DM

Análise de Segurança e Aperfeiçoamento de uma Rede Universitária de Telecomunicações

DISSERTAÇÃO DE MESTRADO

João Pedro Basílio Azevedo
MESTRADO EM ENGENHARIA ELETROTÉCNICA - TELECOMUNICAÇÕES

UNIVERSIDADE da MADEIRA
A Nossa Universidade
www.uma.pt

março | 2019

Análise de Segurança e Aperfeiçoamento de uma Rede Universitária de Telecomunicações

DISSERTAÇÃO DE MESTRADO

João Pedro Basílio Azevedo
MESTRADO EM ENGENHARIA ELETROTÉCNICA - TELECOMUNICAÇÕES

ORIENTADOR
Eduardo Miguel Dias Marques

CO-ORIENTADORA
Lina Maria Pestana Leão Brito

AGRADECIMENTOS

O concretizar deste grande e demoroso desafio que não só se traduz na realização e conclusão desta Dissertação como também no percurso que fiz ao longo do mestrado em Engenharia Eletrotécnica – Telecomunicações, onde poucas são as pessoas que sabem as dificuldades e obstáculos que passei, foi unicamente possível graças à minha força de vontade, mas sobretudo ao apoio incansável que me foi demonstrado por um conjunto de pessoas, às quais gostaria de transmitir, especialmente, o meu sincero e profundo agradecimento e reconhecimento, nomeadamente:

Aos meus pais e à minha irmã que sempre me apoiaram, incentivaram e me mostraram o quão difícil é ultrapassar um obstáculo que nós próprios criámos, sem nos apercebermos, que muito se esforçaram para me proporcionar tudo o que necessitei para alcançar e ultrapassar esta etapa com o maior sucesso possível, fazendo-me acreditar que por maiores que fossem as adversidades eu seria capaz de atingir tudo o que quisesse, nunca desistindo sem nunca antes tentar. Esta conquista também é vossa! Espero continuar a orgulhar-vos ao longo da minha vida.

À minha princesa Sílvia Santos, que antes de ser minha namorada é a minha melhor amiga, pelo seu enorme apoio, incentivo e persistência ao longo de todo este percurso, pela sua compreensão, paciência, motivação e força que me deu e que contribuí para a conclusão deste desafio.

Ao meu tio Carlos Martins pelo apoio, força e motivação que me deu, da maneira que quem o conhece sabe, e que foi fundamental para a construção e início do percurso que agora chegou ao fim.

E ao meu tio Lourenço Basílio pelo apoio, força, motivação e compreensão que me deu ao longo deste percurso e que apesar de ter aceite trabalhos durante a realização desta dissertação, sempre contribuíram para a minha formação pois fizeram-me crescer não só a nível profissional, mas também a nível pessoal.

Um agradecimento a toda a minha restante família, tios, tias, primos, primas e até grandes amigos, amigos, colegas e conhecidos pela amizade e apoio prestado ao longo da minha vida.

Tenho também muito a agradecer ao meu orientador Professor Eduardo Miguel Dias Marques e à minha coorientadora Professora Lina Maria Pestana Leão Brito pela oportunidade de realizar este trabalho, por todo o conhecimento que me transmitiram, pela disponibilidade demonstrada para o esclarecimento de quaisquer dúvidas que tivesse em qualquer altura e pela paciência que tiveram comigo.

Tenho que agradecer também ao Rodrigo Freitas e à Carla Carvalho por toda a vossa ajuda e sobretudo disponibilidade prestada.

De outro modo, gostaria de agradecer a todos os docentes da Faculdade de Ciências Exatas e da Engenharia da Universidade da Madeira, que contribuíram para a minha formação, fazendo-me crescer a nível profissional.

E por último, mas não menos importante, quero dedicar o concluir desta etapa à minha avó Adília e aos restantes avôs e avós que estarão sempre presentes na minha vida e em todo o meu percurso.

A todos, o meu MUITO OBRIGADO por tudo!!!

RESUMO

A Segurança da Informação é hoje uma vertente fundamental da segurança dos recursos e ativos das empresas, das organizações e das instituições, visto todo o mundo estar totalmente interligado através da internet. A mesma é alcançada pela implementação de um conjunto adequado de controlos, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de *software* e *hardware*. Estes controlos precisam ser estabelecidos, implementados, monitorizados, analisados criticamente e melhorados para assegurar que os objetivos da empresa/organização bem como da sua segurança no geral sejam atendidos. O cumprimento das normas não é suficiente, é necessário provar que estão a ser cumpridas com auditorias regulares que produzem os relatórios com as melhores práticas de segurança.

A UMa é uma universidade complexa na medida em que apresenta uma rede de telecomunicações com um grau de complexidade médio alto, por os sistemas da universidade envolverem três edifícios, equipamentos de rede, sistemas de informação, onde milhares de utilizadores (alunos, docentes, funcionários, convidados, etc…) estão diariamente em contacto com eles. Dessa forma, o nível de segurança da universidade, também complexo, apresenta alguns problemas/defeitos. O cerne deste trabalho foi identificar quais os problemas de segurança que a universidade enfrenta, atualmente, tais como a inexistência de normas, processos e/ou procedimentos, formais, para uma boa gestão de segurança, entre outros.

Nesta sequência, efetuou-se um levantamento e um estudo de vários conceitos, normas, metodologias e processos por forma a ver qual seria a melhor abordagem a esses problemas da UMa. Embora terem sido identificadas inúmeras formas de abordar os problemas, optou-se por abordar especificamente a família das normas 27000 por ser vocacionada para a área da segurança da informação, sistemas de gestão.

Deste modo foi efetuada a caracterização à UMa, recorrendo ao levantamento de várias informações sobre a situação e estado atual da rede da UMa, onde foram identificados um conjunto de problemas. Foi definida uma metodologia de análise por forma a analisar e avaliar esse conjunto de problemas para a obtenção do nível de risco de segurança que a UMa enfrenta e por fim foi proposto a definição de um conjunto de políticas para os mitigar.

Como resultados do trabalho, foram definidas seis políticas de segurança, complementadas com onze controlos, associadas aos domínios (Política de Segurança da Informação; Organização de Segurança da Informação; Controlo de Acesso; Segurança Física e Ambiental) das normas abordadas (ISO/IEC 27001 e ISO/IEC 27002).

Palavras chave:

Segurança da Informação; Gestão de Segurança; Análise de Segurança; Políticas de segurança; Norma ISO/IEC 27001; Norma ISO/IEC 27002.

