NOVA IMS Information Management School

MGI

Mestrado em Gestão de Informação
Master Program in Information Management

Plano de Implementação da Norma ISO/IEC 27001 no INEM

(*) **INEM-Instituto Nacional de Emergência Médica, I. P.**

Carlos Manuel Rosa Correia

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre em Gestão de Informação

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

Plano de Implementação da Norma ISO/IEC 27001:2013 na organização INEM-Instituto Nacional de Emergência Médica, I. P.

por

Carlos Manuel Rosa Correia

Dissertação apresentada como requisito parcial para a obtenção do grau de Mestre em Gestão de Informação, Especialização em Gestão de Sistemas e Tecnologias de Informação

Orientador: Professor Doutor Vitor Manuel Pereira Duarte dos Santos

Lisboa, Novembro de 2016

DEDICATÓRIA

"O propósito determina o que é certo, marca o caminho e alimenta a energia no movimento."

(Ralph Smedley)

AGRADECIMENTOS

No decorrer deste trabalho, foram desenvolvidas várias dinâmicas de grupo, reuniões formais de trabalho, muitas sugestões de colegas de trabalho e amigos. A contribuição foi muito positiva e, por isso, quero deixar expresso o meu reconhecimento a todos aqueles que, direta ou indiretamente, contribuíram para a realização deste trabalho.

Ao Instituto Nacional de Emergência Médica (INEM,I.P.), nomeadamente ao Conselho Diretivo e ao Gabinete de Sistemas e Tecnologias de Informação (GSTI), pela aprovação e facilidades concedidas para o desenvolvimento deste trabalho. Ao Dr. José Ferreira e à Engª Anabela Gonçalves um forte agradecimento pela disponibilidade e pela forma solidária e empenhada com que colaboraram. A todos os elementos da equipa do GSTI que me acolheram com simpatia e afeto e, sempre estiveram disponíveis dando um contributo relevante na concretização deste trabalho. A todos e, sem exceção, o meu muito obrigado.

Ao Professor Doutor Vitor dos Santos, meu orientador, registo um especial agradecimento pelo apoio, orientação, colaboração, amizade e disponibilidade, não devendo ainda ficar esquecida a oportunidade que me deu em concretizar este trabalho.

À minha família, pela paciência e pelo apoio que me deu durante a realização deste trabalho.

A todos os outros que, não estão aqui referidos, contribuíram de alguma forma para que fosse possível realizar este trabalho.

Muito obrigado a todos!

RESUMO

Esta dissertação compreende a preparação para a implementação do Sistema de Gestão de Segurança da Informação (SGSI) baseado nas orientações da família das normas ISO/IEC 27000 e foi desenvolvido em ambiente organizacional. No desenvolvimento deste plano de implementação fez parte um conjunto de processos específicos, de modo a responder aos requisitos da norma NP ISO/IEC 27001:2013 e, atendendo à amplitude do seu âmbito e caraterização da organização onde incidiu este trabalho, foram adicionalmente e particularmente adotados *frameworks* em uso interno pela organização.

Nesta dissertação é apresentado um enfoque teórico na caracterização de um Sistema de Gestão de Segurança da Informação (SGSI) e a sua relevância no contexto da dinâmica da organização, do seu impacto com a estrutura dos sistemas e das tecnologias de informação que, continuamente obrigam a gerar novos desafios à segurança da informação. É dado destaque ao Framework documental dos normativos necessários na gestão da segurança da informação e a estrutura de recursos e responsabilidades para garantir a implementação e a continuidade de um SGSI.

Através do levantamento dos processos organizacionais, da análise documental, com entrevistas semiestruturadas e por observação direta procedeu-se a uma avaliação da situação atual em resposta aos requisitos de controlo preconizados pela ISO/IEC 27001. Em adicional, é apresentado o processo de gestão de riscos de segurança da informação como instrumento facilitador na análise, avaliação e controlo dos fatores de risco organizacionais e que teve como resultado a realização da matriz de risco evocando o tratamento a aplicar ao risco em causa.

O resultado final deste trabalho, representa a ”primeira pedra” para a construção do sistema de gestão de segurança da informação. É apresentada através da “Declaração de Aplicabilidade” um conjunto de propostas subdivididas em cinco eixos de ação: Organizacional, Pessoal, Tecnológico, Físico e Ambiental, Legal & Regulatório. Para cada eixo de ação estão definidas medidas específicas a implementar. As medidas apresentadas - ações a realizar, é o resultado do vasto trabalho realizado a montante, em que permitiu analisar e avaliar qual o atual estado de maturidade e capacidade processual, tecnológica e de recursos e, deste modo, documentar, definir e estruturar as linhas orientadoras para implementar um sistema de gestão de segurança da informação, de acordo com os requisitos da ISO/IEC 27001 e 27002, em consonância com os objetivos estratégicos da instituição INEM e com o âmbito e alcance previamente definidos, na sua primeira etapa.

PALAVRAS-CHAVE

Gestão de Segurança da Informação; Norma ISO 27001; Políticas e Procedimentos; Processo de Gestão do risco

ABSTRACT

This dissertation comprises the preparation to the implementation of the Information Security Management System (ISMS) based on the orientation of the ISO/IEC 270000 family standards and was developed in organizational environment. In the development of this implementation plan, a set of specific processes were part of, in order to meet the requirements of the NP ISO/IEC 27001:2013 standard and, giving the breath of its scope and characterization of the organization where this work was focused, were additionally and particularly adopted frameworks for internal use by the organization.

This dissertation presents a theoretical approach in the characterization of an Information Security Management System (ISMS) and its relevance in the context of the dynamics of the organization, its impact with the systems infrastructures and the information technologies that require, continually, the generation of new challenges to the information security. Emphasis is given to the documentary Framework of the necessary standards on the information security management and the resources structure and responsibilities to ensure the implementation and permanency of an ISM.

Through the investigation of organizational processes, documentation analysis, semi-structured interviews and direct observation, an evaluation of the current situation in response to the control requirements suggested by the ISO/IEC 27001 was executed. Additionally, a process of managing security information risks is presented as a tool to facilitate the analysis, evaluation and control of the organizational risk factors resulting in the realization of a risk matrix that evokes the treatment to be applied to the considered risk.

The final result of this dissertation represents the “first stone” to the construction of the Information Security Management System (ISMS). It is presented, through the “Statement of Applicability” a set of proposals divided into five action areas: Organizational, Personal, Technological, Physical and Environmental, Legal & Regulatory. For each action areas a set of specific measures are defined to be implemented. The presented measures – actions to be taken, are the result of an extensive work, which allowed to analyze and evaluate the current maturity state and also procedural, technological and resources capacity, thus, documenting, defining and structuring the guiding lines to implement an Information Security Management System (ISMS), according to the ISO/IEC 27001 and 27002 requirements, in accordance with the strategical objectives of the National Portuguese Institute of Medical Emergency and with the scope and range previously defined, in its first stage.

KEYWORDS

Information Security Management; Standard ISO 27001; Information Security Policies and Procedures; Risk Management Process

Histórico de Alterações

Data	Versão	Descrição	Autor
10/04/2016	**1.0**	**Criação do Documento**	**Carlos Correia**
23/06/2016	**2.0**	**Revisão estrutural**	**Carlos Correia**
15/09/2016	**3.0**	**Revisão de conteúdo**	**Carlos Correia**
20/10/2016	**4.0**	**Revisão final**	**Carlos Correia**

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

LISTA DE SIGLAS E ACRÓNIMOS

ANPC	Autoridade Nacional de Proteção Civil
CD	Conselho Diretivo
CERT	*Computer Security Incident Response Team*
CISO	*Chief Information Officer*
CobiT	*Control Objectives for Information and related Technology*
CODU	Centros de Orientação de Doentes Urgentes
DGS	Direção-Geral de Saúde
eSIS	ecossistema do Sistemas de Informação da Saúde
GM	Gabinete Marketing e Comunicação
GQ	Gabinete de Qualidade
IEC	*International Electrotechnical Commission*
INEM	Instituto Nacional de Emergência Médica
IPQ	Instituto Português da Qualidade
ISIRT	*Information Security Incident Response Team*
ISO	*International Organization for Standardization*
itSMF	*the IT Service Management Forum*
LAN	*Local Area Network*
NP	Norma Portuguesa
OE	Objetivo Estratégico
QUAR	Quadro de Avaliação e Responsabilização
SGIQAS	Sistema de Gestão Integrada da Qualidade, Ambiente e Segurança
SGSI	Sistema de Gestão de Segurança da Informação
SI	Sistema de Informação
SIEM	Serviço Integrado de Emergência Médica
SIRESP	Sistema Integrado das Redes e Segurança de Portugal
SNS	Serviço Nacional de Saúde
SPMS	Serviços Partilhados do Ministério da Saúde
SWOT	*Strengths, Weakness, Opportunities and Threats*
TIC	Tecnologias de Informação e Comunicação
VoIP	*Voice over Internet Protocol*
WAN	*Wide Area Network*

1. INTRODUÇÃO

O objetivo principal deste trabalho é apresentar o Plano de Implementação para suporte na construção do Sistema de Gestão da Segurança da Informação (SGSI) na organização do INEM,I.P. – Instituto Nacional de Emergência Médica, segundo os requisitos da Norma NP ISO/IEC 27001:2013.

Este plano para a implementação da norma NP ISO/IEC 27001:2013 está de acordo com os conceitos e requisitos especificados nesta norma e foi elaborado para facilitar uma implementação satisfatória de um SGSI e compreender de forma mais próxima os requisitos para estabelecer, implementar, manter e melhorar de forma contínua um Sistema de Gestão de Segurança da Informação dentro do contexto da organização do INEM. A realização deste plano é de extrema relevância, importância e utilidade no processo de implementação da norma ISO/IEC 27001, sendo um dos principais *deliverables* na fase de planeamento. Assim, este trabalho teve como principais ações:

Levantamento dos principais processos na organização e a sua integração suportada pelos atuais sistemas e tecnologias de informação, realizando uma classificação dos ativos da informação do INEM, com base na sua importância face aos objetivos estratégicos e operacionais e o enquadramento com a confidencialidade, integridade e disponibilidade necessárias.

A identificação, análise e avaliação dos riscos de segurança da informação permitiu elaborar a matriz de risco e as respetivas diretrizes para o tratamento de cada um dos riscos, nas suas diferentes dimensões. Na obtenção de evidências na aplicabilidade dos requisitos preconizados na norma ISO/IEC 27001, fez-se uma análise detalhada e completa a todos os controlos de referência e, face aos objetivos de controlo, apurou-se qual o atual nível de maturidade e de capacidade na aplicabilidade das boas práticas. Esta avaliação, através do modelo de maturidade, permite orientar a organização a subir de nível e a melhorar de forma incremental atividades na Gestão do Risco e Segurança.

As medidas apresentadas – ações a realizar, estão subdivididas em cinco eixos de ação – Organizacional, Físico e Ambiental, Pessoal, Tecnológico, de Conformidade & Regulação - proporcionando uma visão geral mas, efetiva do que precisa de ser feito, porque precisa de ser feito e como precisa ser feito para implementar um Sistema de Gestão de Segurança da Informação.

1.1. ÂMBITO E CAMPO DE APLICAÇÃO

Nas organizações do setor publico ou privado de várias dimensões, a confiança, a transparência e as boas práticas são ativos que proporcionam uma vantagem competitiva; razão pela qual a maioria das organizações pretendem obter várias certificações ISO (*the International Organization for Standardization*) podendo assim destacar o seu alinhamento prudente às boas práticas definidas nos *standards* internacionais.

A organização INEM I.P. na sua gestão estratégica e operacional é um dos exemplos da aplicabilidade de instrumentos de Gestão da Qualidade pelo que "a revisão e melhoria contínua dos processos permite que a organização mantenha um padrão de avaliação sistemática dos seus procedimentos." (INEM_Plano Estratégico 2014/2016 versão junho 2014, p.42).

Sabemos hoje que, para uma organização, as operações relacionadas com a gestão dos clientes ou utentes e o relacionamento com os seus parceiros são fatores críticos de sucesso. Toda a informação processada, armazenada e partilhada na gestão funcional e operacional de uma organização é um ativo da máxima importância. Seja qual for a forma apresentada (impressa ou escrita em papel, armazenada em dispositivos eletrónicos, transmitida pelo correio, apresentada em filmes e fotos ou falada em conversas) e o meio através do qual a informação é partilhada ou armazenada, "são informações valiosas para a gestão de uma organização e, consequentemente, merecem ou exigem proteção contra vários perigos." (ISO/IEC 27002:2013, p.vi)

Desta forma, a segurança da informação torna-se imperativa. Um programa de gestão efetivo de riscos de segurança da informação reduz a probabilidade de riscos, protegendo a organização contra ameaças e vulnerabilidades e reduzindo o impacto dos seus ativos.

Uma das ferramentas possíveis para este imperativo é a implementação de um Sistema de Gestão de Segurança da Informação (SGSI) assente no *standard* internacional ISO/IEC 27001:2013 em que "esta Norma foi preparada para proporcionar os requisitos para estabelecer, implementar, manter e melhorar de forma contínua um sistema de gestão de segurança da informação." (IPQ NP 27001:2013, p.5)

Este trabalho, pretende de forma detalhada e em conjunto com os atuais processos de gestão da instituição do INEM,I.P. (doravante INEM), identificar os requisitos de segurança da informação, definidos na Norma ISO/IEC 27001:2013, através da análise e avaliação dos riscos de segurança da informação.

1.2. OBJETIVO GERAL

O objetivo geral deste trabalho é realizar uma análise e avaliação dos riscos de segurança da informação e avaliar o nível de maturidade e de capacidade da aplicabilidade dos processos, com base na especificação de requisitos e dos controlos de referência listados na Norma ISO/IEC 27001:2013.

O resultado final deste trabalho, através da análise e avaliação dos riscos permitirá documentar, determinar e direcionar ações de melhoria na gestão funcional e operacionais apropriadas, mas também, adequadas à dimensão e estrutura da organização. Definir quais as prioridades para a gestão dos riscos de segurança da informação que " é conseguida através da implementação de um conjunto adequado de controlos, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware*"[1].

[1] *Information Security is achieved by implementing suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions.* (ISO/IEC 27002:2013 p.vi)

1.3. OBJETIVOS ESPECÍFICOS

No ponto de vista da organização do INEM, os objetivos específicos são:

i. Realizar a análise e avaliação dos riscos de segurança da informação, com base na especificação de requisitos e dos controlos de referência listados na NP ISO/IEC 27001:2013[2].

ii. Determinar e direcionar ações de melhoria na gestão funcional e operacional, adequadas à dimensão e estrutura da organização.

iii. Produzir uma "Declaração de Aplicabilidade que contenha os controlos necessários e a justificação para as inclusões dos controlos, estejam eles implementados ou não, bem como a justificação para as exclusões dos controlos especificados no Anexo A." (IPQ, NP ISO/IEC 27001 Clausula 6.1.3d, p.9)

iv. Dar resposta ao objetivo estratégico (OE) na perspetiva Processos, definido no Plano Estratégico 2014/2016 do INEM – OE 5: Implementar instrumentos de Gestão da Qualidade. Este objetivo estratégico é um dos dez objetivos "identificados no presente Plano foram sistematizados para dar resposta às grandes linhas de ação estratégica, alinhados nas quatro perspetivas Clientes, Processos, Inovação e Aprendizagem, Financeira." (INEM_Plano Estratégico 2014/2016 versão junho 2014, p.42).

v. Com base no ponto iii) e iv) o Gabinete de Sistemas e Tecnologias de Informação (GSTI) irá aplicar operacionalmente a 1ª fase do processo de certificação, como indicador de desempenho do Quadro de Avaliação e Responsabilização QUAR GSTI OE 6: Implementar instrumentos de Gestão da Qualidade, de modo a promover a segurança aos cidadãos.

1.4. MOTIVAÇÃO E JUSTIFICAÇÃO

Desde o primeiro momento da abordagem do propósito para a realização deste trabalho que os responsáveis do GSTI/INEM e eu próprio, sentimos uma forte motivação para a sua realização, sabendo *a priori* que não iria ser tarefa fácil, face à dimensão da organização e a sua estrutura de gestão e meios disponíveis.

Esta motivação foi de igual modo replicada pela NOVA IMS, que desde no primeiro momento, reconheceu o mérito e interesse do projeto e acompanhou de forma efetiva a realização e progressão deste trabalho.

Aquando da reunião de *kick-off* foram evocados os seguintes vetores motivacionais:
O Sistema de Gestão de Segurança da Informação a implementar será uma parte do sistema de gestão organizacional abrangente na organização INEM. Para além de se reconhecer a sua dimensão, este será exequível, finalizado *in time* e ambicioso. A sua aplicação tem forçosamente impacto nos objetivos e exigências da organização e nos procedimentos adotados; visando a assegurar que as

[2] Por ser mais fácil a sua leitura, optou-se pela denominação ISO/IEC 27001; sendo que no âmbito deste trabalho, esta denominação é sempre referente à NP ISO/IEC 27001:2013.

melhores práticas serão aplicadas e documentadas, reforçando e melhorando a organização continuadamente ao longo do tempo.

1.5. ORGANIZAÇÃO DO DOCUMENTO

Nesta secção apresenta-se a organização do presente trabalho e a sintetização do conteúdo de cada capítulo que se encontram estruturados, na seguinte forma:

O primeiro capítulo, apresenta o enquadramento do projeto na perspetiva técnica e organizacional. Estão enunciados os objetivos gerais e os objetivos específicos, circunscrevendo e justificando as razões para a realização deste projeto.

No capítulo 2 referencia-se a família da norma ISO/IEC 27000, o enquadramento da norma ISO/IEC 27001 e seus benefícios na sua aplicabilidade; a interligação com outros *standards* como instrumentos de apoio e suporte no processo de desenvolvimento e implementação.

O capítulo 3 contém a revisão da literatura, onde se apresenta uma revisão conceptual de um SGSI, assim como, a caracterização que um sistema de gestão de segurança de informação deve garantir no adequado funcionamento e continuidade operacional e de negócio da organização, minimizando os riscos. Pela sua importância, justificação e vantagens na implementação de um sistema de segurança da informação numa organização, evoca-se a importância e o comprometimento que a gestão de topo deve demonstrar na aplicabilidade e de melhoria contínua.

Capítulo 4 refere a metodologia aplicada no desenvolvimento deste trabalho, evocando as técnicas usadas na recolha e análise de dados, assim como, o desenho do modelo processual para a realização do plano de implementação do SGSI.

No capítulo 5 fazemos uma breve apresentação da organização estrutural do INEM, onde este trabalho tem a sua principal focalização.

O capítulo 6 é parte integrante da análise realizada para a implementação do sistema de gestão de segurança da informação no INEM, com a definição do âmbito e alcance pretendido, a identificação e descrição das ferramentas necessárias ao processo de análise, avaliação e tratamento do risco.

Capítulo 8 apresenta a Declaração de Aplicabilidade que é um dos principais *deliverables* da fase de planeamento, onde se apresenta uma visão geral mas, efetiva do que precisa de ser feito, porque é que precisa de ser feito e como precisa de ser feito.

Finalmente, o capítulo 9, apresenta as conclusões consideradas relevantes na execução deste trabalho, no ponto de vista pessoal, profissional e para a organização onde incidiu a componente prática, bem como as limitações do projeto proposto e sugestões para futuras investigações.

2. A NORMA ISO/IEC 27000 E SUA INTERLIGAÇÃO COM OUTRAS NORMAS

2.1. A FAMÍLIA DA NORMA ISO/IEC 27000

A ISO (*the International Organization for Standardization*) e a IEC (*the International Electrotechnical Commission*) desenvolveram a família das normas **ISO/IEC 27000**[3] com o principal objetivo de ajudar as organizações a manter os seus ativos de informação, de forma segura, tais como, informações financeiras, propriedade intelectual, dados pessoais dos colaboradores, dos clientes, dos utentes ou informação que foi confiada a terceiras entidades.

Estas normas fornecem diretrizes na introdução, implementação e manutenção do SGSI a aplicar numa organização. Estas recomendações têm também o propósito de fornecer uma base comum no desenvolvimento de práticas e técnicas vocacionadas à segurança organizacional e estabelecer a confiança nos relacionamentos *intra* e *inter* organização.

Desta família faz parte um conjunto de normas especificando quais os requisitos necessários de um sistema de gestão de segurança da informação, a gestão dos riscos, métricas e diretrizes de orientação para a implementação de um sistema de gestão de segurança da informação.

Em síntese, a família de normas ISO/IEC 27000, inclui normas para:

a) definir os requisitos para um SGSI;
b) prestar apoio direto, orientação e / ou interpretação detalhada para o processo global de estabelecer, implementar , manter e melhorar um SGSI ;
c) fornecedor orientações sectoriais e específicas para SGSI; e
d) endereçar diretrizes para realizar auditoria e avaliação de conformidade para SGSI.

A lista de normas da família ISO/IEC 27000, é a seguinte (ISO/IEC 27000:2014, p.3):

- — ISO/IEC 27000, *Information security management systems — Overview and vocabulary*
- — ISO/IEC 27001, *Information security management systems — Requirements*
- — ISO/IEC 27002, *Code of practice for information security controls*
- — ISO/IEC 27003, *Information security management system implementation guidance*
- — ISO/IEC 27004, *Information security management — Measurement*
- — ISO/IEC 27005, *Information security risk management*
- — ISO/IEC 27006, *Requirements for bodies providing audit and certification of information security management systems*
- — ISO/IEC 27007, *Guidelines for information security management systems auditing*
- — ISO/IEC TR 27008, *Guidelines for auditors on information security controls*

[3] **ISO / IEC 27000:2014** ***Information Technology – Security Techniques – Information security management systems – Overview and vocabulary.*** Esta terceira edição, anula e substitui a anterior, editada em 2012. A primeira edição (ISO/IEC 27000:2009) veio substituir a norma emitida pela British Standard BS7799-2, publicada em 2002.

- — ISO/IEC 27010, *Information security management for inter-sector and inter-organizational communications*
- — ISO/IEC 27011, *Information security management guidelines for telecommunications organizations based on* ISO/IEC 27002
- — ISO/IEC 27013, *Guidance on the integrated implementation of* ISO/IEC 27001 *and* ISO/IEC 20000-1
- — ISO/IEC 27014, *Governance of information security*
- — ISO/IEC TR 27015, *Information security management guidelines for financial services*
- — ISO/IEC TR 27016, *Information security management — Organizational economics*
- — ISO 27799:2008, *Health informatics — Information security management in health using* ISO/IEC 27002
- — ISO/IEC 27034:2011, *Information technology - Security techniques — Application security*

De salientar que deste conjunto / série de normas, a única passível a certificação é a norma ISO/IEC 27001, sendo as outras complementos de auxílio à certificação em áreas específicas de atividade.

A **ISO/IEC 27001:2013** ***Information Technology – Security Techniques – Requirements*** é o padrão mais conhecido na família ISO/IEC 27000, fornecendo os requisitos para um sistema de gestão de segurança da informação. Esta norma foi elaborada com o propósito de disponibilizar os "requisitos para estabelecer, implementar, operar, monitorizar, analisar criticamente, manter e melhorar de forma contínua um Sistema de Gestão de Segurança da Informação (SGSI), dentro do contexto da organização. " (NP ISO/IEC 27001:2013¸p.6)

Com base nas boas práticas de gestão da informação, a **ISO/IEC 27002:2013**[4] ***Information Technology – Security Techniques – Code of practice for information security controls***, estabelece as diretrizes e princípios gerais, para analisar os requisitos de cada um dos controlos definidos na ISO/IEC 27001:2013, levando em consideração o ambiente dos riscos de segurança da informação da organização.

Esta norma está estruturalmente desenhada para ser usada por organizações que pretendam:

1. selecionar controlos dentro do processo de implementação de um Sistema de Gestão de Segurança da Informação com base na ISO/IEC 27001;

2. implementar controlos de segurança da informação geralmente aceitos;

3. desenvolver suas próprias diretrizes de gestão de segurança da informação.

[4] A segunda edição desta norma é datada em 2013-10-01. Esta ultima edição ISO/IEC 27002:2013 substitui a primeira edição ISO/IEC 27002:2005, editada em outubro de 2005. Esta primeira edição veio substituir a norma emitida pela British Standard BS7799-1, publicada em 2002.

No entanto, é de realçar que, ao contrário do que acontece com a norma ISO/IEC 27001, que tem carácter obrigatório no contexto de um eventual processo de certificação, a norma ISO/IEC 27002 constitui um mero guia (*code of practice*) com um vasto conjunto de sugestões de controlos de segurança, integrados numa visão muito ampla sobre a organização e a sua gestão da segurança da informação.

A **ISO/IEC 27003:2010** ***Information technology–Security techniques–Information security management system implementation*** incide sobre os aspetos críticos necessários para o sucesso do desenho e implementação de um SGSI, em conformidade com a norma ISO/IEC 27001:2013.

A ISO/IEC 27003:2010 descreve o processo de especificação e o desenho de um SGSI, desde a sua conceção à produção dos planos de implementação, ou seja, fornece a orientação como planear um projeto de SGSI, resultando o plano final de implementação do SGSI.

A **norma ISO/IEC 27004:2009** ***Information technology –Security techniques – Measurement*** fornece um guia com orientações sobre o desenvolvimento e a utilização de métricas e medição, com a finalidade de avaliar a eficácia de um sistema de gestão de segurança da informação já implementado com os controlos ou grupos de controlos especificados na norma ISO/IEC 27001:2013.

A norma **ISO/IEC 27005:2011 -** ***Information security risk management*** contém as diretrizes para a gestão de riscos de segurança da informação. Esta norma suporta os conceitos gerais especificados na norma ISO/IEC 27001:2013 e está desenhada para ajudar na implementação de um sistema de gestão de segurança da informação com base na abordagem de gestão do risco.

ISO/IEC 27005:2011 é aplicável a todos os tipos de organizações (por exemplo, empresas comerciais, agências governamentais, organizações sem fins lucrativos) que pretendem gerir os riscos que possam comprometer a segurança da informação da organização.

Atendendo ao âmbito deste trabalho, não se apresenta as restantes normas da família 27000. Em resumo a lista de normas da família ISO/IEC 27000 aplicadas neste projeto é a seguinte:

- — ISO/IEC 27000, *Information security management systems — Overview and vocabulary*
  Vocabulário e definições a serem utilizadas pelas restantes normas

- — ISO/IEC 27001, *Information security management systems — Requirements*
  Define os requisitos para a implementação de um SGSI

- — ISO/IEC 27002, *Code of practice for information security controls*
  Define as boas práticas para a gestão da segurança da informação

- — ISO/IEC 27003, *Information security management system implementation guidance*
  Guia para a implementação de um SGSI

- — ISO/IEC 27004, Information security management — Measurement
  Define métricas e meios de medição para avaliar a eficácia de um SGSI

- — ISO/IEC 27005, Information security risk management
  Define linhas de orientação para a gestão do risco da segurança da informação

2.2. ENQUADRAMENTO DA NORMA NP ISO/IEC 27001:2013

A norma NP ISO/IEC 27001:2013[5] tem tradução na língua portuguesa, sendo a primeira norma portuguesa de segurança de informação, editada pelo IPQ em 2013-10-14. A motivação de editar esta norma como Norma Portuguesa foi "promover a implementação da ISO/IEC 27001 em Portugal, sabendo que alguns países com forte implementação desta norma e possuem traduções nacionais (por exemplo, Japão, Espanha, Brasil); disponibilizar uma norma portuguesa que possa ser referenciada em iniciativas de conformidade e padronizar a terminologia portuguesa de segurança de informação" (Coelho, 2013).

A norma ISO/IEC 27001 especifica os requisitos referentes a um Sistemas de Gestão de Segurança da Informação, permitindo que as organizações avaliem os seus riscos e implementem os procedimentos necessários para a preservação da confidencialidade, integridade e disponibilidade da informação. Tem como principal objetivo impedir que a informação seja utilizada por terceiros não desejados ou perdida de forma irremediável.

Para além da interligação existente entre esta norma e outras da série 27000, existe um alinhamento explícito com a norma ISO 31000:2013 Gestão do Risco – Princípios e linhas de orientação, onde inclui, os requisitos para a avaliação e tratamento de riscos de segurança da informação à medida das necessidades da organização. Os requisitos definidos na norma ISO/IEC 27001 "são genéricos e pretende-se que sejam aplicáveis a todas as organizações, independentemente do seu tipo, dimensão ou natureza." (NP ISO/IEC 27001:2013, p.6)

A estrutura global da norma ISO/IEC 27001 pode ser apresentada na seguinte forma:

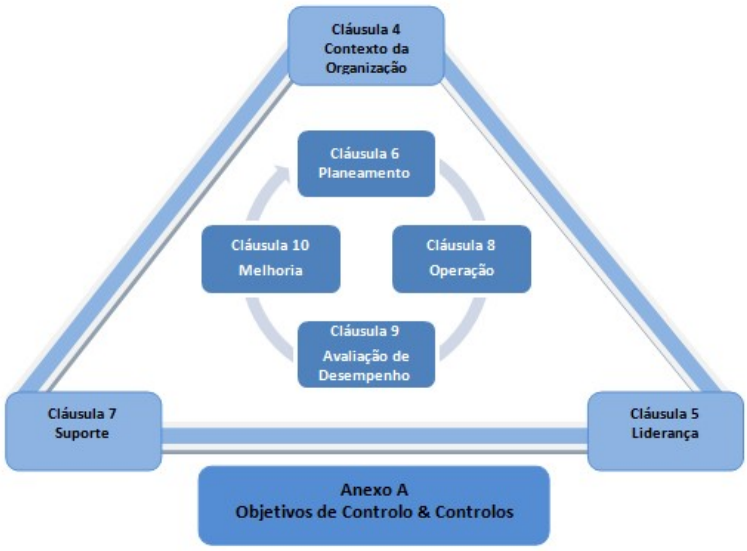


Figura 2-1 Estrutura global da norma ISO/IEC 27001

[5] A norma NP ISO 27001:2013 deriva da versão inglesa ISO/IEC 27001:2013 que por sua vez vem substituir uma primeira edição lançada em 2005. Foi preparada pela comissão técnica de Normalização CT 163 "Segurança em sistemas de informação", cuja coordenação é feita pelo Organismo de Normalização Sectorial, itSMF Portugal (ONS/ITSMF).

