SEGURANÇA E GESTÃO DE RISCO

2ºSEM 2020/21

PROCESSOS E SERVIÇOS DE SEGURANÇA

LUIS AMORIM

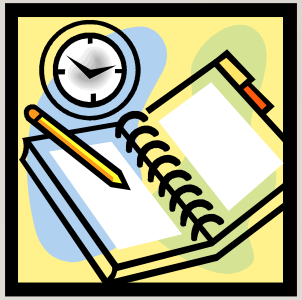
22 Mai 2021

2 AGENDA

- Revisão do processo de análise de risco FRAAP
  - Etapas do processo
    - Pre-FRAAP
    - FRAAP
    - Post-FRAAP
- Ferramentas de Suporte à Gestão dos Riscos
- BusinessImpactAnalysis(BIA)
- GAP Analisys
- Definir uma Política de Segurança

3 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



4 PROCESSO DE ANÁLISE DE RISCO FRAAP

- Pre-FRAAP
  - Resultados esperados
    - (pré) Triagem dos sistemas/processos
    - 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 *Record when and where the meeting is scheduled*
2. Project Executive Sponsor or Owner *Identify the owner or sponsor who has executive responsibility for the project*
3. Project Leader *Identify the individual who is the primary point of contact for the project or asset under review*
4. Pre-FRAAP Meeting Objective *Identify what you hope to gain from the meeting – typically the seven deliverables will be discussed*
5. Project Overview *Prepare a project overview for presentation to the pre-FRAAP members during the meeting*
Your understanding of the project scope
The FRAAP methodology
Milestones
Pre-screening methodology
6. Assumptions *Identify assumptions used in developing the approach to performing the FRAAP project*
7. Pre-screening Results *Record the results of the pre-screening process*

DURING THE MEETING
8. Business Strategy, Goals and Objectives *Identify what the owner's objectives are and how they relate to larger company objectives*
9. Project Scope *Define specifically the scope of the project and document it during the meeting so that all participating will know and agree*
• **Applications/Systems**
• **Business Processes**
• **Business Functions**
• **People and Organizations**
• **Locations/Facilities**
10. Time Dependencies *Identify time limitations and considerations the client may have*
11. Risks/Constraints *Identify risks and/or constraints that could affect the successful conclusion of the project*
12. Budget Identify any open budget/funding issues
13. FRAAP Participants *Identify by name and position the individuals whose participation in the FRAAP session is required*
14. Administrative Requirements *Identify facility and/or equipment needs to perform the FRAAP session*
15. Documentation *Identify what documentation is required to prepare for the FRAAP session (provide the client the FRAAP Document Checklist)*

5 PROCESSO DE ANÁLISE DE RISCO FRAAP

- 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

6 SESSÃO FRAAP

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

Threat	*Existing Control*	*Probability 1 = Low 2 = Medium 3 = High*	*Impact 1 = Low 2 = Medium 3 = High*	*Risk Level*
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

7 SESSÃO FRAAP

- Tratamento dos riscos
  - 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)

Threat	*Existing Control*	*Probability 1 = Low 2 = Medium 3 = High*	*Impact 1 = Low 2 = Medium 3 = High*	*Risk Level*	*New or Enhanced Selected Control*
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	

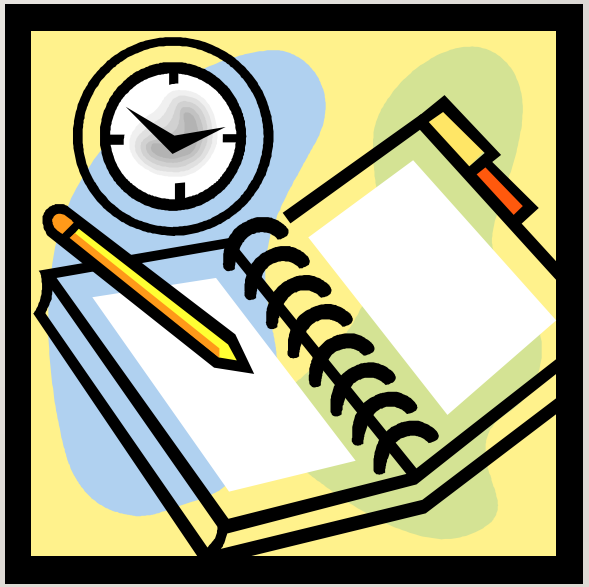
8 SESSÃO FRAAP

- Tratamento dos riscos
  - Calcular os novos níveis de risco
    - Considerando a implementação dos controlos identificados

