

Segurança e Gestão de Risco

2ºSem 2023/24

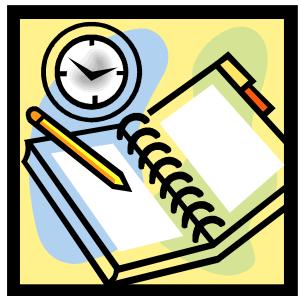
Segurança da Informação

LUIS AMORIM

13 Abr 2024

Síntese da Aula Anterior

- 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



AGENDA

- Ferramentas de Suporte à Gestão dos Riscos
 - Business Impact Analysis(BIA)
 - GAP Analisys
 - Definir uma Política de Segurança
 - Noções de Criptografia

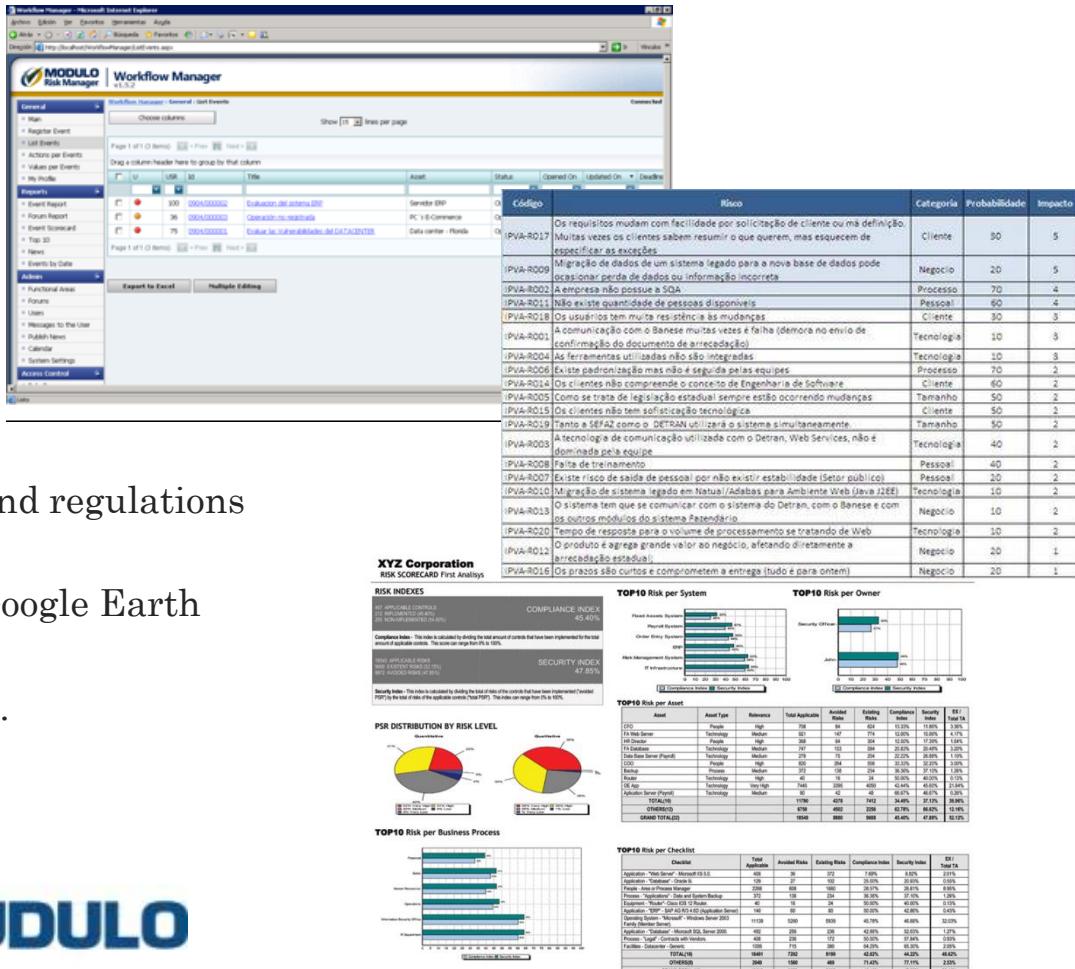
Ferramentas de suporte

- Modulo
 - vsRISK
 - Risk assessment
 - Risk identification
 - Risk analysis
 - Risk Evaluation
 - Risk treatment
 - Risk acceptance
 - Risk communication



Ferramentas de suporte

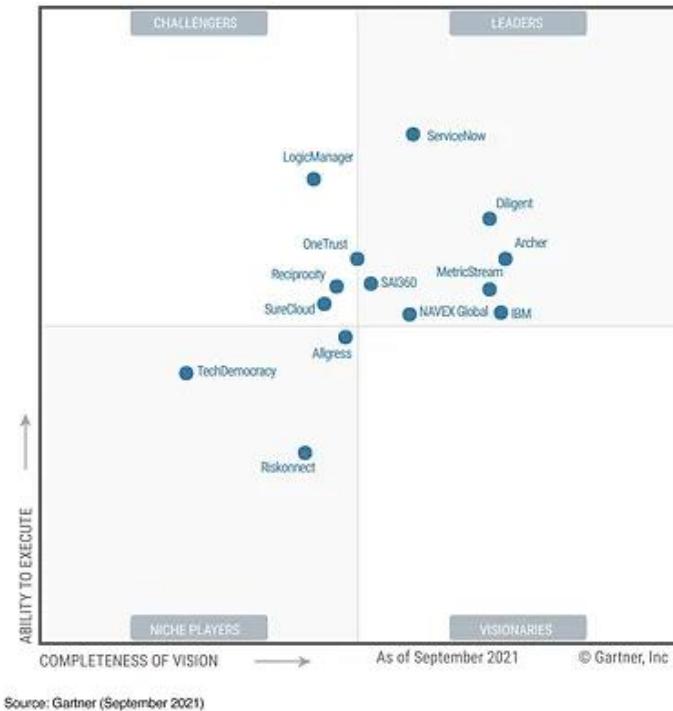
- Modulo
 - Risk Management
 - Risk assessment
 - Risk treatment
 - Risk acceptance
 - Risk communication
 - E também:
 - Asset Inventory & Evaluation
 - Compliance Module with standards and regulations
 - Business Continuity Plan
 - Geo-referenced risk: Risk map with Google Earth
 - Ou
 - WEB Interview: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



Ferramentas de suporte

- Ferramentas mais abrangentes, que permitem outro tipo de avaliações
 - Governance
 - Risk
 - & Compliance
 - Com um conjunto variado de normas

Figure 1: Magic Quadrant for IT Risk Management



Ferramentas de suporte

- Adaptive GRC

✓ Enterprise Risk Manager

1. Stores and manages the customers Risk Register
2. Follows the established principles of Risk Management including ISO 31000
3. Allows the Risk Owner to have multiple stakeholders inputting into a single risk record
4. Has ability to correlate risks with root cause (via Incident Manager), technologies (via EA Manager), governance gaps and compliance status (via Compliance Manager)
5. Provides unmatched management information reporting

The screenshot displays the Adaptive GRC software interface. At the top, there's a navigation bar with the Adaptive GRC logo, user profile, and status indicators (Inherent Risk Analysis, ID: RIS36). A callout bubble on the left says "See the current status of Risk Tasks, Workflows, and Actions." The main area is titled "Compliance Risk" and shows a risk record for "Clinical Research". The record includes fields for Risk Type (Compliance), Risk Owner (John Smith), Business Process (Prevention of conflicts of interest), and Business Unit. It also shows Risk Movement (No change) and Risk Assessment (Impact: Very High, Likelihood: Likely, Inherent Risk Rating: 20 (Red)). The Risk Treatment section indicates Mitigation as the treatment. The Risk Result (Residual Risk) section shows Impact (Residual) and Likelihood (Residual) both at N/A, with a residual risk rating of N/A. A callout bubble at the bottom right says "Investigate Risk Assesment based on impact, likelihood and rating". On the far right, there's a vertical sidebar labeled "Segurança e Gestão de Risco".

Ferramentas de suporte

- Adaptive GRC



✓ Compliance Manager

1. Storage and version management of a unified control objectives framework
2. Advanced Risk Profiling features to build a clear and rapid view of your audit and assessment priorities
3. Dynamic selection of appropriate questions and streamlined compliance assessments

✓ Document Manager

1. An online register of all documents
2. Transparent approval process
3. Status reports and dashboards

✓ Enterprise Architect Manager

1. Connects track between systems together with their governance implications with less time and effort - internal and external systems are efficiently inventoried in one place
2. Gives an instant access to relevant data from other AdaptiveGRC products - incident, risk and other GRC data can flow automatically into EA Manager from other AdaptiveGRC system
3. Key stakeholders such as the Privacy Officer can get easy and instant access to the GRC status of the applications relevant to them

Ferramentas de suporte

- Adaptive GRC



✓ Internal Audit Manager

1. Flexible audit universe
2. Risk assessment for each area
3. Effective audit planning
4. Complete control over the audit process
5. Monitoring of post-audit recommendations

✓ Quality Manager

1. Provides full Quality Management system functionality including Incident Management, Audit Events and Observations, Action Management (CAPA), Exception Management, Deviations, Investigations
2. Streamlines operation of quality management activities
3. Provides full traceability of the suspected or confirmed quality defect's management
4. Makes all of the QMS information available to other modules and creates a holistic view to help identify trends and patterns across all company-wide GRC activities
5. Provides full audit trail and electronic signature options

Ferramentas de suporte

- GRC and Security Assurance

❖ Enterprise Policy Management

1. Centralize the Policy Lifecycle
 - Work from a single source of truth to create, distribute, measure, and maintain policies.
2. Simplify Collaboration
 - Eliminate manual effort with policy templates, workflows, and automation.
3. Track Policy Effectiveness
 - Gain real-time visibility across policy status, attestations, exceptions, and coverage across the business.

❖ IT & Security Risk Management

1. Security Certification Compliance
 - Build, scale and automate your security compliance program.
2. IT & Security Risk Management
 - Proactively identify, measure and monitor risk across your IT ecosystem.



Ferramentas de suporte - GRC and Security Assurance

❖ Third-Party Risk

1. Third-Party Risk Management
 - Build, scale and automate your third-party risk management program.
2. Third-Party Risk Exchange
 - Access risk analytics and control gap reports on thousands of vendors.

