

SEGURANÇA E GESTÃO DE RISCO

2ºSEM 2021/22

REVISÃO

LUIS AMORIM

11 Jun 2022



2 TRABALHOS DE GRUPO

- Os Trabalhos são: (AR - Análise de riscos, AV - Análise de vulnerabilidades)
 - A - AR Sistema de Recrutamento iCreate
 - 3- Digo Amaral, Guilherme Pereira, José Costa
 - B - AV Sistema de Recrutamento iCreate
 - 5- Gonçalo Almeida, Maria Cunha
 - C - AR, no cumprimento do DL65/2021 nos STIC (?)
 - 1- Duarte Mortágua, João Laranjo, José Lucas
 - D - AR Sistema De-Risk, da Trust
 - 4- Pedro Santos, Tiago Oliveira, Dinis Cruz
 - E - Análise de aplicabilidade ao Sistema De-Risk, da Trust
 - 7- Maria Rocha, Pedro Souto, Eridson Barros
 - F - AR sistema Azure DevOps da Link Consulting
 - 6- Alex Lopes, Tiago Pinto, Daniel Andrade
 - G - AV sistema DevOps (interno) da Link Consulting
 - 2- Miguel Mota, Tiago Lucas



3 TRABALHOS DE GRUPO

- Plano – Avaliação dos Riscos
 - pré-FRAAP
 - A realizar até 20 de Junho
 - Acertar data da sessão de FRAAP
 - Enviar relatório até dia 21 de Junho
 - Reuniões FRAAP
 - Entre 17 e 28 de Jun
 - Relatório de FRAAP
 - Descrição e conclusões da avaliação
 - Com Sumário Executivo
 - Enviar até dia 4 de Julho
 - Apresentação das conclusões
 - Colocar em slide as principais conclusões
 - extrair do Sumário Executivo
 - Data de apresentação: dia **12 de Julho**– a confirmar
- Plano - Vulnerability scanner
 - Preparação
 - Assistir à sessão relativa ao mesmo sistema
 - Correr ferramentas
 - Combinar com cliente (feriado ou fds)
 - Até 28 de Junho
 - Relatório até 4 de Julho
 - Alinhado com relatório FRAAP
 - Apresentação das conclusões
 - Colocar em slide as principais conclusões
 - extrair do Sumário Executivo
 - Data de apresentação: dia **12 de Julho**– a confirmar

4 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

PRE-FRAAP

- Resultados esperados

ISSUE
PRIOR TO 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>
Your understanding of the project scope
The FRAAP methodology
Milestones
Pre-screening methodology
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>

DURING THE MEETING
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>
<ul style="list-style-type: none"> Applications/Systems Business Processes Business Functions People and Organizations Locations/Facilities
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 client the FRAAP Document Checklist)</i>

6 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

7

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

8 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

9 ANÁLISE DE APLICABILIDADE AO SISTEMA DE-RISK-RELATÓRIO

- Capa
- Índice
- Sumário Executivo
- Breve descrição da ferramenta e estado de implementação
- Análise de métodos de avaliação do impacto
- Análise de aplicabilidade da ferramenta ao FRAAP
- Vantagens de utilização de ferramenta vs alternativa (excel)
- Conclusões



CRIPTOGRAFIA

Slides externos





REVISÕES

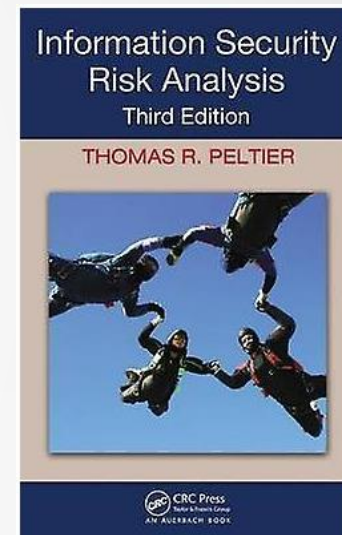


AGENDA/OBJECTIVOS

- 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

13 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

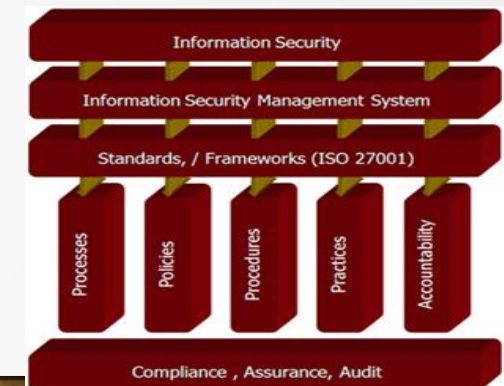


14 SÍNTESE

- Segurança da Informação


- Segurança da Informação, mas actualmente os Sistemas são a base da Informação
- A informação (conjunto de dados devidamente ordenados) é actualmente 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



