

SEGURANÇA E GESTÃO DE RISCO

2ºSEM 2021/22

MODELO DE SEGURANÇA INTEGRADO

PROCESSO DE AVALIAÇÃO DOS RISCOS

LUIS AMORIM

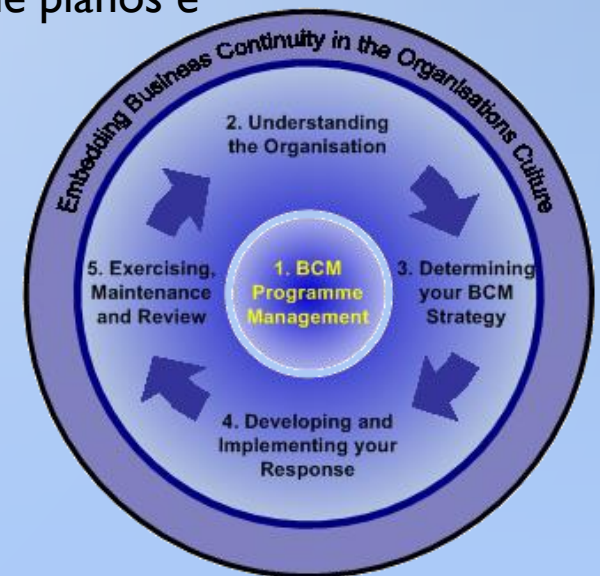
09 Abr 2022

2 SÍNTESE

- Introdução à Gestão de Continuidade de Negócio
- A avaliação e gestão de riscos
- Tratamento dos Riscos
- Controlos de segurança
 - Tecnológicos, Operacionais e de Gestão

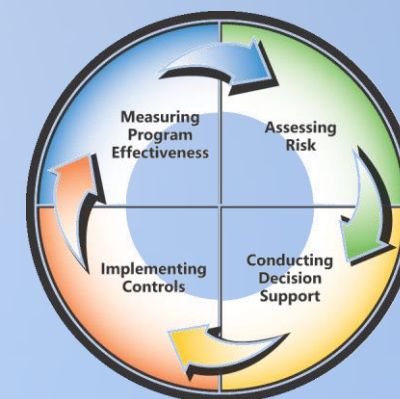
3 SÍNTESE

- 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



4 SÍNTESE

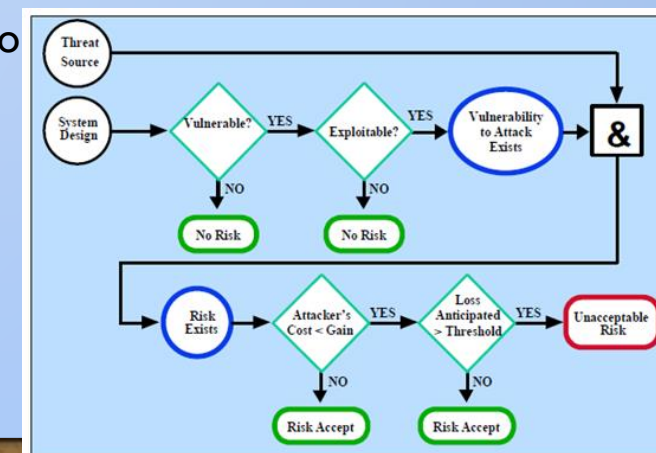
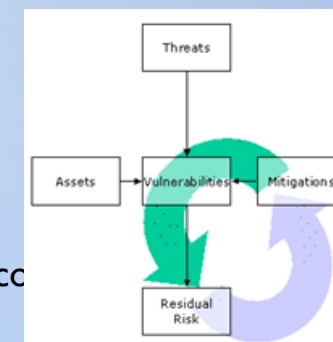
- A análise e gestão de riscos
 - Gestão de Risco como processo (não projeto) mais abrangente
 - A aplicação da Avaliação e Análise de Risco:
 - Sobre os processos e sistemas implementados
 - Sobre novos processos e sistemas (projeto Impact Analysis)
 - Etapas da Avaliação de Riscos (NIST)
 - Formas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



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

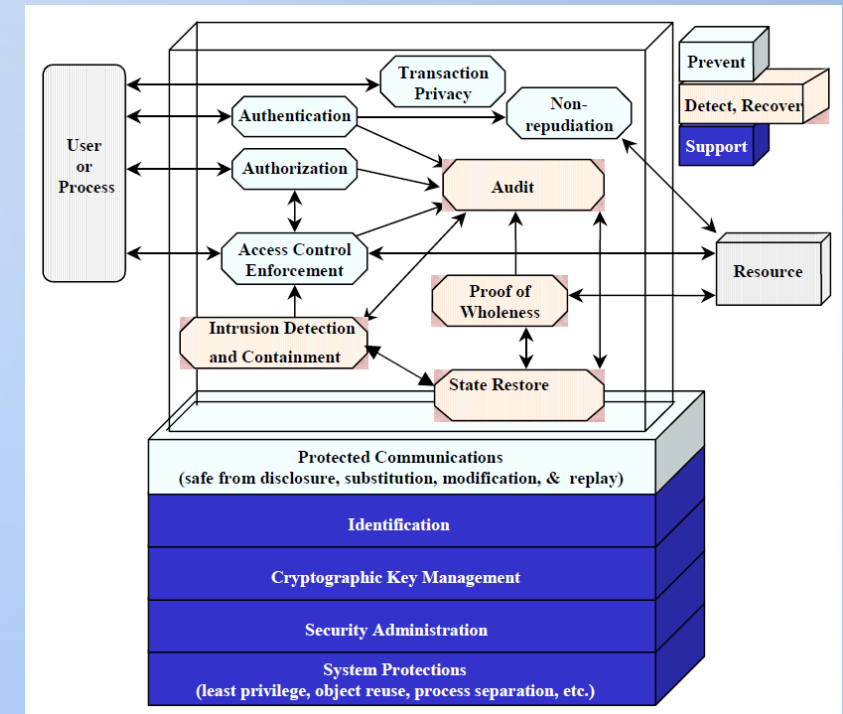
5 SÍNTESE

- 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



6 SÍNTESE

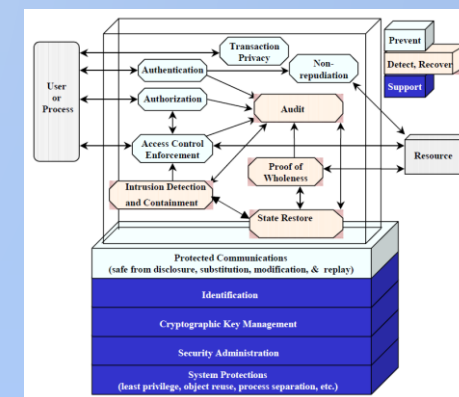
- Controlos de segurança
 - Tecnológicos
 - de Suporte
 - Preventivos
 - Para detecção e recuperação
 - Não tecnológicos:
 - Controlos de Gestão e Organizacionais
 - definição de políticas e normas de protecção da informação
 - definem como os elementos da organização devem actuar
 - Controlos Operacionais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



7 CONTROLOS DE SEGURANÇA

- Exercício – Identificar controlos de segurança

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



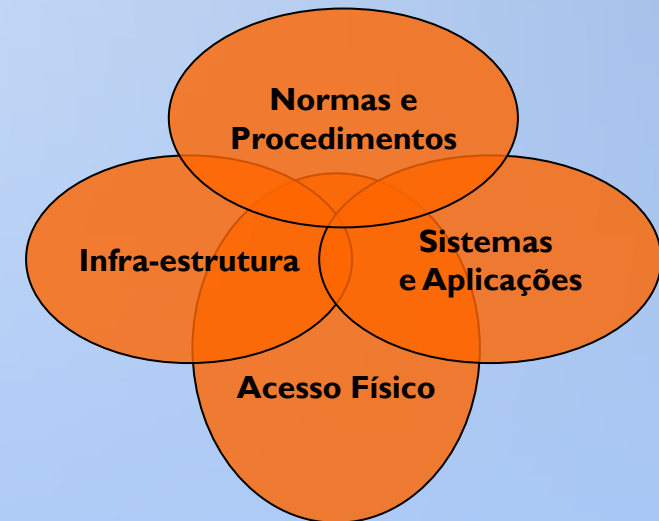
8 AGENDA

➤ **Modelo de segurança integrado**

- O processo de análise de risco FRAAP
 - Introdução
 - Etapas do processo
 - Pre-FRAAP
 - FRAAP
 - Post-FRAAP

