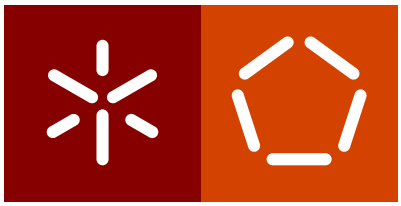
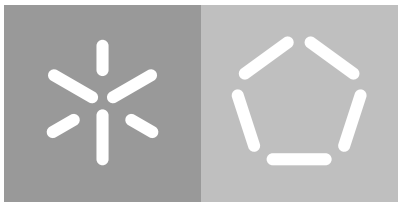


**Universidade do Minho**
Escola de Engenharia
Departamento de Informática

Joana Fernandes Cunha

# Gestão de Segurança de Informação para Sistemas de Confiança Seguros

Julho 2021



**Universidade do Minho**
Escola de Engenharia
Departamento de Informática

Joana Fernandes Cunha

# Gestão de Segurança de Informação para Sistemas de Confiança Seguros

Dissertação de Mestrado
Mestrado em Engenharia Informática

Dissertação supervisionada por
**Professor Doutor José Carlos Bacelar Almeida**

Julho 2021

## DIREITOS DE AUTOR E CONDIÇÕES DE UTILIZAÇÃO DO TRABALHO POR TERCEIROS

# AGRADECIMENTOS

Este trabalho só foi possível graças às pessoas que me acompanharam neste processo e me apoiaram nesta fase da minha vida, a quem desejo agradecer.

Em primeiro lugar, agradeço ao Doutor José Eduardo Pina Miranda, pela sugestão do tema, pelos conhecimentos que me transmitiu, pelo apoio incansável que me prestou ao longo do trabalho realizado, pela disponibilidade de tempo que me concedeu, orientando-me e ajudando-me a encontrar soluções. Por tudo, estou-lhe verdadeiramente grata.

Um agradecimento particular para ao Professor Doutor José Carlos Bacelar Almeida que, sem hesitação, aceitou orientar esta dissertação. Foi um privilégio tê-lo professor e como orientador e beneficiar do seu conhecimento, da sua experiência e dos seus conselhos.

Gostaria também de agradecer à equipa da INCM por ter permitido pôr em prática este trabalho.

Um grande obrigado à minha família pelo apoio incondicional que sempre me deram, pela força e pelos valores que me transmitiram. Sem eles, não seria possível ter chegado até aqui. Um agradecimento especial à minha mãe pela sua ajuda na revisão ortográfica.

Por fim, gostaria de agradecer aos meus amigos e colegas, que me acompanharam no meu percurso académico, sem eles este caminho teria sido muito mais aborrecido. Obrigada pelo apoio moral e intelectual que sempre me deram. Com a vossa força foi muito mais fácil chegar até aqui.

## DECLARAÇÃO DE INTEGRIDADE

Declaro ter atuado com integridade na elaboração do presente trabalho académico e confirmo que não recorri à prática de plágio nem a qualquer forma de utilização indevida ou falsificação de informações ou resultados em nenhuma das etapas conducente à sua elaboração. Mais declaro que conheço e que respeitei o Código de Conduta Ética da Universidade do Minho.

## RESUMO

Com o aumento da nossa dependência nos sistemas de informação também aumenta a necessidade de sistemas mais seguros e resilientes.

A pandemia que vivemos, há mais de um ano, veio agravar a situação e mostrou que temos de preparar os sistemas que suportam o nosso dia-a-dia para situações inesperadas e que podem comprometer o seu bom funcionamento.

Para proteger os sistemas é importante aplicar medidas preventivas. Existem *standards* que definem as melhores práticas para a segurança dos sistemas, que podem ser implementados pelas organizações para melhor se prepararem contra situações adversas. Destacam-se os *standards* desenvolvidos pelo *International Organization for Standardization* (ISO), na área de gestão de segurança de informação, e pelo *National Institute of Standards and Technology* (NIST), na área de sistemas de confiança seguros.

Cada vez mais a preocupação com a segurança da informação tem-se reflectido na legislação e regulamentação Europeia e Portuguesa.

Esta dissertação pretende analisar as melhores práticas na área da segurança de informação, através dessa análise, propor uma abordagem para a sua implementação e utilizá-la num caso prático, sendo este a infraestrutura de chave pública do Cartão de Cidadão.

Desta forma, ao longo desta dissertação são analisados os *standards* relevantes desenvolvidos pelo ISO e NIST. Além disso, com o objectivo de contextualizar o caso prático é analisada a regulamentação e legislação aplicável às infraestruturas de chave pública na Europa e em Portugal bem como as componentes da infraestrutura de chave pública do Cartão de Cidadão.

Com esta análise, foi possível apresentar uma abordagem que reduz a complexidade do processo de implementação dos *standards* e colocá-la em prática num projecto de reestruturação e actualização da gestão de segurança da informação da infraestrutura de chave pública do Cartão de Cidadão.



PALAVRAS-CHAVE: Segurança da Informação, Gestão de Segurança da Informação, Sistemas de Confiança Seguros, Gestão de Risco, Gestão de Incidentes, Infraestrutura de Chave Pública, Regulamento eIDAS.

## ABSTRACT

As our dependence on information systems increases, so does the need for more secure and resilient systems.

The pandemic that we have been experiencing, for over a year, has aggravated the situation and showed that we have to prepare the systems that support our day-to-day activities for unexpected situations that can compromise their proper functioning.

To protect systems it is important to apply preventive measures. There are standards that define the best practices for system security, which can be implemented by organizations to better prepare themselves against adverse situations. The standards developed by ISO, in the subject of information security management, and by NIST, in the subject of secure trust systems, are worth noting.

The concern with information security has been increasingly reflected in European and Portuguese legislation and regulations.

This dissertation intends to analyze the best practices in the area of information security, through this analysis, propose an approach for its implementation and use it in a practical case, this being the public key infrastructure of the Cartão de Cidadão.

Thus, throughout this dissertation, the relevant standards developed by ISO and NIST are analyzed. In addition, in order to contextualize the practical case, the regulations and legislation applicable to public key infrastructures in Europe and Portugal are analyzed, as well as the components of the public key infrastructure of the Cartão de Cidadão.

With this analysis, it was possible to present an approach that reduces the complexity of the standards implementation process and put it into practice in a project to restructure and update the information security management of the Cartão de Cidadão public key infrastructure.



KEYWORDS Information Security, Information Security Management, Trustworthy Secure Systems, Risk Management, Incident Management, Public Key Infraestructure, eIDAS Regulation.

# CONTEÚDO

# LISTA DE FIGURAS

# LISTA DE ACRÓNIMOS

**CISO** *Chief Information Security Officer*.
**CRL** *Certification Revocation List*.
**CVSS** *Common Vulnerability Scoring System*.
**DPO** *Data Protection Officer*.
**EC** Entidade de Certificação.
**eIDAS** *electronic IDentification, Authentication and trust Services*.
**ER** Entidade de Registo.
**ETSI** Instituto Europeu de Normas de Telecomunicações.
**EVC** Entidade de Validação Cronológica.
**HSM** *Hardware Security Module*.
**ICP** Infraestrutura de chave pública.
**IEC** *International Electrotechnical Commission*.
**INCM** Imprensa Nacional-Casa da Moeda.
**ISMS** *Information Security Management System*.
**ISO** *International Organization for Standardization*.
**NIST** *National Institute of Standards and Technology*.
**OCSP** *Online Certificate Status Protocol*.
**PMEs** Pequenas e Médias Empresas.
**PP** *Protection profiles*.
**RGPD** Regulamento Geral de Protecção de Dados.
**ST** *Security target*.
**TOE** *Target of evaluation"*.
**UTC** *Universal Time Coordinated*.

# GLOSSÁRIO

**A**

**AMEAÇA** Potencial causa de um incidente indesejado, que pode resultar em danos a um sistema ou organização.

**ASSINATURA DIGITAL** Os dados em formato electrónico que se ligam logicamente associados a outros dados em formato electrónico e que sejam utilizadas pelo signatário para assinar .

**ATAQUE** Tentativa de destruir, expor, alterar, desabilitar, roubar ou ganhar acesso não autorizado a recursos.

**AUDITORIA** Processo documentado, independente e sistemático para obter evidências de auditoria e avalia-las de forma objectiva para determinar até que ponto os critérios da auditoria são cumpridos.

**AUTENTICAÇÃO** Processo ou acção de verificar a identidade de um utilizador ou processo.

**C**

**CONFIDENCIALIDADE** Propriedade que a informação não é disponibilizada ou divulgada a indivíduos, processos ou entidades não autorizados.

**CONTROLO DE ACESSOS** Meios para garantir que o acesso a recursos é autorizado e restrito baseado em requisitos de segurança e de negócio.

**D**

**DISPONIBILIDADE** Propriedade de ser acessível e utilizável sob pedido de uma entidade autorizada.

**E**

**EVENTO DE SEGURANÇA DA INFORMAÇÃO** Ocorrência que indica uma possível falha da segurança da informação ou controlos.

**F**

**FONTE DE RISCO** Elemento que sozinho ou em combinação tem o potencial de dar origem a um risco.

**I**

**IDENTIFICAÇÃO ELECTRÓNICA** O processo de utilização dos dados de identificação pessoal em formato electrónico que representam de modo único uma pessoa singular ou colectiva ou uma pessoa singular que represente uma pessoa colectiva.

**INCIDENTE DE SEGURANÇA DA INFORMAÇÃO** Um ou múltiplos eventos de segurança da informação que podem causar danos aos recursos de uma organização ou às suas operações.

**INTEGRIDADE** Propriedade de precisão e completude.

**M**

**MEIO DE IDENTIFICAÇÃO ELECTRÓNICA** Uma unidade material e/ou imaterial que contenha os dados de identificação pessoal que seja utilizada para autenticação de um serviço ou linha.

**MONITORIZAÇÃO** Determinar o estado de um sistema, processo ou actividade.

**N**

**NÃO REPÚDIO** Capacidade de provar a ocorrência de um alegado evento ou acção e a entidade que o origina.

**P**

**PARTES INTERESSADAS** Pessoa ou organização que pode afectar, ou ser afectada, ou percepcionar ser afectada por uma decisão ou actividade.

**POLÍTICA** Intenções e direcções de uma organização formalmente expressas pela gestão da organização.

**PONTO DE CONTACTO** Função organizacional ou papel definido que serve como coordenador ou ponto focal de informação relacionada com as actividades de gestão de incidentes.

**PRESTADOR DE SERVIÇOS DE CONFIANÇA** A pessoa singular ou colectiva que preste um ou mais do que um serviço de confiança quer como prestador qualificado quer como prestador não qualificado.

**PRESTADOR QUALIFICADO DE SERVIÇOS DE CONFIANÇA** O prestador de serviços de confiança que preste um ou mais do que um serviço de confiança qualificado e ao qual é concedido o estatuto de qualificado pela entidade supervisora .

**PROCESSO** Conjunto de actividades interligadas ou interactivas que transformam *inputs* em *outputs*.

**R**

**RECURSOS** Elemento de valor para as partes interessadas, pode ser tangível ou intangível.

**REQUISITO** Necessidade ou expectativa que é declarada, geralmente, implícito ou obrigatório.

**RESPOSTA A INCIDENTES** Acções tomadas para mitigar ou resolver um incidente de segurança da informação, inclusive as acções tomadas para proteger e recuperar as condições normais de operação.

**REVOGAÇÃO** Terminação permanente da validade de um certificado antes da sua data de expiração.

**RISCO** Efeito ou incerteza nos objectivos.

**S**

**SEGURANÇA DA INFORMAÇÃO** Preservação da confidencialidade, integridade e disponibilidade de informação.

**SELO ELECTRÓNICO** Os dados em formato electrónico apenso ou logicamente associado a outros dados em formato electrónico para garantir a origem e a integridade destes últimos .

**SELOS TEMPORAIS** Os dados em formato electrónico que vinculam outros dados em formato electrónico a uma hora específica, criando uma prova de que esses outros dados existiam nesse momento.

**SERVIÇO DE CONFIANÇA** Um serviço electrónico geralmente prestado mediante remuneração, que consiste:

- Na criação, verificação e validação de assinatura digital, selo electrónico ou selos temporais, serviços de envio registado electrónico e certificados relacionados com estes serviços; ou
- Na criação, verificação e validação de certificados para a autenticação de sítios web; ou
- Na preservação das assinatura digital, selo electrónico ou certificados electrónicos relacionados com esses serviços

.

**SERVIÇO DE CONFIANÇA QUALIFICADO** Um serviço de confiança que satisfaça os requisitos aplicáveis estabelecidos no Regulamento eIDAS.

**SISTEMA DE IDENTIFICAÇÃO ELECTRÓNICA** Um sistema de identificação electrónica ao abrigo do qual sejam produzidos meios de identificação electrónica para as pessoas singulares ou colectivas, ou para as pessoas singulares que representem pessoas colectivas.

**V**

**VULNERABILIDADE** Fraqueza de um recurso ou controlo que pode ser explorada por uma ou mais ameaças.

Parte I

# MATERIAL INTRODUTÓRIO

# 1

# INTRODUÇÃO

Esta dissertação pretende estudar as melhores práticas nas áreas da segurança da informação e dos sistemas de confiança seguros, utilizando como exemplo prático as *Infraestrutura de chave públicas (ICPs)*. Ao longo da mesma, é descrito o trabalho de Mestrado, desenvolvido no contexto do Mestrado em Engenharia Informática, realizado no Departamento de Informática da Universidade do Minho.

Este tema de dissertação foi proposto pela empresa *DeviseFutures Lda*, com a orientação do Dr. José Eduardo Pina Miranda.

## 1.1 CONTEXTUALIZAÇÃO

Com o aumento da dependência na tecnologia a confiança que é depositada nos sistemas utilizados é cada vez mais importante. Ao mesmo tempo, observa-se um crescimento do número e eficácia dos ciber-ataques. A pandemia vivida no último ano, apesar de ter agravado o problema, também fez com que a preocupação com a segurança aumentasse por parte das organizações. Deste modo, é essencial que as organizações tomem medidas de segurança que protejam os seus recursos. O relatório da IBM [1] mostra que tomar medidas de segurança preventivas (e.g. soluções automatizadas, preparação de equipas de resposta) reduz significativamente o custo de uma fuga de dados.

A segurança da informação "garante a confidencialidade, integridade, disponibilidade e integridade da informação"(ISO/IEC 27000:2018 (en)). Com o objectivo de garantir uniformidade e coerência na segurança da informação as organizações ISO e *International Electrotechnical Commission (IEC)* em conjunto com outras organizações, estabeleceram a família de *standards* ISO/IEC 27000. Esta família de *standards* define os requisitos para estabelecer um sistema de gestão de segurança da informação. Um sistema de gestão de segurança da informação "é uma abordagem sistemática para estabelecer, implementar, operar, monitorizar, rever, manter e melhorar a segurança da informação de uma organização"(ISO/IEC 27000:2018 (en)). A segurança é ainda mais relevante quando falamos de sistemas que lidam com informação sensível ou que prestam serviços críticos onde qualquer

1 *Cost of a Data Breach Report 2020*, https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pt

falha pode significar danos irreparáveis. É, por isso, importante que estes sistemas sejam implementados de forma a fornecer garantias de segurança às partes interessadas.

Actividades de desenvolvimento de sistemas estruturadas que visem a segurança dos sistemas e que resultem em garantias para as partes interessadas promovem o desenvolvimento de sistemas de confiança seguros. Em face disto, o NIST definiu o NIST Special Publication 800-160 , com o objectivo de definir uma base para o desenvolvimento de sistemas de confiança seguros tendo como ponto de partida a engenharia de sistemas. Segundo o NIST Special Publication 800-160 um sistema de confiança seguro cumpre, não só requisitos de segurança específicos, como também outros requisitos críticos.

## 1.2 MOTIVAÇÃO

Uma das áreas onde a segurança é uma preocupação é na área dos sistemas de *e-government*. Estes são geralmente suportados por sistemas críticos onde qualquer falha pode ter consequências graves. As ICPs inserem-se nos sistemas críticos de *e-government*.

Neste sentido, tem-se notado uma crescente preocupação da União Europeia e de Portugal em garantir a segurança dos seus sistemas e de outros sistemas críticos. Consequentemente, têm-se espelhado essas preocupações na regulamentação e legislação Europeia e Portuguesa.

### *Regulamento (UE) Nº910/2014*

O Regulamento (UE) Nº910/2014 do Parlamento Europeu e do Conselho de 23 de Julho de 2014, também conhecido como Regulamento *electronic IDentification, Authentication and trust Services (eIDAS)*, "pretende reforçar a confiança nas transições electrónicas no mercado interno criando uma base para a realização de interacções electrónicas em condições seguras"(Regulamento eIDAS).

Um dos objectivos deste regulamento é garantir que os serviços de identificação e autenticação electrónica são utilizados com segurança, sendo necessário, por parte dos prestadores de serviços, cumprir a legislação aplicável à protecção de dados pessoais, em particular, o Regulamento (UE) Nº2016/679 do Parlamento Europeu e do Conselho de 27 de Abril de 2016, também conhecido como *Regulamento Geral de Protecção de Dados (RGPD)*, RGPD.

O Regulamento eIDAS também afirma que a "segurança dos sistemas de identificação electrónica é fundamental para a fiabilidade do reconhecimento mútuo"(Regulamento eIDAS). Assim, todos "os prestadores de serviços de confiança deverão aplicar boas práticas de segurança adequadas aos riscos inerentes às suas actividades"(Regulamento eIDAS).

O Regulamento eIDAS vai mais além definindo, no Artigo 19º, os requisitos de segurança aplicáveis aos prestadores de serviços de confiança afirmando que os prestadores de serviços de confiança "tomam as medidas de carácter técnico e organizativo que forem

adequadas para gerir os riscos que se colocam à segurança do serviços de confiança que prestam"(Regulamento eIDAS).

Por conseguinte, a organização *Instituto Europeu de Normas de Telecomunicações (ETSI)* desenvolveu um conjunto de *standards* cujos requisitos de segurança estão conforme o Regulamento eIDAS.

Os *standards* da organização ETSI referem outros *standards*, em particular, referem vários *standards* relacionados com a gestão de risco e práticas de segurança da informação (como o ISO/IEC 27002:2013 (E)).

Devido à criticidade destes serviços e da informação que processam, a segurança é essencial para que cumpram a legislação e regulamentação aplicável. Também os sistemas que suportam estes serviços devem fornecer garantias de segurança às partes interessadas.

### 1.2.1 *Regulamento (UE) 2016/679*

O Regulamento RGPD ( RGPD), estabelece as regras relativas ao tratamento, por uma pessoa, empresa ou organização, de dados pessoais relativos a pessoas na União Europeia.

Este regulamento estabelece que "os dados pessoais deverão ser tratados de uma forma que garanta a devida segurança e confidencialidade, incluindo para evitar o acesso a dados pessoais e equipamento utilizado para o seu tratamento, ou utilização dos mesmos, por pessoas não autorizadas"( RGPD). Neste sentido, as organizações têm a obrigação de garantir que, quando são processados dados pessoais, são implementadas medidas de segurança preventivas. Estas devem ser adequadas aos riscos que a organização corre.

### 1.2.2 *Lei nº46/2018*

A Lei nº 46/2018 "estabelece o regime jurídico da segurança do ciberespaço", Lei nº 46/2018.

Esta lei estabelece, no artigo 14º, os requisitos de segurança para a administração pública e operadores de infraestruturas críticas, em particular, afirma que estes "devem cumprir as medidas técnicas e organizativas adequadas e proporcionais para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam", Lei nº 46/2018. As medidas devem "garantir um nível de segurança adequado ao risco em causa, tendo em conta os progressos técnicos mais recentes", Lei nº 46/2018.

Tendo isto em conta, uma forma das organizações cumprirem o estabelecido na Lei nº46/2018 é através da utilização e implementação das melhores práticas internacionalmente aceites, como é o caso da família de *standards* ISO/IEC 27000.

## 1.3 OBJECTIVOS

Esta dissertação foca-se na gestão de segurança da informação de sistemas de confiança seguros, com destaque na área das ICPs, incluindo:

- Analisar as melhores práticas para a gestão de segurança da informação e para os sistemas de confiança seguros;
- Propor uma abordagem para a implementação das melhores práticas analisadas;
- Implementar as melhores práticas no caso prático da ICP do Cartão de Cidadão.

## 1.4 ESTRUTURA DO DOCUMENTO

Ao longo desta dissertação são analisadas e postas em prática as recomendações internacionais no que toca à gestão de segurança da informação e aos sistemas de confiança seguros.

Nas secções 2.1 e 2.2 realiza-se uma análise dos *standards* mais utilizados para a segurança da informação e para os sistemas de confiança seguros, com destaque para os *standards* desenvolvidos pelo NIST e pelo ISO.

De seguida, na secção 3.1, apresenta-se uma visão geral da ICP do Cartão de Cidadão e os mecanismos de segurança da informação implementados. Na secção 3.2 analisa-se a legislação e regulamentação aplicável às ICPs. Este capítulo serve como contextualização para o caso prático apresentado no capítulo 5.

No capítulo 4 apresenta-se uma abordagem à implementação dos conceitos dos *standards* para obter um sistema de confiança seguro e/ou um sistema de gestão de segurança da informação.

Por fim, no capítulo 5 descreve-se a aplicação de um sistema de gestão de segurança da informação utilizando a abordagem definida no capítulo 4 e a regulamentação e legislação analisada na secção 3.2.

Parte II

# NÚCLEO DA DISSERTAÇÃO

# 2

# ESTADO DE ARTE

Neste capítulo é apresentado o estado da arte actual e uma revisão de literatura referente à segurança da informação e aos sistemas de confiança seguros.

## 2.1 SISTEMAS DE CONFIANÇA SEGUROS

O foco desta secção é a abordagem do NIST aos sistemas de confiança seguros, em particular o documento NIST Special Publication 800-160, que trata do problema da segurança de sistemas usando princípios da engenharia de sistemas.

### 2.1.1 *Engenharia de Segurança de Sistemas*

A engenharia de segurança de sistemas é uma vertente especializada da engenharia de sistemas e estabelece a base para as actividades e tarefas de segurança, NIST Special Publication 800-160. Quando correctamente aplicada, ajuda a garantir que o sistema é de confiança.

Neste sentido, é importante definir a noção de segurança que, no caso do referido documento, a define como "a inexistência de condições que podem causar perda de recursos com consequências inaceitáveis"(NIST Special Publication 800-160). O valor de cada recurso deve ser determinado pelas partes interessadas. A partir desse valor, são determinadas as medidas de protecção apropriadas para garantir o bom funcionamento do sistema.

No documento NIST Special Publication 800-160, a protecção do sistema é vista como um objectivo de controlo do sistema e um problema de *design*. A solução do problema passa não só por prevenir, mas também por detectar, minimizar, responder, recuperar e prever a perda de recursos e as suas consequências.

É importante ressalvar que a perda de recursos pode advir de vários acontecimentos, incluindo intencionais, acidentais, erro, fraquezas, defeitos, mau uso, entre outros.

Esta noção de protecção permite que a perda de recursos seja directamente relacionada com o funcionamento incorrecto do sistema.

*Framework da Engenharia de Segurança de Sistemas*

A *framework* da Engenharia de Segurança de Sistemas, apresentada na figura 1 (baseada em figura do NIST Special Publication 800-160), tem como objectivo garantir que a segurança do sistema é adequada aos objectivos de segurança e necessidades de protecção, de acordo com a visão das partes interessadas.

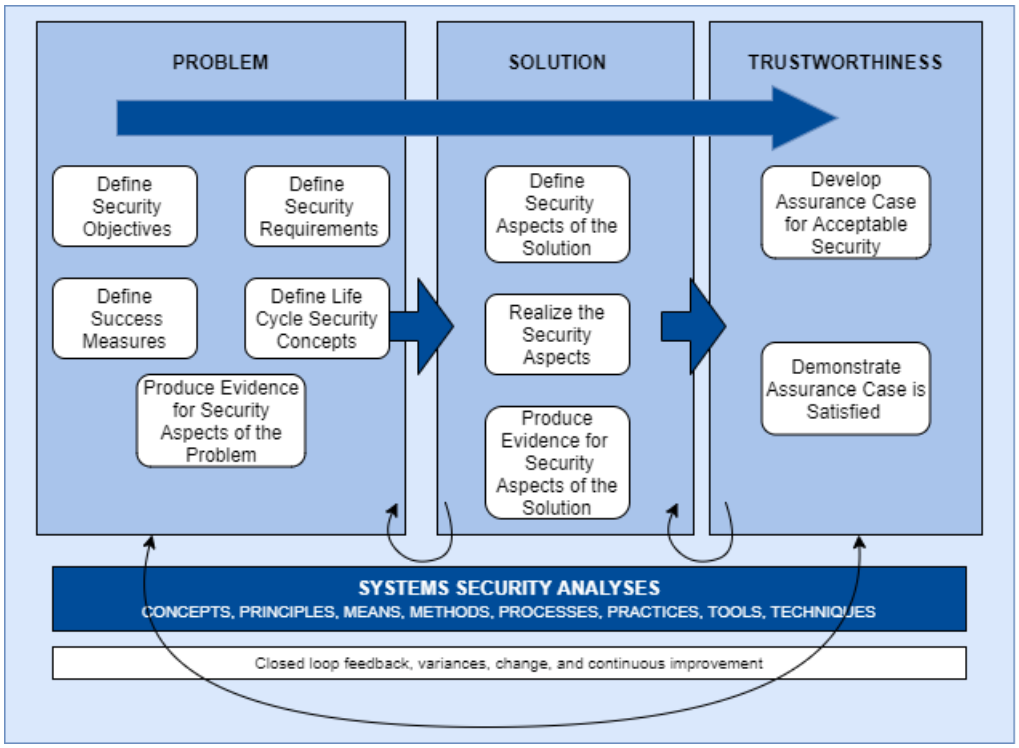



Figura 1: *Framework* da engenharia de sistemas de segurança baseada em figura apresentada no NIST Special Publication 800-160

Esta *framework* divide-se em três contextos: o problema, a solução e a confiança.

- O Problema

  Este contexto tem como objectivo determinar a base para atingir os objectivos de segurança adequados às necessidades do sistema (missão, capacidade, *performance*). Para tal, devem ter-se em conta as restrições impostas pelas partes interessadas (custos, prazos, risco e perdas). Resumindo, nesta fase são determinados os requisitos de segurança de acordo com os objectivos de segurança.

- A Solução

  Nesta fase, os requisitos de segurança determinados são transformados em requisitos de *design* do sistema. Para o efeito, é necessário existir um balanço entre estratégias

reactivas e pro-activas. Aqui é construída a estratégia de protecção do sistema e as métricas de verificação da *performance* das medidas de segurança.

- A Confiança

  Passo em que são recolhidas as provas que garantem a segurança e a confiança que o sistema merece.

  Esta fase fornece a base de prova de que o sistema é merecedor de confiança de acordo com os objectivos de segurança. Esta confiança é conseguida através de um conjunto de provas de que o sistema cumpre os requisitos de segurança a que se propõe. Estas provas são fundamentadas e auditáveis e são usadas para demonstrar propriedades do sistema (e.g. segurança, resiliência, confiabilidade, capacidade de sobrevivência).

### 2.1.2 *Ciclo de vida do sistema*

Com o fim de obter os níveis de segurança desejados é importante alinhar as actividades da engenharia de segurança de sistemas com o ciclo de vida do sistema. Na figura 2 (baseada em figura do NIST Special Publication 800-160) podemos observar os vários processos do ciclo de vida do sistema e as actividades desenvolvidas nesses processos. Estes processos não são mapeados explicitamente a estados do ciclo de vida do sistema, são sim, "processos executados como necessário para conseguir objectivos específicos da engenharia de sistemas"(NIST Special Publication 800-160). Assim, os processos podem ser aplicados "concorrentemente, iterativamente ou recursivamente em qualquer nível da estrutura hierárquica do sistema, (...), ou em qualquer estado do ciclo de vida do sistema", ( NIST Special Publication 800-160).

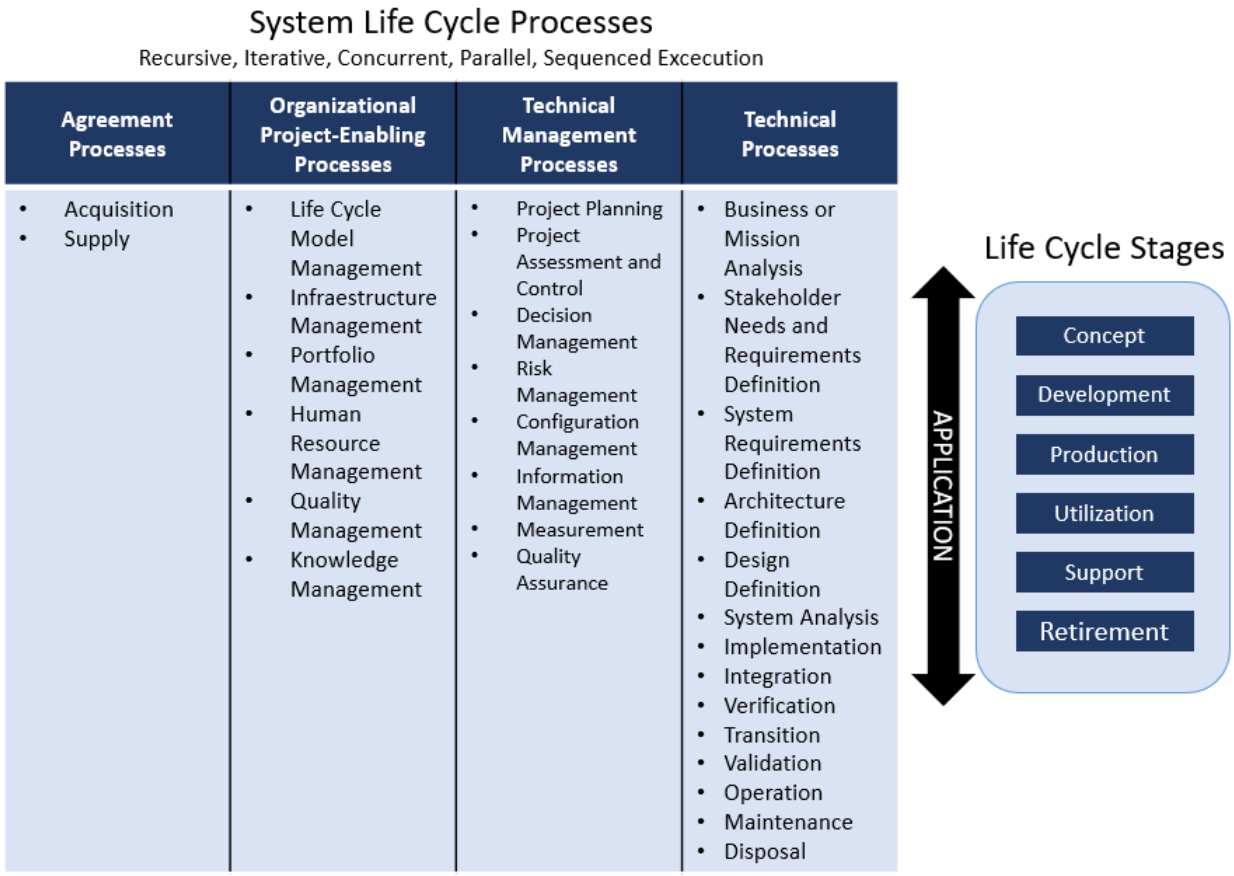



Figura 2: Processos e estados do ciclo de vida de sistemas (baseada em figura do NIST Special Publication 800-160)

Este documento inclui explicitamente as actividades de engenharia de segurança de sistemas desenvolvidas em cada processo do ciclo de vida do sistema. Estas actividades geram um conjunto de resultados que, combinados, constroem um sistema seguro e as provas necessárias para substanciar a confiança no sistema.

*Processo de Acordo*

O processo de acordo subdivide-se em dois processos: o processo de aquisição e o processo de fornecimento.

Neste, as actividades de engenharia de segurança de sistemas têm como objectivo garantir que a segurança e protecção do sistema é tida em conta durante o processo de aquisição e que, no processo de fornecimento, são tidas em conta as preocupações de segurança dos clientes. Assim, o documento define um conjunto de actividades a desenvolver durante estes processos para se garantirem os objectivos. Estas actividades incluem o estabelecimento de acordos entre as partes que definem os requisitos de segurança a cumprir.

No processo de aquisição, a engenharia de segurança de sistemas serve para garantir que a segurança e protecção são considerados na obtenção de um certo produto ou serviço. As actividades da engenharia de segurança de sistemas desenvolvidas durante este processo incluem:

- Definir os aspectos de segurança relacionados com a aquisição (e.g. critérios de segurança a cumprir, produtos ou serviços de segurança necessários);
- Comunicar e seleccionar um ou mais fornecedores que cumpram os requisitos de segurança;
- Elaborar e manter os requisitos de segurança de acordos com os fornecedores;

Realizando estas actividades, é garantido que os aspectos de segurança são integrados nos acordos com os fornecedores e os produtos/serviços adquiridos cumprem os requisitos de segurança necessários.

No processo de fornecimento, a engenharia de segurança de sistemas garante que o produto/serviço prestado cumpre os requisitos de segurança do cliente. Neste caso, as actividades da engenharia de segurança de sistemas envolvem:

- Definir as necessidades de segurança do cliente e uma reposta que satisfaz essas necessidades;
- Desenvolver e manter um acordo com os requisitos de segurança;
- Executar e avaliar o acordo;
- Entregar e assegurar um produto/serviço que cumpre os requisitos de segurança acordados.

Executando estas actividades, é garantido que os produtos/serviços prestados estão de acordo com os critérios de segurança do cliente.

*Processos organizacionais de projectos*

Este processo divide-se em seis sub-processos:

- Gestão do ciclo de vida

  As actividades de engenharia de segurança de sistemas desenvolvidas, têm como objectivo identificar e avaliar as necessidades de segurança do sistema. Estas actividades incluem o desenvolvimento de políticas e procedimentos relacionadas com a segurança do sistema, a definição de papéis e autoridades de segurança, a definição de critérios de segurança para cada estado do ciclo de vida e a análise e melhoria contínua da segurança do sistema.

- Gestão da infraestrutura

  As actividades da engenharia de segurança de sistemas incluem a definição dos requisitos de segurança da infraestrutura, a obtenção dos recursos que permitem cumprir esses requisitos e a manutenção de uma infraestrutura segura.

- Gestão de *portfolio*

  As actividades de engenharia de segurança de sistemas desenvolvidas incluem identificar os requisitos de segurança de cada projecto, alocar os recursos necessários à segurança do projecto, autorizar a inicialização de cada projecto de acordo com os princípios de segurança do plano do projecto, avaliar a segurança de cada projecto para garantir a sua viabilidade, terminar projectos que por razões de segurança não são viáveis e projectos em que o acordo de produto/serviço tenha finalizado.

- Gestão de recursos humanos

  A engenharia de segurança de sistemas, neste processo, tem como objectivo definir os critérios de segurança relativos à qualificação, avaliação, selecção e formação dos recursos humanos. Para tal, as actividades a desenvolver incluem a identificação das competências de engenharia de segurança necessárias e o desenvolvimento de um plano de formação.

- Gestão de qualidade

  As actividades de engenharia de segurança desenvolvidas incluem a definição dos objectivos de segurança da gestão de qualidade, definição de políticas e procedimentos, obtenção e análise dos resultados da avaliação de qualidade.

- Gestão de conhecimento

  As actividades desenvolvidas incluem a identificação do conhecimento de segurança necessário, a partilha desse conhecimento através da organização e a aquisição de conhecimento.

*Processo de gestão técnica*

Este processo é divido em oito processos:

- Planeamento de projecto

  As actividades da engenharia de segurança de sistemas incluem a identificação e definição dos objectivos e restrições de segurança do projecto, definição e comunicação de um plano para a execução do projecto, aquisição dos recursos necessários para garantir que os requisitos de segurança do projecto são cumpridos, implementação das medidas de segurança definidas no plano do projecto.

- Controlo e análise do projecto

  Algumas das actividades de engenharia de segurança de sistema desenvolvidas são: definir a estratégia de controlo e de avaliação tendo em conta a segurança do projecto, monitorizar e avaliar todas as componentes de segurança do projecto, conduzir auditorias e revisões e iniciar actividades de melhoria.

- Gestão de decisão

  As actividades de engenharia de segurança de sistemas incluem, entre outras, definir os aspectos de segurança a ter em conta na tomada de decisões, determinar os resultados pretendidos e critérios de selecção, avaliar as várias alternativas de acordo com os critérios de segurança definidos, registar e avaliar a decisão tomada.

- Gestão de risco

  A engenharia de segurança de sistemas, neste processo, consegue identificar, analisar, tratar e monitorizar os riscos de segurança existentes. Desta forma, algumas das actividades desenvolvidas são:

  - Definir as categorias do risco, classes, tipos e consequências da perda de recursos;
  - Definir regras de aceitação de riscos;
  - Identificar os riscos em cada categoria;
  - Estimar a probabilidade e as consequências da ocorrência de cada risco identificado;
  - Definir e implementar estratégias de tratamento de riscos;
  - Monitorizar e avaliar as medidas de tratamento de risco;
  - Monitorizar o aparecimento de novos riscos.