ABSTRACT

Information Security is today a fundamental aspect of the security of resources and assets of companies, organizations and institutions, since the whole world is totally interconnected through the internet. It is achieved by implementing an adequate set of controls, including policies, processes, procedures, organizational structure, and software and hardware functions. These controls need to be established, implemented, monitored, critically reviewed and improved to ensure that the objectives of the company/organization as well as their overall safety are met. Compliance with standards is not enough, it is necessary to prove that they are being met with regular audits that produce reports with best security practices.

The University of Madeira is a complex university in that it has a medium-high complexity telecommunications network, because the university's systems involve three buildings, network equipment, information systems, where thousands of users (students, teachers , employees, guests, etc ...) are in daily contact with them. In this way, the university security is also complex and presents some problems/faults. The core of this work was to identify the security problems that the university currently faces, such as the lack of formal norms, processes and/or procedures, for good security management, among others.

In this sequence, a survey and a study of several concepts, standards, methodologies and processes was carried out in order to see what would be the best approach to these UMa problems. Although many ways of addressing problems have been identified, it was decided to specifically address the 27000 family of standards because it is geared to the area of information security, management systems.

In this way, the UMa was characterized, using a survey of various information about the current situation and state of the UMa network, where a set of problems were identified. An methodology analysis was defined in order to analyze and evaluate this set of problems to obtain the level of security risk faced by UMa and finally it was proposed the definition of a set of policies to mitigate them.

As a result of the work, six security policies, supplemented by eleven controls, associated to the domains (Information Security Policy, Information Security Organization, Access Control, Physical and Environmental Security) were defined as standards (ISO / IEC 27001 and ISO / IEC 27002).

Key Words:

Information Security; Security Management; Security Analysis; Security Policies; Standard ISO/IEC 27001; Standard ISO/IEC 27002.

LISTA DE ACRÓNIMOS

ISO – International Organization for Standardization

IEC – International Electrotechnical Commission

ITIL – Information Technology Infrastructure Library

COBIT – Control Objectives for Information and related Technology

CASCO – Committee on Conformity Assessment

CCTV – Closed-Circuit Television

SGSI – Sistema de Gestão de Segurança da Informação

ISMS – Information Security Management System

RGPD – Regulamento Geral de Proteção de Dados

UMa – Universidade da Madeira

TI – Tecnologia de Informação

PDCA – Plan Do Check Act

VLAN – Virtual LANs

LAN – Local Area Network

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

1. INTRODUÇÃO

Hoje em dia, a facilidade de lançar ataques é muito grande, dada a profusão de sites na internet que explicam com grandes níveis de detalhe e pormenor como executar estas atividades onde até as ferramentas que são necessárias podem ser encontradas facilmente através de uma pesquisa elementar. Quando a ameaça se concretiza num ataque real, tudo pode acontecer, dependendo dos mecanismos de segurança adicionais que existem no interior do perímetro. Existem muitos tipos possíveis de ataques entre os que se conhecem e os que se hão de criar no futuro, na maioria dos casos explorando as tais vulnerabilidades de software, aplicacional ou de sistema operativo. Só para ter uma ideia, alguns dos ataques mais frequentes são o acesso remoto, as backdoors aplicacionais, o rapto de sessão, os erros de sistema operativo, a negação de serviço e os vírus, no geral. Mas esses ataques só são bem-sucedidos em caso de existência de vulnerabilidades quer sejam conhecidas por parte do atacante ou não. O que quer isto dizer que nenhuma organização pode com toda a certeza assegurar que as medidas de proteção que implementou, na sua rede, sejam as suficientes para a tornar completamente segura [1].

Com o crescente número de ataques e os seus devidos impactos, que hoje em dia causam inúmeras dores de cabeça a empresas e a organizações, as mesmas têm revelado uma preocupação enorme em protegerem-se desses eventuais ataques e exposição ao risco, de uma forma mais rápida.

Não há muito tempo, talvez há uns cinco anos para cá, alguns especialistas em conjunto com algumas empresas de todo o mundo, com competências reconhecidas na área da Cibersegurança haviam já colocado questões da segurança da informação no topo das prioridades devido aos elevados e complexos ataques e ameaças cibernéticas, em crescimento, que já atravessavam vários domínios de atuação. Atualmente temos vários casos, muitos dos quais mediáticos, por terem afetado não só dados pessoais como também dados financeiros de várias empresas de grande nome mundial, como por exemplo o Facebook [2]. Se na altura a situação já era clara para os especialistas, agora a necessidade de lidar com o aumento exponencial do problema torna-se prioritária. É importante, para uma boa caracterização e prevenção de ataques, ter em atenção a sua origem. Atualmente, sensivelmente 70% dos ataques têm origem no interior das organizações, sendo intencionais ou não e isto porque a maioria dos mecanismos de segurança encontram-se direcionados para o exterior e acabam por ser vocacionados para proteger contra-ataques de entidades externas à organização [3].

Nunca como antes a análise de risco subjacente a cada empresa e a definição dos controlos e medidas adequadas para a sua mitigação, conforme indicação e recomendação de algumas normas da família 27000, esteve tão ativa. Ainda que as normas apresentem a base e as indicações para a avaliação e mitigação do risco, nem sempre se adequam à necessidade e realidade de algumas empresas, por exemplo, as pequenas e médias empresas. Desta forma há uma necessidade de aplicar algo mais

rápido e de certa forma mais simples que possa ser feito e/ou implementado, relativamente à gestão do risco – Segurança de informação.

A segurança de um sistema informático é frequentemente objeto de comparação na medida em que o nível de segurança de um sistema é caracterizado a partir da identificação do seu elo mais fraco, ou seja, de que serve a construção de uma porta blindada numa casa toda construída com cimento e ferro se as janelas estiverem abertas? Isto significa que a segurança deve ser abordada num contexto global levando em conta que é necessária a sensibilização dos utilizadores, a segurança lógica, a segurança física, a segurança das telecomunicações, etc… Um sistema informático é seguro se garantir os seguintes requisitos: disponibilidade; confidencialidade; integridade; autenticação; e não repúdio.

A tarefa de efetuar uma análise de segurança e posteriormente um aperfeiçoamento de uma determinada rede, quer seja ela de pequena ou de grande dimensão, empresa ou instituição obriga a que não só haja um grande conhecimento na área das redes bem como um entendimento em todos e mais alguns conceitos no que toca à segurança de computadores e à segurança de informação. Enquanto a análise de segurança a uma rede tem como foco principal a procura de riscos ou ameaças que possam afetar direta ou indiretamente a rede, o aperfeiçoamento foca-se no desenvolvimento de regras, políticas de segurança, auditorias e implementação de normas. A chave destes dois procedimentos é a segurança informática.