❖ Audit Management

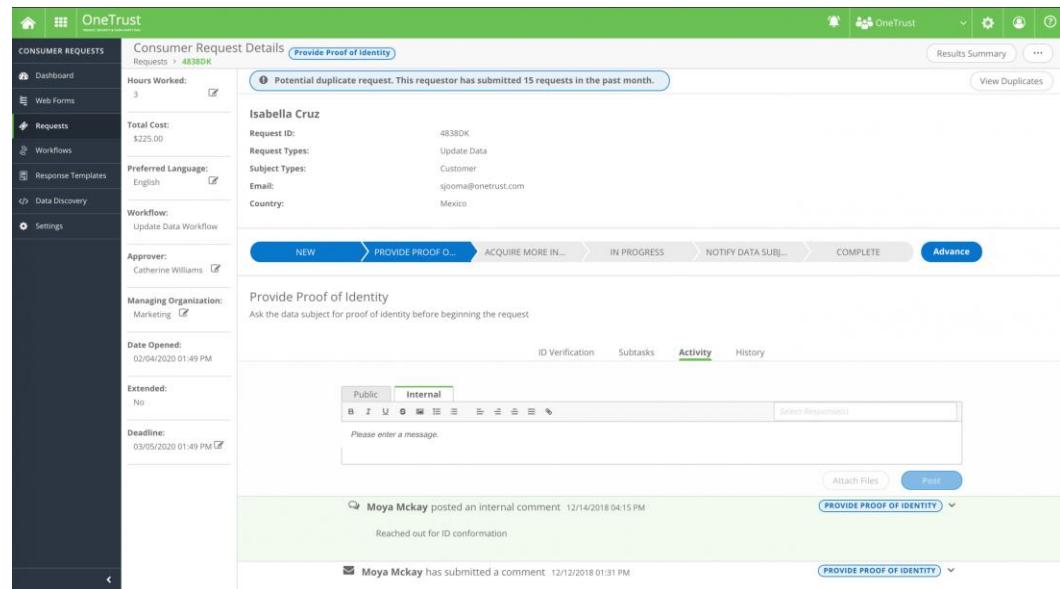
1. Plan and Scope Audits
 - Perform audit readiness assessments and easily scope audits by frameworks, standards, and controls.
2. Assess Control Design and Effectiveness
 - Document your test of design and operating effectiveness. Kick start testing efforts with templated workpapers to guide and standardize documentation.
3. Streamline Evidence Collection
 - Avoid unnecessary evidence hunting across systems, departments, and individuals.

Ferramentas de suporte

- Privacy and Data Governance

- **Privacy Management**
 - ❖ PIA & DPIA Automation
 - ❖ Data Mapping Automation
 - ❖ Privacy Rights Automation (DSAR)
 - ❖ Privacy Incident Management
 - ❖ Third-Party Risk Management
 - ❖ Digital Policy Management
 - ❖ Privacy Training
 - ❖ Data Guidance Research

- **Data Governance**
 - ❖ Data Discovery
 - ❖ Data Catalog



Ferramentas de suporte

- Governace, Risk and Compliance features

✓ Policy and Compliance Management

- Automate and manage policy lifecycles and continuously monitor for compliance.

✓ Risk Management

- Enable fine-grained business impact analysis to appropriately prioritize and respond to risks.

✓ Business Continuity

- Management Plan, exercise, and recover from disasters effectively and efficiently.

✓ Vendor Risk Management

- Continuously monitor, detect, assess, mitigate, and remediate risks in vendor ecosystems.

✓ Operational Risk Management

- Manage operational risk as part of an integrated risk management program.

✓ Continuous Authorization and Monitoring

- Accelerate the process of bringing IT systems online and continuously monitoring them.

✓ Operational Resilience Management

- Gain real-time visibility into the resilience of your technology, people, processes, and facilities.

✓ Privacy Management

- Manage privacy risk and compliance in real time as part of a holistic enterprise risk program.

✓ Regulatory Change Management

- Keep pace with today's complex regulatory landscape with integration to leading content providers.

✓ Audit Management

- Use risk data to scope and prioritize audit plans and automate cross-functional processes.

Ferramentas de suporte

- Governace, Risk and Compliance features

✓ Use Case Accelerators

- Get an operational head start on compliance with popular frameworks and regulations.

✓ Performance Analytics

- Anticipate trends, prioritize resources, and continuously improve with real-time analytics.

✓ Virtual Agent

- Give employees help when they need it with virtual agents that understand simple, human language.

✓ Predictive Intelligence

- Simplify and accelerate everyday work with built-in machine learning.



Ferramentas de suporte - Outros Produtos

Produtos:

- ✓ IT Service Management
- ✓ IT Operations Management
- ✓ Strategic Portfolio Management
- ✓ IT Asset Management
- ✓ Enterprise Asset Management
- ✓ Security Operations
- ✓ Governance, Risk, and Compliance
- ✓ Telecommunications Service Operations Management
- ✓ Operational Technology Management

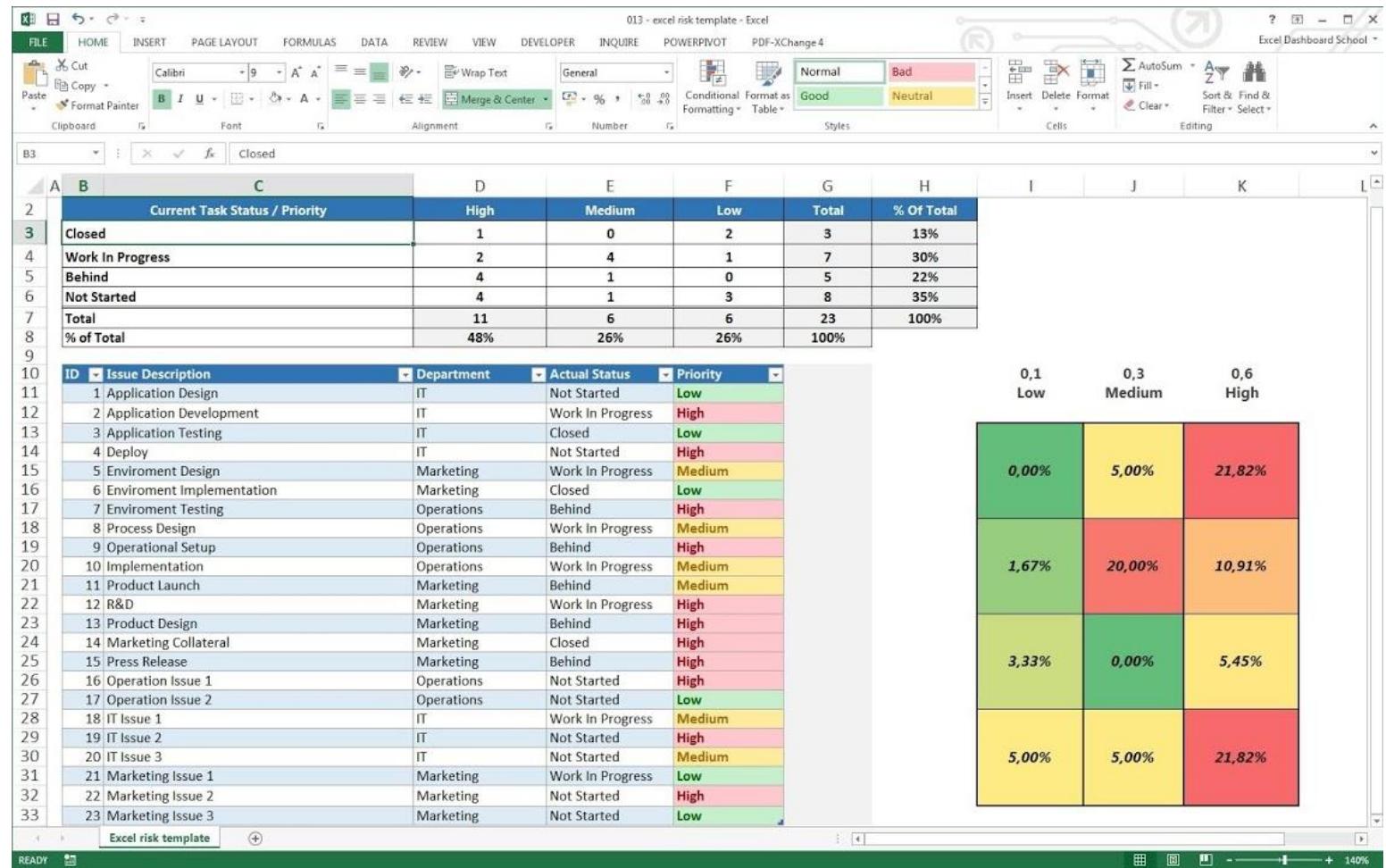
The screenshot shows the ServiceNow instance management dashboard. At the top, there are three boxes: 'Apps ready to update' (30), 'Apps ready to install' (799), and 'Instance Security Center notifications' (-1). Below this is a section titled 'Review your work' with a table of assignments:

Number	Created	State	Priority	Short description
TASK006165	2022-08-22 10:31:26	Not Started	1 - Critical	Now Support - Schedule Business Review
TASK006164	2022-08-22 10:28:34	Not Started	2 - High	Health Assessment
TASK006163	2022-08-22 10:27:23	Not Started	3 - Moderate	Adoption Toolkit
CMDBTASK0001001	2022-08-22 10:40:39	(101)	4 - Low	Connect with Now Support Account Specialist on Tokyo Release updates
TASK006166	2022-08-22 10:38:30	Work in Progress	4 - Low	Connect with Now Support Account Specialist on Tokyo Release updates
UPGR0040451	2022-08-22 10:39:59	(101)	Priority 5	

On the right side, there are two cards: 'Critical Tasks' (1) and 'New tasks' (5). Below them is a donut chart titled 'Open tasks by priority' showing the distribution of tasks across five priority levels: Critical (1, 17%), High (1, 17%), Moderate (2, 33%), Planning (1, 17%), and Low (2, 33%).

Ferramentas de suporte

- Folha de cálculo
 - Excel



AGENDA

- Ferramentas de Suporte à Gestão dos Riscos
 - Business Impact Analysis(BIA)
- GAP Analisys
- Desenvolver uma Política de Segurança
- Noções de Criptografia

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)

Business Impact Analysis(BIA)

- Caraterizar os possíveis impactos para o negócio dos diferentes processos da organização (e dos ativos que deles dependem)
 - Classificados em função do ...
 - ... contexto da organização

<i>Category</i>	<i>If the Asset Was Unavailable:</i>
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?