15 EXEMPLOS

• Biggest data breaches (since 2000)

- 
1. Yahoo, August 2013 > 3 billion accounts
 2. Alibaba, November 2019 > 1.1 billion pieces of user data
 3. LinkedIn, June 2021 > 700 million users
 4. Sina Weibo, March 2020 > 538 million accounts
 5. Facebook, April 2019 > 533 million users
 6. Marriott International (Starwood), September 2018 > 500 million customers
 7. Yahoo, 2014 > 500 million accounts
 8. Adult Friend Finder, October 2016 > 412.2 million accounts
 9. MySpace, 2013 > 360 million user accounts
 10. NetEase, October 2015 > 235 million user accounts
 11. Court Ventures (Experian), October 2013 > 200 million personal records
 12. LinkedIn, June 2012 > 165 million users
 13. Dubsmash, December 2018 > 162 million user accounts
 14. Adobe, October 2013 > 153 million user records
 15. My Fitness Pal, February 2018 > 50 million user accounts

(fonte: <https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>)

Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing

Dec. 11, 2018

WASHINGTON — The cyberattack on the Marriott hotel chain that **collected personal details of roughly 500 million** guests was part of a Chinese intelligence-gathering effort that also hacked health insurers and the security clearance files of millions more Americans, according to two people briefed on the investigation.

The **hackers**, they said, **are suspected of working on behalf of the Ministry of State Security, the country's Communist-controlled civilian spy agency**. The discovery comes as the Trump administration is planning actions targeting China's trade, cyber and economic policies, perhaps within days.

Those moves include indictments against Chinese hackers working for the intelligence services and the military, according to four government officials who spoke on the condition of anonymity. The Trump administration also plans to declassify intelligence reports to reveal Chinese efforts dating **to at least 2014 to build a database containing names of executives** and American government officials with security clearances.

16 EXEMPLOS

- Ameaça: Terrorismo

Planos de ataques da Al Qaeda escondidos em pornografia

Entre eles estavam sequestros de navios de cruzeiros e atentados na Europa semelhantes aos de Bombaim, em 2008

Por: tv24 | 1-5-2012 0:37

Gosto

48
pessoas
gostam
disto.

Like

48

Send

[Casino](#)
[da](#)
[Sorte](#)
[Português](#)
[Jogue](#)
[sem](#)
[necessidade](#)
[de](#)
[depósito](#)
[Ou](#)



A polícia alemã descobriu planos de ataques da Al Qaeda escondidos num vídeo pornográfico que um jovem austríaco tinha escondido na roupa interior.

Entre os alvos encontravam-se navios de cruzeiro e estavam previstos ataques na Europa ao estilo dos que ocorreram na cidade indiana de Bombaim, em Novembro de 2008, em que uma dezena de operacionais armados espalhou o terror durante três dias, matando 164 pessoas.

Esta descoberta só agora revelada foi feita já no ano passado. De acordo com a CNN, tudo começou quando as autoridades germânicas detiveram em Berlim Maqsood Lodin, um austríaco de 22 anos, que estivera recentemente no Paquistão e entrara na Alemanha por terra, depois de ter regressado à Europa através da Hungria.

EXEMPLIFICAÇÃO

- Ameaça: Social Engineering

(<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.

18 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.

20 EXEMPLIFICAÇÃO

- Ameaça: Inundação



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

21 EXEMPLIFICAÇÃO

- Ameaça: Malware

(<http://www.christiantoday.com/article/google.hacked.no.internal.systems.breached.nearly.five.million.gmail.accounts.malware.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.