Uma outra razão para a aplicação da análise de segurança prende-se com o facto de as empresas e as organizações terem a necessidade de cada vez mais protegerem os seus ativos de forma a salvaguardarem toda a informação sensível que neles se encontra implícita. Garantir a manutenção dos ativos é fundamental para a continuidade a médio e a longo prazo do "negócio" das empresas. Os ativos têm a possibilidade de possuírem falhas na sua segurança que podem vir a proporcionar perdas na sua operabilidade por algum tempo. Daí a necessidade de estarmos sempre atentos aos ativos e aos riscos que cada um desses ativos possui, na empresa [4]. A análise irá permitir uma identificação e avaliação dos ativos de forma a saber qual o grau de importância que apresentam e o correspondente nível de risco que possuem. O objetivo é também efetuar uma avaliação económica do impacto de eventos negativos que tenham ou possam ocorrer na rede. Onde esse valor poderá ser utilizado para comparar com o custo da proteção da informação em análise. Quanto à própria gestão do risco, o cerne do mesmo é que uma empresa tem uma quantidade infinita de vulnerabilidades, mas uma quantidade finita de dinheiro disponível para lidar com elas. Portanto, as vulnerabilidades que podem causar mais prejuízos à empresa devem ser tratadas primeiro. Para além disso, é necessário considerar a probabilidade de ocorrerem esses eventos e incluí-los na elaboração de um plano de ação adequado, política de segurança.

Ainda há um enorme trabalho a fazer ao nível da segurança informática e da Cibersegurança no geral, por parte das entidades públicas, empresas privadas e/ou até das universidades pois não existe nenhuma técnica que permita assegurar que um determinado sistema seja inviolável. Mas é preciso saber que através do conhecimento,

das boas práticas, de uma boa análise, de um bom planeamento prévio e de uma política de segurança é possível chegar a um nível de segurança relativamente alto.

A intenção deste trabalho passa essencialmente por isso, em que se pretende, numa primeira fase, obter informação da situação atual da UMa, numa segunda fase efetuar uma análise de segurança a esses problemas identificados, através da investigação ao estado da arte com o propósito de achar uma metodologia para o efeito e posteriormente apresentar uma proposta de solução aos problemas identificados, com recurso à elaboração de um documento de políticas de segurança.

1.1 Motivação

Com o exponencial crescimento e a abertura das empresas/organizações ao mundo exterior através da disponibilização dos mais variados sites (Internet e Extranet) e da implementação de redes convergentes, as questões relacionadas com a segurança e proteção de dados estão cada vez mais a preocupar os gestores de sistemas e redes.

Desta forma há uma maior procura de soluções de segurança robustas e fiáveis com o intuito de assegurar a proteção das infraestruturas tecnológicas, tendo em conta questões fundamentais como a proteção da confidencialidade, da integridade e da disponibilidade da informação das empresas/organizações, sistemas e processos críticos, redução dos custos operacionais e otimização do seu funcionamento.

Dada a necessidade inadiável de ligação à Internet, compreender, definir e implementar medidas de segurança adequadas, deve ser considerada uma decisão inerente ao funcionamento de qualquer organização ligada à Internet ou outro tipo de rede.

Um ambiente como o Campus Universitário, onde vários tipos de utilizadores utilizam vários recursos (espaços, equipamentos e redes) e as entidades externas podem estar interessadas na informação recolhida e produzida no mesmo, precisa de um conjunto específico de políticas, técnicas e mecanismos para assegurar a correta utilização dos recursos.

Este é um desafio que passará por desvendar e por entender quais são essencialmente os pontos fracos da rede da universidade, ou seja, a universidade apresenta-se como um espaço que necessita de alguma análise e melhorias de determinados aspetos de segurança e o que será feito é basicamente a procura do que já está feito e do que não está a ser coberto.

Pelo facto de a fonte dos ataques ser muito diversificada, necessita de um grande grupo de métodos, bem estruturados e organizados, de forma a garantir aos responsáveis e representantes da Universidade um determinado e correto nível de confiança na segurança dos seus recursos.

Todo este trabalho envolve um profundo conhecimento das características da rede do Campus Universitário e dos seus utilizadores e procura no estado da arte, na segurança

da rede e do computador, as melhores escolhas para desenvolver e implementar uma política de segurança capaz de mitigar os problemas e desafios que a rede da UMa enfrenta.

1.2 Objetivos

Já há alguns anos para cá tem existido alguma, possamos chamar, insegurança com o nível de segurança que se encontra implementado. É evidente que não há uma satisfação com a solução que têm implementada atualmente. Todavia, ao longo dos anos tem havido alguma resposta nesse sentido, de aplicar umas ou outras técnicas, ferramentas, mecanismos de segurança de forma a mitigar algumas possíveis falhas e ou vulnerabilidades.

No entanto, continua a haver uma necessidade de melhoria em determinadas situações, no que diz respeito a procedimentos de segurança informática, desenvolvimento de processos e ou regras que indiquem ou encaminhem para uma determinada função, entre outros. É notório que a universidade tem, ainda assim, inúmeros problemas que tenham que ser resolvidos, mas, os objetivos deste trabalho apenas irão focar-se em alguns. Ora o trabalho apresentado tem como principais objetivos a identificação e análise de alguns problemas e/ou desafios que a rede da universidade enfrenta diariamente, assim como propor uma solução para mitigar esses tais problemas através da elaboração de um documento de políticas de segurança.

Numa primeira fase, e quase em simultâneo com a segunda fase pretende-se caracterizar a UMa em termos de estrutura e a nível de segurança, com recurso ao levantamento de dados, através de entrevistas semiestruturadas e também da elaboração de alguns questionários mais específicos. Esses dados acabam por ser agrupados em vários contextos de segurança representando a situação atual da UMa.

Na próxima fase esses mesmos dados são analisados, mediante determinados processos propostos, a fim de definir o nível de risco para cada contexto.

É com base nessa análise que será possível, posteriormente, propor um documento formal com políticas de segurança que se crê que seja o que apresente uma melhoria significativa no nível de segurança aceite pela UMa.

Em todas estas fases serão detalhados os processos utilizados para a realização das mesmas assim como a origem e a base que foi seguida para o efeito.

Acredita-se que, caso seja aceite/aprovado, o documento com as políticas, haverá uma mudança significativa na forma como serão abordadas as questões da segurança da informação, da UMa.