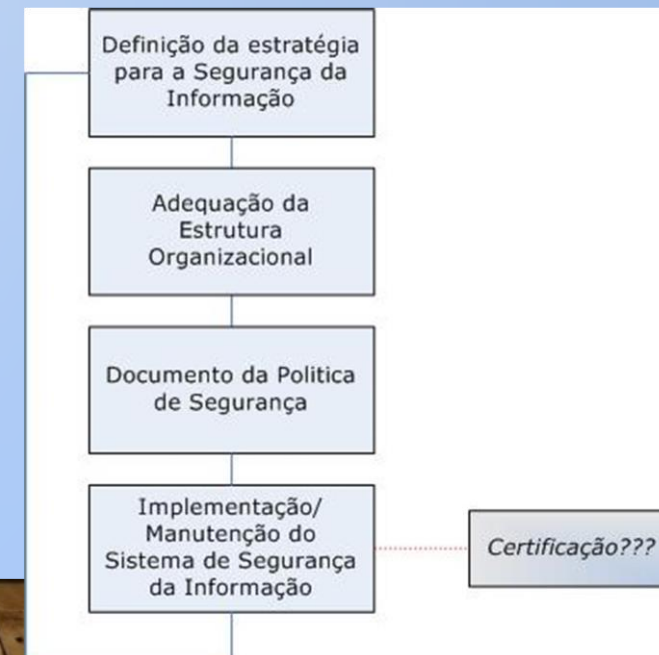
9 ABORDAGEM INTEGRADA À SEGURANÇA

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



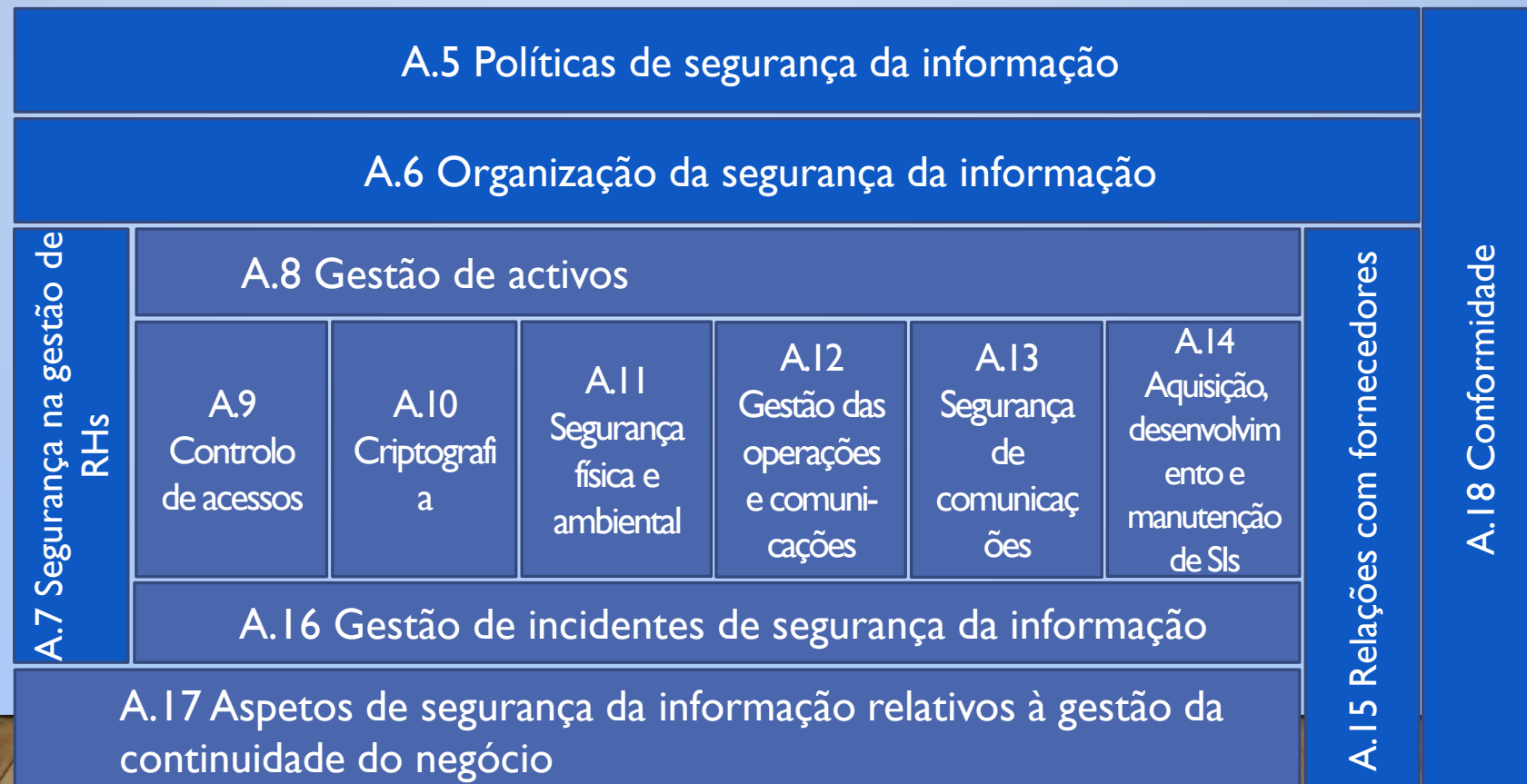
10 ABORDAGEM INTEGRADA À SEGURANÇA

- A definição de estratégia e metodologias deve estar suportada numa Política de Segurança
 - Integrada, ou não, num ISMS - Information Security Management System
 - Inserido, ou não num processo de certificação
- Roadmap para Política de Segurança