- Gestão de configuração

  Algumas das actividade de engenharia de segurança de sistemas desenvolvidas incluem definir medidas de arquivo e de obtenção de artefactos e informação de configuração, estabelecer os requisitos de segurança de hierarquia e estrutura da informação do sistema, estabelecer a nomenclatura de segurança de identificação do sistema e dos seus elementos, definir acções para coordenar e avaliar pedidos de alterações, recolher, transmitir e arquivar informação sobre a segurança da gestão de configuração e executar auditorias à gestão de configuração

- Gestão de informação

  Neste processo, a engenharia de segurança de sistemas garante que todas as necessidades de protecção das partes interessadas e todas as restrições e considerações de

segurança são consideradas. Assim, as actividades desenvolvidas incluem a definição dos requisitos para proteger a informação, nomear papéis com a responsabilidade pela segurança da gestão de informação, manter os recursos de informação arquivados de forma segura, manter o acesso à informação seguro e eliminar informação de forma segura.

- Métricas

  Neste processo é recolhida, analisada e comunicada informação sobre a segurança do sistema. As actividades desenvolvidas incluem a selecção e especificação de métricas relevantes, definição de procedimentos para o levantamento, análise e comunicação de informação relevante, definição de critérios para avaliar, arquivar e comunicar resultados.

- Garantia de qualidade

  Este processo tem como objectivo garantir a qualidade da segurança ao longo de todo o projecto, e deve ser conduzido de forma independente de todos os outros processos do ciclo de vida. As actividades de engenharia de segurança de sistemas desenvolvidas incluem avaliar produtos/serviços, ferramentas e ambiente de acordo com os critérios de segurança estabelecidos, verificar se os resultados dos vários processos do ciclo de vida cumprem os requisitos de segurança impostos, avaliar se os requisitos impostos em acordos são cumpridos, arquivar e comunicar de forma segura informação relevante relativa à garantia de qualidade, analisar, classificar e resolver incidentes de segurança, implementar e monitorizar medidas de tratamento de problemas, informar as partes interessadas de incidentes e problemas.

*Processos técnicos*

Este processo subdivide-se nos seguintes processos:

- Análise de missão ou negócio

  A engenharia de segurança, quando incorporada neste processo, permite identificar os objectivos, requisitos e considerações de segurança a ter em conta para fazer escolhas. Assim sendo, algumas das actividades de engenharia de segurança de sistemas a desenvolver são:

  - Rever e analisar problemas e oportunidades;
  - Identificar e planear sistemas ou serviços que suportam a segurança do sistema;
  - Definir as considerações de segurança iniciais;
  - Identificar, avaliar e seleccionar soluções para atingir a segurança desejada.

- Definição de requisitos e necessidades das partes interessadas

  Neste processo são definidos os requisitos de segurança das partes interessadas. Para tal, algumas das actividades desenvolvidas incluem determinar as preocupações de segurança e protecção das partes interessadas e transpor essas preocupações em requisitos, identificar e planear o acesso a sistemas que possam suportar esses requisitos, identificar os recursos e as classes dos recursos das partes interessadas, determinar a importância de cada recurso e as consequências associadas à sua perda, desenvolver cenários para identificar todas as necessidades de protecção, identificar interacções entre utilizador e sistema, definir métricas de *performance*, recolher dados acerca da protecção de cada recurso, obter consentimento explícito nos requisitos definidos e fornecer informação às partes interessadas sobre a segurança do sistema.

- Definição de requisitos do sistema

  Neste processo os requisitos definidos nos processos anteriores são transpostos em requisitos do sistema e servem como base para a definição da arquitectura, *design*, implementação e integração do sistema. Algumas das actividades de engenharia de segurança de sistemas desenvolvidas são: definir o âmbito da segurança e os seus vários domínios, definir as funções de segurança que o sistema deve executar, incorporar os requisitos de segurança nos requisitos do sistema, avaliar os requisitos e definir métricas de *performance*.

- Definição de arquitectura

  As actividades de engenharia de segurança de sistemas desenvolvidas incluem identificar os principais factores que possam impactar a segurança, definir os requisitos de segurança para a arquitectura do sistema, definir critérios de avaliação, identificar e obter sistemas que suportam a segurança da arquitectura, definir o conceito de funções seguras para a arquitectura de sistemas, seleccionar ou desenvolver ferramentas e técnicas de modelação de segurança, estabelecer funções/propriedades/comportamentos de segurança a entidades da arquitectura, seleccionar os modelos de segurança das arquitecturas possíveis, definir interfaces, interconexões e interacções do sistema com entidades externas, definir os princípios de *design* de segurança, avaliar as possíveis arquitecturas e seleccionar a que melhor se enquadra, obter consentimento das partes interessadas, manter a arquitectura sempre de acordo com os requisitos de segurança e organizar, avaliar e controlar a evolução dos modelos de segurança.

- Definição de *design*

  As actividades de engenharia de segurança de sistemas desenvolvidas incluem: aplicar o conceito de função de segurança definido no processo de definição de arquitectura, determinar e obter as tecnologias de segurança necessárias a cada elemento do sistema,

analisar as várias alternativas de *design* de segurança, analisar e obter elementos que protejam directamente o sistema e gerir o *design* da segurança do sistema.

- Análise do sistema

  Os resultados da análise de segurança do sistema servem como base para os factores de segurança da tomada de decisões. Algumas das actividades desenvolvidas incluem: definir objectivos, âmbito, nível de garantia e fidelidade, seleccionar os métodos a utilizar, identificar e validar suposições, aplicar os métodos seleccionados, rever e arquivar resultados e estabelecer conclusões e recomendações.

- Implementação

  Neste processo, as considerações de segurança de outros processos são postas em prática e criam um elemento do sistema que cumpre os requisitos de segurança, de arquitectura e de *design* do sistema. Algumas das actividades desenvolvidas são: implementar ou adaptar os elementos do sistema de acordo com os requisitos de segurança e procedimentos de implementação, acondicionar e arquivar os elementos do sistema de forma segura, recolher a informação necessária que garante que os elementos do sistema cumprem os requisitos de segurança e registar os resultados da implementação e qualquer anomalia encontrada.

- Integração

  Neste processo, os elementos do sistema implementados são combinados para formarem uma configuração segura do sistema. As actividades desenvolvidas incluem: definir *checkpoints* para as operações de confiança seguras, identificar as restrições de segurança que advêm deste processo, obter os elementos dos sistemas implementados de acordo com critérios de segurança, requisitos e prazos estabelecidos em acordos, combinar elementos do sistema implementados, verificar as características de segurança em termos de comportamento, interacções, *performance* e eficácia entre componentes do sistema e registar os resultados da integração e quaisquer problemas.

- Verificação

  Com este processo, pretende-se produzir as evidências da segurança do sistema. Assim, as actividades desenvolvidas incluem: identificar as acções de verificação de segurança, seleccionar métodos e técnicas para a verificação, integrar as acções de verificação de segurança nos procedimentos de verificação e executar esses procedimentos (procedimento de exactidão, de vulnerabilidades, de intrusão, de abuso e mau uso), analisar os resultados da verificação de segurança, registar resultados e qualquer anomalia, registar as características de incidentes e problemas e obter a aprovação das partes interessadas relativamente aos resultados obtidos.

- Transição

  Neste processo, o sistema passa para o estado operacional. As actividades de engenharia de segurança desenvolvidas incluem: identificar necessidades de alterar as instalações ou a localização e aplicá-las, identificar e providenciar o treino necessário para utilizar e manter o sistema, entregar e instalar o sistema de forma segura, demonstrar que o sistema está instalado correctamente, demonstrar que o sistema instalado é seguro e registar os resultados do processo de transição.

- Validação

  Este processo tem como objectivo demonstrar que o sistema cumpre os objectivos de segurança referentes a rupturas, desastres e ameaças antecipadas. As actividades desenvolvidas incluem: definir as acções de validação da segurança, seleccionar os métodos e técnicas apropriados, desenvolver a estratégia de validação de segurança, definir os procedimentos de validação de segurança, executar os procedimentos em ambientes definidos, rever e registar resultados e obter a aprovação das partes interessadas relativamente aos resultados.

- Operação

  As actividades de engenharia de segurança de sistemas desenvolvidas incluem: desenvolver as considerações de segurança da estratégia de operação ( disponibilidade do serviço, estratégia de recrutamento de operadores, critérios de lançamento e reaceitação, modos de operação, métricas de operação), *design*ar e treinar pessoal necessário à operação do sistema, aplicar recursos para operar o sistema de forma segura, monitorizar a segurança da operação do sistema (aderência à estratégia, garantir que o sistema é operado de forma segura, confirmar a *performance* do sistema), identificar e registar falhas de *performance*, executar operações de contingência e determinar até que ponto os serviços de segurança respondem às necessidades dos clientes.

- Manutenção

  As actividades de engenharia de segurança de sistemas desenvolvidas neste processo incluem: definir a estratégia (manutenção correctiva e preventiva, acções preventivas programadas, estratégia de logística, número e tipo de substituições, prevenção contra modificação e falsificação, níveis e capacidades de pessoal, métricas de *performance* de manutenção e logísticas), rever relatórios de incidentes e problemas para identificar necessidades, implementar procedimentos de correcção de falhas e substituições programadas de elementos do sistema, implementar acções de restauro em caso de falha, substituir ou executar manutenção de elementos do sistema antes de acontecer uma falha, identificar falhas no sistema, implementar operações logísticas (acondicionamento, manuseamento, arquivo e transporte) de forma segura, verificar se a segurança

das acções logísticas é suficiente, registar resultados e gerir incidentes e problemas relacionados com a manutenção e logística.

- Cessação

  A engenharia de segurança de sistemas, quando incorporada neste processo, tem como objectivo a cessação de elementos do sistema (incluindo recursos humanos) de forma segura. Algumas das actividades desenvolvidas incluem: desenvolver os aspectos de segurança a ter em conta (terminação de funções do sistema mas com a manutenção segura dos serviços e funções restantes, término de actividades de recursos humanos, resolução de qualquer alteração ao sistema, solucionar qualquer preocupação de segurança, alterar o sistema e os seus elementos para uso futuro), definir critérios para arquivo seguro, excluir a hipótese de recursos eliminados serem utilizados, remover os sistemas ou elementos do sistema de forma segura, remover credenciais, material sensível e autorizações de acesso de recursos humanos, desmantelar o sistema ou elementos do sistema em componentes, preparar os artefactos apropriadamente para a sua cessação, verificar se a cessação de elementos não resulta em problemas de segurança e arquivar e proteger a informação gerada durante o ciclo de vida.

### 2.1.3 *Papéis, responsabilidades e habilitações*

O papel definido no NIST Special Publication 800-160 é o de engenheiro de segurança de sistema. Este deve ter um conhecimento alargado em várias áreas de segurança.

As suas responsabilidades incluem:

- Resolver as preocupações de segurança e risco das partes interessadas;
- Garantir que a segurança é eficaz e adequada;
- Assistir na análise de alternativas;
- Fornecer provas de que o sistema é de confiança;
- Executar as actividades de gestão de risco e, com os resultados, cooperar com outras equipas no impacto de vulnerabilidades e ameaças.

Por fim, ao definir papéis de segurança específicos é importante entender qual o seu objectivo e responsabilidades associadas, sendo, assim, possível, identificar os conhecimentos apropriados para cumprir essas responsabilidades.

### 2.1.4 *Conceitos de design para a segurança*

Os conceitos apresentados servem como base para garantir a confiabilidade do sistema.

*Arquitectura e design do sistema*

- Abstracções claras - O sistema deve ter "*interfaces* e funções simples e bem definidas"(NIST Special Publication 800-160).
- Mecanismos comuns mínimos - Minimizar os mecanismos comuns a mais do que um utilizador e que todos os utilizadores necessitam.
- Modularidade e camadas - Isolar funções em unidades lógicas e compreender essas unidades para evitar complexidades desnecessárias.
- Dependências parcialmente ordenadas - Definir uma ordem para dependências, com o objectivo de problemas inerentes de circularidade possam ser mais fáceis de gerir.
- Acesso mediado eficazmente - O acesso a recursos do sistema deve ser mediado tendo em conta a minimização dos mecanismos comuns, no entanto, deve-se prestar atenção a situações de má *performance*.
- Minimizar a partilha - Não deve existir partilha de recursos entre as componentes do sistema a não ser quando estritamente necessário, nestes casos, deve ser feita uma avaliação detalhada.
- Reduzir a complexidade - O sistema deve ser o mais simples possível. A simplicidade de um sistema está directamente relacionada com a quantidade de vulnerabilidades do sistema.
- Melhoria segura - O sistema deve ser desenvolvido de forma a facilitar a manutenção da segurança quando são feitas alterações.
- Componentes de confiança - A segurança da componente deve ser proporcional à segurança necessária às suas dependências, porque o nível de confiança atribuído a um conjunto de componentes interligadas é dado pela componente com o nível de confiança mais baixo, assim, este princípio consegue que a confiança no sistema não seja diminuída por uma componente.
- Confiança hierárquica - Para analisar eficazmente o nível de confiança de um sistema é importante eliminar dependências circulares. Organizando as componentes de forma a que as de maior confiança estejam numa camada superior às de menor confiança, permite uma base para garantir a confiança do sistema.
- Limite de modificação inversa - A protecção de uma componente deve ser proporcional ao nível de confiança dessa componente.

- Protecção hierárquica - Não é necessário proteger uma componente de outras componentes de confiança, isto é, uma componente deve estar protegida contra componentes de menor nível de confiança mas não necessita de ser protegida de componentes de nível de confiança igual ou superior.
- Elementos de segurança minimizados - Por forma a simplificar o sistema e os custos associados, é necessário manter apenas os elementos de segurança necessários para o nível de confiança desejado.
- Minimizar privilégios - Os privilégios dados a cada componente devem ser apenas os estritamente necessários para as suas funções.
- Separação de privilégios - Qualquer operação crítica deve ser alvo de autorização de várias entidades.
- Confiança auto-suficiente - A confiança de um sistema deve ser incorporada nele e não deve depender de entidades externas.
- Composição distribuída segura - Num sistema distribuído, a política de segurança deve ser aplicada em todas as componentes do sistema de forma consistente.
- Canais de comunicação de confiança - No caso de ser necessário comunicação entre componentes, estas devem ser feitas através de canais com a segurança exigida pelas suas dependências. Os canais devem ser protegidos contra acesso indesejado e protecção dos dados transmitidos ponto-a-ponto.

*Capacidade de segurança e comportamentos intrínsecos*

Estes princípios "descrevem o comportamento de protecção que deve ser especificado, desenhado e implementado para garantir as propriedades emergentes de segurança do sistema".

Os princípios são:

- Protecção contínua - A protecção das componentes e dados que efectivam a política de segurança devem ter protecção ininterrupta e consistente com a política de segurança. Para garantir a protecção contínua é necessário garantir a protecção durante uma falha e durante a recuperação do sistema, utilizar o conceito de monitor de referência e que qualquer alteração à política de segurança não colocará o sistema num estado inseguro.
- Gestão segura de meta-dados - Devem ser colocadas em prática medidas de protecção que garantam a confidencialidade e integridade dos meta-dados.

- Auto-análise - Uma componente deve ser capaz de analisar o seu estado interno. Este princípio pode ser conseguido através de uma análise "debaixo para cima"da hierarquia de confiança, isto é, componentes de um nível inferior verificam a integridade da informação de uma componente de um nível superior.
- Responsabilidade e rastreabilidade - Todas as acções de segurança devem poder ser rastreadas à entidade que está a ser protegida por elas. Para o efeito, todas as acções que tenham impacto na segurança do sistema devem ser registadas, a política de responsabilidade deve obrigar que registos de auditorias sejam protegidos contra modificação ou acesso não autorizado, analisar eventos associados com a violação da política de segurança.
- Segurança por padrão - A configuração padrão do sistema deve cumprir a política de segurança. Este princípio aplica-se à configuração inicial do sistema e deve seguir o princípio de rejeitar, a não ser que esteja explicitamente autorizado.
- Falha e recuperação segura - Qualquer falha ou acção de recuperação pode violar a política de segurança. O sistema deve detectar falhas reais ou eminentes e executar as medidas para garantir que a política de segurança não é violada e o sistema é capaz de se recuperar mas mantendo-se num estado seguro.
- Segurança económica - Os mecanismos de segurança escolhidos devem ter em conta uma análise de custo-benefício. Isto permite que o custo dos mecanismos de segurança seja proporcional às possíveis perdas em caso de falha.
- *Performance* de segurança - Os mecanismos de segurança não devem prejudicar a *performance* do sistema de forma desnecessária. O impacto dos mecanismos de segurança deve ser analisado e deve existir um balanço entre a *performance* e a segurança do sistema.
- Segurança de factores humanos - Os mecanismos de segurança não devem ser intrusivos ao utilizador e a interface deve ser mantida intuitiva e de fácil utilização e, no caso do utilizador efectuar escolhas inseguras, deve ser avisado de forma clara. Neste caso, é necessário um balanço entre a usabilidade e segurança do sistema.
- Segurança aceitável - As expectativas dos utilizadores quanto ao nível de privacidade e *performance* devem ser tidas em conta. Os utilizadores devem poder restringir as suas acções para proteger a sua privacidade.

*Segurança do ciclo de vida*

Os princípios expostos infra permitem ao ciclo de vida do sistema incorporar a segurança para obter um sistema sempre seguro.

- Procedimentos documentados e que podem ser repetidos - Estes procedimentos facilitam o desenvolvimento de componentes idênticas. Estes procedimentos podem incluir: procedimentos de desenvolvimento e revisão de código, procedimentos para a gestão de configurações, procedimentos para entrega do sistema.
- Rigor procedimental - Este princípio define o âmbito, a complexidade e detalhe dos procedimentos do ciclo de vida, procedimentos estes que contribuem para garantir o nível de confiança do sistema. O rigor destes procedimentos deve ser proporcional ao nível de confiança pretendido.
- Modificação segura do sistema - Qualquer alteração ao sistema deve ser feita de forma a garantir a segurança do mesmo, devendo ser conduzida uma análise à alteração antes da sua implementação.
- Documentação suficiente - Deve ser fornecida documentação de apoio a quem interage com o sistema, esta deve ser escrita de forma clara e apoiada por acções de formação.

*Abordagens ao desenvolvimento de sistemas de confiança seguros*

Aqui são apresentadas três estratégias a aplicar no desenvolvimento de sistemas de confiança seguros.

- Conceito de monitor de referência - Esta estratégia providencia um conjunto de requisitos que qualquer mecanismo de controlo de acessos deve cumprir. Com este conceito são evitadas abordagens *ad hoc* ao desenvolvimento de mecanismos de segurança e proporciona também "a garantia que o sistema não é corrompido por pessoas internas"(NIST Special Publication 800-160). Este conceito é caracterizado por três propriedades: não é possível adulterar o mecanismo, o mecanismo é sempre invocado e é possível garantir que o mecanismo funciona correctamente através de análise e testes.
- Defesa em profundidade - Esta estratégia aplica vários mecanismos para criar barreiras que enfraquecem um ataque por parte de um adversário, no entanto, esta estratégia não substitui uma boa arquitectura e *design* de segurança.
- Isolamento - Existem duas formas possíveis de isolamento: lógico e físico. O isolamento lógico utiliza mecanismos para criar ambientes de processamento isolados. O isolamento físico consiste em utilizar *hardware* diferente para cada componente. Os objectivos desta estratégia podem ser uma combinação de isolamento lógico e físico.

### 2.1.5 *Conceitos fundamentais de engenharia e segurança*

Estes conceitos mostram como os princípios supra apresentados são aplicados no ciclo de vida do sistema.

*Necessidades de protecção*

Para definir as necessidades de protecção é feita uma análise à possível perda de recursos e as consequências associadas. Existem três perspectivas dessa análise:

- Perspectiva das partes interessadas - São tidos em conta os recursos considerados de valor pelas partes interessadas.
- Perspectiva do sistema - São tidos em conta os recursos considerados necessários para a execução e protecção do sistema.
- Perspectiva de negociação - "Considera os aspectos de necessidade de protecção de todas as alternativas viáveis, bem como os relacionados com uma decisão específica"(NIST Special Publication 800-160).

Após a análise, as necessidades de protecção são atendidas através da utilização de funções de segurança adequadas. A selecção destas funções é feita de acordo com possíveis adversidades.

As necessidade de protecção são formalizadas na forma de requisitos do sistema e política de segurança. Os requisitos do sistema determinam a capacidade de protecção e a política de segurança determina como essa capacidade é usada. Na figura 3 (baseada em figura do NIST Special Publication 800-160) podemos observar as entradas para a definição das necessidades de protecção e os resultados da especificação dessas necessidades.

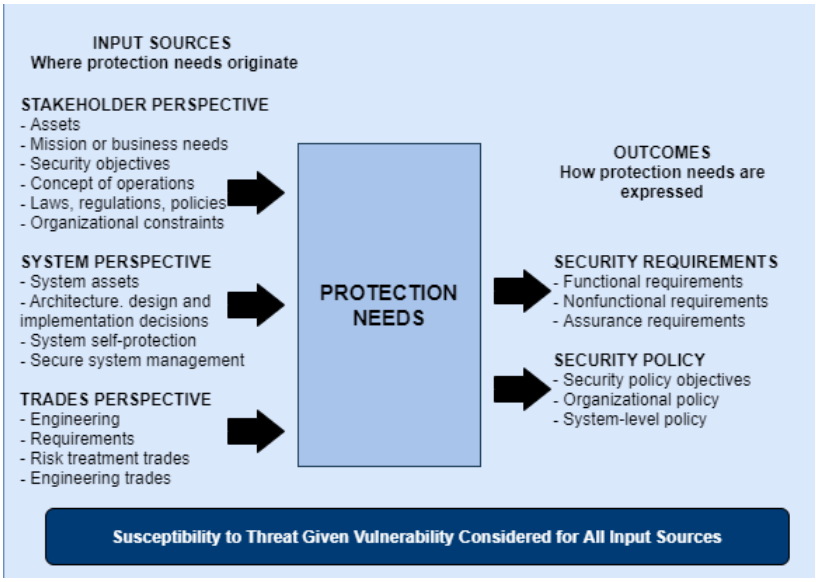



Figura 3: Definição de necessidades de protecção (baseada em figura do NIST Special Publication 800-160)

As necessidades de protecção são revistas continuamente.

*Requisitos de segurança*

O desenvolvimento de requisitos é uma actividade contínua e identifica as necessidades, preocupações, expectativas e restrições de segurança das partes interessadas e transforma-as em requisitos de segurança das partes interessadas. Por sua vez, os requisitos de segurança das partes interessadas são transformados em requisitos do sistema conforme a solução é implementada.

Os requisitos de segurança das partes interessadas definem:

- A necessidade de protecção para a missão ou negócio;
- Os recursos (informação, processos, funções, humanos e sistema);
- Papéis, responsabilidades e acções de segurança;
- Interacções relevantes;
- A garantia a ser obtida com a solução.

Os requisitos de segurança do sistema definem:

- A capacidade de protecção e as características comportamentais e de *performance* da solução;
- Processos, procedimentos e técnicas de garantia;

- Evidências que determinam que o sistema cumpre os requisitos de segurança.

Os requisitos de sistema, onde estão incorporados os requisitos de segurança do sistema, são hierárquicos. A decomposição hierárquica destes requisitos permite transformar uma solução abstracta inicial nos mecanismos e procedimentos a implementar.

Na figura 4 (baseada em figura do NIST Special Publication 800-160) podemos observar os requisitos supra referidos e a sua relação com a verificação e validação do sistema.

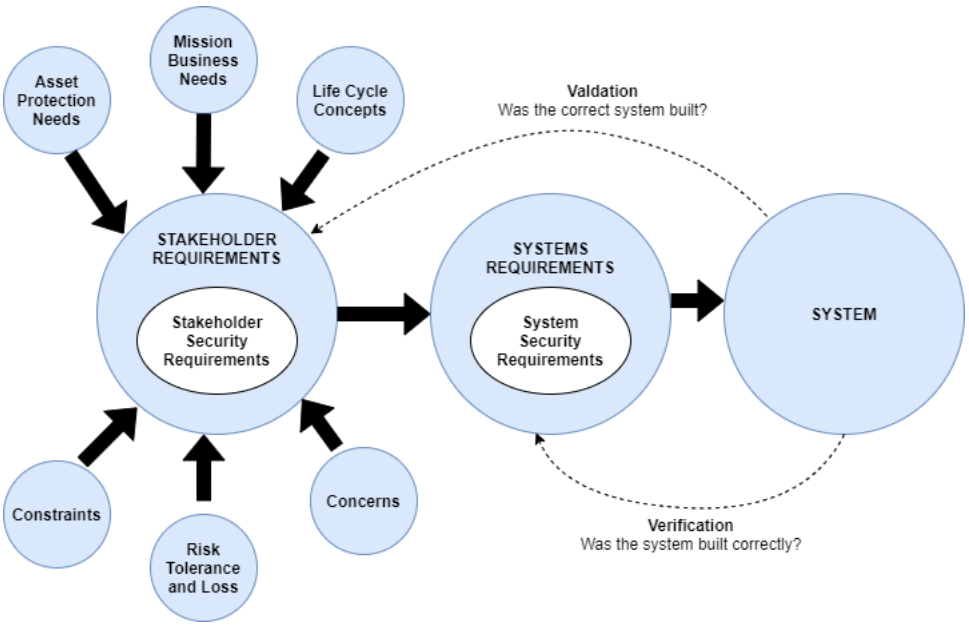



Figura 4: Requisitos das partes interessadas e do sistema (baseada em figura do NIST Special Publication 800-160)

É necessário verificar e validar a solução, isto é, é importante verificar que a solução implementa correctamente os requisitos de *design* e validar que os requisitos das partes interessadas são cumpridos pela solução.

Os requisitos de segurança dividem-se em três tipos:

- Requisitos funcionais de segurança - Determinam a capacidade de protecção do sistema.
- Requisitos não funcionais de segurança - Determinam características qualitativas da segurança do sistema.
- Requisitos de garantia de segurança - Determinam os métodos e as técnicas utilizadas para gerar as evidências necessárias.

Os requisitos são desenvolvidos, principalmente, nos primeiros cinco processos técnicos do ciclo de vida (secção 2.1.2), no entanto, todos os processos técnicos providenciam informação

necessária. Na figura 5 (baseada em figura do NIST Special Publication 800-160) apresenta-se o processo da engenharia de requisitos ao longo dos processo do ciclo de vida.

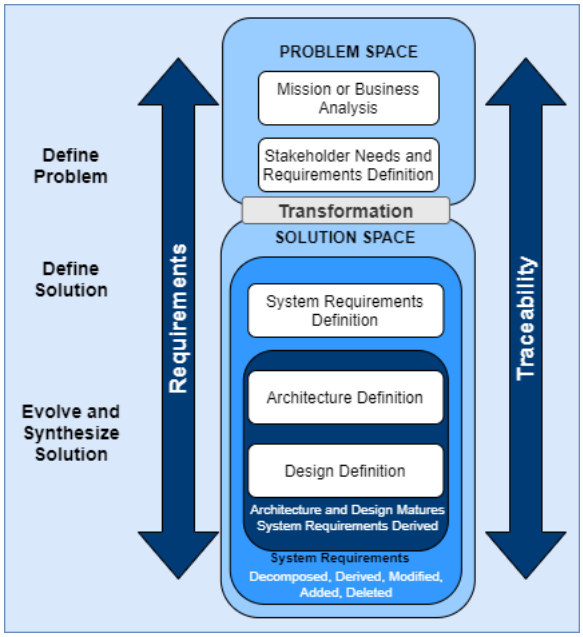



Figura 5: Engenharia de requisitos ao longo dos processos do ciclo de vida (baseada em figura do NIST Special Publication 800-160)

Por fim, a figura 6 (baseada em figura do NIST Special Publication 800-160) mostra os vários factores tidos em conta no processo de análise dos requisitos de segurança.

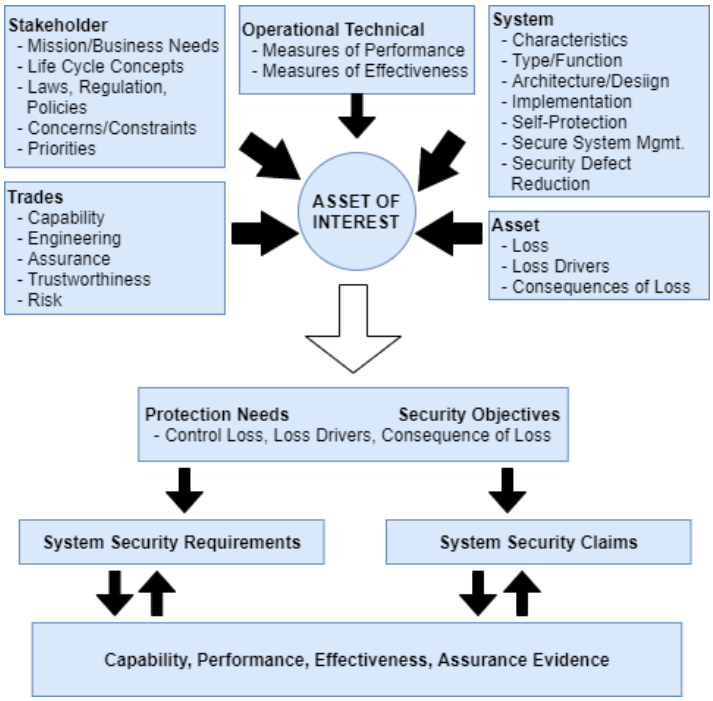



Figura 6: Factores a ter em conta na análise dos requisitos de segurança (baseada em figura do NIST Special Publication 800-160)

*Política de segurança*

A política de segurança define um conjunto de regras que determinam aspectos sobre o comportamento, interacções e resultados dos elementos do sistema que são considerados seguros, NIST Special Publication 800-160.

Existem três objectivos principais da política de segurança:

- Confidencialidade - Regras de acesso, operação e divulgação dos elementos do sistema.
- Integridade - Regras para a modificação, manipulação e destruição dos elementos do sistema.
- Disponibilidade - Regras de acessibilidade, prontidão e continuidade dos serviços dos elementos do sistema.

A política de segurança passa por um processo iterativo que transforma uma declaração abstracta em declarações específicas. Existem três termos associados à política de segurança: objectivos da política de segurança, política de segurança organizacional e política de segurança dos sistema. Estes termos relacionam-se hierarquicamente da seguinte forma: os objectivos da política de segurança incluem a política de segurança organizacional que, por sua vez, inclui a política de segurança do sistema, NIST Special Publication 800-160.

Os objectivos da política de segurança identificam os recursos a proteger e o âmbito da protecção, servindo como base para a política de segurança organizacional e para a política de segurança do sistema.

A política de segurança organizacional define um conjunto de regras que determinam como a organização atinge os objectivos definidos nos objectivos da política de segurança. Nesta política é definido o comportamento a ter na execução de funções relativas à missão e ao negócio e é utilizada para definir processos e procedimentos.

A política de segurança do sistema especifica como o sistema deve cumprir a política de segurança organizacional. A transição da política de segurança organizacional para a política de segurança do sistema envolve actividades de validação e verificação.

Na figura 7 (baseada em figura do NIST Special Publication 800-160) podemos observar um conjunto de estados seguros do sistema e as transições entre eles. A política de segurança ao nível do sistema, divide os estados possíveis do sistema em estados seguros e inseguros. Um sistema é considerado seguro quando não é possível transitar para um estado inseguro, no entanto, na prática, é muito difícil garantir que o sistema transita apenas para estados seguros. Para tornar o processo mais fácil, as políticas de segurança incluem estados que reflectem o conceito de falha sem perda de estado seguro (i.e. capacidade de detectar falhas) e recuperação de confiança (i.e. capacidade de executar acções para transitar o sistema de um estado inseguro para um seguro).

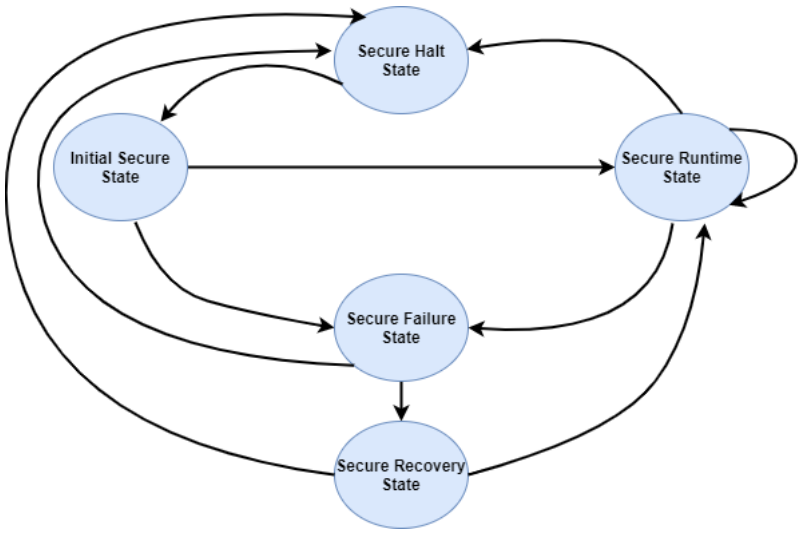



Figura 7: Transições de estados seguras (baseada em figura do NIST Special Publication 800-160)

*Distinguir requisitos, políticas e mecanismos*

- Requisito - condição ou capacidade que o sistema ou elemento deve ter para satisfazer contratos, normas, especificações ou outros, NIST Special Publication 800-160.

- Política de segurança - conjunto de afirmações sobre o que é ou não permitido, NIST Special Publication 800-160.
- Mecanismo de segurança - entidade ou procedimento que aplica a política de segurança, NIST Special Publication 800-160.

Estes termos têm um relação de dependência entre si: os requisitos de segurança do sistema definem a capacidade e comportamento que um mecanismo proporciona e, por sua vez, a política de segurança define os aspectos da política que o mecanismo deve aplicar. Na figura 8 (baseada em figura do NIST Special Publication 800-160) podemos observar esta relação.

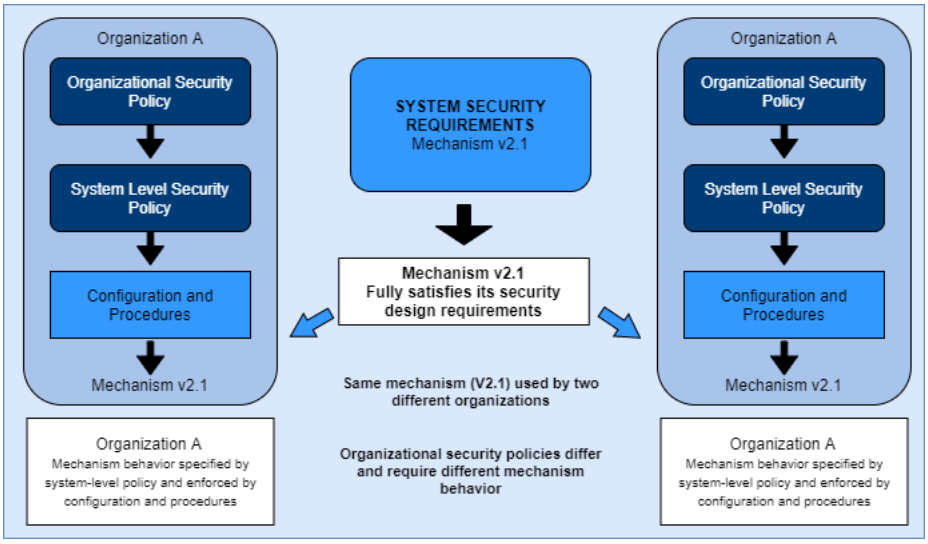



Figura 8: Relação entre mecanismos e aplicação da política de segurança (baseada em figura do NIST Special Publication 800-160)

*Arquitectura da segurança do sistema*

"A arquitectura da segurança do sistema são os conceitos ou propriedades de segurança fundamentais do sistema no seu ambiente e estão incorporados nos seus elementos, relações e nos princípios do seu *design* e evolução"(NIST Special Publication 800-160).

Para obter um sistema de confiança seguro, a arquitectura de segurança do sistema incorpora as funções e restrições de segurança nas funções do sistema e utiliza princípios de *design* descritos na secção 2.1.4.

*Relevância da segurança*

A relevância da segurança é um atributo de outras entidades de engenharia (e.g. arquitectura, requisitos, funções, *design*, entre outros).

Existem três *design*ações utilizadas para caracterizar e analisar este atributo:

- Funções que aplicam segurança - São directamente responsáveis pela segurança.
- Funções que suportam a segurança - Contribuem para que as funções que aplicam segurança funcionem correctamente.
- Funções que não interferem na segurança - Por desing não conseguem interferir com funções que aplicam a segurança ou que suportam a segurança.