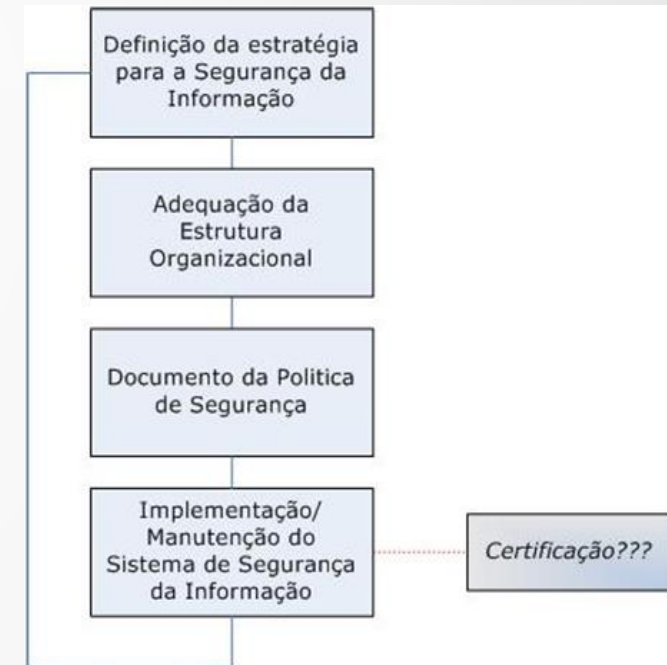
With Google becoming associated with hacking incidents more than a few times in the past months, the company has released a statement regarding the latest hack attack and the security of their users' information.

"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.

22 SÍNTESE

- Segurança da Informação
- Abordagem integrada à Segurança
 - A Segurança de um Sistema de Informação só se consegue atingir considerando de forma integrada - Normas e Procedimentos, Sistemas e Aplicações, Infra-estrutura
 - O Roadmap para Política de Segurança



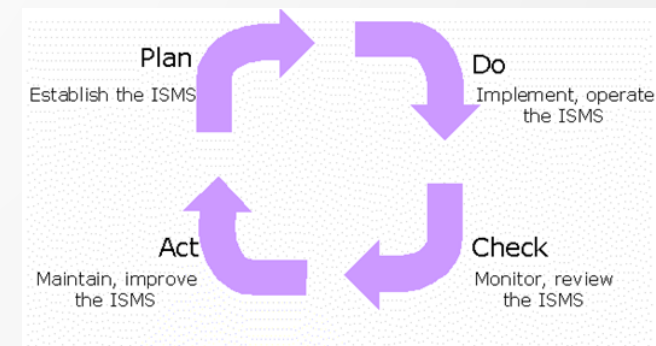
23 SÍNTESE

- 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
- Introdução à ISO 27001
- Introdução à Gestão de Risco



24 SÍNTESE

- Normas e legislação aplicável
- Introdução à ISO 27001
 - ISO/IEC 27001- Information Security Management Systems
 - “specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks.
 - It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof.”
 - O modelo PDCA para o ISMS
 - A versão atual ISO/IEC 27001:2013
- Introdução à Gestão de Risco

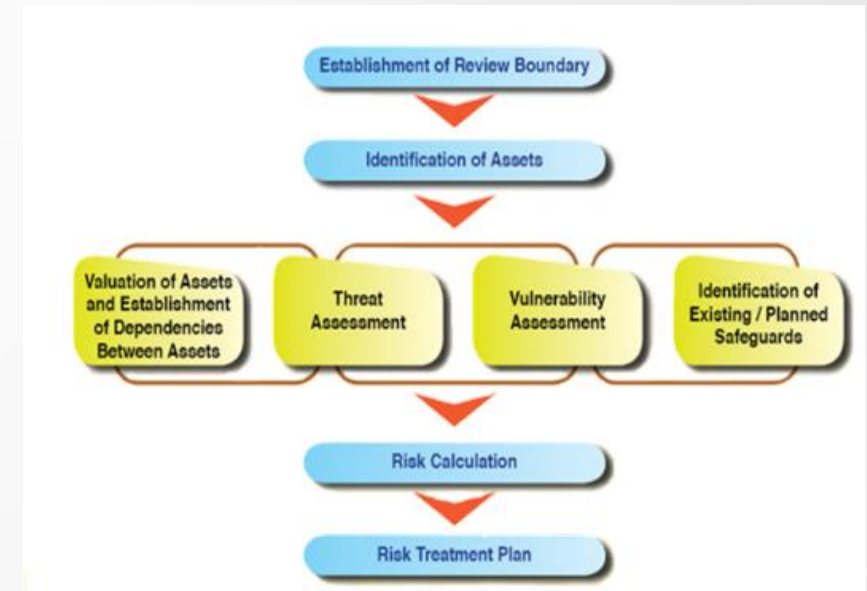


AGENDA/OBJECTIVOS

- 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

26 SÍNTESE

- Introdução à ISO 27001
- 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



27 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:
 - $\text{Risco} = \text{Probabilidade} \times \text{Consequência} \times \text{Severidade}$
 - $\text{Risco} = \text{Valor_Ativo} \times \text{Probabilidade} \times \text{Impacto}$
 - $\text{Risco} = \text{Probabilidade} \times \text{Impacto}$
 - 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”