A norma ISO/IEC 27001 é composta por duas componentes relativamente distintas:

i. A primeira componente está definida as regras e os requisitos de cumprimento da norma e estes devem ser aplicáveis. “A exclusão de quaisquer dos requisitos especificados nas secções 4 a 10 não é aceitável para uma organização que reivindica a sua conformidade face a esta Norma.” (NP ISO/IEC 27001, p.6)

   Nesta componente são os aspetos explícitos, no seguinte diagrama:

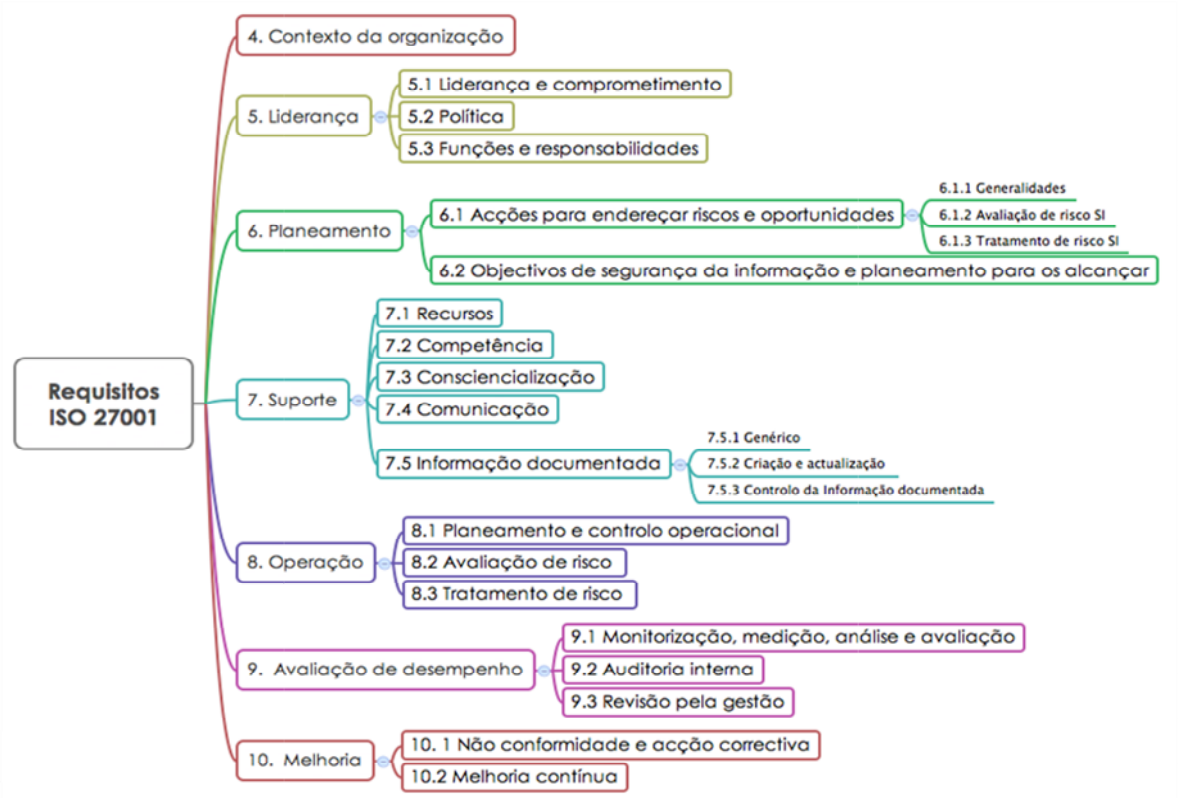


Figura 2-2 Visualização geral dos requisitos genéricos da NP ISO/IEC 27001:2013

ii. A segunda componente da norma, é denominada de Anexo A, que especifica os objetivos de controlo e controlos de referência, denominados de A.5 a A.18 e “são derivados diretamente de e são alinhados com os listados na ISO/IEC 27002:2013 nas secções 5 a 18”. (NP ISO/IEC 27001, p.16)

Estes objetivos de controlo e controlos listados no Anexo A, não são exaustivos e podem ser necessários objetivos de controlo adicionais, ou seja, “as organizações podem conceber controlos, conforme necessário ou identifica-los a partir de qualquer fonte.” (NP ISO/IEC 27001 6.1.3.b), p.16)

Os objetivos de controlo e **controlos de referência**, estão definidos em 8 (oito) **secções**. A ordem das secções não significa o seu grau de importância:

Secção	Descrição do Controlo de referência (Anexo A)	Nº Categorias	Nº Controlos
A.5	Politicas de segurança da informação	1	2
A.6	Organização de segurança da informação	2	7
A.7	Segurança na gestão de recursos humanos	3	6
A.8	Gestão de ativos	3	10
A.9	Controlo de Acessos	4	14
A.10	Criptografia	1	2
A.11	Segurança física e ambiental	2	15
A.12	Segurança de operações	7	14
A.13	Segurança de comunicações	2	7
A.14	Aquisição, desenvolvimento e manutenção de sistemas	3	13
A.15	Relações com fornecedores	2	5
A.16	Gestão de incidentes de segurança da informação	1	7
A.17	Aspetos de segurança da informação na gestão da continuidade do negócio	2	4
A.18	Conformidade	2	8

Figura 2-3 Quadro Geral - Controlos de Referência / Categorias / Controlos

Cada **secção** tem um número de **categorias** principais de segurança da informação.

Cada **categoria** principal contém:

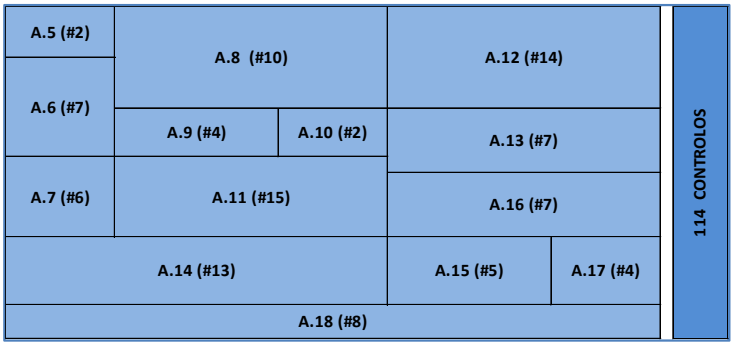
i. um objetivo de controlo que define o que deve ser alcançado

ii. um ou mais controlos que podem ser aplicados para alcançar o objetivo de controlo

Por exemplo:

A **secção A.5** tem uma categoria (A.5.1) e dois controlos (A.5.1.1 e A.5.1.2)

A **secção A.6** tem duas categorias (A.6.1 e A.6.2) e sete controlos



A.*x* identificação da Secção associada ao controlo de referência

#*x* numero de controlos, por Secção

Figura 2-4 Distribuição dos Controlos por Secção

2.3. BENEFÍCIOS NA APLICABILIDADE DA NORMA ISO/IEC 27001

A norma ISO/IEC 27001 é universal para todos os tipos de organizações, sejam elas comerciais, governamentais, com ou sem fins lucrativos, mas transmite flexibilidade na especificação dos requisitos para a implementação de controlos de segurança que podem ser personalizados consoante as necessidades de determinada organização.

Como outras normas do sistema de gestão ISO, a certificação ISO/IEC 27001 é possível, mas não obrigatória. Algumas organizações optam somente por implementar estes *standards* internacionais, a fim de beneficiar das *best practices* que estas normas especificam. "Os responsáveis de Sistemas e Tecnologias de Informação reconhecem, cada vez mais, na adoção de referenciais de boas práticas e de *standards* universais uma mais-valia para o sucesso dos seus projetos." (itSMF-12ª Conferência Anual itSMF Portugal 2015)

Independentemente das organizações se certificarem ou não, a adoção das práticas de gestão documentadas na norma, representa um conjunto de benefícios, nomeadamente:

1. Demonstra um compromisso dos executivos da organização para com a segurança da informação, pois uma das grandes preocupações da atualidade é efetivamente a confiança no tratamento adequado da informação sensível da sua organização.

2. Dotar a organização de ferramentas que demonstre o cumprimento ao Regulamento EU 2016/679 no tratamento e circulação de dados pessoais.

3. Aumenta a fiabilidade e a segurança da informação e dos sistemas, em termos de confidencialidade, disponibilidade e integridade.

4. Garante a realização de investimentos mais eficientes e orientados ao risco, ao invés de investimentos apenas baseados em tendências.

5. Incrementa os níveis de sensibilidade, participação e motivação dos colaboradores da organização para com a segurança da informação.

6. Identifica e endereça de forma continuada oportunidades para melhorias, sendo um processo em melhoria contínua.

7. Aumenta a confiança e satisfação dos clientes, utentes, parceiros, entidades reguladoras e judiciárias, providenciando um elevado compromisso com a proteção da informação, o que representa um nível considerável de conforto para quem interage com entidades que processam e arquivam dados pessoais.

8. A implementação dos controlos provenientes da norma e da análise de risco, melhora o desempenho operacional das organizações, potencia a realização de mais negócios e poder negocial.

No estudo exploratório "Benefícios e fatores condicionadores da obtenção de certificação em gestão da segurança de sistemas de informação", realizado por Silva, D. (2011), refere que "A obtenção de certificações através de normas de Gestão da Segurança de Sistemas de Informação é tida como promotora e evidenciadora dos esforços de proteção do sistema de informação por parte das

organizações.“ A identificação de benefícios e de fatores condicionadores da obtenção de certificação poderá auxiliar os responsáveis organizacionais a antever condições favoráveis ou desfavoráveis para o desenrolar de um processo de certificação sucedido, atuar com vista a gerirem os fatores inibidores da obtenção da certificação, alavancar o processo de certificação em fatores facilitadores e ponderar os possíveis benefícios que a organização poderá recolher com a obtenção da certificação na vertente da Gestão da Segurança de Sistemas de Informação. (Silva, D. 2011).

2.4. A GESTÃO DO RISCO E A NORMA NP ISO 31000:2013

Um dos aspetos preconizados na norma ISO/IEC 27001 é que a organização deve realizar avaliações do risco de segurança da informação, implementar um plano de tratamento do risco e deve manter informação documentada dos resultados do tratamento do risco de segurança da informação. Esta diretiva está associada com a crescente dependência das empresas dos sistemas de informação e tecnologias de informação (Oliveira, 2015) e, que por isso, um sistema de gestão de segurança da informação (SGSI) deve permitir uma eficiente gestão dos riscos de segurança da informação e deve por isso assumir grande importância estratégica nas decisões das organizações.

Como referenciado, a ISO/IEC 27005 contém as diretrizes para a implementação de um sistema de gestão de segurança da informação com base na abordagem de gestão do risco. Contudo, esta norma vai embeber a estrutura aplicacional da norma NP ISO/IEC 31000 Gestão do Risco – Princípios e linhas de orientação[6] que tem como objetivo fornecer princípios e linhas de orientação gerais sobre a gestão do risco, podendo ser aplicada em qualquer tipo de organização e a uma ampla gama de atividades, incluindo estratégias e decisões, operações, processos, funções, projetos, produtos, serviços e ativos.

Em adicional, a ISO/IEC 27005:2008 pretende servir de suporte a alguns conceitos especificados na ISO/IEC 27001 e é estruturada de forma a auxiliar uma implementação satisfatória da segurança da informação baseada numa abordagem de gestão de risco. No entanto, esta norma não apresenta nenhuma metodologia para a gestão de risco da segurança da informação, em específico. Esta opção fica a cargo de cada organização, pois a escolha da metodologia depende, por exemplo, do âmbito do SGSI, contexto da gestão de risco ou do sector/atividade da organização (ISO/IEC 27005, 2008).

[6] A NP ISO 31000:2012 foi preparada pela Comissão Técnica de Normalização CT 180 “Gestão do risco”, cuja coordenação é assegurada pelo Organismo de Normalização Setorial, Associação Portuguesa para a Qualidade (ONS/APQ). Esta Norma é idêntica à versão da ISO 31000:2009 “*Risk management – Principles and guidelines*”.

2.5. O CONTRIBUTO DA NORMA NP EN ISO 9001:2015

A norma NP EN ISO 9001:2015[7] "aplica o enquadramento desenvolvido pela ISO para melhorar o alinhamento entre as suas normas de sistemas de gestão."

Os requisitos do sistema de gestão da qualidade especificados na norma ISO 9001:2015 adota a abordagem por processos, que incorpora o ciclo PDCA (Plan-Do-Check-Act) e o pensamento baseado em risco.

Esta Norma destaca que o pensamento baseado em risco permite a uma organização determinar os fatores suscetíveis de provocar desvios nos seus processos e no seu sistema de gestão da qualidade em relação aos resultados planeados, implementar controlos preventivos para minimizar os efeitos negativos e aproveitar ao máximo as oportunidades que lhe vão surgindo.

A abordagem à gestão do risco por parte da organização e a incorporação da melhoria contínua através do ciclo PDCA permite a uma organização assegurar que os seus processos são dotados com recursos adequados e devidamente geridos e que as oportunidades de melhoria são determinadas e implementadas.

Uma organização que adote a aplicabilidade destes modelos de referência interligados conseguirá retirar partido de um caminho já iniciado podendo aplicar e adequar programas com uma abordagem orientada aos princípios, introduzindo uma visão holística do risco facilitando e contribuindo para a governação e gestão das Tecnologias da Informação e da Comunicação e de uma *framework* para a gestão do risco e da segurança dos ativos de uma organização.

[7] A Norma Europeia EN ISO 9001:2015 foi dada o estatuto de Norma Portuguesa em 2015-10-13 (Termo de Homologação nº132/2015 de 2015-10-13.) A Norma foi preparada pela Comissão Técnica de Normalização CT 80 "Gestão da qualidade e garantia da qualidade", cuja coordenação foi assegurada pelo Organismo de Normalização Setorial, Associação Portuguesa para a Qualidade.

3. SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

3.1. ENQUADRAMENTO

Atualmente, grande parte das empresas/organizações tem as suas áreas produtivas e administrativas de tal forma informatizadas que tornam os sistemas de informação, bem como as tecnologias de informação, instrumentos imprescindíveis. (Carneiro, 2016) Em adicional, estamos a viver tempos excitantes: as tecnologias digitais, dispositivos móveis, o *cloud computing*, o crescimento de dados cooperativos e sua análise e as redes sociais têm trazido enormes benefícios e oportunidades para as organizações. A partilha da informação em tempo real torna-se exigente, face aos objetivos nas organizações e seus gestores na tomada de decisões.

Por este motivo, a informação, os processos de apoio organizacional, os sistemas de informação e as redes são importantes ativos numa organização. Isto é especialmente importante se considerarmos que muitas das vezes, devido à sua elevada criticidade, a informação deve ter garantias quanto à sua confidencialidade, integridade, autenticidade, disponibilidade e não repudio.

Por outro lado, sabemos que, os sistemas de informação e de comunicação são expostos a diversos tipos de ameaças à segurança da informação, incluindo espionagem, sabotagem, vandalismo, incêndio, inundações, danos causados por código malicioso, *hackers*, e ataques de *denial of service* estão tornando-se mais comuns, mais ambiciosos e mais sofisticados.

> Também sabemos que "muitos sistemas de informação não foram projetados para serem seguros. A segurança da informação que pode ser alcançada por meios técnicos é limitada e deve ser apoiada por uma gestão e por procedimentos apropriados. A identificação de controlos a serem implementados requer planeamento cuidadoso e atenção nos detalhes. A gestão da segurança da informação requer pelo menos a participação de todos os colaboradores da organização. Pode ser que seja necessária a participação dos acionistas, fornecedores, terceiras partes, clientes ou outras partes externas."(ISO/IEC 27002:2013, p.vi)
>
> *Many information systems have not been designed to be secure. The security that can be achieved through technical means is limited, and should be support by appropriate management and procedures. Identifying which controls should be in place requires careful planning and attention to detail. Information security management requires, as a minimum, participation by all employees in the organization. It may also require participation from shareholders, suppliers, third parties, customers or other external parties.*(ISO/IEC 27002:2013, p.vi)

Uma das formas para proteger a "alma do negócio" de uma organização e responder a um conjunto possível de vulnerabilidades será implementar um Sistema de Gestão de Segurança da Informação (SGSI) baseado nos requisitos enunciados na norma ISO/IEC 27001, o padrão internacional mais conhecido na família ISO 27000, fornecendo os requisitos para um sistema de gestão de segurança da informação e certificação.

3.2. CONCEITO DE SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

O conceito de Sistema de Gestão da Segurança – SGSI, torna-se relevante no âmbito do desenvolvimento desta dissertação, como também, para que os destinatários deste documento possam ter um registo e um entendimento uniforme baseado sobretudo na definição de alguns autores.

A norma ISO/IEC 27001:2013, define que um SGSI faça parte de e esteja integrado com os processos da organização e com a estrutura global e que a segurança da informação seja considerada na conceção de processos, sistemas de informação e controlos. É expectável que uma implementação de um sistema de gestão de segurança da informação seja dimensionada de acordo com as necessidades da organização.

A definição preconizada pela norma enquadra o SGSI como parte integral do sistema global de gestão de uma organização e, como tal, tem impacto nos objetivos e exigências da organização; sendo que, as políticas e os procedimentos devem ser adaptados ao tamanho e estrutura da organização. Na componente processual e no desenvolvimento dos novos e atuais sistemas de informação, a segurança da informação deve ser considerada, tal como, o cumprimento dos objetivos dos controlos de referência especificados na norma. De realçar que, sendo o SGSI parte integrante da organização e, sendo a organização um órgão dinâmico, implica que os fatores circunscritos no conjunto de práticas e de controlos implementados terão que ser revistos, de um modo contínuo.

3.3. CARACTERIZAÇÃO DE UM SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

As organizações "na sua maioria funcionam com base em processos formais ou *ad-hoc*, apoiados em fluxos de informação, manuseados por pessoas e suportados numa infraestrutura tecnológica" (Martins, 2008) de informação e comunicação. Sendo a informação uma dos ativos mais importantes de uma organização e atendendo à sua importância e sensibilidade, a sua segurança torna-se necessária e imprescindível.

Nesta perspetiva a segurança da informação é uma área de conhecimento que visa à proteção da informação e dos sistemas de informação das ameaças à sua integridade (informação não é modificada de forma inesperada), disponibilidade (informação disponível sempre que necessário) e confidencialidade (acesso restrito a utilizadores legítimos). Para além destas propriedades (atributos) fundamentais, deverá ser considerada a autenticidade (identificação inequívoca do responsável pela informação), utilidade (informação serve o propósito para o qual foi criada) e posse (controlo exclusivo por parte do detentor da informação) a fim de garantir o adequado funcionamento e continuidade operacional e de negócio da organização, minimizando os riscos.

A NP ISO/IEC 27001:2013, na sua seção introdutória, refere que "um Sistema de Gestão de Segurança da Informação (SGSI) deve fazer parte e estar integrado com os processos da organização e com a estrutura de gestão global e que a segurança da informação seja considerada na conceção de processos, sistemas de informação e controlos. Deste modo, um SGSI deverá estar dimensionado de acordo com as necessidades da organização."

Atendendo à relevância, importância e sensibilidade da informação gerada, os sistemas de informação e comunicação do INEM, I.P. devem garantir um conjunto de características de segurança:

Confidencialidade: é necessário garantir que os dados dos utentes / cidadãos socorridos e colaboradores são protegidos, não podendo ser acedidos por pessoas não autorizadas, seja de forma acidental ou deliberada. A confidencialidade da informação irá garantir que, somente pessoas autorizadas terão acesso à informação de acordo com a sua classificação (publica, interna ou confidencial), ou seja, de acordo com o grau de sigilo do seu conteúdo.

Em contra posição, a confidencialidade da informação pode ser posta em risco por razões técnicas ou organizacionais: mecanismos de controlo de acesso insuficientes, transmissão de informação não cifrada pela rede, partilha de senhas entre utilizadores, definição desadequada de privilégios dos utilizadores, falta de cuidado no manuseio da informação, etc.

Disponibilidade: é necessário garantir que os recursos e serviços chave dos sistemas e tecnologias de informação e comunicação estejam acessíveis quando forem necessários (particularmente em situações de emergência), ou seja, a disponibilidade garante que os autorizados a aceder à informação possam fazê-lo sempre que necessário.

Os recursos e serviços podem ficar indisponíveis por avarias nos equipamentos ou no ambiente onde operam (por exemplo, quebras de energia, falhas nas aplicações, erros no manuseamento do sistema, ataques intencionais, causas naturais como incêndios ou inundações), insuficiência de recursos, etc. Para evitar quebras de disponibilidade é necessário existirem mecanismos de redundância, recuperação de falhas e proteção contra ataques, entre outros.

Integridade: garantir a exatidão da informação, isto é, os sistemas de informação e comunicação deverão assegurar que a informação armazenada ou em trânsito (onde ou desde onde) não é corrompida ou alterada indevidamente, de forma deliberada ou acidental, devido a erros operacionais (na introdução e manipulação de dados), erros no *software*, vírus, mau funcionamento do equipamento, etc.

Em situações de transação de informação é, ainda, importante garantir que as entidades intervenientes são quem afirmam ser (autenticidade), e que não podem negar posteriormente a sua participação na transação (não repúdio).

Legalidade: garantia de que a informação foi produzida em conformidade com a lei; regulamentos internos e/ou contratuais.

Autenticidade: garantia de que num processo de comunicação os remetentes sejam exatamente o que dizem ser e que a mensagem ou informação não foi alterada após o seu envio ou validação.

3.4. A CLASSIFICAÇÃO DA INFORMAÇÃO

Diferentes tipos de informações devem ser protegidos de formas distintas. Para que isto seja possível, a informação precisa de ser classificada. A classificação é um dos primeiros passos para a implementação de uma política de segurança da informação.

Possuir uma política de classificação de segurança da informação é uma forma preventiva de avaliarmos a informação gerada nos diferentes sistemas aplicacionais, mas também, zelar pela segurança da informação e fazer cumprir medidas de proteção da informação, de acordo com a sua classificação.

Durante a execução deste projeto, foi elaborado um documento intitulado "Política de Classificação e Manuseamento da Informação" com o objetivo de documentar a caracterização dos diferentes níveis de classificação da informação e seu manuseamento e responder ao requisito preconizado pela norma NP ISO/IEC 27001:2013 - Objetivo de Controlo e Controlo de Referência A.8.2 Classificação da Informação

Na "Política de Classificação e Manuseamento da Informação" são propostos os seguintes níveis de classificação da informação: informação pública; interna e confidencial.

a) Informação pública: estas informações podem ser divulgadas a qualquer pessoa sem que a organização seja prejudicada;

b) Informação interna: são informações que não devem sair da organização, mas se isso acontecer não terá consequências danosas para a organização;

c) Informação confidencial: o acesso a estas informações é realizado conforme a sua necessidade, só sendo permitido o acesso se as informações forem fundamentais para o desempenho satisfatório do trabalho.

A organização poderá ainda estratificar o nível de classificação nos tipos: informação secreta e informação ultra-secreta.

Informação secreta: para este tipo de informação o controlo sobre o uso das informações é total, o acesso não autorizado é crítico para a organização;

Informações ultra-secretas: neste tipo de informação o controlo também é total, pois o acesso não autorizado é extremamente crítico para a organização.

Tal como a vida de uma organização é dinâmica a classificação da informação também é dinâmica, atendendo que as informações consideradas sigilosas em determinada época podem ser, futuramente, de domínio público.

3.5. ÁREAS DE SEGURANÇA DA INFORMAÇÃO

Zúquete (2015), defende que, no âmbito da segurança de sistemas computacionais, podem-se considerar três grandes áreas de atividade, todas relevantes e com as suas especificidades: defesa

contra catástrofes, defesa contra faltas/falhas previsíveis e defesa contra atividades não autorizadas (Zúquete, 2015):

a) Defesa contra catástrofes físicas – garantir que um sistema de informação, ou serviço que esse sistema preste, possa sobreviver a catástrofes onde existam consequências ao nível físico. Podem-se considerar os seguintes exemplos:
   Catástrofes ambientais: tremores de terra, incêndio, inundações, queda de raios;
   Catástrofes políticas: ataques terroristas, motins;
   Catástrofes materiais: degradação irreparável ou perda/roubo de equipamentos computacionais, como discos magnéticos, computadores portáteis, etc.

b) Defesa contra faltas/falhas previsíveis – minimizar o impacto de acontecimentos fortuitos mas, normalmente previsíveis, muito embora não seja previsível o instante em que ocorrem, nem muitas vezes a gravidade com que ocorrem, como por exemplo, falhas temporárias de conectividade de troços de rede, quebra no funcionamento de energia elétrica.

c) Defesa contra atividades não autorizadas – a defesa de sistemas de informação contra iniciativas deliberadas por indivíduos que visam a corrupção ou subversão de sistemas computacionais, como por exemplo, acesso a informação reservada ou confidencial, alteração de informação sem autorização, etc.

3.6. IMPLEMENTAÇÃO DE UM SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

A implementação de um SGSI e a sua aplicação resulta da padronização de boas práticas que inclui a produção de documentação, procedimentos, instruções, ferramentas e técnicas, além da criação de indicadores, registos e na definição de um processo educacional de consciencialização na organização.

O sucesso de um SGSI começa com a garantia da aplicabilidade de uma das mais importantes recomendações da ISO/IEC 27001:2013 em que "a gestão de topo deve demonstrar liderança e comprometimento para com o sistema de segurança da informação."

O projeto e sua metodologia de implementação devem ser reconhecidos por todos os setores da organização. A norma ISO/IEC 27001:2013 na secção 5.1, evoca que a gestão de topo deve demonstrar liderança e comprometimento para com o sistema de gestão de segurança da informação:

a) Assegurando que a política de segurança da informação e os objetivos de segurança da informação estão estabelecidos e são compatíveis com a orientação estratégica da organização;

b) Assegurando a integração dos requisitos do sistema de gestão da informação nos processos da organização;

c) Assegurando que os recursos necessários para o sistema de gestão de segurança da informação estão disponíveis;

d) Comunicando a importância de uma gestão de segurança da informação eficaz e em conformidade com os requisitos do sistema de gestão de segurança da informação;

e) Assegurando que o sistema de gestão de segurança da informação atinge os resultados pretendidos;

f) Orientando e apoiando as pessoas para contribuir ara a eficácia do sistema de gestão de segurança da informação;

g) Promovendo a melhoria continua;

h) Apoiando outras funções de gestão relevantes a demonstrarem a sua liderança, conforme aplicável às suas áreas de responsabilidade.

Tendo em conta que a organização deve estabelecer, implementar, manter e melhorar de forma contínua um sistema de gestão de segurança da informação, de acordo com os requisitos da norma ISO/IEC 27001:2013, dever-se-á aplicar um modelo de gestão que satisfaça este propósito.

O modelo PDCA [*Plan-Do-Check-Act*] é uma das ferramentas de gestão que favorece esse propósito, pois este modelo de gestão está baseado no ciclo de melhoria contínua.

O modelo PDCA, representado na Figura 3-1, é preconizado um ciclo de atividades que, no seu conjunto, define a forma de estabelecimento de um Sistema de Gestão de Segurança da Informação, que integra: a sua implementação e operação, a sua monitorização e revisão e, finalmente, a sua otimização em função dos resultados obtidos em cada interação do processo.

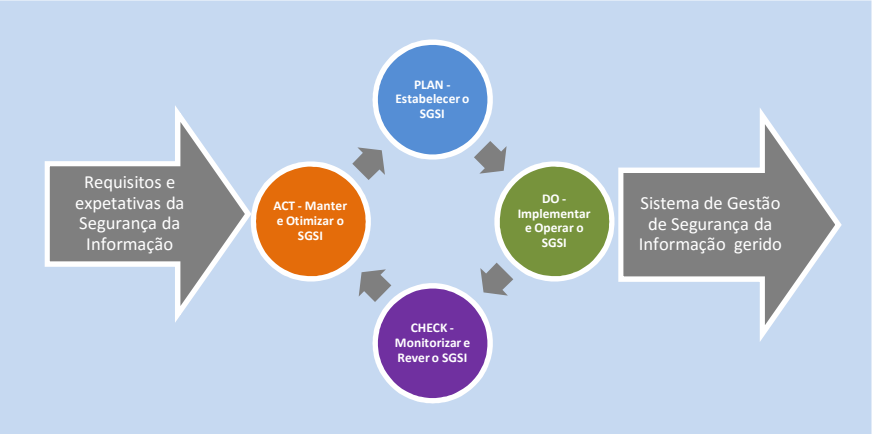


Figura 3-1 Modelo PDCA aplicado aos processos de um SGSI

As fases *Plan-Do* do PDCA corresponde às etapas de construção do SGSI envolvendo o desenho e definição do âmbito, análise de riscos, formalização estratégica de gestão de riscos, documentação e

seleção de controlos aplicáveis para reduzir os riscos quando necessários. Assim, a implementação do SGSI dá-se efetivamente nas duas primeiras fases do primeiro ciclo PDCA.