Em suma, os objetivos deste trabalho são:

- Caracterização da Universidade da Madeira;

- Definição da metodologia para a análise à situação atual da rede de telecomunicações da Universidade da Madeira;
- Proposta de políticas para a rede de telecomunicações da Universidade da Madeira – Documento de política de segurança.

1.3 Estrutura da Tese

Este documento é composto por seis capítulos e os mesmos encontram-se organizados da seguinte forma:

Capítulo 1: Introdução – Este primeiro capítulo apresenta a contextualização, a motivação que levou à realização deste trabalho e os objetivos a serem atingidos.

Capítulo 2: Estado da arte – Neste capítulo é feito um levantamento e descrição de vários conceitos, processos e normas de segurança e todas as definições ligadas direta ou indiretamente à análise e aperfeiçoamento de segurança de uma rede. No primeiro subcapítulo são apresentados os vários conceitos de segurança, no segundo são abordadas as principais normas que serviram de base para o desenvolvimento deste trabalho e por fim, nos restantes subcapítulos são abordados os restantes conceitos e outras normas relacionadas.

Capítulo 3: Caracterização da Universidade da Madeira – Neste capítulo é feita uma breve apresentação da instituição Universidade da Madeira assim como é feita também uma análise à constituição da mesma de forma a obter uma visão geral da sua dimensão. É feito ainda uma descrição da estrutura da rede de telecomunicações da instituição assim como é feito um levantamento dos desafios e/ou problemas que a rede da UMa enfrenta, onde o foco do presente trabalho incide. São ainda apresentados os resultados dos levantamentos do ponto de situação da rede da universidade da Madeira.

Capítulo 4: Metodologia e Análise – Neste capítulo encontra-se a metodologia para a análise dos problemas e para identificação do nível de risco que a instituição enfrenta, onde são descritos, detalhadamente, todos os processos seguidos.

Capítulo 5: Proposta de Implementação da Política de Segurança – Este capítulo apresenta a proposta escolhida para solucionar parte dos desafios/problemas da rede da UMa, com recurso à elaboração de um documento de política de segurança onde são explicados os passos da elaboração da mesma.

Capítulo 6: Conclusão e trabalho futuro – Este capítulo corresponde à retrospetiva geral do trabalho realizado onde são destacados os pontos relevantes abordados ao longo do trabalho. São também apresentadas propostas e ou soluções para um eventual trabalho futuro.

2. ESTADO DA ARTE

A informação sempre teve um valor inestimável para as empresas e, hoje em dia, é considerada um ativo indispensável e um recurso vital de grande importância para as empresas. Com o aumento da competitividade e da concorrência, nesta área, há uma maior preocupação para que as organizações sejam capazes de tomar decisões acertadas em todos os níveis. Antigamente os dados eram armazenados em relatórios, pastas e poderiam ser acondicionados em armários ou cofres onde os únicos riscos que enfrentavam eram apenas os danos por: ação do tempo, as condições ambientais no armazenamento, roubo ou assalto aos armários ou cofres. O processamento, tratamento e armazenamento dos dados digitais trouxe uma série de benefícios, a todos os níveis, para os vários intervenientes (gestores, administradores, utilizadores, etc…), mas, também acabaram por trazer uma série de problemas principalmente em como mantê-los seguros. Apesar das várias e diferentes formas e possibilidades de guardarmos os dados, por exemplo, em data-centers próprios, as ameaças também se apresentam de forma variada e distinta, por exemplo, invasões de hackers, vírus, danos físicos em material e equipamentos, fazendo com que os dados simplesmente desapareçam ou sejam alterados. Ainda existem alguns hábitos nas organizações em que só é reconhecida a importância dos dados quando são destruídos, perdidos ou roubados daí haver a necessidade em tomar as decisões acertadas. O que possibilita essas decisões acertadas é precisamente a realização de análises que os gestores e/ou administradores de rede têm que fazer a fim de estarem sempre atentos à evolução da rede e a todos os perigos que ela representa. Estabelecendo o nível de segurança a que a organização se propõe, e conhecendo "todos os cantos da casa" é possível efetuar uma análise de segurança de forma a obter quais os pontos críticos da organização e posteriormente arranjar soluções para os monitorizar e sobretudo mitigar. Para essas ações é necessário possuir conhecimento na área das Tecnologias da Informação e munir-se de todo o tipo de material (metodologias, normas, ferramentas, etc…).

Depois de abordados os principais desafios que as organizações enfrentam por estarem presentes no mundo virtual (Internet) e tendo em conta os objetivos apresentados, é fundamental ter bem definido os conceitos de segurança, ter o conhecimento de que metodologias existem para desenvolver uma análise de segurança, a uma organização, e em que se basear para propor uma solução para a mitigação dos desafios que a organização enfrenta.

O trabalho de investigação permitiu identificar alguns conceitos e sobretudo normas estabelecidas especificamente para este tipo de contexto. Foram abordados os vários conceitos de segurança pertinentes para este trabalho (Segurança Informática, Cibersegurança, Segurança da Informação), assim como as normas que seguem:

- ISO/IEC 27001:2013 [5]
- ISO/IEC 27002:2013 [6]
- ISO/IEC 27003:2010 [7]

- ISO/IEC 27005:2011 [8]

Hoje em dia, encontram-se diversas metodologias e práticas em segurança da informação para ambientes empresariais que são bem conhecidas na área. Entre elas estão CobiT, ITIL e a família ISO 27000, essas são exemplos de normas que normalizam o modelo como uma organização deve estruturar sua gestão da segurança da informação. É importante referir que a maior parte das normas da família ISO 27000 representam uma linha que orienta as organizações dispostas a se estruturarem para gerir os riscos de segurança da informação.

No geral, foram escolhidas estas quatro normas pelas mais variadas razões sendo que uma delas prende-se com o facto de todas serem normas standard que são globalmente aceites. A razão pela escolha das normas ISO/IEC 27001 e ISO/IEC 27002 foi pelo facto de ambas se complementarem e por reunirem as melhores condições para gerir os riscos associados à segurança da informação. As organizações ao se adequarem aos requisitos das normas, acabam por ter os seus procedimentos internos normalizados o que leva a uma maior produtividade das equipas, minimizando os riscos de falhas nos processos e os custos operacionais mais reduzidos. A razão pela escolha da norma ISO/IEC 27003 tem a ver com o facto de a mesma indicar uma estrutura para a elaboração da política de segurança, mais uma vez baseada sempre nas normas ISO/IEC 27001 e ISO/IEC 27002. Por fim, foi escolhida a ISO/IEC 27005 pelo facto de fornecer as diretrizes para a gestão de riscos de segurança da informação, que permitiu auxiliar com processos para a metodologia seguida na análise de segurança.