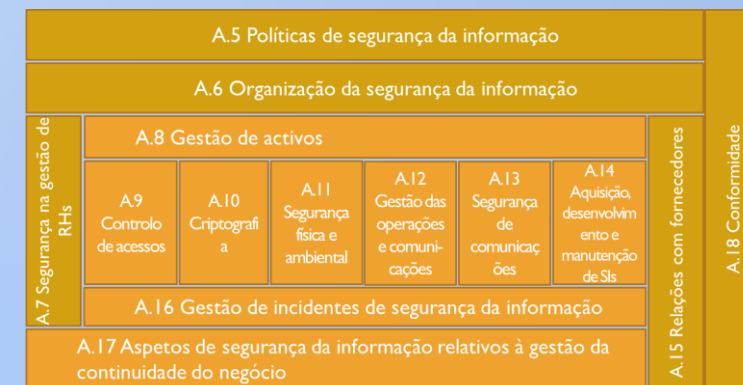
II MODELO DE SEGURANÇA INTEGRADO

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



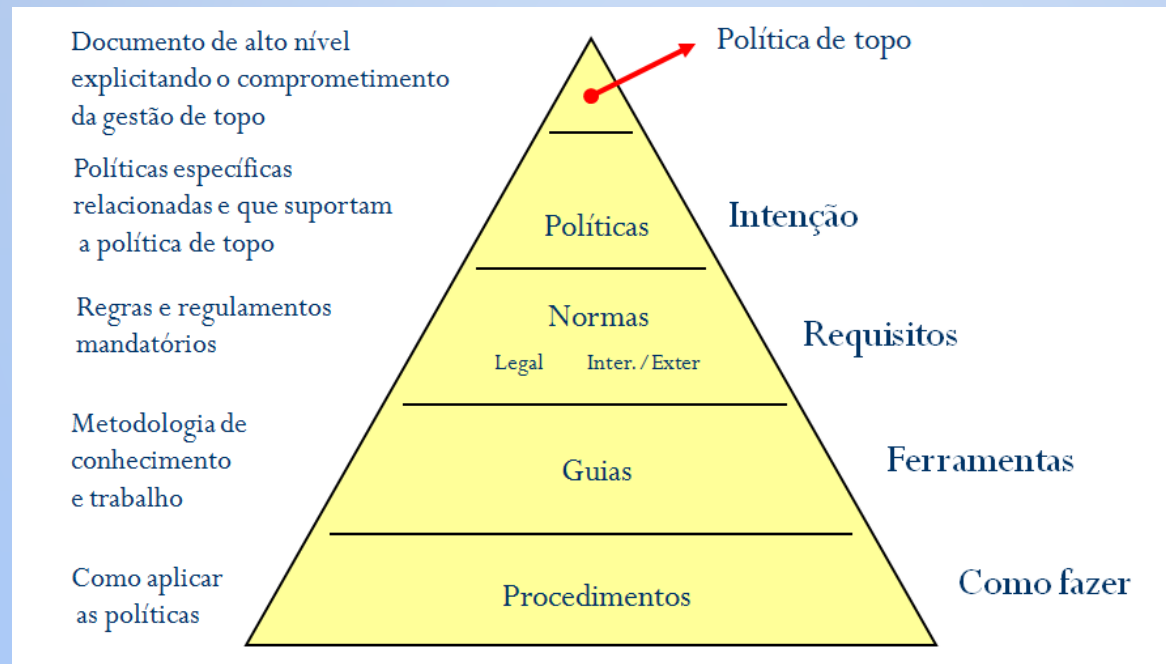
I3 MODELO DE SEGURANÇA INTEGRADO

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



14 MODELO DE SEGURANÇA INTEGRADO

- Estruturação de política de segurança



15 MODELO DE SEGURANÇA INTEGRADO

- Política de segurança

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

16 MODELO DE SEGURANÇA INTEGRADO

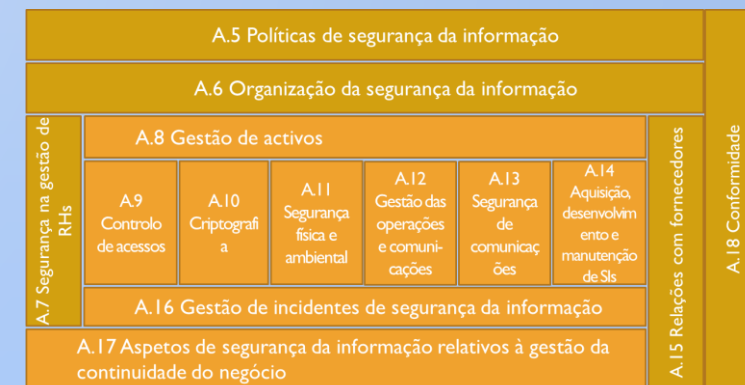
- As Políticas de segurança poderão conter:
 - Os requisitos para o plano de contingência da organização;
 - As necessidades de backup/restore;
 - A forma de seleção e gestão de ferramentas de eliminação de vírus;
 - As especificações de mecanismos para controlo de acessos a sistemas e dados;
 - Forma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

17 MODELO DE SEGURANÇA INTEGRADO

• Organização da Segurança

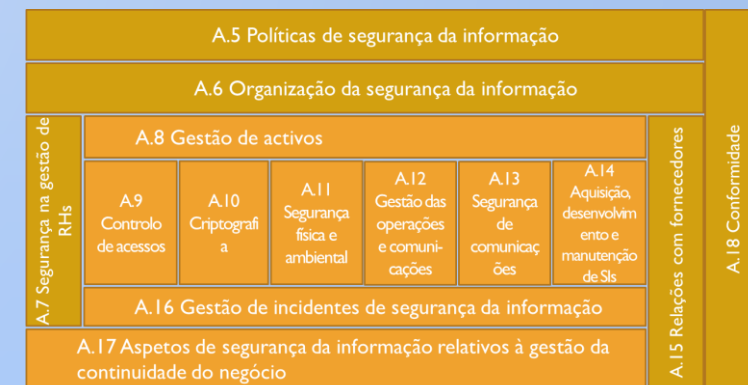
De forma a estabelecer um modelo de referência de gestão para iniciar e controlar a implementação e operação da segurança da informação dentro da organização.

- Papéis e responsabilidades de segurança da informação
- Segregação de funções
- Contacto com autoridades competentes
- Contacto com grupos de interesse especial
- Segurança da informação na gestão de projeto
- Política de dispositivos móveis e Teletrabalho
 - De forma a assegurar a segurança no teletrabalho e na utilização de dispositivos móveis.



18 MODELO DE SEGURANÇA INTEGRADO

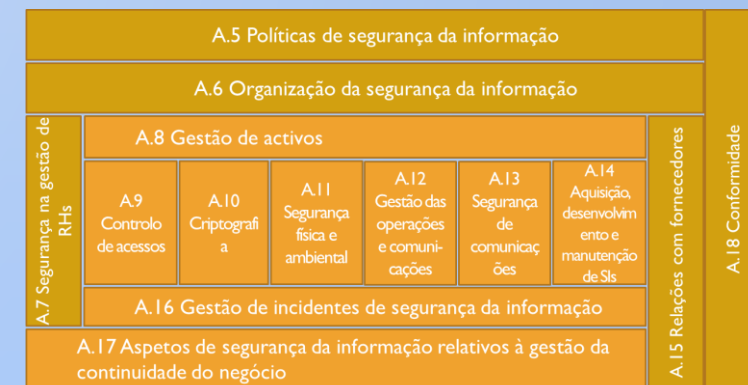
- Segurança na gestão de RHs
 - Antes, durante a após a relação contratual
 - Verificação de credenciais
 - Acordos de confidencialidade
 - Termos e condições de trabalho
 - Responsabilidades
 - Resposta a incidentes de segurança
 - Educação e Treino
 - Ações disciplinares
 - Término das responsabilidades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



20 MODELO DE SEGURANÇA INTEGRADO

• Controlo de acessos à informação

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

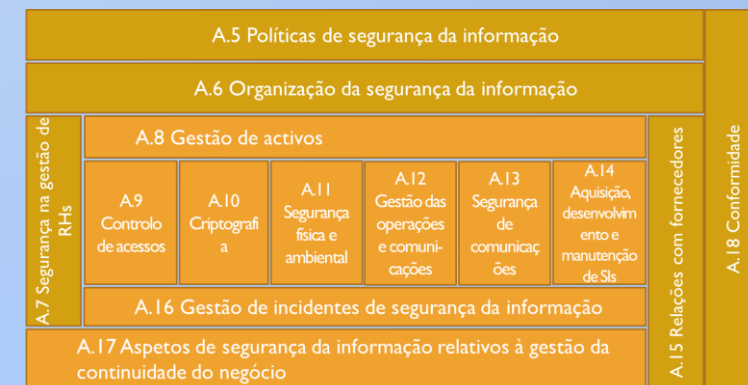


21 MODELO DE SEGURANÇA INTEGRADO


• Criptografia

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

- Política sobre a utilização de controlos criptográficos
- Gestão de chaves
 - utilização, proteção e vida útil das chaves criptográficas ao longo de todo o seu ciclo de vida.