No ciclo do modelo PDCA, as fases *Check-Act* estão relacionados com a verificação e a medição do desempenho dos processos em comparação com as políticas do SGSI. Que medidas de segurança especificadas estão sendo aplicadas, às soluções de segurança utilizadas e à melhoria contínua do conjunto de segurança, além das auditorias periódicas de cada componente do sistema.

O objetivo que a norma pretende obter com este modelo é a correta gestão dos sistemas de segurança da informação, tendo como base as expectativas e necessidades específicas da organização do INEM.

O Sistema de Gestão de Segurança da Informação deve ser realizado tendo em conta, não somente o processo de análise/avaliação e tratamento de riscos, como também, medidas de controlo sugeridas em normas da família ISO/IEC 27000 e o modelo de processo PDCA (Plan – Do – Check – Act).

3.7. FATORES CRÍTICOS DE SUCESSO

A implementação de um sistema de segurança da informação numa organização é um processo transversal a todas as áreas orgânicas. "Ao implementar este programa, estará a transmitir uma imagem de preocupação nesta matéria, cada vez mais importante e com maior visibilidade, conseguindo simultaneamente gerir o risco a que se encontra sujeita. O programa de segurança serve, deste modo, vários objetivos: a criação de uma base de proteção e confiança sobre a qual é desenvolvida uma atividade; um sinal claro e inequívoco de que a organização tem preocupações fundamentais com a integridade e preservação dos seus ativos (quer sejam processos, serviços, informação ou outros); a afirmação pública de dedicação de um cuidado particular aos interesses de parceiros, cidadãos, utentes ou fornecedores. São estes os resultados visíveis de quaisquer esforços neste campo. É igualmente nestes fatores que reside a força do argumento da segurança como opção estratégica e não apenas técnica ou tecnológica, com impacto positivo e inegável sobre a organização" (Silva et al, 2003).

Identificam-se alguns fatores críticos para o sucesso da implementação do sistema de segurança da informação, dentro da organização, nomeadamente:

a) Uma Política de Segurança cujos objetivos e atividades reflitam os objetivos estratégicos e a missão da organização;

b) Comprometimento e apoio visível do conselho diretivo;

c) Uma implementação da segurança da informação consistente com a cultura organizacional;

d) Um claro entendimento dos requisitos de segurança, avaliação de risco e gestão de risco;

e) Uma divulgação partilhada das diretrizes sobre as normas e política de segurança da informação para todos os colaboradores, prestadores de serviços e parceiros.

4. METODOLOGIA

Apresentam-se neste capítulo, as principais fontes de suporte teórico e prático que serviram de base para a realização deste trabalho.

Tendo como foco principal realizar o Plano de Implementação do Sistema de Gestão de Segurança da Informação (SGSI), segundo os requisitos da norma ISO/IEC 27001:2013, procurou-se definir um modelo que permitisse identificar quais as funções críticas e vitais no cumprimento da organização do INEM que, pela sua missão tem uma caracterização crítica no âmbito da emergência médica pré-hospitalar e com uma cobertura de âmbito nacional, cobrindo a totalidade do país com o acionamento de diferentes meios aéreos e por terra.

4.1. DIAGRAMA DE PROCESSOS – PLANO DE IMPLEMENTAÇÃO

Este modelo, foi desenhado com o objetivo principal de identificar e visualizar as diferentes fases envolvidas para a realização do Plano de Implementação do Sistema de Gestão de Segurança da Informação (SGSI), as suas interligações e os documentos a produzir no final de cada processo.

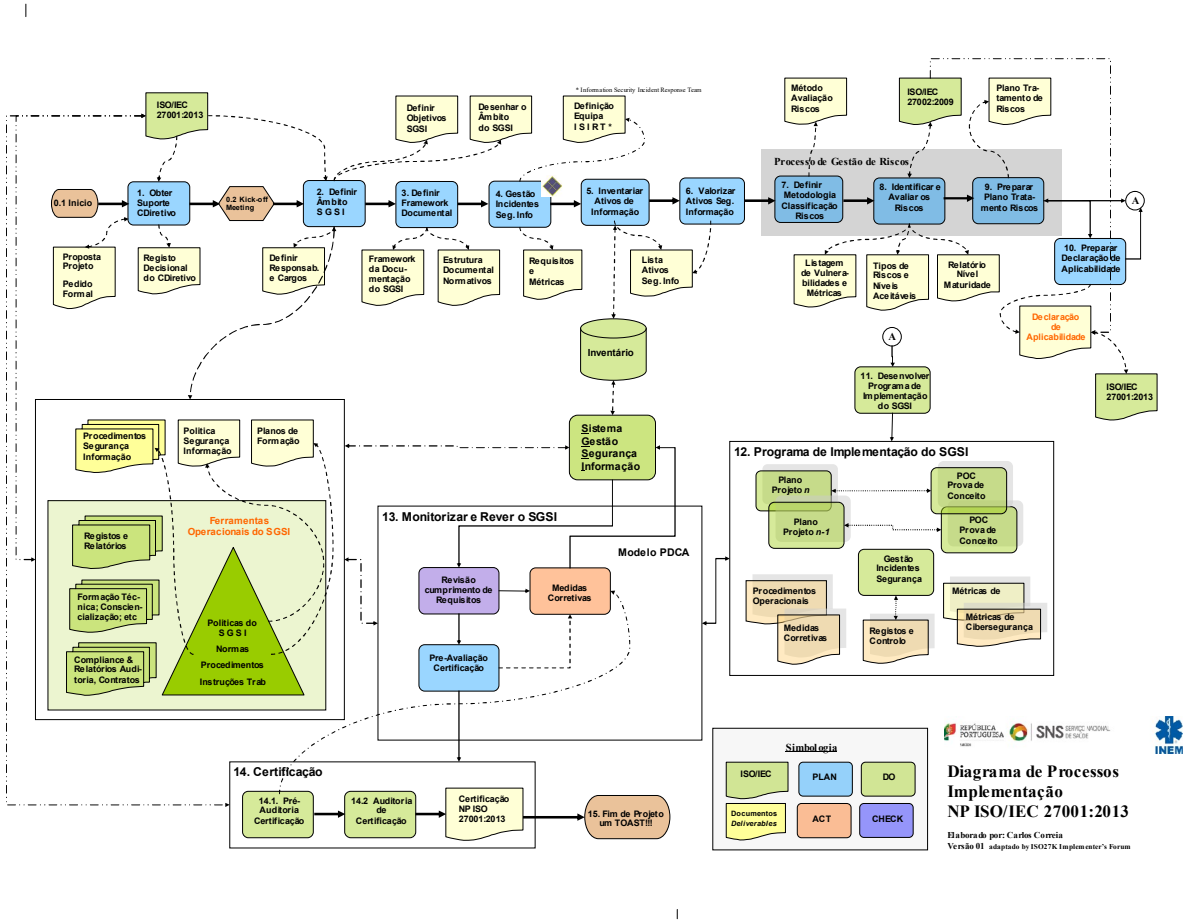


Figura 4-1 – Diagrama de Processos – Fase Plano de Projeto
(Diagrama adaptado ISO27K Forum (2015)

No Diagrama de Processos foi aplicado um esquema cromático de cores por fase. As fases identificadas espelham a metodologia de gestão de melhoria contínua PLAN-DO-CHECK-ACT [PDCA].

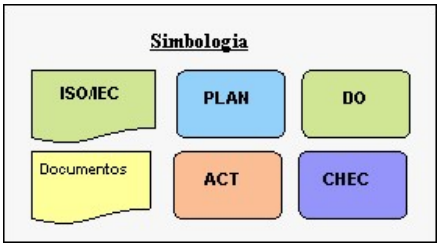


Figura 4-2 – Simbologia - Diagrama de Processos

A elaboração deste diagrama processual foi definido com base das necessidades específicas para produzir um plano de implementação que, na norma ISO/IEC 27001:2013 é referenciado como a "Declaração de Aplicabilidade" (NP ISO/IEC 27001 Clausula 6.1.3d, p.9).

Atendendo que este trabalho, em concreto, tem *focus* na fase de PLANO da implementação de um SGSI, o Diagrama apresenta de forma detalhada os processos necessários para esta fase e a identificação, onde fazem parte os processos identificados de 1 (um) a 10 (dez) e a produção dos seus respetivos *deliverables*.

Procurou-se com este modelo, de uma forma genérica, definir um conjunto de atividades que permitisse compreender a interligação dos atuais processos funcionais, a estratégia da organização e seu alinhamento com os sistemas e tecnologias de informação envolventes, assim como, identificar o nível de capacidade e maturidade que a organização tem para responder e alcançar a implementação de um Sistema de Gestão de Segurança da Informação, orientando-a com um conjunto de objetivos a alcançar (atividades a realizar) aplicáveis ao processo de implementação da norma ISO/IEC 27001:2013.

4.2. TÉCNICAS DE RECOLHA E ANÁLISE DE DADOS

A problemática acerca da segurança da informação e do papel dos sistemas e tecnologias de informação na organização é, hoje em dia, uma matéria amplamente discutida. De forma a minimizar o risco de dispersão, tomou-se como ponto de partida realizar uma revisão da literatura sobre um sistema de gestão de segurança da informação, a importância da segurança da informação no contexto de uma organização, as vantagens que um sistema de gestão da segurança da informação poderá trazer no processo de implementação sobretudo no alinhamento às boas práticas e no aumento das capacidades operacionais, de gestão e de governação dos sistemas e das tecnologias de informação. A revisão literária sobre o tema, permitiu uma aproximação mais efetiva e explorar opiniões contrastantes.

Para além desta exploração bibliográfica foram exploradas técnicas de recolha e análise de informação. Estas técnicas tiveram como objetivo orientar a seleção da problemática a abordar em diferentes áreas bem como a forma de análise sobre as mesmas.

A recolha de informação para análise e posterior formulação das atividades a realizar teve como base uma recolha da informação assente em três técnicas basilares:

Análise Documental: Análise de documentos como procedimentos, instruções e apresentações institucionais. Foram, também, analisados documentação técnica sobre sistemas de informação no âmbito da sua implementação, gestão operacional e atual manutenção. No contexto da gestão estratégica da instituição foram consultados documentos sobre a definição do plano estratégico e a tomada de conhecimento das diferentes ferramentas de gestão existentes, assim como, os estatutos decretados à instituição permitindo a identificação prévia e relevante das principais responsabilidades e atividades desenvolvidas por cada uma das área orgânicas e sua interligação. A conjugação de todas estas informações recolhidas permitiu identificar de forma ordenada e efetiva os tópicos a abordar nas entrevistas realizadas posteriormente.

Entrevista semi-estruturada: A aplicabilidade desta técnica teve como principal propósito obter informação detalhada no âmbito dos objetivos de controlos preconizados pela norma ISO/IEC 27001:2013, identificando qual o estado dos controlos implementados ou parcialmente implementados e identificar quais os controlos inexistentes ou a melhorar no contexto da gestão dos riscos de segurança da informação. As entrevistas com um carácter semi-diretivo, permitiu absorver a informação necessária sobre os processos organizacionais, as suas relações inter-funcionais, os recursos envolventes, identificar vulnerabilidades e pontos de melhoria.

Esta abordagem metodológica quantitativa e qualitativa foi complementada com a criação de grupos de trabalho, onde foram realizadas entrevistas com base nas perguntas formuladas, investigando questões sensíveis ou informação privilegiada e obtendo uma perceção pessoal, explorando emoções, experiências ou sentimentos.

Observação direta: Esta técnica permitiu completar a informação reunida nas entrevistas e nas discussões de grupos de trabalho, visto que possibilitou recolher informação e "ver" aspetos que os entrevistados e participantes não têm conhecimento ou sobre os quais não desejam falar ou esclarecendo pontos que poderão ter ficado menos explorados. Esta técnica tornou-se de suma importância pelo reforço naturalístico da recolha de dados, tornando-se num processo interativo e incremental.

5. CARACTERIZAÇÃO DO INSTITUTO NACIONAL DE EMERGÊNCIA MÉDICA

Instituto Nacional de Emergência Médica (INEM) é o organismo do Ministério da Saúde (MS) ao qual compete assegurar o funcionamento, no território de Portugal continental, de um Sistema Integrado de Emergência Médica (SIEM), de forma a garantir aos sinistrados ou vítimas de doença súbita a pronta e correta prestação de cuidados de saúde, designadamente através das redes de telecomunicações relativas à emergência médica, da prestação de socorro no local da ocorrência, do transporte assistido das vítimas para o hospital (unidade de saúde) adequado e de articulação entre os vários estabelecimentos hospitalares, conforme disposto na nova Lei Orgânica do INEM, aprovada pelo Decreto-Lei n.º 34/2012, de 14 de fevereiro.(INEM,2015)

5.1. MISSÃO, VISÃO E VALORES

O INEM tem por missão definir, organizar, coordenar, participar e avaliar as atividades e o funcionamento de um Sistema Integrado de Emergência Médica.

Missão
Garantir a prestação de cuidados de emergência médica.

Visão
Ser uma organização inovadora, sustentável, motivadora e de referência na prestação de cuidados de emergência médica.

Valores
Para além do rigor e seriedade no serviço prestado, o INEM assume como valores:

Competência	**Ter um conhecimento profundo na área de emergência médica, nos seus vários domínios.**
Credibilidade	**Receber a confiança e o reconhecimento da sociedade.**
Ética	**Atuar de forma íntegra, paciente e generosa.**
Eficiência	**Alcançar os melhores resultados possíveis com os recursos disponíveis.**
Qualidade	**Assumir um compromisso com as necessidades e expetativas dos cidadãos.**

Figura 5-1 – Valores do INEM

5.2. A ESTRUTURA ORGANIZACIONAL DO INEM

A gestão operacional da atividade do INEM (de acordo com os Estatutos do INEM aprovados pela Portaria nº 158/2012, de 22/05) é assegurada pelos seus serviços desconcentrados (Delegações Regionais) nas respetivas áreas geográficas (Norte, Centro e Sul) em articulação com as restantes Unidades Orgânicas. De acordo a organização interna, o INEM tem uma estrutura orientada para três grandes vertentes: **a área operacional, a área de apoio e logística e a área de apoio à gestão.**

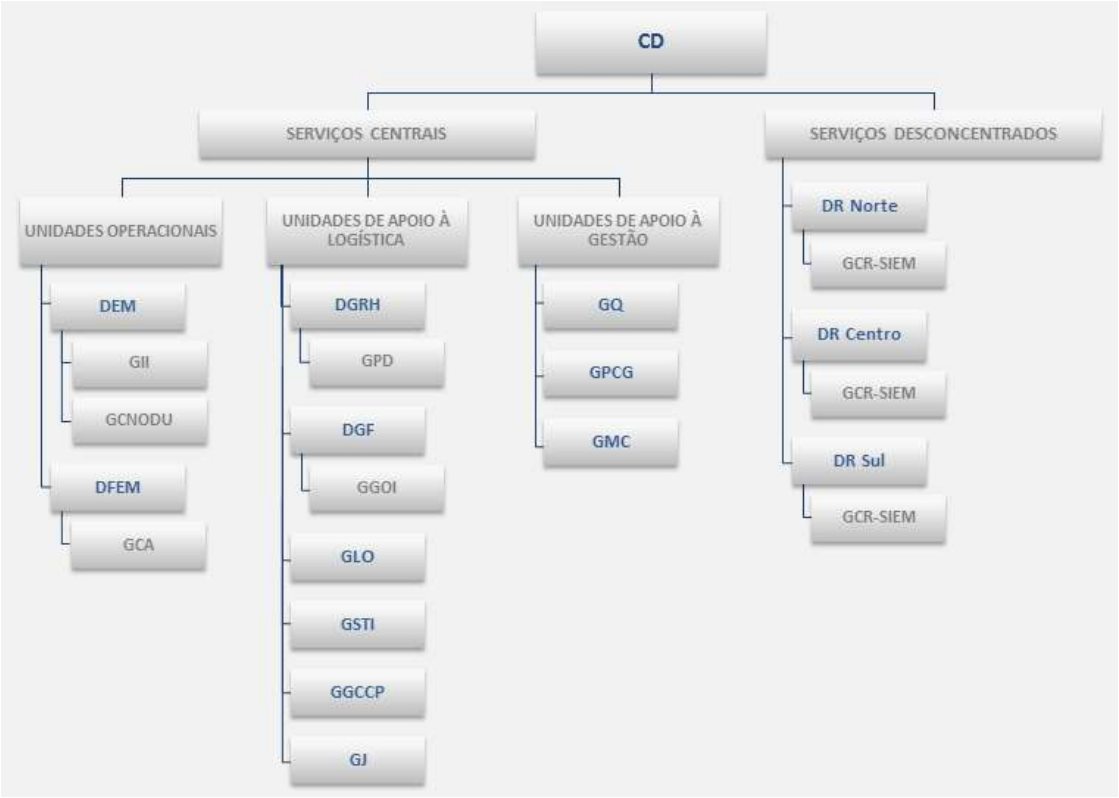


Figura 5-2 Organograma do INEM
(Fonte: site institucional do INEM)

O órgão de gestão do INEM **é** dirigido pelo Conselho Diretivo, constituído por um Presidente e por um Vogal.

CD: Conselho Diretivo

<u>Unidades Operacionais</u>

DEM: Departamento de Emergência Médica

GII**:** Gabinete de Investigação e Inovação

GCNODU: Gabinete de Coordenação Nacional de Doentes Urgentes

DFEM: Departamento de Formação em Emergência Médica

GCA: Gabinete de Certificação e Acreditação

Unidades de Apoio à Logística

DGRH: Departamento de Gestão de Recursos Humanos

GPD: Gabinete de Planeamento e Desenvolvimento

DGF: Departamento de Gestão Financeira

GGOI: Gabinete de Gestão Orçamental e Investimentos
GLO: Gabinete de Logística e Operações
GSTI: Gabinete de Sistemas e Tecnologias de Informação
GGCCP: Gabinete de Gestão de Compras e Contratação Pública
GJ: Gabinete Jurídico

Unidades de Apoio à Gestão

GQ: Gabinete de Qualidade
GPCG: Gabinete de Planeamento e Controlo de Gestão
GMC: Gabinete de Marketing e Comunicação

Serviços Desconcentrados

DRN: Delegação Regional do Norte

GCR – SIEM: Gabinete de Coordenação Regional do SIEM

DRC: Delegação Regional do Centro

GCR – SIEM: Gabinete de Coordenação Regional do SIEM

DRS: Delegação Regional do Sul

GCR – SIEM: Gabinete de Coordenação Regional do SIEM

5.3. ÁREAS DE ATUAÇÃO DO INEM

Para assegurar o cumprimento das suas atribuições, o INEM, I.P., **presta um conjunto de serviços, que se indicam, por área de atuação:**

Atividade dos Centros de Orientação de Doentes Urgentes (CODU)

- Assegurar, em todo o território de Portugal continental, 24 horas por dia, o atendimento de chamadas de emergência médica encaminhadas pelo número telefónico de emergência 112;
- Avaliar, através de um sistema de algoritmos de triagem médica, no mais curto espaço de tempo, os pedidos de socorro recebidos, com o objetivo de determinar os recursos necessários e adequados a cada caso;
- Aconselhar o cidadão a realizar manobras básicas de emergência, sempre que indicado;
- Selecionar e acionar os meios de emergência médica apropriados;
- Aconselhar as equipas no terreno, sempre que necessário, bem como validar protocolos de atuação a não-médicos;
- Proceder à correta referenciação do doente urgente/emergente;

- Assegurar o contacto com as unidades de saúde, preparando a receção hospitalar das vítimas para tratamento urgente/emergente, com base em critérios clínicos, geográficos e de recursos da unidade de saúde de destino;
- Gerir a rede de telecomunicações de emergência;
- Promover a resposta integrada ao doente urgente/emergente.

E, ainda no âmbito da atividade dos CODU, serviços para responder a necessidades específicas, como:

- Prestar aconselhamento médico a situações de emergência, na área da saúde, que se verifiquem a bordo de embarcações: o **CODU Mar** garante os cuidados a prestar, procedimentos e terapêutica a administrar à vítima, podendo também acionar a evacuação do doente, organizar o acolhimento em terra e o encaminhamento para o serviço hospitalar adequado;
- Prestar informação a situações de intoxicação: através do **Centro de Informação Antivenenos (CIAV)** presta, em tempo útil, as informações necessárias e adequadas a profissionais de saúde ou ao público em geral, visando uma abordagem correta e eficaz das vítimas de intoxicação;
- Prestar apoio psicológico em emergência: através do serviço do **Centro de Apoio Psicológico e Intervenção em Crise (CAPIC)**, intervém com os utentes em situações de crises psicológicas, comportamentos suicidas, vítimas de abusos/violência física ou sexual, entre outros.

Atividade pré-hospitalar

- Prestar cuidados de emergência médica em ambiente pré-hospitalar e providenciar o transporte para as unidades de saúde adequadas;
- Promover o adequado transporte inter-hospitalar do doente urgente/emergente.

Atividade de transporte de doentes

- Definir os critérios e requisitos necessários ao exercício da atividade de transporte de doentes, incluindo os dos respetivos veículos, e proceder ao licenciamento desta atividade e dos veículos a ela afetos;
- Fiscalizar a atividade de transporte de doentes, sem prejuízo da competência sancionatória atribuída a outros organismos.

Atividade de Formação e promoção da Formação dos profissionais indispensáveis às ações de Emergência Médica bem como do público em geral

- Definir, planear, coordenar e certificar a formação em emergência médica
- Ministrar a formação em emergência médica aos elementos do SIEM, incluindo dos estabelecimentos, instituições e serviços do Serviço Nacional de Saúde (SNS);

- Homologar os curricula dos cursos ou estágios que versem sobre emergência médica.

Outras atividades de planeamento, coordenação e prestação de assistência médica

- Colaborar na elaboração dos planos de emergência/catástrofe com as Administrações Regionais de Saúde, com a Direção-Geral de Saúde (DGS) e com a Autoridade Nacional de Proteção Civil (ANPC), no âmbito das respetivas leis reguladoras e orientar a atuação coordenada dos agentes de saúde nas situações de exceção, como sejam catástrofes ou acidentes graves, integrando a organização definida em planos de emergência/catástrofe, sem prejuízo das atribuições de outras entidades;
- Contribuir, em articulação com a DGS, para a definição e atualização das políticas de planeamento civil de emergência na área da saúde;
- Assegurar a proteção e socorro a altas individualidades;
- Garantir a assistência em eventos de alto risco, nomeadamente nos acontecimentos com elevado número de participantes/assistentes;
- Missões internacionais: assegurar a representação internacional, no domínio das suas competências e atribuições específicas e promover a cooperação com as comunidades lusófonas, sem prejuízo das competências próprias do Ministério dos Negócios Estrangeiros, sob coordenação da DGS, enquanto entidade responsável pela coordenação da atividade do Ministério da Saúde no domínio das relações internacionais.

Atividade de divulgação do SIEM e do desempenho do INEM

- Desenvolver ações de sensibilização e informação dos cidadãos no que respeita ao SIEM;
- Promover a realização de estágios de observação nos seus meios e locais de trabalho, com vista a dar a conhecer o funcionamento do SIEM, numa perspetiva útil e pedagógica;
- Dinamizar um programa de ações de sensibilização, através de visitas de estudo, visando fomentar a adequada utilização dos serviços e meios de emergência médica pré-hospitalares;
- Disponibilizar e atualizar informações na página da internet em www.inem.pt.

6. ANÁLISE DA IMPLEMENTAÇÃO DA 27001 NO INEM

Para levar a cabo o plano de implementação, tomou-se como linha de orientação o diagrama de processos, permitindo a produção de vários *deliverables* que fundamentam a matéria necessária para a implementação do SGSI. Se não soubermos "o que interessa proteger e qual o modelo base em que deve assentar essa proteção, não é possível conceber e implantar uma segurança adequada." (Zúquete,2015). Deste modo, foi realizado o levantamento dos principais processos e ativos e a sua integração com o âmbito da segurança da informação. Face aos objetivos estratégicos e operacionais da organização, definiu-se o alcance e a estrutura do SGSI a implantar.

No desenho para a implementação do SGSI, foi ainda executado a apreciação do risco (*risk assessment*). Esta etapa de extrema relevância, envolveu as atividades de identificação do risco, a sua análise e avaliação de cada risco. A Matriz de Risco produzida teve como *input* o resultado das anteriores atividades e o plano de tratamento de riscos a aplicar.

6.1. LEVANTAMENTO DA SITUAÇÃO ATUAL

Os objetivos da implementação do SGSI devem ser pensados tendo em conta os requisitos e prioridades da informação da organização INEM. Para a produção deste *output*, foi aplicado uma abordagem *top-down* procurando identificar as funções críticas e vitais na organização do INEM, na perspetiva da disponibilidade e segurança da informação, tendo como aspeto crítico a garantia da continuidade funcional e operacional do INEM no cumprimento da sua missão.

A informação foi obtida através da consulta a vários documentos da instituição do INEM e um questionário estruturado que serviu de *guideline* na determinação dos objetivos para a implementação do SGSI, mas também, com o propósito de definir prioridades e transformar o implícito no explícito.

Os pontos abordados foram os seguintes:

i. Áreas orgânicas críticas da organização que servem a instituição na sua missão.
ii. Levantamento da infraestrutura TIC e classificação dos ativos
iii. Ligações contratuais/formais com entidades externas e as áreas orgânicas.
iv. Serviços subcontratados no âmbito da infraestrutura dos sistemas e telecomunicações.
v. Informação crítica e/ou sensível.
vi. Consequências prováveis na divulgação de certa informação por partes não autorizadas.
vii. Acordos contratuais, organizacionais ou legais relacionados com a segurança da informação, em termos de requisitos de armazenamento de dados, privacidade ou qualidade dos dados e requisitos específicos.
viii. Leis relacionadas com o tratamento de risco ou segurança da informação se aplicam à instituição do INEM.

Na realização deste trabalho foram consultados os seguintes documentos internos do INEM:

Estatutos do INEM, publicado na Portaria nº158/2012 de 22 maio

Plano Estratégico do 2014-2016

Plano Estratégico de Sistemas de Informação

Política Interna dos Sistemas e Tecnologias de Informação

Política de Gestão de Risco

SGIQAS (ISO 9001:2015 e ISO 14000) Sistema de Gestão Integrada da Qualidade, Ambiente e Segurança e Política Integrada Qualidade, Ambiente e Segurança

Processo de Gestão P.10-5.GSTI - Gestão das Telecomunicações e Informática

Processo de Gestão PG.13-1.GSTI-Instalação Posto Trabalho Backoffice

Processo de Gestão PG.14-1 GSTI - Acesso Empresas Externas_Prestadores de Serviço

Arquitetura Geral da Rede LAN/WN

Lista de Servidores e Aplicações (Serviços Aplicacionais) e Lista de Equipamentos Ativos de Rede

6.2. ANÁLISE SWOT

A análise SWOT apresentada, tem por base a informação obtida no levantamento da situação atual. Está circunscrita no âmbito da segurança da informação sobre a infraestrutura dos sistemas e tecnologias de informação no seu alinhamento à missão e objetivos estratégicos do 2016-2018 do INEM, tendo em prospetiva a linha de projetos desenhados no horizonte Portugal 2020.

A análise realizada permite relacionar os pontos fortes e fracos da organização com as principais tendências do seu meio envolvente, tendo como objetivo gerar medidas para lidar com as oportunidades e ameaças identificadas.

Pontos Fortes	Pontos Fracos
Organização crítica com cobertura nacional, no serviço de emergência pré-hospitalar. Infraestrutura dos centros de processamento de dados (*Data Centers)* localizados geograficamente pelas delegações regionais. Disponibilidade assegurada com arquitetura redundante nos serviços voz e SIADEM. Configuração normalizada de *software* base nos *end-points*. Alta confiança e conhecimento experiencial da equipa técnica do GSTI. Reconhecimento na aplicabilidade e implementação de boas práticas.	Arquitetura LAN em estrela; equipamento core com tecnologia obsoleta (ativos e passivos) sem possibilidade de expansão e sem redundância na *layer* de distribuição. Infraestrutura de *storage* obsoleta e sem cobertura técnica pelo fabricante. Centralização dos sistemas críticos num único *Data Center*. Governação TIC com configuração reativa e pouco preventiva. Administração e manutenção dos principais sistemas de informação controlada por prestadores externos. Descentralizado controlo dos ativos de informação e inadequada identificação. Inexistente política no controlo de acessos aplicacionais. Processo contratação pública morosa.