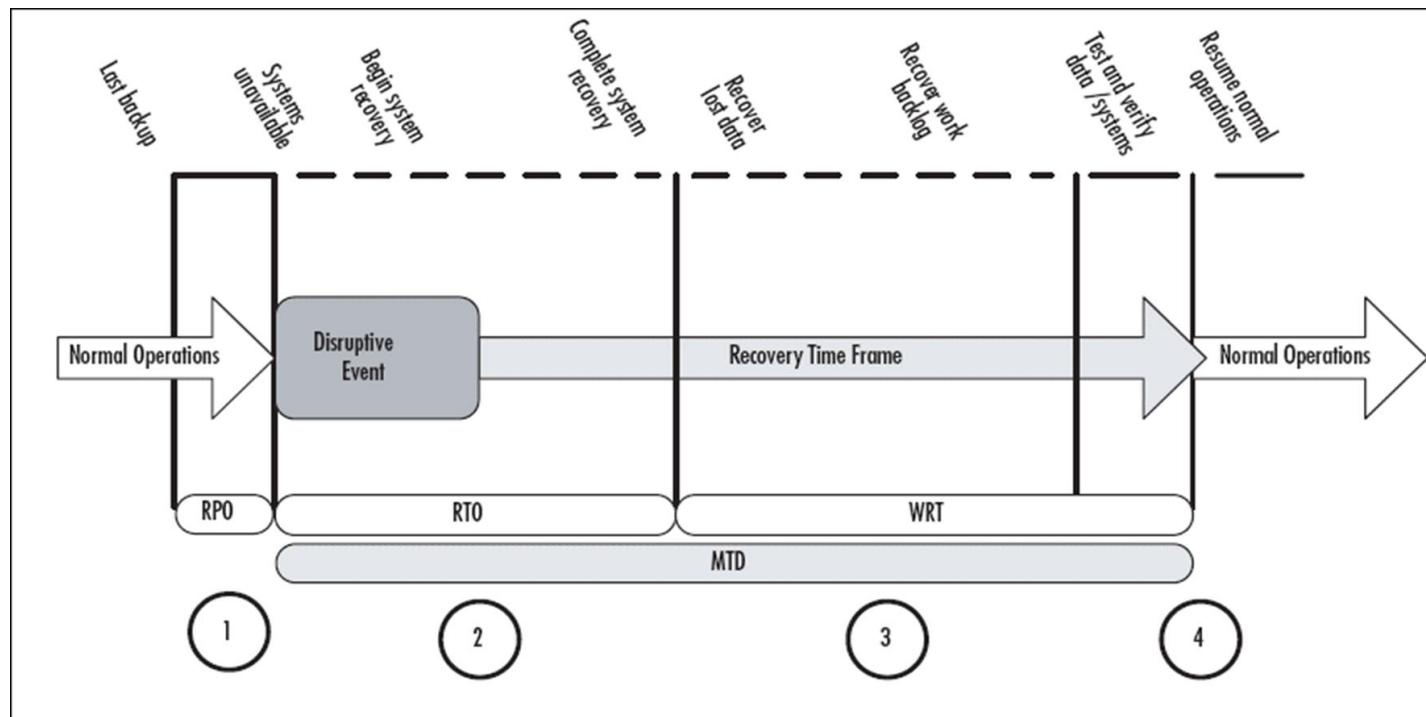
Business Impact Analysis(BIA)

- 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	
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

Business Impact Analysis (BIA)

- Caraterizar os requisitos de recuperação
 - R P O = Recovery Point Objective - maximum acceptable amount of data loss measured in time
 - R T O = Recovery Time Objective - the maximum tolerable amount of time needed to bring all critical systems back online
 - W R T = Work Recovery Time - the maximum tolerable amount of time that is needed to verify the system and/or data integrity
 - M T D = Maximum Tolerable Downtime - total amount of time that a business process can be disrupted without causing any unacceptable consequences



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

23

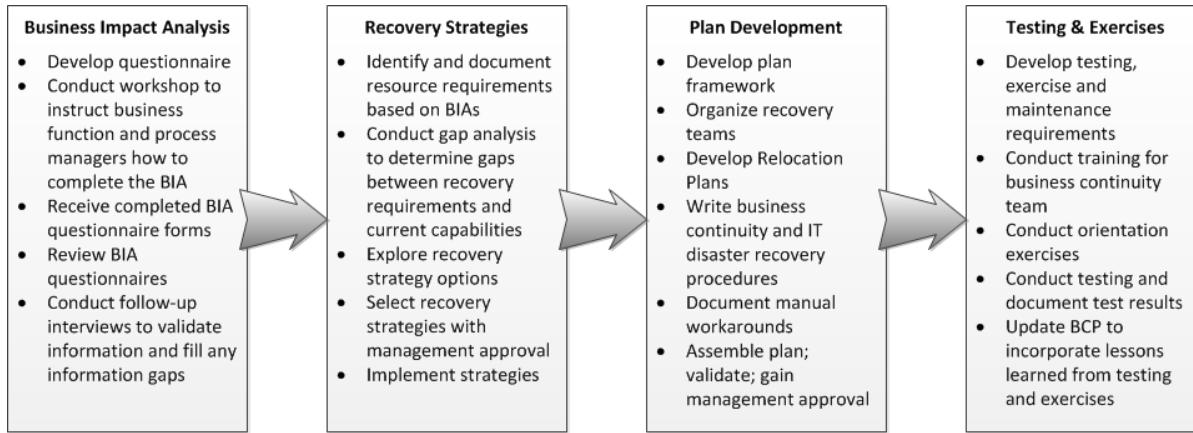
Business Impact Analysis(BIA)

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

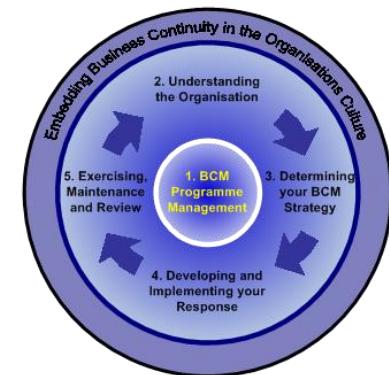


24

Business Impact Analysis(BIA)

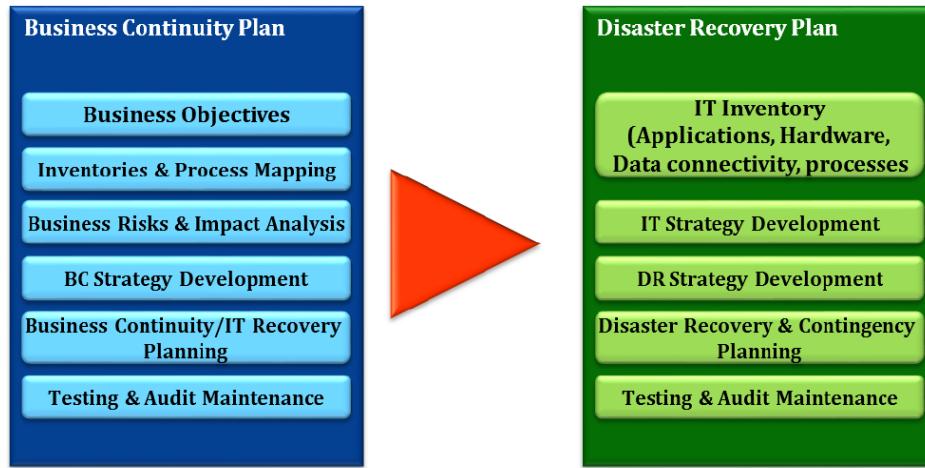


- No final
 - Testar
 - Exercitar os Planos de Continuidade



25

Business Impact Analysis(BIA)



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

Business Impact Analysis (BIA)

- Um Plano 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

Business Impact Analysis (BIA)

- Processo de triagem

- Como resultado de um processo de 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)

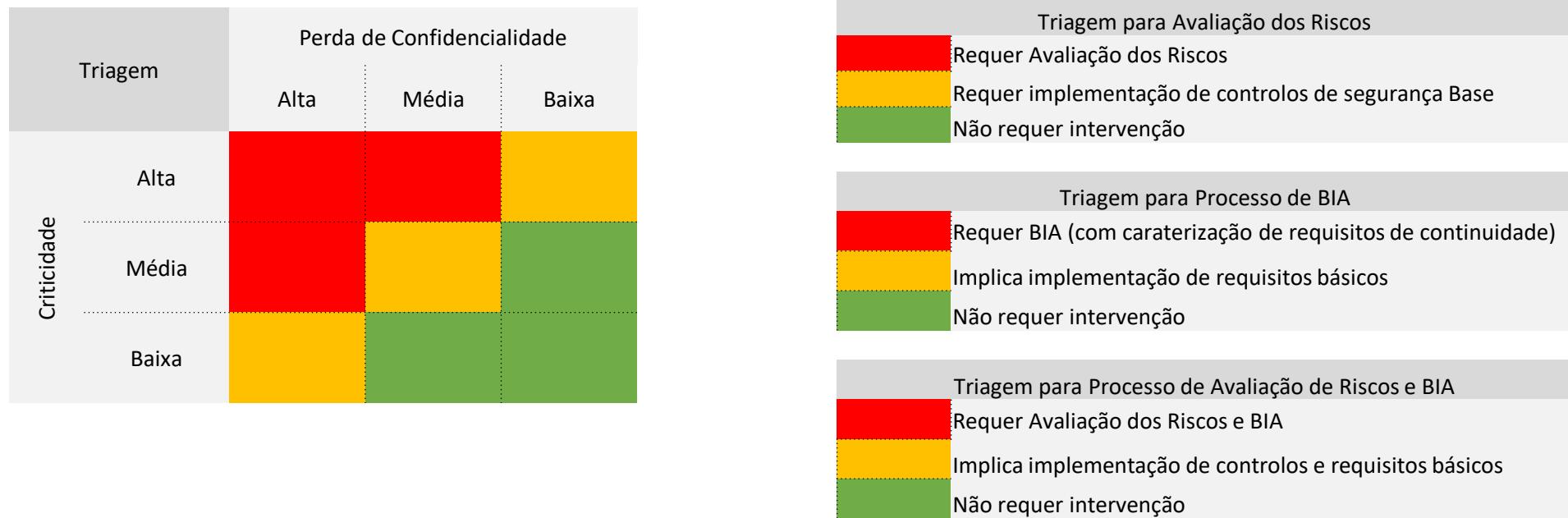
<i>Disclosure Impact Level</i>	<i>Definition</i>
High	Information is of such a nature that its unauthorized disclosure would cause media attention and negative customer response.
Medium	Information is of such a nature that its unauthorized disclosure might cause media attention and negative customer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

		Disclosure		
		High	Medium	Low
C r i t i c a l i t y	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

<i>Criticality Impact Level</i>	<i>Definition</i>
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.