Esta divisão tem como objectivo garantir que a análise da segurança do sistema determina o potencial de interferência em relação à capacidade de protecção do sistema.

*Criticidade de protecção da função de segurança*

Este princípio pretende determinar até que ponto as funções de segurança impactam a capacidade de protecção do sistema relativamente a consequências de falha. A análise da criticidade de protecção foca-se nas consequências de falhas.

*Fiabilidade e garantia*

É através da fiabilidade e garantia que é possível provar um sistema como "adequadamente seguro".

- Fiabilidade

  A fiabilidade da segurança é conseguida devido às actividades serem feitas com base num conjunto de princípios de *design* de segurança, que, por sua vez, são baseados em requisitos de segurança verificáveis. A fiabilidade do sistema é avaliada em cada elemento individual e também na composição dos vários elementos. A fiabilidade do sistema também inclui o reconhecimento de estados inseguros e como transitar de estados inseguros para estados seguros, pelo que, a fiabilidade do sistema também é baseada na antecipação de falhas e as perdas que delas podem resultar.

- Garantia

  A garantia é a medida de confiança dada à combinação das funções de segurança para prevenir perda de recursos e as consequências associadas. A base para a garantia da segurança do sistema são afirmações acerca da segurança, que reflectem os atributos de um sistema de confiança seguro. O nível de garantia depende de três factores: âmbito (quanto maior o âmbito maior a garantia), profundidade (quanto mais minuciosa for a análise maior a garantia) e rigor (quanto mais rigorosos os métodos, processos e ferramentas, maior a garantia). As actividades de verificação e validação focadas em providenciar garantias de segurança, são incorporadas nos processos técnicos e os seus resultados combinados constroem a garantia nas funções de segurança.

*Eficácia, performance e custo da segurança do sistema*

É importante ser feita uma avaliação do custo-benefício das funções de segurança, e deve ser escolhido o caso que encontra o melhor balanço entre custo-benefício, que pode ser um conjunto de funções menos custosas em vez de uma mais custosa ou, até, que uma função de segurança não possa ser utilizada porque impacta negativamente a *performance* de tal forma que é mais benéfico não a utilizar.

O custo da segurança do sistema deve ter em consideração os objectivos de fiabilidade e o custo de outras actividades necessárias.

## 2.2 GESTÃO DA SEGURANÇA DE INFORMAÇÃO

Sendo a informação um recurso vital de uma organização, a sua segurança é essencial para garantir a sua confidencialidade, integridade e disponibilidade.

### 2.2.1 *Sistema de Gestão de Segurança de Informação*

Um sistema de gestão de segurança de informação, segundo o ISO/IEC 27000:2018 (en), "consiste em políticas, procedimentos, directrizes, e os recursos e actividades associadas, geridos colectivamente pela organização, com o objectivo de proteger os seus recursos de informação"(ISO/IEC 27000:2018 (en)).

Para a implementação eficaz de um sistema de gestão de segurança de informação, o ISO/IEC 27000:2018 (en) define um conjunto de princípios que incluem:

- "Consciencializar para a necessidade da segurança da informação";
- "Definir responsabilidades de segurança de informação";
- "Incorporar o compromisso de gestão nos interesses das partes interessadas";
- "Realçar valores sociais";
- "Incorporar a segurança como um elemento essencial dos sistemas e redes de informação";
- "Activar a prevenção e detecção de incidentes de segurança da informação";
- "Garantir uma abordagem extensiva da gestão de segurança da informação";
- "Reavaliar continuamente a segurança da informação e proceder a alterações de forma apropriada".

Um sistema de gestão de segurança da informação é importante para proteger os recursos de informação e a sua aplicação permite:

- Garantir que os recursos são protegidos adequadamente e continuamente;
- Assegurar uma estrutura para identificar e avaliar riscos, seleccionar, avaliar e melhorar controlos;
- Cumprir requisitos legais e regulamentares.

Para estabelecer, manter, monitorizar e melhorar o sistema de gestão de segurança de informação, a organização deve:

- Identificar os recursos de informação e os requisitos de segurança associados;
- Avaliar e tratar riscos;
- Seleccionar, implementar, manter, monitorizar e melhorar controlos;

A família de *standards* de sistemas de gestão de segurança de informação auxilia as organizações a criar esse sistema de forma estruturada, permite que este cumpra as necessidades da organização e promove uma base para que as partes interessadas confiem na segurança da informação da organização.

Nesta dissertação focar-me-ei nos ISO/IEC 27000:2018 (en), ISO/IEC 27001:2013 (E) e ISO/IEC 27002:2013 (E).

*Requisitos*

O *standard* ISO/IEC 27001:2013 (E) define requisitos "para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança de informação"(ISO/IEC 27001:2013 (E)), nas seguintes áreas:

- Contexto da organização

  É determinado o âmbito do sistema de gestão de segurança de informação, tendo em conta todas as questões relevantes internas e externas, qualquer requisito de partes interessadas e relações e dependências entre actividades.

- Liderança

  A administração da organização estabelece uma política de segurança da informação apropriada e garante o correcto funcionamento do sistema de gestão de segurança da informação, inclusive, promovendo a sua melhoria continua. Para além disso, garante que são atribuídas responsabilidades e autoridades no que toca à segurança da informação.

- Planeamento

  A organização, de acordo com o seu contexto, idealiza a forma de responder aos riscos e às oportunidades e como integrar e implementar essa resposta nos processos do sistema de gestão de segurança de informação. Para isso, é importante que a organização defina e aplique um processo de avaliação de riscos que inclui estabelecer os critérios de risco, identificar riscos e donos de risco, analisar e avaliar riscos. É também importante definir as medidas de tratamento dos riscos que devem resultar num plano de tratamento de risco adequado.

- Suporte

  A organização assegura que os recursos e competências necessários ao sistema de gestão de segurança da informação são disponibilizados, que os recursos humanos estão cientes da política de segurança de informação, que as necessidades de comunicação (interna e externa) são determinadas e que a informação documentada é elaborada, revista, acessível e protegida adequadamente.

- Operação

  A organização implementa processos e planos para cumprir os requisitos e objectivos de segurança da informação e documenta a informação necessária para garantir que esses processos são cumpridos. A avaliação de riscos é feita periodicamente e os seus resultados são documentados. Além disso, o plano de tratamento de riscos é implementado e os seus resultados também são documentados.

- Avaliação de *performance*

  A organização avalia a *performance* e eficácia da segurança da informação de acordo com critérios estabelecidos pela mesma e analisa os resultados dessa avaliação. Para tal, a organização efectua auditorias internas de acordo com programas estabelecidos. A administração da organização tem a responsabilidade de rever o sistema de gestão de segurança de informação para assegurar a sua pertinência e eficácia.

- Melhoria

  De acordo com os resultados da avaliação feita, a organização toma medidas de correcção apropriadas e eficazes. A melhoria do sistema de gestão de segurança da informação deve ser uma actividade continua para tornar o sistema mais adequado e eficaz.

Na versão anterior deste *standard* ( ISO/IEC 27001:2005 (E)) era recomendado o uso do método PDCA (*Plan-do-check-act*) aplicado aos processos da gestão de segurança da informação. Na figura 9 observa-se como o método é aplicado. Na versão actual do *standard*

ISO/IEC 27001:2013 (E) não é definido nenhum método em específico, no entanto o método PDCA ainda é amplamente utilizado.

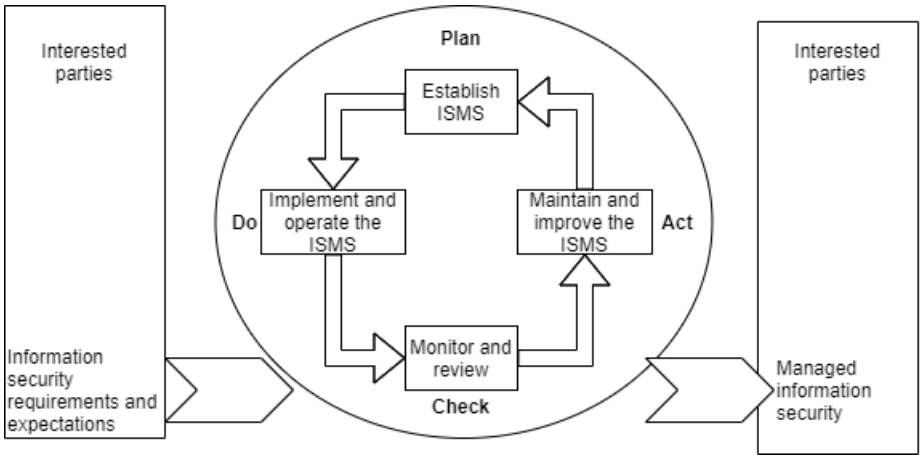



Figura 9: Método PDCA aplicado aos processos da gestão de segurança da informação (baseada em figura do ISO/IEC 27001:2005 (E))

*Controlos*

O *standard* ISO/IEC 27002:2013 (E) define orientações para as organizações seleccionarem, implementarem e gerirem controlos para a segurança da informação.

- Políticas de segurança da informação

  A organização deve definir, aprovar, publicar e comunicar uma política de segurança da informação que responda aos requisitos da organização, que contenha os objectivos, princípios e as responsabilidades de papéis específicos na segurança da informação. As políticas devem ser revistas regularmente e devem ter um *owner* responsável pelo seu desenvolvimento e revisão. A administração da organização deve demonstrar o seu compromisso explícito para com a política de segurança de informação.A gestão de incidentes deve ser integrada nas políticas de segurança de informação.

- Organização da segurança da informação

  Devem ser definidas e atribuídas responsabilidades pela protecção de recursos, pela execução de processos e pelas actividades de gestão do risco. Deve ainda ser tida em conta a segregação de papéis quando são atribuídas essas responsabilidades para reduzir a probabilidade de usos e alterações não autorizadas. A segurança da informação deve ser sempre parte integrante da gestão de um projecto. Devem também ser definidas medidas para proteger dos riscos associados ao uso de dispositivos móveis e ao tele-trabalho.

- Segurança de recursos humanos

Antes da contratação, devem ser verificados os antecedentes dos candidatos e os contratos devem ter expressas as responsabilidades, quer da organização quer do candidato, para a segurança da informação. A administração tem o papel de garantir que as políticas e procedimentos da segurança da informação são cumpridos por todos os recursos humanos e deve-lhes ser disponibilizado todo o conhecimento e acções de formação necessárias para cumprirem as suas funções, as acções de formação devem ser periódicas e devem ser criados processos disciplinares para recursos humanos que criem falhas na segurança da informação. Aquando da cessação de funções dos recursos humanos devem ser definidas e comunicadas as responsabilidades que continuarão a ter (e.g. contrato de confidencialidade).

- Gestão de recursos

  Deve ser efectuado o inventário de todos os recursos associados à informação e deve ser documentada a sua importância, esses recursos devem ter um responsável (indivíduo ou entidade) que garante que os mesmos são inventariados, protegidos e classificados adequadamente. Devem ser definidas, documentadas e implementadas regras para o uso dos recursos e para a devolução de recursos aquando da cessação de funções quer de funcionários quer de entidades externas. A informação deve ser classificada de acordo com os requisitos legais, valor, criticidade, entre outros, pelo responsável do recurso de informação e pode ser feita em termos de confidencialidade, integridade e disponibilidade. De acordo com a mesma, devem ser implementados procedimentos para o manuseamento, processamento e arquivo de informação, devendo, também, ser implementados procedimentos para a remoção, destruição e transporte de equipamentos media.

- Requisitos de negócio para controlo de acessos

  Devem ser estabelecidas políticas de controlo de acessos (incluindo acesso a redes e serviços de rede, acesso a informação e funções do sistema). As regras são determinadas pelos responsáveis pelos recursos de acordo com os riscos associados. Para permitir a atribuição de direitos de acesso devem existir procedimentos para a gestão de identificação de utilizadores, incluindo a remoção ou anulação de identificações de utilizadores que cessem funções, devem também existir procedimentos para atribuir ou retirar direitos de acesso aos utilizadores e direitos de acesso privilegiados devem ser restritos e controlados, incluindo o uso de programas que possam reescrever os controlos do sistema e de aplicações e acesso ao código fonte de programas. Os direitos de acesso devem ser revistos regularmente e ajustados adequadamente. Todos os utilizadores devem manter a confidencialidade da informação de autenticação secreta de acordo com a práticas da organização e os sistemas de gestão de *passwords* devem

ser interactivos e garantir a qualidade das mesmas. Quando adequado, devem existir procedimentos de registo de acessos.

- Criptografia

  Os controlos criptográficos têm como objectivo garantir a confidencialidade, integridade e autenticidade da informação. Devem ser definas e implementadas políticas para o uso desses controlos e para a gestão de chaves criptográficas. Estas políticas devem incluir os algoritmos usados e tamanho de chaves (tendo em conta a legislação e regulamentação aplicável), papéis e responsabilidades relacionados com os controlos criptográficos (e.g. implementação da política, geração de chaves), distribuição, arquivo e *backups* de chaves criptográficas, entre outros.

- Segurança física e de ambientes

  Devem ser definidos perímetros de segurança física que protejam áreas consideradas críticas para a segurança da informação e as áreas de segurança devem recorrer a controlos de acesso. Todas as entradas nestas áreas são registadas e devem existir procedimentos para realizar trabalho nas mesmas. A organização deve aplicar protecção física contra desastres naturais e ameaças externas. É importante que as áreas de carga e descarga sejam pensadas de forma a não permitir acessos não autorizados às instalações e, preferencialmente, isoladas de instalações de processamento. A segurança física deve ser aplicada aos equipamentos, inclusive equipamentos de suporte (e.g. electricidade, comunicações, água, ventilação), que devem estar protegidos contra condições naturais (e.g. temperatura, humidade), desastres naturais, acessos não autorizados. Devem ser tomadas medidas para manter a continuidade e integridade dos equipamentos. A saída de recursos das instalações deve ser sempre autorizada, monitorizada e com medidas que garantam a sua segurança de acordo com o risco associado. No caso de cessação ou reutilização de equipamentos deve-se garantir que qualquer informação sensível foi eliminada. No caso de equipamentos que contenham informação confidencial, estes devem ser destruídos fisicamente ou a informação destruída de forma a não ser possível a sua recuperação.

- Segurança das operações

  Devem existir procedimentos documentados que especifiquem as instruções operacionais (e.g. instalação e configuração de sistemas, processamento e manuseamento de informação, tratamento de erros). Todas as alterações significativas devem ser registadas, planeadas, analisadas e devem passar por um procedimento de aprovação formal para serem implementadas. Os ambientes de desenvolvimento,teste e operação devem estar separados. A organização deve proteger-se contra *malware* focando-se na prevenção, detecção, reparação e consciencialização dos utilizadores, sendo, por isso,

importante que a organização defina e implemente procedimentos para a instalação de *software* que controle, de forma eficaz, a segurança do sistema, incluindo uma estratégia de *roll-back*. É importante existir uma política de *backups* (onde são definidos os requisitos de *backup*) e um plano de *backup* que deve ser testado com regularidade. Os próprios *backups* devem ser arquivados num local remoto. Devem ser mantidos registos dos acontecimentos relevantes (e.g. falhas, eventos de segurança, acessos ao sistema, alterações ao sistema), que devem ser protegidos contra acessos ou alterações não autorizadas. As vulnerabilidades devem ser detectadas e tratadas eficazmente, sendo, para isso, necessário definir o processo e as responsabilidades para gerir as vulnerabilidades.

- Segurança de comunicações

  As redes que suportam as instalações de processamento de dados devem ser protegidas contra acessos não autorizados sendo necessário, para o efeito, definir procedimentos e responsabilidades para a sua gestão, garantir a confidencialidade e integridade dos dados que passam nas redes e a disponibilidade dos serviços de rede. A transferência de informação deve seguir procedimentos e políticas que a protejam e que definam o uso aceitável dos meios de comunicação. Devem ser feitos acordos de confidencialidade com os funcionários e partes externas que garantam a confidencialidade da informação.

- Aquisição, desenvolvimento e manutenção de sistemas

  Os requisitos de sistemas de informação devem incluir os requisitos de segurança e a sua identificação deve ser introduzida nos estados iniciais dos projectos. Estes devem ser tidos em conta aquando da aquisição de produtos, devem ser definidos critérios para a aceitação de produtos e sistemas, inclusive nos contratos com fornecedores, e a avaliação/teste dos mesmos é feita de acordo com esses critérios. O desenvolvimento de *software* e sistemas deve seguir uma política de desenvolvimento seguro e as melhores práticas no que toca a técnicas de programação seguras. Para isso, é importante garantir que os *developers* recebem o treino apropriado e que existem ambientes de desenvolvimento seguros (pessoas, processos e tecnologia associada ao desenvolvimento). Quaisquer alterações devem ser controladas, mesmo durante o ciclo de vida do desenvolvimento, para garantir que são avaliadas, testadas e aprovadas. No caso de *software* externo, são desencorajadas alterações e caso haja a necessidade de o fazer devem ser analisados os riscos associados.

- Relações com fornecedores

  Os acordos com fornecedores devem ter em conta os requisitos de segurança de informação. A organização deve identificar os controlos a aplicar, tanto por esta como pelo fornecedor. Deve ainda verificar, monitorizar e rever com regularidade se os termos e condições dos acordos são cumpridos.

- Gestão de incidentes de segurança da informação

  Para uma eficaz gestão de incidentes é importante que a organização defina e implemente procedimentos para a detecção, análise e resposta a eventos de segurança, assim como manuseamento de evidências. Todos os funcionários e fornecedores da organização têm a responsabilidade de comunicar fraquezas e eventos de segurança (e.g. controlos ineficazes, falha humana, quebra de confidencialidade, integridade ou disponibilidade, não conformidades com as políticas, violação de acessos), o processo de comunicação deve ser fácil e acessível. Os eventos de segurança devem ser analisados e classificados como incidentes ou não, esta análise deve ser registada. A reposta aos incidentes deve seguir procedimentos documentados e deve incluir, entre outros, a recolha de evidências, escalonamento de incidentes e registo de todas as actividades. Posteriormente à resposta ao incidente, é importante existir um processo de lições aprendidas onde é utilizado o conhecimento retirado da análise e resposta, para evitar e diminuir o impacto de incidentes futuros. A recolha de evidências deve seguir um procedimento formal que garanta a sua identificação, recolha e preservação para, quando necessário, servirem de prova em acções legais ou disciplinares. Infra abordar-se-á, de novo, este assunto, aprofundando-o.

- Aspectos de segurança de informação de gestão de continuidade de negócio

  A gestão de continuidade de negócio da organização deve ter em atenção a continuidade da segurança de informação. A organização deve estabelecer e implementar os controlos de segurança nos processos, procedimentos, sistemas e ferramentas da continuidade de negócio e, quando não é possível a sua manutenção, deve implementar controlos compensatórios. Estes controlos de segurança devem ser revistos com regularidade. Deve ser considerada a necessidade de instalações secundárias de processamento de informação para garantir a disponibilidade dos sistemas em situações adversas. Estes devem ser testados para garantir que cumprem as suas funções.

- Conformidade

  Os requisitos legais, regulamentares e contratuais da organização e a forma como estes são cumpridos, devem ser identificados e documentados. Estes requisitos incluem a protecção de registos, direitos de propriedade intelectual, privacidade e protecção de informação pessoal e controlos criptográficos. Uma revisão independente da gestão da segurança da informação deve ser feita regularmente ou sempre que haja uma alteração significativa e deve confirmar se os procedimentos e sistemas estão de acordo com as políticas e *standards*, devendo ainda identificar oportunidades de melhoria e não conformidades. No caso de revisão de conformidade técnica, esta deve ser feita

preferencialmente através de ferramentas automáticas que geram relatórios técnicos para análise.

### 2.2.2 *Gestão de Risco*

O *standard* ISO 31000:2018 (E) define um conjunto de orientações para a gestão de risco. Neste *standard* a gestão de risco é definida como um processo iterativo que faz parte de todas as actividades da organização. Na figura 10 observam-se os princípios, *framework* e processos para a gestão de risco definidos no ISO 31000:2018 (E).

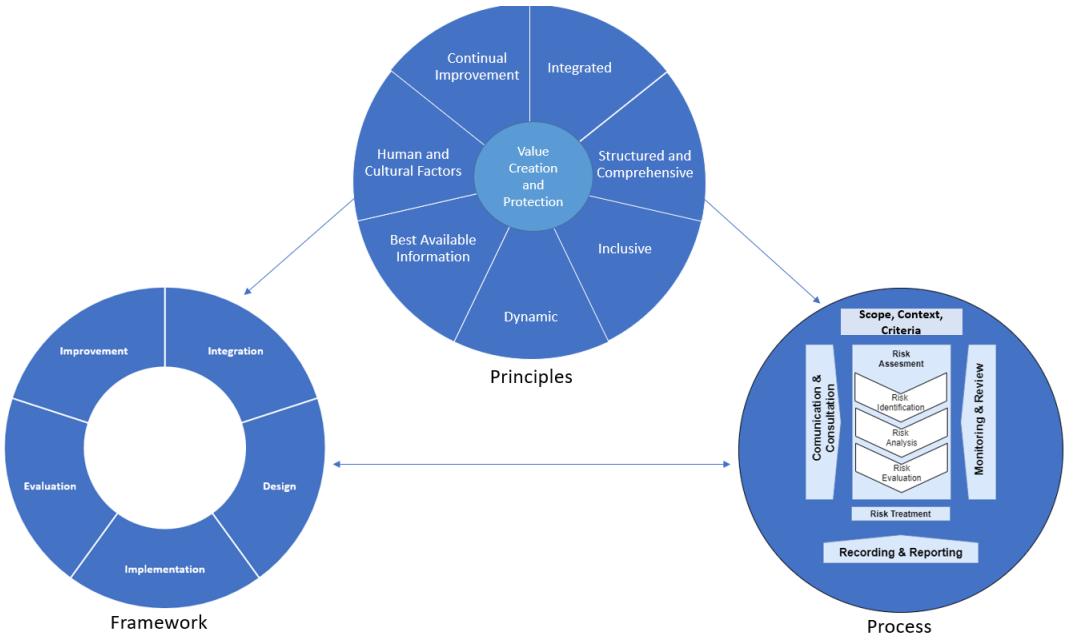



Figura 10: Princípios, *framework*, processo (baseada em figura do ISO 31000:2018 (E))

- Princípios

  Os princípios seguintes definem a base para a gestão de risco, segundo o ISO 31000:2018 (E):

  - A gestão de risco deve ser integrada em todas as actividades da organização;
  - A gestão de risco deve ser abordada de forma compreensiva e estruturada;
  - Os processos e *framework* da gestão de risco são adaptados a cada organização;
  - As partes interessadas são envolvidas na gestão de risco;
  - A gestão de risco é dinâmica e por isso responde a alterações de forma eficaz;
  - A gestão de risco baseia-se na informação actual, passada e expectativas futuras;
  - A gestão de risco é influenciada por factores humanos e culturais;

  - Melhoria contínua da gestão de risco;

- *Framework*

  É da responsabilidade da administração e órgãos de supervisão garantir a integração da gestão de risco em todas as actividades da organização. A administração é responsável por implementar e adaptar todas as componentes da *framework* e definir a abordagem à gestão de risco. Os órgãos de supervisão são responsáveis por supervisionar a gestão de risco e garantir que a mesma cumpre os objectivos. As componentes da *framework* da gestão de risco são:

  - Integração

    Para uma integração eficaz é importante compreender o contexto e estrutura da organização pois o risco é gerido em todas os níveis dessa estrutura. A gestão de risco deve fazer parte dos objectivos, propósitos e estratégia da organização e todas as pessoas da organização têm responsabilidade na gestão de risco.

  - *design*

    Para o *design* da *framework* é importante compreender quer o contexto interno quer o contexto externo da organização. A administração deve identificar os papéis, autoridades e responsabilidades relevantes à gestão de risco (inclusive *risk owners*) e alocar os recursos necessários à gestão de risco (e.g. pessoas, processos, procedimentos, conhecimento). A abordagem à comunicação deve garantir que a informação é registada e partilhada de forma eficaz.

  - Implementação

    A implementação da *framework* implica o desenvolvimento de um plano que envolve prazos e recursos, a definição de um processo de tomada de decisões e a garantia que a abordagem à gestão de risco é compreendida e praticada.

  - Avaliação

    A *performance* da *framework* deve ser monitorizada e deve ser verificado se esta cumpre os objectivos da organização.

  - Melhoria

    A melhoria contínua da *framework* deve contribuir para o aperfeiçoamento da gestão de risco através da identificação e implementação de oportunidades de melhoria.

- Processo

  O processo de gestão do risco, é um processo iterativo, deve ser integrado em toda a estrutura, operações e processos da organização e envolve a aplicação sistemática de políticas, procedimentos e práticas.

– Comunicação e aconselhamento

  A comunicação e aconselhamento deve acontecer ao longo de todo o processo de gestão de risco e tem como objectivo troca de informação que auxilie a tomada de decisões.

– Âmbito, contexto e critério

  A abordagem à gestão de risco deve ser adaptada a cada organização e, para isso, é importante definir o âmbito das actividades de gestão de risco, o contexto interno e externo da organização e a quantidade e tipo de risco que pode ou não ser aceite, de acordo com os objectivos da organização. O critério de risco deve ter em conta a capacidade da organização e como o nível de risco, consequências e probabilidade são definidos e medidos.

– Avaliação de risco

  Neste processo são identificados, analisados e avaliados os riscos da organização. A identificação de riscos deve ter em atenção os seguintes factores: fontes de risco, eventos, causas, ameaças, vulnerabilidades, alterações no contexto, natureza e valor de recursos, consequências e impacto. A análise de riscos deve basear-se nas fontes de risco, consequências, probabilidade, eventos, cenários e controlos. A avaliação de riscos compara os resultados da análise de risco com os critérios de risco, para tomar a decisão do que deve ser feito de seguida (aceitar o risco, analisar de novo, reconsiderar objectivos, tratar o risco).

– Tratamento de riscos

  Este processo é iterativo e envolve seleccionar, planear, implementar e avaliar a eficácia das medidas de tratamento, decidir se o risco residual é aceitável e, caso não seja, aplicar novas medidas. A selecção das medidas de tratamento deve ter em conta a relação custo-benefício. Algumas opções para tratamento de risco são:

  * Evitar o risco eliminando a actividade que o levanta;
  * Aceitar ou aumentar o risco para aproveitar uma oportunidade;
  * Remover a fonte do risco;
  * Alterar a probabilidade do risco;
  * Alterar as consequências;
  * Partilhar o risco; e
  * Reter o risco.

  A implementação da medida escolhida deve ser monitorizada e revista. Os planos de tratamento de risco definem como implementar as medidas de tratamento. Estes devem explicar a razão para as medidas escolhidas, identificar os responsáveis

pela implementação do plano, as acções a desenvolver, os recursos necessários, as métricas de *performance* e as expectativas de prazos para completar o plano.

– Revisão e monitorização

A monitorização contínua e a revisão periódica ao longo de todo o processo de gestão de risco garantem a melhoria do processo. Aquelas devem ser parte integrante do processo e ter responsabilidades definidas para a sua concretização.

– Registos e relatórios

O processo de gestão de risco e os seus resultados devem ser registados e comunicados.

### 2.2.3 *Gestão de incidentes*

Uma parte importante da segurança de informação é a gestão de incidentes. Assim, é importante que a organização tenha um plano de como detectar, comunicar, analisar e responder a incidentes e também aprender com os mesmos. O ISO/IEC 27035-1:2020 (E), ISO/IEC 27035-2:2020 (E) e ISO/IEC 27035-3:2020 (E) definem uma abordagem estruturada que pode ser seguida pelas organizações para a gestão de incidentes.

Na figura 11 observa-se a relação entre ameaças, vulnerabilidades, eventos, incidentes, recursos e operações. É importante notar que nem todos os eventos de segurança são considerados incidentes, devendo ser definidos critérios para classificar eventos como incidentes.

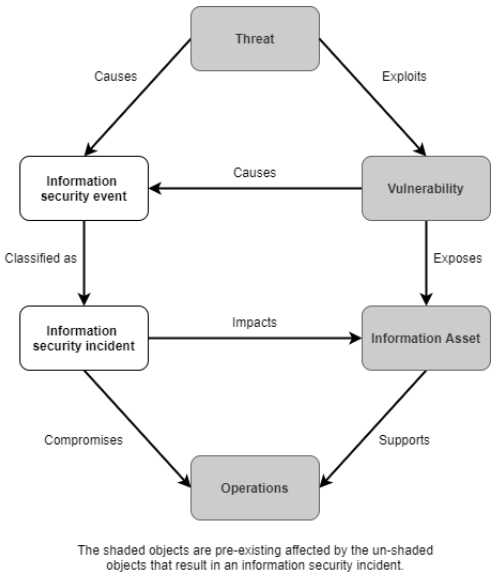



Figura 11: Relação entre ameaças, vulnerabilidades, eventos, incidentes, recursos e operações (baseada em figura do ISO/IEC 27035-1:2020 (E))

A gestão de incidentes deve fazer parte da estratégia para a segurança da informação sendo o seu principal objectivo evitar incidentes e minimizar o seu impacto nas operações da organização. Na figura 12, observa-se a relação entre a gestão de incidentes e o sistema de gestão de segurança de informação definido no ISO/IEC 27001:2013 (E).

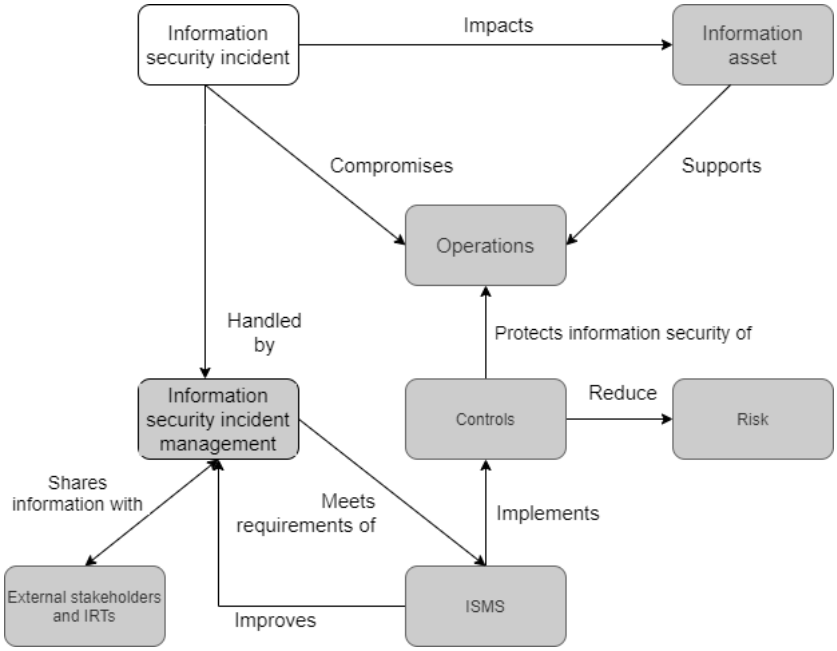



Figura 12: Relação entre a gestão de incidentes e o sistema de gestão de segurança da informação (baseada em figura do ISO/IEC 27035-1:2020 (E))

A gestão de incidentes definida no ISO/IEC 27035-1:2020 (E) divide-se em 5 fases distintas:

- Planear e preparar
- Detecção e comunicação
- Avaliação e decisão
- Respostas
- Lições aprendidas

Na figura 13 observa-se o fluxo da gestão de incidentes.

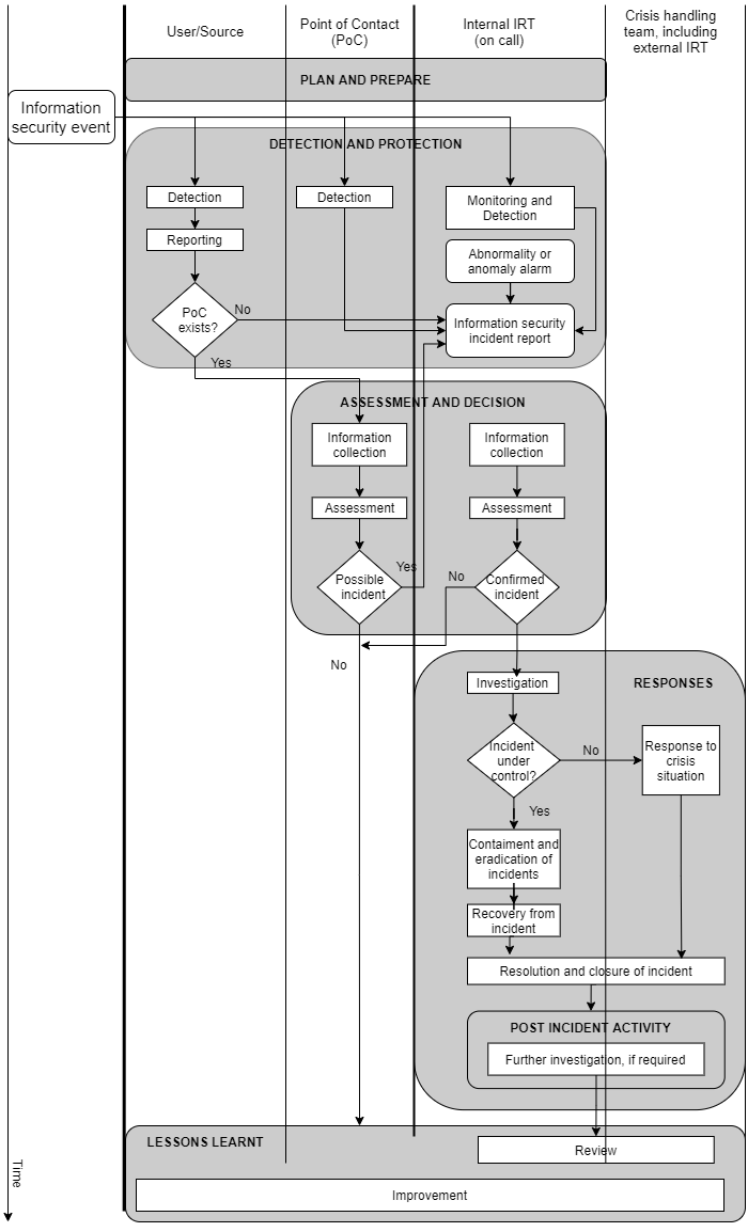



Figura 13: Diagrama de fluxo de eventos e incidentes (baseada em figura do ISO/IEC 27035-1:2020 (E))

*Planear e preparar*

As actividades desenvolvidas ao longo desta fase, descritas nos documentos ISO/IEC 27035-1:2020 (E) e ISO/IEC 27035-2:2020 (E) incluem:

- Definir e implementar uma política de gestão de incidentes;
- Definir um plano para a gestão de incidentes;

- Criar uma equipa de resposta a incidentes;
- Acções de formação e consciencialização acerca da gestão de incidentes;
- Adquirir, preparar e testar os recursos de suporte.

- Política de gestão de incidentes

  Este é um documento de alto nível onde é definido, entre outros, o que constitui um incidente, os tipos e categorias de incidentes, como são comunicados os incidentes, os papéis, responsabilidades e autoridade para cada fase do processo de gestão de incidentes.

- Plano de gestão de incidentes

  Este plano é baseado na política de gestão de incidentes e é composto por vários documentos que servem para guiar a detecção, comunicação, avaliação e resposta a incidentes. Devem existir documentos que detalhem as actividades desenvolvidas ao longo de todas as fases da gestão de incidentes. Devem ser definidos formulários para a comunicação de incidentes, procedimentos que identificam os passos a seguir e por quem são executados, incluindo procedimentos operacionais (e.g. desligar um sistema afectado, activar os procedimentos de continuidade de negócio, entre outros). Este plano deve ser testado com regularidade. O ISO/IEC 27035-2:2020 (E) refere 3 formas de exercícios: baseado em discussão, *tabletop* e *live*. O tipo de exercício a utilizar ou até uma combinação de tipos é definido de acordo com o objectivo do teste, tempo e recursos disponíveis. Todos os exercícios passam por 3 fases: o planeamento e preparação, execução e, por fim, *debriefing* e análise *post-mortem*.

- Equipa de reposta a incidentes

  Esta equipa ocupa-se das actividades de resposta, avaliação e lições aprendidas da gestão de incidentes. Esta equipa carece de uma política de resposta e de um processo de resposta. Tem o papel, não só de responder a incidentes, mas também de contribuir para a prevenção de incidentes. Deve, em conjunto com outras equipas da organização, monitorizar e responder a incidentes, gerir os registos de incidentes, gerir a segurança da organização, gerir a capacidade e *performance* dos sistemas. Os elementos desta equipa devem ter habilitações técnicas na área de segurança (e.g. análise de risco, modelação de ameaças, análise de vulnerabilidades).

*Detecção e comunicação*

É nesta fase que ocorre a detecção, a recolha de informação e a comunicação de eventos e vulnerabilidades.