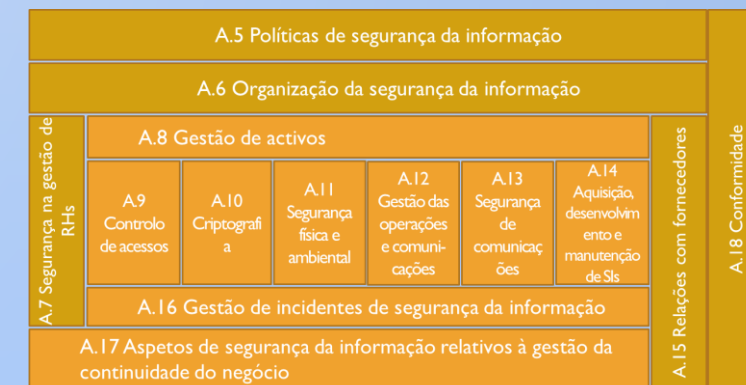


22 EXERCÍCIO

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

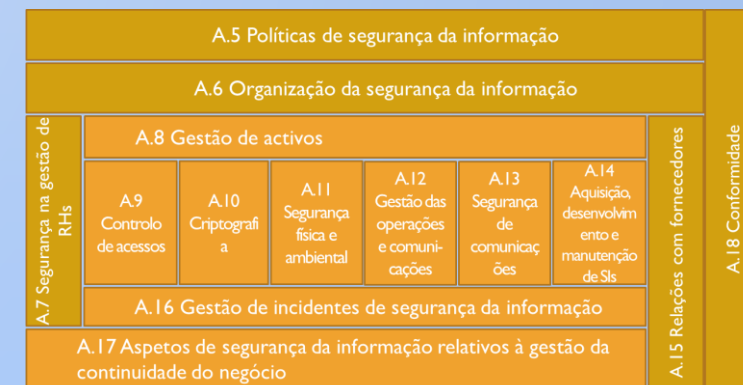
24 MODELO DE SEGURANÇA INTEGRADO

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



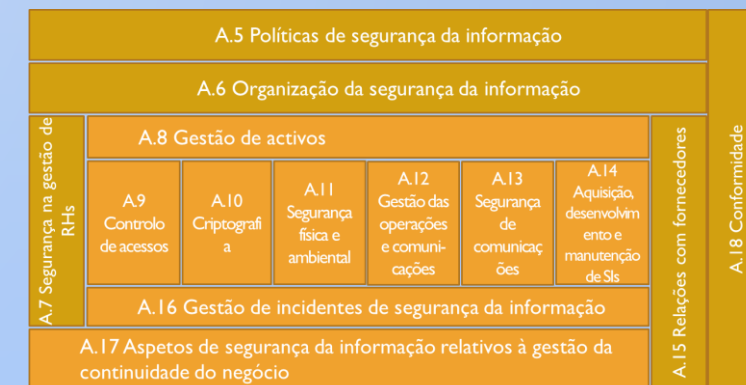
25 MODELO DE SEGURANÇA INTEGRADO

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



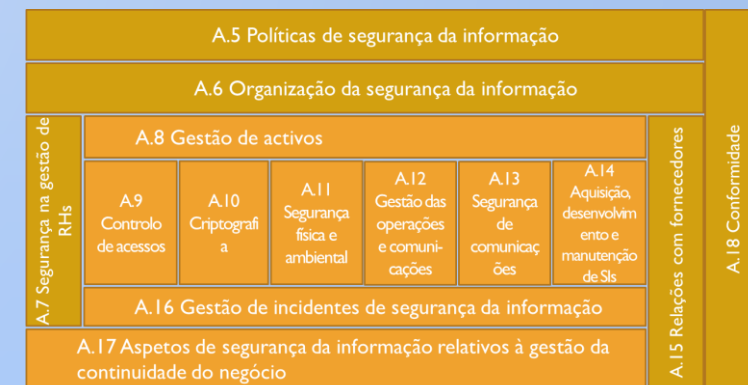
26 MODELO DE SEGURANÇA INTEGRADO

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



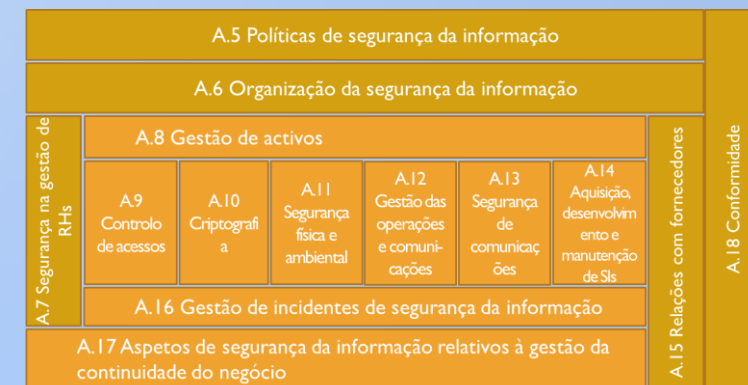
27 MODELO DE SEGURANÇA INTEGRADO

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



28 MODELO DE SEGURANÇA INTEGRADO

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



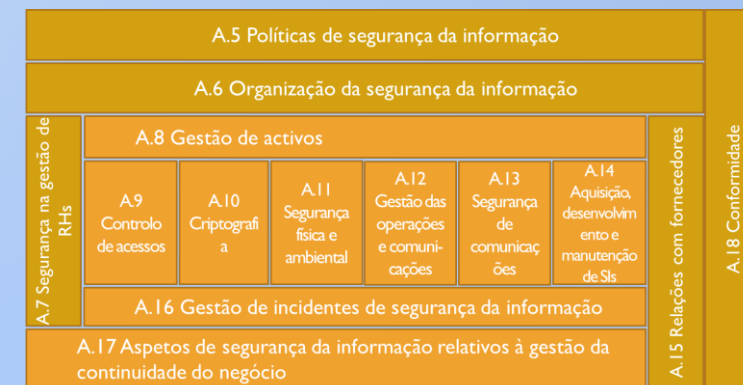
29 EXERCÍCIO DE GRUPO

- Idealizar um sistema de Gestão de Incidentes

34 MODELO DE SEGURANÇA INTEGRADO

• Continuidade de negócio

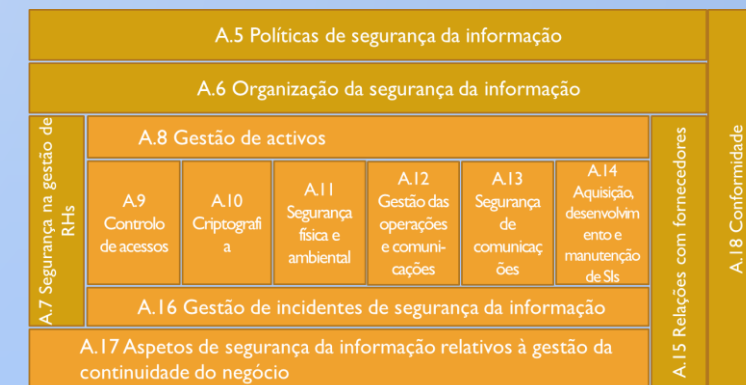
- Inclusão da segurança da informação no processo de gestão da continuidade do negócio
- Análise de impacto no negócio e identificação de processos críticos
- Estabelecimento das redundâncias necessárias à continuidade
- Desenvolvimento e implantação de planos de continuidade, incluindo segurança da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