Business Impact Analysis (BIA)

- Processo de triagem



Business Impact Analysis (BIA)

- Exercício prático
 - Identificar processos de negócio de uma loja de computadores
 - Quantificar a criticidade e o impacto
 - Identificar que processos da organização requerem uma
 - avaliação de riscos

AGENDA

- Ferramentas de Suporte à Gestão dos Riscos
- BusinessImpactAnalysis(BIA)
 - GAP Analisys
- Definir uma Política de Segurança
- Noções de Criptografia

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

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 – CO₂ 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.

GAP Analysis

- Implementação de segurança ISO27002
 - Necessário avaliar o cumprimento de todos os controlos da norma

Controlos da ISO/IEC 27002:2022						
Controlo	Descrição do Controlo	Estado	Constatação Doc. Reun. Obs.	Evidências		
5. Controlos organizacionais						
5.1 Políticas de segurança da informação	A política de segurança da informação e as políticas específicas do tópico devem ser definidas, aprovadas pela gestão, publicadas, comunicadas e	Não Implementado		X		Não evidenciadas políticas formalizadas e revistas
5.2 Papéis e responsabilidades de segurança da informação	Os papéis e responsabilidades de segurança da informação devem ser definidos e atribuídos de acordo com as necessidades da organização.	Implementado	X			Papeis estabelecidos em documento publicado pelos RHs
5.3 Segregação de funções	Deveres e áreas de responsabilidade conflitantes devem ser segregados.	Parcialmente Implementado	X	X		A segregação de funções está estabelecida para o CISO, no entanto ao nível do IT, apesar de evidenciado, requer de formalização
5.4 Gestão de responsabilidades	A gestão deve exigir que todo o pessoal aplique a segurança da informação de acordo com a política de segurança da informação estabelecida, políticas específicas do tópico e procedimentos da organização.	Não Implementado				

GAP Analysis

- Cumprimento da ISO27002

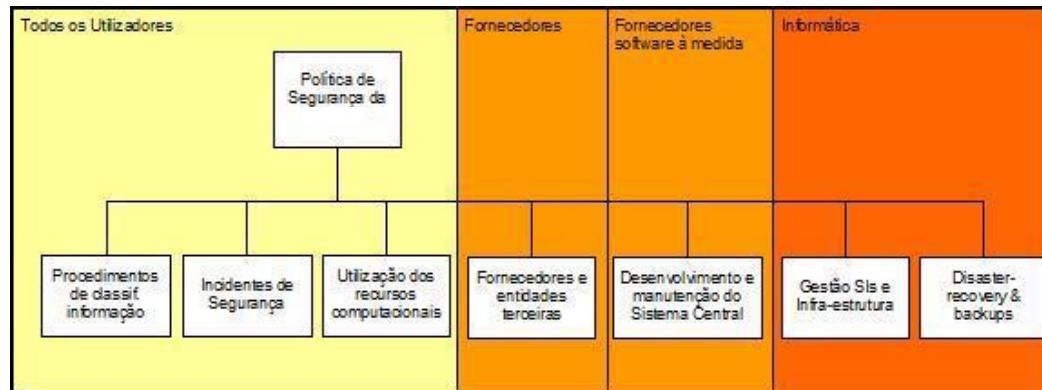
		Comments
1 SCOPE	This international standard establishes guidelines and general principles for initiating, implementing, maintaining and improving information security management in an organization.	
2 TERMS DEFINITIONS	For better understanding, ISO 27002 identifies and defines key information security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

AGENDA

- Ferramentas de Suporte à Gestão dos Riscos
 - BusinessImpactAnalysis(BIA)
 - GAP Analisys
- Definir uma Política de Segurança
- Noções de Criptografia

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).
 - Face ao negócio, estrutura orgânica e recomendações efectuadas, é proposta a seguinte organização para os elementos constitutivos da Política de Segurança:



Implementação de Política de Segurança

- Definição de Política de Segurança

15-04-2023

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:

- A certificação ISO/IEC 27001, aliando a empresa às melhores práticas de segurança da informação;
- Um serviço de qualidade aos seus clientes regido pelo cumprimento das melhores práticas de segurança da informação;
- A implementação de controlos de segurança que contribuam para manter a confidencialidade, integridade e disponibilidade da informação e sistemas de informação da XXX;
- 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;
- A caraterização e tratamento adequado de potenciais eventos e incidentes de segurança;
- A melhoria contínua dos processos de gestão segurança da informação.

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

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

Implementação de Política de Segurança

- **Exercício prático**

- Desenvolver práticas de Salvaguarda de informação
 - Definir **Política de Backups**
 - Definir **Procedimentos de Operação**, alinhados com essa política

AGENDA

- Ferramentas de Suporte à Gestão dos Riscos
- BusinessImpactAnalysis(BIA)
- GAP Analisys
- Definir uma Política de Segurança
- Noções de Criptografia

Noções de criptografia

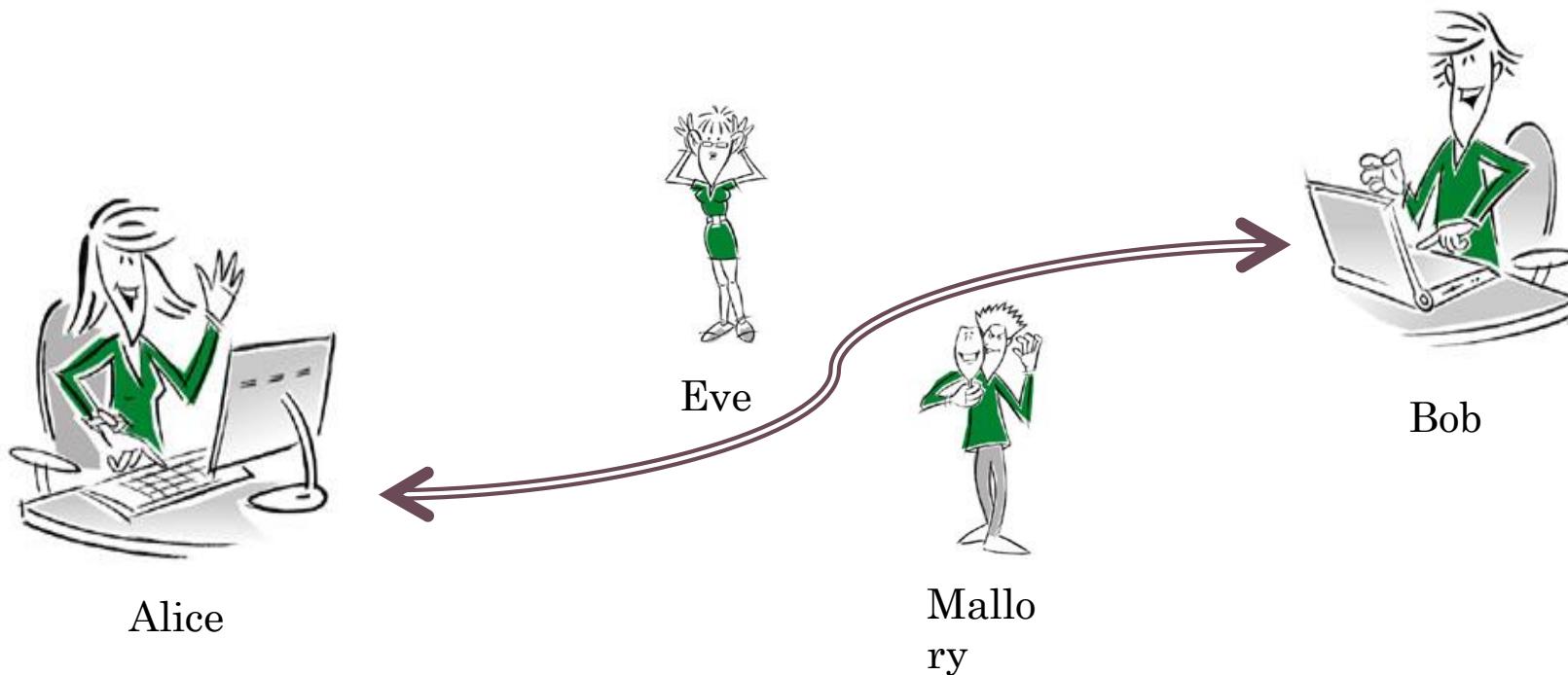
- Criptografia
(*kryptós*=secreto,escondido + *grápho*=grafia,escrita)
- O que é?
 - “Escrita secreta por meio de abreviaturas ou de sinais convencionados de modo a preservar a confidencialidade da informação”
- Em que consiste?
 - Transformação de textos originais, chamados texto original (**plaintext**) ou texto claro (**cleartext**), em informação transformada, chamada texto cifrado (**ciphertext**), texto código (**codetext**) ou simplesmente cifra (**cipher**), que têm a aparência de um texto random ilegível

Noções de criptografia

- O Porquê da Criptografia?
 - Proteger dados (informação)
 - Informações Militares (Tácticas/Estratégias)
 - Informações Científicas (Segurança de Estado)
 - Informações Industriais (Espionagem Industrial)
 - Informações Bancárias (Movimentos Bancários)
 - Informações Comerciais (Comércio Electrónico)
 - Informações Pessoais
 - Etc...

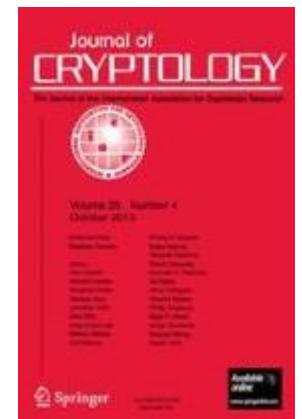
Noções de criptografia

- Utilização de criptografia para protecção
 - Concorrentes ou Inimigos;
 - Hackers;
 - ...