Threat	*Existing Control*	*Probability 1 = Low 2 = Medium 3 = High*	*Impact 1 = Low 2 = Medium 3 = High*	*Risk Level*	*New or Enhanced Selected Control*	*New Risk Level*
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		

9 SESSÃO FRAAP

- Tratamento dos Riscos
  - Prioritizar implementação de controlos
  - Planear essa implementação



10 SESSÃO FRAAP

- Tratamento dos Riscos
  - Na implementação de controlos, devem ser consideradas as normas e legislação em vigor:
    - Information Technology – Code of Pratice 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

11 PROCESSO DE ANÁLISE DE RISCO FRAAP

- 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

12 SUMÁRIO EXECUTIVO

- Exemplo de Sumário executivo
  - 1 (a 2) páginas
  - Principais conclusões
  - Apelando (e apontando) para o resto do documento

A rapidez na implantação de novos serviços é, muitas vezes, a chave para o sucesso em muitas áreas de negócio. Contudo, em várias ocasiões, a necessidade de minimizar o período de implantação dos serviços faz esquecer os possíveis riscos que a rede representa para a integridade dos dados corporativos.

Nesse sentido, foi efectuado um levantamento exaustivo na RUTV (documento "Levantamento e Planeamento de Actividades", apresentado pela XKT), de forma a detectar as fraquezas no que diz respeito a redes e equipamentos de comunicação, serviços de rede e sistemas operativos.

No que diz respeito aos serviços de rede, a proliferação de serviços activos que não são necessários e a falta de configuração de alguns deles comprometem seriamente a segurança.

No que diz respeito aos sistemas operativos, encontrámos fraquezas devido às configurações *out of the box*, aos privilégios inadequados ou aos sistemas de ficheiros inseguros.

Estes são apenas alguns exemplos, no que diz respeito à segurança, da situação actual da infra-estrutura informática do RUTV.

Sendo que a segurança da informação não se restringe aos equipamentos informáticos e de comunicação, foi realizada uma avaliação de segurança, tendo sido identificados os activos da RUTV a proteger, ameaças e vulnerabilidades a que estão expostos. Da análise efectuada foram elaboradas recomendações com o objectivo de minimizar os danos potenciais associados à concretização das ameaças.

As recomendações elaboradas abordam a vertente de segurança organizacional, segurança física e ambiental, controlo e classificação dos activos informacionais, sistemas de informação, e assegurar a continuidade do negócio, sendo as principais fraquezas identificadas as seguintes:

- Ausência de uma abordagem global à segurança da informação;
- Reduzida segurança física das instalações de processamento de informação;
- Antivírus não instalado em todas as máquinas e sem as necessárias actualizações;
- Ausência de um plano de recuperação em caso de desastre;
- Inexistência de procedimentos documentados para a operação e administração de sistemas e redes.

13 METODOLOGIAS DE GESTÃO DE RISCOS

- 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)

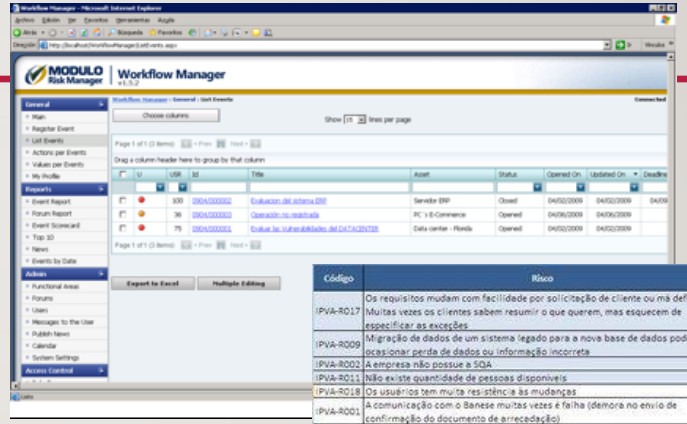
  - Link de referência: http://rm-inv.enisa.europa.eu/rm_ra_methods.html