35 MODELO DE SEGURANÇA INTEGRADO

• Conformidades

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



36 MODELO DE SEGURANÇA INTEGRADO

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

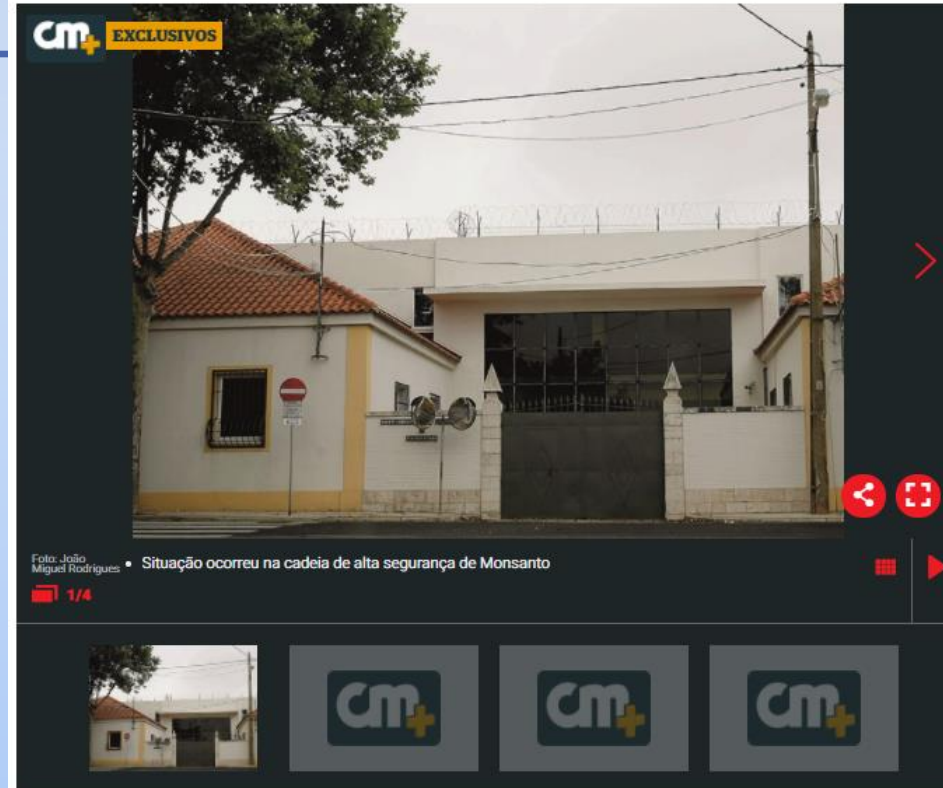
37 EXEMPLOS DE AMEAÇAS

- 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



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.

38 EXEMPLOS DE AMEAÇAS

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

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

Lioman Lima - @liomanlima
BBC News Mundo

19 junho 2019



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

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

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

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

Até que cerca de 700 mil pessoas ficaram sem eletricidade.

39 EXERCÍCIO DE GRUPO

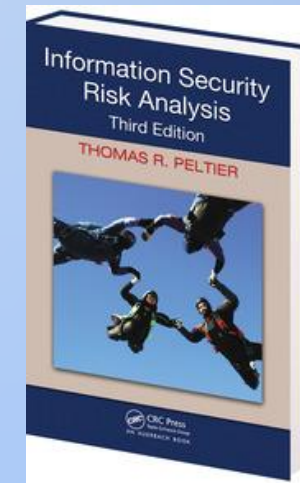
- Conduzir uma Avaliação dos Riscos

40 AGENDA

- Modelo de segurança integrado
- **O processo de análise de risco FRAAP**
 - Introdução
 - Etapas do processo
 - Pre-FRAAP
 - FRAAP
 - Post-FRAAP
 - Ferramentas de apoio ao processo

41 PROCESSO DE ANÁLISE DE RISCO FRAAP

- Facilitated Risk Analysis and Assessment Process
 - É uma metodologia de análise e avaliação de risco desenvolvido por Thomas R. Peltier
 - Tem por base as normas existentes (nomeadamente a 17799/27002)
 - Que transmitem as boas práticas, não a metodologia
 - Resulta da experiência da equipa em projectos
 - Tem sido utilizada, e melhorada, nos últimos 15 anos
 - Prima por:
 - Ser dirigido pelo responsável de negócio
 - Levar dias, em vez de semanas
 - Boa relação custo-benefício
 - Utilizar especialistas/experiencia interna



42 PROCESSO DE ANÁLISE DE RISCO FRAAP

- Facilitated Risk Analysis and Assessment Process
 - Este processo envolve a análise de I sistema, plataforma, processo de negócio de cada vez
 - A afinação do processo, baseada na experiência prática, torna-se
 - Rápido
 - Fácil de implementar
 - Envolve a organização

44 PROCESSO DE ANÁLISE DE RISCO FRAAP

- Método Qualitativo vs Quantitativo

<i>Quantitative Risk Assessment</i>	<i>Qualitative Risk Assessment</i>
Advantages	Advantages
The results are based substantially on independently objective processes and metrics.	Calculations are simple.
Great effort is put into asset value definition and risk mitigation.	It is not necessary to determine monetary value of asset.
Cost-benefit assessment effort is essential.	It is not necessary to quantify threat frequency.
Results can be expressed in management-specific language.	It is easier to involve nonsecurity and nontechnical staff.
	It provides flexibility in process and reporting.

45 PROCESSO DE ANÁLISE DE RISCO FRAAP

- Método Quantitativo vs Qualitativo

<i>Quantitative Risk Assessment</i>	<i>Qualitative Risk Assessment</i>
Disadvantages	Disadvantages
Calculations are complex.	It is very subjective in nature.
Historically, it only works well with a recognized automated tool and associated knowledge base.	Limited effort is required to develop monetary value for targeted assets.
There is a large amount of preliminary work.	There is no basis for the cost-benefit analysis of risk mitigation.
It is not presented on a personnel level.	
Participants cannot be coached easily through the process.	
It is difficult to change directions.	
It is difficult to address out-of-scope issues.	

46 PROCESSO DE ANÁLISE DE RISCO FRAAP

- Avaliação qualitativa vs Avaliação quantitativa (visto anteriormente)

“Many discussions of security risk analysis methodologies mention a distinction between quantitative and qualitative risk analysis, but virtually none of those discussions clarify the distinction in a rigorous way”

(Posted By Jeff Lowder On September 4, 2008 @ 6:00 am In Risk Analysis)

- Quantitative Risk Analyses assign fixed numerical values (within a margin of error) to both the probability and utility (business impact) of an outcome;
- Qualitative Risk Analyses don't. Instead, they represent both the probability and utility of an outcome using an interval scale, where each interval includes a range of numerical values (beyond the margin of error) and each interval is typically represented by a non-numerical label (such as the words “High”, “Medium”, “Low”), not the ranges of values those labels represent.

47 PROCESSO DE ANÁLISE DE RISCO FRAAP

- Facilitated Risk Analysis and Assessment Process

- Durante o processo a equipa envolvida é conduzida a participar na discussão e identificação de

- potenciais ameaças
- níveis de risco
- possíveis controlos a aplicar



48 PROCESSO DE ANÁLISE DE RISCO FRAAP

- Vantagens do FRAAP
 - É realizado em alguns dias, em vez de semanas/meses
 - Envolve o responsável de negócio
 - Participa no processo
 - Compreende as necessidades de implementação
 - Envolvido na selecção de controlos eficientes (custo-benefício)
 - Envolve as áreas de negócio
 - Reconhecimento da participação e controlo do processo
 - Permite à equipa participar na selecção de controlos apropriados
 - Facilita a Gestão da Mudança

49 PROCESSO DE ANÁLISE DE RISCO FRAAP

- Equipa envolvida
 - Responsável de negócio do processo, sistema ou activo
 - Gestor de Projecto - nomeado pelo gestor de negócio
 - O seu papel é acompanhar o desenrolar do projecto e garantir as condições necessárias requeridas pela equipa (sala, agendar reunião...)
 - Facilitador
 - consultor com conhecimento do FRAAP
 - Escriba ou secretário(a)
 - responsável por documentar as reuniões
 - Especialistas relacionados com o objecto
 - Negócio
 - IT
 - Users



50 PROCESSO DE ANÁLISE DE RISCO FRAAP

- Facilitador
 - Consultor que ajude a conduzir o grupo no sentido de obter os resultados esperados
 - Ameaças, probabilidades, impacto, nível de risco
 - Guiar a equipa pelas várias áreas de interesse
 - Identificando o maior número de ameaças
 - Manter o grupo focado no tema
 - Actuar como regulador e árbitro da sessão
 - Controlar o tempo



51 PROCESSO DE ANÁLISE DE RISCO FRAAP

- Facilitador
 - Deve observar as seguintes regras
 - Encorajar a participação de todos
 - Aceitar todas as sugestões
 - Envolver os participantes, escutando opiniões
 - Estar atento às movimentações, gestos, silêncios
 - Actuar como regulador e árbitro da sessão
 - Deve ser imparcial, sem tomar posições particulares, mas guiando a equipa quando está perdida ou é preciso consenso
 - Ser objectivo