Noções de criptografia

- A International Association for Cryptologic Research (IACR) é uma organização científica internacional que mantém a pesquisa nesta área.
 - Organiza conferências
 - **Eurocrypt 2023, 23 - 27 April 2023, Lyon, France.**
 - **Crypto 2023, 19 - 24 August 2023, Santa Barbara, USA**
 - Workshops
 - **Fast Software Encryption, 20 - 24 March 2023, Beijing, China**
 - **Cryptographic Hardware and Embedded Systems (CHES),**
10 - 14 September 2023, Prague, Czechia.
 - **Real World Crypto Symposium, 25 - 27 March 2024. Toronto, Canada**
 - Publicações



Noções de criptografia

- Protecção da informação
 - **O foco da segurança da informação deve ser**
 - protegê-la de algum mal (roubo, alteração, acesso não autorizado)
 - ao mesmo tempo que mantém a informação disponível para quem precisa
 - As técnicas criptográficas estão já disponíveis há alguns anos, mas só por questões de conformidade ou utilização de boas práticas se tem incrementado a sua utilização.
 - A cifra tem-se tornado uma comodidade, vindo já embebida em aplicações ou bases de dados.



Noções de criptografia

- As ameaças que a informação enfrenta:
 - Perda ou Roubo de Media - Tapes ou discos de backup armazenados ou em transito
 - Roubo de Informação por utilizadores com acesso
 - Distribuição não intencional (envio para um destinatário diferente)
 - Hacking (aplicacional), alterando aplicações ou configurações com impacto nos dados
 - Roubo de dispositivos móveis

Noções de criptografia

- Utilização de criptografia
 - Numa primeira fase generalizou-se a protecção dos dados em transito:
 - SSL
 - VPNs
 - Mas devemos também considerar os riscos da informação permanecer em claro nas origem e no destino
 - roubar um carro no parque ou garagem é muito mais fácil do que tentar roubá-lo numa auto-estrada



Noções de criptografia

- **Protecção da informação em vários pontos**
 - **Segurança de dados armazenados**
 - Cifrar dados armazenados - em disco, tape,..
 - Mas podemos estar a aplicar uma medida desnecessária à maioria dos dados.
 - Necessário pensar como partilhar alguns dos dados com utilizadores que não têm acesso a chaves ou por razões de auditoria
 - **Segurança nos Servidores**
 - A utilização de dispositivos cifrados (tudo cifrado) pode não ser a melhor opção para atacantes internos.
 - Segurança a nível aplicacional
 - Os dados quando utilizados pelas aplicações ganham contexto e significado, quem e como deve aceder
 - Para além do controlo de acessos que já está vulgarizado, existem já soluções ao nível aplicacional que fazem uso de PKIs:
 - gestão documental;
 - e-mail;
 - autenticação de utilizadores;
 - software publishing.

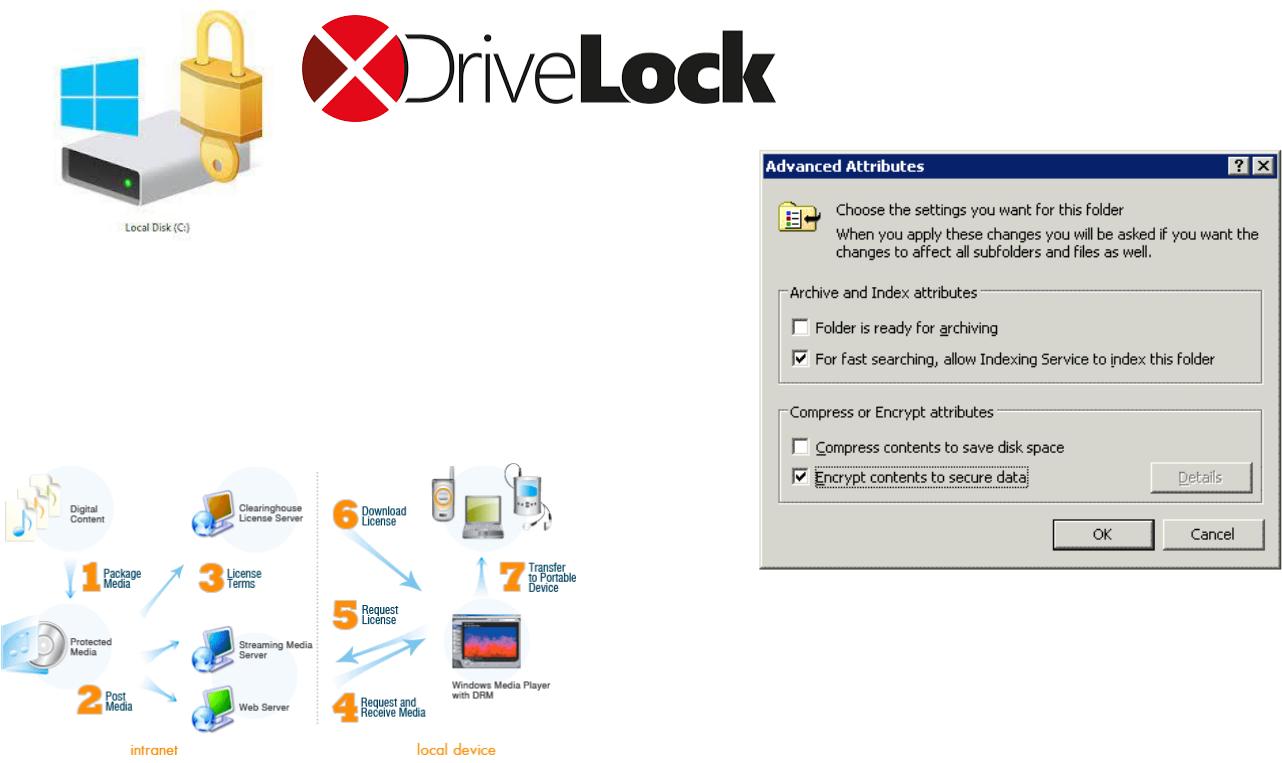
Noções de criptografia

- Protecção da informação em vários pontos
 - **Segurança dos Terminais de utilizador**
 - Considerando como forte ameaça causada pelo Teletrabalho
 - onde o acesso remoto a informação
 - cópia dessa informação para pastas locais, nos PCs ou Portáteis
 - e-mails com attachs em claro para contas pessoais
 - acumulação durante largos anos de informação desnecessária para o trabalho actual), mas que não é apagada
 - Face à mobilidade e número de dispositivos que cada utilizador dispõe, é necessário controlar um conjunto variado de dispositivos:
 - SmartPhones,
 - PDAs,
 - PENs USB,
 - cartões de memória, ...

Noções de criptografia

- A resposta pode ser proteger a diversos níveis, de acordo com o tipo de informação ou dispositivo:

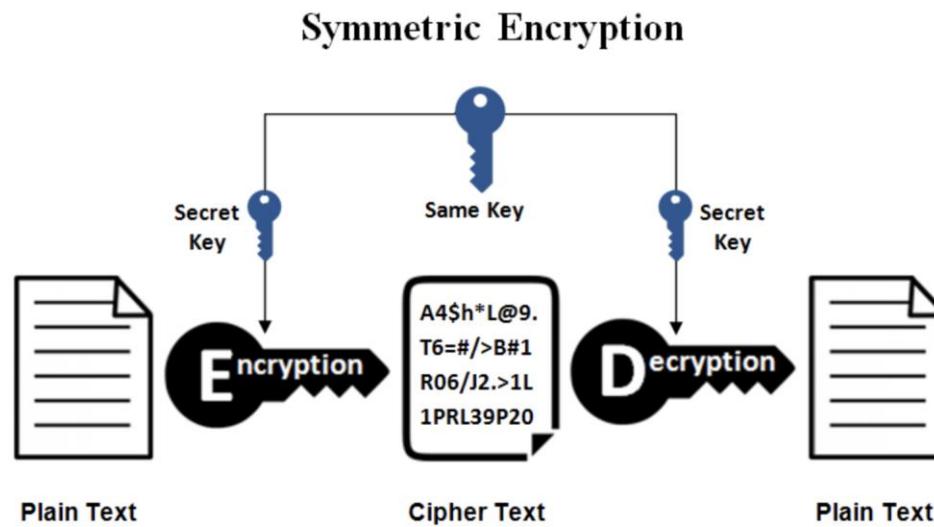
- discos, Tapes, PENs
- File System
- ou um nível acima DRM



Noções de criptografia

- **Sistemas criptográficos simétricos**

- Usam a mesma chave para encriptar e desencriptar mensagens; ou pelo menos, chaves que possam ser determinadas de forma simples e directa uma a partir da outra.

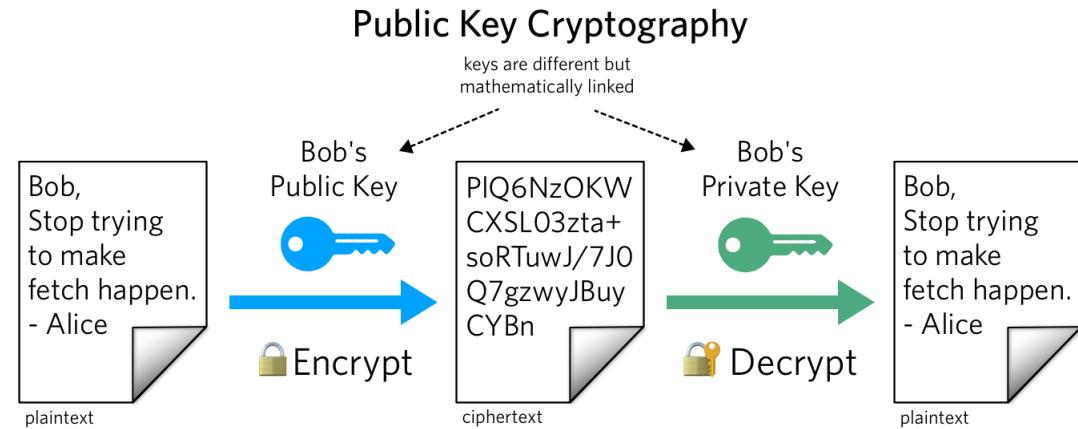


Noções de criptografia

- Sistemas criptográficos simétricos
 - Necessitam de um canal seguro para a divulgação das chaves.
 - Só os utilizadores do grupo podem ter acesso às chaves.
 - Com a saída de um utilizador do grupo, o sistema fica comprometido
- Exemplos
 - Cifra de Vigenère
 - Sistema de Gronsfeld
 - Código Playfair
 - Substituição de Hill
 - Data Encryption Standard (DES)
 - International Data Encryption Algorithm (IDEA)
 - One Time Pad (One time key, ou Chave Única)
 - Advanced Encryption Standard (AES)

Noções de criptografia

- **Sistemas criptográficos assimétricos (chave pública)**
 - Tipo de encriptação que usa duas chaves distintas, uma para a encriptação e outra para a desencriptação de mensagens (chave pública e chave privada, respectivamente).