15 AGENDA

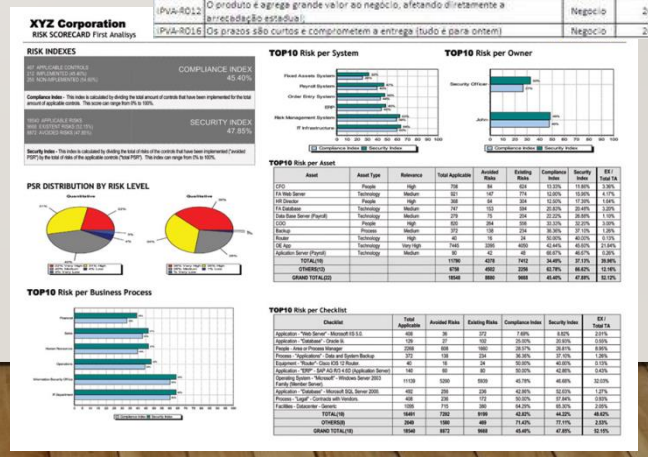
- Revisão do processo de análise de risco FRAAP
  - Etapas do processo
    - Pre-FRAAP
    - FRAAP
    - Post-FRAAP
- ➢ Ferramentas de Suporte à Gestão dos Riscos
- Business Impact Analysis(BIA)
- GAP Analisys
- Definir uma Política de Segurança

16 FERRAMENTAS DE SUPORTE

- Modulo
  - Risk Management
    - Risk assessment
      - Risk identification
      - Risk analysis
      - Risk Evaluation:
    - Risk treatment
    - Risk acceptance
    - Risk communication
  - E também:
    - Asset Inventory & Evaluation
    - Compliance Module with standards and regulations
    - Business Continuity Plan
    - Geo-referenced risk: Risk map with Google Earth
    - Ou
      - WEB Interview: For remote usage.
      - PDA use
      - Live Up-date