Oportunidades	Ameaças
Conceptualizar arquitetura rede LAN integrada com rede SIRESP, a infraestrutura de servidores aplicacionais e de voz garantindo disponibilidade, redundância de serviço e monitorização. Implementar *wireless LAN Controller* com gestão centralizada. Nova tecnologia de *storage* integrada com a infraestrutura *cloud computing*. Implementar no SIADEM arquitetura (*AlwaysON*) redundante com distribuição geográfica. Implementar planos de *disaster recovery* com recurso físico aos *Data Centers* e *firewall* com IDS/IPS - monitorização e relatórios. Habilitar colaboradores com cultura de segurança da informação. Na equipa do GSTI, adaptar *know-how* nas componentes de segurança da informação.	Indisponibilidade na recuperação de dados e/ou perda de dados. Indisponibilidade da rede LAN e perda de serviço total ou parcial. Incapacidade de implementar eficaz plano de *disater recovery.* Rede *wifi* sem controlo / monitorização. Vulnerabilidades na segurança de perímetro, com possibilidade de ataque. Quebras de confidencialidade no acesso a dados. Transação de documentos com perda de integridade e confidencialidade. Dificuldade na concretização atempada de controlos, por motivos contratuais (produtos e serviços).

Tabela 1 - Análise SWOT (*Strengths, Weakness, Opportunities and Threats*)

6.3. DEFINIÇÃO DO ÂMBITO E ALCANCE DO SGSI

Tendo em mente a execução do Plano de Implementação do SGSI, deve ser definida a sua estrutura. O desenho do âmbito do SGSI teve como *input* a fase anterior - os requisitos e prioridades da informação da organização INEM. O resultado desta fase foi elaborar um documento com a definição do âmbito e que servirá de guia às decisões de implementação que irão surgir durante o processo.

O resultado compreendeu as seguintes definições:

i. Implementar um Política de Segurança ajustada aos objetivos estratégicos da organização e sua missão.

ii. Cumprimento de confidencialidade dos dados clínicos do cidadão socorrido, de acordo com a Lei 67/98, de 26 outubro – Lei da Proteção de Dados Pessoais[8] e a Lei 46/2007, de 24 agosto – Lei do Acesso a Documentos Administrativos.

iii. Manter uma relação integrada entre os requisitos englobados na norma ISO/IEC 27001 e os outros *standards* existentes na organização, como por exemplo, o SGIQAS (ISO 9001:2015 e ISO 14000) e a Política de Gestão do Risco (ISO/IEC 31000).

iv. Implementar os requisitos da ISO/IEC 27001 como uma ferramenta de auxílio à gestão das TIC, melhorando os seus processos associados com uma focalização na componente da segurança da informação.

[8] O Regulamento EU 2016/679 será aplicável a partir de 25 de maio de 2018 e revoga a Lei 67/98, de 26 outubro – Lei da Proteção de Dados Pessoais.

v. Conceptualizar uma arquitetura TIC que responda com eficácia às possíveis vulnerabilidades existentes.

vi. Aplicar uma cultura de segurança da informação transversal a toda a organização.

vii. Definir uma estrutura de recursos que garantam o SGSI e imprimam processos de melhoria contínua.

viii. Aplicar o processo de gestão do risco na infraestrutura TIC.

ix. Aplicar um Framework de gestão documental no SGSI.

x. No desenho e implementação de novos projetos esteja contemplado os requisitos de segurança de informação.

6.4. RESPONSABILIDADES E CARGOS

As estruturas organizacionais são consideradas as entidades chave para a tomada de decisão dentro da organização. Este facilitador apresenta um conjunto de funções diretamente relacionadas com segurança da informação e pretende que seja executado um conjunto de práticas associadas a cada uma delas, que ofereçam como resultado à organização a tomada de boas decisões. (Santos et al, 2014). A estrutura organizativa e os recursos para assegurar a segurança da informação variam de empresa para empresa, dependendo entre outros aspetos, da sua dimensão. Por exemplo, numa pequena empresa, vários cargos são ocupados por uma mesma pessoa.

No âmbito do SGSI, o requisito **5.3 Funções, responsabilidades e autoridades na organização** da norma ISO/IEC 27001:2013, indica que "a gestão de topo deve assegurar que são atribuídas e comunicadas as responsabilidades e autoridades para funções que são relevantes para a segurança da informação."

A ISO/IEC27003 define detalhes que auxiliam na definição das responsabilidades e cargos de gestão de segurança da informação. Em adicional, o recente **Regulamento EU 2016/679**[9] do Parlamento Europeu e do Conselho da União Europeia de 27 abril de 2016, designa a nomeação do Encarregado da Proteção de Dados. Com base nestes documentos, são descritos os papéis/cargos e as responsabilidades que são necessárias, na instituição do INEM, para a implementação do Sistema de Gestão de Segurança da Informação (SGSI).

a) A responsabilidade final sobre a segurança da informação deve estar ao nível hierárquico da administração – **Conselho Diretivo (CD)**, sendo também o órgão responsável pela promoção da melhoria contínua e avaliação do desempenho do Sistema de Gestão Integrado – Qualidade, Ambiente e Segurança.

[9] O Regulamento 2016/679 do Parlamento Europeu e do Conselho da União Europeia, de 27 de abril de 2016, designado como Regulamento Geral sobre a Proteção de Dados, foi publicado no dia 4 de maio 2016, entrou em vigor no dia 24 de maio de 2016 e será aplicável a partir de 25 de maio de 2018. Este Regulamento define o novo regime jurídico da proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados, revogando a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).

b) A organização deverá nomear um promotor e coordenador dos processos de segurança da informação, normalmente designado por ***Chief Information Security Officer*** **(CISO)** ou **Gestor de Segurança**.

c) A nomeação do **Encarregado da Proteção de Dados (*Data Protection Officer*)** enquadrado com a Administração Pública da Saúde e com o enquadramento jurídico geral do Regulamento EU 2016/679.

d) Cada **Trabalhador/Colaborador** é responsável pela sua função / cargo e por manter a segurança da informação no local de trabalho e na organização.

e) Criação de um **Comité de segurança da informação** que permita estabelecer uma ligação estreita entre os papéis / cargos de gestão de segurança de informação.

f) **Equipa técnica pluridisciplinar ISIRT - *Information Security Incident Response Team*** que possa estar disponível, ou seja, dedicada à análise, avaliação e resolução de eventos e incidentes relacionados com a segurança da informação.

g) **Responsável dos RH – Membro do Departamento de Recursos Humanos** (RH) com a responsabilidade de fazer a ligação entre a segurança da informação e os trabalhadores e colaboradores da instituição do INEM (internos e externos). Planear e gerir ações de formação e sensibilização sobre segurança da informação, gerir e controlar o processo a ter com os funcionários/trabalhadores e prestadores externos de serviço no antes, durante e depois da contratação.

h) **Responsável pela Área Orgânica ou Chefe Departamento/Gabinete** pessoa responsável pela segurança da informação de uma área orgânica ou departamental sendo responsável por efetivar os requisitos sobre segurança da informação, definidos na(s) Política(s) de Segurança.

i) **Donos (*Owners*) / Responsáveis dos Ativos (de Segurança da Informação)** – pessoa diretamente responsável pela gestão de um ativo e por todos os eventos ou incidentes de segurança que ocorrerem relacionadas com aquele ativo.

j) **Responsável por processos nas áreas estratégicas** – ter a responsabilidade por determinado processo considerado crítico para a empresa, por exemplo, um gestor do projeto na implementação de uma nova tecnologia ou mudança funcional e/ou operacional.

Na organização, deve ser nomeada uma pessoa responsável como chefia da segurança da informação, denominada por Gestor da Segurança (também denominado por *Chief Information Security Officer* (CISO) ou *Information Security Manager*) e as restantes devem ser nomeadas tendo em conta as competências demonstradas para a ocupação do cargo / função. Em paralelo e em consonância com o CISO, deve também ser nomeado o Encarregado da Proteção de Dados (*Data Protection Officer*) como a entidade responsável e centralizadora pelo cumprimento do Regulamento EU 2016/679.

Os responsáveis das áreas orgânicas, departamentos e ou gabinetes integrantes no âmbito do SGSI, são potenciais membros da equipa de implementação do SGSI e potenciais promotores na sensibilização e importância da segurança da informação na organização INEM.

6.5. FRAMEWORK DA DOCUMENTAÇÃO DO SGSI

A definição de um Framework Documental é fundamental para o suporte e estrutura do Sistema de Gestão de Segurança da Informação. Neste âmbito a estrutura documental deverá incluir um conjunto de políticas e normas (Normativos) que orientam as atividades operacionais e asseguram a proteção da informação da organização no seu dia-a-dia. Neste contexto, alguns autores referem que as políticas, normas e procedimentos de segurança da informação constituem os mecanismos formais que definem os objetivos de uma organização em termos de segurança, bem como as medidas a serem tomadas para a concretização dos mesmos (Silva et al. 2003).

O Framework Documental apresentado, segue a recente linha de orientação do ecossistema do Sistema de Informação da Saúde (eSIS), onde a organização do INEM faz parte e, tem na sua estrutura um conjunto de documentos que é dividido em 4 níveis hierárquicos, descritos na Figura 6-1 e na Tabela 1.

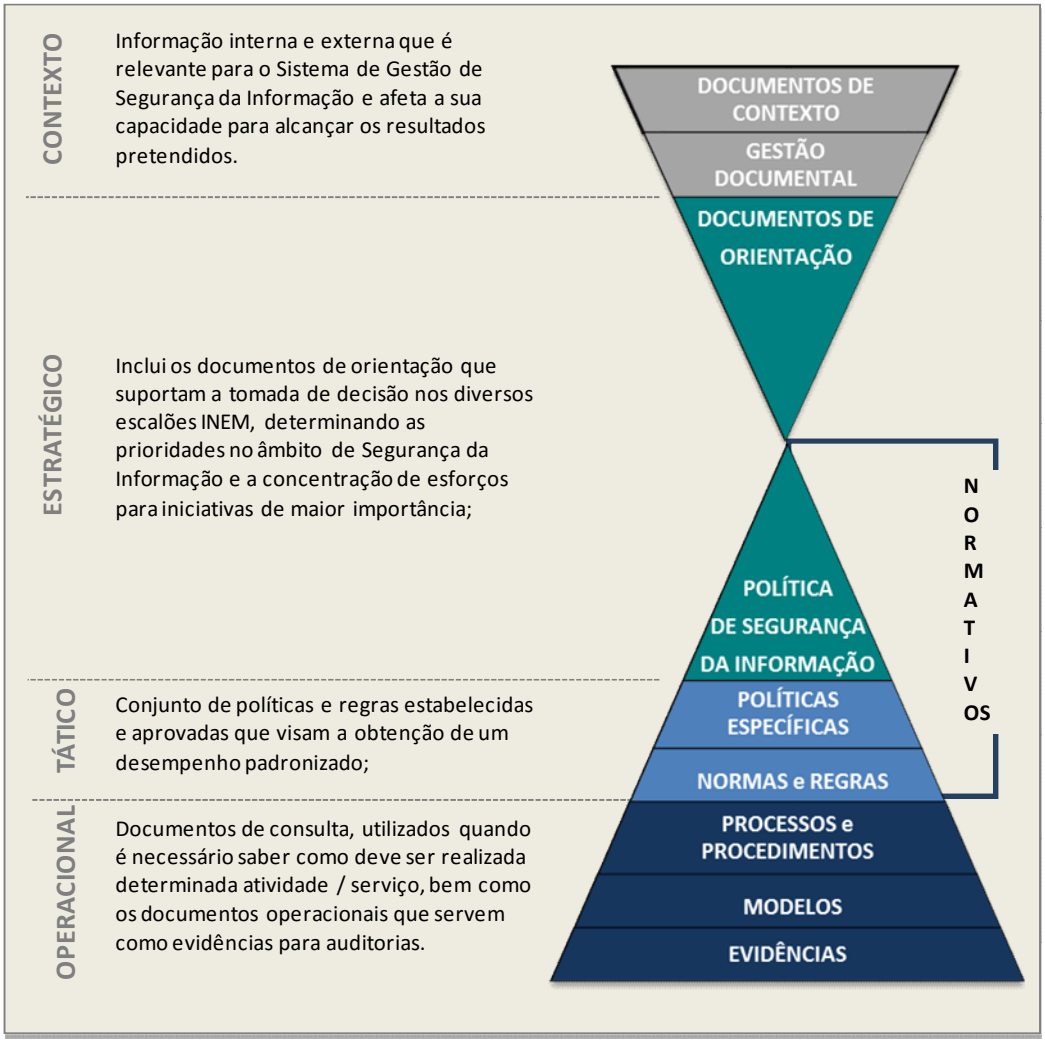


Figura 6-1 Estrutura Documental no âmbito de Segurança da Informação

Tabela 2 - Responsabilidade pela Gestão Documental no âmbito do Risco e Segurança da Informação

NÍVEL		TIPOS DE DOCUMENTOS	EXEMPOLOS DE DOCUMENTOS	RESPONSÁVEL	APROVADOR
1	CONTEXTO	DOCUMENTOS DE CONTEXTO	Descrição do Contexto interno e externo Requisitos legais e contratuais Requisitos das partes interessadas	Coordenador do Gabinete de Sistemas e Tecnologias de Informação (GSTI)	Coordenador do GSTI
		GESTÃO DOCUMENTAL	*Frameworks* da Documentação Procedimentos de Gestão Documental	Coordenador do Gabinete Qualidade (GQ)	Coordenador do GQ
2	ESTRATÉGICO	DOCUMENTOS DE ORIENTAÇÃO	Âmbito do SGSI, Princípios SI, Estratégia SI, Objetivos SI, Estruturas Organizacionais SI	Gestor de Segurança	Conselho Diretivo
		POLÍTICA SI	Política de Segurança da Informação	Gestor de Segurança	Conselho Diretivo
3	TÁTICO	POLÍTICAS ESPECÍFICAS	Políticas específicas de alto nível dentro das respetivas áreas de SI mapeadas às cláusulas da norma ISO/IEC 27001:2013	Gestor de Segurança	Comité de Segurança da Informação
		NORMAS E REGRAS	Normas e Regras técnicas dentro das respetivas áreas de SI mapeadas às cláusulas da norma ISO/IEC 27001:2013	Gestor de Segurança	Comité de Segurança da Informação
4	OPERACIONAL	PROCESSOS E PROCEDIMENTOS	Processos e procedimentos detalhados	Gestores de processos e estruturas TIC	Gestor de Segurança
		MODELOS	Modelos de registos, relatórios, planos e programas, cláusulas contratuais, etc	Gestores de processos Gestores das estruturas TIC	Gestor de Segurança
		EVIDÊNCIAS	Registos, Relatórios, Planos etc.	Responsável GSTI Gestores de processos Gestores das estruturas TIC	Gestor de Segurança

Os Normativos de Segurança da Informação do INEM serão categorizados na seguinte forma:

1) A "Política de Segurança da Informação do INEM" é o documento do nível Estratégico que tem caráter efetivo e define a Segurança da Informação do INEM para orientar o desenvolvimento de todos os documentos dos níveis Tático e Operacional da Framework, bem como todas as atividades operacionais relacionadas com a Segurança da Informação. Todos os Normativos de Segurança da Informação dos níveis Tático e Operacional (políticas específicas, normas internas, procedimentos etc.) devem ser baseados ou refletir as preocupações e considerações estabelecidas por este documento.

2) Políticas específicas de segurança da informação são os documentos que estabelecem regras, orientações e responsabilidades de alto nível dentro das respetivas áreas de Segurança da Informação mapeadas às cláusulas da norma ISO/IEC 27001:2013. As políticas específicas devem, também, ser baseadas ou refletir as preocupações e considerações estabelecidas pela "Política de Segurança da Informação do INEM" e respeitar os "Princípios de Segurança da Informação do INEM";

3) Normas e regras de segurança da informação são os documentos mais detalhados que fazem menção especial às tecnologias, métodos, procedimentos de implementação e outros detalhes, sendo o tempo da sua aplicabilidade inferior ao das políticas, tendo em conta a sua natureza mais técnica. As normas e regras devem ser baseadas ou refletir as preocupações e considerações estabelecidas pela(s) política(s) específica(s) dentro do respetivo domínio de Segurança da Informação.

A documentação dos procedimentos deve ter uma referência à pessoa responsável pelo documento. É necessário que os documentos do **Framework Documental de Segurança da Informação**, sejam geridos e disponibilizados aos interessados, quando necessário. Isto inclui o seguinte:

a) Estabelecer o procedimento administrativo de gestão de documentos

b) Aprovação formal dos documentos antes da sua emissão

c) Assegurar que alterações e atual revisão dos documentos sejam identificadas

d) Proteção e controlo dos documentos como um ativo de informação da organização

6.6. GESTÃO DE INCIDENTES DE SEGURANÇA INFORMAÇÃO

Com a rápida evolução tecnológica e o aparecimento de dispositivos com o objetivo de fornecer suporte aos sistemas de informação, a gestão de eventos de segurança da informação torna-se fundamental para garantir as propriedades básicas de segurança dos recursos críticos." (Seixas, 2013)

Os incidentes de segurança da informação são eventos imprevistos que têm uma elevada probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação (Casaca et al., 2010), os quais têm origem nas vulnerabilidades dos sistemas operativos, abuso das

contas ou permissões inválidas de utilizadores e erros não intencionais dos utilizadores. Ao comprometer a disponibilidade, integridade e confidencialidade da informação, os incidentes de segurança, podem ter consequências desastrosas nos objetivos da organização.

A organização deve assegurar uma abordagem consistente e eficaz relativo à gestão de incidentes de segurança da informação. Para isso, dever-se-á implementar uma plataforma ou adaptar a uma existente, que permita registar em detalhe e classificar os eventos e incidentes de segurança da informação, assim como, registar as ações desencadeadas na resolução e escalonamento.

Definir uma equipa técnica pluridisciplinar ISIRT - *Information Security Incident Response Team* dedicada à análise e resolução de incidentes de segurança da informação com permissões para registar em detalhe as ações realizadas e escalonamento. A formalização da estrutura desta equipa responde ao requisito de controlo A.12.6 Gestão de vulnerabilidades técnicas.

A formalização desta equipa permitirá dar resposta a incidentes de segurança de forma a melhorar a eficácia geral da reação a incidentes de segurança, articulando as suas ações e a partilha de informação relevante com o centro de coordenação da resposta a incidentes (CERT.PT, 2016) a operar no Centro Nacional de Cibersegurança[10].

Para uma eficaz e consistente gestão de incidentes, torna-se necessário:

- Estabelecer um procedimento formal que explicite como analisar e avaliar um evento, atribuir um nível de classificação / severidade ao incidente, matriz de responsabilidades por competência, escalonamento e *reporting*.

- Criar uma equipa técnica pluridisciplinar ISIRT - *Information Security Incident Response Team* dedicada à análise e resolução de incidentes de segurança da informação com permissões para registar em detalhe as ações realizadas e escalonamento.

- Implementar uma plataforma de registo dos eventos e incidentes de segurança da informação, as ações desencadeadas na resolução e escalonamento.

- Estabelecer um estreito contacto com o Centro Nacional de Cibersegurança.

6.6.1. Gestão de incidentes de violação de dados pessoais

Com o objetivo de cumprir o Regulamento EU 2016/679 de 27 abril 2016, deverá o INEM implementar um "sistema de gestão de incidentes de violação de dados pessoais". Este sistema terá como propósito principal, registar e documentar "quaisquer violações de dados pessoais,

[10] Centro Nacional de Cibersegurança desenvolve duas atividades:

1. Em articulação com as restantes autoridades nacionais, emite um código único de perigosidade nacional;
2. Produz e dissemina às partes interessadas, alertas de segurança contendo a seguinte informação:

- Enumeração de sistemas afetados; Descrição da vulnerabilidade em questão; Descrição do impacto causado com a exploração da vulnerabilidade; Medidas para mitigar ou resolver a vulnerabilidade.

http://www.cncs.gov.pt/pagina-inicial/index.html

compreendendo os factos relacionados com as mesmas, os respetivos efeitos e a medida de reparação adotada. Essa documentação deve permitir à autoridade de controlo verificar o cumprimento do disposto no presente artigo."- Regulamento EU 2016/67 Secção 2, artigo 33º.

6.6.2. Gestão de incidentes de segurança: métricas de cibersegurança

A segurança da informação é suportada na identificação e avaliação do risco, a qual tem por base a identificação dos principais ativos críticos da organização e dos possíveis métodos de ataque, passíveis de serem realizados por um adversário, os quais são geralmente executados segundo os vetores de ataque físico, humano e da infraestrutura tecnológica. Neste enquadramento, os controlos de segurança da informação, integram-se nas dimensões de segurança "Organizacional, Física e Ambiental, Humana e Tecnológica", com o principal objetivo de prevenir, detetar, deter, desviar, recuperar ou reagir a uma ameaça (Martins, 2008).

A gestão de incidentes de segurança deverá obter evidências que permitam responder às seguintes métricas e controlos de cibersegurança:

Métricas de Cibersegurança	
1	Número e Tipo de ameaças detetadas
2	Número por tipo de vulnerabilidades descobertas e tratadas
3	Número de incidentes detetados e resolvidos
4	Indicadores de performance da rede dados LAN / WAN
5	Número de mecanismos de segurança implementados
6	Percentagem de *software* sem atualizações (*patches*)
7	Quantidade de *software* instalado sem autorização
8	Número de violações à política de "secretária limpa"
9	Número de violações de segurança informática reportados
10	Percentagem de trabalhadores com formação em TI e/ou cibersegurança
11	Valor da informação e/ou dos ativos críticos
12	Custos associados à perda da confidencialidade, disponibilidade e integridade
13	Número de reclamações associado à violação de dados pessoais

Tabela 3 - Tabela de métricas de cibersegurança

6.7. PROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

O conceito de "risco" tem-se tornado cada vez mais presente na vida das organizações. Desde sempre que o gestor de topo tem presente na sua consciência que gerir a vida da sua organização ou do seu sistema implica também a gestão do risco (Oliveira, 2015).

A gestão de risco é um instrumento facilitador na análise e monitorização dos riscos organizacionais. Este processo de controlo visa otimizar os recursos para melhorar a eficiência e a eficácia, auxiliando os decisores a fazer escolhas conscientes, a priorizar ações com a finalidade de promover a melhoria contínua. (Politica de Gestão do Risco,INEM)

Trata-se de um processo iterativo e contínuo de identificação, análise, avaliação e controlo de fatores de risco, cujo objetivo é reduzir não só a probabilidade de um evento impactante de forma negativa ocorrer, mas também a magnitude do seu impacto.

O processo de gestão de riscos de segurança da informação[11], como mostra a Figura 6-2 pode ser iterativo no processo de avaliação de riscos e/ou para as atividades de tratamento do risco. Um enfoque iterativo na execução do processo de avaliação de riscos torna possível aprofundar e detalhar a avaliação em cada repetição. O enfoque iterativo permite minimizar o tempo e o esforço despendidos na identificação de controlos e, ainda assim, assegura que riscos de alto impacto ou de alta probabilidade possam ser adequadamente avaliados.

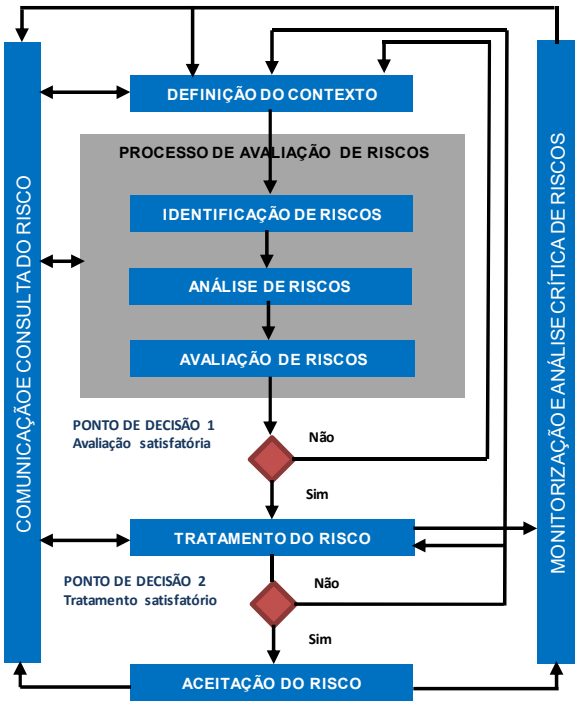


Figura 6-2 Processo de gestão de riscos de segurança da informação
(Fonte ISO/IEC 27005:2008)

[11] O processo de gestão de riscos de segurança da informação, também definido na NP ISO/IEC 27001:2013, está alinhado com as diretrizes genéricas disponibilizadas na NP 31000:2013.

Na primeira iteração, o contexto é estabelecido. Em seguida, executa-se um processo de avaliação de riscos. Se ele fornecer informações suficientes para que se determine de forma eficaz as ações necessárias para reduzir os riscos a um nível aceitável, então a tarefa está completa e o tratamento do risco pode suceder-se. Por outro lado, se as informações forem insuficientes, executa-se uma outra iteração do processo de avaliação de riscos, revendo o contexto (por exemplo: os critérios de avaliação de riscos, de aceitação do risco ou de impacto), possivelmente em partes parciais do seu âmbito - ver Figura 6-2, "Ponto de Decisão 1". A eficácia do tratamento do risco depende dos resultados do processo de avaliação de riscos.

De realçar, que o tratamento de riscos envolve um processo cíclico para:

- avaliar um tratamento do risco;
- decidir se os níveis de risco residual são aceitáveis;
- gerar um novo tratamento do risco, se os níveis de risco não forem aceitáveis; e
- avaliar a eficácia do tratamento.

É possível que o tratamento do risco não resulte num nível de risco residual que seja aceitável. Nessa situação, pode ser necessário uma outra iteração do processo de avaliação de riscos, com mudanças nas variáveis do contexto, seguida para uma fase adicional de tratamento do risco - ver Figura 6-2, "Ponto de Decisão 2".

A atividade de aceitação do risco terá que assegurar que os riscos residuais sejam explicitamente aceitos pelos gestores da organização. Esta aceitação é relevantemente importante para uma situação em que a implementação de controlos é adiada, por exemplo, devido aos custos.

Durante o processo de gestão de riscos de segurança da informação, é importante que os riscos e a forma com que são tratados sejam comunicados ao pessoal das áreas operacionais e gestores apropriados. Mesmo antes do tratamento do risco, informações sobre riscos identificados podem ser muito úteis no âmbito da gestão de incidentes de segurança da informação e ajudar a reduzir possíveis prejuízos.

A consciencialização dos gestores e aos técnicos no que diz respeito aos riscos, à natureza dos controlos aplicados para mitigá-los e às áreas definidas como de interesse pela organização, auxiliam a lidar comos incidentes e eventos não previstos da maneira mais efetiva. Convém que os resultados detalhados de cada atividade do processo de gestão de riscos de segurança da informação, assim como as decisões sobre o processo de avaliação de riscos e sobre o tratamento do risco (representadas pelos dois pontos de decisão 1 e 2, na Figura 6-2), sejam documentados.

A norma NP ISO 27001:2013 especifica que aquando do planeamento do sistema de gestão de segurança da informação, a organização deve determinar os riscos e as oportunidade que têm que ser endereçados, de forma a:

a) assegurar que o SGSI possa atingir os resultados pretendidos;
b) evitar ou reduzir os efeitos indesejáveis;
c) atingir a melhoria contínua.

Num SGSI, a definição do contexto, o processo de avaliação de riscos, o desenvolvimento do plano de tratamento do risco e a aceitação do risco fazem parte da fase de "planeamento".

Na fase "executar" do SGSI, as ações e controlos necessários para reduzir os riscos para um nível aceitável são implementados de acordo com o plano de tratamento do risco. Na fase “verificar” do SGSI, os gestores determinarão a necessidade de revisão da avaliação e tratamento do risco à luz dos incidentes e mudanças nas circunstâncias. Na fase “agir”, as ações necessárias são executadas, incluindo a reaplicação do processo de gestão de riscos de segurança da informação. A Tabela 4, resume as atividades relevantes de gestão de riscos de segurança da informação para as quatro fases do processo do SGSI:

Processo do SGSI	Processo de gestão de riscos de segurança da informação
Planear	Definição de contexto Processo de avaliação de riscos Definição do plano de tratamento do risco Aceitação do risco
Executar	Implementação do plano de tratamento do risco
Verificar	Monitorização e análise crítica dos riscos
Agir	Manter e melhorar o processo de Gestão de Riscos de Segurança da Informação

Tabela 4 - Alinhamento do processo SGSI e do processo de Gestão de Riscos de Segurança da Informação

A ISO/IEC 27005:2008 define como linha de orientação que a organização use o método de avaliação que melhor se adeque às suas circunstâncias, para cada aplicação específica do processo.

Para o objetivo concreto deste projeto, o método de avaliação do risco estará alinhado com a “Política de Gestão do Risco” do INEM, onde engloba “um conjunto de princípios e procedimentos que proporcionam uma atuação pró-ativa na identificação, análise, avaliação e monitorização contínua dos riscos inerentes às diferentes áreas orgânicas.”

6.7.1. Análise e avaliação dos riscos de segurança da informação

No contexto específico de segurança da informação, risco é a possibilidade de uma ameaça explorar vulnerabilidades de um ativo ou conjunto de ativos, do qual pode resultar prejuízo num sistema. É medido em termos de combinação da probabilidade de um evento negativo ocorrer (ex. uma ameaça conseguir explorar uma vulnerabilidade) e as perdas ou prejuízos causados num ativo ou conjunto de ativos. Um Sistema de Gestão de Segurança da Informação "preserva a confidencialidade, integridade e disponibilidade da informação através da aplicação de um processo de gestão do risco" (Norma ISO 2701:2013 p.5).

Deste modo a organização deve definir e aplicar um processo de gestão do risco de segurança da informação que para além de identificar e analisar os riscos, deve avaliar os riscos de segurança da informação.