AGENDA/OBJECTIVOS

- Objectivos
 - 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



29 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

- Business Impact Analysis (BIA)
 - Um processo de Business Impact Analysis pretende determinar os efeitos que as falhas dos Sistemas de Informação Críticos têm 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
 - Classificar esses recursos (em termos de importância e prioridade)

SÍNTESE

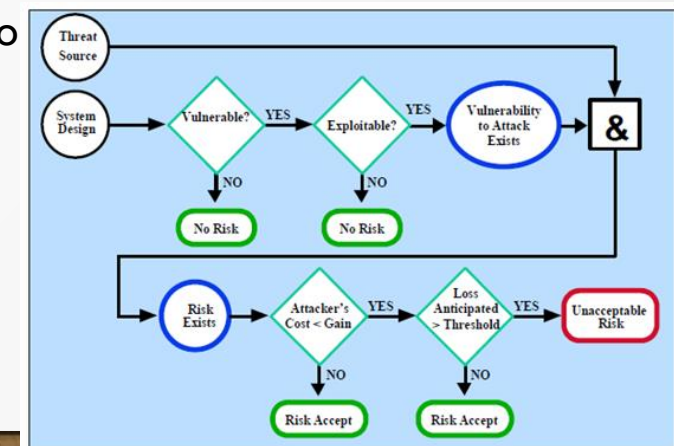
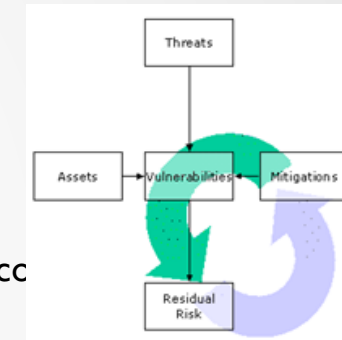
- Objectivos do BIA
 - Identificar os processos de negócio críticos
 - Identificar o número mínimo de colaboradores para recuperar cada processo
 - Estabelecer a sequência de recuperação
 - Determinar o espaço necessário para a equipa de recuperação
 - Identificar equipamentos específicos necessários
 - Identificar outro material necessário
 - Criar procedimento para contornar problemas, no caso do IT ficar inoperacional
 - Determinar o impacto de recuperação de sites que servem mais um serviço ou departamento de negócio
 - Identificar as relações e dependências externas críticas
 - Identificar o impacto na organização em termos de perdas e cumprimento de requisitos legais ou normativos

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

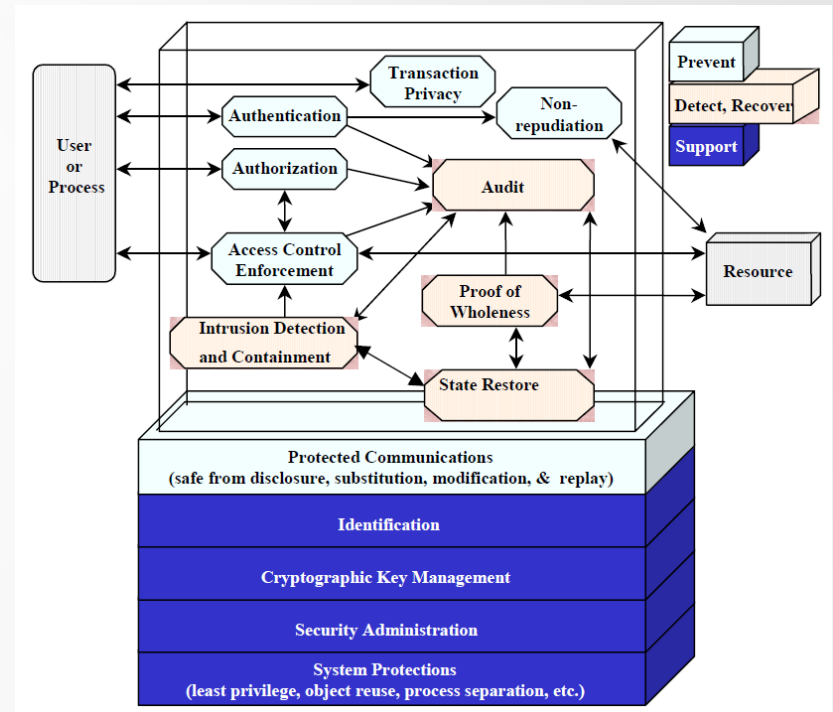
SÍNTESE

- 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
 - Análise de opções de mitigação utilizando o Risk Mitigation Checklist (extraído do NIST)
 - Passos para a implementação de controlos
 - Ter em atenção que a implementação de controlos pode gerar novas vulnerabilidades