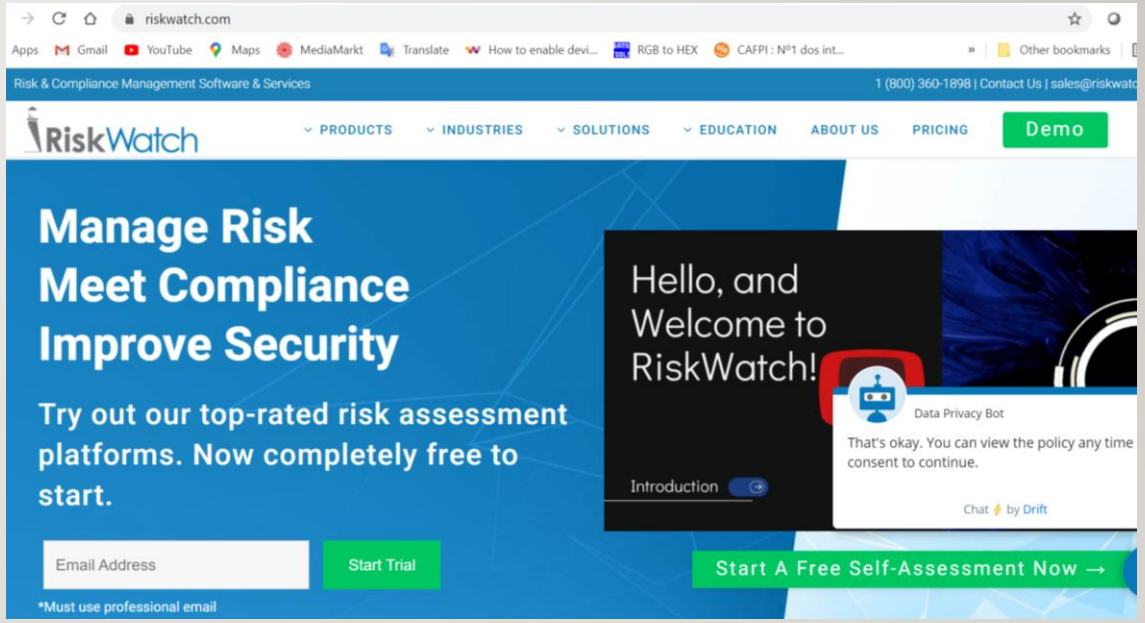


Código	Risco	Categoria	Probabilidade	Impacto
IPVA-R017	Os requisitos mudam com facilidade por solicitação de cliente ou má definição. Muitas vezes os clientes sabem resumir o que querem, mas esquecem de especificar as exceções	Cliente	80	5
IPVA-R009	Migração de dados de um sistema legado para a nova base de dados pode ocasionar perda de dados ou informação incorreta	Negocio	20	5
IPVA-R002	A empresa não possue a SQA	Processo	70	4
IPVA-R011	Não existe quantidade de pessoas disponíveis	Pessoal	60	4
IPVA-R018	Os usuários tem muita resistência às mudanças	Cliente	30	3
IPVA-R001	A comunicação com o Banese muitas vezes é falha (demora no envio de confirmação do documento de arrecadação)	Tecnologia	10	3
IPVA-R004	As ferramentas utilizadas não são integradas	Tecnologia	10	3
IPVA-R006	Existe padronização mas não é seguida pelas equipes	Processo	70	2
IPVA-R014	Os clientes não compreende o conceito de Engenharia de Software	Cliente	60	2
IPVA-R005	Como se trata de legislação estadual sempre estão ocorrendo mudanças	Tamanho	50	2
IPVA-R015	Os clientes não tem sofisticação tecnológica	Cliente	50	2
IPVA-R019	Tanto a SEFAZ como o DETRAN utilizará o sistema simultaneamente	Tamanho	50	2
IPVA-R003	A tecnologia de comunicação utilizada com o Detran, Web Services, não é dominada pela equipe	Tecnologia	40	2
IPVA-R008	Falta de treinamento	Pessoal	40	2
IPVA-R007	Existe risco de saída de pessoal por não existir estabilidade (Setor público)	Pessoal	20	2
IPVA-R010	Migração de sistema legado em Natual/Adabas para Ambiente Web (Java J2EE)	Tecnologia	10	2
IPVA-R013	O sistema tem que se comunicar com o sistema do Detran, com o Banese e com os outros módulos do sistema Fazendário	Negocio	10	2
IPVA-R020	Tempo de resposta para o volume de processamento se tratando de Web	Tecnologia	10	2
IPVA-R012	O produto é agrega grande valor ao negócio, afetando diretamente a arrecadação estadual;	Negocio	20	1
IPVA-R016	Os prazos são curtos e comprometem a entrega (tudo é para ontem)	Negocio	20	1



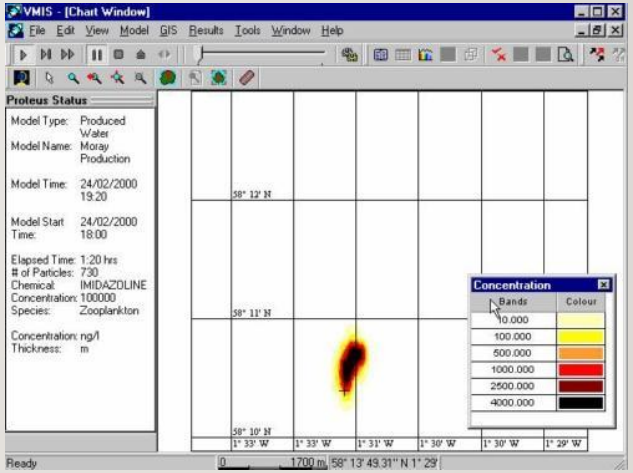
17 FERRAMENTAS DE SUPORTE

- RiskWatch
  - Risk Management
    - Risk assessment
      - Risk identification
      - Risk analysis
      - Risk Evaluation:
    - Risk treatment : Phase III : Define safeguard details
    - Risk acceptance : Phase III : "what-if" scenarios



18 FERRAMENTAS DE SUPORTE

- Proteus
  - Risk Management
    - Risk assessment
      - Risk identification
      - Risk analysis
      - Risk Evaluation:
    - Risk treatment
    - Risk acceptance
    - Risk communication
  - E também:
    - Asset Inventory & Evaluation
    - Document Management
    - Business Continuity
    - Remote auditing: Distribute questionnaires
    - Incident Management
    - Automated Alert MAnagement (SMS and email)



infogov.