Os restantes conceitos apresentados serviram para reforçar a importância da certificação das organizações de forma a facilitar a gestão dos riscos de segurança.

Por fim, o último subcapítulo apresenta duas formas de efetuar avaliações onde a pessoa ou o gestor que efetua a análise e avaliação, necessita de optar ou por uma avaliação quantitativa ou por uma avaliação qualitativa. Neste trabalho optou-se por avaliar quantitativamente pelo facto de ser possível a apresentação e avaliação através de valores numéricos e também pelo facto de ter sido disponibilizado valores aproximados do custo (€) dos ativos da UMa.

2.1 Segurança

Cada vez mais a economia mundial depende das comunicações, da informática, da rede, da internet, o que por sua vez, à medida que há esta evolução das tecnologias, pelo facto das mesmas serem recentes e não tanto conhecidas, tornam-se bastante vulneráveis a questões de segurança.

A palavra segurança, com origem no termo em latim "*securus"*, que significa "sem temor, garantido", é um adjetivo e um substantivo feminino de dois géneros (segurar +

-ança). Este adjetivo muita das vezes pode ser associado como: autoconfiança; garantia; evidência; proteção; certeza; estabilidade; vigilante; guarda-costas; entre outros…

Recorrendo ao dicionário, dos mais variados conceitos de segurança que existem, destaca-se: "conjunto das ações e dos recursos utilizados para proteger algo ou alguém".

O termo segurança pode ser utilizado para se referir à pessoa que fala com confiança e certeza sobre um determinado assunto, ou seja, que demonstra conhecimento do assunto e que possui também uma boa dicção sobre o mesmo. Por exemplo: "O orador do discurso sobre as novas tecnologias, muito jovem e ainda inexperiente, demonstrou uma enorme segurança e simpatia para com o público."

O mesmo tema pode ser utilizado em vários contextos: segurança militar; segurança pública, segurança nacional, segurança no trabalho, segurança alimentar, segurança financeira, etc… das quais se dará uma maior relevância para este caso a segurança informática, a segurança de informação e a Cibersegurança [9].

Do ponto de vista da administração de redes e informática, seja de uma empresa ou organização, é conveniente interpretar o tema "segurança" de uma forma muito abrangente.

"Um sistema que é seguro é aquele que funciona nas condições desejadas e previamente definidas."

Este ponto de vista tem uma vantagem de ir logo para o objetivo final, embora deixe sempre a importante tarefa de definir as "condições desejadas" de funcionamento do sistema [10].

Ou seja, o facto de termos segurança é termos ausência de ameaças aos valores essenciais que queremos garantir. No entanto, ter ou não ter ameaças é algo que não se controla.

Por fim, dentro de um ambiente, no geral, existem dois tipos de segurança:

- Segurança Lógica
- Segurança Física

A **segurança lógica** é a forma como um sistema é protegido no nível de sistema operativo e de aplicação, ou seja, diz respeito a segurança da utilização do software, proteção de dados dos processos e dos programas e acesso autorizado dos utilizadores.

De seguida, encontram-se os principais objetivos a considerar no domínio da segurança lógica:

- Restringir o acesso aos programas e arquivos;
- Assegurar que os operadores possam trabalhar sem uma supervisão minuciosa e não possam modificar os programas nem os arquivos que não correspondam ao seu domínio de trabalho;

- Assegurar que sejam utilizados os dados, os arquivos e os programas de acordo com procedimentos corretos;
- Que a informação transmitida seja recebida só pelo destinatário ao qual foi enviada e não também a outros;
- Que a informação recebida seja a mesma que tenha sido transmitida;
- Que existam sistemas alternativos secundários de transmissão entre diferentes pontos;
- Que se disponha de passos alternativos de emergência para a transmissão de informação [11].

Na Tabela 1 encontram-se as funções e os objetivos a ter em conta quando se pretende assegurar a segurança lógica.

Tabela 1 - Objetivos Segurança Lógica [11].

Segurança Lógica	**Objetivos**
Gestão e controlo de acessos	O acesso ao SI informatizado deve ser condicionado pelo uso de passwords.
Gestão do SI informatização e da rede	Assegurar uma segura e adequada gestão de todos os computadores existentes na rede.
Segurança dos Sistemas Aplicacionais	Manutenção da segurança dos sistemas aplicacionais.

A **segurança física** é, muitas das vezes, um dos aspetos menos atendidos quando são elaborados os esquemas da rede e/ou sistema informático. Normalmente não é tido em conta que poderá existir um individuo interno que possa tentar ter acesso fisicamente à sala de operações do departamento de informática.

A segurança física é a segurança que é feita a nível das infraestruturas materiais: salas bastidores ou de operações, espaços que se encontram abertos ao público, postos de trabalho do pessoal e etc… Ou seja, serve para garantir a proteção dos Sistemas de Informação quanto às suas dimensões físicas (hardware, software, documentação e meios magnéticos).

A mesma consiste na aplicação de barreiras físicas e procedimentos de controlo, como medidas de prevenção e contramedidas perante ameaças aos recursos e informação confidencial da empresa ou da organização. Refere-se as barreiras físicas para proteger o acesso físico às salas de operações ou de bastidores, pudendo utilizar diferentes formas de proteção (fechaduras eletrónicas com registo, uso de câmeras de videovigilância, etc…). Refere-se aos procedimentos de controlo e aos mecanismos de segurança para proteger o hardware e os meios de armazenamento de dados [11].

Nas seguintes tabelas (Tabela 2 e Tabela 3) encontram-se os principais objetivos e ameaças a considerar no domínio da segurança física.

Tabela 2 - Objetivos Segurança Física [11].

Segurança Física	Objetivos
Do pessoal	Reduzir os riscos devidos a erros humanos, roubo, fraudes, e/ou má utilização dos recursos existentes.
Do equipamento	Proteger o hardware computacional, outros equipamentos, as suas interligações e o fornecimento de energia.
Das instalações	Requisitos da localização e estrutura dos edifícios destinados aos centros de informática garantindo um nível de segurança adequado.

Tabela 3 - Ameaças Segurança Física.

Segurança Física: Ameaças	Desastres naturais, incêndios acidentais, trovoadas, inundações.
	Ameaças ocasionadas por elementos humanos.
	Distúrbios, sabotagens internas e externas deliberadas.