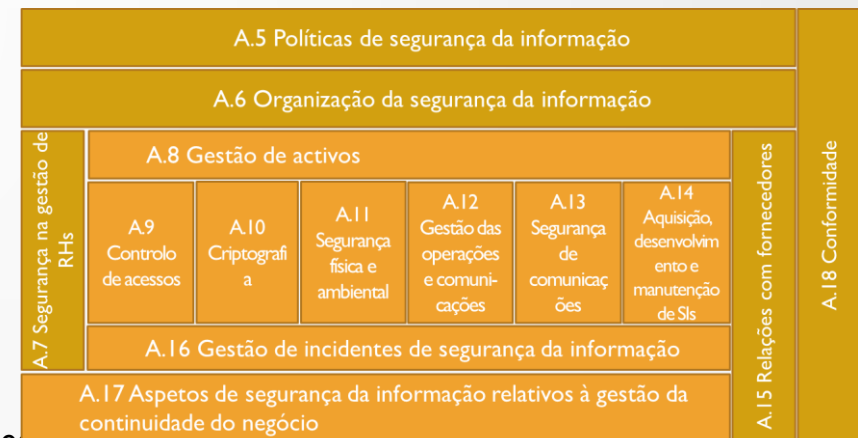
34 SÍNTESE

- 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 17799 ou 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

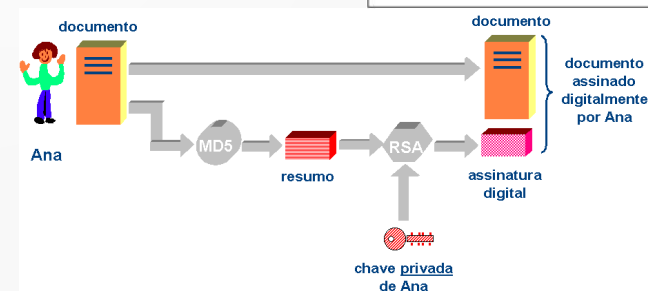
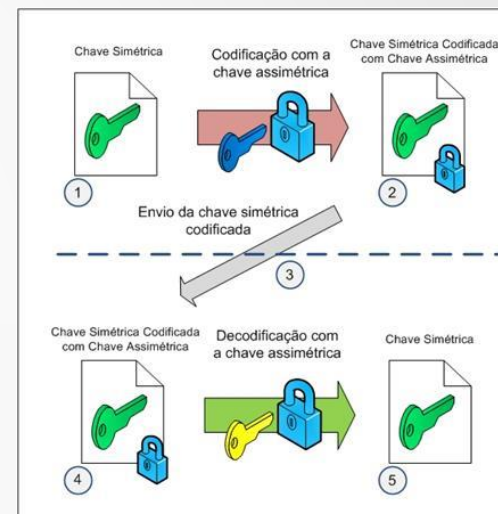


AGENDA/OBJECTIVOS

- Objectivos
 - 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

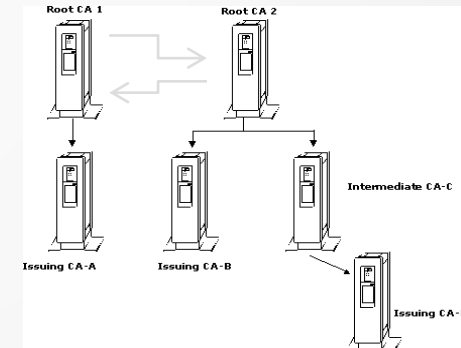
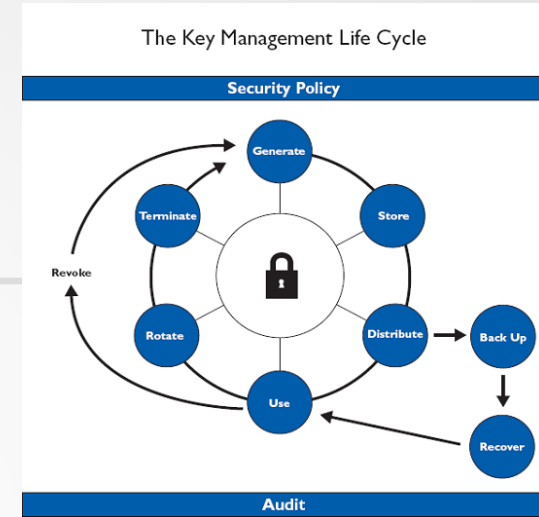
37 SÍNTESE

- 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
- Gestão de chaves



SÍNTESE

- Noções de criptografia
- Gestão de chaves
 - técnicas e procedimentos relacionados com o ciclo de vida das chaves criptográficas
 - Certificate Storage model
- Relações de confiança entre CAs



39 EXEMPLOS DE AMEAÇAS

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

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



Foto: João Miguel Rodrigues • Situação ocorreu na cadeia de alta segurança de Monsanto

cm+ 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 implementas?