19 AGENDA

- Revisão do processo de análise de risco FRAAP
  - Etapas do processo
    - Pre-FRAAP
    - FRAAP
    - Post-FRAAP
- Ferramentas de Suporte à Gestão dos Riscos
- ➢ Business Impact Analysis(BIA)
- GAP Analisys
- Desenvolver uma Política de Segurança

20 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)

21 BUSINESS IMPACT ANALYSIS (BIA)

- Como conclusão do processo de triagem (ou pré-triagem) pode ser requerida a realização de (Exemplo 3 do livro)
  - Análise de Riscos + processo de Business Impact Analysis
  - Ou para impactos mais baixos
    - Aplicação de controlos base
    - Ou um processo base de BIA (p.e. com requisitos base de recuperação)

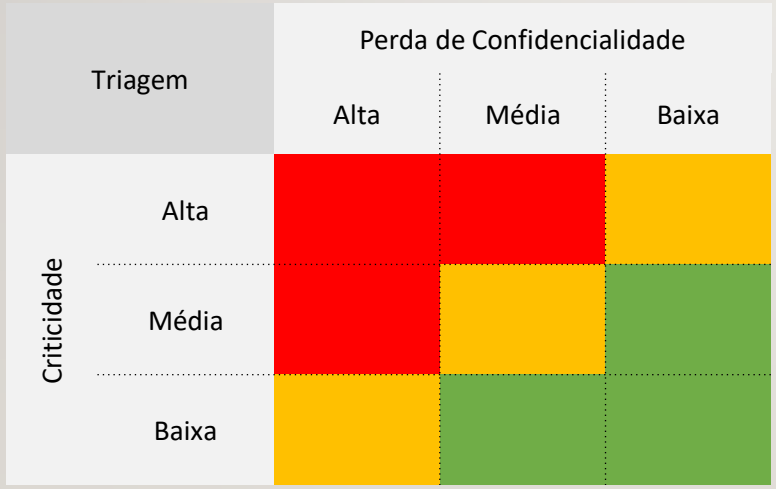
Disclosure Impact Level	*Definition*
High	Information is of such a nature that its unauthorized disclosure would cause media attention and negative customer response.
Medium	Information is of such a nature that its unauthorized disclosure might cause media attention and negative customer response.
Low	Information is of such a nature that its unauthorized disclosure would have little or no impact on the organization.

Criticality Impact Level	*Definition*
High	Information is of such a nature that its unauthorized modification or destruction would cause media attention and negative customer response.
Medium	Information is of such a nature that its unauthorized modification or destruction might cause media attention and negative customer response.
Low	Information is of such a nature that its unauthorized modification or destruction would have little or no impact on the organization.

Criticality \ Disclosure	High	Medium	Low
High	6- BIA & Risk Assessment	5- BIA & Risk Assessment	4- BIA & Baseline Controls
Medium	5- BIA & Risk Assessment	4- BIA & Risk Assessment	3- Baseline BIA & Controls
Low	4- R/A & BIA Baseline	3- Baseline BIA & Controls	2- Baseline BIA & Controls