Identificar os riscos de segurança da informação numa organização é o primeiro passo para o desenho de um sistema de gestão de segurança da informação. Existem três fontes principais para a identificação dos riscos da informação:

1) Uma fonte é obtida a partir da análise de riscos[12] para uma organização, tendo em conta os seus objetivos e estratégias globais. Através da análise de riscos, poder-se-á identificar as ameaças e vulnerabilidades aos ativos de informação e realizar uma estimativa da probabilidade[13] de ocorrência das ameaças e do impacto potencial que poderá ter nos processos funcionais e operacionais.

2) Uma outra fonte é a legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que a organização tem com os seus parceiros, colaboradores e fornecedores de serviços, além do seu ambiente sociocultural.

3) A terceira, é um conjunto particular de princípios, objetivos e os requisitos de negócio para o processamento de informação que uma organização tem que desenvolver para apoiar as suas operações.

Nesta fase do projeto, cujo foco é identificar, analisar e avaliar os riscos de segurança da informação, tomou-se como critérios para a classificação e avaliação do risco as escalas que estão definidas e aplicadas na organização do INEM, inscrita na "Politica de Gestão do Risco" em vigor desde janeiro de 2016.

---

[12] Processo destinado a compreender a natureza do risco e a determinar o nível de risco. A análise do risco fornece a base para a avaliação do risco e as decisões sobre o tratamento do risco. (NP ISO 31000:2013)

[13] Na terminologia da gestão do risco, a palavra probabilidade é o termo equivalente de verosimilhança, utilizada para indicar a possibilidade de algo ocorrer, quer essa possibilidade seja definida, medida ou determinada de forma objetiva ou subjetiva, qualitativa ou quantitativamente [como uma probabilidade ou frequência num determinado período de tempo]. (NP ISO 31000:2013)

Tomou-se esta opção, atendendo que a gestão do risco deve estar integrada em todos os processos e práticas da organização para que possa ser eficaz e eficiente. Nesta medida, importa definir a sua abrangência, os seus objetivos e a forma como vai ser implementada. O processo de gestão de riscos do INEM foi definido com base no Processo de Gestão de Riscos sugerido pela norma ISO 31000:2013 – Gestão do risco – Princípio e linhas de orientação.

A norma NP ISO 31000:2013 recomenda que "as organizações desenvolvam, implementem e melhorem continuamente uma estrutura cujo objetivo é integrar um processo para gerir o risco na governação, estratégia e planeamento, gestão, processos de reporte, políticas, valores e cultura".

6.7.2. Categorização do Risco

A norma NP ISO 31000:2013 define risco de uma forma abrangente e generalista: "Efeito da incerteza na consecução dos objetivos."Sendo que, um efeito é um desvio, positivo ou negativo, relativamente ao esperado. A incerteza é o estado, ainda que parcial, de deficiência de informação relacionada com a compreensão ou conhecimento de um evento, sua consequência e probabilidade.

O risco é frequentemente caraterizado pela referência aos eventos potenciais e consequências ou à combinação de ambos. Também com frequência se expressa o risco como a combinação das consequências de um dado evento e a respetiva probabilidade de ocorrência.

É importante compreender que os riscos são classificados de diversas maneiras e podem manifestar-se de formas diferentes. Deve ter-se em consideração que cada organização é única e, como tal, deverão definir-se os seus riscos específicos. A "Política de Gestão do Risco" do INEM, define que as categorias do risco são inseridas em diferentes níveis e áreas, sendo elas:

Estratégicos	Riscos relacionados com a implementação da estratégia da organização;
Regulamentares	Riscos relacionados com requisitos e alterações do enquadramento legal e regulamentar;
Envolvência	Riscos internos e de relacionamento externo, inerentes ao contexto económico, sociocultural e político onde a organização se insere;
Financeiros	Riscos relacionados com a gestão financeira e contratação pública;
Recursos Humanos	Riscos relacionados com a gestão dos recursos humanos, entre outros, processos de recrutamento e vencimentos;
Operacionais	Riscos associados às operações da organização, incluindo, entre outros, desempenho operacional, segurança e saúde no trabalho, segurança das infraestruturas e equipamentos e gestão ambiental.

Tabela 5 - Categorias de Risco

6.7.3. Método de Avaliação do Risco

A norma NP ISO 31000:2013 define que a análise de riscos envolve a apreciação das causas e das fontes de risco, as suas consequências positivas e negativas, e a probabilidade de que essas consequências possam ocorrer.

A finalidade da avaliação de riscos é auxiliar na tomada de decisões com base nos resultados da análise de riscos, sobre quais riscos necessitam de tratamento e a prioridade para a implementação do tratamento (NP ISO 31000:2013).Compara o nível de risco encontrado durante o processo de análise com os critérios de risco estabelecidos quando o contexto foi considerado.

Inserido no processo de análise e avaliação de riscos, será utilizada uma matriz de risco, baseada nas variáveis da probabilidade e impacto, apresentada com o seguinte modelo:

Área	Identificação do Risco	Avaliação do Risco			Medidas a implementar	Responsável
		Probabilidade	Impacto	Nível de Risco		

Tabela 6 - Matriz de Avaliação do Risco

Para tal, é necessário definir a probabilidade e o impacto/gravidade/severidade (conforme a situação).

Probabilidade – (P) – O nível de probabilidade reflete a verificação de uma ou mais condições que é razoável esperar de um incidente envolvendo o fator de risco avaliado.

Nível	Classificação	Descrição
1	Muito remota	Probabilidade de 1 ocorrência até uma vez em cada 50 anos (P ≤ 1 ocorrência / 50 anos)
2	Remota	Probabilidade de 1 ocorrência em cada 5 anos (1 ocorrência / 50 anos <P ≤ 1 ocorrência / 5 anos)
3	Improvável	Probabilidade de 1 ocorrência em cada ano (1 ocorrência / 5 anos <P ≤ 1 ocorrência / ano)
4	Provável	Probabilidade de 1 ocorrência por mês (1 ocorrência / ano <P ≤ 1 ocorrência / mês)
5	Frequente	Probabilidade de ocorrência mais do que uma vez por mês (P> 1 ocorrência / mês)

Tabela 7 - Tabela da Probabilidade

Impacto – (I) – Perda ou ganho na ocorrência de uma ameaça. Pode ser determinado pela avaliação e pelo processamento de vários resultados da ocorrência de um evento ou pela extrapolação de estudos experimentais ou dados e registos do passado.

Nível	Classificação	Descrição
1	Baixo	Degradação de operações, atividades, projetos, programas ou processos da organização, que causam impactos mínimos nos objetivos (prazo, custo qualidade, imagem, etc.) relacionados com as metas ou padrões ou com a capacidade de entrega de produtos/serviços às partes interessadas (clientes externos/internos, beneficiários).
2	Ligeiro	Degradação de operações, atividades, projetos, programas ou processos da organização, causando impactos pequenos nos objetivos.
3	Moderado	Interrupção de operações ou atividades da organização, de projetos, programas ou processos, que causam impactos significativos nos objetivos, porém recuperáveis.
4	Grave	Interrupção de operações, atividades, projetos, programas ou processos da organização, que causam impactos de reversão muito difícil nos objetivos.
5	Muito Grave	Paralisação de operações, atividades, projetos, programas ou processos da organização, que causam impactos irreversíveis nos objetivos.

Tabela 8 - Tabela do Impacto

O risco é classificado em função da combinação do Impacto (I) e da Probabilidade (P).

(P x I = Risco)

Para determinar qualitativamente o nível de risco, dever-se-á multiplicar a Probabilidade (P) pelo Impacto (I). Recorrendo à tabela infra podemos identificar o nível de risco associado a um determinado risco identificado.

***NIVEIS DE RISCO* = (P x I = Risco)**					
Probabilidade / *Impacto*	*1* *Muito Remota*	*2* *Remota*	*3* *Improvável*	*4* *Provável*	*5* *Frequente*
1 - Baixo	***1***	***2***	***3***	***4***	***5***
2 - Ligeiro	***2***	***4***	***6***	***8***	***10***
3 - Moderado	***3***	***6***	***9***	***12***	***15***
4 - Grave	***4***	***8***	***12***	***16***	***20***
5 - Muito Grave	***5***	***10***	***15***	***20***	***25***

Tabela 9 - Tabela de avaliação dos níveis de risco

O código das cores da tabela matriz constitui a base de decisão sobre a aceitabilidade do risco e sobre as medidas de prevenção e controlo a desencadear.

Como ilustrado na Tabela 10 em baixo, deverão ser estabelecidas as prioridades e os respetivos prazos de atuação. De entre os níveis de risco, será de priorizar por um lado, os de mais fácil implementação e, por outro lado, os de grau de risco mais elevado.

NIVEIS DE RISCO / PRIORIDADES DE INTERVENÇÃO / PRAZOS		
Nível de Risco	Prioridade de Intervenção	Prazo
1 – Baixo [1-4]	Atuação não prioritária	*Logo que possível*
2 – Significativo [5-9]	Intervenção a médio prazo	*06 Meses*
3 – Elevado [10-15]	Intervenção a curto prazo	*03 Meses*
4 - Muito Elevado [16-20]	Atuação urgente	*01 Mês*
5 – Inaceitável (25)	Atuação muito urgente	*Imediato*

Tabela 10 - Tabela de estabelecimento de prioridades

Como resultado desta análise será definido uma lista de riscos priorizada, de acordo com os critérios de avaliação de riscos, em relação aos cenários de incidentes que podem levar esses riscos.

6.7.4. Tratamento do Risco de Segurança da Informação

Após uma análise dos riscos e contrapondo com o nível de risco que se considera adequado face à avaliação realizada, haverá uma decisão quanto ao tratamento a dar ao risco em causa. As opções do tratamento do risco devem ser selecionadas com base no resultado do processo de avaliação de riscos, no custo calculado para a implementação dessas opções e nos benefícios previstos.

A noma ISO/IEC 27005:2008 define como diretrizes para o tratamento do risco quatro opções:
i) modificação do risco; ii) retenção do risco; iii) ação de evitar o risco e iv) partilha do risco. O tratamento do risco é a implementação de medidas que permitam modificar o risco, passando a haver um maior controlo ou diminuição do mesmo.

i) **Ação de modificação do risco** – esta atividade compreende a aplicabilidade de controlos apropriados e devidamente justificados, de modo a satisfazer os requisitos legais, regulatórios e contratuais. Esta opção deverá ter e conta custos e prazos para a implementação dos controlos, além de aspetos técnicos, culturais e ambientais.

ii) **Retenção / Aceitar o risco** – após uma análise e avaliação crítica do possível plano de tratamento do risco, a organização poderá decidir aceitar as condições do risco, sem outras ações adicionais. Se o nível de risco atende aos critérios para a aceitação do risco, não há necessidade de se implementar controlos adicionais e pode haver a retenção do risco. A NP 27001:2013 no item 6.1.3 na alínea f) preconiza que "*obter por parte dos responsáveis pelos riscos a aprovação do plano de tratamento do risco de segurança da informação e a aceitação dos riscos residuais de segurança da informação*." Para além de

que "*a organização deve manter informação documentada sobre o processo de tratamento do risco de segurança da informação*."

iii) **Ação de evitar o risco** – esta atividade ou condição terá como origem que o determinado risco seja evitado. Quando os riscos identificados são considerados demasiado elevados e quando os custos de implementação de outras opções de tratamento do risco excederem os benefícios, pode-se decidir que o risco seja evitado completamente, seja através da eliminação de uma atividade planeada ou existente (ou de um conjunto de atividades), seja através de mudanças nas condições em que a operação da atividade ocorre. Por exemplo, para riscos causados por danos naturais, pode ser uma alternativa mais rentável transferir fisicamente as instalações de um *data center* para um local onde o risco não existe ou está sob controlo.

iv) **Partilha do risco** – A ação de partilhar um risco envolve a decisão de partilhar certos riscos com entidades externas. A partilho do risco pode criar novos riscos ou modificar riscos existentes e identificados. A partilha poderá ser efetuada através da contratação de um seguro que cubra as consequências ou através da subcontratação de um parceiro cujo papel seja monitorizar o sistema de informação e tomar medidas imediatas que impeçam um ataque antes que ele possa causar um determinado nível de dano ou prejuízo.

De realçar que é possível partilhar a responsabilidade da gestão de riscos, no entanto não é normalmente possível partilhar a responsabilidade legal por um impacto. Os clientes/utentes provavelmente irão atribuir um impacto adverso como sendo falha da organização.

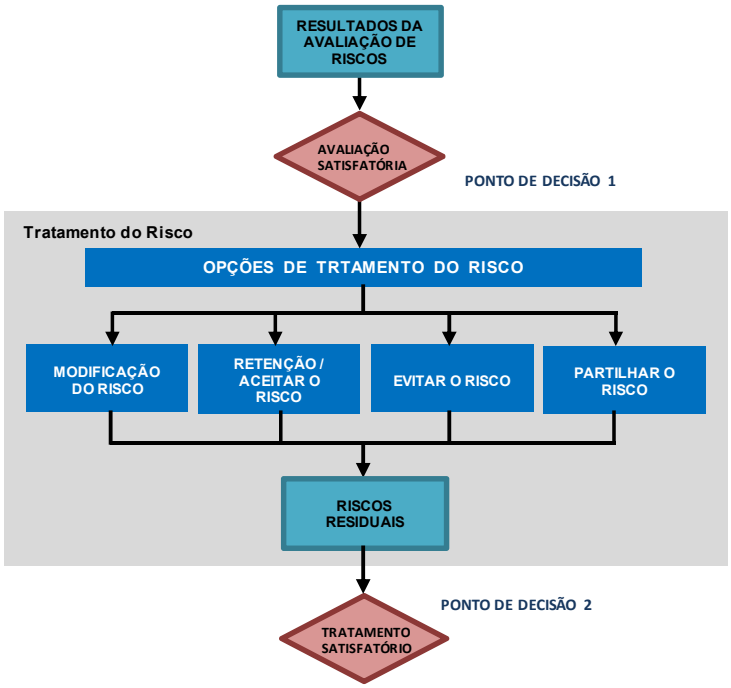


Figura 6-3 Atividade de tratamento do risco
(Fonte ISO/IEC 27005:2008)

As quatro opções para o tratamento do risco não são mutuamente exclusivas. Por vezes, a organização pode beneficiar substancialmente de uma combinação de opções, tais como, a redução da probabilidade do risco, a partilha ou retenção dos riscos residuais. Algumas formas de tratamento do risco podem lidar com mais de um risco de forma efetiva, por exemplo, a formação técnica para um grupo específico da organização e a consciencialização em segurança da informação direcionada para toda a comunidade de uma organização.

A ISO/IEC 27005:2008 refere nas suas diretrizes que a definição de um plano de tratamento do risco deve identificar claramente a ordem de prioridade e quais as formas específicas de tratamento do risco a serem implementadas, assim como os seus prazos de execução.
As informações sobre os riscos devem ser trocadas e/ou partilhadas entre o responsável da decisão e todas as outras partes interessadas e envolvidas. O desenvolvimento plano de comunicação dos riscos deverá contemplar as operações normais / rotineiras, mas também, as situações de emergência. Pelo que, a atividade de comunicação dos riscos deve ser realizada de forma contínua.

6.7.5. Matriz de Risco

Seguindo a "boa prática", após a definição da metodologia para a avaliação do risco foi realizada a Matriz de Risco no âmbito das responsabilidades do Gabinete de Sistemas e Tecnologias da Informação (GSTI), inscritas nos estatutos do INEM[14], mas também, nos ativos da infraestrutura de suporte aos sistemas e tecnologias de informação, atualmente no INEM. Tendo presente as categorias de risco enunciadas na "Política de Gestão de Risco" do INEM, a identificação e a avaliação do risco fez-se em seis dimensões:

(i) riscos estratégicos relacionados com a organização;
(ii) regulamentares de enquadramento legal;
(iii) de envolvência no seu relacionamento interno e externo;
(iv) financeiros relacionados com a gestão financeira e contratação pública;
(v) com a gestão dos recursos humanos no processo de recrutamento e formação; e
(vi) riscos operacionais relacionados com o desempenho e gestão operacional.

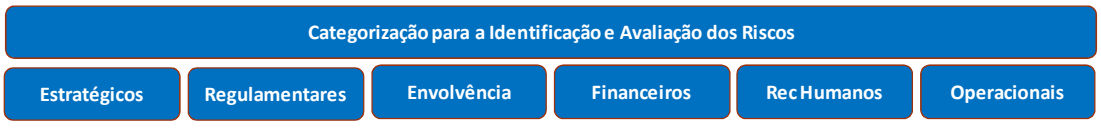


Figura 6-4 Dimensões na identificação e avaliação dos riscos

A metodologia aplicada para a elaboração da Matriz de Risco teve a participação de um número alargado de membros do GSTI, através de grupos de trabalho focalizados na identificação de

[14] Estatutos do INEM, Portaria nº 158/2012, publicado no Diário da Republica, 1º série – Nº99-22 de maio de 2012.

ameaças e vulnerabilidades existentes e a estimativa da probabilidade de ocorrência e potencial impacto, conforme o método definido para a avaliação de risco (item 6.6.3 – Método de Avaliação do Risco).

A Matriz de Risco produzida após a identificação e avaliação do nível de risco permitiu elaborar uma das mais importantes etapas do planeamento do SGSI, o plano de tratamento de risco. Para cada risco identificado foi definida a(s) medida(s) a implementar, correspondente ao plano de ação de tratamento. O plano de ação apresentado tem listado e registado para cada ameaça ou risco, uma medida de tratamento com a identificação do responsável pela sua implementação, para além da informação detalhada da ação que será efetuada.

Deve-se salientar que a maioria das apreciações de risco, bem como a maioria dos processos de gestão de risco implementados, não visam a obtenção de um sistema totalmente seguro, até porque na maioria das vezes isso seria impossível. Em vez disso, o objetivo final é chegar aquilo que possa ser entendido como o nível de segurança aceitável a um custo aceitável. As diversas *frameworks* existentes neste contexto diferem na interpretação que fazem deste processo e no modo como o conseguir e manter (Oliveira, 2015). Por outro lado, devemos estar consciente que " a gestão do risco é um processo contínuo e que não termina com a implementação de uma medida de segurança. Através de uma monitorização constante, é possível identificar quais as áreas bem sucedidas e quais precisam de revisões e ajustes." (Martins, A e Santos, C. (2005).

7. AUTOAVALIAÇÃO DOS REQUISITOS DE CONTROLO

A avaliação aos requisitos de controlo permite conhecer qual o atual estado da capacidade que a organização tem na resposta aos requisitos de controlo especificados na norma ISO/IEC 27001 e, deste modo, poder proceder com uma clara definição do plano de implementação do SGSI. Para tal, optou-se como plano de ação, materializar os requisitos e objetivos de controlo, através de uma ferramenta que permita ler e analisar, em qualquer altura, o estado de implementação dos controlos em cada uma das secções de A.5 a A18, definido no *Quadro A.1 Objetivo de Controlo e Controlos, do Anexo 1* (NP ISO/IEC 27001:2013).

Com o objetivo de "tirar a fotografia" da situação atual, foi elaborado um questionário onde está formulado um conjunto de questões específicas para cada controlo de referência e seus objetivos. O conjunto de questões formuladas está fundamentado na ISO/IEC 27002:2013, por ser o instrumento preconizado no estabelecimento de diretrizes e princípios gerais para a gestão de segurança da informação.

Este questionário insere perguntas fechadas predefinidas e questões abertas. Das 14 cláusulas de controlos de segurança (A.5 a A.18), com um coletivo total de 114 controlos, foram formuladas 318 questões, com a seguinte distribuição:

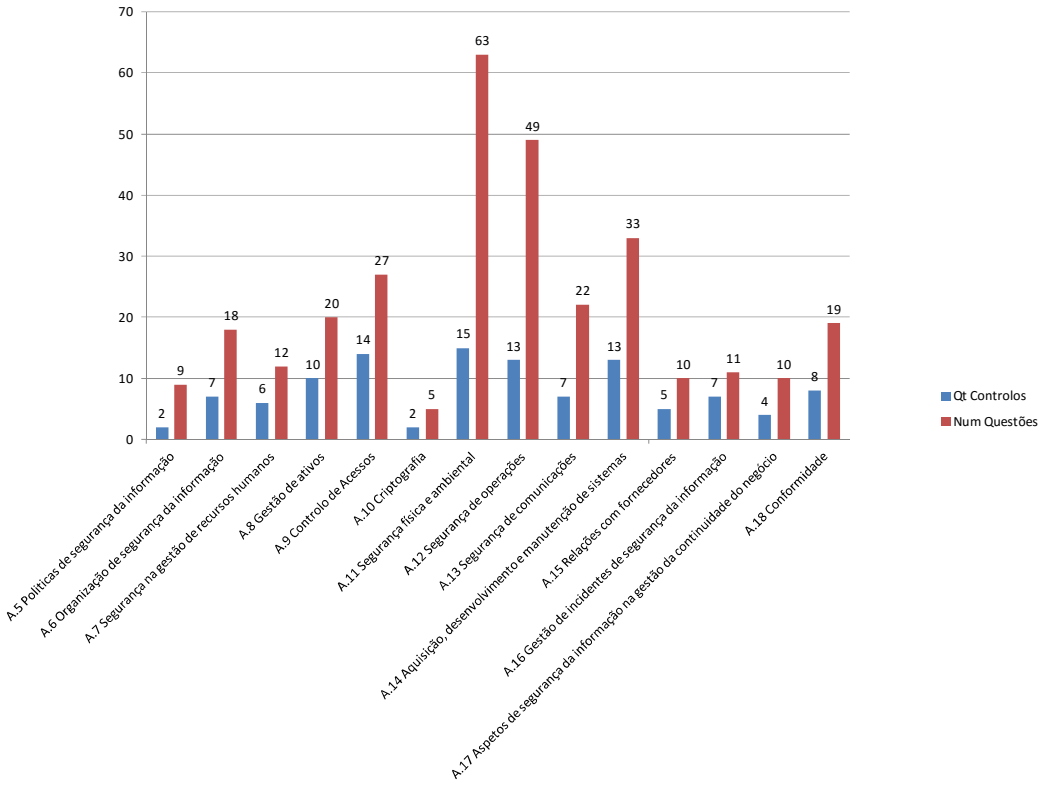


Figura 7-1 Relação entre o número de controlos e questões formuladas

As entrevistas com um carácter semi-diretivo, permitiram recolher a informação necessária sobre os processos organizacionais, as suas relações interfuncionais, os recursos envolventes, identificar vulnerabilidades e pontos de melhoria.

7.1. RELATÓRIO DE AVALIAÇÃO DOS REQUISITOS DE CONTROLO

O relatório de análise e avaliação dos requisitos de controlo foi obtido através de reuniões com membros da equipa do GSTI, com a formalização de questões específicas para cada controlo de referência e seus objetivos, inseridos no âmbito do SGSI. Esta análise pretendeu obter evidências na aplicabilidade, envolvimento e desenvolvimento de boas práticas em resposta aos requisitos da NP ISO/IEC 27001:2013 e, deste modo, avaliar qual o atual nível de maturidade da organização fornecendo bases de orientação ao cumprimento dos objetivos de controlo.

No final, foi produzida documentação e colocada à disposição do Conselho Diretivo, do GSTI e todos os elementos relacionados com a segurança da informação, onde está descriminado a situação atual face ao objetivo de controlo, qual o atual nível de maturidade ou de capacidade, a análise de risco associada e as ações a desenvolver.

Para averiguar o nível de maturidade[15] / capacidade, no âmbito da implementação do Sistema de Gestão de Segurança da Informação, foi aplicado o "Modelo de Capacidade das boas práticas eSIS"[16] onde estabelece seis níveis de capacidade e cujo conteúdo descritivo é semelhante aos níveis de maturidade caracterizados pelo *Framework* CobiT, a descrição é a seguinte:

Níveis de Maturidade / Capacidade		
Nível 0 – INEXISTENTE – A boa prática não é aplicável. Não existe qualquer política, procedimento, boa prática reconhecível. A Entidade ainda não reconheceu a necessidade de implementar a boa prática.	**Nível 2 – AD-HOC** – As boas práticas foram desenvolvidas até o estágio em que práticas similares são seguidas por diferentes pessoas. Não há formação formal ou comunicação das boas práticas e a responsabilidade é individual. Existe uma alta confiança no conhecimento das pessoas, havendo erros comuns.	**Nível 4 – GERIDO** – A gestão monitoriza e mede a conformidade com as boas práticas e toma ações quando estas parecem não funcionar efetivamente. As boas práticas baseiam-se em referenciais de indústria e estão sob constante melhoria. São utilizadas ferramentas e automação de uma maneira limitada e fragmentada. Existem evidências substanciais para auditorias.
Nível 1 – INICIAL – Existe uma evidência que a Entidade reconheceu que a prática deve ser implementada. No entanto, não há qualquer boa prática padronizada; existem algumas boas práticas aplicadas caso-a-caso por iniciativas individuais. O desenvolvimento das boas práticas foi iniciado, mas ainda vai exigir o trabalho significativo para cumprir requisitos.	**Nível 3 – DEFINIDO** – As boas práticas foram documentadas, formalizadas e comunicadas em ações de formação. É obrigatório que as boas práticas sejam seguidas; no entanto, as mesmas ainda não estão implementadas e ativamente apoiadas pela gestão de topo. É pouco provável que sejam detetados desvios. As boas práticas não são sofisticadas, representam apenas a formalização das práticas existentes.	**Nível 5 – OTIMIZADO** – As boas práticas foram aperfeiçoados ao nível de melhores práticas, baseando-se no resultado de melhorias contínuas e comparação com outras entidades similares. Os sistemas TIC são utilizados de forma integrada para automatizar fluxos de trabalho.

[15] O termo "maturidade" refere-se ao grau de formalidade e otimização de processos, de práticas *ad hoc*, passos definidos formalmente, para as métricas de processos formalmente bem definidos, para no final obter uma otimização ativa dos processos. (CobiT,2015)

[16] O "Modelo de Capacidade das boas práticas eSIS" é um documento emitido pela SPMS para ser utilizado no âmbito do programa de promoção da "Framework de referência de governança e gestão eSIS" junto das Entidades do SNS, onde o INEM se insere.

Cada nível de capacidade é constituído por um conjunto de objetivos a alcançar (atividades a realizar) aplicáveis ao processo de implementação do Sistema de Gestão de Segurança da Informação.

O modelo de capacidade é concebido de tal forma que a capacidade nos níveis inferiores fornece progressivamente bases para os níveis superiores, orientando a Entidade a subir de nível e melhorar de forma incremental boas práticas implementadas (Modelo de Capacidades das boas práticas eSIS, 2016).

A opção pela utilização do "Modelo de Capacidade das boas práticas eSIS", é substanciada por ser um modelo comum de avaliação a ser utilizado pelas Entidades do eSIS, onde o INEM se insere, seguindo as boas práticas implementadas, neste caso na Gestão do Risco e da Segurança.

Esta leitura gráfica fornece os dados necessários para a progressão do objetivo que a instituição pretende atingir. A capacidade descrita nos níveis inferiores fornece progressivamente bases para os níveis superiores, orientando o INEM a subir de nível aplicando e implementando progressivamente atividades na Gestão do Risco e Segurança. Após a finalização das avaliações de todos os controlos, as ações a implementar irão dar fundamento a planos de ação.

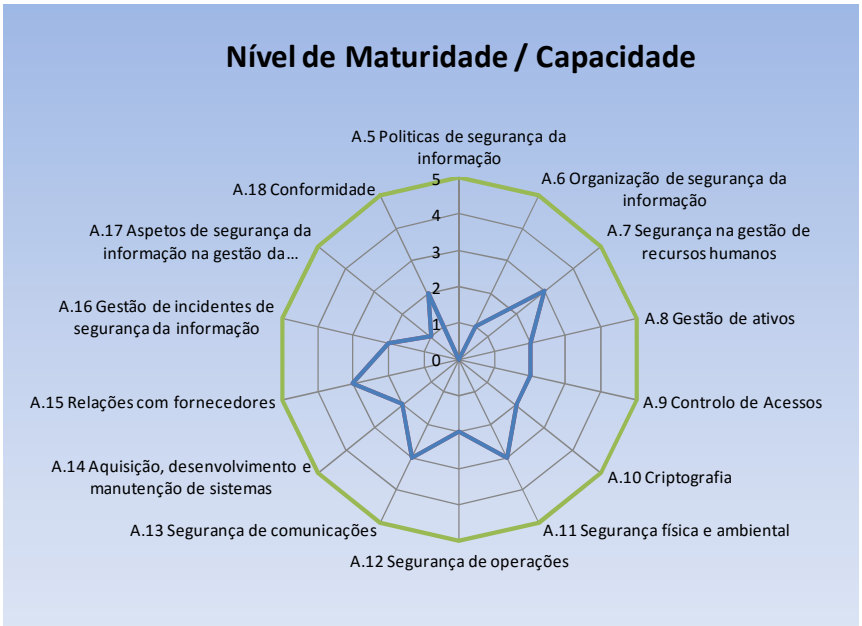


Figura 7-2 Níveis de maturidade obtidos

De realçar que a instituição não possuía, no início dos trabalhos uma avaliação formal dos riscos especificamente relacionados com a segurança da informação. Considerou-se que uma análise completa dos controlos de segurança da informação seria o caminho adequado para apurar o atual nível de maturidade e identificação dos riscos.