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.

AGENDA/OBJECTIVOS

- Objectivos
 - 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

IMPLEMENTAÇÃO DE POLÍTICA DE SEGURANÇA

- 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



AGENDA/OBJECTIVOS

- Objectivos
 - 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**

44 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

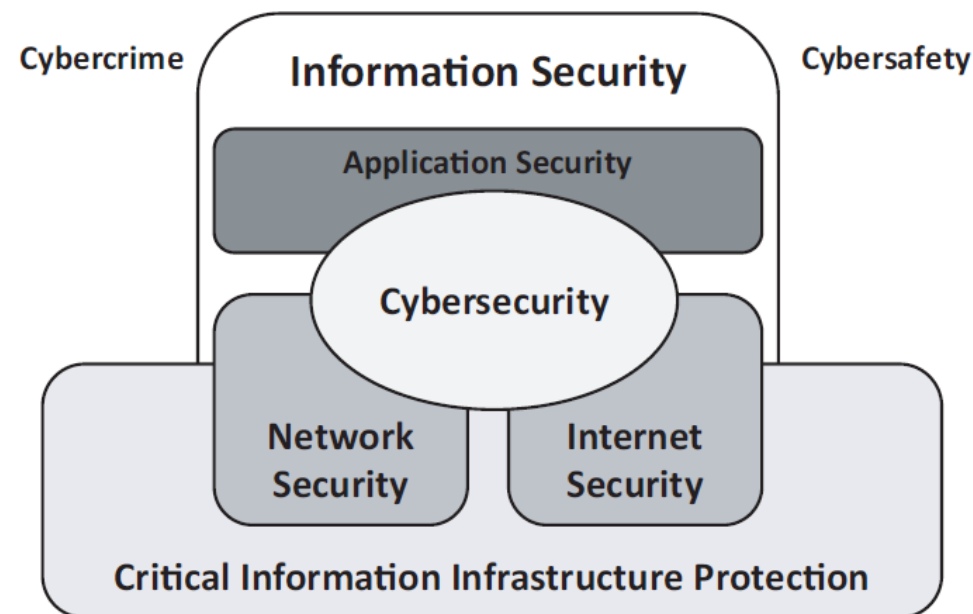


Figure 1 — Relationship between Cybersecurity and other security domains

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

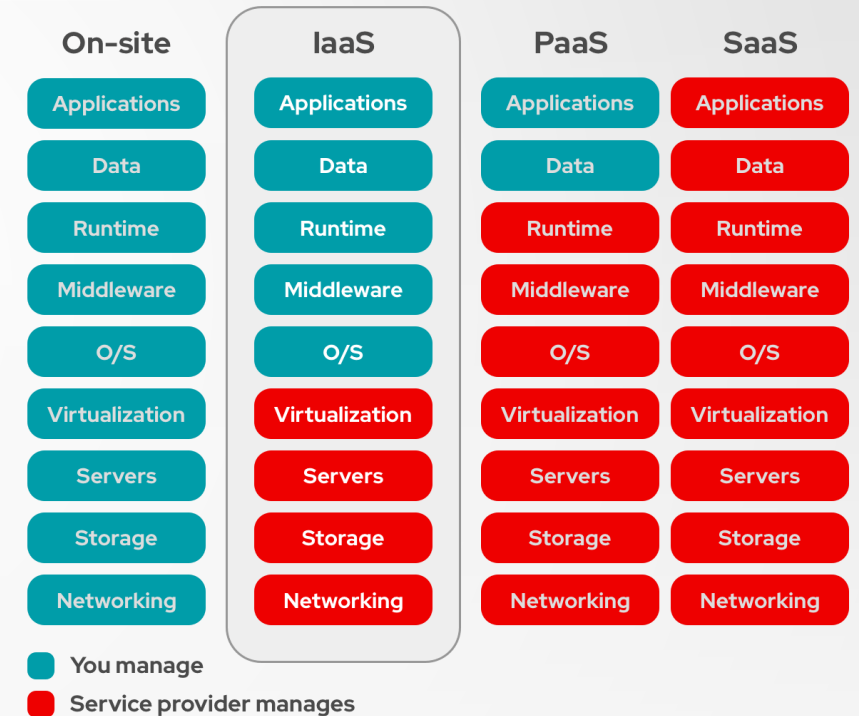


SEGURANÇA DE SERVIÇOS NA CLOUD

- 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

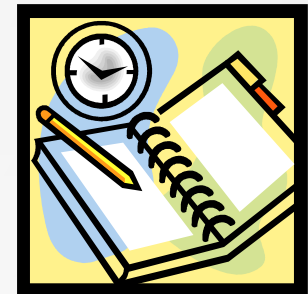
Control 6.1.3 and the associated implementation guidance and other information specified in ISO/IEC 27002 apply. The following sector-specific guidance also applies.

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.

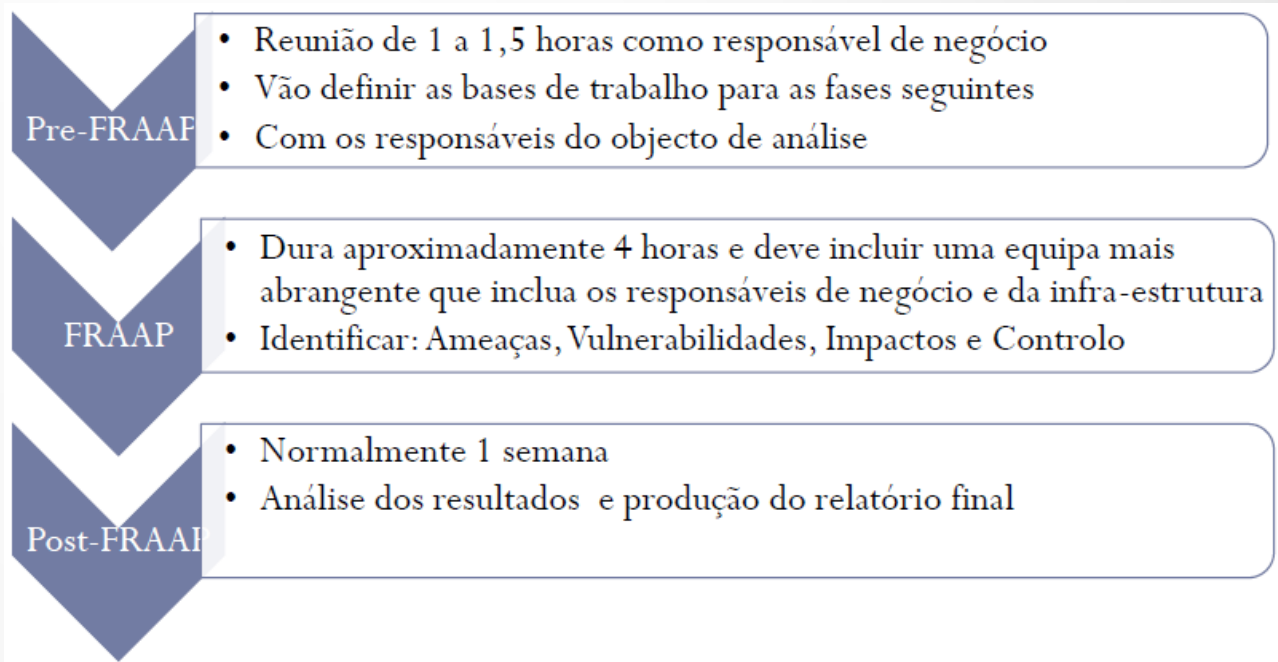
SÍNTESE

- Facilitated Risk Analysis and Assessment Process
 - Este processo envolve a análise de 1 sistema processo, plataforma, processo de negócio definido de cada vez
 - Pre-FRAAP
 - Reunião de 1 a 1,5 horas como responsável de negócio
 - Vão definir as bases de trabalho para as fases seguintes
 - FRAAP
 - Dura aproximadamente 4 horas e deve incluir uma equipa mais abrangente que inclua os responsáveis de negócio e da infra-estrutura
 - Identificar: Ameaças, Vulnerabilidades, Impactos e Controlos
 - Post-FRAAP
 - Normalmente 1 a 2 semanas
 - Análise dos resultados e produção do relatório final



SÍNTESE

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



51 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 principio
 - Mini-Brainstorming (identificar ameaças para introdução na reunião FRAAP)

ISSUE
PRIOR TO 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>
Your understanding of the project scope
The FRAAP methodology
Milestones
Pre-screening methodology
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>

DURING THE MEETING
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>
• Applications/Systems
• Business Processes
• Business Functions
• People and Organizations
• Locations/Facilities
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 client the FRAAP Document Checklist)</i>