22 BUSINESS IMPACT ANALYSIS (BIA)

- Processo de triagem

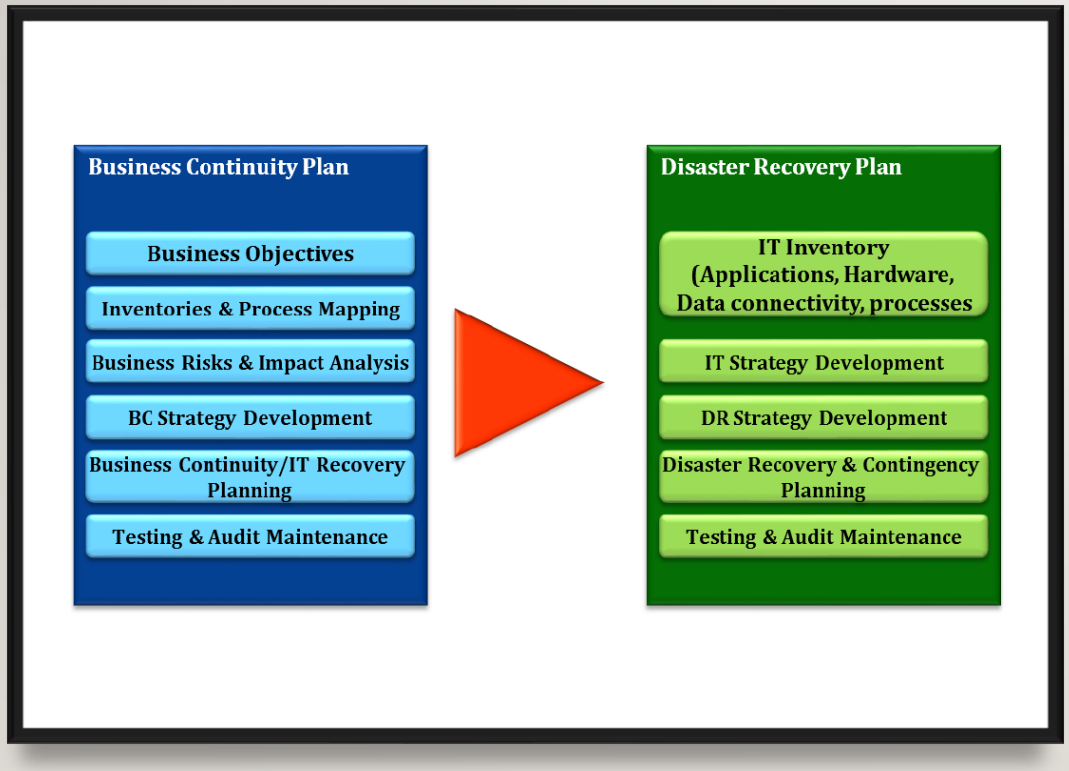


Triagem para Avaliação dos Riscos
Requer Avaliação dos Riscos
Requer implementação de controlos de segurança Base
Não requer intervenção

Triagem para Processo de BIA
Requer BIA (com caraterização de requisitos de continuidade)
Implica implementação de requisitos básicos
Não requer intervenção

Triagem para Processo de Avaliação de Riscos e BIA
Requer Avaliação dos Riscos e BIA
Implica implementação de controlos e requisitos básicos
Não requer intervenção

23 BUSINESS IMPACT ANALYSIS(BIA)



- Os resultados do Business Impact Analysis são importantes no estabelecimento de
  - Planos de Continuidade de Negócio
    - Disaster Recovery

24 BUSINESS IMPACT ANALYSIS (BIA)

- Um processo de Continuidade de Negócio tem 3 fases
  - Resposta
  - Recuperação
  - Reposição

- BIA tem reflexo direto na fase de Recuperação
  - É preciso conhecer os processos críticos de negócio
  - E, assim, saber quais devem ser recuperados primeiro

25 BUSINESS IMPACT ANALYSIS(BIA)

- Durante o processo é preciso definir quais os possíveis impactos para o negócio

Category	*If the Asset Was Unavailable:*
Competitive disadvantage	What would be the impact to our competitive standing?
Direct business loss	What would be the impact to our business revenues or profits?
Loss of public confidence or reputation	What would be the impact to our customer confidence, public image, or shareholder or supplier loyalty?
Poor morale	What would be the impact to our employee morale?
Fraud	What level of goods, services, or funds would be diverted?
Wrong management decisions	What would be the impact to management having access to information to make informed business decisions?
Business disruption	What other applications, programs, systems, or business processes would be impacted?
Legal liability	Could the organization be in breach of legal, regulatory, or contractual obligations?
Privacy loss	Could our customers, clients, or employees suffer loss of personal privacy information?
Safety risk	What would be the impact to our customers', clients', and employees' health and safety?

26 BUSINESS IMPACT ANALYSIS(BIA)

- Impactos podem causar
  - Perdas Intangíveis
  - Perdas Tangíveis

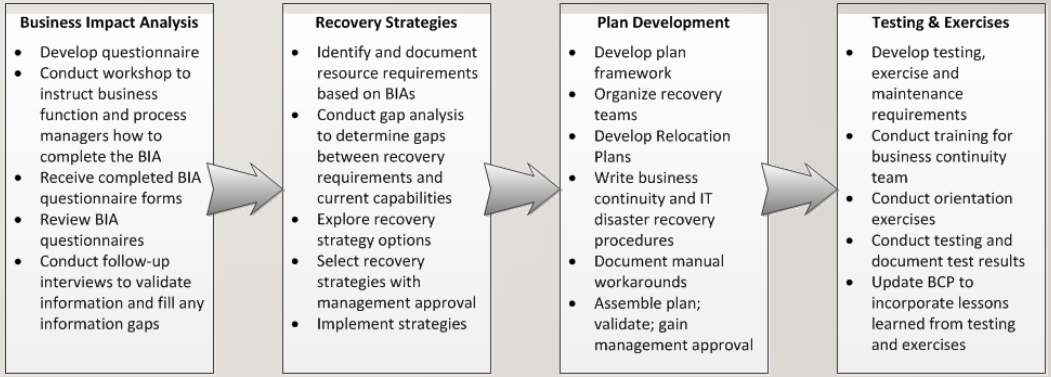
Impact Value	*Intangible Loss (Dollar Loss Difficult to Estimate)*				*Tangible Loss*
	Health and Safety	*Interruption of Production Impact*	*Public Image*	*Environmental Release*	*Financial*
1	Loss of life or limb	1 week	Total loss of public confidence and reputation	Permanent damage to environment	More than $10M
2	Requires hospitalization	3 days	Long-term blemish of company image	Long-term (1 year or more) damage to environment	$1,000,001–$10M
3	Cuts, bruises, requires first aid	1–2 days	Temporary blemish of company image	Temporary (6 months to 1 year) damage	$100,001–$1M
4	Major exposure to unsafe work environment	1 day	Company business unit image damaged	Department noncompliant	$50,001–$100,000
5	Little or no negative impact Minor exposure to unsafe work environment	<4 hours	Little or no image impact	Little or no impact	$0–$50,000