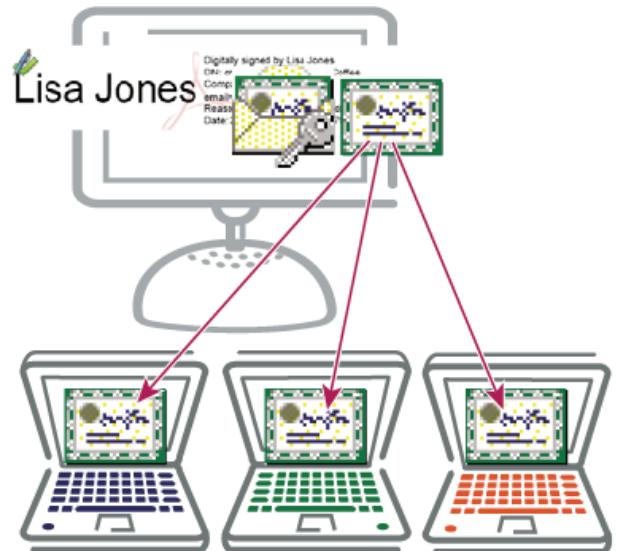


Noções de criptografia

- Sistemas criptográficos assimétricos (chave pública)
 - Evita o problema da divulgação das chaves, dos sistemas simétricos.
 - Cerca de 1000 vezes mais lento que os algoritmos simétricos
 - Utilizações mais comuns ...
 - Distribuição de chaves sem “segredos” pré-acordados
 - Assinaturas digitais e não repúdio
 - Identificação utilizando protocolos de “desafio-resposta” com chaves públicas
 - Encriptação (mas muito mais lento)
 - Exemplos
 - Diffie - Hellman (# 1º sistema de chave pública inventado)
 - HM (Merkle e Hellman)
 - RSA (Ron Rivest, Adi Shamir e Leonard Adleman)
 - PGP (Pretty Good Privacy)

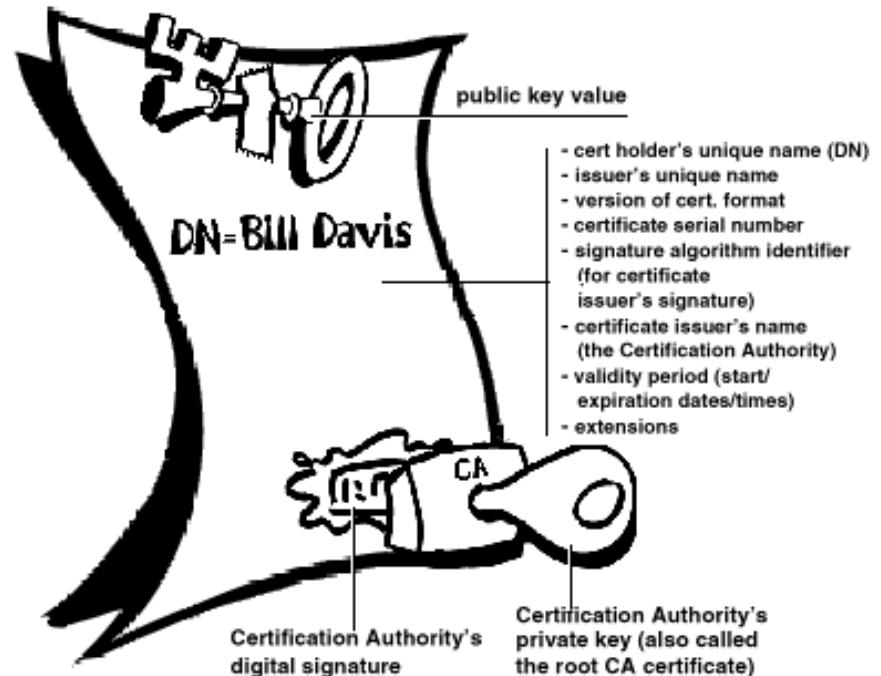
Noções de criptografia

- Sistemas criptográficos assimétricos
 - **PKI – Public Key Infrastructure**
 - Infraestrutura necessária para a gestão do “ciclo de vida” das chaves criptográficas de sistemas assimétricos
 - Geração
 - Distribuição
 - Renovação
 - Revogação
 - etc.
 - **Chave Privada** = Chave Privada
 - **Certificado Digital** = Chave Pública
 - + Metainformação (Subject, Issuer, Validity, Usage, etc.)



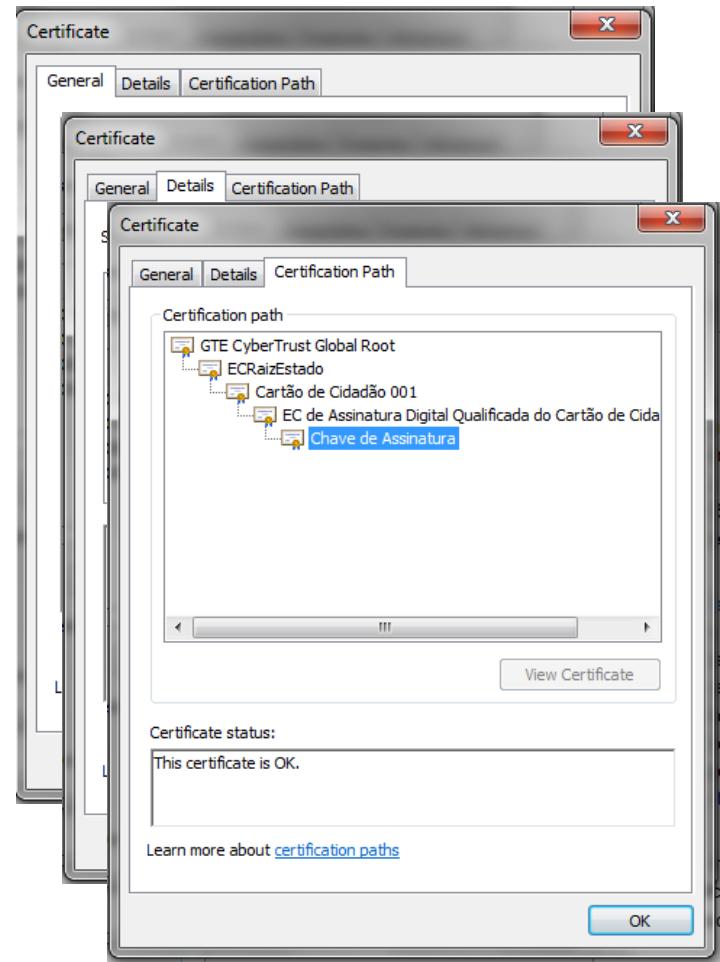
Noções de criptografia

- Digital Certificate:
 - É um documento eletrónico que liga a identidade física de um entidade (pessoa, organização ou computador) à sua chave pública
 - Em sistemas seguros (particularmente em PKIs) um certificado digital é emitido para
 - autenticar a(s) parte(s) envolvidas numa transação,
 - assinar eletronicamente documentos assegurando a integridade do seu conteúdo e/ou não repúdio de transações eletrónicas
 - ITU-T X.509 define o formato dos certificados digitais



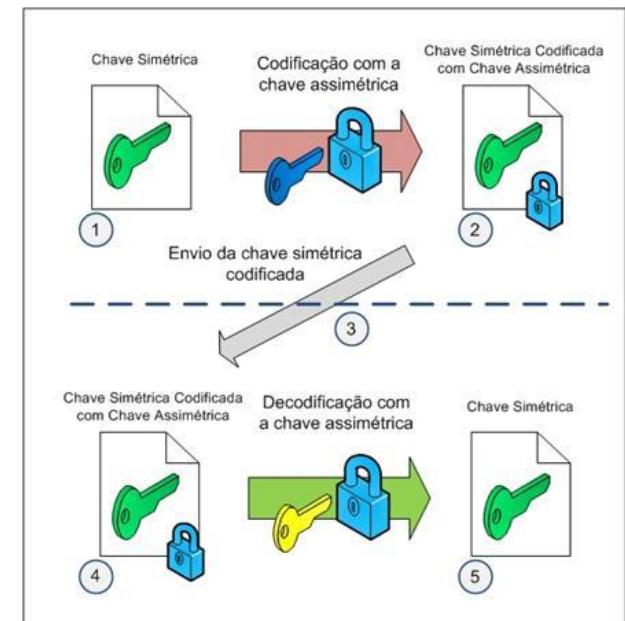
Noções de criptografia

- Sistemas criptográficos assimétricos
 - Standards
 - Certificados Digitais: X509v3
 - Certificate Revocation Lists (CRLs)
 - Certificate Trust Lists (CTLs)
 - Sistemas de Directório: X500
(importante para a definição dos campos ‘Subject’ e ‘Issuer’)
 - Outros
 - EMV Certificate: utilizado na área da banca
 - ‘more compact than x.509 certificates and are created using the ISO/IEC 9796-2 digital signature algorithm that provides “message recovery”’
 - PGP – Pretty Good Privacy (Philip Zimmermann em 1991)



