo D – *Service Desk* (AR)
 - Ana Vidal
 - Simão Andrade
 - Wilmara Francisco
- Grupos constituídos
 - Grupo E – Scubic (AR)
 - Filipe Silveira
 - Ricardo Covelo
 - Telmo Sauce
 - Grupo G – TICE (AR)
 - Diogo Silveira – 85117
 - Filipe Antão - 103470
 - Paulo Pinto - 103234
 - Grupo H – *Scotty* (AR)
 - Diogo Maia - 111707
 - Francisco Cunha - 114661
 - Luis Peixoto - 115447



Trabalhos de Grupo

- Plano – Avaliação dos Riscos
 - pré-FRAAP
 - A realizar entre 27 e 31 de Maio
 - Acertar data da sessão de FRAAP
 - Enviar relatório até dia 01 de Junho
 - Reuniões FRAAP
 - Entre 03 e 11 de Jun
 - Relatório de FRAAP
 - Descrição e conclusões da avaliação
 - Com Sumário Executivo
 - Enviar até dia 15 de Junho
 - Apresentação das conclusões
 - Colocar em slide as principais conclusões
 - extrair do Sumário Executivo
 - Data de apresentação: dia **17 de Junho**– a confirmar
- Plano - Vulnerability scanner
 - Preparação
 - Assistir à sessão relativa ao mesmo sistema
 - Correr ferramentas
 - Combinar com cliente (feriado ou fds)
 - Até 10 de Junho
 - Descrição e conclusões da avaliação
 - Com Sumário Executivo
 - Relatório até 15 de Junho
 - Alinhado com relatório FRAAP
 - Apresentação das conclusões
 - Colocar em slide as principais conclusões
 - extrair do Sumário Executivo
 - Data de apresentação: dia **17 de Junho**– a confirmar

Trabalhos de Grupo

- Avaliação
 - Fase Inicial (20%)
 - Condução da reunião + documento com conclusões da sessão inicial (Pre-Fraap ou ferramentas)
 - Realização da Atividade (30%)
 - Reunião FRAAP
 - Ferramentas utilizadas
 - Relatório Final (40%)
 - Apresentação dos resultados (10%)
 - 3 a 4 slides com resumo do relatório

Post-FRAAP - Relatório

- Capa
- Índice
- Sumário Executivo
- Metodologia
 - Explicação da metodologia
 - *Como correu o processo*
- Avaliação de Risco
 - Ameaças
 - Vulnerabilidades
 - Controlos a implementar
- Planeamento/priorização
- Conclusões

Post-FRAAP

- Sumário executivo (composição)
 - Lista de participantes no processo
 - Resumo do âmbito e princípios estabelecidos
 - 2 ou 3 parágrafos com um resumo de como decorreu o processo
 - Onde e quando decorreu
 - Identificar constrangimentos e factos assumidos
 - Resumo da metodologia
 - Resumo das principais conclusões da avaliação
 - Maiores riscos e controlos
 - Referenciação à restante documentação
 - Conclusões
 - Visão sobre o processo todo
 - Controlos a considerar e um plano de acção /prioritização

Vulnerability scanner - Relatório

- Capa
- Índice
- Sumário Executivo
- Ferramentas utilizadas
 - Introdução à ferramenta, vantagens, alternativas
- Condições de realização do scan
- Resultados do scan
 - principais resultados
 - report em anexo
- Análise do scan vs FRAAP
- Vantagens da utilização do scan na Gestão de Risco
 - ciclo de vida
- Conclusões

Segurança e Gestão de Risco

2ºSem 2023/24

Revisões

LUIS AMORIM

01 Jun 2024