27 BUSINESS IMPACT ANALYSIS(BIA)

- 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

28 BUSINESS IMPACT ANALYSIS(BIA)

- Aplicar os resultados do BIA
  - Para estabelecer estratégias de recuperação
  - Estabelecer ou rever os planos de Continuidade
    - Se o tempo máximo de *downtime* for inferior ao definido anteriormente



29 BUSINESS IMPACT ANALYSIS(BIA)

Business Impact Analysis
- Develop questionnaire
- Conduct workshop to instruct business function and process managers how to complete the BIA
- Receive completed BIA questionnaire forms
- Review BIA questionnaires
- Conduct follow-up interviews to validate information and fill any information gaps

Recovery Strategies
- Identify and document resource requirements based on BIAs
- Conduct gap analysis to determine gaps between recovery requirements and current capabilities
- Explore recovery strategy options
- Select recovery strategies with management approval
- Implement strategies

Plan Development
- Develop plan framework
- Organize recovery teams
- Develop Relocation Plans
- Write business continuity and IT disaster recovery procedures
- Document manual workarounds
- Assemble plan; validate; gain management approval

Testing & Exercises
- Develop testing, exercise and maintenance requirements
- Conduct training for business continuity team
- Conduct orientation exercises
- Conduct testing and document test results
- Update BCP to incorporate lessons learned from testing and exercises

- No final
  - Testar
  - Exercitar os Planos de Continuidade

31 AGENDA

- Revisão do processo de análise de risco FRAAP
  - Etapas do processo
    - Pre-FRAAP
    - FRAAP
    - Post-FRAAP
- Ferramentas de Suporte à Gestão dos Riscos
- BusinessImpactAnalysis(BIA)
- GAP Analisys
- Definir uma Política de Segurança

32 GAP ANALYSIS

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

- Para tal é preciso resposta para:
  - O que precisa ser feito para ficar no estado desejado
    - Ou estado "compliant", quando numa auditoria/certificação
  - Qual o estado actual
  - O que é preciso ser feito, para atingir o estado de conformidade/compliance

33 GAP ANALYSIS

- É importante ter os requisitos legais ou normas a cumprir devidamente mapeados
  - Começar por elaborar essa listagem
  - Pode ser realizado o GAP Analysis
    - Por cada norma ou requisito legal

The following is a list of the SANS Standards that every fire company should have for reference purposes. This list is taken from the SAQCC (Fire) Manual and is regarded as being the minimum that is needed in order to carry out effective reconditioning of fire equipment. All standards are subject to revision and any reference to a standard is deemed to be a reference to the latest edition of that standard.

SANS 1475-1	The production of reconditioned fire-fighting equipment. Part 1: Portable & wheeled (mobile) rechargeable fire extinguishers.
SANS 1475-2	The production of reconditioned fire-fighting equipment. Part 2: Fire hose reels and above-ground hydrants.
SANS 10105-1	The use and control of fire-fighting equipment. Part 1: Portable and wheeled (mobile) fire extinguishers.
SANS 10105-2	The use and control of fire-fighting equipment. Part 2: Fire hose reels, hydrants and booster connections.
SANS 543	Fire hose reels (with semi-rigid hose).
SANS 1128-1	Fire fighting equipment – Part 1: Components of underground and above-ground hydrant systems.
SANS 1151	Portable rechargeable fire extinguishers – Halogenated hydro carbon type.
SANS 1322	Portable non-refillable fire extinguishers – General purpose type.
SANS 1567	Portable rechargeable fire extinguishers – CO_2 type.
SANS 1825	Portable gas cylinder test stations – Approval and general requirements.
SANS 1910	Portable refillable fire extinguishers.
SANS 10019	Transportable metal containers for compressed gas – Basic design, manufacture, use and maintenance.
SANS 10400-T	The application of the National Building Regulations. Part T: Fire protection.
SANS 10400-W	The application of the National Building Regulations. Part W: Fire installation.