52 PROCESSO DE ANÁLISE DE RISCO FRAAP

- Escriba ou secretário(a)
 - Responsável por documentar as reuniões
 - Assegura que todas as ameaças, controlos e acções são registadas
 - Libertando o facilitador desta função, permite-lhe desempenhar melhor a sua função principal



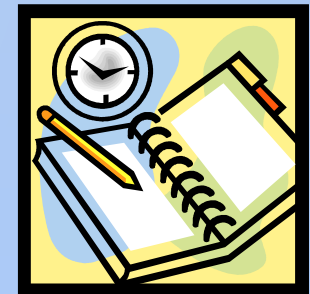
53 PROCESSO DE ANÁLISE DE RISCO FRAAP

- Especialistas relacionados com o objeto em análise
 - São elementos da própria organização que conhecem o sistema ou processo em análise
 - Deve ser uma equipa equilibrada, entre as várias áreas de competência
 - Conhecimento do negócio, familiarizados com a missão do objecto em análise
 - Utilizadores que conheçam as vulnerabilidades e ameaças
 - Técnicos IT com conhecimento da infra-estrutura e sistemas em causa
 - Elementos devem conseguir funcionar em equipa



54 PROCESSO DE ANÁLISE DE RISCO FRAAP

- 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



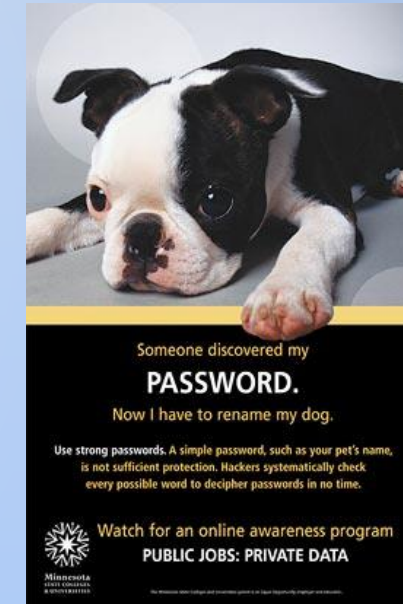
55 PROCESSO DE ANÁLISE DE RISCO FRAAP

- Antes de iniciar deve existir um Programa de Sensibilização
 - Dar a conhecer o processo
 - Envolver os participantes
 - Este Programa deve ser conduzido de forma a
 - Avaliar o conhecimento relativo a avaliação de risco
 - Determinar o que os gestores e outros funcionários pretendem aprender
 - Verificar o nível de aceitação do programa de segurança
 - Traçar forma de conquistar a aceitação
 - Identificar possíveis aliados

56 PROCESSO DE ANÁLISE DE RISCO FRAAP

- Ferramentas para um Programa de Sensibilização?

- eMail
- Site
- Cartazes
- Questionários
 - Mail
 - Electrónicos
 - Papel
- Sessão de apresentação



57 PROCESSO DE ANÁLISE DE RISCO FRAAP

- Programa de Sensibilização deve
 - Ser adaptado à organização
 - Ferramentas e linguagem
 - Seleccionar as ferramentas adequadas a cada grupo
 - Encontrar áreas não conformes
 - Trabalhar no sentido de reduzir exposição
 - E resolver possíveis atritos
 - Sem comprometer resultados da avaliação
 - Envolver os utilizadores

58 PROCESSO DE ANÁLISE DE RISCO FRAAP

- Pontos chave
 - Garantir o envolvimento dos participantes
 - O processo é da organização, não é do consultor/facilitador
 - Não utilizar expressões como o meu projecto
 - É o Vosso ou Nosso projecto



59 PROCESSO DE ANÁLISE DE RISCO FRAAP

- Conceitos chave – funções
 - Owner
 - Deve ser o mais alto responsável da unidade onde o objecto do processo pertence
 - É responsável por:
 - Estabelecer a classificação da informação
 - Identificar controlos razoáveis e prudentes
 - Monitorizar a adequação de implementação de controlos
 - Autorizar o acesso a quem necessita
 - Ou inibição
 - Custodian
 - Nomeado pelo owner como responsável do controlo
 - User
 - Empregados autorizados a aceder à informação



60 SESSÃO PRE-FRAAP

- Reunião de Pre-FRAAP
 - Reunião de 1 a 1,5 horas com o responsável de negócio
 - Deve incluir
 - Gestor de Negócio/Processo e Gestor de Projecto
 - Facilitador
 - Escriba

6 | SESSÃO PRE-FRAAP

- Resultados esperados
 1. Pré-triagem
 2. Definição do âmbito
 3. Diagrama com a descrição/detalhe do sistema ou processo a avaliar
 4. Estabelecimento da equipa a incluir no processo
 5. Requisitos para a reunião FRAAP
 6. Acordar definições de principio
 7. Mini-Brainstorming

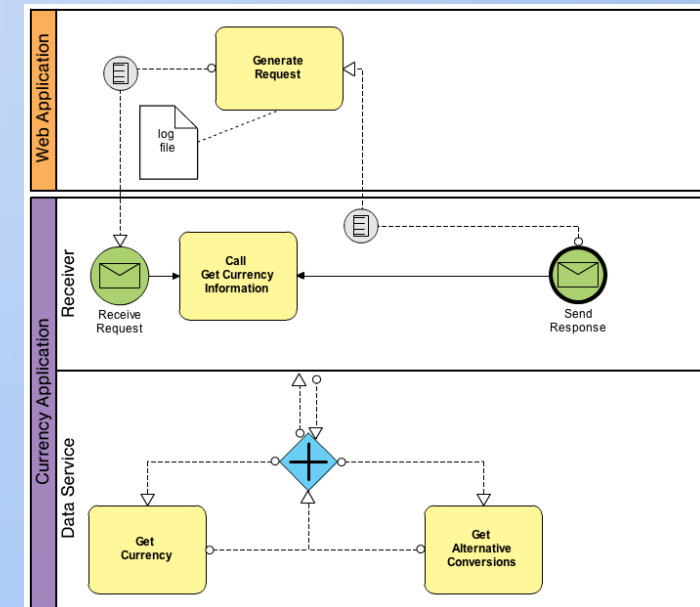
62 SESSÃO PRE-FRAAP

- Resultados do Pre-FRAAP
 - Pré-triagem
 - Utilizar um elemento de avaliação ou a conjugação de vários
 - Escolha dos elementos depende dos propósitos do objecto em análise
 - A conjugação dos elementos determina a necessidade ou não de uma Avaliação de Risco

Impacto Sensibilidade	Alto	Médio	Baixo
Alto	Avaliação Risco	Avaliação Risco	Avaliação Risco
Médio	Avaliação Risco	Avaliação Risco	Implementar Controlos base
Baixo	Avaliação Risco	Implementar Controlos base	n.a.

64 SESSÃO PRE-FRAAP

- Resultados do Pre-FRAAP
 - Diagrama com a descrição/detalhe do sistema ou processo a avaliar
 - Diagrama com a descrição do processo em análise
 - Para documentação e informação da equipa FRAAP
 - “uma imagem vale por mil palavras”
 - Estabelecimento da equipa a incluir no processo
 - Identificar entre 15 a 30 elementos



65 SESSÃO PRE-FRAAP

- Resultados do Pre-FRAAP
 - Requisitos para a reunião FRAAP
 - Agendamento
 - Sala
 - Materiais ...
 - Acordar definições de principio
 - O que é Activo, Ameaça, Vulnerabilidades, Probabilidade, Impacto, Risco, ...