Pela análise dos resultados obtidos, considera-se que as boas práticas relacionadas com os processos de segurança da informação possuem um nível de maturidade médio geral de 2. Por outro lado, existem processos com nível de maturidade adequada à sua realidade, estando classificado de nível 3. Isto significa que, de forma geral, há um reconhecimento à boa prática

nos processos relacionados com a gestão de segurança da informação e que alguns dos processos estão em desenho estrutural para serem definidos e implementado formalmente. Existe um conhecimento tácito nos elementos da equipa do GSTI que lhes permite realizar com confiança a maioria dos suas tarefas, pelo que muitos dos processos tem uma responsabilidade única não havendo uma partilha do "saber fazer" e formal documentação, formação e/ou transmissão de conhecimento. Diversos planos de ação criados têm como propósito formalizar e realizar pequenas melhorias em processos, não estando necessariamente relacionados a incrementos do nível de maturidade.

Por outro lado, existem planos de ação que estão em fase de análise técnica – projeto piloto e provas de conceito (POC), pela necessidade imperiosa da sua implementação, com o objetivo de satisfazer os requisitos e os riscos identificados. Inserido neste grupo de planos de ação com carácter prioritário, existem alguns que necessitam de recursos financeiros elevados ou exigem mudanças maiores em processos, pelo que serão acompanhados em pormenor pela coordenação. No entanto, os planos de ação que não necessitam de recursos financeiros elevados foram selecionados para serem executados, também, em primeira instância.

Como anteriormente referido, esta é a avaliação do momento, de acordo com os *inputs* fornecidos. Pelo que, a cada novo ciclo de avaliação os controlos aplicáveis serão reavaliados e os planos de ação revistos.

8. DECLARAÇÃO DE APLICABILIDADE

A Declaração de Aplicabilidade é um documento de relevante importância e utilidade no processo de implementação da NP ISO/IEC 27001:2013 e um dos principais *deliverables* da fase de planeamento. Este documento é a principal ligação entre a avaliação, tratamento de riscos e a implementação do sistema de segurança da informação onde está definido, o que se pretende, ou seja, o que fazer com a segurança da informação, fornecendo uma visão geral mas, efetiva do que precisa de ser feito, porque é que precisa de ser feito e como precisa de ser feito. É um documento direcionado aos gestores de topo/intermédios e auditores, pelo que deverá apresentar uma linguagem e um *interface* com adequada leitura, não sendo direcionado para o quotidiano operacional.

Em síntese, a Declaração de Aplicabilidade deve conter:

- Controlos selecionados
- Razão ou razões para a seleção dos controlos
- Objetivos de controlos e controlos atualmente implementados
- Exclusões (incluindo justificação para a exclusão)
- Interface com fácil leitura

Deve-se "produzir uma Declaração de Aplicabilidade que contenha os controlos necessários e a justificação para as inclusões dos controlos, estejam eles implementados ou não, em como a justificação para as exclusões dos controlos do Anexo A." (NP ISO/IEC 27001 6.1.3.d), p.9), ou seja, a Declaração de Aplicabilidade deve documentar para cada controlo aplicável se já está implementado ou não e a forma como cada controlo é implementado, como por exemplo, fazendo referencia a um documento (política, processo, instrução de trabalho, etc.) ou descrevendo o procedimento ou tecnologia/equipamento utilizado na implementação da medida de segurança.

Por outro lado, um controlo pode ser justificado como "não aplicável", se realmente não for possível aplica-lo ou a sua aplicabilidade está fora do alcance e do âmbito da organização. Controlos "não aplicados" são também controlos com inexistência de risco e que seja justificável serem controlos "não aplicáveis", ou pela sobreposição de um outro controlo.

8.1. DECLARAÇÃO DE APLICABILIDADE: EIXOS DE AÇÃO

Na prática, a Declaração de Aplicabilidade remete claramente para o "Relatório de análise e avaliação dos requisitos de controlo", onde de forma detalhada descreve os objetivos e os controlos aplicados e a aplicar no Sistema de Gestão da Segurança da Informação na instituição do INEM e a forma como serão aplicados.

Contudo e tendo presente que a Declaração de Aplicabilidade é direcionada para os gestores, auditores e decisores, tomou-se como abordagem apresentar o plano de ação de forma concisa e com uma linguagem sem vínculo literalmente tecnicista. O plano de ação está assente em cinco eixos de ação: Organizacional, Físico e Ambiental, Pessoal, Tecnológico e Conformidade & Regulação, no horizonte temporal 2017-2018.

Os eixos de ação indicados - **Organizacional, Físico e Ambiental, Pessoal, Tecnológico e Conformidade & Regulação**, resultam da perceção de que a segurança da informação "como matéria transversal que é, deve envolver todos os níveis da organização e ser encarada como um facilitador dos processos e aumentar os níveis de confiança internos e externos. É este o grande argumento sobre o qual qualquer organização poderá capitalizar o seu investimento nesta área. Ao implementar este programa, estará a transmitir uma imagem de preocupação nesta matéria, cada vez mais importante e com maior visibilidade, conseguindo simultaneamente gerir o risco a que se encontra sujeita." (Silva et al. 2003).

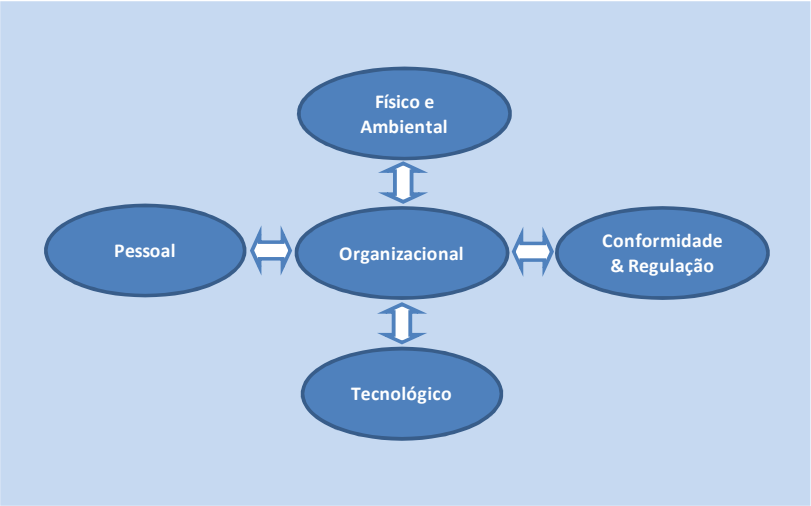


Figura 8-1 Eixos de Ação

Na seleção das medidas apresentadas, procurou-se considerar como critérios de validação:

- A existência de justificação para a sua necessidade com base na análise e avaliação de risco, anteriormente realizada;
- É específico, mensurável, alcançável dentro de um período de tempo aceitável e é realista a sua implementação;
- Leva à criação de procedimentos ou instruções de trabalho para resolver ou limitar o problema e à necessidade de atribuir responsabilidades de controlo;
- Impera a implementação com nova tecnologia, face ao carácter obsoleto e a não garantia ao modelo conceptual do SGSI.

De realçar que, existe uma relação entre os eixos de ação e as medidas propostas. No entanto, é relevante a sequência com que devem ser implementadas. Para isso, deverá ser aplicado as prioridades e os respetivos prazos estabelecidos de acordo com a tabela que relaciona os níveis de risco com o prazo / prioridade de intervenção.

8.2. EIXO I: ORGANIZACIONAL

O **eixo de ação I: Organizacional**, tem como finalidade proporcionar diretrizes e estabelecer um modelo de operacionalização no apoio à implementação e gestão para a segurança da informação na instituição do INEM.

Para o **Eixo I – Organizacional** são definidas quatro Medidas, que se desenvolvem a seguir, a saber:

Medida 1: Política de Segurança da Informação

Medida 2: Estrutura organizacional de segurança da informação

Medida 3: Liderança e Comprometimento

Medida 4: *Framework* documental do SGSI

Para cumprir com os requisitos do **Eixo I** deverão ser executadas as seguintes ações:

M1: Política de Segurança da Informação

- Definir e Aprovar Política de Segurança da Informação
- Comunicar e Disponibilizar a Política de Segurança da Informação

Medida 1 - Política de Segurança da Informação				
	Ações	**Descrição**	**Conclusão**	**Responsável e Participante**
Definir e Aprovar Política de Segurança da Informação				
1.1.1	Estabelecer política de segurança da informação	Uma política de segurança que seja um comprometimento com os requisitos aplicáveis com a NP 27001:2013; desenhada ao propósito da missão do INEM; um modelo de referência na definição clara da estratégia e dos objetivos relacionados com a segurança da informação e melhoria contínua.	1ºtrimestre 2017	CD e GSTI; GQ
1.1.2	Rever política de segurança da informação	Estabelecer plano de revisão da política de segurança da informação, no mínimo, anual ou sempre que se justifique aos objetivos do INEM.	1ºtrimestre 2018	CD e GSTI; GQ

(continua)

Medida 1 - Política de Segurança da Informação (continuação)				
	Ações	**Descrição**	**Conclusão**	**Responsável e Participante**
Comunicar e Disponibilizar a Política de Segurança da Informação				
1.1.3	Estabelecer ações de comunicação da política de segurança da informação	Definição de um programa de comunicação da política de segurança da informação a todos os colaboradores, parceiros e prestadores de serviços do INEM, com o propósito do adequado entendimento e compromisso de todas as partes.	1ºtrimestre 2017	CD e GQ; GMC
1.1.4	Disponibilizar a política de segurança da informação	Estabelecer uma plataforma com vários canais de comunicação e disponibilidade da política de segurança da informação e que esta esteja acessível e atualizada.	1ºtrimestre 2017	GQ; GMC

Medida 2: Estrutura organizacional de segurança da informação

- Responsabilidades e Cargos
- Contacto com autoridades competentes e grupos de interesse

Medida 2 - Estrutura organizacional de Segurança da Informação				
	Ações	**Descrição**	**Conclusão**	**Responsável e Participante**
Responsabilidades e Cargos				
1.2.1	Atribuir responsabilidades, cargos e autoridades	Definir uma estrutura organizacional enquadrada com a segurança da informação (ver detalhe, subcapítulo 6.4 Responsabilidades e Cargos), em destaque: Conselho Diretivo como órgão responsável pela promoção do SGSI; Gestor de Segurança da Informação (CISO); Comité de Segurança da informação; Equipa técnica pluridisciplinar; Responsáveis de processo e dos ativos de segurança da informação.	1ºtrimestre 2017	CD

		A gestão de topo deve assegurar que os recursos necessários para o SGSI estão disponíveis, de modo a garantir que o SGSI está em conformidade com os requisitos e comunicados internamente na organização e reportam o seu desempenho.		
Contacto com autoridades competentes e grupos de interesse				
1.2.2	Estabelecer protocolos com autoridades estaduais	Estabelecer protocolo articulado com o Gabinete Nacional de Segurança; CERT.PT (Centro Nacional de Cibersegurança); SPMS no enquadramento das entidades do eSIS (ecossistema dos Sistemas Informação da Saúde); CNPD (Comissão Nacional Proteção de Dados); ANACOM (Autoridade Nacional de Comunicações)	2ºtrimestre 2017	Gestor da Segurança; Encarregado da Proteção de Dados; Gabinete de Crise
1.2.3	Manter contactos com grupos especializados em segurança de informação	Devem ser mantidos contactos apropriados com grupos e associações vocacionadas e especializadas em segurança da informação, e.g., Grupo Segurança na Sociedade da Informação (GSSI); Associação Portuguesa para a Promoção da Segurança da Informação (AP2SI); Proteccaodedados; Associação Portuguesa de Cibersegurança (APCIBER).	2ºsemestre 2017	Gestor da Segurança e GSTI

Medida 3: Liderança e Comprometimento

- Assegurar alinhamento na Política de Segurança
- Promover melhoria contínua

Medida 3 - Liderança e Comprometimento				
	Ações	**Descrição**	**Conclusão**	**Responsável e Participante**
Assegurar alinhamento na Política de Segurança da Informação				
1.3.1	Comprometimento e apoio visível da direção para com o SGSI	A gestão de topo deve assegurar que a política de segurança da informação está alinhada e integrada com a estratégia e a missão do INEM, comunicando a sua importância na	2ºsemestre 2017	CD

		gestão operacional e que todas as funções são relevantes para os resultados pretendidos.		
Promover a melhoria contínua				
1.3.2	Proporcionar a aplicabilidade de melhoria contínua no SGSI	Estabelecer na gestão de topo um compromisso para a melhoria contínua do sistema de gestão de segurança da informação.	2ºtrimestre 2017	Comité de Segurança

Medida 4: Framework documental do SGSI

- Estrutura documental
- Responsabilidades pela gestão documental

Medida 4 - Framework documental do SGSI				
	Ações	**Descrição**	**Conclusão**	**Responsável e Participante**
Estrutura documental				
1.4.1	Implementar estrutura documental no âmbito do SGSI	Estrutura documental do INEM no âmbito do Sistema de Gestão de Segurança da Informação deverá incluir um conjunto de políticas e normas (Normativos) que orientam as atividades na proteção da informação, bem como elaborar documentação operacional que servem com evidências para auditorias "mostra que fazes, como dizes". (ver detalhe no sub-capítulo 6.4 Framework da Documentação do SGSI)	2ºsemestre 2017	Gestor da Segurança e GSTI
Responsabilidades pela gestão documental				
1.4.2	Definir os responsáveis na elaboração dos Normativos e aprovação	A elaboração documental normativa deverá respeitar o que está definido na sua estrutura, no que respeita à elaboração e aprovação.	2ºsemestre 2017	Gestor da Segurança

8.3. EIXO II: PESSOAL

O **eixo de ação II: Pessoal**, no âmbito da segurança da informação tem como componentes principais a (i) admissão e cessação contratual; (ii) funções e responsabilidades; (iii) formação técnica; (iv) ações de consciencialização, educação.

Na componente de contratualização de prestadores de serviços e admissão de colaboradores "é necessário a idoneidade dos colaboradores, efetuando a verificação dos seus dados, credenciando-os para o manuseamento dos dados e informação a que terão acesso, apresentando-lhe a filosofia de segurança da informação da organização e garantindo a sua aceitação." (Martins, 2008). Aquando da cessação e alteração da relação contratual, devemos garantir procedimentos de recolha de todos os recursos da organização na sua posse (ex. portátil, telemóvel), bem como garantir a desativação de todas as suas formas de identificação e autenticação em sistemas da organização, como por exemplo, desativar a conta no domínio e alterar *passwords* de acesso a recursos aplicacionais.

As responsabilidades têm de ser apropriadamente distribuídas de forma a eliminar as oportunidades de modificações não autorizadas. Se não for possível uma separação, têm de ser fornecidos outros tipos de controlo, como a monitorização pela administração ou o registo das atividades. Deve ser garantido que as áreas técnicas e serviços, cuja responsabilidade seja apenas de uma pessoa, não venham a ser alvo de modificações/alterações que não possam ser detetadas.

A constante evolução dos sistemas e tecnologias de informação e a consequente refinação às formas de ataque que vão surgindo, torna-se exigente um constante e específico plano de formação técnica para a equipa do GSTI, com o propósito de responder à dimensão tecnológica de segurança de informação e aos requisitos de controlo da norma ISO/IEC 27001.

Desenvolver um programa de consciencialização com a aplicabilidade de uma política técnica, na ótica do utilizador, onde aborde ações de sensibilização a uma cultura de sigilo e da responsabilização de todos os colaboradores no âmbito da segurança da informação e dos sistemas de informação.

Para o **Eixo II – Pessoal** identificam-se as seguintes três Medidas:

Medida 5: Política de segurança na abrangência contratual e nos recursos da função

Medida 6: Programa de consciencialização sobre segurança da informação

Medida 7: Formação técnica

No cumprimento para com os requisitos do **Eixo II – Pessoal** deverão ser executadas as seguintes ações:

Medida 5: Política de segurança na abrangência contratual e nos recursos da função

- Verificação de antecedentes no processo de contratualização
- Definição do perfil funcional
- Controlo no acesso aos recursos durante o período de contratualização
- Requisitos formais na cessação e alteração contratual

Medida 5 - Política de segurança na abrangência contratual e nos recursos da função				
	Ações	**Descrição**	**Conclusão**	**Responsável e Participante**
Verificação de antecedentes no processo de contratualização				
2.5.1	Verificar antecedentes na contratualização de novos colaboradores e prestadores de serviço.	Na admissão de novos colaboradores, a verificação dos seus antecedentes deve ser requerida no momento da seleção de candidatos, assim como referências dos empregadores anteriores. Para colaboradores externos à entidade (e.g. consultores), um processo de revisão semelhante deve ser conduzido pelo respetivo requerente (ou pessoa responsável pelo orçamento do departamento). Devem ser celebrados acordos de sigilo e confidencialidade, antes do acesso a dados ou sistemas de informação.	Março 2017	Depto. Recursos Humanos e Unidades Orgânicas
Definição de perfil funcional				
2.5.2	Definir Perfil Funcional correspondente ao nível de acesso à rede e aos recursos aplicacionais.	Em correspondência com a função e responsabilidades assignar um Perfil Funcional específico que define o acesso à rede e os níveis de acesso aos recursos aplicacionais e suas funcionalidades. Durante o percurso contratual qualquer mudança na função/responsabilidades implica mudança de Perfil Funcional.	Março 2017	GSTI e Depto. Recursos Humanos; Responsável Hierárquico

Controlo no acesso aos recursos durante o período de contratualização				
2.5.3	Implementar meios de controlo na deteção do acesso não autorizado a sistemas e serviços.	Através de plataforma de gestão de identidades obter, auditar e validar a correta correspondência entre o acesso aos recursos aplicacionais nos seus diferentes níveis e a função/responsabilidades do colaborador e/ou prestador de serviços.	Março 2017	GSTI e Depto. Recursos Humanos; Responsável Hierárquico
Requisitos formais na cessação e alteração contratual				
2.5.4	Definir e implementar processo com requisitos formais na cessação e alteração contratual	No término ou alteração da prestação de serviços (funções/responsabilidades) deve ser assegurado o procedimento que garanta a entrega ou recolha dos equipamentos em posse pelo colaborador (e.g. portátil, telefone) e garantir a desativação na identificação e autenticação ao acesso aos sistemas aplicacionais.	Março 2017	GSTI e Depto. Recursos Humanos; Responsável Hierárquico

Medida 6: Programa de consciencialização sobre segurança da informação

- Política de utilização dos sistemas e tecnologias de informação
- Ações de formação sobre preocupações relacionadas com a segurança da informação
- Sensibilização no uso da Política de Segurança ao posto de trabalho
- Disponibilizar e divulgar informação relacionada com a segurança da informação

Medida 6 - Programa de consciencialização sobre segurança da informação				
	Ações	**Descrição**	**Conclusão**	**Responsável e Participante**
Política de utilização dos sistemas e tecnologias de informação				
2.6.1	Implementar Política de utilização dos sistemas e tecnologias de informação	Apresentar formalmente um conjunto de regras que devem ser aplicadas no uso dos vários serviços relacionados com os sistemas de informação e tecnologias associadas. Nesta política deverá existir referência a procedimento disciplinar formal que seja acionável em caso de violação de segurança da informação.	on going	GSTI e Gabinete Juridico

Ações de formação sobre preocupações relacionadas com a segurança da informação				
2.6.2	Desenvolver ações de formação sobre preocupações relacionadas com a segurança da informação	Todos os colaboradores da organização que direta ou indiretamente fazem uso dos serviços da rede devem ser destinatários de ações de consciencialização em segurança de informação. O colaborador deve acusar a receção da formação por escrito.	Junho 2017	GSTI e Depto. Recursos Humanos; Gabinete de Marketing e Comunicação
Sensibilização no uso da Política de Segurança ao posto de trabalho				
2.6.3	Promover o conhecimento da Política de Segurança da Informação	Estabelecer um claro entendimento da existência da Política de Segurança da Informação e que esta está alinhada com os objetivos estratégicos do INEM e sua missão. Que todas áreas orgânicas são responsáveis por implementar a segurança da informação conforme definido pelas normas, procedimentos e regras.	Junho 2017	CD e Depto. Recursos Humanos; Responsáveis Hierárquicos
Disponibilizar e divulgar informação relacionada com a segurança da informação				
2.6.4	Definir plataforma(s) de divulgação, consulta e formação (*e-learning*)	Estabelecer uma plataforma ou adaptação de uma existente acessível a todos os colaboradores, parceiros e prestadores de serviço com informação, de modo a que os utilizadores estejam cientes das ameaças relacionadas com a segurança da informação e estarem preparados para aplicar a Politica de Segurança da Informação. Implementar uma plataforma *e-learning* que permita a formação sobre temas relacionados com a segurança de informação mas, que poderá ser aproveitada com ferramenta de auto-formação em diversas áreas. Projetar *flyer* com dez regras básicas a aplicar no posto de trabalho em cumprimento às medidas de segurança, como por exemplo, a adoção da política	Setembro 2017	GSTI e Depto. Recursos Humanos; Responsável Hierárquico

		de secretária limpa, regras da palavra-passe.		

Medida 7: Formação técnica

- Definir e concretizar plano de formação técnica especializada

Medida 7 – Formação técnica				
	Ações	**Descrição**	**Conclusão**	**Responsável e Participante**
Definir e concretizar plano de formação técnica especializada				
2.7.1	Definir e concretizar plano de formação técnica especializada	A gestão de risco e segurança da informação exige colaboradores com muito boa formação em tecnologias de segurança da informação e administração de sistemas, servidores e redes; pelo que deve ser estabelecido e Concretizado um plano de formação específico à equipa do GSTI em resposta à evolução tecnológica e aquisição de competências alinhadas com as medidas e tratamento a aplicar. Este plano de formação deve ser um processo contínuo.	Fase I e II 1º e 2º semestre 2017, respetivamente	GSTI e Depto. Recursos Humanos; Depto. Financeiro

8.4. EIXO III: FÍSICO E AMBIENTAL

O **eixo de ação III: Físico e Ambiental**, enquadra os aspetos relacionados com a proteção física das instalações da organização, onde operam os sistemas computacionais e as áreas operacionais que operam ou contenham informação sensível ou crítica e recursos de processamento de informação no suporte à sua atividade. Este eixo de ação visa garantir a prevenção na ocorrência de acontecimentos graves ou catástrofes onde, existam consequências ao nível físico, seja de âmbito nacional ou regional, que possam danificar o normal funcionamento na resposta à sua missão e consequências no acesso à informação. "Estes acontecimentos fortuitos são normalmente previsíveis, muito embora não seja previsível o instante em que ocorrem, nem muitas vezes a gravidade com que ocorrem"(Zúquete,2014). Deste modo, deve ser estabelecido um conjunto de procedimentos e de meios instalados que possam responder eficazmente a faltas ou falhas previsíveis e defesa contra atividades não autorizadas[17].

Neste âmbito, deveremos considerar os seguintes aspetos:

i. Identificação de áreas com afetação ao processamento, tratamento e arquivo de informação.
ii. Infraestrutura de energia elétrica com autonomia redundante em caso de falha/quebras de funcionamento.
iii. Adequada e segregada infraestrutura de caminhos de cabos elétricos e cablagem da rede dados. No caso dos centros de processamento de dados (*data centers*), garantir adequada refrigeração, sistema de controlo de incêndio, inundação e alarmística.
iv. Acessos físicos controlados às instalações classificadas de risco, integrada com a credenciação pessoal.
v. Procedimentos de proteção e prevenção nos componentes computacionais de *hardware*, *software*, meios magnéticos e documentação, em termos dos riscos por roubo, perda, extravios ou por danos físicos.

Neste eixo de ação, a instituição do INEM, abrange satisfatoriamente os requisitos preconizados pela ISO/IEC 27001; nomeadamente: na definição dos perímetros de segurança física com controlos de entrada física; as áreas críticas têm agregado infraestrutura redundante de energia elétrica, meios de refrigeração, de segurança contra incêndio, controlo e deteção. Tem definido e aplicáveis planos de manutenção preventiva com regulares testes funcionais, nomeadamente contra interrupções de energia elétrica. O tratamento de equipamento eletrónico segue procedimentos abrangidos e certificados pela ISO 14001 (Sistema de Gestão Ambiental) e as áreas de cargas e descargas de equipamento informático, está abrangido pelos procedimentos logísticos. A manutenção dos equipamentos é mantida de forma correta; o GSTI tem "em marcha" um programa de reutilização (5R-Reciclar, Recusar, Reduzir, Reutilizar, Repensar) de equipamentos informáticos, assegurando de forma contínua a disponibilidade e a integridade dos mesmos.

Como pontos de abrangência aos requisitos da norma ISO/IEC 27001, são propostas as seguintes medidas:

Medida 8: Execução de testes, nos *Data Centers*, para falhas previsíveis

Medida 9: Realizar planos de contingência e *disaster recovery plan*

[17] As atividades não autorizadas podem ter origem: nos sujeitos pertencentes à organização, dona do sistema computacional que se quer proteger e os sujeitos que a ele não pertencem. Os primeiros são mais difíceis, uma vez que possuem normalmente privilégios acrescidos, em relação aos segundos, que podem usar para iniciar atividades não autorizadas. (Zúquete,A. 2014)

Medida 10: Procedimentos de segurança nos equipamentos/ativos em uso fora das instalações

Medida 11: Requalificar bastidores técnicos da rede dados e voz

Medida 12: Redefinir localização de *Data Center* de Lisboa

No cumprimento às medidas a aplicar no eixo III-Físico, descrevem-se as ações seguintes:

Medida 8: Execução de testes, nos *Data Centers*, para falhas previsíveis

- Realizar simulacros operacionais nos sistemas computacionais em caso de falha energética
- Documentar e aplicar melhoria contínua na mitigação do risco

Medida 8 - Execução de testes, nos Data Centers, para falhas previsíveis				
	Ações	**Descrição**	**Conclusão**	**Responsável e Participante**
Realizar simulacros operacionais por sistema computacional em caso de falha energética				
3.8.1	Planear e realizar simulacros operacionais para falhas previsíveis de energia elétrica.	A redundância na componente energética implica *delays* entre a passagem UPS - Gerador. Torna-se exigível validar o tempo útil de autonomia da UPS com os procedimentos de *shutdown/start-up* dos sistemas de informação. Avaliar comportamento (em contínuo) do gerador em funcionamento.	2º sem. 2017	GSTI e Unidades Orgânicas
Documentar e aplicar melhoria contínua na mitigação do risco				
3.8.2	Documentar *modus operandi* na interligação com os planos de *disaster recovery* dos sistemas de informação.	A "boa prática" sugere documentar o método operacional com a identificação dos atores do processo (GSTI e Unidades Orgânicas), a definição do *escalation procedure*, tempos de resposta e de resolução. A realização de testes planeados permite mitigar riscos de forma controlada, melhorar os procedimentos e validar os procedimentos entre as partes envolvidas.	2º sem. 2017	GSTI e Unidades Orgânicas

Medida 9: Realizar planos de contingência e disaster recovery plan

- Realizar e documentar plano(s) de contingência em caso de quebras prolongadas de energia e de telecomunicações
- Validar planos de continuidade operacional (*disaster recovery plan*)
- Rever e avaliar os planos de continuidade operacional

Medida 9 - Realizar planos de contingência e *disaster recovery plan*				
	Ações	**Descrição**	**Conclusão**	**Responsável e Participante**
Realizar e documentar plano(s) de contingência em caso de quebras prolongadas de energia e de telecomunicações				
3.9.1	Planear a realização de planos de contingência operacional e funcional em caso de quebras prolongadas de energia.	A falha de energia prolongada poderá implicar inacessibilidade aos sistemas de informação, também por tempo determinado. Uma falha ou quebra de serviço nas telecomunicações na rede dados, coloca em risco o acesso a sistemas críticos. Prever falhas ou quebras parciais de energia e/ou telecomunicações de dados/voz em termos geográficos, implica a passagem de serviços e reorganização funcional e operacional. A reposição ao estado inicial, implica também oscilação no acesso aos sistemas de informação e telecomunicações.	2º sem. 2017	GSTI e Unidades Orgânicas
Validar planos de continuidade operacional (*disaster recovery plan*)				
3.9.2	Validar entre as partes afetas os planos de continuidade operacional.	No seguimento do anterior item 3.9.1 deverá ser validado, pelas unidades orgânicas abrangidas, os planos de contingência na continuidade operacional. O envolvimento e participação nestas ações trazem maior e melhor conhecimento partilhado e melhoria contínua.	1º sem. 2018	GSTI e Unidades Orgânicas
Rever e avaliar os planos de continuidade operacional				
3.9.3	Rever e avaliar periodicamente os planos de contingência	As mudanças operacionais ou mudanças tecnológicas ou de sistemas de informação, implica revisão dos planos de contingência.	2º sem. 2018	GSTI e Unidades Orgânicas

		Ações de formação regulares é também uma mais-valia, na resposta a condições previsíveis.		