A detecção de incidentes pode ser feita quer por pessoas quer por tecnologias de segurança de informação.

A organização começa por monitorizar os eventos de segurança para detectar incidentes. A partir do momento em que o incidente de segurança da informação é registado, a equipa de monitorização verifica se se trata efectivamente de um incidente e, no caso de se verificar que é um incidente, faz uma avaliação inicial onde determina a sua gravidade, o tipo, a importância do sistema afectado e o nível de alarme.

As actividades de monitorização, segundo o ISO/IEC 27035-3:2020 (E), incluem:

- Monitorização contínua de eventos de segurança;
- Monitorização através da consola;
- Monitorização de informação pública; e
- Reforço ou alteração das regras do sistema de monitorização enquanto está a decorrer uma intrusão.

As actividades de detecção, segundo o ISO/IEC 27035-3:2020 (E), incluem a identificação de incidentes recolhendo, analisando e qualificando eventos de segurança e fazendo uma correlação de incidentes e triagem de eventos adequada.

Existem dois métodos comuns para a detecção: detecção pro-activa e detecção reactiva. A detecção pro-activa envolve uma procura activa de incidentes. Alguns métodos de detecção pro-activa incluem:

- *Scanning* de vulnerabilidades;
- Testes de intrusão;
- Monitorização de rede;
- Detecção utilizando sistemas de *software*;
- Entre outros.

A detecção reactiva envolve a produção de um aviso de um possível incidente, alguns métodos de detecção reactiva incluem:

- Relatórios e alertas de utilizadores;
- Alertas accionados por sistemas de *software*;
- Reclamações e sugestões de utilizadores;
- Entre outros.

Nesta fase é importante a recolha de informação tanto de fontes internas como de fontes externas, incluindo evidências digitais e registos de todas as actividades, dos resultados e decisões tomadas ao longo desta fase.

A notificação de eventos de segurança pode ser feita por utilizadores ao ponto de contacto, que, por sua vez, se considerar tratar-se de um incidente, contacta a equipa de resposta a incidentes, ou pode advir das actividades de monitorização e detecção da própria equipa de resolução de incidentes.

A notificação de incidentes antecede a comunicação formal e o âmbito desta é recolher relatórios de incidentes, incluindo de fontes públicas. Para uma comunicação eficaz é importante estabelecer directrizes, as quais devem identificar: o que constitui um incidente (incluindo categorias, tipos de incidentes e prioridades); quem deve receber os relatórios; método de comunicação (e.g. via email); informação crítica a incluir no relatório; entre outros. Um formulário pode auxiliar a que a informação dos relatórios seja mais pertinente. Os relatórios podem ser submetidos por clientes, utilizadores, fornecedores, entre outros, e devem ser monitorizadas fontes públicas para potenciais ameaças. Devem ser estabelecidos procedimentos para lidar com relatórios falsos (e.g. relatórios *spam*, relatórios maliciosos).

A comunicação deve ser feita de acordo com as políticas da organização, devendo ser definido um ponto de contacto, que deve possuir as competências para determinar se os eventos são incidentes e iniciar, consoante a sua avaliação, os processos de resposta a incidentes.

*Avaliação e decisão*

Nesta fase é avaliado se um evento de segurança da informação se classifica como um incidente. Logo após ser comunicado um evento de segurança devem ser distribuídas responsabilidades e fornecer procedimentos para cada pessoa notificada.

De acordo com o ISO/IEC 27035-3:2020 (E) este processo começa com a triagem da informação recebida de eventos que é feita nas seguintes etapas:

1. Determinar da severidade do incidente;
2. Determinar se existe correlação com outros incidentes;
3. Definir a prioridade do incidente de acordo com critérios previamente estabelecidos;
4. Atribuir o incidente a alguém do processo de resposta.

É importante que a organização analise os incidentes por forma a descobrir o seu impacto na mesma. Algumas das questões que esta análise deve responder são:

- Qual o problema;

- Quem é afectado por ele;
- Quão espalhado está;
- Quão sério é; e
- Qual pode ser uma estratégia para a resposta.

A análise pode ser feita de várias formas:

- Análise ao sistema;
- Análise de rede;
- Análise de *malware*; e
- Análise forense.

Deve ser feita uma análise do incidente isolado e também uma análise da relação entre incidentes e da ocorrência repetida do mesmo incidente. Os dados devem ser recolhidos por pessoas com conhecimentos em levantamento e preservação de evidências, devem ser preservados de forma segura e quando o incidente é transferido para a equipa de resposta a incidentes esses dados devem-lhes ser transmitidos.

*Respostas*

As actividades desta fase dependem directamente da fase anterior. O objectivo não é apenas resolver o incidente e/ou recuperar os sistemas mas, também, prevenir e preparar para a ocorrência de incidentes similares.

Esta fase envolve a investigação do incidente de acordo com a classificação que lhe foi atribuída, e a equipa de resposta a incidentes deve verificar se o incidente se encontra sob controle ou se é necessário escalar a resposta.

A resposta a incidentes passa pelas seguintes actividades:

- Contenção

  Esta actividade pode ser iniciada logo na fase de detecção e análise. Algumas estratégias de contenção incluem:

  - Implementar blocos de *firewall*;
  - Desconectar o sistema afectado das redes locais e/ou públicas;
  - Desligar o sistema;
  - Bloquear mecanismos de transmissão entre sistemas;
  - Revogar contas de utilizadores que possam ter sido utilizadas durante o ataque;

  - Entre outros.

  Previamente às acções de contenção é importante que todos os dados necessários para a análise e evidências sejam colectados uma vez que as alterações ao sistema os podem afectar.

- Erradicação

  Esta actividade implica a eliminação de componentes (e.g. código malicioso, sistemas e/ou informação comprometida, contas e passwords). Algumas estratégias de erradicação incluem:

  - Eliminação de discos;
  - Actualização de *firmware*; e
  - Destruição física.

  É importante ter em atenção que a erradicação pode resultar na destruição de componentes de forma negligente o que pode significar danos para a organização.

- Recuperação

  Esta medida pretende reverter o sistema a um estado normal e seguro. Algumas estratégias de recuperação incluem:

  - Reconstrução de sistemas;
  - Alterar contas e passwords;
  - Tornar os sistemas mais resistentes; e
  - Recuperação através da continuidade de negócio.

No caso do incidente não estar sob controlo deve ser iniciado o processo de resposta a uma situação de crise.

Na figura 14 observa-se o fluxo das actividades de resposta.

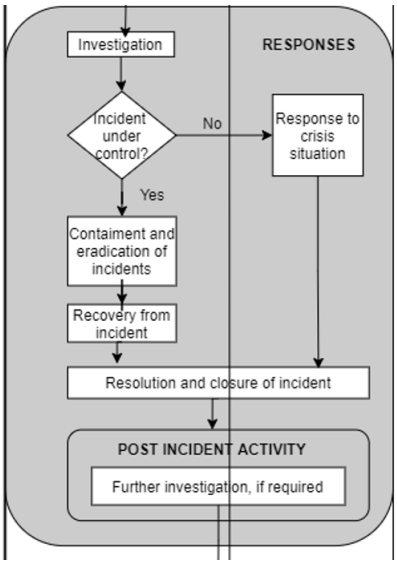



Figura 14: Fluxo das actividades de resposta a incidentes

Após a resolução do incidente deve ser feita uma análise da informação recolhida, um relatório dos resultados da análise e as partes interessadas devem ser notificadas.

É importante que todos os envolvidos na resposta registem todas as actividades para posterior análise e que as evidências digitais sejam recolhidas e guardadas de forma segura.

*Lições aprendidas*

Após o fecho de um incidente, a organização deve aprender de acordo com a informação que conseguiu retirar ao longo da sua resolução, compilar a informação recolhida de vários incidentes ou vulnerabilidades para procurar padrões, áreas mais afectadas e analisar onde podem ser executadas acções preventivas.

A análise de vulnerabilidades deve ser feita regularmente e após um incidente e não se deve focar apenas num sistema/serviço/rede.

A informação recolhida quer de incidentes quer de vulnerabilidades deve ser apresentada à administração da organização em reuniões periódicas.

Após a análise da informação pode ser notada a necessidade de alterações:

- Alterações aos controlos implementados

  A organização deve ter em conta as recomendações e implementar as alterações necessárias. No caso de não ser viável a implementação das mesmas num curto prazo, devem ser tidas em conta nos objectivos da organização a longo prazo. As recomendações podem passar por:

  - Adicionar ou melhorar controlos técnicos;
  - Acções de consciencialização;

  - Actualização de políticas e procedimentos;
  - Entre outros.

- Alterações à análise de risco

  Da análise de incidentes e vulnerabilidades pode advir a necessidade de uma actualização à análise de risco que tenha em conta novas ameaças.

- Alteração do plano de gestão de incidentes

  A equipa de resposta a incidentes deve rever as actividades de resposta e verificar a sua eficácia com o objectivo de determinar se há melhorias necessárias. No caso de um incidente significativo, deve ser feita uma reunião para discutir a eficácia do plano e determinar que áreas podem ser melhoradas. Os resultados devem ser documentados e todas as alterações devem ser previamente testadas.

Posterior à resolução de um incidente também é importante avaliar a equipa de resposta a incidentes. Métricas de *performance* podem facilitar o processo de avaliação da equipa.

*Categorização, classificação e critérios de incidente*

O ISO/IEC 27035-2:2020 (E) fornece exemplos de como categorizar e classificar incidentes.

Algumas categorias de incidentes são: desastres naturais, inquietação social, danos físicos, falha de infraestrutura, perturbação de radiação, falhas técnicas, ataques técnicos, violação de regras, comprometimento de funções, comprometimento de informação, conteúdo prejudicial, entre outros.

A classificação de incidentes pode ser feita de várias formas, como, por exemplo, definir orientações e usar uma escala para avaliar as consequências de incidentes. Exemplos de orientações que podem ser definidas são:

- Divulgação de informação não autorizada;
- Modificação de informação não autorizada;
- Repúdio de informação;
- Indisponibilidade de informação e/ou serviços;
- Destruição de informação e/ou serviços.

É importante ter em conta as consequências em termos de perdas financeiras, protecção de informação pessoal, interesse económico e comercial, obrigações legais e regulamentares, *performance* de operações de gestão e de negócio, deterioração de relações com funcionários, clientes, fornecedores, entre outros.

A definição de critérios para os incidentes é importante para conseguir uma resposta mais eficiente. Estes critérios devem ter em conta a importância da informação/sistema, impacto do incidente, danos causados, nível de alarme e a sua severidade.

O impacto do incidente é determinado de acordo com o tipo de incidente e pode ser baixo, moderado, importante ou muito importante.

A escala do incidente pode ser:

- Baixa - quando é possível existir impacto nos serviços críticos da organização;
- Moderado - quando o impacto nos serviços críticos é parcial, há pouca fuga de informação e as perdas financeiras são baixas;
- Importante - quando existe impacto significativo nos serviços críticos, existem grandes fugas de informação sensível ou as perdas financeiras são consideráveis;
- Muito importante - quando os serviços críticos são interrompidos ou as perdas financeiras são fatais;

Os critérios para a importância dos sistemas e/ou informação pode ser baixa, moderada, importante ou muito importante de acordo com a sua indispensabilidade para as actividades críticas da organização.

O nível de alarme pode ser classificado como preocupante, cauteloso, alerta ou sério e é determinado de acordo com a dimensão do incidente e a quantidade de sistemas afectado pelo mesmo.

*Vulnerabilidades*

Para avaliar as características e severidade de vulnerabilidades é comum ser utilizada a *framework Common Vulnerability Scoring System (CVSS)*. Esta baseia-se em 3 grupos de métricas:

- Características constantes;
- Características que se alteram com o passar do tempo; e
- Características únicas do ambiente de utilizador.

Na figura 15 observa-se o conjunto de métricas que compõe cada grupo.

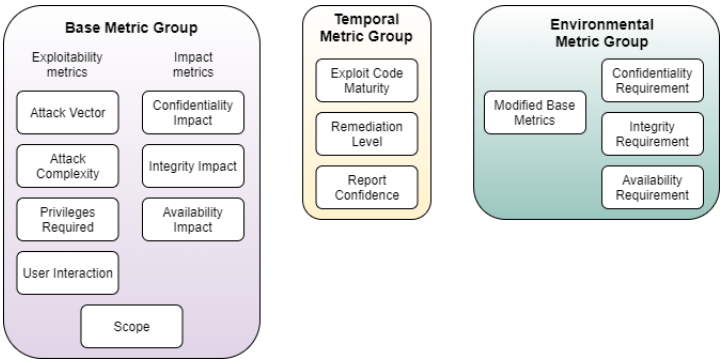



Figura 15: Grupos de métricas (baseada em figura do Common Vulnerability Scoring System)

A avaliação de acordo com esta *framework* resulta numa pontuação entre 0 e 10. Na figura 16 observa-se o processo utilizado para pontuar as vulnerabilidades.

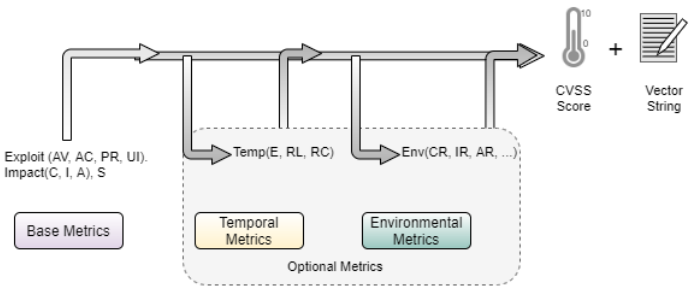



Figura 16: Processo de pontuação (baseada em figura do Common Vulnerability Scoring System)

A escala de pontuação da vulnerabilidade pode ser traduzida para uma escala qualitativa que se mostra na tabela 1.

| Rating | Score |
|---|---|
| Nenhum | 0.0 |
| Baixo | 0.1 - 3.9 |
| Médio | 4.0 - 6.9 |
| Alto | 7.0 - 8.9 |
| Crítico | 9.0 - 10.0 |

Tabela 1: Tabela qualitativa de escala de pontuação

### 2.2.4 *Avaliação de segurança*

Alguns sistemas de confiança seguros requerem a utilização de produtos que garantam certas propriedades de segurança. O *Common Criteria* (um conjunto de 3 *standards* Common Criteria Part 1, Common Criteria Part 2 e Common Criteria Part 3) tem como objectivo uniformizar

a avaliação de segurança de produtos de tecnologia de informação proporcionando uma base de requisitos para as funcionalidades de segurança dos produtos. As avaliações feitas segundo estes *standards* dão garantias aos utilizadores das propriedades de segurança dos produtos adquiridos.

*Target of evaluation" (TOE)* é o termo usado para identificar o *software*, *firmware* e/ou *hardware* alvo de avaliação. Para cada TOE deve ser definido um *Security target (ST)*.

Um ST é um documento que mostra os requisitos específicos de um TOE e, geralmente, são definidos por quem desenvolve o TOE. A figura 17 mostra a estrutura de um ST.

Os *Protection profiles (PP)* são documentos que descrevem os requisitos gerais de um tipo de TOE e, geralmente, são definidos pela comunidade de utilizadores, por quem desenvolve o produto ou por uma organização. Na figura 18 observa-se a estrutura destes documentos. Nestes documentos são definidos os requisitos de segurança que descrevem o comportamento expectável do TOE.

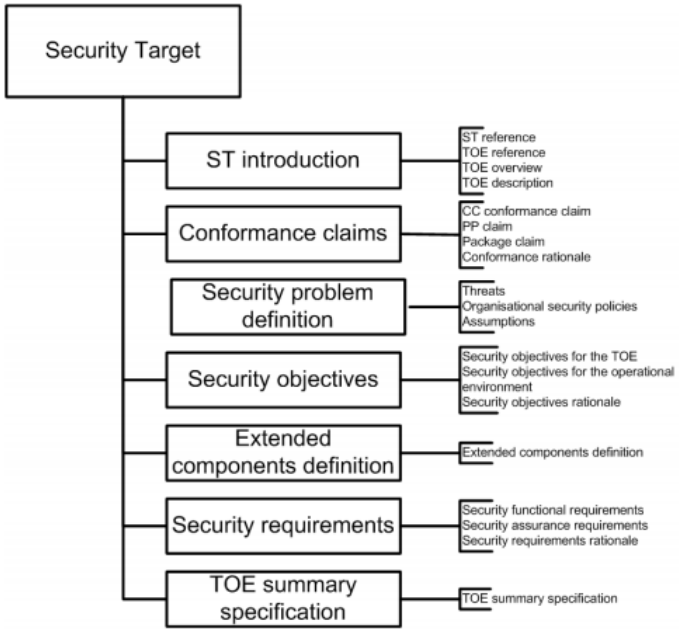



Figura 17: Estrutura e conteúdo do *Security Target* (Common Criteria Part 1)

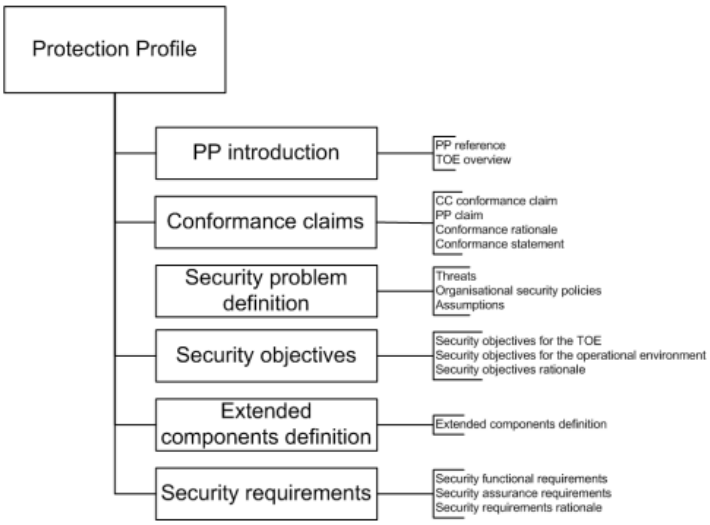



Figura 18: Estrutura e conteúdo do *Protection Profile* (Common Criteria Part 1)

A garantia que o *Common Criteria* proporciona é baseada numa avaliação da confiança do produto. As vulnerabilidades são um ponto importante a ter em conta

O *Common Criteria* define 7 níveis que demonstram o nível de garantia que o TOE cumpre os requisitos de segurança definidos.

- EAL1 - Testado funcionalmente

  Neste nível, a avaliação permite provar que o produto funciona de forma coerente com a sua documentação. A análise é feita através da procura de potenciais vulnerabilidades e documentação fornecida, não sendo necessário o suporte da equipa de desenvolvimento. Este nível é útil quando é necessária alguma confiança no entanto as ameaças não são preocupantes.

- EAL2 - Testado estruturalmente

  Este nível requer a cooperação da equipa de desenvolvimento para fornecer informação do *design* e resultados de testes. Aumenta a garantia em relação ao anterior no entanto não requer grande aumento de investimento ou tempo.

- EAL3 - Testado e verificado metodicamente

  Para obter este nível é feita uma análise aos requisitos funcionais de segurança descritos no ST do TOE, é utilizada documentação guia, descrição da arquitectura e *design* para compreender o comportamento de segurança do TOE. Este requer uma análise de vulnerabilidades que demonstre resistência a atacantes com o potencial de ataque básico. Aumenta a garantia em relação ao nível anterior pois requer testes mais completos das funcionalidades de segurança e mecanismos/procedimentos que proporcionam confiança de modificações não autorizadas durante o desenvolvimento.

- EAL4 - Desenhado, testado e revisto metodicamente

  Neste nível são analisadas todos os requisitos de segurança funcionais definidos no ST e para compreender o comportamento de segurança do TOE é utilizada a "especificação completa e funcional da *interface*, documentação guia, descrição do *design* do TOE, e um subconjunto da implementação"(Common Criteria Part 3). Este nível requer testes independentes das funções de segurança do TOE e análise de vulnerabilidades que demonstre resistência a intrusão de atacantes com um potencial de ataque básico mas superior ao anterior. Representa uma melhoria em relação ao anterior pois requer mais detalhes do *design*, a representação da implementação de todas as funções de segurança do TOE e melhores mecanismos/procedimentos que proporcionam a garantia de que não existem modificações não autorizadas durante o desenvolvimento.

- EAL5 - Desenhado e testado semi-formalmente

  Este nível requer análise de vulnerabilidades independente que demonstre resistência a intrusão de atacantes com um potencial de ataque moderado. A garantia aumenta em relação ao anterior pois requer descrições semi-formais de *design* e uma arquitectura mais estruturada.

- EAL6 - *design* verificado e testado semi-formalmente

  Este nível requer a análise de vulnerabilidades que demonstre resistência a atacantes com potencial de ataque alto. Neste nível é necessário uma análise mais compreensiva, representação estruturada da implementação, arquitectura estruturada e melhoria na gestão de configurações e controlos de ambiente.

- EAL7 - *design* verificado e testado formalmente

  Este nível requer representações formais, incluindo da implementação. É adequado a TOEs utilizados em aplicações de alto risco onde se justifica o aumento de custos derivado deste tipo de análise.

### 2.2.5 *Métricas*

As métricas são utilizadas para auxiliar o processo de tomada de decisões e melhorar a *performance* das actividades da organização. O objectivo é monitorizar o estado das actividades e melhorar essas actividades de acordo com os resultados obtidos, NIST Special Publication 800-55. Neste sentido as métricas de segurança de informação são baseadas em objectivos e metas de *performance* e devem monitorizar o cumprimento desses objectivos e metas.

As métricas devem ser quantificáveis, os dados recolhidos devem ser de fácil obtenção e os processos a avaliar devem ser mensuráveis, isto é, só devem ser considerados processos consistentes, documentados e repetíveis.

O NIST Special Publication 800-55 define três tipos de métricas que são utilizados dependendo do estado de maturidade do programa de segurança de informação da organização. Na figura 19 observa-se o tipo de métrica indicada para cada estado de maturidade, no entanto vários tipos de métricas podem ser usados simultaneamente. Consoante o programa de segurança da informação se vai tornando mais avançado, mais informação haverá, e esta será de obtenção mais fácil, o que permite melhor avaliação de resultados.

| Processes | Evolving | Defined and Documented | Well Established | Self-Regenerating |
|---|---|---|---|---|
| Operating Procedures | Being Defined | Stabilizing | Institutionalized | Self-Adjusting |
| Data Availability | Non Existent | Can Be Collected | Available | In Standardized Repository |
| Collection Difficulty | High | Medium | Low | Integral to Business Processes |
| Collection Automation | Low | Medium | High | Full |
| | IT Security Goals | Implementation | Efficiency and Effectiveness | Business Impact |

Figura 19: Maturidade do programa de segurança de informação e tipos de métricas (baseada em figura do NIST Special Publication 800-55)

Na figura 20 observa-se o processo de desenvolvimento das métricas de segurança de informação sendo que não precisam de ser necessariamente actividades sequenciais.

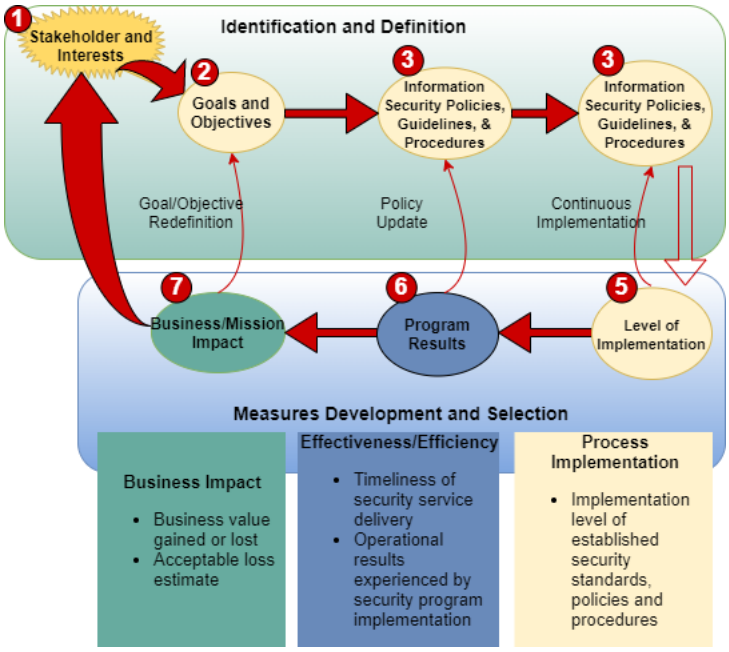



Figura 20: Processo de desenvolvimento das métricas (baseada em figura do NIST Special Publication 800-55)

O NIST Special Publication 800-55 define um *template* que pode ser utilizado para o desenvolvimento de métricas.

É importante definir objectivos de *performance* que estabelecem referências de sucesso. O grau de sucesso é medido segundo a proximidade do resultado da métrica ao objectivo de *performance*.

O processo de implementação do programa de métricas de segurança da informação é descrito na figura 21. A implementação das métricas de segurança envolve monitorizar a *performance* dos controlos de segurança e aplicar acções de melhoria de acordo com os resultados.

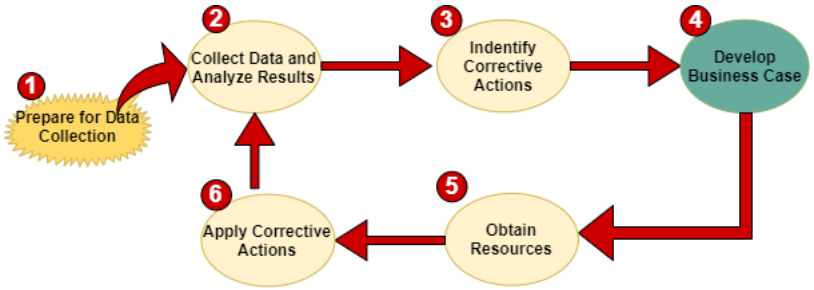



Figura 21: Implementação das métricas (baseada em figura do NIST Special Publication 800-55)

# 3

# INFRAESTRUTURA DE CHAVE PÚBLICA

Neste capítulo é apresentada uma contextualização das componentes da ICP do Cartão de Cidadão assim como da regulamentação e legislação aplicável.

## 3.1 COMPONENTES DA INFRAESTRUTURA DE CHAVE PÚBLICA DO CARTÃO DE CIDADÃO

O termo *e-Government* pretende reflectir o uso de novas tecnologias de informação na administração pública, com o objectivo de facilitar o acesso dos cidadãos a informação e serviços do estado.

No sentido de fortalecer a sociedade de informação e do *e-Government*, o Governo Português, na Resolução do Conselho de Ministros nº171/2005, decidiu "criar e desencadear a colocação em funcionamento de uma Entidade de Certificação Electrónica do Estado - Infra-Estrutura de Chaves Públicas".

Uma ICP resolve o problema de confiança nas transacções electrónicas, pois proporciona a base de confiança que garante a identidade de cada uma das partes. A criação desta entidade tornou possível mecanismos de autenticação digital forte de identidades e assinaturas electrónicas. Um dos projectos que a ICP tornou possível foi a adição de mecanismos de assinatura digital e autenticação ao Cartão de Cidadão.

O Cartão de Cidadão "fornece os mecanismos necessários para a autenticação digital forte da identidade do Cidadão perante os serviços de Administração Pública, assim como as assinaturas electrónicas indispensáveis aos processos de desmaterialização que têm vindo a ser disponibilizados pelo Estado", Declaração de Práticas de Certificação da EC do Cartão de Cidadão.

A ICP do estado funciona independentemente de ICP privadas ou estrangeiras e permite a interoperabilidade com outras ICP, nomeadamente no âmbito de países da União Europeia(UE), Resolução do Conselho de Ministros nº171/2005.

### 3.1.1 *Hierarquia de certificação*

No modelo hierárquico da Entidade de Certificação Electrónica do Estado, existe uma Entidade de Certificação Raiz, na qual todos os utilizadores confiam plenamente. A Entidade de Certificação Raiz assina o seu próprio certificado e o das *Entidades de Certificação (ECs)* no nível directamente abaixo dela. Os certificados das ECs intermédias são assinados pela EC no nível directamente acima e assinam os certificados das EC directamente abaixo, conforme a Declaração de Práticas de Certificação da Entidade Certificadora Eletrónica do Estado.

Na figura 22 observa-se a hierarquia da ICP do Cartão de Cidadão.

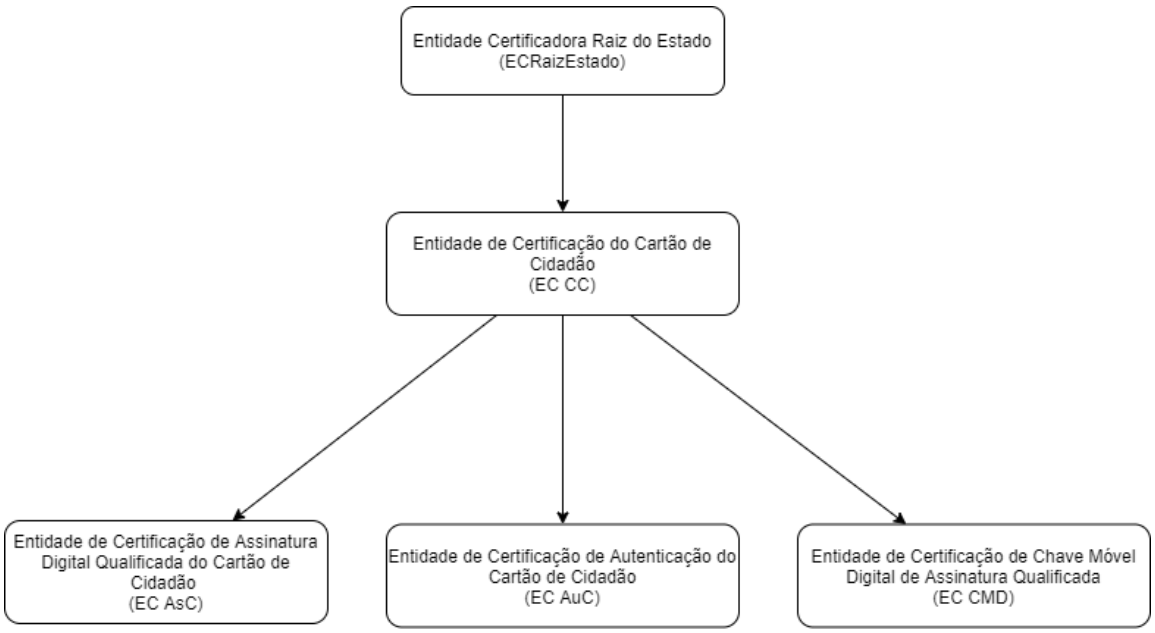



Figura 22: Hierarquia da Infraestrutura de Chave Pública do Cartão de Cidadão

### 3.1.2 *Infraestrutura de Chave Pública do Cartão de Cidadão*

Os certificados digitais introduzem confiança na associação entre chave pública e titular da mesma. Esta confiança só é possível se uma terceira parte de confiança, neste caso uma EC, "assinar a chave pública emitindo um certificado que liga a chave pública à entidade que tem na sua posse a chave privada correspondente", ITU-T Recomendation x.509. O certificado emitido pela EC contém, no mínimo, informação sobre o subscritor (e.g. nome) e a chave pública, e é assinado digitalmente pela EC. A política de certificados de cada EC define concretamente a informação que o certificado deve ter.

A ICP do Cartão de Cidadão é constituída por várias entidades de certificação, cada uma com um propósito diferente, emitindo certificados com objectivos distintos e em conformidade com a Política de Certificados do SCEE e Requisitos Mínimos de Segurança.

*Entidade de Certificação do Cartão de Cidadão*

A Entidade de Certificação do Cartão de Cidadão emite certificados para as entidades certificadoras subordinadas e para serviços necessários no âmbito do Cartão de Cidadão, nomeadamente, para a Entidade de Certificação de Assinatura Digital Qualificada ( Política de Certificado de Assinatura Digital Qualificada), para a Entidade de Certificação de Autenticação ( Política de Certificado da EC de Autenticação do Cartão de Cidadão), para a Entidade de Certificadora de Documentos ( Política de Certificado de Entidade Certificadora de Documentos) e o certificado para o serviço de Validação *Online Certificate Status Protocol (OCSP)* ( Política de Certificado de Validação on-line OCSP emitido pela EC do Cidadão).

Esta entidade providencia a gestão de serviços de certificação, isto é, emissão, operação, suspensão e revogação de certificados aos seus subscritores, neste caso, às entidades subordinadas, de acordo com a Declaração de Práticas de Certificação da EC do Cartão de Cidadão.

Por questões de segurança, a Entidade de Certificação do Cartão de Cidadão funciona exclusivamente em modo *offline*.

A emissão dos certificados é feita com recurso a uma cerimónia auditada em zona de alta segurança e o certificado é entregue directamente ao representante da entidade que se encontra presente na cerimónia. Este processo não é mediado por nenhuma entidade de registo.

*Entidade de Certificação de Assinatura Digital Qualificada do Cartão de Cidadão*

A Entidade de Certificação de Assinatura Digital Qualificada de acordo com a Declaração de Práticas de Certificação da EC de Autenticação do Cartão de Cidadão, emite, opera, suspende e revoga certificados digitais de assinatura qualificada, conforme a Política de Certificado de Assinatura Digital Qualificada, a utilizadores finais, neste caso, cidadãos portugueses. Este certificado é colocado no *smartcard* do Cartão de Cidadão e entregue ao utilizador final no estado inactivo. Para além desses certificados, esta entidade também emite certificado para o Serviço de Validação Cronológica ( Política de Certificado de Validação Cronológica) e para o serviço de validação *online* OCSP ( Política de Certificado de Validação on-line OCSP emitido pela EC AsC).

Os titulares dos certificados são identificados e autenticados pela Entidade de Registo. Posteriormente a Entidade de Registo entrega ao titular o Cartão de Cidadão com os certificados e procede à sua activação com o consentimento expresso do titular.

Esta EC não suporta renovação de certificados, mas suporta a renovação de chaves do certificado onde é gerado um novo par de chaves e é emitido um novo certificado, no pedido de novo Cartão de Cidadão.

*Entidade de Certificação de Autenticação do Cartão de Cidadão*

A Entidade de Certificação de Autenticação do Cartão de Cidadão de acordo com a Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão emite, opera, suspende e revoga certificados digitais de autenticação, conforme a Política de Certificado da EC de Autenticação do Cartão de Cidadão que estão presentes no Cartão de Cidadão. Emite, também, certificado para o serviço de validação *online* OCSP ( Política de Certificado de Validação on-line OCSP emitido pela EC AuC).

Tal como no caso da Entidade de Certificação de Assinatura Digital Qualificada, os titulares são identificados e autenticados pela Entidade de Registo. Neste caso, os certificados de autenticação são activados, obrigatoriamente, no acto de entrega, após a autenticação do titular, através dos seus dados biométricos.

Esta entidade não suporta renovação de certificados, mas suporta a renovação de chaves do certificado, onde é gerado um novo par de chaves e é emitido um novo certificado, no pedido de novo Cartão de Cidadão.

*Entidade de Certificação de Chave Móvel Digital de Assinatura Qualificada do Cartão de Cidadão*

A Entidade de Certificação de Chave Móvel Digital de Assinatura Qualificada do Cartão de Cidadão, de acordo com a Declaração de Práticas de Certificação da EC de Chave Móvel Digital de Assinatura Qualificada do Cartão de Cidadão, emite, opera, suspende e revoga certificados digitais de assinatura digital, conforme Política de Certificado de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão, para os seus subscritores. Emite, também, certificado para o serviço de validação *online* OCSP.

A validação da identidade do titular do certificado é feita recorrendo ao Cartão de Cidadão ou Bilhete de Identidade, de forma *online* ou presencial, conforme Declaração de Práticas de Certificação da EC de Chave Móvel Digital de Assinatura Qualificada do Cartão de Cidadão. O par de chaves é gerado em *hardware* criptográfico e é guardado, juntamente com o certificado digital correspondente, num ambiente criptográfico seguro protegido por palavra-passe fornecida pelo titular.

### 3.1.3 *Entidade de registo*

O registo de subscritores é o processo de reunir informação do subscritor e verificar a sua identidade.

As *Entidade de Registo (ER)* autenticam o subscritor e emitem o pedido de certificação à ER. A autenticação feita pela ER serve para garantir a identidade de quem pede o certificado. A ER também tem autoridade nos pedidos de revogação ou suspensão de certificados.

No caso da ICP do Cartão de Cidadão, a Entidade de Registo é assumida pelo Instituto dos Registos e Notariado (IRN), entre outros, conforme indicado na Declaração de Práticas de Certificação de cada entidade de certificação da ICP do Cartão de Cidadão, ( Declaração de Práticas de Certificação da EC de Autenticação do Cartão de Cidadão, Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão, Declaração de Práticas de Certificação da EC de Chave Móvel Digital de Assinatura Qualificada do Cartão de Cidadão).