Activo	É um recurso com valor. Pode ser uma pessoa, um processo, informação, ...
Ameaça	É qualquer coisa (acto humano intencional ou não, ou causada pela natureza), que tem o potencial de causar danos
Probabilidade	Quantificação da possibilidade uma dada ameaça acontecer
Impacto	O efeito de uma ameaça sobre um activo, expresso em termos tangíveis ou intangíveis
Vulnerabilidades	É uma fragilidade que pode ser usada para colocar em perigo ou causar danos a um activo de informação
Riscos	Risco é a combinação de ameaça com probabilidade e impacto, expresso em níveis de valor acordados

66 SESSÃO PRE-FRAAP

- Resultados do Pre-FRAAP
 - Mini-Brainstorming
 - No sentido de identificar algumas ameaças como introdução à reunião FRAAP

Confidencialidade	Integridade	Disponibilidade
Dados de cliente podem ser interceptados	Dados podem ser introduzidos (inadvertidamente) incorretamente	Ficheiros guardados em pastas pessoais podem não estar disponíveis
Roubo interno de informação	Programa com falhas pode alterar dados	Falhas de hardware podem ter impacto na disponibilidade servers
Documento papel ou electrónicos podem chegar a pessoas não autorizadas	Introdução intencional de dados errados	Falha no circuito de dados pode impedir acesso a sistema
Informação confidencial deixada à vista na secretária	Falha na reposição de backup	Catástrofes ambientais
Conversas fora do escritório podem divulgar informação sensível	Upgrade de software corrompe base de dados	Upgrades de software podem impedir acesso

67 SESSÃO PRE-FRAAP

- Checklist
para reunião
 - Garantir abordagem de todos os pontos

ISSUE	REMARKS
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>	

68 SESSÃO PRE-FRAAP

- Checklist
para reunião

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>	

69 AGENDA

- Revisão da sessão anterior
 - O Processo FRAAP - Facilitated Risk Analysis and Assessment Process
- O processo de análise de risco FRAAP
 - Etapas do processo
 - Pre-FRAAP
 - FRAAP
 - Post-FRAAP
 - Ferramentas de apoio ao processo
 - Exercício Prático

70 SESSÃO FRAAP

- Sessão de trabalho
 - Não deve durar mais que quatro horas
 - É suficiente, na maioria dos casos
 - Difícil arranjar mais disponibilidade
 - Envolver todos os elementos da equipa
 - Identificados no Pre-FRAAP
 - E devidamente convocados

71 SESSÃO FRAAP

- FRAAP
 - Resultados esperados
 - Identificação das Ameaças
 - Identificação das Vulnerabilidades
 - Identificação dos Controlos Existentes
 - Calculo dos Riscos
 - Identificação de novos controlos
 - Caracterização dos Riscos Residuais



72 SESSÃO FRAAP

- Sessão de trabalho
 - Requisitos da reunião
 - Assegurar materiais necessários
 - Projector
 - Quadro
 - Canetas
 - Disposição da Sala em U
 - Importante para assegurar a participação de todos
 - Todos estão na linha da frente, com o facilitador
 - Desencorajar a utilização de portáteis ou PDAs
 - Lembrar para desligar os telemóveis
 - Ou colocar em silêncio

73 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

09/04/22

74 SESSÃO FRAAP

- Sessão de trabalho - Introdução
 - Explain the FRAP process and cover definitions
 - Responsável de negócio irá
 - Abrir a sessão
 - Introduzir o facilitador
 - Facilitador deverá
 - Apresentar a agenda
 - Explicar o processo
 - Review scope statement - Owner
 - Importante identificar
 - O que foi assumido
 - Constrangimentos identificados
 - Deve ser entregue uma cópia do Scope Statment à equipa



75 SESSÃO FRAAP

- Sessão de trabalho - Introdução
 - Review Visual Diagram – Technical support
 - Deve fazer a apresentação do diagrama, explicando o processo
 - Cerca de 5 min.
 - Discuss definitions - Facilitator
 - Apresenta as definições acordadas
 - Se o processo já é conhecido na organização, estas definições já devem estar interiorizadas



Activo	É um recurso com valor. Pode ser uma pessoa, um processo, informação, ...
Ameaça	É qualquer coisa (acto humano intencional ou não, ou causada pela natureza), que tem o potencial de causar danos
Probabilidade	Quantificação da possibilidade uma dada ameaça acontecer
Impacto	O efeito de uma ameaça sobre um activo, expresso em termos tangíveis ou intangíveis
Vulnerabilidades	É uma fragilidade que pode ser usada para colocar em perigo ou causar danos a um activo de informação
Riscos	Risco é a combinação de ameaça com probabilidade e impacto, expresso em níveis de valor acordados

76 SESSÃO FRAAP

- Sessão de trabalho - Introdução
 - Review Objectives - Facilitator
 - São revistos os objectivos a atingir
 - Identificar ameaças
 - Estabelecer níveis de risco
 - Identificar controlos
 - Serve como introdução à segunda parte da sessão

77 SESSÃO FRAAP

- Sessão de trabalho - Introdução
 - Identify roles and introduction - team
 - Os elementos da equipa identificam-se
 - Nome
 - Departamento
 - Localização
 - Contacto

78 SESSÃO FRAAP

- Sessão de trabalho - Introdução
 - Review session agreements
 - Todos os elementos devem participar
 - Devem cingir-se aos seus papéis
 - Focar-se no ponto da agenda
 - Todas as ideias têm um valor igual
 - Escutar os outros pontos de vista
 - Todas as questões/contributos serão registados
 - Mesmo os que forem preteridos
 - Colocar e registar a ideia, antes de discuti-la
 - Assegurar que o escriba assenta todas as questões
 - Uma temática (C-I-D) de cada vez
 - Limite de tempo por ativo/atividade (3 a 5 minutos)



79 SESSÃO FRAAP

- Condução da reunião
 - Idealmente deve ser respeitada a disposição em U
 - O facilitador deve começar por colocar o primeiro atributo em discussão, colocando os resultados do mini-brainstorming

<u>Confidencialidade</u> assegurar que a informação não é acedida ou divulgada a pessoas que não devem ter acesso
Dados de cliente podem ser interceptados
Roubo interno de informação
Documento papel ou electrónicos podem chegar a pessoas não autorizadas
Informação confidencial deixada à vista na secretária
Conversas fora do escritório podem divulgar informação sensível

80 SESSÃO FRAAP

- Condução da reunião
 - Solicitar a participação de todos na identificação de ameaças
 - Dar 3 a 5 minutos para pensar em possíveis ameaças
 - Começar numa ponta
 - Percorrer todos
 - Cada elemento só sugere 1 ameaça de cada vez
 - Dar várias voltas até que se esgotem as sugestões
 - Ter em atenção
 - Os manipuladores
 - Centrar no tópico em discussão



81 SESSÃO FRAAP

- Condução da reunião
 - Passar ao segundo atributo
 - Começar na outra ponta
 - Utilizar cores diferentes
 - Ir colocando anotações à volta da sala

Integridade Assegurar a precisão, consistência e confiabilidade da informação
Dados podem ser introduzidos (inadvertidamente) incorretamente
Programa com falhas pode alterar dados
Introdução intencional de dados errados
Falha na reposição de backup
Upgrade de software corrompe base de dados

82 SESSÃO FRAAP

- Utilização de Checklists
 - Para ameaças
 - Para controlos
 - Permite reduzir o tempo de identificação
 - Complementa a identificação feita pelos elementos da equipa

83 SESSÃO FRAAP

- Threats Checklists
 - consultar ISO 27005
 - Ou/e Appendix G
 - Table G.1 Sample Threat Checklist
 - Table G.2 Natural Threat List