34 GAP ANALYSIS

- Implementação de segurança ISO27002
  - Necessário avaliar o cumprimento de
    - 14 capítulos
    - Com total de 114 controlos

5. Security Policy Management

5.1 Establish a comprehensive information security policy

5.1.1 Information security policy document

Control: An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.

5.1.2 Review your information security policy

Control: The information security policy should be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

35 GAP ANALYSIS

- Cumprimento da ISO27002

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

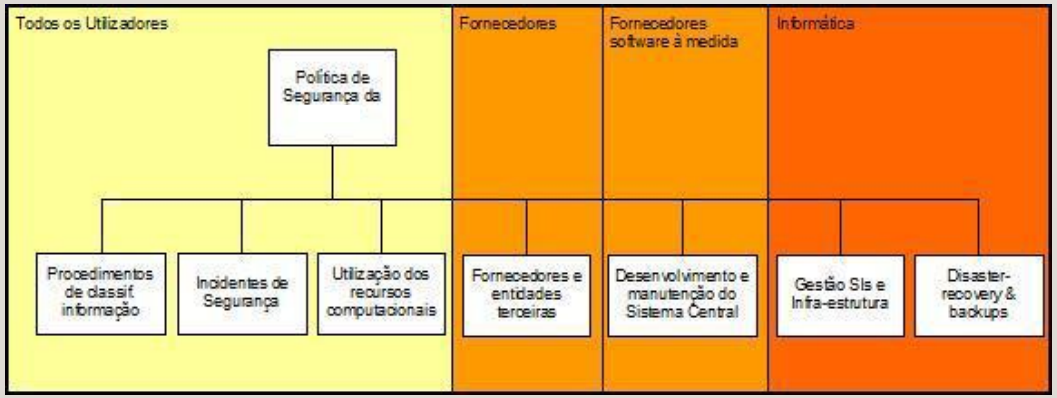
36 AGENDA

- Revisão do processo de análise de risco FRAAP
  - Etapas do processo
    - Pre-FRAAP
    - FRAAP
    - Post-FRAAP
- Ferramentas de Suporte à Gestão dos Riscos
- BusinessImpactAnalysis(BIA)
- GAP Analisys

➢ Definir uma Política de Segurança

37 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 especificas relativamente à administração de sistemas destinam-se apenas aos técnicos da Informática).
  - Face ao negócio, estrutura orgânica e recomendações efectuadas, é proposta a seguinte organização para os elementos constitutivos da Política de Segurança:



38 IMPLEMENTAÇÃO DE POLÍTICA DE SEGURANÇA

- Definição de Política de Segurança

Política de Segurança da Informação

A Segurança da Informação da XXX apoia-se nos princípios básicos da segurança da informação, nomeadamente no que respeita à preservação da Confidencialidade, Integridade e Disponibilidade, em particular nos projetos de desenvolvimento seguro.

A XXX obriga-se a cumprir as disposições do Sistema de Gestão da Segurança da Informação e a regular a sua atividade no sentido de assegurar:

1. A certificação ISO/IEC 27001, aliando a empresa às melhores práticas de segurança da informação;
2. Um serviço de qualidade aos seus clientes regido pelo cumprimento das melhores práticas de segurança da informação;
3. A implementação de controlos de segurança que contribuam para manter a confidencialidade, integridade e disponibilidade da informação e sistemas de informação da XXX;
4. Que os seus colaboradores têm a formação e os conhecimentos adequados, contribuindo para o incremento da segurança e da qualidade dos serviços prestados aos clientes da XXX;
5. A caraterização e tratamento adequado de potenciais eventos e incidentes de segurança;
6. A melhoria contínua dos processos de gestão segurança da informação.

Esta política encontra-se alinhada com os objetivos de segurança identificados.

39 IMPLEMENTAÇÃO DE POLÍTICA DE SEGURANÇA

- **Políticas específicas**
  - 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

44

SEGURANÇA E GESTÃO DE RISCO

2ºSEM 2020/21

PROCESSOS E SERVIÇOS DE SEGURANÇA

LUIS AMORIM

22 Mai 2021