### 3.1.4 *Entidade de Validação Cronológica*

A *Entidade de Validação Cronológica (EVC)* tem o papel de emitir selos temporais, que beneficiam da presunção de exactidão de data e da hora que indicam, e da integridade dos dados aos quais a data e hora estão associados ( ETSI EN 319 422 e RFC 3161). Isto é feito através dos selos temporais que vinculam dados a uma data e hora, provando a sua existência numa dada altura.

Os selos temporais emitidos pela EVC, de acordo com a Declaração de Práticas de Validação Cronológica, podem ser utilizados sempre que é necessário vincular dados em formato electrónico a uma hora específica, criando uma prova de que esses dados existiam nesse momento. Em particular, podem ser utilizados para validade a longo prazo de documentos.

A EVC tem de usar sempre uma fonte e tempo de confiança e incluir um valor de tempo de confiança em cada um dos selos temporais emitidos.

A EVC tem de usar uma chave para assinar os selos temporais gerada apenas para esse efeito.

### 3.1.5 *Serviço de estado de revogação*

Um certificado é emitido com uma data de validade e pode ser usado durante esse período. No entanto, podem surgir circunstâncias em que seja necessário revogar um certificado. É da responsabilidade da EC indicar o estado de revogação dos certificados que emitem.

Existem duas formas principais de proporcionar aos utilizadores o estado de revogação de certificados:

- *Certification Revocation List (CRL)*
- *Online Certificate Status Protocol*(OCSP)

Uma CRL é uma lista que identifica certificados revogados, assinada pela EC e disponibilizada livremente num repositório público, conforme o RFC 5280. A periodicidade de emissão de CRL varia, dependendo da política de cada EC, e os certificados revogados são

identificados pelo seu número de série. Cada CRL tem definido um campo de *nextUpdate* que indica a data e hora de emissão da próxima CRL, significando na prática, que após essa data e hora, a CRL não é válida.

O OCSP, conforme o RFC 6960, permite que aplicações determinem o estado de um certificado. O OCSP permite obter o estado do certificado no momento do pedido, enquanto na CRL o estado do certificado será o do momento em que a mesma foi emitida. O pedido ao serviço OCSP deve conter a seguinte informação: versão do protocolo; pedido do serviço; identificador do certificado; e outras extensões. Após receber o pedido, o serviço deve confirmar se o mesmo está correcto e a sua resposta deve ser assinada digitalmente, incluindo a data e hora da resposta.

Existem várias razões para a revogação de certificados, no caso da ICP do Cartão de Cidadão consideram-se as seguintes razões válidas para a revogação de um certificado, conforme a Declaração de Práticas de Certificação da EC do Cartão de Cidadão:

- Comprometimento ou suspeita de comprometimento da chave privada;
- Perda da chave privada;
- Inexactidões graves nos dados fornecidos;
- Equipamento tecnológico deixa de ser utilizado no âmbito do Cartão de Cidadão;
- Comprometimento ou suspeita de comprometimento da chave privada da EC da hierarquia;
- Revogação do certificado de uma EC da hierarquia;
- Incumprimento por parte da EC ou titular das responsabilidades acordadas;
- Sempre que hajam razões credíveis que induzam que os serviços de certificação possam ter sido comprometidos, de tal forma que coloquem em causa a fiabilidade dos certificados;
- Por resolução judicial ou administrativa.

Depois de efectuado o pedido de revogação por alguma entidade com legitimidade para tal, este é tratado de forma imediata e nunca superior a 24h. Após a verificação de que o pedido é válido, a revogação é feita de forma imediata.

Os serviços de estado de revogação são utilizados pelas partes confiantes, que têm a responsabilidade de verificar o estado do certificado antes de o utilizarem.

A Entidade de Certificação do Cartão de Cidadão publica no repositório, uma nova CRL sempre que há uma revogação e todos os meses quando não existem revogações. As restantes entidades de certificação da ICP do Cartão de Cidadão a CRL é publicada semanalmente e uma delta-CRL diária.

Este serviço está disponível 24 horas por dia, 7 dias por semana, sendo que em caso de falha do sistema estão preparados mecanismos para poder continuar com o serviço activo.

### 3.1.6 *Geração de chaves*

A geração de chaves criptográficas da Entidade de Certificação do Cartão de Cidadão é efectuada em cerimónia auditada, usando um *hardware* criptográfico seguro (*Hardware Security Module (HSM)*) que cumpre os requisitos FIPS 140-2 nível 3 , conforme FIPS PUB 140-2, e *Common Criteria* EAL 4+, conforme Common Criteria Part 3.

O HSM é também usado para a manutenção, armazenamento e qualquer outras operações que envolvam as chaves.

O par de chaves é gerado com base no algoritmo RSA e as chaves têm dimensão de 4096 bits.

### 3.1.7 *Personalização*

Para o cidadão, o Sistema de Ciclo de Vida, personaliza fisicamente o chip criptográfico presente no Cartão de Cidadão com o par de chaves e certificado. O par de chaves é gerado automaticamente usando *hardware* criptográfico seguro (HSM) que cumpre os requisitos FIPS 140-2 nível 3, conforme FIPS PUB 140-2 e Common Criteria EAL4+, conforme Common Criteria Part 3.

Os certificados emitidos para o cidadão são enviados para o sistema de personalização de acordo com a norma PKCS#10 (RFC 2986).

### 3.1.8 *Recursos Humanos*

Para garantir o bom funcionamento das EC são necessários vários recursos humanos com conhecimento especializado em várias áreas.

Os recursos humanos ao serviço da ICP do Cartão de Cidadão estão divididos em vários grupos de trabalho. Estes grupos de trabalho são constituídos por pessoas devidamente autenticadas e que cumprem um conjunto de requisitos de qualificações, experiência, antecedentes e credenciação. Para além disso, são também realizadas acções de formação e treino em assuntos necessários ao desempenho das suas funções.

Assim, os papéis de confiança foram agrupados em sete grupos de trabalho distintos para segregação de papéis, sendo eles, conforme Declaração de Práticas de Certificação da EC do Cartão de Cidadão:

- Grupo de Trabalho de Inicialização - instala, configura e interliga o *software* e *hardware* da EC e prepara os comunicados necessários para as operações dos restantes grupos de trabalho;
- Grupo de Trabalho de Informação - assegura a disponibilidade de toda a informação necessária para o funcionamento da EC e gere o Ambiente de Informação;
- Grupo de Trabalho de Política - elabora todas as políticas da EC e garante a sua actualização, assume o papel de Administrador de Segurança;
- Grupo de Trabalho de Auditoria - realiza a auditoria interna a todos os processos e cerimónias da EC, desempenha o papel de Auditor de Sistemas;
- Grupo de Trabalho de Operação - executa as tarefas de rotina da EC, incluindo operações *backup* e de monitorização de sistemas, desempenha o papel de Operador de Sistemas e Administrador de Registo;
- Grupo de Trabalho de Autenticação - gere todas as palavras-passes não pessoais e *tokens* de autenticação e gere o Ambiente de Autenticação. Este grupo assume o papel de Administrador de Sistemas e Administrador de Registo;
- Grupo de Trabalho de Monitorização e Controlo - responsável pela gestão de incidentes e supervisiona o desempenho dos controlos de segurança existentes;
- Grupo de Trabalho de Gestão - nomeia os membros dos restantes grupos de trabalho, revê e aprova as políticas propostas e gere o Ambiente de Gestão, onde estão guardados alguns artefactos sensíveis;
- Grupo de Trabalho de Custódia - existem vários grupos de custódia, cada um responsável por um conjunto de artefactos guardados em ambientes seguros.

Na figura 23 podemos observar as incompatibilidades de funções em cada EC.

| Se pertence ao Grupo/Subgrupo ... | Pode pertencer ao Grupo/Subgrupo ... ? | Instalação | Políticas | Operação | | Autenticação | | Auditoria | Monitorização e Controlo | Custódia | Gestão | Gestão da Informação |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Subgrupo 1 | Subgrupo 2 | Subgrupo 1 | Subgrupo 2 | | | | | |
| Instalação | | | | | | | | x | | x | x | |
| Políticas | | | | | | x | x | x | x | x | x | |
| Operação | Subgrupo 1 | | | | x | x | x | x | | x | x | |
| | Subgrupo 2 | | | x | | x | x | x | | x | x | |
| Autenticação | Subgrupo 1 | | x | x | x | | x | x | | x | x | x |
| | Subgrupo 2 | | x | x | x | x | | x | | x | x | x |
| Auditoria | | x | x | x | x | x | x | | x | x | x | x |
| Monitorização e Controlo | | | x | x | x | | | x | | x | x | x |
| Custódia | | x | x | x | x | x | x | x | x | | x | x |
| Gestão | | x | x | x | x | x | x | x | x | x | | x |
| Gestão da Informação | | | | | | x | x | x | x | x | x | |

Figura 23: Incompatibilidade de funções (Declaração de Práticas de Certificação da EC do Cartão de Cidadão)

As EC implementam procedimentos de controlo de acesso, com divisão de responsabilidades, para que operações críticas ao sistema apenas possam ser executadas por um conjunto (mínimo 2) de pessoas autenticadas.

### 3.1.9 *Ambientes*

Cada EC da ICP do Cartão de Cidadão está dividida em vários ambientes, com objectivos diferentes e com controlo de acessos distinto. A existência destes ambientes é importante para assegurar o armazenamento seguro de artefactos relacionados com a operação das EC, todos eles se encontram em espaços seguros e com acesso restrito a pessoas autorizadas para tal:

- Ambiente de produção
- Ambiente de operação
- Ambiente de informação

- Ambiente de autenticação
- Ambiente de gestão
- Ambiente de custódia

O Ambiente de produção, onde estão localizados os sistemas das EC, está protegido por um mínimo de 4 níveis de segurança física: edifício em si, bloco de alta segurança, área de alta segurança e, por fim, sala de alta segurança onde estão localizados os sistemas de acordo com a Norma Técnica - D 02. Para aceder a cada um dos níveis, é necessário autorização para aceder ao nível imediatamente anterior e todos os acessos físicos são automaticamente registados. Para aceder à sala de alta segurança, é necessário controlo duplo, com dois factores de autenticação, um deles sendo autenticação biométrica. Para além disso, o *hardware* criptográfico e *tokens* físicos são guardados em cofres e armários seguros.

O ambiente de produção tem também equipamento redundante de energia e ventilação, detectores de inundação e mecanismos necessários para evitar e apagar fogos.

### 3.1.10 *Políticas e Práticas*

Por forma a garantir o bom funcionamento e a segurança dos serviços da ICP do Cartão de Cidadão, são implementadas várias políticas e práticas através das quais as actividades da ICP do Cartão de Cidadão são conduzidas.

*Documentos Públicos*

- Declaração de Práticas de Certificação

  Para cada EC que constitui a ICP do Cartão de Cidadão, foi elaborada uma Declaração de Práticas de Certificação, onde são definidos os procedimentos e práticas utilizados. Estes documentos seguem a estrutura definida e proposta no documento RFC 3647, de acordo também com a estrutura recomendada pelo SCEE e pelos ETSI EN 319 411-1 e ETSI EN 319 411-2.

  Este documento "explica o que um Certificado fornece, assim como os procedimentos que deverão ser seguidos por Partes de Confiantes e por qualquer pessoa interessada, para confiarem nos Certificados emitidos"(Declaração de Práticas de Certificação da EC do Cartão de Cidadão). É um documento público, disponível 24/7 no repositório público da ICP do Cartão de Cidadão.

- Política de Certificados

Estes documentos ( Política de Certificado da EC do Cidadão, Política de Certificado de Assinatura Digital Qualificada, Política de Certificado da EC de Autenticação do Cartão de Cidadão e Política de Certificado de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão) apresentam o perfil de certificado de cada uma das EC e complementa a Declaração de Práticas de Certificação.

- Declaração de Divulgação de Princípios

  Este documento segue a estrutura definida no anexo A do ETSI EN 319 411-1 e "pretende resumir, de forma simples e acessível, as características descritas nas Políticas de Certificado e Declaração de Políticas de Certificação da Infraestrutura de chave pública da Entidade de Certificação do Cartão de Cidadão", Declaração de Divulgação de Princípios.

*Gestão de Risco*

Existem procedimentos para a identificação, análise e mitigação de riscos associados às actividades da ICP do Cartão de Cidadão. Isto incluí também a análise de recursos e a sua importância para as actividades da ICP.

Em função da análise efectuada são concretizadas todas as medidas necessárias para garantir o nível de segurança desejado.

*Gestão de Incidentes*

A ICP do Cartão de Cidadão tem em prática uma política de gestão de incidente que determina a base para a identificação e classificação de incidentes. Existem, também, procedimentos de resposta a incidentes para uma resolução rápida e eficiente dos mesmos.

Tal como é recomendado no ETSI EN 319 401, existem papéis de confiança definidos para dar seguimento a eventos de segurança, sendo eles, o Grupo de Monitorização e Controlo (responsável por "monitorizar eventos, gerir alarmes e classificar incidentes"(Declaração de Práticas de Certificação da EC do Cartão de Cidadão) e o Grupo de Operação (responsável por "monitorizar, reportar e quantificar todos os incidentes e avarias de *software* e *hardware*"(Declaração de Práticas de Certificação da EC do Cartão de Cidadão).

*Continuidade de Negócio*

A ICP do Cartão de Cidadão tem em prática um Plano de Continuidade de Negócio em caso de desastre. Este plano define os procedimentos para continuar com as operações críticas mesmo em caso de desastre.

Para ser possível continuar com as actividades em caso de desastre, a organização tem instalações secundárias, *hardware* redundante e cópias de segurança.

*Cessação de Actividades*

A ICP do Cartão de Cidadão tem em prática um Plano de Acção em caso de cessação de actividade onde estão definidas as várias acções a executar, incluindo:

- Notificação das entidades que intervêm na actividade
- Cessação de relações contratuais
- Revogação dos certificados
- Transferência de funções quando aplicável

*Gestão de Alterações*

A ICP do Cartão de Cidadão implementa procedimentos para a gestão eficaz de alterações.

As alterações a *hardware*, *software* e recursos humanos são sempre registadas e as alterações a *software* são executadas e auditadas por membros dos Grupos de Trabalho.

Qualquer sugestão de alteração de *hardware* ou *software* padece da aprovação do Grupo de Gestão.

Para a alteração de documentos é necessária a aprovação do Grupo de Trabalho de Políticas, sendo eles os responsáveis pela actualização dos documentos de acordo com a alteração. Posteriormente, o documento é analisado pelo Grupo de Trabalho da Informação e pelo Grupo de Gestão, que, aceitando as alterações, aprova o documento.

*Gestão de Recursos Humanos*

A ICP tem em prática uma política de recursos humanos que define regras para a nomeação de papéis de confiança, funções a desempenhar por cada Grupo de Trabalho, descritos na secção 3.1.8, requisitos de formação entre outros.

*Gestão de Ambientes*

A gestão de ambientes da ICP do Cartão de Cidadão inclui, entre outros, as regras de acesso a cada ambiente, definido na secção 3.1.9 e os responsáveis por esses ambientes.

## 3.2 Legislação e normas aplicáveis

Nesta secção apresentar-se-á a legislação, portuguesa e europeia, bem como as normas europeias, em particular do *European Telecommunications Standards Institute*, que se aplicam à ICP do Cartão de Cidadão e são relevantes para o desenvolvimento desta dissertação.

### 3.2.1 *Regulamento eIDAS*

O Regulamento (UE) Nº 910/2014, também conhecido como regulamento eIDAS, estabelece normas aplicáveis a todos os serviço de confiança. No entanto, é necessária uma distinção entre serviço de confiança qualificados e não qualificados, devido ao tipo de serviço que estes últimos prestam.

De forma a garantir o alto nível de segurança dos serviços de confiança qualificados, o eIDAS prevê um esquema de supervisão activa do prestador qualificado de serviços de confiança e, também, dos serviços de confiança qualificados que eles providenciam, ENISA(2016).

O regulamento eIDAS define 9 tipos diferentes de serviços de confiança qualificados, sendo eles:

- Emissão de certificados qualificados para assinaturas electrónicas, selos electrónicos e autenticação de *websites*;
- Serviço de preservação qualificado para assinaturas electrónicas qualificadas e selos electrónicos;
- Serviço de validação qualificado para assinaturas e selos electrónicos;
- Serviço de selos temporais qualificado; serviço de envio registado electrónico qualificado, ENISA(2016).

Para distinguir os serviços de confiança qualificados dos não qualificados, foi criada uma marca de confiança da União Europeia, conforme a figura 24. Esta marca pretende contribuir para a transparência do mercado.

Figura 24: Marca de confiança (ENISA(2016))

Todos os prestadores qualificados de serviços de confiança estão sujeitos a uma avaliação de conformidade, pelo menos uma vez de dois em dois anos, pelo organismo de avaliação da conformidade, que analisa se são cumpridos os requisitos do regulamento eIDAS.

*Requisitos aplicáveis a todos os prestadores de serviços de confiança*

Os prestadores de serviços de confiança devem tomar medidas no que toca ao processamento e protecção de dados pessoais, em particular, devem fazê-lo de acordo com o RGPD, e, em caso de falha de segurança ou perda de integridade, a entidade supervisora e o(s) subscritor(es) a quem diz respeito a falha, deve(m) ser notificado(s) o mais rápido possível.

O regulamento também afirma, no artigo 19º, que os prestadores de serviços de confiança devem tomar as devidas medidas de segurança para gerir o risco, para prevenir e minimizar o impacto de incidentes de segurança, tendo em conta os últimos avanços tecnológicos. Essas medidas devem garantir que o nível de segurança é proporcional ao nível do risco.

*Requisitos para prestadores qualificados de serviços de confiança*

No artigo 24º do Regulamento eIDAS são definidos os requisitos aplicáveis aos prestadores qualificados de serviços de confiança. Nesta secção iremos salientar os requisitos mais importantes para esta dissertação.

No artigo 24º é definido que os prestadores qualificados de serviços de confiança devem notificar a entidade supervisora de qualquer alteração no que diz respeito à prestação do serviço de confiança qualificado, especialmente em caso de cessação, esta é uma medida importante para proteger os subscritores do serviço.

Este artigo define as regras para os recursos humanos, devendo o prestador qualificado de serviços de confiança garantir a segregação de funções, e contratar pessoal com competências adequadas às funções a desempenhar, para além disso, deve também garantir a sua formação contínua.

Neste artigo, é também referido que o prestador qualificado de serviços de confiança tem de informar o subscritor dos termos e condições de uso do serviço antes de entrar em qualquer relação contratual com o mesmo, e tem de garantir a disponibilidade e integridade do documento de termos e condições.

O prestador qualificado de serviços de confiança deve manter um plano de cessação de actividade e de continuidade de negócio actualizados.

*Requisitos para prestadores qualificados de serviços de confiança que emitam selos temporais qualificados*

O artigo 42º do Regulamento eIDAS, define os requisitos dos prestadores qualificados de serviços de confiança que emitem selos temporais qualificados:

- O selo temporal deve "vincular a data e a hora aos dados de forma a tornar razoavelmente impossível a alteração dos dados de forma não detectável", Regulamento eIDAS;

- A data e hora deve ser de uma fonte horária exacta ligada à *Universal Time Coordinated (UTC)*;
- O selo temporal deve ser assinado utilizando para o efeito uma assinatura digital avançada, ou por método equivalente.

*Requisitos para prestadores qualificados de serviços de confiança que emitam certificados qualificados para assinatura digital*

No artigo 28º do Regulamento eIDAS, é indicado que os certificados qualificados de assinaturas electrónicas têm que cumprir os requisitos do anexo I do referido regulamento, onde é definido o conteúdo dos certificados. Para além disso, os certificados qualificados de assinaturas electrónicas não podem estar "sujeitos a requisitos obrigatórios que excedam os requisitos estabelecidos no anexo I", no entanto, podem incluir características adicionais desde que não prejudiquem a interoperabilidade e reconhecimento das assinaturas electrónicas qualificadas.

*Requisitos para sistemas de identificação electrónica*

Um sistema de identificação electrónica é um sistema que permite que uma pessoa prove a sua identidade electronicamente.

No artigo 8º são definidos três níveis de garantia para os meios de identificação electrónica :

- Reduzido

  Neste nível, a entidade considera que a pessoa tem em sua posse elementos de prova de identidade reconhecidos e que estes são genuínos. Estes meios de identificação electrónica utilizam, pelo menos, um factor de autenticação e são tomadas as medidas razoáveis para verificar que são utilizados sob o controlo da pessoa a que pertence, Regulamento de execução (UE) 2015/1502

- Substancial

  Neste nível, a entidade verifica que a pessoa tem em sua posse elementos de prova de identidade genuínos, no processo de registo é apresentado um documento de identidade. Estes meios de identificação electrónica utilizam, pelo menos, dois factores de autenticação e são concebidos de modo a presumir que só são utilizados sob o controlo da pessoa a que pertence, Regulamento de execução (UE) 2015/1502.

- Elevado

  Neste nível, a prova de identidade é feita de forma idêntica ao nível substancial, no entanto, elementos de identificação com fotografia ou dados biométricos são

> controlados para verificar se estes são válidos de acordo com uma fonte qualificada, e quando pessoa não possui tais elementos de identificação a entidade obtém-nos com os mesmos procedimentos aplicados a nível nacional. Estes meios de identificação electrónica têm as mesmas características das de nível substancial, protegendo ainda contra a duplicação, manipulação e ataques, e são concebidos para a pessoa a quem pertence proteger eficazmente contra a utilização por terceiros, Regulamento de execução (UE) 2015/1502.

Em qualquer um dos níveis a prova e verificação de identidade não é necessária quando já existem meios de identificação electrónica de nível igual ao requerido.

O Regulamento de execução (UE) 2015/1502 define as especificações mínimas e os procedimentos aplicáveis para a atribuição dos níveis de garantia supra referidos.

### 3.2.2 *Decreto-Lei nº 12/2021*

Apesar do Regulamento eIDAS ser obrigatório, é da responsabilidade dos Estados-Membros assegurar a sua execução. Nesse sentido, foi publicado o Decreto-Lei nº12/2021 onde são designadas as autoridades portuguesas que realizam as actividades de supervisão previstas no Regulamento e consolida-se "a legislação existente tanto sobre a validade, eficácia e valor probatório dos documentos electrónicos, como sobre o Sistema de Certificação Electrónica do Estado - Infraestrutura de Chave Pública", Decreto-Lei nº12/2021.

No artigo 13º do Decreto-Lei nº12/2021 são estabelecidos os deveres do prestador qualificado de serviços de confiança, em particular, o prestador qualificado de serviços deve adoptar medidas que mantenham a integridade e autenticidade dos dados, e quando é este que gere os dados de criação de assinaturas deve garantir a sua confidencialidade durante o processo de criação. Para além disso, o prestador deve também manter os documentos e registos relativos à prestação destes serviços durante sete anos após o fim de validade do respectivo certificado.

### 3.2.3 *Standards do ETSI*

O ETSI define *standards* na área de tecnologias de informação e comunicação. Nesta dissertação abordamos os *standards* produzidos pelo ETSI relacionados com os serviços de confiança no âmbito do Regulamento eIDAS.

Neste sentido, esta dissertação foca-se em quatro *standards*:

- ETSI EN 319 401 (*"Electronic Signatures and Infrastructures (ESI); General policy requirements for Trust Service Providers"*)

- ETSI EN 319 411-1 (*"Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements"*)
- ETSI EN 319 411-2 (*"Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates"*)
- ETSI EN 319 421 (*"Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps "*)

*Serviços de Certificação*

O ETSI EN 319 411-1 define os serviços de certificação que suportam a emissão de certificados.

Na figura 25 observa-se a divisão dos serviços e a forma como se relacionam.

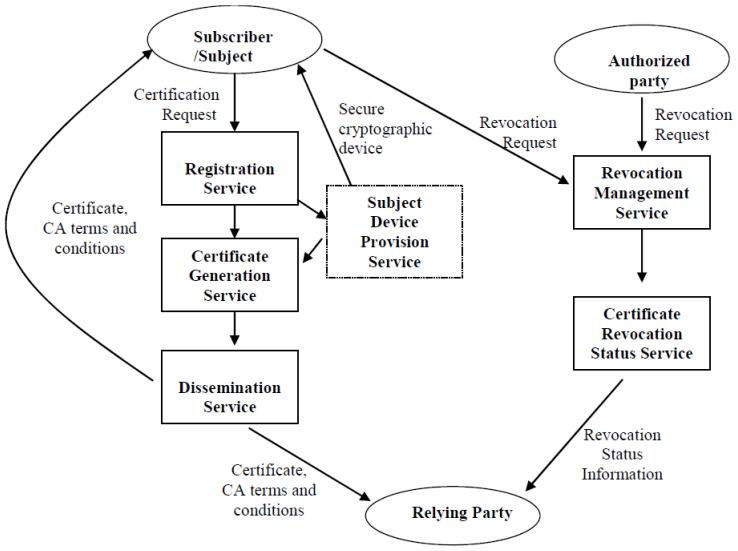



Figura 25: Serviços de certificação ( ETSI EN 319 411-1

- Serviço de registo

  Verifica a identidade e atributos do subscritor e comunica ao serviço de geração de certificado o resultado.

- Serviço de geração de certificado

  Cria e assina certificados com base na informação verificada pelo serviço de registo. Pode incluir geração de pares de chaves.

- Serviço de disseminação

Disponibiliza os certificados aos subscritores. Partilha os termos e condições e outras políticas e práticas relevantes.

- Serviço de gestão de revogação

  Processa pedidos de revogação e determina as acções a tomar.

- Serviço de estado de revogação

  Disponibiliza a informação do estado de revogação dos certificados às partes interessadas.

- Serviço de provisão de dispositivo ao sujeito

  Prepara e disponibiliza os dispositivos criptográficos seguros.

*Declaração de Práticas do Serviço de Confiança*

O prestador qualificado de serviços de confiança deve manter actualizada e sempre disponível uma declaração de práticas onde identifica como cumpre os requisitos a que se propõe. Este documento também deve identificar as obrigações de organizações externas. É também importante que contenha as medidas a tomar no caso de cessação de actividades.

Os ETSI EN 319 411-1 e ETSI EN 319 411-2 estabelecem uma Declaração de Práticas de Certificação, aplicável a serviços de certificação, definida no RFC 3647 como um documento que "estabelece práticas relacionadas com os serviços do ciclo de vida"(RFC 3647) dos certificados.

No caso da Entidade de Validação Cronológica, para além do que é definido no ETSI EN 319 401, a declaração de práticas deve, também, indicar informação específica relativa ao serviço de validação cronológica. O ETSI EN 319 421 fornece um modelo para o documento de divulgação de princípios da Entidade de Validação Cronológica.

*Termos e Condições*

O prestador qualificado de serviços de confiança deve disponibilizar aos seus utilizadores os termos e condições do serviço. Este documento deve conter toda a informação sobre a política do serviço aplicada, limitações de uso, informação para as partes de confiança, obrigações dos subscritores, limitações de responsabilidade, informações de contacto entre outros.

O ETSI EN 319 411-1 e o ETSI EN 319 411-2 definem requisitos adicionais para serviços de certificação e o ETSI EN 319 411-1 providencia, no anexo A, um modelo que pode ser utilizado para o documento de termos e condições.

*Política de Segurança de Informação*

O ETSI EN 319 401 define o que a política de segurança da informação deve abordar.

A política de segurança da informação é um documento de alto nível, isto é, apenas define princípios gerais. Este documento estabelece a abordagem da organização em relação à segurança da informação. Isto inclui controlos de segurança e procedimentos operacionais que devem ser cumpridos pela organização, assim como legislação aplicável.

Infra, abordaremos com mais detalhe este assunto, em especial o proposto pelo ISO/IEC 27002:2013 (E) no que toca à política de segurança de informação.

*Política de Certificados*

A política de certificados define as regras pelas quais a EC se rege. Este deve ser um documento de alto nível, definido independentemente de detalhes da operação da EC.

O prestador de serviço de confiança que emita certificados tem de ter uma política de certificados de acordo com o ETSI EN 319 411-1, no caso de emitir certificados qualificados deve também seguir o ETSI EN 319 411-2.

*Gestão de incidentes*

A gestão de incidentes, de acordo com o ETSI EN 319 401, é importante para garantir que as consequências de incidentes são minimizadas.

A gestão de incidentes deve incluir a monitorização dos sistemas, a nomeação de papéis de confiança no que toca à resposta a incidentes, procedimentos de notificação sempre que justificável (isto inclui a notificação em caso de falha de segurança ou perda de integridade que afectem o serviço ou dados pessoais no prazo de 24 horas).

A gestão de incidentes também deve incluir a resolução de vulnerabilidades, sendo que esta deve ser feita no prazo máximo de 48 horas após a sua identificação.

*Gestão de recursos humanos e controlo de acessos*

O ETSI EN 319 401 define os seguintes papéis de confiança:

- Administrador de segurança
- Administrador de sistema
- Operador de sistema
- Auditor de sistema

Adicionalmente, para o prestador qualificado de serviços de confiança que emite certificados, existem, ainda, os papéis de operador de registo e operador de revogação.

Deve ser definida uma política de controlo de acessos, tendo em conta que certas operações requerem controlo duplo (como a emissão de certificados pela Entidade de Certificação Raíz) e que deve ser sempre seguido o princípio do mínimo de permissões necessárias.

Para garantir a segurança do serviço é importante existir segregação de papéis, em particular, o papel de administrador de segurança e papéis relacionados com a operação do sistema.

*Continuidade de negócio*

Um requisito importante destes *standards* é a necessidade de existir um plano de continuidade de negócio para activar em caso de desastre. O ETSI EN 319 411-1 determina ainda que o plano de continuidade de negócio deve conter a informação sobre os procedimentos a seguir em caso de comprometimento da chave privada da EC.

*Cessação de actividade*

O prestador qualificado de serviços de confiança deve ter um plano de acção em caso de cessação de actividade. Este plano, de acordo com o ETSI EN 319 401, deve ter informação sobre a transferência das obrigações do prestador qualificado de serviços de confiança para outra organização e sobre a notificação das entidades afectadas.

*Gestão de Risco*

O prestador qualificado de serviços de confiança deve executar uma análise do risco para identificar, analisar e avaliar os riscos e deve seleccionar medidas de tratamento de riscos, sendo que estas devem ser proporcionais ao nível de risco. Esta análise, de acordo com o ETSI EN 319 401, deve ser revista regularmente e deve ser aprovada pela gestão do prestador qualificado de serviços de confiança, que para além disso, deve também aceitar o risco residual identificado.

Infra será abordado o ISO 31000:2018 (E) que contém mais informação de como deve ser conduzida a gestão de risco na organização.

*Arquivo de evidências*

Os registos arquivados devem ser mantidos durante um período de tempo adequado, mesmo depois da cessação de actividades e deve ser mantida a confidencialidade e integridade desses registos. Adicionalmente, deve existir uma fonte de tempo precisa para certos eventos e esta deve ser sincronizada com a UTC pelo menos uma vez por dia.

A informação a registar, de acordo com o ETSI EN 319 401, inclui informação emitida e recebida pelo prestador qualificado de serviços de confiança, qualquer evento de segurança e qualquer evento relacionado com o registo, disseminação, geração, gestão de revogação,

preparação de dispositivo, ciclo de vida de chaves e ciclo de vida de certificados. A forma de aceder a esta informação deve ser documentada.

Adicionalmente, no caso do serviço de validação cronológica, devem ser registados eventos de sincronização de relógio e eventos de perda de sincronização.

*Backups*

O prestador qualificado de serviços de confiança deve efectuar cópias de segurança,regularmente, de informação e *software* essencial. Estas devem ser mantidas, preferencialmente, num local remoto, conforme ETSI EN 319 411-1.

Os planos de *backup* devem estar de acordo com as necessidades do plano de continuidade de negócio.

# 4

# ABORDAGEM À GESTÃO DE SEGURANÇA DA INFORMAÇÃO

A gestão de segurança da informação para sistemas de confiança seguros obriga a um conhecimento extenso dos *standards* apresentados nas secções 2.1 e 2.2. Em consequência, a sua implementação não é muito comum nas *Pequenas e Médias Empresas (PMEs)* (especialmente, nas que têm poucos recursos, como é o caso das PMEs portuguesas). Este capítulo tem como objectivo ser o ponto de partida para PMEs que pretendem desenvolver e disponibilizar um sistema de confiança seguro, e efectuar a sua gestão de segurança da informação. Nesse sentido, são apresentadas as actividades mais importantes e referenciados os *standards* utilizados em cada uma, diminuindo-se, na medida do possível, a complexidade inerente aos vários *standards*, e possibilitando uma maior adopção dos mesmos pelas PMEs.

A abordagem capta actividades de ambos os *standards* analisados nas secções 2.1 e 2.2. Ao longo desta secção estes documentos também serão comparados.

O objectivo do NIST Special Publication 800-160 é o desenvolvimento e operação de um sistema de confiança seguro, enquanto que o objectivo do ISO/IEC 27001:2013 (E) é a implementação e manutenção de um sistema de gestão de segurança da informação *Information Security Management System (ISMS)*. É importante referir que o NIST Special Publication 800-160 se centra na segurança do sistema enquanto que o ISO/IEC 27001:2013 (E) aborda a segurança da informação de uma organização.

O ISMS definido pelo ISO/IEC 27001:2013 (E) é desenvolvido para uma organização e, consequentemente, pode-se aplicar a todos os projectos da mesma, sendo a segurança de informação necessariamente integrada ao longo do desenvolvimento e gestão do projecto. O objectivo principal do NIST Special Publication 800-160 é obter um sistema de confiança seguro através da aplicação de princípios de engenharia de segurança de sistemas ao longo do desenvolvimento de um sistema.

Como o ISMS se aplica a toda a organização, um dos controlos definidos no ISO/IEC 27002:2013 (E) é a integração da segurança da informação no desenvolvimento de sistemas. Isto é um ponto em comum com o *standard* do NIST Special Publication 800-160, no entanto os controlos propostos pelo ISO/IEC 27002:2013 (E) são mais genéricos.

Sendo que os *standards* abordados nesta dissertação têm âmbitos distintos podem ser utilizados em conjunto como forma de se complementarem sendo o âmbito de aplicação da família de *standards* ISO/IEC 27000 direccionada à organização e o NIST a sistemas.

## 4.1 Actividades para o desenvolvimento de um sistema de confiança seguro e para a criação de um ISMS

Esta secção divide-se nas seguintes fases, que correspondem a uma adaptação das fases de desenvolvimento e disponibilização de *software* (Murch (2012)):

- Análise
- Implementação
- Avaliação
- Operação e manutenção

O objectivo é adicionar a estas fases as actividades necessárias para disponibilizar um sistema de confiança seguro e efectuar a sua gestão de segurança da informação.

Em todas as actividades é necessário que a organização faça uma avaliação custo-benefício e as decisões tomadas devem ser proporcionais à segurança necessária.

### 4.1.1 *Análise*

A fase de análise é a fase em que são definidos e analisados os requisitos e os objectivos de segurança do sistema.

A segurança do sistema e a segurança da informação dependem directamente do contexto em que o sistema ou organização se insere.

Neste contexto, definem-se, desde logo, o âmbito, os objectivos e os requisitos de segurança.

No NIST Special Publication 800-160, os requisitos e objectivos de segurança funcionam também como uma base para a tomada de decisões do que representa uma segurança adequada, sendo necessário uma avaliação que tenha em conta o que é relevante para atingir um sistema de confiança seguro, sem que se comprometam, de forma desnecessária, outros aspectos importantes como *performance*, disponibilidade, custos financeiros, entre outros.

O desenvolvimento de um ISMS é feito de acordo com objectivos e requisitos de segurança da informação da organização.

Neste contexto é definida a política de segurança (tal como descrita na secção 2.1.5) ou política de segurança da informação (tal como descrita na secção 2.2.1). Este é um documento

essencial, que serve como base para toda a segurança do sistema ou segurança da informação de uma organização.

*Análise de risco*

Conhecer, controlar e tratar riscos é essencial para a segurança de um sistema ou organização.

O desenvolvimento de um ISMS tem de estar de acordo com riscos e oportunidades identificados numa análise de risco. Esta análise é feita antes da implementação do ISMS é repetida periodicamente. Com os resultados da análise a organização prepara o ISMS para responder aos riscos e oportunidades identificados.

Para uma análise e avaliação de risco eficaz e coerente a organização estabelece a gestão de risco. A gestão de risco é abordada em detalhe na secção 2.2.2.

No NIST Special Publication 800-160, os riscos associados ao sistema são um factor importante a ter em conta ao longo do seu desenvolvimento. Nos processos definidos, destaca-se o processo técnico de gestão do risco abordado na secção 2.1.2.

*Definição de objectivos*

Os objectivos de segurança são estabelecidos tendo em consideração as seguintes vertentes:

- Confidencialidade;
- Integridade;
- Disponibilidade;
- Autenticidade;
- Não-repúdio;

Juntamente com os objectivos são definidas métricas que auxiliem a posterior avaliação de cumprimento desses objectivos.

Tanto o ISO/IEC 27001:2013 (E) como o NIST Special Publication 800-160 denotam a importância da definição de objectivos.