Threat	Applicable Yes/No
Integrity	
Data stream could be intercepted.	
Faulty programming could (inadvertently) modify data.	
Copies of reports could be diverted (written or electronically) to unauthorized or unintended persons.	
Data could be entered incorrectly.	
Intentional incorrect data entry.	
Use of outdated programs could compromise integrity of information.	
Faulty hardware could result in inaccurate data entry and analysis.	
Third parties could modify data.	
Files could be accidentally deleted.	
Hackers could change data.	
Internal Users could launch unauthorized programs to access and or modify bank data.	
Reports could be falsified	
Internal theft of information by employees could be modified and used later.	
Network sniffing could intercept user passwords and allow unauthorized modification of information	
Information could be outdated.	
Hackers could obtain unauthorized access into network to corrupt system resources.	
Physical intrusion by unauthorized persons.	
Documents could be falsified to appear as official company documents.	
Unauthorized or fictitious sales could be approved.	
Information could be misinterpreted due to language barriers.	
Fraudulent programming could impact data integrity, example: hidden hooks.	
Computer viruses could modify data.	
Information could be misdirected.	
Transactions could be intentionally not run or misrouted.	
Newer or upgraded software could cause corruption of documents or files.	
Non-standard procedures could cause misinterpretation of information.	
Unauthorized persons may use an unattended workstation.	
Information to and from 3rd parties could be corrupted in transmission.	
Account Information may be shared.	
A power failure could corrupt information.	
Information could be submitted in a vague or misleading manner.	
Someone could impersonate a customer to corrupt records (identity theft).	
Information could be taken outside the company	
Integrity of information could be compromised due to decay of information	

84 SESSÃO FRAAP

- Threats Checklists
 - Table G.I Sample Threat Checklist

Threat
Human - Accidental
Fire: Internal-major
Fire: Internal-Catastrophic
Fire: External
Accidental explosion – on site
Accidental explosion – off site
Aircraft crash
Train crash
Derailment
Auto/Truck crash at site
Fire: Internal-minor
Human error – maintenance
Human error – operational
Human error – Programming
Human error – users
Toxic contamination
Medical emergency
Loss of key staff

Threat
Human - Deliberate
Sabotage/Terrorism: External - Physical
Sabotage/Terrorism: Internal - Physical
Terrorism: Biological
Terrorism: Chemical
Bombing
Bomb Threat
Arson
Hostage taking
Vandalism
Labor dispute/Strike
Riot/Civil disorder
Toxic contamination

85 SESSÃO FRAAP

- Antes do próximo ponto, fazer pausa
 - Dá oportunidade para
 - Verificar mensagens
 - Tomar um café
 - Limpar

86 SESSÃO FRAAP

- Identificação de Controlos existentes
 - Rever todas as ameaças identificando os controlos existentes
 - Esta caracterização permite à equipa identificar melhor o risco actual
 - Razão pela qual é fundamental ter elementos da infra-estrutura
 - Conhecem os controlos actuais

<i>Threat</i>	<i>Existing Control</i>
Confidentiality	
Insecure e-mail could contain confidential information	
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
Employee is not able to verify the identity of a client (e.g., phone masquerading)	

87 SESSÃO FRAAP

- Estabelecimento do nível de risco
 - Verificar se os elementos da equipa estão familiarizados com os termos e definições de Probabilidade e Impacto
 - Resumir as ameaças e controlos existentes
 - Caracterizar os níveis de avaliação para
 - Probabilidade
 - Impacto
 - Explicar os níveis de avaliação
 - Quando existe risco, os elementos tendem a classificar com nível máximo

88 SESSÃO FRAAP

- Estabelecimento do nível de risco
 - Definições e níveis de avaliação
 - Probabilidade

<i>Term</i>	<i>Definition</i>
Probability	Chance that an event will occur or that a specific loss value may be attained should the event occur
High	Very likely that the threat will occur within the next year
Medium	Possible that the threat may occur within the next year
Low	Highly unlikely that the threat will occur within the next year

- Impacto

<i>Term</i>	<i>Definition</i>
Impact	A measure of the magnitude of loss or harm on the value of an asset
High	Entire mission or business impacted
Medium	Loss is limited to single business unit or objective
Low	Business as usual

89 SESSÃO FRAAP

- Estabelecimento do nível de risco
 - Definições e níveis de avaliação
 - Matriz de probabilidade x impacto
 - Caracterizar o risco residual

		IMPACT		
P R O B A B I L I T Y		High	Medium	Low
	High	A	B	C
	Medium	B	B	C
	Low	C	C	D

A - Corrective action must be implemented
B - Corrective action should be implemented
C - Requires monitor
D - No action required at this time

90 SESSÃO FRAAP

- Estabelecimento do nível de risco
 - Avaliação das ameaças e controlos identificados

<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>
Confidentiality				
Insecure e-mail could contain confidential information		3	3	High
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

91 SESSÃO FRAAP

- Identificar novos controlos ou melhoria dos existentes
 - Para os riscos que requerem essa necessidade
 - Identificados em conjunto com o owner
 - (vantagem em envolver os utilizadores)

<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>
Confidentiality					
Insecure e-mail could contain confidential information		3	3	High	Information classification policy and handling standards are being implemented
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	

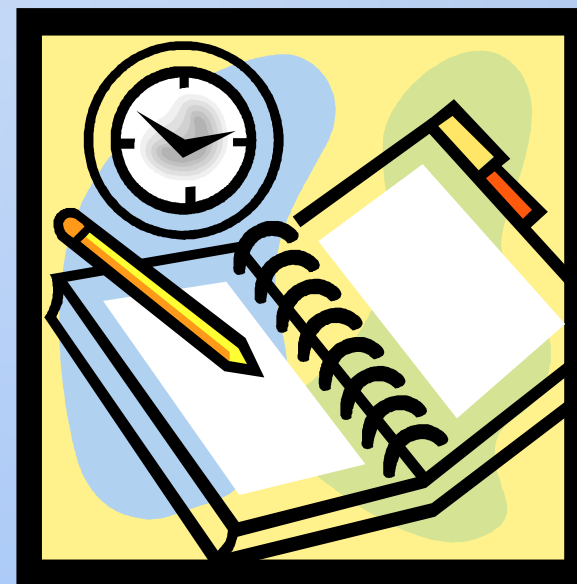
92 SESSÃO FRAAP

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

93 SESSÃO FRAAP

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



94 SESSÃO FRAAP

- Estabelecimento do nível de risco
 - Na implementação de controlos, devem ser consideradas as normas e legislação em vigor:
 - Information Technology – Code of Practice for Information Security Management (ISO/IEC 27002)
 - “Security Technologies for Manufacturing and Control Systems” (ISA-TR99.00.01-2004)
 - “Integrating Electronic Security into Manufacturing and Control Systems Environment” (ISA-TR99.00.02-2004)
 - Federal Information Processing Standards Publications (FIPS Pubs)
 - National Institute of Standards and Technology
 - CobiT® Security Baseline
 - Health Insurance Portability and Accountability Act (HIPAA)
 - The Basel Accords
 - Privacy Act of 1974
 - Gramm–Leach–Bliley Act (GLBA)
 - Sarbanes–Oxley Act (SOX)
 - “Information Security for Banking and Finance” (ISO/TR 13569)
 - FFEIC examination guidelines

95 PROCESSO DE ANÁLISE DE RISCO FRAAP

- Post-FRAAP
 - Realizado pela equipa de consultores
 - 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



96 PROCESSO DE ANÁLISE DE RISCO FRAAP

- Post-FRAAP
 - Relatório final
 - com sumário executivo
 - Resumo da reunião de equipa
 - Identificação de controlos complementares
 - Análise do processo
 - Apresentação das conclusões ao Gestor de Negócio



97 METODOLOGIAS DE GESTÃO DE RISCO

- Para suporte à Gestão de Risco pode ser utilizados referenciais como
 - ISO/IEC 27001 - Information security management systems – Requirements
 - ISO/IEC 27002 - Information technology- Security techniques - code of practice for information security management
 - ISO/IEC 27005:2011 Information technology - Security techniques - Information security risk management
 - SP800-30 (NIST) - Risk Management Guide for Information Technology Systems
 - Referenciais locais ou sectoriais como:
 - CRAMM (UK.Telcos)
 - Dutch A&K analysis (Holanda)
 - MAGERIT (Espanha)
 - MIGRA (Itália)
- Link de referência: http://rm-inv.enisa.europa.eu/rm_ra_methods.html

SEGURANÇA E GESTÃO DE RISCO

2ºSEM 2021/22

MODELO DE SEGURANÇA INTEGRADO

PROCESSO DE AVALIAÇÃO DOS RISCOS

LUIS AMORIM

09 Abr 2022