2.1.1 Segurança Informática

Quando falamos em segurança informática, atualmente, a primeira coisa que pensamos é na Internet, pois é nessa rede mundial onde os ataques aos nossos computadores e também aos das pequenas e grandes empresas/instituições ocorrem com maior frequência [12]. A segurança na verdade assenta-se em 5 fundamentais pilares:

i. **Confidencialidade** – Este princípio tem a capacidade de limitar o acesso a informação apenas às entidades (utilizadores, técnicos, administradores, pessoas no geral, processos, máquinas, etc…) autorizadas.
ii. **Integridade** – Este princípio tem a capacidade de assegurar a precisão, exatidão e a consistência da informação durante todo o seu ciclo de vida, ou seja, garantir que a informação não foi alterada ou foi alterada com a sua devida autorização e concordância.
iii. **Disponibilidade** – Este princípio tem a capacidade de garantir que a informação esteja disponível sempre que houver necessidade de acesso, ou seja, não permite que o acesso a determinada informação seja interrompido durante todo o seu ciclo de vida.
iv. **Autenticação** – Este princípio consiste em garantir a identidade do utilizador quando o mesmo comprova a sua identidade perante um sistema, por diversos meios (dados biométricos, passwords, etc…).
v. **Não repúdio** – Este princípio consiste em impedir que um indivíduo ou uma entidade negue a execução de uma determinada ação, ou seja, garante que a pessoa ou entidade é quem diz ser.

De uma forma geral a segurança informática envolve os métodos, processos ou técnicas para o tratamento automático da informação em formato digital, possuindo um maior alcance, na medida em que inclui a proteção das redes e a infraestrutura tecnológica. Ou seja, a segurança informática consiste em garantir que os recursos materiais ou softwares de uma empresa ou organização sejam utilizados apenas no âmbito previsto [13].

A segurança informática agrega em si imensos aspetos na medida em que não está apenas ligada à proteção de equipamentos, mas também se encontra ligada à proteção dos dados privados, ainda para mais agora com a vinda do Regulamento Geral de Proteção de Dados, RGPD.

Se não há dúvidas que a sensibilização ajuda de certa forma os utilizadores e as restantes partes ligadas ao negócio a terem outra postura perante este tema, também se verifica que a educação sobre o mesmo não ajuda a prevenção de todos os cenários. Daí entrar em ação as legislações, como é o caso do RGPD, para dar um forte sentido às regras que necessitam de ser cumpridas.

Um outro foco a ver e rever é que existe uma enorme diferença de cultura de privacidade nas empresas e ou organizações entre pessoal da chefia e o pessoal que está mais ligado à produção, na medida em que ambos devem ter igual noção de quais são os elementos mais valiosos da empresa que devem ser protegidos.

Existem inúmeros problemas e de tal forma graves tais como o Ransomware, o malware bancário e a espionagem onde as empresas e as organizações têm que saber principalmente definir as suas prioridades de forma a proteger os seus ativos.

Embora um sistema informático possa ser protegido do ponto de vista **lógico** (através do desenvolvimento de software) ou **físico** (em termos de manutenção elétrica), as ameaças podem vir de programas maliciosos ou chegar por via remota.

Das ferramentas mais comuns, encontram-se as firewalls, a encriptação da informação, o uso de passwords de acesso e os programas de antivírus.

Pode dizer-se também que a segurança informática tem como objetivo assegurar que os recursos de um sistema de informação possam ser utilizados conforme uma empresa ou organização ou até um utilizador o tenha decidido, sem interferências.

2.1.2 Cibersegurança

Embora tenhamos uma perceção geral sobre o que representa a Cibersegurança, em certas ocasiões, o termo pode ser utilizado como sinónimo de segurança de computadores, segurança informática ou segurança da informação, mas essa ideia não é a mais correta.

O problema surge quando é necessário aplicar corretamente os conceitos, de acordo com as ideias que desejamos expressar. Embora existam diferentes definições para a Cibersegurança, é muito importante saber utilizá-las corretamente, de acordo com o contexto, e identificar as suas diferenças com os outros termos, por exemplo, o de segurança da informação [14].

A Cibersegurança, também conhecida como segurança do ciberespaço é o conjunto de meios e tecnologias que visam proteger de danos e intrusão ilícita, programas, computadores, redes e dados.

É ainda importante referir que a Cibersegurança não é somente responsabilidade do pessoal de TI, nem apenas da empresa ou organização. Trata-se sim de um trabalho de equipa. O desenvolvimento de um Ciberespaço seguro exige a participação de TODOS: empresa, organização, governo e restantes utilizadores.

Quanto aos utilizadores, os riscos a que os utilizadores de sistemas informáticos se submetem aumentam diariamente e são necessárias políticas de segurança apropriadas para a mitigação dos riscos.

2.1.3 Segurança da Informação

O conceito de segurança informática está intimamente relacionado com o conceito de segurança de informação onde está incluído a segurança dos dados e também dos sistemas em si.

Como visto anteriormente, o propósito da segurança em todos os campos de aplicação é reduzir os riscos até um certo determinado nível, para os interessados, em reduzir as ameaças latentes. Quanto à informação, a mesma pode ser encontrada em diversas formas, por exemplo, no formato digital (arquivos em meios eletrónicos ou óticos), na forma física (escrita ou impressa em papel), assim como de forma não representada, como pode ser uma ideia ou até o próprio pensamento da pessoa. A informação pode ainda ser armazenada, processada ou transmitida de diversas maneiras (estados): no formato eletrónico, na forma verbal ou por meio de mensagens escritas ou impressas.

O que quer isto dizer que independentemente da sua forma ou estado, a informação requer adequadas medidas de proteção, de acordo com a sua importância e criticidade e é onde a segurança da informação entra [14].

A segurança da informação, como mostra a Figura 1, é então um processo organizado e estruturado que permite preservar a confidencialidade, a integridade e a disponibilidade da informação e que se baseia em metodologias, normas, técnicas, ferramentas, estruturas organizacionais, tecnologias, entre outros.

Figura 1 - Triângulo representativo dos três pilares da Segurança da Informação [15].

A **Confidencialidade** – necessidade de assegurar que a informação seja acessível somente por pessoas devidamente autorizadas, ou seja, o acesso à informação é restrito apenas a utilizadores legítimos.

A **Integridade** – necessidade de garantir a veracidade e complementaridade da informação e dos seus métodos de processamento, ou seja, o conteúdo da informação não pode nunca ser modificado de forma inesperada.