Medida 10: Procedimentos de segurança nos equipamentos/ativos em uso fora das instalações

- Procedimento em caso de roubo, violação ou perda de computadores portáteis
- Definir e aplicar política sobre equipamentos não vigiados e de secretária limpa

Medida 10 - Procedimentos de segurança nos equipamentos/ativos em uso fora das instalações				
	Ações	**Descrição**	**Conclusão**	**Responsável e Participante**
Procedimento em caso de roubo, violação ou perda de computadores portáteis				
3.10.1	Implementar procedimento para perda, roubo ou violação de computadores portáteis (laptops e tablets) e outros dispositivos móveis.	A perda, roubo ou violação de equipamentos portáteis / dispositivos móveis é um evento previsível. Definir procedimentos de segurança para equipamentos e ativos fora das instalações e da sua usabilidade como precaução/prevenção tendo em consideração os diferentes riscos decorrentes do trabalho fora das instalações da organização. Definir procedimentos sobre "o que fazer", em termos de formalidade e participação. Definir "o que fazer" no imediato caso haja uma perda, roubo ou violação num equipamento/informação.	2º sem. 2017	Gestor de Segurança
Definir e aplicar política sobre equipamentos não vigiados e de secretária limpa				
3.10.2	Definir e aplicar política sobre equipamentos não vigiados e de secretária limpa.	Definir uma política para a proteção de equipamentos, colocados em zonas não vigiadas e que possam causar interrupção das operações da organização. Definir uma política de secretária limpa de papéis e suportes de dados amovíveis e de ecrã limpo para os recursos de processamento de informação.	2º sem. 2017	Gestor de Segurança

Medida 11: Requalificar bastidores técnicos da rede dados/voz

- Refrigeração e ligação à rede protegida
- Acomodamento, higiene e documentação
- Plano de auditoria na validação dos procedimentos operacionais

Medida 11 - Requalificar bastidores técnicos da rede dados				
	Ações	**Descrição**	**Conclusão**	**Responsável e Participante**
Refrigeração e ligação à rede protegida				
3.11.1	Instalar sistema de refrigeração e ligação à rede protegida UPS.	Na rede de distribuição dados/voz, localizadas nos edifícios da Sede e na Infante D.Pedro, existem bastidores técnicos com densidade de equipamentos instalados que deverão ter sistema de refrigeração e ligação à rede protegida com UPS, de modo a prever falhas de serviço e garantir disponibilidade.	2º sem. 2017	GSTI
Acomodamento, higiene e documentação				
3.11.2	Definir e aplicar procedimento standard sobre acomodamento de cablagem e equipamento; higiene e documentação.	Seguindo o exemplo no site do Porto, deve ser definido a boa prática sobre o acomodamento de cablagem (passivos) e instalação de equipamentos ativos nos bastidores técnicos. Neste procedimento, definir regras de higiene, produção de documentação técnica e auditorias.	2º sem. 2017	GSTI
Plano de auditoria na validação dos procedimentos operacionais				
3.11.3	Definir plano de auditorias regulares na validação dos procedimentos operacionais.	A operacionalidade dos procedimentos implica a sua validação e aprendizagem sobre a boa prática aplicada.	2º sem. 2017	GSTI

Medida 12: Redefinir localização do *Data Center* em Lisboa

- Realizar estudo alternativo da localização do Data Center

Medida 12 - Redefinir localização de *Data Center* de Lisboa				
	Ações	**Descrição**	**Conclusão**	**Responsável e Participante**
Realizar estudo alternativo da localização do *Data Center*				
3.12.1	Realizar estudo alternativo para localização do *Data Center* em Lisboa.	O *Data Center* de Lisboa encontra-se em cota abaixo do nível da rede de águas pluviais. Existe a previsibilidade de inundação com volumetria de água que afeta o funcionamento dos servidores e equipamentos de rede dados e voz, provocando indisponibilidade prolongada nos serviços.	Janeiro 2018	GSTI

8.5. EIXO IV: TECNOLÓGICO

O **eixo de ação IV: Tecnológico**, tem como principais objetivos garantir o adequado e correto processamento, transmissão e armazenamento dos dados e informação, indispensáveis para garantir a segurança da informação (Martins, 2008). O eixo tecnológico foi conceptualmente dividido em três dimensões: (1) a dimensão aplicacional; (2) a dimensão lógica e (3) a dimensão rede.

(1) Dimensão Aplicacional

Na dimensão aplicacional estão compreendidos fundamentalmente os componentes relacionados com:

i. a definição matricial dos sistemas aplicacionais em utilização na organização, sua categorização e a identificação dos seus responsáveis (*owners*);

ii. a preocupação com a aquisição e/ou desenvolvimento local das aplicações de software, quais os requisitos com a sua implementação e manutenção. Nesta componente, deveremos ter em conta a separação dos ambientes de desenvolvimento, testes e produção de forma a impedir riscos de segurança.

Na análise realizada foram identificados as seguintes medidas, com as respetivas ações:

M14: Aquisição e/ou desenvolvimento aplicacional

- Enquadramento ao propósito e expressão de necessidades
- Planeamento e aceitação de sistemas
- Definição técnica integrada
- Modificações, Manutenção e Controlo

M15: Gestão de ativos

- Categorizar e classificar as aplicações/ativos
- Definir formalmente os responsáveis das aplicações
- Manter a relação matricial atualizada

M16: Separação dos ambientes de desenvolvimento e de produção

- Disponibilizar diferentes ambientes de processamento

Para cada uma das medidas enunciadas, na dimensão aplicacional do eixo IV-Tecnológico, descrevem-se em detalhe as seguintes ações:

M14: Aquisição e/ou desenvolvimento aplicacional

- Enquadramento ao propósito e expressão de necessidades
- Planeamento e aceitação de sistemas
- Definição técnica integrada
- Gestão de alterações alinhado com o ITIL *framework*

Medida 14 - Aquisição e/ou desenvolvimento aplicacional				
	Ações	**Descrição**	**Conclusão**	**Responsável e Participante**
Enquadramento ao propósito e expressão de necessidades				
4.14.1	Formalizar propósito e expressão de necessidades para um novo sistema e aplicação.	A realização do enquadramento à necessidade de um novo ou alteração de sistema e aplicação, permitirá o planeamento na infraestrutura TIC e cabimento financeiro. Determinar os requisitos de segurança da informação.	Maio 2017	Dirigentes unidades orgânicas e GSTI
Planeamento e aceitação de sistemas				
4.14.2	Definir critérios de aceitação e validação para novos sistemas e aplicações de TIC.	Com base na expressão de necessidades será possível realizar planeamento de modo a minimizar o risco de falhas nos sistemas e avaliar previamente os requisitos de desempenho, capacidade computacional e segurança da informação. Evitar que as vulnerabilidades das aplicações possam ser exploradas pelas ameaças como resultado do desenvolvimento de aplicações efetuadas *ad-hoc* internamente, quer pelas adquiridas por entidades externas que, normalmente a organização não tem acesso ao código fonte.	Maio 2017	GSTI e Gestor de Segurança
Definição técnica integrada				
4.14.3	Definir requisitos técnicos de arquitetura e segurança da informação; planeamento e implementação.	Definição da arquitetura dos equipamentos e requisitos técnicos. Interoperabilidade com os sistemas de informação do INEM. Planeamento e implementação da solução. Testes funcionais, operacionais e de vulnerabilidades em termos de	Maio 2017	GSTI e Gestor de Segurança

		segurança de informação. Documentação e Formação de utilizadores e administração do sistema.		
Gestão alterações alinhado com ITIL framework				
4.14.4	Implementar processo de gestão de alterações alinhado com o Framework ITIL.	A gestão de alterações deve envolver os representantes (departamentos, gabinetes, áreas operacionais) que diretamente tenham impacto com a alteração a implementar. Estes intervenientes têm a função de interagir, participar e de responsabilizarem-se pelas decisões e ações planeadas na alteração e/ou modificação a implementar. Deverá ser nomeado um elemento (CAB-*Change Advisory Board*) com a responsabilidade de estabelecer a ligação com todos os intervenientes do processo, coletar as informações necessárias e fazer a gestão de prioridades das alterações a aplicar. O processo gestão alterações, engloba alterações do tipo: requeridas (RFC - Request for Change), de manutenção (configurações, novas ou atualizações de versões; incluindo componentes de sistema operativo ou de servidores), reparação ou resolução de falhas/problemas e alterações de emergência.	Junho 2017	GSTI e Gestores Aplicacionais; Gestor de Segurança

M15: Gestão de ativos

- Categorizar e classificar as aplicações/ativos
- Definir formalmente os responsáveis das aplicações e processos
- Manter a relação matricial atualizada

Medida 15 – Gestão de ativos				
	Ações	**Descrição**	**Conclusão**	**Responsável e Participante**
Categorizar e classificar as aplicações/ativos				
4.15.1	Atribuir categorização às aplicações: quanto à criticidade operacional e funcional; classificação dados/informação.	Na relação matricial das aplicações/ativos em utilização, diferenciar quais as críticas e altamentes críticas quanto à sua disponibilidade operacional e funcional; o tipo (classificação) de dados/informação em processamento, tratamento e armazenamento; a(s) unidade(s) orgânica(s) que interagem; os termos contratuais; níveis de serviços e escalonamento operacional.	Maio 2017	GSTI e Dirigentes nas unidades orgânicas
Definir formalmente os responsáveis das aplicações e processos				
4.15.2	Definir os responsáveis das aplicações. Definir os responsáveis do processo.	Toda e qualquer aplicação (em uso, em desenvolvimento, ou fim de vida) deverá ter um *owner* com as responsabilidades de atribuir e controlar níveis de acesso, a sua evolução funcional e contratual (interna ou externa). A identificação inequívoca do responsável de processo, onde faz parte o *software* aplicacional ou sistema é de extrema relevância na validação às alterações funcionais e de processo.	Março 2017	GSTI e Dirigentes nas unidades orgânicas
Manter a relação matricial atualizada				
4.15.3	Manter e controlar a relação matricial das aplicações durante os estados da sua "vida útil".	A melhoria contínua e evolutiva da organização, obriga a estados evolutivos das aplicações e estruturais, pelo que a relação matricial deverá espelhar os vários estados.	a partir de Março 2017	GSTI e Gestor de Segurança

M16: Separação dos ambientes de desenvolvimento e de produção

- Disponibilizar diferentes ambientes de processamento

Medida 16 - Separação dos ambientes de desenvolvimento e de produção				
	Ações	**Descrição**	**Conclusão**	**Responsável e Participante**
Disponibilizar diferentes ambientes de processamento				
4.16.1	Preparar e disponibilizar infraestrutura e recursos para as atividades de produção, testes e aceitação.	As atividades de desenvolvimento de *software*, testes (funcionais e pré-produção) e produção têm de estar separadas, (idealmente) com recurso a diferente hardware. A mudança da classificação de um *software* no estado de desenvolvimento para o estado de produção tem estar claramente definida e documentada. O acesso às ferramentas de desenvolvimento não é possível a partir dos sistemas de produção e o uso de *software* de análise de problemas tem de ser autorizado individualmente. O controlo de acessos aos sistemas e aplicações com diferentes funções (por exemplo, testes) tem de ser configurado de maneira diferente e de modo evidente para o utilizador. Os utilizadores têm de ser incentivados a usar diferentes senhas para sistemas e aplicações com diferentes funções.	1º Semestre 2017	GSTI

(2) Dimensão Lógica

Na dimensão lógica compreende fundamentalmente, os processos relacionados com o acesso autorizado à informação, o adequado e correto armazenamento da informação e o registo de *logs* e a sua retenção. A componente do acesso à informação inclui as operações de identificação e autenticação dos utilizadores internos à rede computacional e a autenticação dos utilizadores para ligações externas, sendo que a identificação e autenticação são os principais agentes responsáveis no controlo de acessos lógico e de uma ampla criticidade no domínio da confidencialidade (acesso restrito a utilizadores legítimos) e integridade (informação não é modificada de forma inesperada).

Na dimensão lógica faz ainda parte, os sistemas de armazenamento da informação que é a componente relacionada com os sistemas relacionados com base-dados, *file server, mail server, web*

server, application server, sistemas de gestão documental e *workflow*, dispositivos e equipamentos de leitura de dados, etc.

Inserido no processo de acesso à informação através de vários equipamentos tecnológicos é fundamental a possibilidade de registo de *logs* e a sua retenção. Nesta componente dever-se-á garantir que a retenção e a cópia dos *logs* são realizadas em tempo real (em sincronização com relógios) com o registo do que aconteceu ao nível dos utilizadores, dos processos, dos serviços e registar as atividades não usais ou de infração. Esta componente é de extrema importância, no sentido em que poderemos reconstruir o que aconteceu e, caso necessário, efetuar análise forense.

Para esta dimensão, consideram-se, no curto prazo, as seguintes medidas a implementar:

M17: Implementar políticas de identificação e autenticação

- Política da criação de acessos à rede e serviços
- Política de autenticação de utilizadores para ligações externas
- Política de responsabilidade dos utilizadores na utilização dos sistemas e tecnologias de informação
- Política de acesso dos prestadores de serviços externo

M18: Gestão de Acesso dos Utilizadores

- Criação e remoção de Utilizadores
- Gestão de privilégios
- Gestão das palavras-passe do utilizador
- Revisão dos direitos/privilégios de acesso dos utilizadores

M19: Sistema de Gestão de Incidentes e Eventos

- Retenção de *logs* e correlação de eventos

No cumprimento às medidas a aplicar na dimensão lógica, descrevem-se as ações seguintes:

M17: Implementar políticas de identificação e autenticação

- Política da criação de acessos à rede e serviços
- Política de autenticação de utilizadores para ligações externas
- Política de responsabilidade dos utilizadores na utilização dos sistemas e tecnologias de informação
- Política de acesso dos prestadores de serviços externo

Medida 17 - Implementar políticas de identificação e autenticação				
	Ações	**Descrição**	**Conclusão**	**Responsável e Participante**
Política da criação de acessos à rede e serviços				
4.17.1	Estabelecer uma política circunscrita à	Definir um conjunto de procedimentos administrativos na gestão e administração da *Active Directory* e		

	Administração da *Active Directory* e Office 365 no contexto das atribuições de acesso dos colaboradores e prestadores de serviços do INEM à sua rede corporativa.	*Office 365*, na atribuição de recursos de acesso aos colaboradores e prestadores de serviços que tenham sido especificamente autorizados.	Janeiro 2017	GSTI
Política de autenticação de utilizadores para ligações externas				
4.17.2	Aplicar política no acesso remoto de utilizadores.	As ligações externas representam um potencial acesso não autorizado à informação, pelo que deve ser sujeito à autenticação. É importante determinar o nível de proteção necessário, para tal, deveremos recorrer a uma análise de risco e utilização de sub-redes lógicas protegidas por VPN e autenticação com geração de código de acesso em tempo real. (*smart cards/one time-password)*. Efetivar um controlo e verificação periódica na validação dos acessos remotos.	Março 2017	GSTI
Política de responsabilidade dos utilizadores na utilização dos sistemas e tecnologias de informação				
4.17.3	Aplicar política de responsabilidades na utilização de equipamentos e nos serviços de informação.	Os utilizadores devem ter consciência das suas responsabilidades na manutenção e no uso efetivo das boas práticas a aplicar no âmbito da segurança da informação e manuseamento dos equipamentos informáticos. Garantir proteção no posto de trabalho com bloqueamento de ecrã, acesso BIOS, que as sessões ativas devem ser terminadas após finalização da tarefa, desativar automaticamente sessão de trabalho e acessos às aplicações após período de inatividade, limitação no tempo de ligação no acesso à rede por	Abril 2017	GSTI e Gestor de Segurança

		ligações não seguras.		
Política de acesso dos prestadores de serviços externo				
4.17.4	Estabelecer protocolo com os prestadores de serviços no âmbito dos sistemas de informação.	Implementar política que defina a orientação do acesso à rede institucional para entidades externas com responsabilidade no suporte e manutenção aos sistemas de informação e de comunicação. Aplicar procedimentos no acesso lógico e físico, verificação de registos entrada/saída e emissão de relatórios de intervenção.	a partir de Março 2017	GSTI e Gestor de Segurança

M18: Gestão de Acesso dos Utilizadores

- Criação e remoção de Utilizadores
- Gestão de privilégios
- Gestão das palavras-passe (password) do utilizador
- Revisão dos direitos de acesso dos utilizadores

Medida 18 – Gestão de Acesso dos Utilizadores				
	Ações	**Descrição**	**Conclusão**	**Responsável e Participante**
Criação e remoção de Utilizadores				
4.18.1	Implementar procedimento formal de registo e remoção de utilizadores; verificação periódica	Deve ser implementado procedimento formal que cubra as fases do ciclo de vida do acesso do utilizador, desde o registo inicial de novos colaboradores até à sua remoção, por não necessidade no acesso aos serviços e sistemas de informação. Verificação periódica com auditorias detalhadas sobre os direitos de acesso: que tem acesso ao quê? E, porquê? Analisar a existência de utilizadores redundantes. Manutenção do registo formal de todos os colaboradores/entidades para utilizar o serviço.	Fevereiro 2017	GSTI e Depto. Recursos Humanos; Gabinete Jurídico

Gestão de Privilégios				
4.18.2	Definir perfil ou grupo funcional base alienado com os privilégios necessários à função.	Os privilégios deverão ser atribuídos e concedidos, de acordo com a função na organização, definindo um perfil funcional base e atribuir privilégios adicionais apenas quando necessário.	Março 2017	GSTI e Dirigentes nas unidades orgânicas; Gestores Aplicacionais
Gestão das palavras-passe do utilizador				
4.18.3	Aplicar processo formal na atribuição de palavras-passe e forçar mudança de palavra-passe.	A atribuição de palavra-passe deverá ter regras específicas, com geração segura e aleatória. Implementar, regras automáticas para forçar a mudança de *password* por períodos de tempo.	Janeiro 2017	GSTI e Gestor de Segurança
Revisão dos direitos/privilégios de acesso dos utilizadores				
4.18.4	Manter o controlo efetivo sobre o acesso aos dados e serviços aplicacionais.	Os direitos/privilégios dos utilizadores devem ser revistos regularmente (mínimo duas vezes ano) e, principalmente aquando mudança de função ou serviço. Para manter o controlo efetivo sobre o acesso aos dados e serviços de informação, deverá ser formalmente implementado um procedimento que garanta auditorias periódicas direitos/privilégios dos utilizadores. As autorizações de acessos especiais e de exceção devem ser revistos com mais frequência.	a partir de Junho 2017	GSTI e Gestor de Segurança

No decorrer deste trabalho foi iniciado um conjunto de testes à plataforma Gestão de Identidades, com o objetivo disponibilizar uma ferramenta de gestão e administração que responda às ações enunciadas na **Medida 18: Gestão de Acessos dos Utilizadores**. No fecho deste documento, a implementação da plataforma Gestão de Identidades está em análise processual para validação.

M19: Gestão e Correlação de Eventos de Segurança

- Retenção de *logs* e correlação de eventos

Medida 19 –Gestão e Correlação de Eventos de Segurança				
	Ações	**Descrição**	**Conclusão**	**Responsável e Participante**
Monitorização de logs, análise e reporting				
4.19.1	Implementar ferramenta de gestão centralizada de *logs*.	Aplicar subscrição de eventos na plataforma de servidor/cliente com a funcionalidade de recolher eventos e guardar em repositório para análise e reporting. O sistema de eventos e correlação de eventos de segurança (SIEM-*System of Incident and Event Management*) poderá ser do tipo: 1. *Operations Management Suite | Insight & Analytics – Microsoft* https://www.microsoft.com/en-us/cloud-platform/insight-and-analytics 2. *EventLog Analyzer is an IT Compliance & Event Log Management Software for* SIEM) https://www.manageengine.com/	Junho 2017	GSTI

(3) Dimensão Rede

A dimensão rede engloba a gestão da infraestrutura da rede de dados (LAN, WAN, NAS ou SAN)[18] e de telecomunicações responsáveis por garantir a interconexão da plataforma de servidores e clientes (*end-points*). Adicionalmente, faz parte a componente tecnológica de segurança dos ativos de informação e proteção de comunicações, com a aplicabilidade de sistemas de controlo de tráfego (firewall), sistema de inspeção de conteúdos dos dados em trânsito na rede (IDS-*Intrusion Detection System*) e os sistemas de antivírus para detetar e remover código malicioso no sistema de ficheiros e a criptografia.

Na análise e avaliação de risco realizada sobre esta dimensão e com o objetivo de cumprir as características básicas de disponibilidade, integridade e confidencialidade de segurança da informação, são apresentadas as seguintes medidas de ação:

M20: Planear e implementar arquitetura LAN/WAN redundante

- ReDefinir e implementar arquitetura da rede LAN
- Redundância na rede VPN e *internet service infrastrutucture*
- Monitorização e gestão centralizada da rede LAN e *wireless* (WLAN)
- Uniformização / Certificação do tipo de cablagem (cat.6) rede passivo

M21: Sistema de firewall redundante

- Substituir e implementar novo sistema de firewall redundante com IPS
- Desenvolver Prova de Conceito da solução

M22: Sistema de Antivírus

- Implementar política de antivírus ativo em todos os equipamentos cliente e servidores
- Relatórios de desempenho e estado atual das instalações de antivírus

[18] LAN-Local Area Nework; (rede de computadores conectados em rede numa pequena área geográfica, e.g. no edifício da Sede); WAN-Wide Area Network (rede de comunicações de dados na interligação entre locais com longa distância, e.g. na interligação entre as Delegações);
NAS-Network attached Storage; SAN-Storage Area Network (redes destinadas exclusivamente para o armazenar dados)

M20: Planear e implementar arquitetura LAN/WAN redundante

- ReDefinir e implementar arquitetura da rede LAN
- Redundância na rede VPN e *internet service infrastrutucture*
- Monitorização e gestão centralizada da rede LAN e *wireless* (WLAN)
- Uniformização / Certificação do tipo de cablagem (cat.6) rede passivo

Medida 20 – Planear e implementar arquitetura LAN redundante				
	Ações	**Descrição**	**Conclusão**	**Responsável e Participante**
ReDefinir e implementar/migrar arquitetura da rede LAN				
4.20.1	Redefinir arquitetura da rede LAN Caderno Encargos Implementação / Migração da rede LAN	Para garantir a disponibilidade e o crescimento tecnológico dos serviços críticos de sistemas de informação com uma redefinição da arquitetura da rede dados ao nível do core, na rede *data center* e rede de distribuição, com a seguinte caracterização genérica: Equipamentos core redundantes ativo-ativo com resposta a alta densidade e grande performance, links agregados a 10/40Gpbs entre o core e a plataforma de servidores com protocolo fabric SPB (*Shortest Path Bridging*). Duplas fontes de alimentação. Na rede distribuição os equipamentos com portas Gigabit PoE com uplinks fibra 10Gbps agregados. Camada do Data Center separada da camada de Distribuição.	Março 2017 Abril 2017 Dezembro 2017	GSTI
Redundância na rede VPN e internet service infrastructure				
4.20.2	VPN Routing redundante ao site de Lisboa.	Desviar *routing* automático, no circuito VPN, para o site do Porto, em caso de falha ou indisponibilidade na entrada de *routing* no site em Lisboa. Mantendo atual *routing* entre os sites Porto e Coimbra Explorar a possibilidade de estabelecer ligação entre as centrais telefónicas Lisboa e Porto via *control network point-to-point.*	On going	GSTI

4.20.3	Aquisição de link redundante para o *internet service infrastrutcture.*	Aquisição contratual de link redundante na infraestrutura de internet com ponto redundante de entrada no site do Porto.	Janeiro 2017	GSTI
Monitorização e gestão centralizada da rede LAN e wireless (WLAN)				
4.20.4	Aquisição *software* de monitorização e gestão centralizada e avançada da rede LAN e WLAN.	Monitorização central da infraestrutura de rede com correlação e alarmística de eventos. Gestão centraliza dos equipamentos ativos de rede, incluindo os equipamentos AP-Access Points wireless. (interligado com o item 4.20.1)	Dezembro 2017	GSTI
Uniformização do tipo de cablagem (cat.6) rede passivo				
4.20.5	Instalação e renovação da cablagem rede dados para categoria 6.	Em algumas áreas organizacionais/operacionais a atual cablagem (rede passivos) está obsoleta, não standardizada e certificada.	2º sem. 2017	GSTI

M21: Sistema de firewall redundante

- Substituir e implementar novo sistema de firewall redundante com IPS
- Desenvolver Prova de Conceito da solução

Medida 21 – Sistema de firewall redundante				
	Ações	**Descrição**	**Conclusão**	**Responsável e Participante**
Implementar sistema de firewall redundante com IPS				
4.21.1	Implementar sistema de firewall redundante em substituição da atual tecnologia	Garantir sistema de firewall na deteção de tráfego nas portas de entrada nos sites de Lisboa e Porto, em modo redundante e com tecnologia IDS (*Intrusion Detection System*). Este requisito só é possível com o fecho do item 4.20.3 Aquisição de link redundante para o *internet service infrastrutcture.*	Janeiro 2017	GSTI

Desenvolver Prova de Conceito da solução				
4.21.2	Aplicar Prova de Conceito (POC) para validação da solução do sistema de firewall.	Aplicar prova de conceito na solução de sistema de firewall, antes de avançar com aquisição, de modo a validar os requisitos necessários.	On going	GSTI

M22: Sistema de Antivírus

- Política de antivírus ativo em todos os equipamentos cliente e servidores
- Relatórios de desempenho e estado atual das instalações de antivírus

Medida 22 – Sistema de Antivírus				
	Ações	**Descrição**	**Conclusão**	**Responsável e Participante**
Política de antivírus ativo em todos os equipamentos cliente e servidores				
4.22.1	Implementar política de antivírus ativo em todos os equipamentos cliente e servidores.	Implementar política de antivírus ativo em todos os equipamentos PC, Laptops e Tablets que estejam conectados à rede de dados do INEM, para consulta ou modificação de dados. É fundamental que cada equipamento PC, Laptops e Tablets pertencente à rede institucional do INEM tenham o *software* de antivírus instalado, e que esteja a funcionar corretamente. Para garantir a integridade da nossa rede e evitar possíveis ataques de vírus, é imprescindível que cada computador cliente (*end-point*) e servidor tenham sempre o antivírus ativo.	Janeiro 2017	GSTI
Relatórios de desempenho e estado atual das instalações de antivírus				
4.22.2	Produzir relatórios regulares de desempenho e relatórios do estado atual da instalação de	A emissão regular (mensal) de relatórios de desempenho do antivírus permitirá avaliar os tipos de programas maliciosos que estão “em ataque”; qual a resposta do antivírus perante estes ataques; quais os ficheiros corrigidos que foram	Março 2017	GSTI

	antivírus.	infetados. Relatórios do estado atual da instalação do antivírus, permitirá analisar a distribuição de equipamentos conectados na rede com antivírus ativo; desativo; versão antivírus e planear as tarefas agregadas de administração desta ferramenta de segurança da informação.		

8.6. EIXO V: CONFORMIDADE & REGULAÇÃO

O **eixo de ação V: Conformidade & Regulação**, remonta para o objetivo de controlo A.18 da norma NP ISO/IEC 27001:2013, em que estabelece controlos para o cumprimento de conformidade com requisitos legais e contratuais e que internamente a organização assegure e mantenha uma revisão regular do "*Framework* da Documentação do SGSI" e conformidade técnica.

No âmbito dos sistemas de informação de suporte ao processo pré-hospitalar com afetação à privacidade e proteção de dados, a instituição está em conformidade com o atual modelo de enquadramento regulatório, nomeadamente com a Lei 67/98, de 26 outubro – Lei da Proteção de Dados Pessoais; Lei 26/2016, de 22 agosto – Lei do Acesso a Documentos Administrativos e Lei 12/2005, de 26 janeiro – Informação Genética Pessoal e Informação de Saúde. Em algumas aplicações, existe formalidade legal com a CNPD ao abrigo da atual Lei 67/98, de 26 outubro – Lei da Proteção de Dados Pessoais.

Contudo, este eixo de ação no médio prazo, torna-se de extrema relevância face ao novo Regulamento Geral da Proteção de Dados 2016/679[19], doravante designado por RGPD 2016/679, em que estabelece uma mudança de paradigma regulatório face ao modelo em vigor. O RGPD 2016/679 impera maior exigência no tratamento e proteção dos dados pessoais. As entidades/organizações tem que demonstrar evidências do cumprimento deste regulamento, sendo que passa para o cidadão/utente a devolução do controlo dos seus dados pessoais.

A Proteção de Dados e a Cibersegurança estão a viver um momento crítico em termos regulatórios, com diversos temas críticos, como por exemplo: Revisão da Diretiva de Comunicações Eletrónicas, a Diretiva de Cibersegurança[20] 2016/148, o Regulamento RGPD 2016/679; pelo que será necessário a nossa preparação perante o quadro regulatório estruturante no que concerne à proteção de dados, implicando transformações organizacionais com a inclusão e/ou alteração de formais procedimentos, regras e em alguns casos com novas tecnologias. (Melo, M. 2016-Palestra Proteção Dados e Cibersegurança, 2016)

Embora só comece a ser aplicado em maio de 2018, o novo quadro legal europeu tem novidades significativas que terão um impacto considerável na vida das organizações, públicas e privadas, assim como na atividade das autoridades de supervisão. Sendo a proteção de dados pessoais um direito fundamental em Portugal e na União Europeia (UE), os cidadãos ocupam um lugar central nesta transformação. O RGPD 2016/679 vem substituir a atual diretiva e as legislações nacionais de proteção de dados, sendo diretamente aplicável em todos os Estados-Membros da UE, pelo que é

[19] Regulamento Geral de Proteção de Dados 2016/679
http://ec.europa.eu/justice/data-protection/reform/index_en.htm
http://www.proteccaodedados.pt/2016/legislacao-ue/directiva-ue-2016680-de-27-de-abril-de-2016/

[20] Um dos desafios mais críticos na sociedade é a prevenção de ciberameaças para impedir que possam ameaçar os sistemas internos das organizações, seja por cibercriminosos, *hacktivistas* ou grupos terroristas. As medidas utilizadas para responder a estas ameaças vieram a contribuir para a criação do termo "cibersegurança". A Cibersegurança visa garantir a segurança dos vários utilizadores no ciberespaço. O desafio atual da cibersegurança é maioritariamente para com medidas sociais, legais e tecnológicas de modo a garantir a integridade, confidencialidade, disponibilidade e a segurança geral de toda a informação no ciberespaço de modo a conseguir a confiança dos utilizadores necessária para desenvolver uma sociedade "ciber-consciente". (Vian,P. 2016)

imprescindível começar a planear o futuro, a delinear planos de ação e a adaptar as organizações às novas exigências legais. (APDSI, 2016 - Conferência sobre o novo regulamento europeu para a proteção de dados, 2016).