No NIST Special Publication 800-160, a aplicação da engenharia de segurança de sistemas pretende garantir que os objectivos de segurança das partes interessadas são cumpridos. Por conseguinte, é necessário definir quais são esses objectivos.

Segundo o NIST Special Publication 800-160, estes objectivos definem o âmbito e o que é considerado como adequadamente seguro, isto é, qual é o nível de segurança necessário que melhor representa uma boa relação de custo-benefício. Juntamente com estes objectivos são definidas métricas de sucesso que influenciam o desenvolvimento dos requisitos de segurança e das afirmações de garantia.

No ISO/IEC 27002:2013 (E), os objectivos de segurança da informação são definidos ao nível da organização e devem ser integrados nos objectivos dos projectos desenvolvidos pela organização. Estes objectivos serão cumpridos eficazmente com a implementação de um sistema de gestão (i.e. ISMS).

Os objectivos não são estáticos e podem sofrer alterações ao longo do ciclo de vida do sistema.

*Identificação de requisitos*

No contexto de identificação de requisitos são tidas em conta as preocupações de segurança das partes interessadas e as propriedades de segurança necessárias. Os requisitos não são estáticos ao longo do tempo sendo necessário revê-los e possivelmente alterá-los periodicamente.

Os requisitos têm em consideração, por exemplo:

- O âmbito da segurança da informação;
- Requisitos das partes interessadas;
- Os objectivos de segurança;
- Questões de *performance* do sistema;
- Imposições legais, contratuais ou regulamentares;
- Recursos e o seu valor;
- Custos financeiros;
- Limites de prazos;
- Outras questões que possam ser relevantes;

Para o NIST Special Publication 800-160, a identificação de requisitos de segurança encontra-se presente em todos os processos do ciclo de vida do sistema. Nos processos técnicos, abordados na secção 2.1.2, destacam-se o processo de definição de requisitos e necessidades das partes interessadas e o processo de definição de requisitos do sistema, que descrevem actividades direccionadas à identificação de requisitos de segurança e a transformação desses requisitos em requisitos do sistema. Destaca-se também a secção 2.1.5, que descreve de forma detalhada a actividade de levantamento de requisitos de segurança.

Estes requisitos são analisados e transformados em requisitos do *design* do sistema, como parte do contexto de solução da *framework* proposta pelo NIST Special Publication 800-160, abordada em detalhe na secção 2.1.1.

Para o ISO/IEC 27001:2013 (E) os requisitos de segurança são uma das bases para a implementação do ISMS. Estes requisitos advêm da análise do risco e dos recursos de informação. Os requisitos de segurança não são estáticos e a análise de risco efectuada periodicamente pode resultar em alterações aos mesmos.

*Papéis e responsabilidades*

Os papéis e responsabilidades definidos no ISO/IEC 27002:2013 (E) e no NIST Special Publication 800-160 são distintos.

No NIST Special Publication 800-160, é definido o papel de engenheiro de segurança de sistemas que participa numa equipa de engenheiros, descrito em detalhe na secção 2.1.3. Este papel é o principal responsável pela segurança do sistema.

Já o ISO/IEC 27002:2013 (E) requer que a organização defina vários papéis com diferentes responsabilidades para a segurança da informação. Pode ser definido um responsável principal pela segurança da informação, no entanto, é importante definir papéis com responsabilidades mais específicas para a segurança da informação (e.g. *resource owner*, *process owner*, gestor de risco, gestor de incidentes, entre outros). Aquando da definição de papéis e responsabilidades é necessário que a organização tome precauções no que toca à segregação de papéis para diminuir a possibilidade de abuso dos recursos da organização e o risco que daí advém, no caso de não ser possível segregar papéis (e.g. organização pequena com poucos recursos) é necessário implementar mecanismos que facilitem a monitorização de actividades. Apesar de certos papéis terem responsabilidades acrescidas no que toca à segurança da informação, todos os recursos humanos têm a responsabilidade na segurança da informação da organização.

*Políticas*

As políticas definem as bases para a segurança da organização e sistema. São os primeiros documentos a definir e todos os restantes regem-se por estes.

Enquanto o NIST Special Publication 800-160 define uma política de segurança, o ISO/IEC 27002:2013 (E) define uma política de segurança da informação. No entanto, ambos referem a importância deste documento, essencial a qualquer sistema ou organização.

Para o NIST Special Publication 800-160, a política de segurança é expressa em termos de confidencialidade, integridade e disponibilidade. A política define um conjunto de regras que determinam o comportamento necessário para conseguir a segurança desejada. A política de segurança é determinada a partir dos objectivos. O NIST Special Publication 800-160 não especifica o conteúdo da política deixando a cargo do engenheiro de segurança de sistemas as decisões das regras a definir na política. A política de segurança é abordada em detalhe na secção 2.1.5.

O ISO/IEC 27002:2013 (E) detalha o conteúdo da política de segurança da informação. Segundo este, a política inclui os objectivos e princípios para a segurança da informação, o compromisso em satisfazer os requisitos de segurança e em melhorar o sistema de gestão de segurança da informação e determinar responsabilidades na gestão de segurança da informação. A política de segurança da informação, geralmente, é um documento de alto nível que é suportado por políticas específicas. No entanto, para organizações menos complexas, pode ser indicada a definição de uma política de segurança da informação que incorpora políticas específicas. A política de segurança da informação é abordada com mais detalhe na secção 2.2.1.

Em ambos os casos a definição da política está directamente ligada aos objectivos de segurança e aos requisitos identificados, sendo dependente destes.

### 4.1.2 *Implementação*

Nesta fase são implementados os controlos que permitem manter a segurança. Estes controlos têm em conta os requisitos, os objectivos e a análise de risco efectuada.

Na implementação do sistema de gestão de segurança de informação definido no ISO/IEC 27000:2018 (en) são implementados controlos que permitem as garantias necessárias da segurança da informação. Os controlos implementados podem ser seleccionados a partir do ISO/IEC 27002:2013 (E) ou a partir de qualquer conjunto de controlos que melhor se aplique à organização. Contudo, é possível adaptar os controlos definidos no ISO/IEC 27002:2013 (E) a qualquer organização de acordo com a sua complexidade.

Os controlos definidos no ISO 27002 incluem, entre outros:

- Perímetros de segurança física (e.g. barreiras físicas, mecanismos de controlo de acessos físicos ao local, alarmes, entre outros);
- Controlos de acessos;
- Controlos criptográficos;
- Controlos que previnem e detectam *malware*;
- Mecanismos de monitorização;
- Processos que regem actividades da organização;

Todos os controlos implementados devem ser proporcionais aos objectivos de segurança da informação e à complexidade da organização, sendo necessário efectuar uma avaliação da relação custo-benefício da implementação dos controlos. A organização tem a responsabilidade de providenciar os recursos necessários para implementar o ISMS.

Neste contexto, destacam-se os seguintes processos técnicos 2.1.2 definidos pelo NIST:

- Processo de definição de arquitectura
- Processo de definição de *design*;
- Processo de implementação;
- Processo de integração;
- Processo de transição.

Estes processos têm como objectivo fazer com que o sistema final cumpra todos os requisitos de segurança definidos e que os resultados destes sirvam como prova de que o nível confiança pretendido é atingido.

No contexto de implementação salienta-se que o NIST Special Publication 800-160, está directamente relacionado com o desenvolvimento de um sistema e foca-se na integração da segurança nos processos envolvidos na implementação desse sistema, enquanto a família de *standards* ISO/IEC 27000:2018 (en) foca-se na implementação de um sistema de gestão de segurança da informação em que a organização implementa mecanismos de controlo para prevenir e detectar qualquer tipo de falha na segurança da informação.

Pode-se concluir que enquanto a abordagem do NIST Special Publication 800-160 deve ser sempre implementada em conjunto com a implementação do sistema, o ISMS pode ser implementado de forma independente e em qualquer fase de maturidade da organização. Ainda assim, a segurança da informação deve ser integrada no desenvolvimento de projectos e sistemas dentro da organização.

### 4.1.3 *Avaliação*

A fase de avaliação é a fase em que os controlos implementados são testados.

Numa organização ou sistema em que a segurança seja um factor importante é necessário conseguir provar que essa segurança existe verdadeiramente.

No contexto da solução da *framework* da engenharia de segurança de sistemas, abordada na secção 2.1.1, definida no NIST Special Publication 800-160, são obtidas as evidências de segurança do sistemas através de métodos de verificação e validação. No contexto da confiança é desenvolvido o caso que demonstra que o sistema é seguro e apresenta o nível de confiança desejado.

O NIST Special Publication 800-160, define, dentro dos processos técnicos, abordados na secção 2.1.2, o processo de verificação e o processo de validação que têm como objectivo provar que o sistema e elementos do sistema cumprem os requisitos de segurança. Do processo de verificação de segurança resultam provas que demonstram as características de segurança pretendidas e também podem ser identificadas anomalias que necessitam de

ser corrigidas. O processo de validação pretende provar que o sistema atinge o nível de confiança necessário e cumpre com os objectivos e requisitos.

No ISMS, definido no ISO/IEC 27001:2013 (E), a avaliação da segurança da informação é feita periodicamente, através de auditorias internas e revisões periódicas. A avaliação de segurança da informação aplica-se a todo o ISMS da organização e pode identificar oportunidades de melhoria ou necessidade de acções correctivas nos controlos, políticas, objectivos e procedimentos da organização.

### 4.1.4 *Operação e manutenção*

Nesta fase são desenvolvidas as actividades de segurança correntes do sistema/organização.

A segurança é importante na fase de operação e manutenção, devendo ser garantido que o sistema ou organização se mantém sempre num estado seguro.

No ISMS, é importante a definição de certos procedimentos que guiam a execução de determinadas actividades na organização. Algumas actividades importantes para as quais é necessário definir procedimentos incluem, entre outros:

- Gestão de incidentes, em particular, a detecção e monitorização de incidentes, a comunicação de incidentes, o manuseamento de evidências e a resposta a incidentes;
- *Backup*;
- Recuperação de sistemas;
- Gestão de alterações, em particular, comunicação, aceitação e implementação de alterações;

A organização tem de ter em conta a manutenção da segurança da informação mesmo em situações adversas. Assim, a organização avalia quais são os requisitos de segurança da informação numa situação adversa, implementa um plano de continuidade de negócio e dispõe dos recursos necessários para cumprir esses requisitos. Dependendo da criticidade das operações da organização e da sensibilidade da sua informação, pode não ser necessário garantir a continuidade de negócio. A continuidade de negócio é alvo de uma avaliação custo-benefício bem ponderada. Na secção 2.2.1 este assunto é abordado com mais detalhe.

A formação dos recursos humanos é essencial para manter a segurança da informação e são efectuadas acções de formação periódicas.

A operação e manutenção de um sistema de confiança seguro é preparada de acordo com as características de segurança desejadas para garantir que quando o sistema se encontrar em operação seja seguro. Quando o sistema se encontrar em operação é necessário monitorizar aspectos de segurança e disponibilizar recursos para a manutenção da segurança do sistema. Os processos definidos no NIST Special Publication 800-160, que têm especial destaque

neste contexto, são os processos técnicos de operação, manutenção, gestão de configurações e gestão de informação. Estes processos são abordados em detalhe na secção 2.1.2.

# 5

# GESTÃO DE SEGURANÇA DE INFORMAÇÃO DA INFRAESTRUTURA DE CHAVE PÚBLICA DO CARTÃO DE CIDADÃO

Esta dissertação foi desenvolvida com o apoio da empresa *Devise Futures* e inserida num projecto de reestruturação e actualização da gestão de segurança de informação da Infraestrutura de Chave Pública do Cartão de Cidadão.

O projecto foi acompanhado pela equipa da *Imprensa Nacional-Casa da Moeda (INCM)* (que produz o Cartão de Cidadão) responsável pela segurança da informação do Cartão de Cidadão, em particular, pelo *Chief Information Security Officer (CISO)* e pelo *Data Protection Officer (DPO)* do Cartão de Cidadão.

Esta secção centra-se no desenvolvimento desse projecto e a sua relação com os tópicos dos capítulos anteriores.

Estando a Infraestrutura de Chave Pública do Cartão de Cidadão implementada *a priori*, este projecto concentrar-se-á no desenvolvimento do ISMS.

Na fase inicial, foi feita uma análise da documentação existente e de não conformidades previamente identificadas. Esta actividade encontra-se inserida na fase de análise descrita na secção 4.1.1.

Esta secção foi dividida de acordo com os vários temas importantes para a construção de um ISMS.

Todos os temas começaram com um levantamento de requisitos da regulamentação aplicável (nomeadamente ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2 que podem ser encontrados no anexo A) e controlos indicados no ISO/IEC 27002:2013 (E) (referente às actividades descritas na secção 4.1.1), estes não como factor obrigatório mas sim como recomendação, visto a Infraestrutura de Chave Pública não ter acreditação ISO/IEC 27001:2013 (E). Seguidamente, de acordo com a informação levantada da regulamentação e *standards* foi avaliada a documentação e controlos existentes e identificadas oportunidades de melhoria.

Foram efectuadas reuniões regulares com a equipa responsável pela segurança da informação do Cartão de Cidadão onde foi dado o seu parecer em relação aos documentos elaborados ao longo do projecto.

Os documentos resultantes deste projecto serão adoptados em breve pelo Cartão de Cidadão.

*Política de Segurança de Informação*

Inicialmente, foi notado que não existia uma Política de Segurança da Informação, sendo este um documento essencial que rege a gestão de segurança da informação da organização. Este documento insere-se nas actividades da fase de análise, descrita na secção 4.1.1.

Para a elaboração do documento, primeiro foram avaliados os requisitos obrigatórios para conformidade com a regulamentação aplicável, isto é, ETSI EN 319 401, Regulamento eIDAS, RGPD e legislação nacional e, de seguida, foram analisados os controlos indicados no ISO/IEC 27002:2013 (E). Com estes requisitos e recomendações foi elaborada uma lista para facilitar a posterior análise de conformidade.

No apêndice A.1 podemos consultar os requisitos da regulamentação aplicável à política de segurança da informação.

No caso da ICP do Cartão de Cidadão foi estipulado o prazo de 2 anos para revisão de documentos.

Esta política está directamente relacionada com as secções 3.2.3, 2.2.1 e 4.1.1.

A política de segurança de informação foi documentada de acordo com os processos e controlos já implementados na organização. Esta define os princípios de segurança de informação pelos quais a ICP do Cartão de Cidadão se rege. Estes princípios incluem:

- A classificação de informação adequada e de acordo com os requisitos legais, regulamentares e contratuais relevantes;
- Responsabilidade dos recursos humanos de assegurar a classificação da informação, manusear a informação de acordo com essa classificação e respeitar os requisitos legais e regulamentares, políticas, procedimentos e regras;
- O acesso a informação é baseado em privilégios mínimos e necessidade de saber. A informação deve estar simultaneamente segura e disponível para aqueles que lhe podem aceder de acordo com o nível de classificação;
- A informação é protegida contra acessos não autorizados;
- As violações da política de segurança são reportadas e existem procedimentos para acções disciplinares, caso necessário;
- A política de segurança de informação e os documentos relacionados são revistos regularmente (de dois em dois anos);
- São efectuadas avaliações regulares por forma a confirmar que a configuração dos sistemas da ICP do Cartão de Cidadão não viola a política de segurança de informação;

- São efectuadas, com regularidade, auditorias internas e testes de vulnerabilidades para verificar conformidade;

Os princípios acima elencados visão garantir a confidencialidade, integridade, privacidade, autenticidade e não repúdio da informação.

O âmbito de protecção da política de segurança de informação engloba as componentes definidas na secção 3.2.3.

Os tópicos abrangidos pela política incluem:

- Compromisso da gestão da ICP com os princípios para a gestão de segurança de informação;
- Comunicação de alterações;
- Relação com fornecedores;
- Classificação de informação;
- Acções de consciencialização e disciplinares;
- Revisão de políticas;
- Comunicação de incidentes;
- Legislação aplicável.

*Gestão de incidentes*

A gestão de incidentes insere-se na fase de operação e manutenção descrita na secção 4.1.4.

Este tema foi iniciado através da elaboração de uma lista com os requisitos da regulamentação aplicável (regulamentos do ETSI) e recomendações ISO/IEC 27002:2013 (E), ISO/IEC 27035-1:2020 (E), ISO/IEC 27035-2:2020 (E) e ISO/IEC 27035-3:2020 (E).

Os requisitos da regulamentação aplicável podem ser consultados em anexo no apêndice A.2.

As recomendações ISO/IEC 27002:2013 (E), abordado na secção 2.2.1, incluem:

- Definir responsabilidades que garantam a gestão de incidentes;
- Definir procedimentos para a gestão de incidentes;
- Utilizar conhecimento obtido a partir da análise e resolução de incidentes;
- Colectar evidências.

Além disso, é importante as recomendações ISO/IEC 27035-1:2020 (E), ISO/IEC 27035-2:2020 (E) e ISO/IEC 27035-3:2020 (E), abordados na secção 2.2.3.

Como a ICP do Cartão de Cidadão já tinha em prática processos, metodologias e planos para a gestão de incidentes, essa documentação foi analisada de acordo com os requisitos a fim de confirmar o que era praticado e onde existia espaço para melhoria.

A gestão de eventos de segurança é baseada nas várias fases definidas no ISO/IEC 27035-1:2020 (E), 2.2.3. Concretamente existem 4 fases: detecção e comunicação, avaliação e decisão, resposta e lições aprendidas. A figura 26 resume o processo de gestão de incidentes.

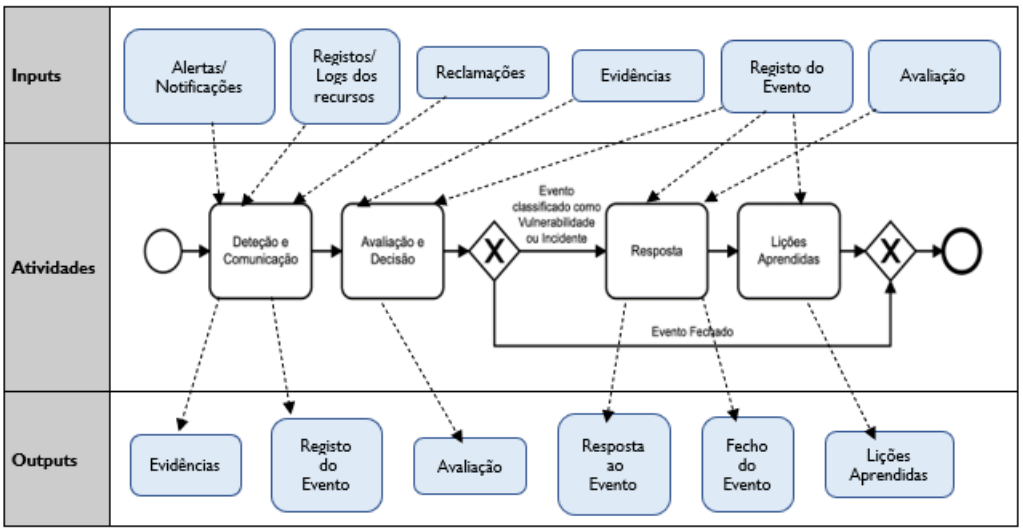



Figura 26: Diagrama do processo de gestão de incidentes

Após a detecção de um evento é necessário classificá-lo. Este pode ser classificado como incidente, vulnerabilidade, fraqueza de segurança de informação (similar a vulnerabilidade) ou evento (quando não pode ser classificado em nenhuma das categorias anteriores).

Quando um evento é classificado como incidente são recolhidas as evidências do mesmo de acordo com o seguinte fluxograma da figura 27.

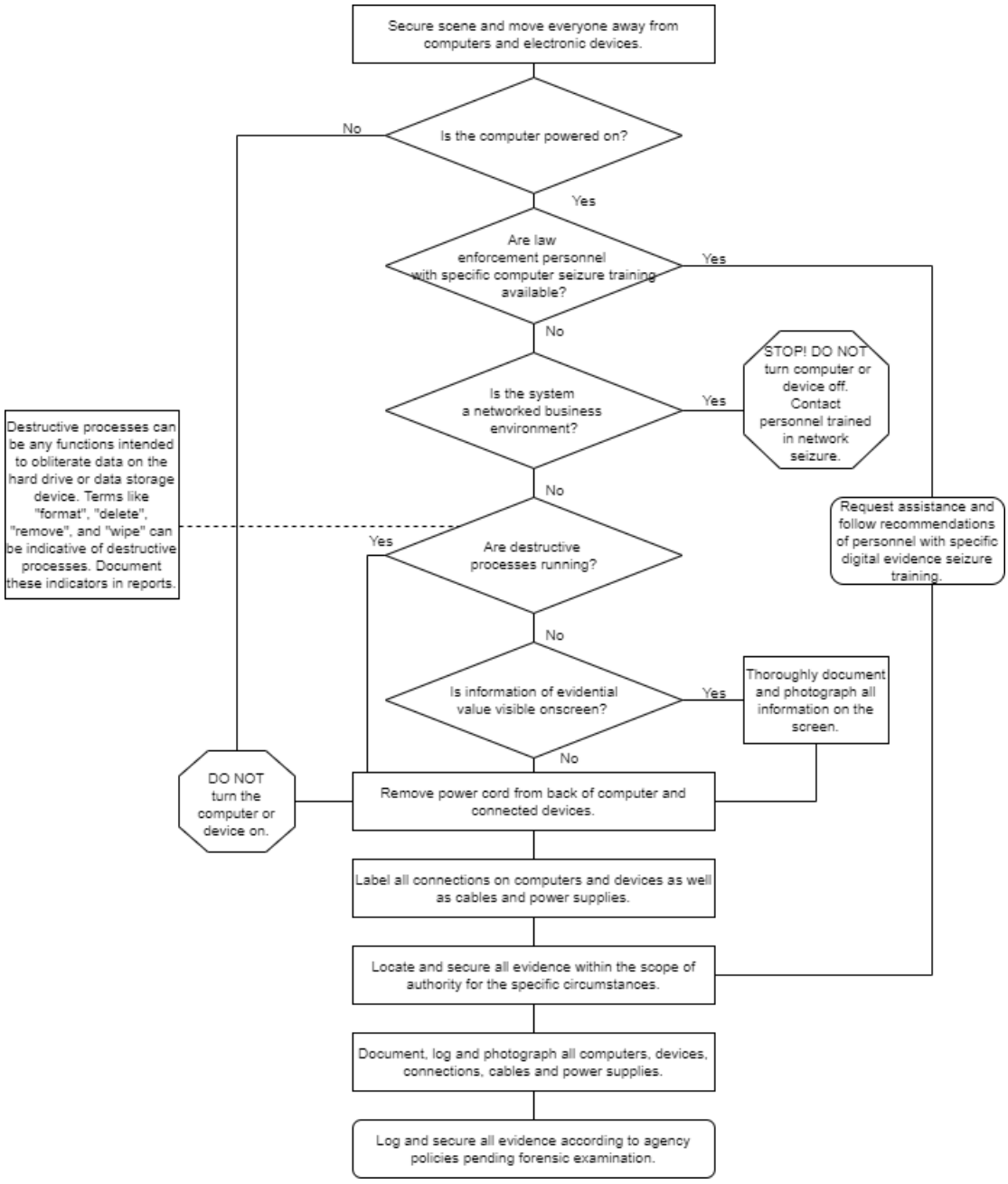



Figura 27: Fluxograma de recolha de evidência digital (baseada em figura do Electronic Crime Scene Investigation: A Guide for First Responders)

A classificação de incidentes, responsabilidade do gestor de incidentes, é obtida através categoria e prioridade do mesmo.

Para a categorização do incidente começa-se por identificar o serviço onde o mesmo ocorreu, de seguida defini-se a categoria, atributo amplo que identifica o principal recurso afectado, e subcategoria, já com especificidade e, por último, define-se o tipo de incidente, isto é, acção que despoletou o incidente.

A prioridade do incidente é dada de acordo com o impacto e urgência. O impacto está relacionado com as consequências que o incidente pode causar nos serviços/recursos e a urgência está relacionada com o tempo necessário para resolver o incidente. O impacto pode ser alto, médio ou baixo. É dado tendo em conta o impacto na reputação, na actividade/processo/serviço, custo financeiro, número de cidadãos e recursos humanos afectados. A urgência é dada tendo em conta o RTO (*recovery time objective*) (indica o intervalo de tempo para a recuperação do serviço após o desastre), os recursos afectados e critérios de priorização, esta pode ter um valor entre 1 (mais baixo) e 5 (mais alto). Para obter a classe de prioridade de acordo com o impacto e urgência segue-se a matriz da figura 28.

| Classe de Prioridade | | Impacto | | |
|---|---|---|---|---|
| | | A | M | B |
| Urgência | 5 | 0 | I | I |
| | 4 | I | I | I |
| | 3 | 2 | 2 | 3 |
| | 2 | 2 | 3 | 4 |
| | I | 3 | 4 | 5 |

Figura 28: Matriz de impacto-urgência

Para as vulnerabilidades identificadas estas são classificadas de acordo com: categoria (da mesma forma que os incidentes), severidade de acordo com o CVSS 2.2.3 e prioridade, que é calculada tendo em conta o impacto e a severidade. Na figura 29 podemos observar como é calculada a classe de prioridade.

| Classe de Prioridade | | Impacto | | | |
|---|---|---|---|---|---|
| | | A | M | B | N |
| Severidade | I | 0 | 0 | 0 | 0 |
| | 2 | I | I | I | 0 |
| | 3 | 2 | 2 | I | 0 |
| | 4 | 3 | 3 | 2 | 0 |
| | 5 | 4 | 4 | 4 | 0 |

Figura 29: Matriz de impacto-severidade

Na fase de resposta é avaliada a necessidade de efectuar notificações a entidades internas e externas e a necessidade de escalonamento da resposta. Os envolvidos na resposta ao incidente/vulnerabilidade registam todas as actividades desenvolvidas. A resposta é iniciada por uma equipa de resposta rápida, mas pode ser necessário escalar o incidente para equipas com competências diferentes.

O escalonamento de incidentes pode ser funcional ou hierárquico. O incidente começa por ser escalonado no sentido funcional e só depois no sentido hierárquico. O escalonamento

é efectuado de acordo com um RTO previamente estabelecido. Para o escalonamento de incidentes existem equipas para cada nível de escalonamento e uma sala de crise que é utilizada no último nível onde se reúne a equipa definida para responder ao incidente.

Sendo a monitorização muito importante para a detecção de eventos, foi definida uma política de registo de auditoria e monitorização. A monitorização é efectuada nos seguintes níveis: físico, infraestrutura, aplicacional e cerimónia. Os registos dos eventos podem ser automáticos ou manuais e devem conter informação sobre a sua data e hora, identidade da entidade responsável pelo evento, categoria/tipo do evento (LC - ciclo de vida do certificado; LTS - ciclo de vida do selo temporal/validação cronológica; BO - operações e verificações de *BackOffice*; Session - Sessão de administração ou operação) e descrição do evento.

*Gestão de Recursos Humanos*

A gestão de recursos humanos insere-se na fase de análise descrita na secção 4.1.1.

Foram analisados os requisitos da regulamentação ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, e, como recomendação, o ISO/IEC 27002:2013 (E). Consequentemente, foi elaborada uma lista que serviu como base para a elaboração dos documentos necessários.

Os requisitos da regulamentação aplicável podem ser consultados no apêndice A.3.

As recomendações ISO/IEC 27002:2013 (E), abordado na secção 2.2.1, incluem: a segregação de papéis, a verificação de antecedentes, um acordo contratual entre o empregador e os recursos humanos, planos de treino regulares, processos disciplinares, procedimentos para a cessação de funções de recursos humanos, entre outros.

A gestão de recursos humanos está relacionada com a identificação de papéis e responsabilidades abordada na secção 4.1.1.

A ICP do Cartão de Cidadão tinha documentos definidos destinados à gestão de recursos humanos que foram analisados de acordo com os requisitos. Esta análise permitiu identificar o que era necessário adicionar e alterar para melhorar a gestão de recursos humanos.

Foi elaborada a política para a nomeação e substituição dos recursos humanos e regras que identificam e caracterizam a organização dos recursos humanos.

Os recursos humanos foram organizados em grupos de trabalho que reflectem as funções de confiança da ICP do Cartão de Cidadão. Assim, os antigos grupos de trabalho, descritos na secção 3.1.8 foram transformados em 9 grupos que têm por base os papéis de confiança do ETSI EN 319 401, descritos na secção 3.2.3, e os requisitos CEN TS 419 261. Na figura 30 observa-se a relação que existe entre os novos grupos de trabalho e os antigos.

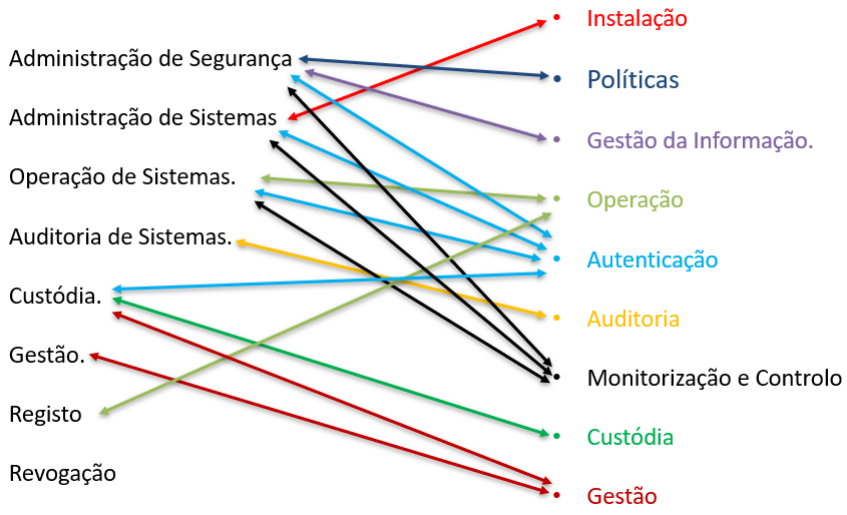



Figura 30: Relação entre novos grupos de trabalho e antigos grupos de trabalho

De seguida, descrevem-se as funções e responsabilidades dos novos grupos de trabalho:

- Grupo de trabalho de administração de sistemas

  A sua função é instalar, configurar e manter os sistemas informáticos. Este grupo é responsável por gerir o ambiente de produção, alterar a configuração de segurança da aplicação, entre outros. Os membros deste grupo de trabalho devem ter conhecimentos sólidos de informática, conhecimentos sólidos sobre normas de segurança de informação e competências de organização.

- Grupo de trabalho de operação de sistemas

  A sua função é operar diariamente os sistemas informáticos e tarefas de rotina essenciais. Este grupo é responsável por tarefas de monitorização, gerir o ambiente de operação, emitir e revogar/suspender certificados quando o processo não é automático.

- Grupo de trabalho de administração de segurança

  A sua função é gerir e implementar as regras, políticas e práticas de segurança. Este grupo é responsável por consolidar e analisar pontos de controlo de segurança, analisar e implementar a gestão de risco, garantir a melhoria contínua dos processos, gerir o ambiente de informação, entre outros. Os membros deste grupo de trabalho devem ter conhecimentos sólidos sobre infraestruturas de chave pública, conhecimentos avançados sobre o Regulamento eIDAS, conhecimentos sobre normas e *standards* aplicáveis, conhecimentos sólidos sobre normas de segurança da informação, entre outros. Um membro deste grupo de trabalho assume o papel de Gestor de Risco que é responsável por gerir o processo de gestão de risco e liderar este grupo nas actividades de gestão de risco.

- Grupo de trabalho de auditoria de sistemas;

  A sua função é efectuar auditoras internas a todas as acções relevantes e necessárias para assegurar a operacionalidade. Este grupo é responsável por auditar a execução de processos e cerimónias, registar todas as operações sensíveis, investigar suspeitas de fraudes procedimentais, verificar periodicamente a funcionalidade dos controlos de segurança, registar todos os procedimentos passivos de auditoria, validar que todos os recursos usados são seguros, gerir o ambiente de auditoria, entre outros. Os membros deste grupo de trabalho devem ter conhecimentos básicos sobre infraestruturas de chave pública, conhecimentos sólidos da documentação da ICP do Cartão de Cidadão e da sua documentação, conhecimentos sobre o Regulamento eIDAS, conhecimentos sólidos sobre normas e *standards* de segurança da informação e inerentes a entidades de certificação.

- Grupo de trabalho de custódia

  A sua função é gerir, guardar e disponibilizar artefactos sensíveis e artefactos físicos no ambiente de custódia. Este grupo de trabalho é responsável por gerir o ambiente de custódia, identificar e manter um inventário dos artefactos à sua guarda, registar levantamentos e devoluções dos artefactos, registar alterações dos artefactos e verificar periodicamente a integridade dos artefactos.

- Grupo de trabalho de gestão

  A sua função é gerir a ICP do Cartão de Cidadão. Este grupo de trabalho é responsável pela segurança da informação da ICP do Cartão de Cidadão, analisar e aprovar planos de tratamento de risco e riscos residuais, nomear os membros dos restantes grupos de trabalho, rever, analisar e aprovar políticas, garantir a disponibilização de recursos para a implementação de políticas propostas e aprovadas, gerir o ambiente de gestão, entre outros.

- Grupo de trabalho de registo

  A sua função é verificar a identidade e os atributos específicos do titular que efectua o pedido de certificado. Este grupo de trabalho é responsável por aprovar a emissão de certificados de titulares, gerir o ambiente de registo, entre outros. Os membros deste grupo de trabalho devem ter conhecimentos sólidos sobre legislação relevante, formação e conhecimento na validação de documentos de identificação, entre outros.

- Grupo de trabalho de revogação

  A sua função é operar a mudança no estado dos certificados de utilizador final. Este grupo é responsável por processar pedidos de alteração de estado dos certificados, distribuir o novo estado do certificado, aprovar a revogação de certificados de titulares e gerir o ambiente de revogação.

- Grupo de trabalho de personalização;

  A sua função é operar os equipamentos e ferramentas que colocam o par de chaves e certificados do titular no Cartão de Cidadão. Este grupo é responsável por instalar, configurar e manter os equipamentos e ferramentas de personalização, executar tarefas de monitorização dos sistemas utilizados na personalização e gerir o ambiente de personalização.

Cada grupo de trabalho tem um número mínimo de elementos que se pode observar na tabela da figura 31. Existe também segregação de papéis, na figura 32 observa-se a matriz de incompatibilidades para pertencer aos grupos de trabalho.

| **Grupo de Trabalho** | **Nº Mínimo de Elementos** |
|---|---|
| Administração de Sistemas | 2 |
| Operação de Sistemas | 2 |
| Administração de Segurança | 2 |
| Auditoria de Sistemas | 2 |
| Custódia | 2 |
| Gestão | 2 |
| Registo | 2 (por local de registo) |
| Revogação | 2 (por local de revogação) |
| Personalização | 2 |

Figura 31: Tabela número mínimo de elementos por grupo de trabalho

| | Administração de Sistemas | Operação de Sistemas | Administração de Segurança | Auditoria de Sistemas | Custódia | Gestão | Registo | Revogação | Personalização |
|---|---|---|---|---|---|---|---|---|---|
| Administração de Sistemas | | | X | X | X | X | X | X | X |
| Operação de Sistemas | | | X | X | X | X | | | |
| Administração de Segurança | X | X | | X | X | X | | | |
| Auditoria de Sistemas | X | X | X | | X | X | X | X | X |
| Custódia | X | X | X | X | | X | X | X | X |
| Gestão | X | X | X | X | X | | X | X | X |
| Registo | X | | | X | X | X | | | X |
| Revogação | X | | | X | X | X | | | |
| Personalização | X | | | X | X | X | X | | |

Figura 32: Tabela de segregação de papéis

Para além dos grupos de trabalho foram também definidos papéis com responsabilidades específicas, nomeadamente:

- *Risk owner*

  Responsável por gerir, monitorizar e controlar um risco identificado. Deve ser capaz de gerir o processo de tratamento do risco e ter o conhecimento, recursos e autoridade para tratar o risco.

- *Process owner*

  Um membro do Grupo de Trabalho responsável pelo processo que fica com a responsabilidade para criar, gerir, manter, supervisionar e melhorar o processo. As actividades desenvolvidas pelo *process owner* incluem: estabelecer e implementar métricas; garantir que o processo cumpre os objectivos; acompanhar as actividades dos processos; entre outros.

- *Resource owner*

  Responsável por gerir, monitorizar e controlar os recursos que lhe foram designados. As actividades desenvolvidas pelo *resource owner* incluem: participar na gestão de inventário; assegurar a adequada classificação e protecção dos recursos; definir as restrições de acesso dos recursos; assegurar que a correcta destruição ou eliminação de recursos.

*Gestão de Documentação*

Não sendo a gestão de documentos obrigatória, é um factor importante para agilizar a gestão de segurança da informação. Assim foi desenvolvido um documento de regras que define a estrutura e composição da documentação da ICP do Cartão de Cidadão.