A **Disponibilidade** – necessidade de assegurar o acesso à informação e bens associados por quem esteja devidamente autorizado, ou seja, a informação não só deve como também tem que estar sempre acessível, sempre que seja necessário [15].

Desta forma, quer dizer que as ameaças à segurança da informação são relacionadas diretamente à perda de umas destas três características.

Existirá uma perda de **confidencialidade** quando houver uma quebra de sigilo de uma determinada informação, por exemplo, quando é descoberta a password de utilizador/administrador ou quando a mesma é revelada por alguém que não o próprio, permitindo assim que sejam expostas informações restritas as quais seriam acessíveis apenas por um determinado utilizador (ou grupo de utilizadores).

Existirá uma perda de **integridade** quando uma determinada informação fica exposta a pessoas não autorizadas e que efetuam alterações que não foram aprovadas e não estão sob o controlo do proprietário da informação.

Existirá uma perda de **disponibilidade** quando a informação deixa de estar disponível ou acessível por quem precisar dela, por exemplo, quando há uma perda de comunicação com um sistema importante da empresa ou organização, que aconteceu com a quebra de um servidor ou de uma aplicação crítica ou que apresentou uma falha devido a um erro causado por um motivo interno ou externo ao equipamento ou por ação não autorizada de pessoal com ou sem má intenção.

2.2 Normas

Hoje em dia são tantas as normas disponíveis e exigidas pelo mercado que ficamos confusos com o âmbito e o objetivo de cada uma. Qual a melhor a utilizar, qual a mais eficaz, qual deveríamos utilizar para ter o máximo rendimento possível, uma maior proteção, maior segurança. Antes de mais é preciso saber o que é uma norma e quais as áreas que as mesmas cobrem.

Uma norma consiste num número determinado de documentos que resultam de um consenso, que são aprovados por um organismo de normalização que é reconhecido, que estabelecem regras, guias ou características de produtos ou serviços, e que são assentes em resultados consolidados, científicos, técnicos ou experimentais. Como referido anteriormente, as normas são aprovadas por um organismo reconhecido o que quer dizer que as empresas ou organizações que atendam às suas exigências possam receber um certificado de excelência quando auditadas. Em muitos casos, alguns clientes exigem que as companhias possuam determinadas certificações para efetuarem negócio com as mesmas de forma a garantirem que os serviços e os produtos estejam de acordo com as boas práticas internacionais, podendo ser de gestão, de segurança, de inovação ou de processo. Para as companhias e ou instituições serem certificadas, as mesmas passam por auditorias realizadas por entidades certificadoras, que fazem a verificação de todos os processos e conformidades. É de referir que estas auditorias tanto podem ser realizadas internamente como também externamente.

Como referido anteriormente, existem várias normas para diversas áreas. Segue alguns exemplos das áreas e o seu principal objetivo.

I. **A Norma de gestão de qualidade** permite que uma empresa/instituição trabalhe de forma mais eficiente reduzindo assim as falhas do produto/serviço;
II. **A Norma de gestão ambiental** permite a uma empresa/instituição a redução dos impactos ambientais e a tornar-se mais sustentável;
III. **A Norma de saúde e segurança** permite a redução dos acidentes no ambiente de trabalho;
IV. **A Norma de segurança de TI** permite a preservação das informações mais sensíveis em segurança;
V. **A Norma de construção** auxilia a construir uma casa;
VI. **Norma de gestão de energia** permite a redução do consumo de energia;
VII. **Norma de segurança de alimentos** evita que os alimentos sejam contaminados [16].

Alguns dos benefícios gerais das normas:

- Fazer com que as empresas, instituições, organizações cumpram a legislação europeia e nacional;
- Garantir a segurança dos produtos, equipamentos e sistemas;
- Assegurar a compatibilidade e a interoperabilidade;

- Promover um entendimento técnico comum;
- Diminuir os erros;
- Reduzir os custos…

Apenas a título de curiosidade, abaixo encontram-se algumas siglas que dizem respeito às normas:

ISO – Norma Internacional

IEC - Norma Internacional Eletrotécnica

EN – Norma Europeia

NP – Norma Portuguesa

DNP – Documento Normativo Português

ENV – Pré-Norma Europeia

2.2.1 Norma de segurança da informação

Fazer uma gestão da informação eficiente garante, em todas as empresas, organizações e ou instituições, benefícios que vão desde a proteção de dados estratégicos à obtenção de novos negócios ou projetos. Para que ambas possam usufruir de uma gestão adequada é necessário garantir que as políticas, os processos, hardwares e softwares supram as suas necessidades, considerando todos os riscos e as atividades das mesmas. Uma das formas de ter a certeza de que está a ser tudo feito de forma correta é seguir orientações de normas de segurança da informação, neste caso, que determinam os controlos, as regras e as diretrizes para a área em questão.

Existem algumas normas que regem a elaboração e a aplicação de um Sistema de Gestão de Segurança da Informação (SGSI), onde têm o objetivo de garantir a confidencialidade, a integridade e a disponibilidade da informação, fatores estes essenciais para um sistema corporativo seguro, embora todas as restantes normas da família 27000 sejam normas de segurança da informação [17].

- ✓ **ISO/IEC 27001**
- ✓ **ISO/IEC 27002**

2.2.2 Família ISO/IEC 27000

A família ISO/IEC27000 compreende normas de segurança da informação que foram publicadas pela Organização Internacional de Normalização (ISO) e pela Comissão Internacional de Eletrotécnica (IEC). Esta família fornece recomendações das melhores práticas em gestão de segurança da informação, dos riscos e controlos dentro do

contexto de um sistema de gestão de segurança da informação assim como a mesma surge como forma de definir alguns termos e definições para uma futura implementação de um SGSI. A mesma abrange mais do que apenas a privacidade, a confidencialidade e as questões técnicas de segurança [18].

A ISO/IEC27000 [19] é uma norma que serve de apoio às empresas, organizações e/ou entidades de quaisquer sectores, sejam eles públicos ou privados, de forma a entender os princípios, conceitos e fundamentos que permitem uma melhor gestão dos seus ativos de informação. Essencialmente estas normas permitem a que a empresa em causa seja incentivada a avaliar os seus riscos de segurança da informação, a implementar os controlos de segurança da informação apropriados e de acordo com as necessidades pretendidas, utilizando sempre as sugestões e orientações, sempre que pertinente. Tendo em conta que a segurança da informação é um sistema dinâmico, ou seja, em constante evolução, o conceito de sistema de gestão de segurança da informação incorpora as atividades de feedback e de melhoria contínua que permitem atender a mudanças das ameaças ou impactos de incidentes de segurança da informação. Ou seja, um SGSI fornece um modelo para o estabelecimento, implementação, operacionalização, monitorização, revisão, manutenção e melhoria da proteção dos ativos de informação com o propósito de alcançar os objetivos propostos por uma empresa com base numa avaliação correta e numa gestão dos riscos inerentes a uma empresa. Quanto à norma propriamente dita, a mesma tem a seguinte estrutura.