Noções de criptografia

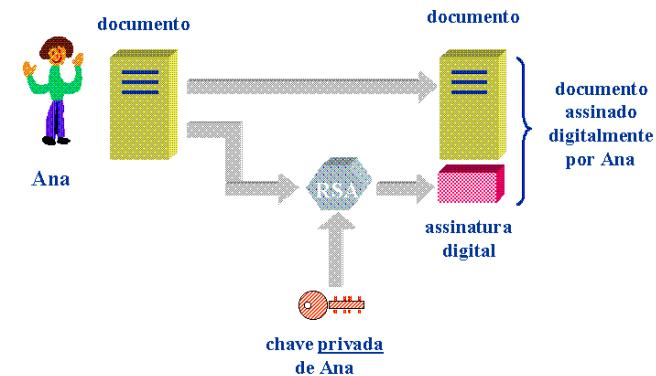
- A combinação dos dois métodos...
 - Codificando-se a mensagem com o método da chave simétrica e trocando a chave simétrica com o método de chave pública.
 - Chave de sessão simétrica
 - processamento mais rápido
 - Partilhada recorrendo a criptografia assimétrica
 - mais lenta
 - mas mais segura



Noções de criptografia

- **A Assinatura Digital**

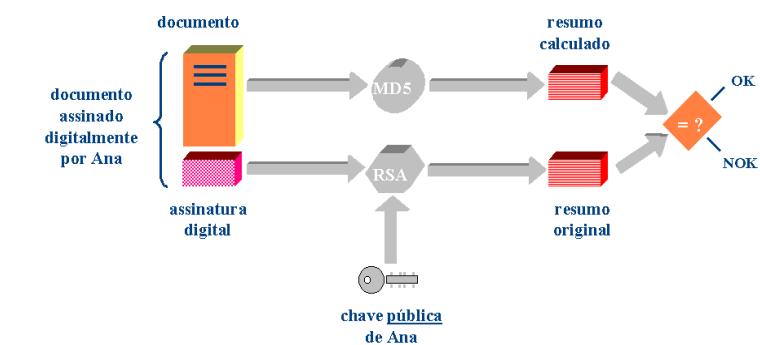
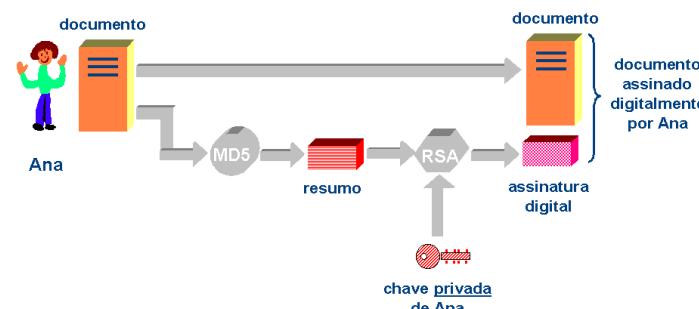
- Proporcionado pela criptografia assimétrica
- que permite garantir a autenticidade de quem envia a mensagem, associada à integridade do seu conteúdo
- No caso de se pretender enviar uma mensagem garantindo a integridade:
 - Mensagem é cifrada na origem com a chave privada
 - Destinatário utiliza a chave pública do emissor, para decifrar a mensagem
 - Fica garantida assim a
 - autenticidade,
 - integridade e
 - não-repudiação da mensagem recebida



Noções de criptografia

- **A Assinatura Digital**

- Para assegurar o não-repúdio de forma eficiente deverá ser utilizado um Digest (informação resumida do documento)
 - Função Hashing
- É pouco prático ou inviável em documentos grandes, estar a utilizar a assinatura sobre todo o documento

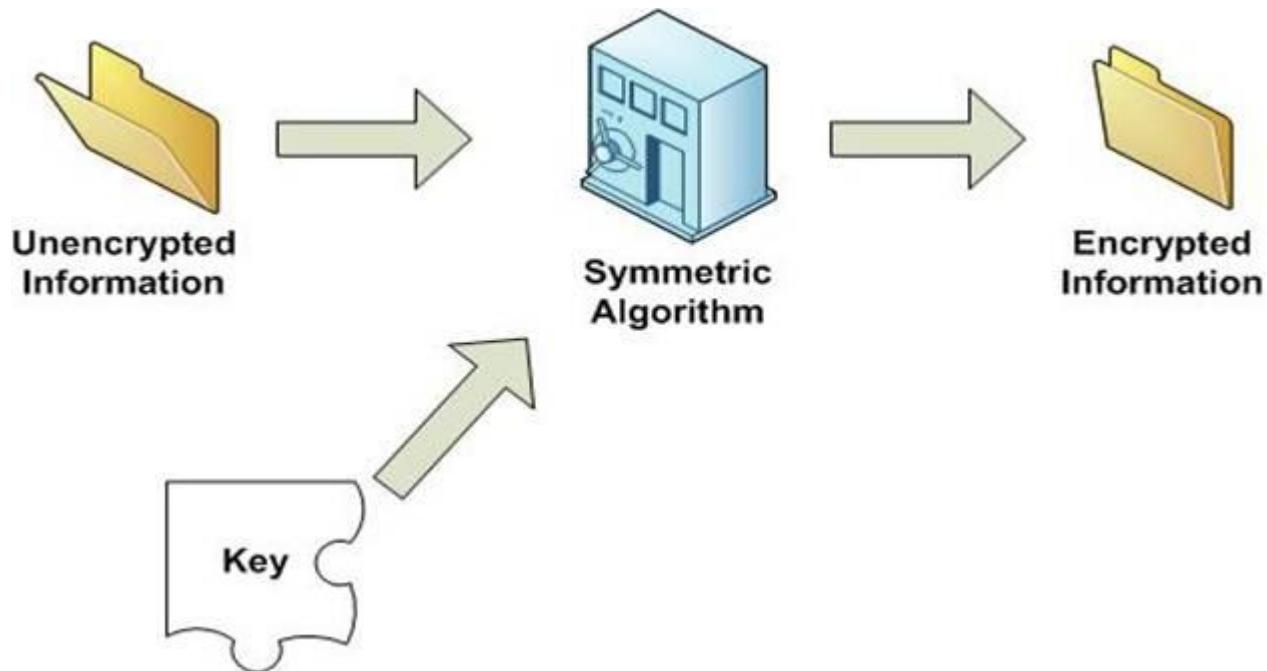


AGENDA

- Ferramentas de Suporte à Gestão dos Riscos
- BusinessImpactAnalysis(BIA)
- GAP Analisys
- Definir uma Política de Segurança
- Noções de Criptografia
 - Gestão de Chaves

Gestão de chaves

- A Cifra requer:
 - os dados a proteger
 - algoritmos de cifra
 - chaves de cifra

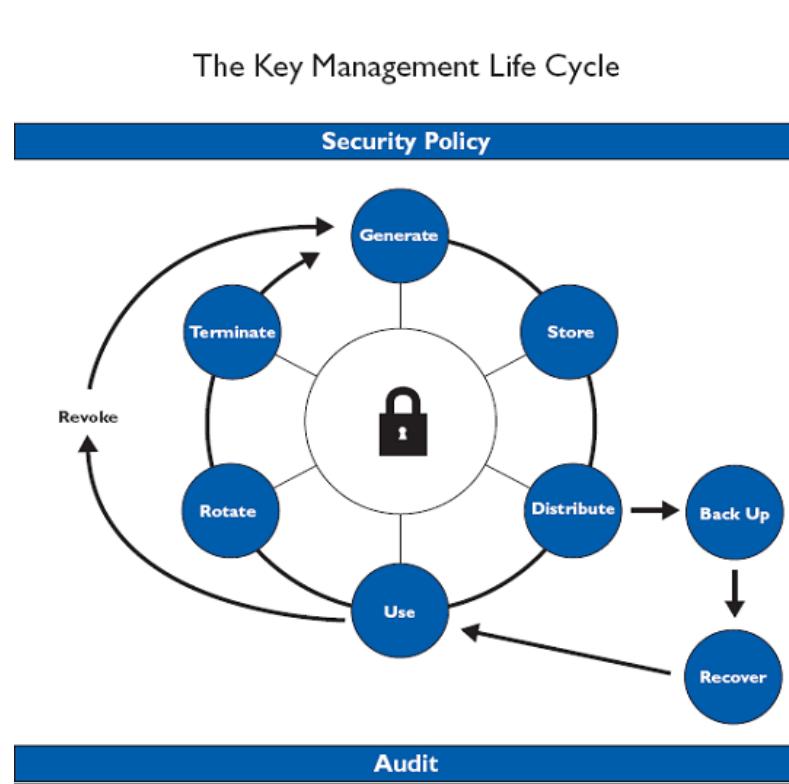


Gestão de chaves

- O processo de cifrar é uma comodidade disponibilizada por um conjunto variado de ferramentas
- Ter em atenção que nenhum algoritmo é inquebrável
 - A questão é quanto tempo leva a quebrar
- **O foco deve ser dado também ao nível da Gestão de chaves**
 - Uma gestão de chaves fraca pode comprometer processos e algoritmos de cifra robustos
 - Dar acesso, apenas, a pessoas autorizadas e de acordo com políticas de aprovação e atribuição

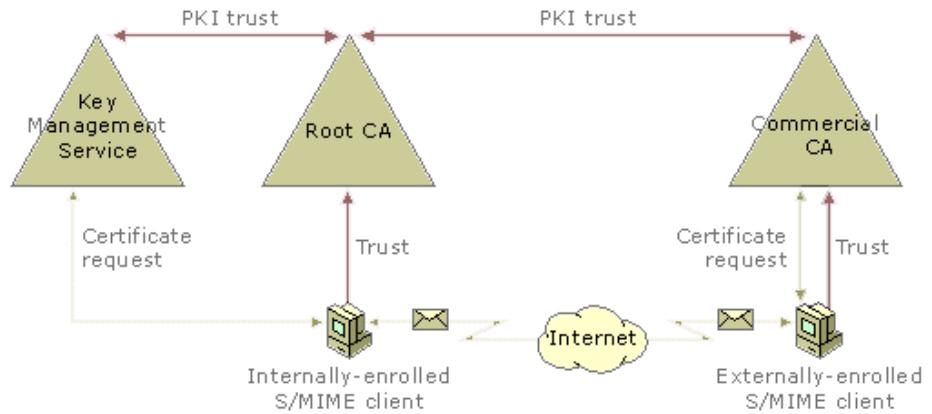
Gestão de chaves

- Para uma gestão eficaz, é necessário perceber que as **chaves têm um ciclo de vida**:
 - Geração de chaves
 - Armazenamento de chave
 - Distribuição de chave
 - Utilização da chave
 - Rotação da chave
 - Backup da chave
 - Recuperação de chave
 - Revogação da chave
 - Desactivação da chave
 - Aplicação de políticas
 - Auditorias