A classificação de informação é recomendada pelo ISO/IEC 27002:2013 (E). Os documentos podem ser classificados como:

- Restrito - Informação que pode comprometer a organização. Esta informação requer medidas de segurança moderadas quanto ao seu acesso, manuseamento, disseminação, armazenamento e destruição.
- Público - Informação que não compromete a organização. Esta informação não requer medidas especiais de acesso, manuseamento, disseminação, armazenamento e destruição.
- Confidencial - Informação que compromete a organização. Só está disponível a elementos autorizados e sob condições restritas. Esta informação requer medidas de segurança quanto ao seu acesso, manuseamento, disseminação, armazenamento e destruição.

Para estruturar a documentação são utilizadas as seguintes tipologias:

- Regras - Documentos genéricos que permitem definir o contexto e conceitos comuns ao funcionamento da ICP do Cartão de Cidadão.
- Políticas - Documentos de alto nível sobre um determinado tópico, descrevem a forma como esse tópico é observado nas práticas da ICP do Cartão de Cidadão.
- Procedimentos - Documentos que contêm instruções para a realização de uma determinada tarefa.
- Planos - Documentos que descrevem acções a executar periodicamente ou em virtude de determinada ocorrência.
- Processos - Documentos que descrevem a sequência de actividades a efectuar no âmbito da gestão operacional.
- Formulários - Documentos que permitem registar os valores de entrada e/ou saída de uma determinada cerimónia ou procedimento.
- Diagramas - Documentos de apoio que descrevem virtualmente um determinado conceito, processo ou estrutura.

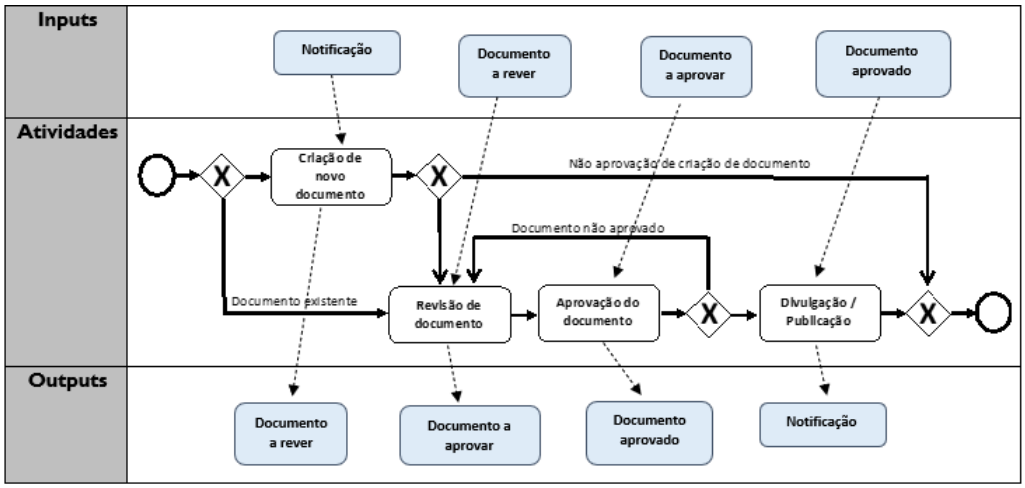



Figura 33: Diagrama do processo de gestão de documentos

- Minutas - *Templates* a fornecer a determinados destinatários, com informação relevante para esse destinatário.

Existe um processo para a criação, armazenamento, revisão, aprovação e divulgação de documentos. A figura 33 representa esse processo.

Para a revisão de documentos foi definido o prazo de 2 anos, por forma a garantir uma revisão periódica de toda a documentação, ou sempre que for notada a necessidade de alterações.

*Plano de Continuidade de Negócio*

A continuidade de negócio insere-se nas actividades da fase de operação e manutenção descritas na secção 4.1.4.

Foi elaborada uma lista com os requisitos identificados no apêndice A.4 e recomendações ISO/IEC 27002:2013 (E). Com o auxílio dessa lista foi analisado o que era praticado pela ICP do Cartão de Cidadão e verificado onde existiam oportunidades de melhoria.

A continuidade de negócio da ICP do Cartão de Cidadão foca-se na recuperação dos serviços críticos da ICP do Cartão de Cidadão. A disponibilidade dos serviços e preservação da informação tem em conta os RTO (*recovery time objective*) e RPO (*recovery point objective*) definidos. O RPO indica o período máximo de perda de dados possível que pode acontecer derivado de um incidente, i.e. indica há quanto tempo foi efectuado o último *backup*.

Foram criados dois planos distintos: um para incidentes disruptivos (incidente em que um ou mais sistemas críticos redundantes tenham sido destruídos/comprometidos na totalidade) e outro para incidentes não disruptivos (incidente em que nenhum sistema crítico redundante tenha sido destruído/comprometido na totalidade, i.e. uma das componentes redundantes continua a funcionar sem perda de integridade).

O plano de continuidade em caso de incidentes não disruptivos descreve a recuperação dos serviços críticos através da utilização de equipamentos redundantes e cópias de segurança.

O plano de continuidade em caso de incidente disruptivo descreve acções para a recuperação dos serviços críticos em caso de desastre e quando não é possível recuperação dos serviços nas instalações primárias da ICP do Cartão de Cidadão, existindo para o efeito instalações secundárias, semelhante às primárias, que se encontra o mais sincronizado possível com as instalações primárias.

No caso de comprometimento de chave privada da Entidade Certificadora são tomadas as seguintes medidas:

- Revogação do certificado da Entidade de Certificação e todos os certificados emitidos no ramo da hierarquia de confiança dessa Entidade de Certificação conforme procedimentos existentes;
- Notificação das Entidades de Certificação subordinadas, Entidade Gestora de Políticas de Certificação e todos os titulares de certificados emitidos no ramo de hierarquia de confiança da Entidade de Certificação;
- Reinicialização das configurações e parâmetros de segurança do HSM;
- Substituição de todas as credenciais de acesso físico e lógico aos sistemas e infraestruturas;
- Geração de novo par de chaves para a Entidade de Certificação, e pedido de novo certificado à Entidade de Certificação do nível superior conforme procedimentos existentes;
- Renovação de todos os certificados emitidos no ramo da hierarquia de confiança da Entidade de Certificação;

No caso de comprometimento de chave privada da Entidade de Validação Cronológica são tomadas as seguintes medidas:

- Desactivação imediata do serviço, a fim de não serem gerados mais selos temporais;
- Revogação do certificado da Entidade de Validação de Cronológica de acordo com procedimentos existentes;
- Destruição da chave privada;
- Geração de novo par de chaves através do *backoffice*, criação e activação de nova Entidade de Validação Cronológica de acordo com procedimentos existentes.

No caso de perda de sincronização de relógio são tomadas as seguintes medidas:

- Identificação e resolução da origem do incidente;
- Restabelecer a sincronização do relógio e reactivar o serviço de acordo com procedimentos existentes;

*Gestão de Alterações*

A gestão de alterações insere-se no contexto da operação e manutenção, definida na secção 4.1.4.

Foi elaborada uma lista de acordo com os requisitos ETSI EN 319 401, que podem ser consultados no apêndice A.5 e recomendações ISO/IEC 27002:2013 (E). A documentação de gestão de alterações que existia foi analisada de acordo com os requisitos e recomendações.

Foi desenvolvida uma política que descreve os controlos a considerar quando é identificada a necessidade de alteração ou melhoria de um recurso.

O processo de gestão de alterações foi divido em 4 categorias que seguem processos distintos: alterações na infraestrutura, alterações de recursos humanos, alterações a ambientes e alterações a documentos.

A figura 34 resume o processo de alterações na infraestrutura.

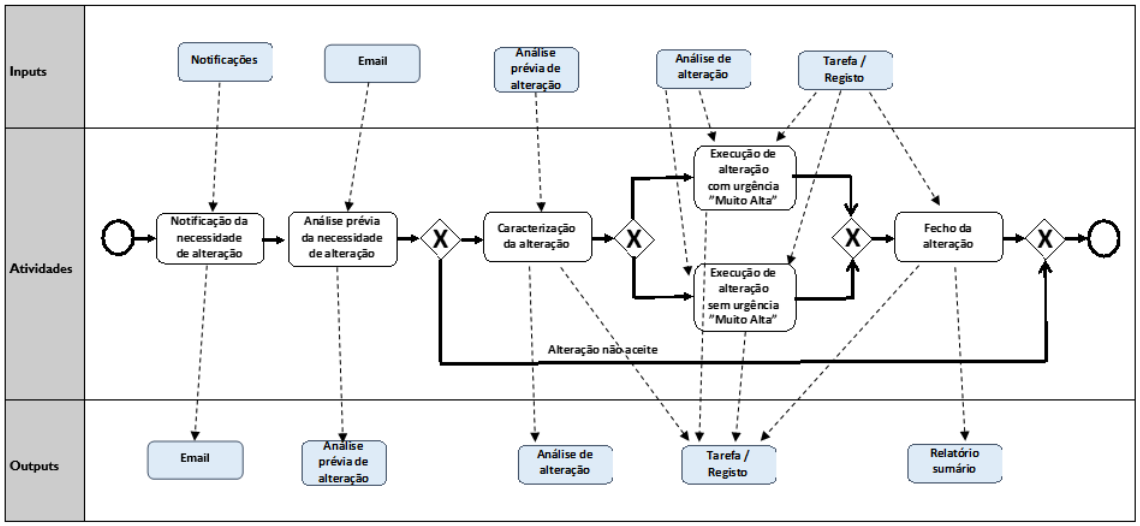



Figura 34: Processo de alterações na infraestrutura

As alterações à infraestrutura são analisadas pelo grupo de administração de segurança e categorizadas de acordo com o impacto e urgência da mesma. Alterações com urgência muito alta são executadas de modo rápido e controlado enquanto alterações com menor urgência são executadas de modo controlado e com necessidade de autorização do grupo de gestão.

Na gestão de melhorias, o processo começa quando existe uma notificação de sugestão de melhoria ao grupo de auditoria e é analisada pelo mesmo. Se a melhoria for aceite, o processo é encaminhado para a gestão de alterações. A figura 35 resume este processo.

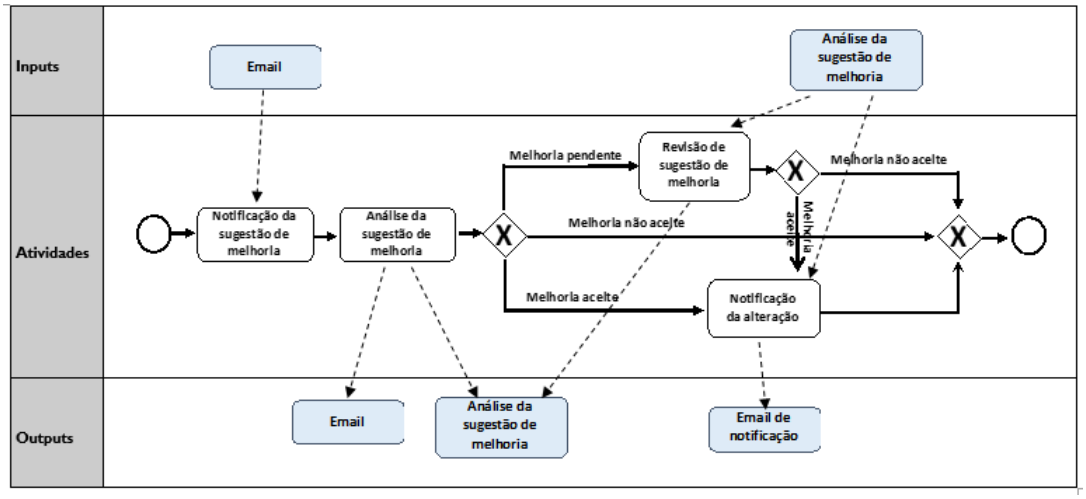



Figura 35: Processo de melhorias

*Gestão de Ambientes*

A gestão de ambientes insere-se no contexto de implementação, definido na secção 4.1.2.

Foi elaborada uma lista com os requisitos da regulamentação aplicável e recomendações ISO. A ICP do CC já tinha em prática políticas e regras de ambientes. Estes documentos foram analisados de acordo com a lista previamente elaborada.

Um ambiente é definido como um espaço delimitado, de acesso restrito, onde podem encontrar-se (de forma temporária ou definitiva) artefactos relacionados com o funcionamento da ICP do Cartão de Cidadão.

Os ambientes de referências são:

- Ambiente de produção

  Ambiente onde se encontram alojados os equipamentos que suportam a actividade da ICP do Cartão de Cidadão.

- Ambiente secundário de produção

  Ambiente que pode ser activado em caso de incidente ou desastre que afecte o ambiente de produção.

- Ambiente de informação

  Ambiente onde se encontram arquivados documentos, cópias de software, registos relacionados com a operação.

- Ambiente do grupo de trabalho

  Ambiente onde se encontram guardados todos os artefactos entregues à guarda do Grupo de Trabalho.

- Ambiente pessoal

  Ambiente onde se encontram armazenados os artefactos entregues à guarda de um elemento de um qualquer Grupo de Trabalho.

O ambiente de produção segue regras de segurança física impostas pela Norma Técnica - D 02.

O ambiente de produção está dividido em 4 níveis de segurança física:

- Nível 1

  Edifício em si, materializa-se pela entrada e zona de recepção no edifício. Controla o acesso físico ao edifício, que é restrito a pessoal autorizado. É requerida a identificação de todo o pessoal. Visitantes são alvo de identificação e registo e o acesso só é concedido se tiver sido previamente aprovado.

- Nível 2

  Materializa-se pela zona de trabalho global. Todas as pessoas que circulam neste nível têm de utilizar cartão identificador visível.

- Nível 3

  Materializa-se numa zona de antecâmara para as instalações da ICP do Cartão de Cidadão. Esta área garante que o pessoal que circula no nível 2 não circula nas imediações da entrada que possibilita o acesso ao nível 4. O acesso só é permitido a pessoal com autorização expressa. Têm mecanismos de controlo de acessos (e.g. mecanismos de identificação baseada em dois factores), mecanismos de detecção de intrusão e alarme, vídeo vigilância, detecção de incêndios.

- Nível 4

  Materializa-se por uma sala de bastidores da ICP do Cartão de Cidadão. O acesso a esta área apenas é permitido a pessoas previamente autorizadas. O acesso de pessoas de serviços de suporte/manutenção a esta área, tem que ser autorizado e acompanhado por um elemento de um Grupo de Trabalho.

A figura 36 apresenta um exemplo do *layout* dos níveis de segurança.

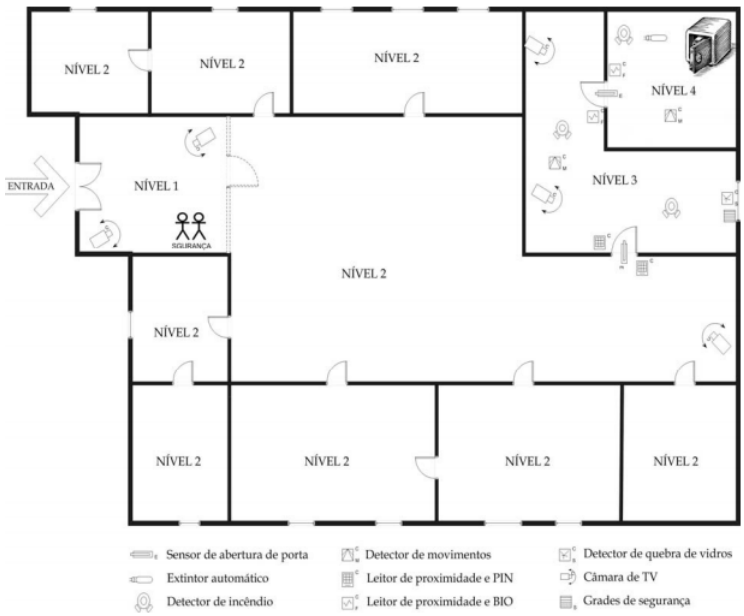



Figura 36: *Layout* dos níveis de segurança (Norma Técnica - D 02)

Nos níveis de segurança física aplica-se o conceito de defesa em profundidade, isto é, o acesso a um nível de segurança mais elevado só é possível quando previamente se tenha alcançado o nível imediatamente anterior.

Foi definido um procedimento para o acesso ao ambiente de produção da ICP do Cartão de Cidadão. Este procedimento define os requisitos de segurança que devem ser respeitados pelos recursos humanos e visitantes. O acesso ao ambiente de produção pode acontecer nas seguintes situações: auditoria interna e externa, realização de cerimónias, realização de manutenção dos sistemas de suporte de infraestrutura e limpeza do espaço. Outras situações têm de ser formalmente aprovadas previamente.

A entrada no ambiente de produção nível 3 e 4 é autorizada aos seguintes grupos de trabalho: gestão, auditoria, administração de sistemas e administração de segurança. No nível 4 todo os elementos registam a sua presença no livro de registo de presenças. Sempre que necessária a entrada de visitantes nos níveis 3 e 4 é solicitada autorização ao grupo de administração de segurança indicando a sala que se pretende aceder e o motivo da visita. O grupo de auditoria audita mensalmente o acesso a ambientes, inclusive o acesso ao ambiente de produção com base no livro de registo de presenças e *logs* de acesso. A entrada ou saída de equipamentos do ambiente de produção é previamente autorizada pelo grupo de administração de segurança e pelo *resource owner* do equipamento.

O ambiente de produção secundário cumpre as mesmas regras de segurança que o ambiente de produção principal.

*Gestão de Risco*

A gestão do risco está relacionada com a secção 4.1.1 e insere-se nas actividades da fase de operação e manutenção descritas na secção 4.1.4.

Foi elaborada uma lista com os requisitos ETSI EN 319 401, que podem ser consultados no apêndice A.7 e recomendações ISO 31000:2018 (E). Essa lista serviu como base para análise da gestão de risco praticada pela ICP do Cartão de Cidadão.

Foi definida uma política de gestão de risco que descreve a abordagem para a gestão de risco e, define boas práticas, regras e compromissos que todos os elementos dos Grupos de Trabalho devem cumprir, nomeadamente na identificação, quantificação e qualificação dos riscos.

Foi também definido um processo que descreve as várias actividades da gestão de risco. A figura 37 resume o processo de gestão de risco.

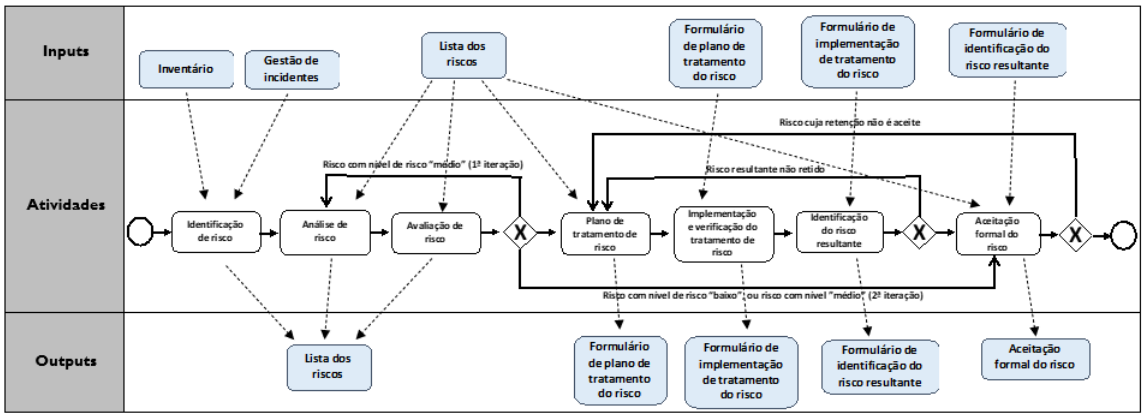



Figura 37: Processo de gestão de risco

As actividades de gestão de risco foram distribuídas de forma a dar corpo a uma gestão do tipo PDCA - *Plan, Do, Check* e *Act*:

- *Plan* - identificar, analisar e qualificar riscos, determinar pontos de controlo a implementar, identificar regras para a aceitação de riscos;
- *Do* - implementar as medidas para tratamento do risco;
- *Check* - monitorização contínua de vulnerabilidades, ameaças,incidentes e determinar acções preventivas e correctivas;
- *Act* - criar mecanismos de comunicação interna e externa dos níveis de risco e respectivas medidas para tratamento estabelecidas e assegurar a manutenção e melhoria contínua dos pontos de controlo implementados.

A identificação de risco reconhece e descreve os riscos que podem impedir a ICP do Cartão de Cidadão de atingir os seus objectivos. Esta actividade envolve a identificação dos vários serviços e actividades/processos associados, e a sua contextualização em termos de fonte de risco, local onde se realiza, processo e/ou actividade, e ameaça. Para além disso, foram definidos os seguintes factores a ter em conta para esta actividade:

- Fontes de risco tangíveis e intangíveis;
- Causas e eventos;
- Ameaças e oportunidades;
- Vulnerabilidades e competências;
- Alterações no contexto interno e externo;
- Indicadores de riscos emergentes;
- Alterações no contexto interno e externo;
- Indicadores de riscos emergentes;
- Tipo e valor do activo e recursos;
- Consequências e o seu impacto nos objectivos;
- Limitações de conhecimento e fidedignidade da informação;
- Factores relacionados com o tempo;
- Preconceitos, pressupostos, convicções e opiniões dos envolvidos.

Para as fontes de risco identificadas são determinadas possíveis ameaças que possam impactar negativamente a Confidencialidade, Integridade, Disponibilidade, Autenticidade e Não Repúdio dos recursos. Assim, são utilizados os seguintes métodos:

- Recolha baseada em auditorias internas ou externas;
- Publicações oficiais de organismos reconhecidos nacional e internacionalmente;
- Ocorrências verificadas na Gestão de Incidentes;
- Requisitos de disponibilidade de partes interessadas;
- Normas, contratos e legislação;

A análise de risco tem como objectivo entender a natureza do risco e as suas características, incluindo o nível de risco, consequências, probabilidade, eventos, cenários, controlos e a sua eficácia. Assim, são considerados os seguintes factores:

- Probabilidade dos eventos e as suas consequências;
- Natureza e dimensão das consequências;
- Complexidade e conectividade;
- Volatilidade e factores relacionados com o tempo;
- Eficácia dos controlos existentes;
- Sensibilidade e níveis de confiança.

O nível de risco é quantificado de acordo com os valores de impacto e probabilidade.

O impacto mede o grau em que um serviço ou actividade/processo será afectado na confidencialidade, integridade, disponibilidade, autenticidade e não repúdio, caso se concretize,o grau é medido entre 1(baixo) e 4(muito alto). O valor do impacto é também influenciado pela criticidade do serviço ou actividade/processo, calculada com base no cumprimento de RTO e RPO e varia entre 1(baixa) e 4(muito alta). O impacto é dado pela seguinte fórmula, onde CIDANr indica o valor de impacto na confidencialidade, integridade, disponibilidade, autenticidade e não repúdio:

$$\text{Impacto} = \text{Max(CIDANr)} \times \text{Criticidade}$$

A probabilidade da concretização das ameaças é baseada em ocorrências registadas anteriormente e/ou tendo em conta os controlos existentes.

A avaliação de risco compara os resultados da análise com critérios de risco estabelecidos com o objectivo de determinar se são necessárias acções adicionais. O critério de risco é baseado na qualificação de risco e define, de acordo com a sua qualificação, os riscos que necessitam de medidas de tratamento.

Para cada risco a tratar é identificado um *risk owner* que fica com a responsabilidade do tratamento do risco. O tratamento do risco envolve as seguintes actividades:

- Seleccionar o tipo de tratamento do risco;
- Planear e implementar o tratamento do risco;
- Verificar a eficácia do tratamento efectuado;
- Decidir se o risco resultante é aceitável;
- Se o risco resultante não for aceitável, efectuar o tratamento do risco resultante.

Os tipos de tratamento de risco são os definidos no ISO 31000:2018 (E), abordado na secção 2.2.2. No caso da medida de tratamento envolver reter o risco é necessário que o risco seja qualificado como baixo ou é identificado no plano de tratamento de risco a razão

para o reter (e.g. custo de tratamento superior aos danos possíveis, não existem opções de tratamento, entre outros), neste caso, é necessária a aceitação formal por parte do Grupo de Gestão.

Os resultados da gestão de risco são documentados e divulgados aos vários elementos dos Grupos de Trabalho.

*Gestão de Inventário*

A gestão de inventário insere-se nas actividades da fase de operação e manutenção descrita na secção 4.1.4

Foi elaborada uma lista com os requisitos ETSI EN 319 401, que podem ser consultados no apêndice A.8, e recomendações ISO/IEC 27002:2013 (E) para a gestão de inventário. A gestão de inventário praticada pela ICP do Cartão de Cidadão foi analisada de acordo com os requisitos.

Foi definida uma política que descreve a abordagem, princípios orientadores, metodologia e responsabilidades para a gestão de inventário.

Foi também elaborado um processo para a gestão de inventário que pretende garantir que a lista dos recursos esteja devidamente identificada e actualizada. A figura 38 resume o processo de gestão de inventário.

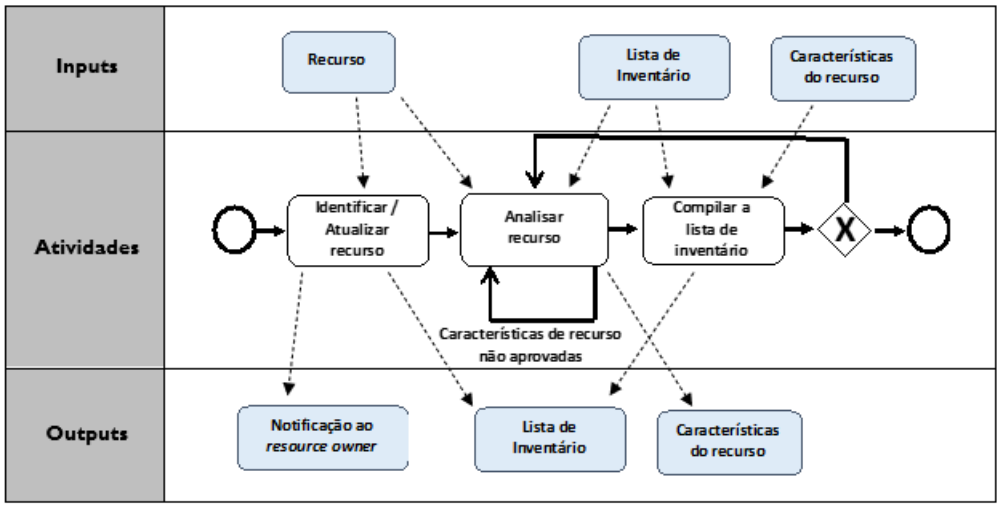



Figura 38: Processo de gestão de inventário

Todos os recursos são classificados de acordo com a sua especificidade técnica, relevância e características. A cada recurso é atribuído um *resource owner* que o classifica e caracteriza preenchendo a lista de inventário.

A especificidade técnica de cada recurso pode ser classificada como:

- Acessório de ambiente;

- Acessório de *hardware* criptográfico;
- Ambiente;
- *Software*;
- Ficheiro;
- Componentes de operação;
- Documentos;
- *Hardware*
- *Hardware* criptográfico;
- Média;
- Recursos humanos;
- Segurança física;
- Sistemas lógicos de suporte;
- Sistemas físicos de suporte.

A relevância é calculada tendo em conta a importância que o recursos tem para os objectivos dos processos/actividades e serviços da ICP do Cartão de Cidadão e varia entre 1(baixa) e 4 (muito elevada).

A caracterização dos recursos inclui os seguintes campos:

- Nº de identificação;
- Nome;
- Tipo;
- Identificador de Ambiente;
- *Resource Owner*;
- Estado;
- Âmbito;
- Relevância;
- Requisitos de segurança;

- Outras características;
- Observações;
- Recursos associados.

Os resultados da gestão de inventário são documentados e divulgados através de mecanismos apropriados aos elementos dos vários grupos de trabalho.

A lista de inventário é revista regularmente e sempre que se verificar necessário notificam-se os *resource owners* para reverem os recursos.

*Plano de Cessação de Actividade*

Foi elaborada uma lista com os requisitos ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2 e ETSI EN 319 421, que podem ser consultados no apêndice A.9. O plano de cessação de actividade praticado pela ICP do Cartão de Cidadão foi analisado de acordo com a lista.

Foi definido um plano que determina as acções a executar em caso de cessação de actividade da ICP do Cartão de Cidadão.

Assim, tomada a decisão de terminar a actividade da ICP do Cartão de Cidadão (imposta por acto administrativo ou legislativo), as acções a executar são as seguintes:

- Notificação das partes interessadas, em particular, entidade supervisora (Autoridade Nacional de Segurança (GNS)), conselho gestor do SCEE e cidadãos.
- Cessação de relações contratuais;
- Revogação dos certificados emitidos no âmbito da ICP do Cartão de Cidadão, quer para o cidadão, quer para os sistemas inerentes;
- As listas de certificados revogados (CRLs) serão mantidas acessíveis publicamente no repositório da ICP do Cartão de Cidadão, até à expiração do certificado com a data de validade mais longa;
- Todas as chaves privadas das entidades e os seus *backups* de certificação são destruídas.
- Os dados sujeitos a arquivo (incluindo documentação em arquivos, repositórios e arquivos de registo de eventos, cofre digital, e chaves públicas das entidades) continuarão arquivados pelo período de tempo definido pela legislação nacional e/ou regulamento 910/2014.
- É elaborado um plano e cerimónia de desmantelamento dos equipamentos. A destruição/eliminação dos equipamentos será efectuada por empresa especializada com acompanhamento pelo *resource owner* e por um elemento do grupo de auditoria.

- O grupo de gestão faz um relatório de término de actividade que será submetido à entidade supervisora e à entidade responsável pela guarda dos dados sujeitos a arquivo e das listas de certificados revogados.

*Gestão de Backup*

A gestão de *backups* insere-se nas actividades da fase de operação e manutenção descritas na secção 4.1.4.

Os *backups* são importantes para prevenir a perda indesejada de dados e também podem servir para repor os serviços aquando de um incidente.

Foi elaborada uma lista composta pelos requisitos ETSI EN 319 401 e ETSI EN 319 411-1, que pode ser consultada no apêndice A.10, e recomendações ISO/IEC 27002:2013 (E). A gestão de *backups* praticada pela ICP do Cartão de Cidadão foi analisada de acordo com essa lista.

As recomendações ISO/IEC 27002:2013 (E) incluem: definir uma política de *backup*, definir um plano de *backup*, monitorizar a execução de *backups*, determinar o período de retenção de informação, entre outros.

Tendo isto em consideração, foi definida uma política de gestão de *backup* que estipula as regras que os procedimentos de *backup* devem obedecer incluindo regras para o seu armazenamento.

A informação crítica é armazenada com periodicidade adequada aos RTO e RPO, essa periodicidade é revista anualmente. A informação considerada crítica inclui chaves privadas das entidades de certificação e serviços, *logs*, CRL e delta-CRL das entidade de certificação, bases de dados das várias componentes.

As operações de *backup* e *restore* são registadas, quer sejam efectuadas manualmente (no âmbito de cerimónias auditadas) que sejam efectuadas automaticamente. No caso dos *backups* efectuados através de um processo automático o sistema de monitorização monitoriza a realização do *backup* e guarda o registo de todas as verificações.

Os artefactos de armazenamento (i.e. dispositivo criptográfico de backup, dispositivos *Write Once Read Many*), encontram-se guardados em cofre físico que cumpre a norma EN 1143-1:2019 dentro de uma sala com o mesmo nível de segurança do ambiente de produção. O transporte de artefactos é efectuado de forma segura por elementos dos grupos de trabalho.

O período de retenção dos *backups* é o seguinte:

- O último *backup* da EC do Cartão de Cidadão é guardado pelo período de 20 anos (cumprindo a obrigação prevista na alínea r) do artigo 24º, do DL2 (1999));

- Nos *backups* em *tapes* o *backup* incremental é retido até ao *backup* total e o *backup* total é retido durante 2 semanas. O *backup* total de cada ano é retido durante 20 anos (cumprindo a obrigação prevista na alínea r) do artigo 24º, do DL2 (1999)).

No final do período de retenção, os *backups* são destruídos de modo seguro.

Os *backups* são verificados e validados anualmente pelo Grupo de Administração de Sistemas, e auditado pelo Grupo de Auditoria.

*Credenciação de módulos criptográficos*

A credenciação de módulos criptográficos insere-se nas actividades da fase de implementação 4.1.2.

De acordo com o ETSI EN 319 411-1, aplicam-se à ICP do Cartão de Cidadão, os seguintes requisitos:

- *"**OVR-6.5.2-01**: TSP's key pair generation, including keys used by revocation and registration services, shall be carried out within a secure cryptographic device which is a trustworthy system which:"*
  (a) *"a) is assured to EAL 4 or higher in accordance with ISO/IEC 15408 [1], or equivalent national or internationally recognized evaluation criteria for IT security provided this is a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures; or"*
  (b) *"b) meets the requirements identified in ISO/IEC 19790 [3] or FIPS PUB 140-2 [12] level 3."*

Os módulos criptográficos utilizados pela ICP do Cartão de Cidadão têm certificação EAL 4 +. Esta certificação está descrita na secção 2.2.4.

*Métricas*

As métricas inserem-se nas actividades da fase de avaliação descrita na secção 4.1.3.

Para todos os processos foram definidos indicadores e objectivos. Estes têm como objectivo avaliar a capacidade e eficiência dos processos. A avaliação é feita anualmente e é da responsabilidade do grupo de trabalho de administração de segurança.

Os resultados da avaliação destes indicadores são comunicados ao grupo de gestão. Para alguns indicadores foram definidos *thresholds*, no caso dos indicadores excederem esses *thresholds* o Grupo de Administração de Segurança elabora um plano de actividade para identificar a razão dos números obtidos e um conjunto de acções para a sua normalização.

*Auditorias*

As auditorias inserem-se nas actividades da fase de avaliação descrita na 4.1.3.

As auditorias internas são importantes para avaliar se a organização cumpre os requisitos necessários e, também, para avaliar a eficácia e adequação da gestão de segurança de informação. Nesse sentido, o ISO/IEC 27002:2013 (E) recomenda a definição de um programa de auditoria e também a definição de critérios, responsabilidades e o âmbito de auditorias.

Assim, foi estabelecido um plano de auditoria que descreve as auditorias internas a realizar e a sua periodicidade. Esse documento pretende orientar o grupo de trabalho de auditoria na realização das auditorias.

As auditorias internas são efectuadas com a seguinte periodicidade:

- Todos os meses - monitorização, eventos de segurança de informação, acessos remotos, acessos a ambientes e emissão de CRL da EC Raiz, entre outros;
- Todos os dois meses - incidentes de segurança de informação, registo de auditoria (*logs*) e análise documental;
- Todos os semestres - *tokens* no cofre físico, operações de *restore* e relatório de disponibilidade do Centro de Dados Principal e Secundário;
- Anualmente - teste do plano de continuidade de negócio, ambientes e *backups*;
- Todos os 2 anos - emissão de certificado de sub-EC;
- Todos os 4 anos - Emissão de certificado da EC Raiz;

*Documentos públicos*

Foram analisados os documentos públicos da ICP do Cartão de Cidadão Declaração de Práticas de Certificação da EC do Cartão de Cidadão, Declaração de Práticas de Certificação da EC de Autenticação do Cartão de Cidadão, Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão, Declaração de Práticas de Certificação da EC de Chave Móvel Digital de Assinatura Qualificada do Cartão de Cidadão, Política de Certificado de Assinatura Digital Qualificada, Política de Certificado da EC de Autenticação do Cartão de Cidadão, Política de Certificado de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão, Política de Certificado de Validação Cronológica, Política de Certificado da EC do Cidadão e Declaração de Divulgação de Princípios de acordo com os requisitos ETSI EN 319 401 e ETSI EN 319 411-1, que podem ser consultados no apêndice A.11, e as alterações feitas na restante documentação.

- Declaração e divulgação de princípios

  Foram elaborados três documentos deste tipo: um para a Entidade de Certificação do Cartão de Cidadão, um para a Entidade de Certificação de Chave Móvel Digital e um para a Entidade de Validação Cronológica. Este documento foi elaborado de acordo o anexo A do ETSI EN 319 411-1, tendo a estrutura indicada no anexo. Este documento também serve o papel dos termos e condições.

- Declaração de práticas de certificação Este documento define os procedimentos e práticas utilizadas pelas entidades de certificação.Foi elaborado um documento deste tipo para cada uma das entidades de certificação do Cartão de Cidadão. Estes documentos seguem a estrutura definida no documento RFC 3647, de acordo também com a estrutura recomendada pelo SCEE e pelos ETSI EN 319 411-1 e ETSI EN 319 411-2.

- Política de certificação

  Este documento descreve os perfis dos certificados, lista de certificados revogados (CRL) e OCSP emitidos pela entidade de certificação. Foi elaborado um documento deste tipo por cada entidade de certificação do Cartão de Cidadão. Cada certificado emitido pelas entidades de certificação contém um campo com o OID(*Object Identifier*) da respectiva política de certificação.