52 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



53 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

Prioritizar e
planear
implementação
de controlos

SESSÃO FRAAP

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

- 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 breeches	1	2	Low		
Employee is not able to verify the identity of a client (e.g., phone masquerading)		1	1	Low		

SESSÃO FRAAP

Definição de
níveis e matriz
de avaliação de
risco

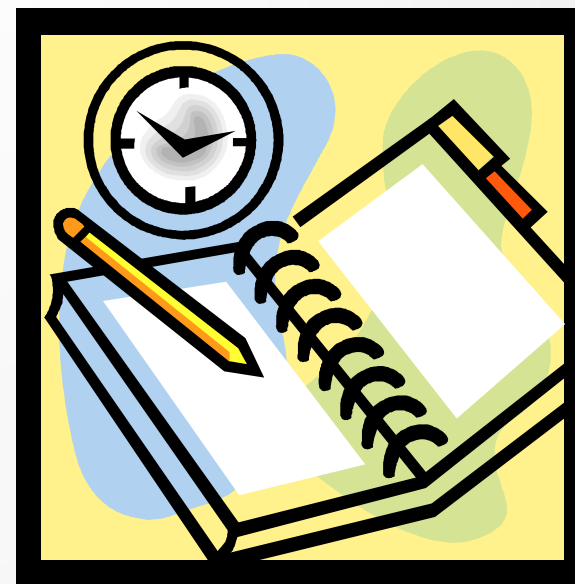
Avaliação das
ameaças com os
controles já
implementados

Identificar novos
controles para
Riscos maiores

Avaliar novo
nível de risco

Prioritizar e
planear
implementação
de controles

- Estabelecimento do nível de risco
 - Prioritizar implementação de controles
 - 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



58 TRABALHOS DE GRUPO

- Os Trabalhos são: (AR - Análise de riscos, AV - Análise de vulnerabilidades)
 - A - AR Sistema de Recrutamento iCreate
 - 3- Digo Amaral, Guilherme Pereira, José Costa
 - B - AV Sistema de Recrutamento iCreate
 - 5- Gonçalo Almeida, Maria Cunha
 - C - AR, no cumprimento do DL65/2021 nos STIC (?)
 - 1- Duarte Mortágua, João Laranjo, José Lucas
 - D - AR Sistema De-Risk, da Trust
 - 4- Pedro Santos, Tiago Oliveira, Dinis Cruz
 - E - Análise de aplicabilidade ao Sistema De-Risk, da Trust
 - 7- Maria Rocha, Pedro Souto, Eridson Barros
 - F - AR sistema Azure DevOps da Link Consulting
 - 6- Alex Lopes, Tiago Pinto, Daniel Andrade
 - G - AV sistema DevOps (interno) da Link Consulting
 - 2- Miguel Mota, Tiago Lucas



59 TRABALHOS DE GRUPO

- Plano – Avaliação dos Riscos
 - pré-FRAAP
 - A realizar até 20 de Junho
 - Acertar data da sessão de FRAAP
 - Enviar até dia 20 de Junho
 - Reuniões FRAAP
 - Entre 17 e 28 de Jun
 - Relatório de FRAAP
 - Descrição e conclusões da avaliação
 - Com Sumário Executivo
 - Enviar até dia 1 de Julho
 - Apresentação das conclusões
 - Colocar em slide as principais conclusões
 - extrair do Sumário Executivo
 - Data de apresentação: dia **8 de Julho**– a confirmar
- Plano - Vulnerability scanner
 - Preparação
 - Assistir à sessão relativa ao mesmo sistema
 - Correr ferramentas
 - Combinar com cliente (feriado ou fds)
 - Até 28 de Junho
 - Relatório até 2 de Julho
 - Alinhado com relatório FRAAP
 - Apresentação das conclusões
 - Colocar em slide as principais conclusões
 - extrair do Sumário Executivo
 - Data de apresentação: dia **8 de Julho**– a confirmar

60 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

62 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

63 ANÁLISE DE APLICABILIDADE AO SISTEMA DE-RISK-RELATÓRIO

- Capa
- Índice
- Sumário Executivo
- Breve descrição da ferramenta e estado de implementação
- Análise de métodos de avaliação do impacto
- Análise de aplicabilidade da ferramenta ao FRAAP
- Vantagens de utilização de ferramenta vs excel
- Conclusões



64

SEGURANÇA E GESTÃO DE RISCO

2ºSEM 2021/22

REVISÃO

LUIS AMORIM

11 Jun 2022