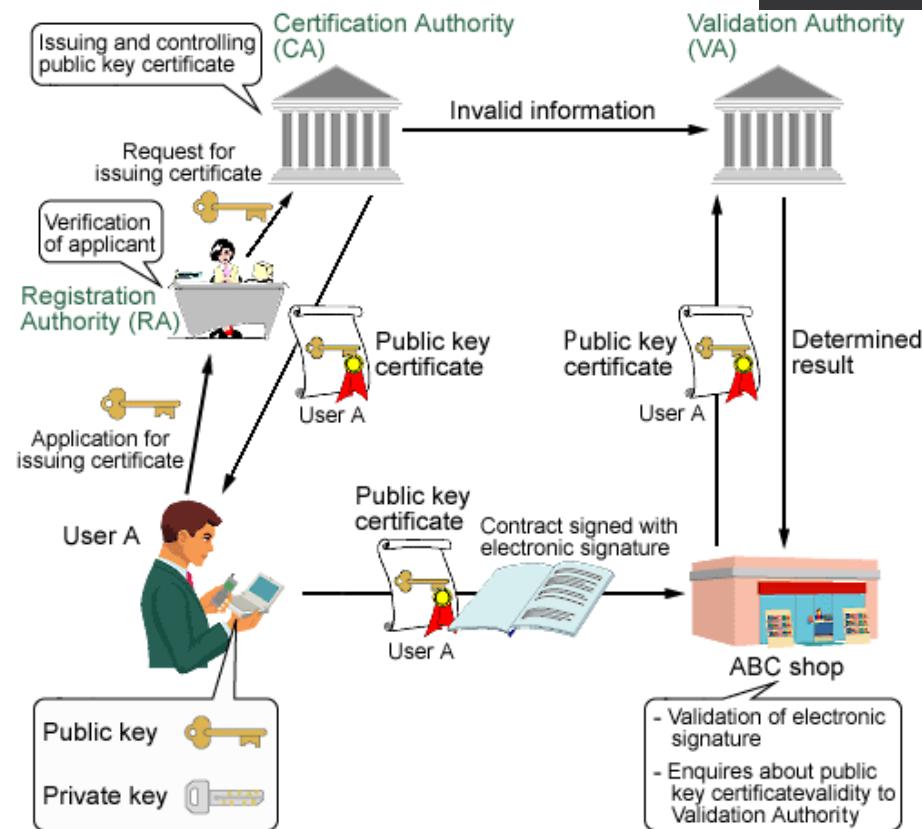
Gestão de chaves

- O que é a Gestão de chaves
 - É o conjunto de técnicas e procedimentos relacionados com o ciclo de vida das chaves criptográficas
 - Mas também das relações entre as entidades emissoras
 - Mantendo as chaves e essas relações em segurança



Gestão de chaves - PKI

- **Public Key Infrastructure (PKI)**
 - Certificate Authority (CA)
 - CA é uma organização que emite certificados utilizando uma assinatura digital, que vincula um certificado digital à identidade de uma entidade
 - Registration Authority (RA):
 - RA autentica a identidade das entidades e requer à CA a emissão do certificado para cada uma desssa entidades
 - Hierarquicamente, a RA opera na dependência da CA e atua como interface da CA para com o utilizador ou entidade requerente
 - Validation Authority (VA):
 - VA pode fazer parte do serviço fornecido pela CA ou por um terceiro.
 - Valida os certificados digitais, emite comprovativos digitais e serviços confiáveis de reconhecimento como prova de que uma transação eletrónica ocorreu



Gestão de chaves - PKI

- Registration service: (RA)
 - Verifica Identidade e atributos específicos da entidade (pessoa ou empresa). Resultados passados para “certificate generation service”
- Certificate generation service: (CA)
 - Cria e assina certificados baseados na identidade e atributos verificados pelo “registration service”.
- Dissemination service: (CA)
 - Dissemina os certificados aos requerente, e, se consentido por este, divulga para terceiras partes
 - Também é responsável por disseminar os termos e condições da CA, e as políticas e práticas de certificação
- Revocation management service: (CA)
 - Processa os pedidos e relatórios referentes à revogação, para determinar as medidas a serem tomadas.
 - Resultados distribuídos através do revocation status service.
- Revocation status service: (CA)
 - Providencia a informação do estado de revogação de certificados
 - Pode ser um serviço em tempo-real, ou ser baseado em informação que é publicada periodicamente
- Subject device provision service: (opcional - RA)
 - Disponibiliza um dispositivo de criação de assinatura
 - Exemplos de utilização:
 - Um serviço que gera o par de chaves e entrega a chave privada à entidade requerente;
 - Um serviço que prepara o subject's secure-signature-creation device (SSCD) e o entrega à entidade

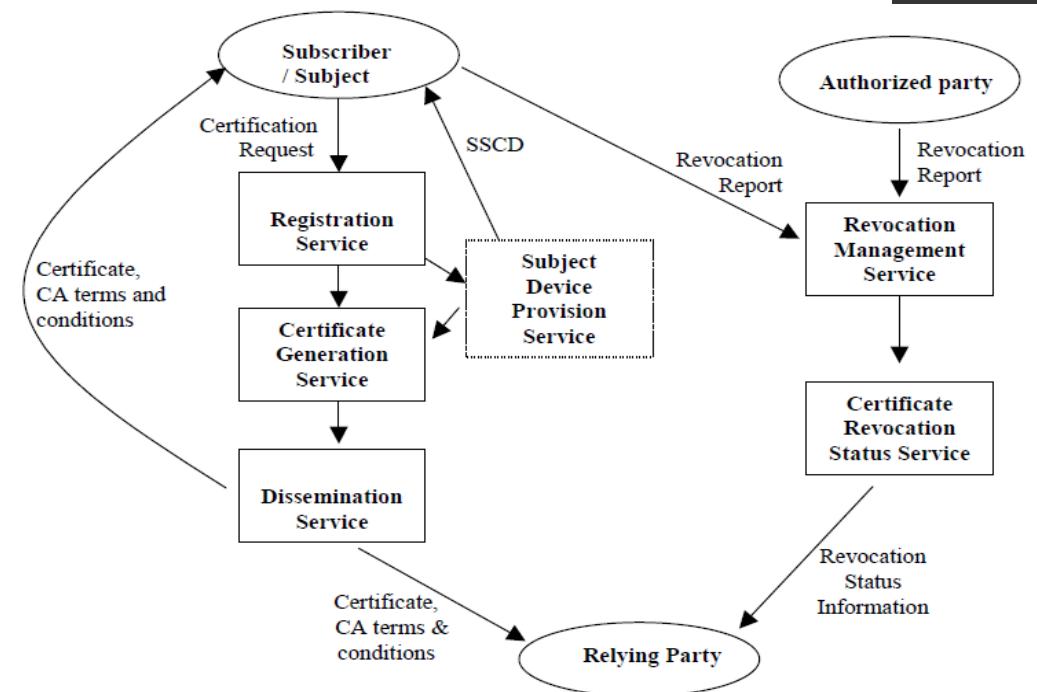
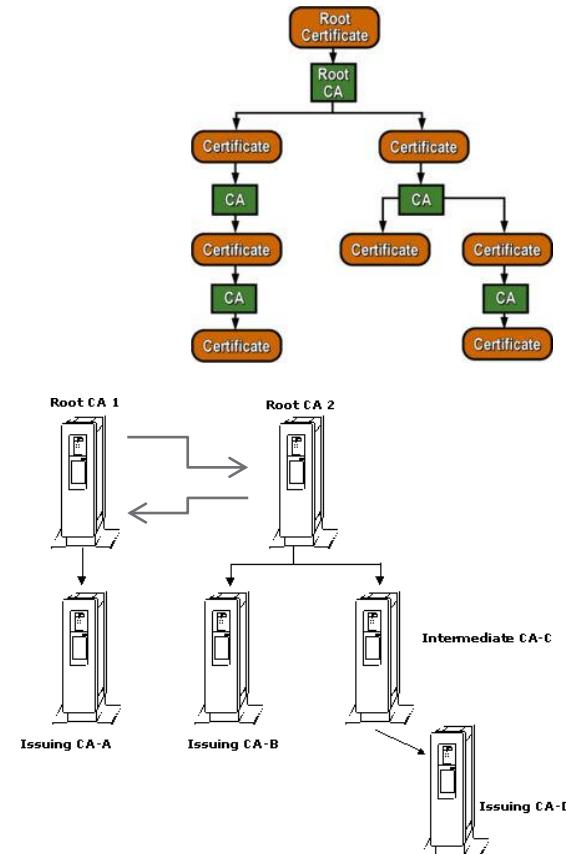


Figure 1: Illustration of subdivision of certification services used in the present document

Gestão de chaves - PKI

- Relações de confiança entre CAs
 - Existe um modelo hierárquico que estabelece as relações de confiança entre CAs diferentes, dentro da hierarquia de confiança mesmo.
 - No entanto, se os seus CAs não compartilham de uma raiz comum CA, deve ser realizada uma certificação cruzada
 - As CAs raiz devem desenvolver relações de confiança bilateral.
 - Constituindo um modelo híbrido de relações de confiança



Gestão de chaves - PKI

- Alguns referenciais
 - CEN - CWA 14167
 - Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures
 - Part 1: System Security Requirements
 - Part 2: cryptographic module for CSP signing operations — Protection Profile (MCSO-PP)
 - European Telecommunications Standards Institute (ETSI)
 - ETSI TS 101456 - Electronic Signatures and Infrastructures (ESI);
 - Policy requirements for certification authorities issuing qualified certificates
 - Baseado no IETF RFC 3647 - Internet X.509 Public Key Infrastructure
 - Para maior detalhe consultar o RFC 3647
 - ETSI TS 102 176 - Algorithms and Parameters for Secure Electronic Signatures
 - Part 1: Hash functions and asymmetric algorithms
 - Part 2: Secure channel protocols and algorithms for signature creation devices
 - ETSI TS 101 861 - Time stamping profile
 - Federal Information Processing Standard (FIPS), do NIST
 - FIPS 140-2 - Security Requirements for Cryptographic Modules

Ferramentas Uteis

- OpenPGP:
 - Kleopatra
- Cifra de disco
 - VeraCrypt

Segurança e Gestão de Risco

2ºSem 2023/24

Segurança da Informação

LUIS AMORIM

13 Abr 2024

74