# 6

# CONCLUSÃO

Neste capítulo apresentam-se as conclusões extraídas deste trabalho, as principais contribuições que proporciona à área estudada e uma descrição de trabalho futuro.

Ao longo desta dissertação foram analisados as melhores práticas na área da gestão de segurança de sistemas de segurança da informação e nos sistemas de confiança seguros, em particular, a família de *standards* ISO/IEC 27000 e o documento NIST Special Publication 800-160.

O objectivo da análise foi obter um conhecimento profundo destas práticas para propor uma abordagem de implementação que simplifique o processo, em particular, para as organizações com menos recursos. Disto resulta o capítulo 4, que propõe uma abordagem com base nas várias fases do desenvolvimento de *software*.

Com o trabalho realizado conclui-se que a implementação quer da família de *standards* ISO/IEC 27000 quer do *standard* NIST Special Publication 800-160 resultam em sistemas seguros, no entanto as abordagens à segurança diferem bastante entre ambos.

Enquanto o ISO/IEC 27000:2018 (en) foca-se na gestão de segurança da informação, o NIST Special Publication 800-160 trata da segurança em geral do sistema.

A proposta de resposta do ISO/IEC 27000:2018 (en) ao problema da segurança da informação é essencialmente relacionada com a implementação de um sistema de gestão de segurança da informação composto por políticas, procedimentos, directrizes, regras e todos os recursos e actividades que permitem a segurança da informação. Os documentos publicados indicam requisitos e controlos que devem ser cumpridos e implementados, respectivamente. Apesar disso, cada organização pode , e deve, implementar o sistema de gestão de segurança da informação adaptado à complexidade e necessidade da organização. No entanto, para organizações com recursos limitados, a sua implementação continua a ser um processo complicado e com custos elevados.

O documento publicado pelo NIST, NIST Special Publication 800-160, aplica princípios da engenharia de sistemas à segurança do sistema e propõe uma abordagem estruturada com actividades bem definidas. As actividades desenvolvidas ao longo do ciclo de vida do sistema resultam em garantias de confiança da segurança do sistema.

Apesar de não ser possível implementar sistemas completamente seguros devem ser tomadas medidas preventivas quanto aos riscos a que estes estão sujeitos. A implementação de qualquer uma das duas abordagens resulta em garantias de segurança fortes.

Com esta dissertação foi possível entender a complexidade por detrás do processo de segurança de um sistema crítico, em particular, no caso da ICP do Cartão de Cidadão. Este processo, apesar de ser complexo, é essencial ao bom funcionamento destes sistemas. A implementação de medidas preventivas gera confiança, algo que, actualmente, cada vez mais preocupa os utilizadores.

Com a abordagem proposta no capítulo 4 pretende-se estruturar e facilitar o processo de desenvolvimento de sistemas de confiança seguros e da sua gestão de segurança da informação.

No caso prático da ICP do Cartão de Cidadão, abordado nesta dissertação, não foi possível aplicar os conceitos desde o início do projecto (visto o mesmo já se encontrar em produção), tal como seria ideal, de modo a preparar o sistema desde uma fase inicial. Contudo, foi possível adaptar a abordagem ao caso e conseguir, no final, um sistema que fornece garantias de segurança às partes interessadas e que cumpre a legislação e regulamentação aplicável.

Parte III

# APÊNDICES

# A

# REQUISITOS DA REGULAMENTAÇÃO APLICÁVEL

## A.1 REQUISITOS ETSI 319 401 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

De seguida são apresentados os requisitos obrigatórios do ETSI 319 401:

- *"**REQ-6.3-01**: The TSP shall define an information security policy which is approved by management and which sets out the organization's approach to managing its information security."*
- *"**REQ-6.3-02**: Changes to the information security policy shall be communicated to third parties, where applicable. This includes subscribers, relying parties, assessment bodies, supervisory or other regulatory bodies."*
- *"**REQ-6.3-03**: A TSP's information security policy shall be documented, implemented and maintained including the security controls and operating procedures for TSP's facilities, systems and information assets providing the services."*
- *"**REQ-6.3-04**: The TSP shall publish and communicate the information security policy to all employees who are impacted by it."*
- *"**REQ-6.3-05**: The TSP shall retain overall responsibility for conformance with the procedures prescribed in its information security policy, even when the TSP's functionality is undertaken by outsourcers."*
- *"**REQ-6.3-06**: TSP shall define the outsourcers' liability and ensure that outsourcer are bound to implement any controls required by the TSP."*
- *"**REQ-6.3-07**: The TSP's information security policy and inventory of assets for information security (see clause 7.3) shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness."*
- *"**REQ-6.3-08**: Any changes that will impact on the level of security provided shall be approved by the management body referred to in **REQ-6.1-07**."*

- *"**REQ-6.3-09**: The configuration of the TSPs systems shall be regularly checked for changes which violate the TSPs security policies."*
- *"**REQ-6.3-10**: The maximum interval between two checks shall be documented in the trust service practice statement."*

## A.2 Requisitos ETSI 319 401 Gestão de Incidentes

Os requisitos ETSI 319 401 (ref.), em particular, secção 7.9 "*Incident Management*", são os seguintes:

- *"**REQ-7.9-01**: System activities concerning access to IT systems, use of IT systems, and service requests shall be monitored."*
- *"**REQ-7.9-02**: Monitoring activities should take account of the sensitivity of any information collected or analysed."*
- *"**REQ-7.9-03**: Abnormal system activities that indicate a potential security violation, including intrusion into the TSP's network, shall be detected and reported as alarms."*
- *"**REQ-7.9-04**: The TSP shall monitor the following events:"*
  (a) *start-up and shutdown of the logging functions; and"*
  (b) *availability and utilization of needed services with the TSP's network."*
- *"**REQ-7.9-05**: The TSP shall act in a timely and co-ordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security."*
- *"**REQ-7.9-06**: The TSP shall appoint trusted role personnel to follow up on alerts of potentially critical security events and ensure that relevant incidents are reported in line with the TSP's procedures."*
- *"**REQ-7.9-07**: The TSP shall establish procedures to notify the appropriate parties in line with the applicable regulatory rules of any breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein within 24 hours of the breach being identified."*
- *"**REQ-7.9-08**: Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the TSP shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay."*
- *"**REQ-7.9-09**: The TSP's systems shall be monitored including the monitoring or regular review of audit logs to identify evidence of malicious activity implementing automatic mechanisms to process the audit logs and alert personnel of possible critical security events."*

- *"**REQ-7.9-10**: The TSP shall address any critical vulnerability not previously addressed by the TSP, within a period of 48 hours after discovery."*
- *"**REQ-7.9-11**: For any vulnerability, given the potential impact, the TSP shall [CHOICE]:"*
  (a) *create and implement a plan to mitigate the vulnerability; or"*
  (b) *document the factual basis for the TSP's determination that the vulnerability does not require remediation."*
- *"**REQ-7.9-12**: Incident reporting and response procedures shall be employed in such a way that damage from security incidents and malfunctions are minimized."*

## A.3 REQUISITOS ETSI 319 401 GESTÃO DE RECURSOS HUMANOS

Os requisitos ETSI EN 319 401, em particular, as secções 7.2 *"Human Resources"* e secção 7.1.2 *"Segregation of duties"*, são os seguintes:

- *"**REQ-7.2-01**: The TSP shall ensure that employees and contractors support the trustworthiness of the TSP's operations."*
- *"**REQ-7.2-02**: The TSP shall employ staff and, if applicable, subcontractors, who possess the necessary expertise, reliability, experience, and qualifications and who have received training regarding security and personal data protection rules as appropriate for the offered services and the job function."*
- *"**REQ-7.2-03**: TSP's personnel should be able to fulfil the requirement of "expert knowledge, experience and qualifications"through formal training and credentials, or actual experience, or a combination of the two."*
- *"**REQ-7.2-04**: This should include regular (at least every 12 months) updates on new threats and current security practices."*
- *"**REQ-7.2-05**: Appropriate disciplinary sanctions shall be applied to personnel violating TSP's policies or procedures."*
- *"**REQ-7.2-06**: Security roles and responsibilities, as specified in the TSP's information security policy, shall be documented in job descriptions or in documents available to all concerned personnel."*
- *"**REQ-7.2-07**: Trusted roles, on which the security of the TSP's operation is dependent, shall be clearly identified."*
- *"**REQ-7.2-08**: Trusted roles shall be named by the management."*

- *"**REQ-7.2-09**: Trusted roles shall be accepted by the management and the person to fulfil the role."*
- *"**REQ-7.2-10**: TSP's personnel (both temporary and permanent) shall have job descriptions defined from the view point of roles fulfilled with segregation of duties and least privilege (see clause 7.1.2), determining position sensitivity based on the duties and access levels, background screening and employee training and awareness."*
- *"**REQ-7.2-11**: Where appropriate, job descriptions shall differentiate between general functions and TSP's specific functions. These should include skills and experience requirements."*
- *"**REQ-7.2-12**: Personnel shall exercise administrative and management procedures and processes that are in line with the TSP's information security management procedures."*
- *"**REQ-7.2-13**: Managerial personnel shall possess experience or training with respect to the trust service that is provided, familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions."*
- *"**REQ-7.2-14**: All TSP's personnel in trusted roles shall be free from conflict of interest that might prejudice the impartiality of the TSP's operations."*
- *"**REQ-7.2-15**: Trusted roles shall include roles that involve the following responsibilities:"*
  (a) *Security Officers: Overall responsibility for administering the implementation of the security practices."*
  (b) *System Administrators: Authorized to install, configure and maintain the TSP's trustworthy systems for service management."*
  (c) *System Operators: Responsible for operating the TSP's trustworthy systems on a day-to-day basis. Authorized to perform system backup."*
  (d) *System Auditors: Authorized to view archives and audit logs of the TSP's trustworthy systems."*
- *"**REQ-7.2-16**: TSP's personnel shall be formally appointed to trusted roles by senior management responsible for security requiring the principle of "least privilege"when accessing or when configuring access privileges."*
- *"**REQ-7.2-17**: Personnel shall not have access to the trusted functions until the necessary checks are completed."*
- *"**REQ-7.1.2-01**: Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the TSP's assets. "*

## A.4 REQUISITOS ETSI 319-401 E ETSI 319 411-1 PARA A CONTINUIDADE DE NEGÓCIO

Os requisitos ETSI 319-401, em particular a secção 7.11 *"Business Continuity Management* e 6.3 *"Certificate Status Services"*, são os seguintes:

- *"**CSS-6.3.10-02**: Revocation status information shall be available 24 hours per day, 7 days per week. Upon system failure, service or other factors which are not under the control of the TSP, the TSP shall make best endeavours to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the CPS."*
- *"**REQ - 7.11-01**: The TSP shall define and maintain a continuity plan to enact in case of a disaster."*
- *"**REQ - 7.11-02**: In the event of a disaster, including compromise of a private signing key or compromise of some other credential of the TSP, operations shall be restored within the delay established in the continuity plan, having addressed any cause for the disaster wich may recur (e.g. security vulnerability) with appropriate remediation measures."*

Os requisitos ETSI 319-411-1, em particular a secção 6.4.8 *"Compromise and disaster recovery"*, são os seguintes:

- *"**OVR-6.4.8-02**: TSP's systems data necessary to resume CA operations shall be backed up and stored in safe places, preferably also remote, suitable to allow the TSP to timely go back to operations in case of incident/disasters."*
- *"**OVR-6.4.8-04**: Adequate back-up facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure."*
- *"**OVR-6.4.8-08**: The TSP's business continuity plan (or disaster recovery plan) shall address the compromise, loss or suspected compromise of a CA's private key as a disaster."*
- *"**OVR-6.4.8-09**: The processes planned as per requirement OVR-6.4.8-08 shall be in place."*
- *"**OVR-6.4.8-10**: Following a disaster, the TSP shall, where practical, take steps to avoid repetition of a disaster."*
- *"**OVR-6.4.8-11**: The TSP shall inform the following of the compromise: all subscribers and other entities with which the TSP has agreements or other form of established relations, among which relying parties and TSPs;"*
- *"**OVR-6.4.8-12**: The TSP shall make the information in OVR-6.4.8-11 available to other relying parties;"*
- *"**OVR-6.4.8-13**: The TSP shall indicate that certificates and revocation status information issued using this CA key may no longer be valid; and"*

- *"**OVR-6.4.8-14**: The TSP shall revoke any CA certificate that has been issued for the compromised TSP when a TSP is informed of the compromise of another CA."*

## A.5 Requisitos ETSI 319-401 gestão de alterações

Os requisitos ETSI 319-401, em particular a secção 7.7 *"Operations security"*, são os seguintes:

- *"**REQ-7.7-03**: Change control procedures shall be applied for releases, modifications and emergency software fixes of any operational software and changes to the configuration which applies the TSP's security policy;"*
- *"**REQ-7.7-04**: The procedures shall include documentation of the changes."*

## A.6 Requisitos ETSI 319 401 para a gestão de ambientes

Os requisitos ETSI 319-401, em particular a secção 7.6 *"Physical and environmental security"*, são os seguintes:

- *"**REQ-7.6-01**: The TSP shall control physical access to components of the TSP's system whose security is critical to the provision of its trust services and minimize risks related to physical security."*
- *"**REQ-7.6-02**: Physical access to components of the TSP's system whose security is critical to the provision of its trust services shall be limited to authorized individuals."*
- *"**REQ-7.6-03**: Controls shall be implemented to avoid loss, damage or compromise of assets and interruption to business activities."*
- *"**REQ-7.6-04**: Controls shall be implemented to avoid compromise or theft of information and information processing facilities."*
- *"**REQ-7.6-05**: Components that are critical for the secure operation of the trust service shall be located in a protected security perimeter with physical protection against intrusion, controls on access through the security perimeter and alarms to detect intrusion."*

Os requisitos ETSI 319-411-1, em particular a secção 6.4.2 *"Physical security controls"* e secção 6.4.8 *"Compromise and disaster recovery"*, são os seguintes:

- *"**OVR-6.4.2-02**: The facilities concerned with certificate generation and revocation management shall be operated in an environment which physically protects the services from compromise through unauthorized access to systems or data."*

- *"**OVR-6.4.2-03**: Every entry to the physically secure area shall be subject to independent oversight and non-authorized person shall be accompanied by an authorized person whilst in the secure area."*
- *"**OVR-6.4.2-04**: Every entry and exit shall be logged."*
- *" **OVR-6.4.2-05**: Physical protection shall be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the certificate generation and revocation management services."*
- *"**OVR-6.4.2-06**: Any parts of the premises shared with other organizations shall be outside the perimeter of the certificate generation and revocation management services."*
- *"**OVR-6.4.2-07**: Physical and environmental security controls shall be implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation."*
- *"**OVR-6.4.2-08**: The TSP's physical and environmental security policy for systems concerned with certificate generation and revocation management services shall address the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery."*
- *"**OVR-6.4.2-09**: Controls shall be implemented to protect against equipment, information, media and software relating to the TSP's services being taken off-site without authorization."*
- *"**OVR-6.4.2-10**: Other functions relating to TSP's operations may be supported within the same secured area provided that the access is limited to authorized personnel."*
- *"**OVR-6.4.2-11** : Root CA private keys shall be held and used physically isolated from normal operations such that only designated trusted personnel have access to the keys for use in signing subordinate CA certificates."*
- *"**OVR-6.4.8-02**: TSP's systems data necessary to resume CA operations shall be backed up and stored in safe places, preferably also remote, suitable to allow the TSP to timely go back to operations in case of incident/disasters."*
- *OVR-6.4.8-04: Adequate back-up facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure."*
- *"**OVR-6.4.8-05**: Back-up arrangements should be regularly tested to ensure that they meet the requirements of business continuity plans."*

## A.7 Requisitos ETSI 319 401 para a Gestão de Risco

Os requisitos ETSI 319-401 em particular a secção 5 *"Risk management"* e secção 7.3 *"Asset management"*, são os seguintes:

- *"**REQ-5-01**: The TSP shall carry out a risk assessment to identify, analyse and evaluate trust service risks taking into account business and technical issues."*
- *"**REQ-5-02**: The TSP shall select the appropriate risk treatment measures, taking account of the risk assessment results. The risk treatment measures shall ensure that the level of security is commensurate to the degree of risk."*
- ***REQ-5-03**: The TSP shall determine all security requirements and operational procedures that are necessary to implement the risk treatment measures chosen, as documented in the information security policy and the trust service practice statement."*
- *"**REQ-5-04**: The risk assessment shall be regularly reviewed and revised."*
- ***REQ-5-05**: The TSP's management shall approve the risk assessment and accept the residual risk identified."*
- *"**REQ-7.3.1-01**: The TSP shall ensure an appropriate level of protection of its assets including information assets."*
- *"**REQ-7.3.1-02**: The TSP shall maintain an inventory of all information assets and shall assign a classification consistent with the risk assessment."*
- *"**REQ-7.3.2-01**: All media shall be handled securely in accordance with requirements of the information classification scheme. Media containing sensitive data shall be securely disposed of when no longer required."*

## A.8 Requisitos ETSI 319 401 para a Gestão de Inventário

Os requisitos ETSI 319-401 em particular a 7.3.1 *"Asset management - general requirements"*, são os seguintes:

- *"**REQ-7.3.1-01**: The TSP shall ensure an appropriate level of protection of its assets including information assets."*
- *"**REQ-7.3.1-02**: The TSP shall maintain an inventory of all information assets and shall assign a classification consistent with the risk assessment."*

## A.9 Requisitos ETSI 319 401, ETSI 319 411-1, ETSI 319 411-2 e ETSI 319-421 para a cessação de actividade

Os requisitos ETSI 319-401 em particular a secção 6.1 *"Policies and practices - Trust service practice statement"* e secção 7.12 *"TSP termination and termination plans"*, são os seguintes:

- *"**REQ-6.1-11**: The TSP shall state in its practices the provisions made for termination of service (see clause 7.12)."*
- *"**REQ-7.12-01**: Potential disruptions to subscribers and relying parties shall be minimized as a result of the cessation of the TSP's services, and in particular continued maintenance of information required to verify the correctness of trust services shall be provided. In particular:"*
- *"**REQ-7.12-02**: The TSP shall have an up-to-date termination plan.*

  *Before the TSP terminates its services at least the following procedures apply:"*
- *"**REQ-7.12-03**: Before the TSP terminates its services, the TSP shall inform the following of the termination: all subscribers and other entities with which the TSP has agreements or other form of established relations, among which relying parties, TSPs and relevant authorities such as supervisory bodies."*
- *"**REQ-7.12-04**: Before the TSP terminates its services, the TSP shall make the information of the termination available to other relying parties."*
- *"**REQ-7.12-05**: Before the TSP terminates its services, the TSP shall terminate authorization of all subcontractors to act on behalf of the TSP in carrying out any functions relating to the process of issuing trust service tokens."*
- *"**REQ-7.12-06**: Before the TSP terminates its services, the TSP shall transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the TSP for a reasonable period, unless it can be demonstrated that the TSP does not hold any such information."*
- *"**REQ-7.12-07**: Before the TSP terminates its services, the TSP's private keys, including backup copies, shall be destroyed, or withdrawn from use, in a manner such that the private keys cannot be retrieved."*
- *"**REQ-7.12-08**: Before the TSP terminates its services, where possible TSP should make arrangements to transfer provision of trust services for its existing customers to another TSP."*
- *"**REQ-7.12-09**: The TSP shall have an arrangement to cover the costs to fulfil these minimum requirements in case the TSP becomes bankrupt or for other reasons is unable to cover the costs by itself, as far as possible within the constraints of applicable legislation regarding bankruptcy."*

- *"**REQ-7.12-10**: The TSP shall state in its practices the provisions made for termination of service. This shall include:"*
  (a) *notification of affected entities; and"*
  (b) *where applicable, transferring the TSP's obligations to other parties."*
- *"**REQ-7.12-11**: The TSP shall maintain or transfer to a reliable party its obligations to make available its public key or its trust service tokens to relying parties for a reasonable period."*

Os requisitos ETSI 319-401, em particular a secção 6.4.9 *"Certification authority or registration authority termination"*, são os seguintes:

- *"**OVR-6.4.9-02**: Requirement REQ-7.12-06 of ETSI EN 319 401 [8], shall apply to the following information for their respective period of time as indicated to the subscriber and relying party (see in particular REG-6.3.4-17 and CSS-6.3.10-02):"*
  (a) *registration information (see clauses 6.2.2, 6.3.1 and 6.3.4);"*
  (b) *where applicable, transferring the TSP's obligations to other parties."*
  (c) *event log archives (see clauses 6.4.5 and 6.4.6)."*
- *"**OVR-6.4.9-03**: Requirement REQ-7.12-10 of ETSI EN 319 401 [8], shall also include the handling of the revocation status for unexpired certificates that have been issued."*
- *"**OVR-6.4.9-04**: When another cross certified TSP stops all operations, including handling revocation (see 6.4.9-03), all cross certificates to that TSP shall be revoked.*
  *NOTE: Affected entities to be informed of termination under ETSI EN 319 401 [8], REQ-7.12-10 include cross certified TSP."*

Os requisitos ETSI 319-401, em particular a secção 6.4.9 *"Certification authority or registration authority termination"*, são os seguintes:

- *"**CSS-6.3.10-12**: The TSP shall document precisely in its practices statements and in its terms and conditions how requirements CSS-6.3.10-02 to CSS-6.3.10-11 are met, including:"*
  (a) *how the revocation status information is provided in the case of TSP termination (see clause 6.4.9)."*
- *"**OVR-6.4.5-03**: The information shall be maintained as necessary to meet legal requirements beyond the termination of the TSP (see clause 6.4.9)."*
- *"**OVR-6.4.5-05**: The TSP shall document precisely the period of retention of the information mentioned above in its practices statements and shall indicate which information is subject to be handed-over through its termination plan."*

Os requisitos ETSI 319-421, em particular a secção 7.14 *"TSA termination and termination plans"*, são os seguintes:

- *The requirements identified in ETSI EN 319 401 [4], clause 7.12 shall apply. In addition the following particular requirements apply: "*
  (a) *When the TSA terminates its services, the TSA shall revoke the TSU's certificates."*

## A.10 Requisitos ETSI 319 401 e ETSI 319 411-1 para a gestão de backups

Os requisitos ETSI EN 319 401, em particular a secção 7.10 *"Collection of evidence"* são os seguintes:

- *"**REQ-7.10-01**: The TSP shall record and keep accessible for an appropriate period of time, including after the activities of the TSP have ceased, all relevant information concerning data issued and received by the TSP, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service."*
- *"**REQ-7.10-02**: The confidentiality and integrity of current and archived records concerning operation of services shall be maintained."*
- *"**REQ-7.10-03**: Records concerning the operation of services shall be completely and confidentially archived in accordance with disclosed business practices."*
- *"**REQ-7.10-04**: Records concerning the operation of services shall be made available if required for the purposes of providing evidence of the correct operation of the services for the purpose of legal proceedings."*
- *"**REQ-7.10-07**: Records concerning services shall be held for a period of time as appropriate for providing necessary legal evidence and as notified in the TSP's terms and conditions (see clause 6.3)."*
- *"**REQ-7.10-08**: The events shall be logged in a way that they cannot be easily deleted or destroyed (except if reliably transferred to long-term media) within the period of time that they are required to be held.*

  *EXAMPLE: This can be achieved, for example, through the use of write-only media, a record of each removable media used and the use of off-site backup or by parallel storage of the information at several (e.g. 2 or 3) independent sites."*

Os requisitos ETSI EN 319 411-1, em particular as secções 6.4.6 *"Records archival"*, 6.4.8 *"Compromise and disaster recovery"*, 6.5.2 *"Private key protection and cryptographic module engneering controls"* e 6.5.3 *"Other aspects of key management"*, são os seguintes:

- *"**OVR-6.4.6-01**: The TSP shall retain the following for at least seven years after any certifcate based on these records ceases to be valid:"*
  (a) *a) log of all events relating to the life cycle of keys managed by the CA, including any subject key pairs generated by the CA;"*
  (b) *b) documentation as identified in clause 6.3.4"*
    - *"**REG-6.3.4-07**: The TSP shall record the agreement with the subscriber and if the subscriber and subject are two separate entities and the subject is a natural or legal person, with the subject."*
    - *"**REG-6.3.4-17**: The records identified above shall be retained for the period of time as indicated to the subscriber (as part of the terms and conditions."*
- *"**OVR-6.4.8-02**: TSP's systems data necessary to resume CA operations shall be backed up and stored in safe places, preferably also remote, suitable to allow the TSP to timely go back in case of incidente/disasters."*
- *"**OVR-6.4.8-03**: In line with ISO/IEC 27002, clause 12.3: Back-up copies of essential information and software should be taken regularly."*
- *"**OVR-6.4.8-04**: Adequate back-up facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure."*
- *"**OVR-6.4.8-05**: Back-up arrangements should be regularly tested to ensure that they meet the requirements of business continuity plans."*
- *"**OVR-6.4.8-06**: Backup and restore functions shall be performed by the relevant trusted roles specified in clause 6.4.4."*
- *"**GEN-6.5.2-06**: The CA private signing key shall be backed up, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment (see clause 6.4.2)."*
- *"**GEN-6.5.2-07**: The number of personnel authorized to carry out the CA private signing key back up, storage and recovery shall be kept to a minimum and be consistent with the CA's practices."*
- *"**GEN-6.5.2-08**: Copies of the CA private signing keys shall be subject to the same or greater level of security controls as keys currently in use."*
- *"**GEN-6.5.2-09**[CONDITIONAL]: Where the CA private signing keys and any copies are stored in a dedicates secure cryptographic device, access controls shall be in place to ensure that the keys are not accessible outside this device."*

- *"**GEN-6.5.3-06**: All copies of the CA private signing keys shall be destroyed at the end of their life cycle."*

## A.11 REQUISITOS ETSI 319 401 E ETSI 319 411-1 PARA OS DOCUMENTOS PÚBLICOS

Os requisitos ETSI 319 401, em particular a secção 6.1 "Trust Service Practice Statement"e 6.2 "Terms and Conditions"são os seguintes:

- *"**REQ-6.1-03**: The TSP shall have a statement of the practices and procedures used to address all the requirements identified for the applicable TSP's policy."*
- *"**REQ-6.1-04**: The TSP's trust service practice statement shall identify the obligations of all external organizations supporting the TSP's services including the applicable policies and practices."*
- *"**REQ-6.1-05**: The TSP shall make available to subscribers and relying parties its practice statement, and other relevant documentation, as necessary to assess conformance to the service policy."*
- *"**REQ-6.1-07**: The TSP's management shall implement the practices."*
- *"**REQ-6.1-08**: The TSP shall define a review process for the practices including responsibilities for maintaining the TSP's practice statement."*
- *"**REQ-6.1-09**: The TSP shall notify notice of changes it intends to make in its practice statement."*
- *"**REQ-6.1-10**: The TSP shall, following approval as in REQ-6.1-06 above, make the revised TSP's practice statement immediately available as required under REQ-6.1-05 above."*
- *"**REQ-6.1-11**: The TSP shall state in its practices the provisions made for termination of service (see clause 7.12)."*
- *"**REQ-6.2-01**: TSP shall make the terms and conditions regarding its services available to all subscribers and relying parties."*
- *"**REQ-6.2-02**: The terms and conditions shall at least specify for each trust service policy supported by the TSP the following:"*
  (a) *the trust service policy being applied;"*
  (b) *any limitations on the use of the service provided including the limitation for damages arising from the use of services exceeding such limitations;"*
  (c) *the subscriber's obligations, if any;"*

(d) *information for parties relying on the trust service;"*

(e) *the period of time during which TSP's event logs are retained;"*

(f) *limitations of liability;"*

(g) *the applicable legal system;"*

(h) *procedures for complaints and dispute settlement;"*

(i) *whether the TSP's trust service has been assessed to be conformant with the trust service policy, and if so through which conformity assessment scheme;"*

(j) *the TSP's contact information; and"*

(k) *any undertaking regarding availability."*

- *"**REQ-6.2-03**: Subscribers and parties relying on the trust service shall be informed of precise terms and conditions, including the items listed above, before entering into a contractual relationship."*
- *"**REQ-6.2-04**: Terms and conditions shall be made available through a durable means of communication."*
- *"**REQ-6.2-05**: Terms and conditions shall be available in a readily understandable language."*
- *"**REQ-6.2-06**: Terms and conditions may be transmitted electronically."*

Os requisitos ETSI 319 411-1, em particular a secção 5.2 "Certifications Practice Statement requirements", são os seguintes:

- *"**OVR-5.2-02**: The TSP's CPS should be structured in accordance with IETF RFC 3647 [i.3]"*
- *"**OVR-5.2-03**: The TSP's CPS shall include the complete CA hierarchy, including root and subordinate CA's"*
- *"**OVR-5.2-04**: The TSP's CPS shall include the signature algorithms and parameters employed."*
- *"**OVR-5.2-05**: The TSP shall publicly disclose its CPS through an online means that is available on a 24x7 basis."*
- *"**OVR-5.2-10**: The TSP's CPS shall specify the practice regarding the use of CA keys for signing certificates, CRLs and OCSP."*

# BIBLIOGRAFIA


Decreto-lei n.º 290-d/99 de 2 de agosto. *Diário da República*, Nº 178/1999, 1999.

Resolução do conselho de ministros n.º 171/2005 - aprova a criação da entidade de certificação electrónica do estado (ecee). *Diário da República*, Nº211/2005, 2005.

Regulamento (ue) nº910/2014 do parlamento europeu e do conselho de 23 de julho de 2014 relativo identificacao eletronica e aos servicos de confianca para as transacoes eletronicas no mercado interno e que revoga a diretiva 1999/93/ce. *Jornal Oficial da União Europeia*, L257, p. 73, 2014.

Regulamento de execucao (ue) 2015/1502 da comissao de 8 de setembro de 2015 que estabelece as especificações técnicas mínimas e os procedimentos para a atribuição dos níveis de garantia dos meios de identificação eletrónica, nos termos do artigo 8.o, n.o 3, do regulamento (ue) n.o 910/2014 do parlamento europeu e do conselho relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno. *Jornal Oficial da União Europeia*, L235, p. 7, 2015.

Regulamento (ue) nº2016/679 do parlamento europeu e do conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a diretiva 95/46/ce (regulamento geral sobre a proteção de dados). *Jornal Oficial da União Europeia*, L119, p. 1, 2016.

Lei n.º 46/2018 de 13 de agosto estabelece o regime jurídico da segurança do ciberespaço, transpondo a diretiva (ue) 2016/1148, do parlamento europeu e do conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a união. *Diário da República*, Nº155/2018, 2018.

Decreto-lei n.º 12/2021 de 9 de fevereiro. *Diário da República*, Nº 27/2021, 2021.

*Política de Certificado de Validação on-line OCSP emitido pela EC AuC*. Cartão de Cidadão, 2019.

*Declaração de Divulgação de Princípios*. Cartão de Cidadão, 2020a.

*Declaração de Práticas de Certificação da EC de Autenticação do Cartão de Cidadão*. Cartão de Cidadão, 2020b.

*Declaração de Práticas de Certificação da EC de Assinatura Digital Qualificada do Cartão de Cidadão*. Cartão de Cidadão, 2020c.

*Declaração de Práticas de Certificação da EC do Cartão de Cidadão*. Cartão de Cidadão, 2020d.

*Declaração de Práticas de Validação Cronológica*. Cartão de Cidadão, 2020e.

*Declaração de Práticas de Certificação Entidade Certificadora Eletrónica Raiz*. Cartão de Cidadão, 2020f.

*Política de Certificado de Assinatura Digital Qualificada*. Cartão de Cidadão, 2020g.

*Política de Certificado da EC de Autenticação do Cartão de Cidadão*. Cartão de Cidadão, 2020h.

*Política de Certificado de Entidade Certificadora de Documentos*. Cartão de Cidadão, 2020i.

*Política de Certificado da EC do Cidadão*. Cartão de Cidadão, 2020j.

*Política de Certificado de Validação Cronológica*. Cartão de Cidadão, 2020k.

*Política de Certificado de Validação on-line OCSP emitido pela EC do Cidadão*. Cartão de Cidadão, 2020l.

*Política de Certificado de Validação on-line OCSP emitido pela EC AsC*. Cartão de Cidadão, 2020m.

CEN TS 419 261. Security requirements for trustworthy systems managing certificates and time-stamps. Standard, European Committee for Standardization, March 2015.

*Declaração de Práticas de Certificação da EC de Chave Móvel Digital de Assinatura Qualificada do Cartão de Cidadão*. Chave Móvel Digital, 2018a.

*Política de Certificado de Chave Móvel Digital de Assinatura Digital Qualificada do Cartão de Cidadão*. Chave Móvel Digital, 2018b.

Common Criteria Part 1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model. Standard, International Organization for Standardization, April 2017.

Common Criteria Part 2. Common Criteria for Information Technology Security Evaluation - Part 1: Part 2: Security functional components. Standard, International Organization for Standardization, April 2017.

Common Criteria Part 3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components. Standard, International Organization for Standardization, April 2017.

Common Vulnerability Scoring System. Common Vulnerability Scoring System version 3.1 - Specification Document. Standard, FIRST.

Electronic Crime Scene Investigation: A Guide for First Responders. Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition. Special report, National Institute of Justice.

EN 1143-1:2019. Secure storage units - Requirements, classification and methods of test for resistance to burglary - Part 1: Safes, ATM safes, strongroom doors and strongrooms. Standard, European Committee for Standardization, April 2019.

*Política de Certificados do SCEE e Requisitos Mínimos de Segurança*. Entidade de Certificação Electrónica do Estado, 2016.

ETSI EN 319 401. Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers. Standard, European Telecommunications Standards Institute, April 2018.

ETSI EN 319 411-1. Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements. Standard, European Telecommunications Standards Institute, April 2018.

ETSI EN 319 411-2. Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates. Standard, European Telecommunications Standards Institute, April 2018.

ETSI EN 319 421. Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps. Standard, European Telecommunications Standards Institute, March 2016.

ETSI EN 319 422. Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles. Standard, European Telecommunications Standards Institute, March 2016.

*Security guidelines on the appropriate use of qualified electronic signatures*. European Union Agency For Network And Information Security, 2016.

FIPS PUB 140-2. Security Requirements For Cryptographic Modules. Standard, National Institute of Standards an Technology, May 2001.

ISO 31000:2018(E). Risk management — Guidelines. Standard, International Organization for Standardization, Geneva, Switzerland, February 2018.

ISO/IEC 27000:2018(en). Information technology — Security techniques — Information security management systems — Overview and vocabulary. Standard, International Organization for Standardization, Geneva, Switzerland, February 2018.

ISO/IEC 27001:2005(E). Information technology — Security techniques — Information security management systems — Requirements. Standard, International Organization for Standardization, Geneva, Switzerland, October 2005.

ISO/IEC 27001:2013(E). Information technology — Security techniques — Information security management systems — Requirements. Standard, International Organization for Standardization, Geneva, Switzerland, October 2013.

ISO/IEC 27002:2013(E). Information technology — Security techniques — Code of practice for information security controls. Standard, International Organization for Standardization, Geneva, Switzerland, October 2013.

ISO/IEC 27035-1:2020(E). Information technology – Security techniques – Information security incident management — Part 1: Principles of incident management. Standard, International Organization for Standardization, Geneva, Switzerland, 2020.

ISO/IEC 27035-2:2020(E). Information technology – Security techniques – Information security incident management — Part 2: Guidelines to plan and prepare for incident response. Standard, International Organization for Standardization, Geneva, Switzerland, 2020.

ISO/IEC 27035-3:2020(E). Information technology — Security techniques – Information security incident management — Part 3: Guidelines for ICT incident response operations. Standard, International Organization for Standardization, Geneva, Switzerland, 2020.

ITU-T Recomendation x.509. Information technology — Open systems interconnection - The Directory: Public Key and attribute certificate frameworks. Standard, International Telecommunication Union, November 2008.

Richard Murch. *The Software Development Lifecycle - A Complete Guide*. 2012.

NIST Special Publication 800-160. Systems Security Engineering - Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. Standard, National Institute of Standards an Technology, November 2016.

NIST Special Publication 800-55. Performance Measurement Guide for Information Security. Standard, National Institute of Standards an Technology, July 2008.

Norma Técnica - D 02. Requisitos Mínimos de Segurança Física de Instalações de Entidades Certificadores. Norma técnica, Gabinete Nacional de Segurança, September 2008.

RFC 2986. PKCS #10: Certification Request Syntax Specification. Standard, Internet Engineering Task Force, November 2000.

RFC 3161. Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) . Standard, Internet Engineering Task Force, August 2001.

RFC 3647. Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. Standard, Internet Engineering Task Force, November 2003.

RFC 5280. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Standard, Internet Engineering Task Force, May 2008.

RFC 6960. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. Standard, Internet Engineering Task Force, June 2013.

A presente dissertação foi proposta pela empresa *DeviseFutures Lda.*