Para dar resposta ao novo regulamento, são propostas as seguintes medidas:

M23: Designar um Encarregado da Proteção de Dados / Data Protection Officer

M 24: Sistema de Gestão de Notificações de Incidentes

M25: Tecnologia e interoperabilidade entre sistemas

M26: Revisão contratual dos prestadores de serviços

No cumprimento do **eixo V** deverão ser executadas as seguintes propostas de ação:

M23: Designar um Encarregado da Proteção de Dados / *Data Protection Officer*

- Definir Encarregado da Proteção de Dados
- Estabelecer uma cultura consistente e integrada

Medida 23 - Designar um Encarregado da Proteção de Dados / Data Protection Officer				
	Ações	**Descrição**	**Conclusão**	**Responsável e Participante**
Definir Encarregado da Proteção de Dados				
5.23.1	Encarregado da Proteção de Dados (*Data Protection Officer*)	Definir o Encarregado da Proteção de Dados no desempenho das seguintes funções : - informa e aconselha sobre a avaliação do impacto; - coopera e é o ponto de contacto com a autoridade de controlo e com os titulares dos dados (cidadãos); - controla e monitoriza a conformidade com o regulamento e politicas organizacionais aplicáveis à proteção de dados; - sensibiliza tudo o que concerne à proteção de dados – posição profilática.	Maio 2018	CD e Gestor de Segurança (CISO); Coordenador GSTI
Estabelecer uma cultura consistente e integrada				
5.23.2	Cultura de cibersegurança e *privacy by design*	Ter uma estratégia em matéria de cibersegurança. Se desenhar ou implementar um novo sistema incluir o privacy by design (as questões da proteção de dados pessoais). Aplicar uma cultura consistente e	Maio 2018	CISO e Data Protection Officer

		integração dos atores: estabelecer códigos de conduta para os analistas e programadores de sistemas aplicacionais; código de conduta para os técnicos da saúde, por exemplo, na utilização de equipamentos móveis com processamento de imagem e vídeo em qualquer lugar e no tempo.		

M 24: Sistema de Gestão de Notificações de Incidentes

- Desenvolver e disponibilizar plataforma notificação de incidentes
- Permitir ao cidadão autenticação no acesso à plataforma de notificação de incidentes
- Estabelecer canal seguro de comunicação com a autoridade de controlo

Medida 24 - Sistema de Gestão de Notificações de Incidentes				
	Ações	**Descrição**	**Conclusão**	**Responsável e Participante**
Desenvolver e disponibilizar plataforma notificação de incidentes				
5.24.1	Notificação de incidentes	Desenvolver e implementar plataforma que permita o registo de incidentes categorizados na proteção de dados pessoais. Uniformização com formato estruturado para leitura, tratamento e disponibilidade efetiva dos dados pessoais do cidadão (Direito à Portabilidade). Deteção e alarmística na violação de dados pessoais. A entidade INEM como responsável pelo tratamento de dados, deverá poder demonstrar que o cidadão deu o seu consentimento à operação de tratamento dos dados, como também, retirar o consentimento.	Maio 2018	Coordenador GSTI e Gestor de Segurança
Permitir ao cidadão autenticação no acesso à plataforma de notificação de incidentes				
5.24.2	Iteração com o cidadão	Criar interface que permita ao cidadão/utente a total decisão no controlo dos seus dados pessoais, como por exemplo, pedir a eliminação imediata dos seus dados, após o diagnóstico clínico; solicitar a	Maio 2018	CISO e Data Protection Officer

		passagem dos seus dados para outra entidade (Direito ao Esquecimento e Direito à Potabilidade)		
Estabelecer canal seguro de comunicação com a autoridade de controlo				
5.24.3	Protocolo de comunicação com a autoridade de controlo	Estabelecer canal de comunicação com a autoridade de controlo, sobre notificações de violação de dados pessoais (*data breach*), em que deverá notificá-la, sempre que possível, no prazo de 72 horas após ter tido conhecimento do ocorrido, a menos que seja capaz de demonstrar em conformidade com o princípio da responsabilidade - *Accountability* e *Enforcement*.	Maio 2018	CISO e Data Protection Officer

M 25: Tecnologia e interoperabilidade entre sistemas

- Adaptação tecnológica
- Validar a Interoperabilidade entre sistemas

Medida 25 – Tecnologia e Interoperabilidade entre sistemas				
	Ações	**Descrição**	**Conclusão**	**Responsável e Participante**
Adaptação tecnológica				
5.25.1	Avaliar os atuais sistemas que contenham dados pessoais	Identificação dos sistemas que contenham dados pessoais e avaliar a necessidade de alteração tecnológica que satisfaça a gestão de dados pessoais nas funcionalidades: recolher; tratar; partilhar; arquivar; controlar e que possam responder às regras de notificação preconizadas pelo RGPD 2016/679.	Maio 2018	CISO e Coordenador GSTI
Validar a Interoperabilidade entre sistemas				
5.25.2	Estabelecer protocolos de comunicação entre sistemas na transmissão de dados pessoais	Aplicar modelo de dados estrutural à confidencialidade, à integridade entre sistemas e que os dados estejam disponíveis em formato para o cidadão e entidades correlacionadas com o INEM de âmbito nacional e internacional.	Maio 2018	CISO e Coordenador GSTI

M26: Revisão contratual dos prestadores de serviços

- Garantir cumprimento ou execução

Medida 26 - Revisão contratual dos prestadores de serviços				
	Ações	**Descrição**	**Conclusão**	**Responsável e Participante**
Garantir cumprimento ou execução				
5.26.1	Rever e validar contratação com prestadores de serviço em conformidade com o RGPD 2016/679.	O regulamento RGPD 2016/679 impera o princípio de "*Accountability*" aos prestadores de serviço em caso de sanção a aplicável por não cumprimento ou execução na gestão de dados pessoais em estejam envolvidos, seja no desenvolvimento de *software* ou no tratamento de dados.	Maio 2018	Data Protection Officer e GGCCP

O resumo de conjunto de medidas apresentadas, subdivididas nos cinco eixos de ação Pessoal, Tecnológico, Físico e Ambiental, Legal & Regulatório, é o seguinte:

Eixo I:	Medidas	Ações		Controlo	Conclusão	Responsavel e Participante
Organizacional	**Medida 1: Política de Segurança da Informação**	**1.1.1**	○ Definir e Aprovar Política de Segurança da Informação	Req. 5.2 A.5.1.1	1ºtrimestre 2017	CD e GSTI; GQ
		1.1.2	○ Rever a Política de Segurança da Informação	A.5.1.2	1ºtrimestre 2018	CD e GSTI; GQ
		1.1.3	○ Implementar programa de comunicação para os colaboradores, parceiros e prestadores de serviço	Req. 5.2	1ºtrimestre 2017	CD e GQ; GMC
		1.1.4	○ Disponibilizar plataforma com vários canais de comunicação	Req. 5.2	1ºtrimestre 2017	GQ; GMC
	Medida 2: Estrutura organizacional de segurança da informação	**1.2.1**	○ Atribuir Responsabilidades e Cargos	Req 5.3 e 7.1/.2 A.6.1.1	1º trimestre 2017	CD
		1.2.2	o Estabelecer protocolos e contactos com autoridades competentes	A.6.1.3 A.6.2.2	2º trimestre 2017	Gestor da Segurança; Encarregado da Protecão de Dados; Gabinete de Crise
		1.2.3	○ Manter contactos com grupos especializados de seg. informação	A.6.1.4	2º trimestre 2017	Gestor da Segurança e GSTI
	Medida 3: Liderança e Comprometimento	**1.3.1**	○ Assegurar alinhamento na Política de Segurança	A.6.1.5	2º trimestre 2017	CD
		1.3.2	○ Promover a melhoria contínua	Req 5 e 10	2º trimestre 2017	Comité de Segurança
	Medida 4: Framework documental do SGSI	**1.4.1**	○ Implementar estrutura documental do âmbito do SGSI	Req 7.5	2º semestre 2017	Gestor da Segurança e GSTI
		1.4.2	o Definir responsabilidades pela gestão documental	Req 7.5	2º semestre 2017	Gestor de Segurança

Eixo II: Pessoal	Medidas	Ações		Controlo	Conclusão	Responsavel e Participante
	Medida 5: Política de segurança na abrangência contratual e nos recursos da função	**2.5.1**	o Verificar de antecedentes no processo de contratualização	A.7.1.1	março 2017	Depto. Recursos Humanos e Unidades Orgânicas
		2.5.2	o Atribuir perfil funcional	A.9.1 A.9.2	março 2017	GSTI e Depto. Recursos Humanos; Responsável Hierárquico
		2.5.3	o Controlar acesso aos recursos durante o período de contratualização	A.7.2.1	março 2017	GSTI e Depto. Recursos Humanos; Responsável Hierárquico
		2.5.4	o Definir requisitos formais na cessação e alteração contratual	A.7.3.1	março 2017	GSTI e Depto. Recursos Humanos; Responsável Hierárquico
	Medida 6: Programa de consciencialização sobre segurança da informação	**2.6.1**	○ Política de utilização dos sistemas e tecnologias de informação	A.7.2.1/A.7.2.3 A.9.3 / A.9.4	on going	GSTI e Gabinete Jurídico
		2.6.2	o Ações de formação sobre preocupações relacionadas com a segurança da informação	A.7.2.2	junho 2017	GSTI e Depto. Rec Humanos; GMC
		2.6.3	○ Sensibilização no uso da Política de Segurança ao posto de trabalho	A.7.2.1	junho 2017	CD e Depto. Rec Humanos; Resp Hierárquicos
		2.6.4	o Disponibilizar e divulgar informação relacionada com a segurança da informação	A.5.1.2	setembro 2017	GSTI e Depto. Rec Humanos; Responsável Hierárquico
	Medida 7: Formação técnica	**2.7.1**	o Definir e concretizar plano de formação técnica especializada	Req 7.2	2º semestre 2017	GSTI e Depto. Rec.Humanos; Depto. Financeiro

Eixo III: Físico e Ambiental	Medidas	Ações		Controlo	Conclusão	Responsavel e Participante
	Medida 8: Execução de testes, nos *Data Centers*, para falhas previsíveis	**3.8.1**	○ Realizar simulacros operacionais por sistema computacional em caso de falha energética	A.17.1.1	2º semestre 2017	GSTI e Unidades Orgânicas
		3.8.2	○ Documentar e aplicar melhoria contínua na mitigação do risco	A.12.1 A.16.1.7	2º semestre 2017	GSTI e Unidades Orgânicas
	Medida 9: Realizar planos de contingência e *disaster recovery plan*	**3.9.1**	○ Realizar e documentar plano(s) de contingência em caso de quebras prolongadas de energia e de telecomunicações	A.17.1.1	2º semestre 2017	GSTI e Unidades Orgânicas
		3.9.2	○ Validar planos de continuidade operacional (*disaster recovery plan*)	A.17.1.2 A.17.2	1º semestre 2018	GSTI e Unidades Orgânicas
		3.9.3	○ Rever e avaliar os planos de continuidade operacional	A.17.1.3 A.17.2	2º semestre 2018	GSTI e Unidades Orgânicas
	Medida 10: Procedimentos de segurança nos equipamentos/ativos em uso fora das instalações	**3.10.1**	o Estabelecer procedimento em caso de roubo, violação ou perda de computadores portáteis	A.6.1.1 A.6.1.2	2º semestre 2017	Gestor de Segurança
		3.10.2	○ Definir e aplicar política sobre equipamentos não vigiados e de secretária limpa	A.11.2.8 A.11.2.9	2º semestre 2017	Gestor de Segurança
	Medida 11: Requalificar bastidores técnicos da rede dados e voz	**3.11.1**	○ Refrigeração e ligação à rede protegida	A.11.2.2	2º semestre 2017	GSTI
		3.11.2	○ Acomodamento, higiene e documentação	A.11.2.4	2º semestre 2017	GSTI
		3.11.3	○ Plano de auditoria na validação dos procedimentos operacionais	A.11.2.5	2º semestre 2017	GSTI
	Medida 12: Redefinir localização *Data Center* em	**3.12.1**	○ Realizar estudo alternativo da localização do Data Center em Lisboa	A.11.2.2	janeiro 2018	GSTI

Eixo IV: Tecnológico	Dimensão Aplicacional					
	Medidas	**Ações**		**Controlo**	**Conclusão**	**Responsavel e Participante**
	M14: Aquisição e/ou desenvolvimento aplicacional	**4.14.1**	o Realizar enquadramento ao propósito e expressão de necessidades	A.17.1	maio 2017	Dirigentes unidades orgânicas e GSTI
		4.14.2	o Definir planemento e aceitação de sistemas	A.12.1.3	maio 2017	GSTI e Gestor de Segurança
		4.14.3	o Validar definição técnica integrada	A.14 e A.17	maio 2017	GSTI e Gestor de Segurança
		4.14.4	o Implementar gestão de alterações alinhado com framework ITIL	A.12.1.2	junto 2017	GSTI e Gestores Aplicacionais; Gestor de Segurança
	M15: Gestão de ativos	**4.15.1**	○ Categorizar e classificar as aplicações/ativos	A.8.1.1	maio 2017	GSTI e Dirigentes nas unidades orgânicas
		4.15.2	○ Eleger formalmente os responsáveis das aplicações	A.8.1.2	março 2017	GSTI e Dirigentes nas unidades orgânicas
		4.15.3	○ Manter a relação matricial atualizada	A.8.1.3	a partir março 2017	GSTI e Gestor de Segurança
	M16: Separação dos ambientes de desenvolvimento e de produção	**4.16.1**	○ Disponibilizar diferentes ambientes de processamento	A.12.1.4 A.14.3.1	1º semestre 2017	GSTI

Eixo IV: Tecnológico	Dimensão Lógica					
	Medidas	**Ações**		**Controlo**	**Conclusão**	**Responsavel e Participante**
	M17: Implementar políticas de identificação e autenticação	**4.17.1**	○ Política da criação de acessos à rede e serviços	A.9.1.1	janeiro 2017	GSTI
		4.17.2	○ Política de autenticação de utilizadores para ligações externas	A.9.1.2	março 2017	GSTI
		4.17.3	○ Política de responsabilidade dos utilizadores na utilização dos sistemas e tecnologias de informação	A.9.3	abril 2017	GSTI e Gestor de Segurança
		4.17.4	○ Política de acesso dos prestadores de serviços externo	A.15.1	on going	GSTI e Gestor de Segurança
	M18: Gestão de acesso de utilizadores	**4.18.1**	○ Criação e remoção de Utilizadores	A.9.2.1	fevereiro 2017	GSTI e Depto RH; G Juridico
		4.18.2	○ Gestão de privilégios	A.9.1.2 A.9.2.4 /.5/.6	março 2017	GSTI; Unid Organicas e Gestores Aplicacionais
		4.18.3	○ Gestão das palavras.passe do utilizador	A.9.4.3	janeiro 2017	GSTI e Gestor de Segurança
		4.18.4	○ Revisão dos direitos/privilégios de acesso dos utilizadores	A.9.2.3 A.9.2.5/.6	a partir junho 2017	GSTI e Gestor de Segurança
	M19: Gestão e Correlação de Eventos de Segurança	**4.19.1**	○ Monitorização de *logs,* análise e *reporting*	A.12.4.3	junho 2017	GSTI

Eixo IV: Tecnológico	Dimensão Rede				
	Medidas	**Ações**	**Controlo**	**Conclusão**	**Responsavel e Participante**
	M20: Planear e implementar arquitetura LAN/WAN redundante	**4.20.1** ○ Redefinir e implementar arquitetura da rede LAN	A.17.1 A.17.2	março a dezembro	GSTI
		4.20.2 ○ Redundância na rede VPN e internet service infrastrutucture	A.17.2.1	on going	GSTI
		4.20.3 ○ Aquisição de link redundante para internet service infrastrutcture	A.17.2.1	janeiro 2017	GSTI
		4.20.4 ○ Monitorização e gestão centralizada da rede LAN e wireless (WLAN)	A.11.2.3	dezembro 2017	GSTI
		4.20.5 ○ Uniformização do tipo de cablagem (cat.6) rede passivo	A.11.2.3	2ºsemestre 2017	GSTI
	M21: Sistema de firewall redundante	**4.21.1** ○ Substituir e implementar novo sistema de firewall redundante com IDS	A.11.1.1/4 A.14.1	janeiro 2017	GSTI
		4.21.2 ○ Desenvolver Prova de Conceito da solução	A.11.1.1/4 A.14.1	on going	GSTI
	M22: Sistema de Antivírus	**4.22.1** ○ Política de antivírus ativo em todos os equipamentos cliente e servidores	A.12.2	janeiro 2017	GSTI
		4.22.2 ○ Realizar e disponibilizar relatórios de desempenho e estado atual das instalações de antivírus	A.12.2	março 2017	GSTI

Eixo V: Conformidade & Regulação	**Medidas**	**Ações**	**Controlo**	**Conclusão**	**Responsavel e Participante**
	Medida 23: Designar um Encarregado da Proteção de Dados / Data Protection Officer	**5.23.1** ○ Atribuir cargo de Encarregado da Proteção de Dados	A.18 Reg EU 2016/679	maio 2018	CD e Gestor Seg.; Coord GSTI
		5.23.2 ○ Estabelecer uma cultura consistente e integrada	A.18 Reg EU 2016/679	maio 2018	Gestor Seg. e Data Protection Officer
	M 24: Sistema de Gestão de Notificações de Incidentes	**5.24.1** ○ Desenvolver e disponibilizar plataforma notificação de incidentes	A.18 Reg EU 2016/679	maio 2018	Coord GSTI e Gestor Seg
		5.24.2 ○ Permitir ao cidadão autenticação no acesso à plataforma de notificação de incidentes	A.18 Reg EU 2016/679	maio 2018	Gestor Seg e Data Protection Officer
		5.24.3 ○ Estabelecer canal seguro de comunicação com a autoridade de controlo	A.18 Reg EU 2016/679	maio 2018	Gestor Segurança e Data protection Officer
	M25: Tecnologia e interoperabilidade entre sistemas	**5.25.1** o Avaliar adaptação tecnológica	A.18 Reg EU 2016/679	maio 2018	Coord GSTI e Gestor Seg
		5.25.2 o Validar a Interoperabilidade entre sistemas	A.18 Reg EU 2016/679	maio 2018	Gestor Seg e Coord GSTI
	M26: Revisão contratual dos prestadores de serviços	**5.26.1** o Garantir cumprimento ou execução	A.18 Reg EU 2016/679	maio 2018	Data ProtectionOfficer e GGCCP

9. CONSIDERAÇÕES FINAIS

9.1. CONCLUSÕES

Em primeiro lugar, quero registar que o desenvolvimento deste trabalho em ambiente organizacional, proporcionou uma experiência enriquecedora na envolvência com várias pessoas sobre o tema da gestão dos riscos e segurança da informação, bem como o conhecimento adquirido sobre os processos de emergência médica pré-hospitalar assentes na infraestrutura dos sistemas e tecnologias de informação do INEM. Por outro lado, estou convicto que a partilha do conhecimento entre os vários intervenientes que fizeram parte deste trabalho, resultou numa experiência enriquecedora para todos.

A realização deste trabalho permitiu alavancar um conjunto de fatores beneficiadores para a governação dos sistemas e tecnologias de informação em utilização na organização do INEM, em que a *layer* do risco e da segurança da informação, potenciou "um olhar diferente" aquando o desenvolvimento de novos projetos, aumentou a sensibilidade e participação dos colaboradores envolvidos na administração de sistemas e redes e, sobretudo, permitiu reconhecer que a aplicabilidade das "boas práticas" são ferramentas facilitadoras num processo de melhoria contínua. Prova é que, durante o decorrer deste trabalho foram inicializadas determinadas ações pela equipa do GSTI/INEM como resultado da sua envolvência no desenvolvimento deste projeto e do reconhecimento da aplicabilidade das "boas práticas" como fator diferenciador e facilitador nos processos de gestão e administração dos sistemas de informação. Estes primeiros passos, registam evidências de que é possível ultrapassar barreiras, mesmo quando existem dificuldades ou oposições internas.

Atrevo-me a afirmar que, perante o atual nível de maturidade obtido na vertente da gestão da segurança dos sistemas de informação, permite antever que existem condições favoráveis para a concretização das medidas propostas e que não existem fatores inibidores para a obtenção, no médio prazo, da certificação em gestão da segurança de sistemas de informação, ou seja, na obtenção da certificação da ISO/IEC 27001.

Sabemos que não existem sistemas com arquiteturas perfeitas, como também, não existe uma segurança de informação com total eficácia. Aliás, é costume dizer-se que "não existe segurança da informação eficaz. Qualquer sistema é vulnerável a um ataque." Contudo, também sabemos que ao implementar um SGSI, estamos a transmitir uma imagem de preocupação com a integridade e preservação dos seus ativos de informação, cada vez mais importante e com maior visibilidade, conseguindo simultaneamente gerir o risco a que se encontra sujeita. Na implementação do Sistema de Gestão de Segurança da Informação (SGSI) é sempre necessário avaliar bem quais os riscos reais e quais os prejuízos inerentes. Na perspetiva financeira será necessário um investimento adicional para a implementação do SGSI. Este investimento está dependente da dimensão e impacto das vulnerabilidades identificadas e dos fatores de risco associados ao desempenho da instituição, mas também, no impacto ao nível da sua reputação.

Por outro lado, segurança da informação é sinónimo de limitar ações, impor barreiras, vigiar ações, o que poderá criar atritos com o funcionamento, mais ou menos liberal, no âmbito da gestão das redes computacionais e organizacionais. Deste modo e, como matéria transversal que é, será necessário

uma mudança cultural na instituição na forma como esta terá de olhar para a informação e para a segurança da informação. Uma mudança que deve ser aceite e praticada por todas as unidades orgânicas, parceiros e prestadores de serviços.

Face ao objetivo traçado, desde o momento inicial, este trabalho tornou-se exequível. Estou convicto que a sua aplicação terá forçosamente impacto nos objetivos e exigências na organização, tornando-se numa opção estratégica. O comprometimento da gestão de topo na implementação do SGSI é vital para assegurar e reforçar os recursos necessários para a implementação do Sistema de Gestão de Segurança da Informação. Será uma árdua tarefa mas, na minha opinião, as vantagens resultantes da construção deste sistema de gestão recompensam todo o esforço que a organização, como um todo, tem que ter para que o SGSI seja implementado.

9.2. LIMITAÇÕES E RECOMENDAÇÕES PARA TRABALHOS FUTUROS

Se por um lado a realização deste trabalho e a análise dos resultados obtidos permitiu retirar proveitos relevantes para a definição do rumo a implementar com o Sistema de Gestão de Segurança da Informação, por outro lado, este teve algumas limitações de ordem técnica por não ser possível realizar testes de penetração a algumas das aplicações, com recurso a ferramentas especializadas e, deste modo, poder definir com maior rigor recomendações e medidas que possam analisar e validar a arquitetura de um sistema computacional.

Como trabalho futuro, perspetivam-se as desafiantes tarefas que surgirão aquando da implementação do SGSI, no seu enquadramento na operacionalização das etapas DO (Implementar e Operar) – CHECK (Monitorizar e Rever) – ACT (Manter e Otimizar), para além da interação transversal que haverá com as unidades orgânicas na concretização das diversas medidas propostas.

A segurança da informação, para além de ter uma componente técnica e infraestrutural em tecnologias de informação, tem sobretudo uma componente processual e humana “forte” dentro da organização. Envolver, desde de início, as pessoas que fazem parte dos processos organizacionais sobre o tema da segurança de informação e das boas práticas a aplicar é, sem dúvida, uma mais-valia no desenvolvimento do nosso trabalho pois, a obtenção e partilha de conhecimento é imensa. Este envolvimento e partilha é de extrema importância na fase de planeamento do SGSI pois, permitirá abrir o caminho para a sua implementação.

BIBLIOGRAFIA

Carneiro, A. (2016). Auditoria e Controlo de Sistemas de Informação. FCA- Editora de Informática, Lda. Lisboa

Casaca, J. & Correia, M. (2010). Porque é necessária a segurança da informação? Da estratégia às políticas de segurança. Lusíada. Política Internacional e Segurança, nº3, pp.89-116.

Casaca, J. (2014). Gestão do Risco na Segurança da Informação - Conceitos e Metodologias.

CERT.PT (2016). Coordenação da resposta a incidentes. Disponível em: http://www.cncs.gov.pt/cert-pt/coordenacao-da-resposta-aincidentes/index.html [consultado em abril 8, 2016].

CNCS (2015). Centro Nacional de Cibersegurança. Disponível em: http://www.cncs.gov.pt/pagina-inicial/index.html [consultado em outubro 7, 2015].

Coelho, P. (2013). Certificação APCER NP ISO/IEC 27001:2013. itSMF Seminário Anual 2013. Lisboa.

INEM (2015). Site institucional do INEM. www.inem.pt [consultado em abril 5, 2015].

ISO 31000:2013 (2013). Gestão do risco – Princípios e linhas de orientação. Norma Portuguesa. Instituto Português da Qualidade. Caparica.

ISO/IEC 27000 (2008). Information technology - Security techniques - information security management systems - Overview and vocabulary. BSI-British Standard. UK

ISO/IEC 27001:2013 (2013). Tecnologias de Informação. Técnicas de Segurança. Sistemas de gestão de segurança da informação – Requisitos. Norma Portuguesa. Instituto Português da Qualidade. Caparica.

ISO/IEC 27002 (2013) - Information Technology - Security Techniques: Code of practice for information security management. International Standard. www.iso.org

ISO/IEC 27003 (2010) - Information Technology - Security Techniques: Information security management system implementation. International Standard. www.iso.org

ISO/IEC 27005 (2008). Information technology - Security techniques - information security management. BSI-British Standard. UK

ISO27K Forum information Security (2015). http://www.iso27001security.com/html/toolkit.html [consultado em fevereiro,2 2016].

itSMF-12ª Conferência Anual itSMF Portugal 2015. "Para além do ITIL: Tradição e Novas Tendências". Disponível em http://www.itsmf.pt/Default.aspx?tabid=212&language=pt-PT [consultado em março,23 2016).

Martins, A., e Santos, C.(2005). Uma metodologia para a implantação de um sistema de gestão de segurança da informação. Journal of Information Systems and Technology Management, V. n.2, pp. 121-136.

Martins, I. (2013). Auditoria dos sistemas de informação das instituições financeiras. Instituto Politécnico de Lisboa. Instituto Superior de Contabilidade e Administração de Lisboa.

Martins, J. (2008). Framework de Segurança de um Sistema de Informação. Universidade do Minho e Academia Militar.

Melo, M. (2016). Ciclo de Palestras-Proteção de Dados e Cibersegurança. Regulamento Geral sobre a Proteção de Dados. Faculdade de Direito da Nova. Lisboa.

Oliveira, R. (2015). Análise de risco associado a quebras de serviço. Dissertação Mestre em Segurança Informática. Universidade de Lisboa-Faculdade de Ciências-Departamento de Informática

Regulamento UE 2016/679 (2016). Regulamento Geral sobre a Proteção de Dados. Parlamento Europeu e do Conselho da União Europeia, de 27 de abril de 2016. Publicado no dia 4 de maio 2016.

Rigon, E. e Westphall, C. (2013). Modelo de Avaliação da maturidade da segurança da informação. *Revista Eletrónica de Sistemas de Informação, v.12 (jan-abr),* pp. 1-19.

Santos, S., Rodrigues, L. &Pereira, D. (2014). Práticas de Segurança da Informação num Centro Hospitalar. Artigo 14ª CAPSI/2014

Seixas, S. M. (2013). Modelo para a Gestão de Eventos de Segurança da Informação. Minho, Portugal: Universidade do Minho - Escola de Engenharia.

Silva, D. (2011). Benefícios e Fatores Condicionadores da Obtenção de Certificação em Gestão da Segurança de Sistemas de Informação. Dissertação de Mestrado em Engenharia e Gestão de Sistemas de Informação, Universidade do Minho-Escola de Engenharia.

Silva, P. T., Carvalho, H. & Torres, C. B. (2003). Segurança dos Sistemas de Informação. Editora Centro Atlântico. Vila Nova de Famalicão.

Vian,P. (2016). Desenvolvimento de um quadro situacional para a cibersegurança em Portugal. Universidade Nova de Lisboa – Faculdade de Direito

Zúquete, A. (2015). Segurança em Redes Informáticas (3ªed. atualizada e aumentada). FCA-Editora de Informática, Lda. Lisboa.