0. Introdução
1. Âmbito
2. Termos e Definições
3. Sistemas de Gestão de Segurança da Informação
   3.1. Introdução
   3.2. O que é um SGSI?
   3.3. Processo de abordagem
   3.4. O porquê de um SGSI ser importante
   3.5. Estabelecer, monitorizar, manter e melhorar o SGSI
   3.6. Fatores críticos de sucesso do SGSI
   3.7. Benefícios da família de normas SGSI
4. Família de normas SGSI
   4.1. Informação geral
   4.2. Descrição das normas – Visão geral e Terminologia
   4.3. Especificação das normas – Requisitos
   4.4. Descrição das normas – Diretrizes gerais
   4.5. Descrição das normas – Orientações específicas do setor

Anexo A (informativo) – Formas verbais para expressão de disposições

Anexo B (informativo) – Termos e termos de propriedade

Dentro da família ISO 27000 existe um variado leque de normas, como mostra a Figura 2, todas elas importantes para um SGSI. Embora algumas ainda estejam em

desenvolvimento e outras publicadas ainda estejam sujeitas a revisões periódicas, destacam-se as seguintes.

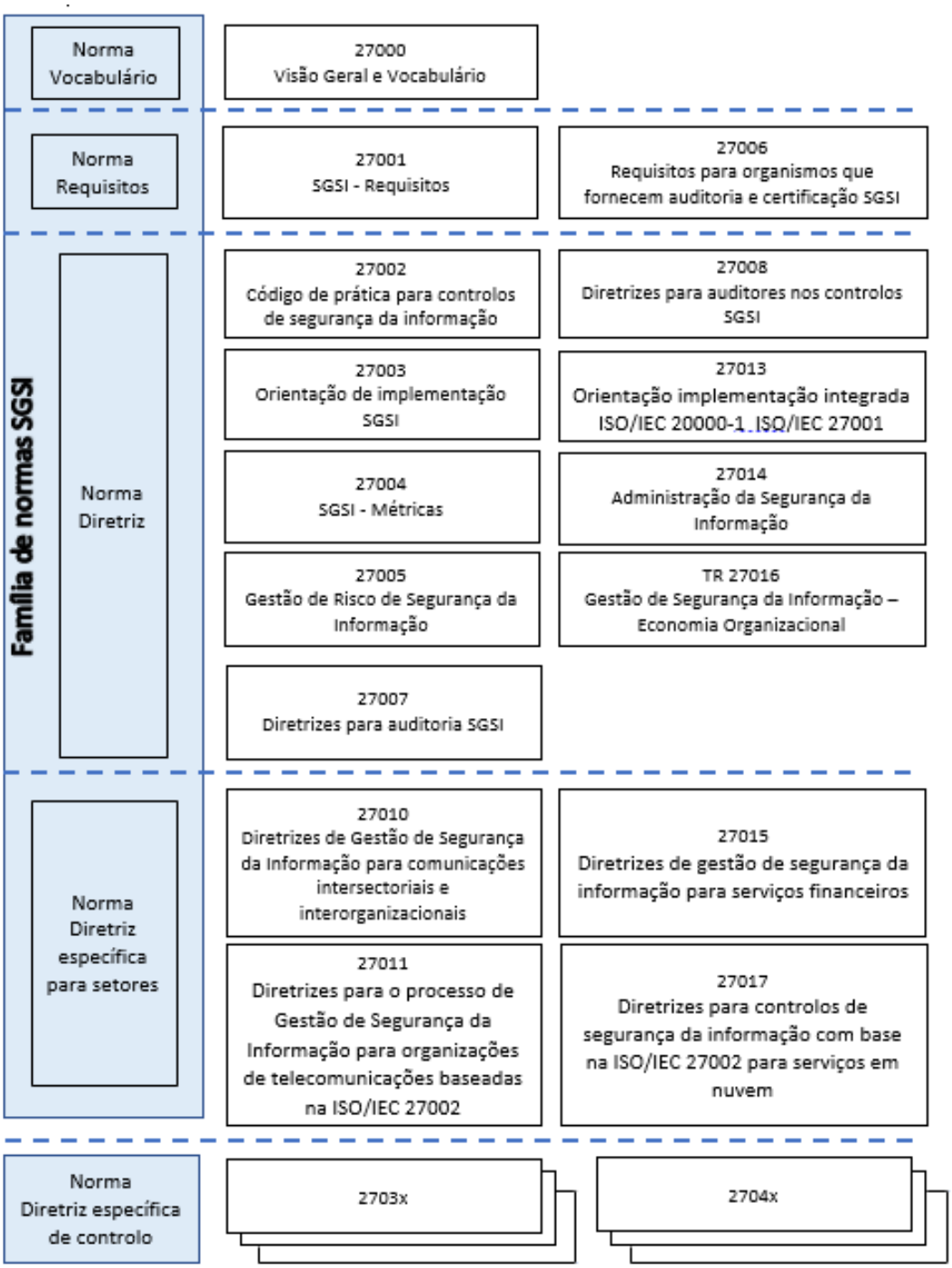


Figura 2 - Principais normas da Família 27000.

2.2.3 Norma ISO/IEC 27001

A ISO/IEC 27001 é uma das normas de segurança da informação que faz parte da família das normas ISO/IEC 27000, cuja última versão foi publicada no ano de 2013 e é uma especificação rigorosa e abrangente que tem como finalidade proteger e preservar as informações sob os princípios da confidencialidade, integridade e disponibilidade.

A norma é responsável por efetuar uma descrição de um sistema de gestão de segurança da informação genérico que, como referido anteriormente, é um sistema que engloba todos os tipos de práticas, procedimentos e instrumentos que são necessários para gerir dentro da empresa, organização ou instituição, um determinado tema. Visto o tema ser a segurança da informação, esta norma aborda os passos baseados em PDCA (Planear, Implementar, Monitorizar e Ajustar continuamente), fazendo com que o círculo gire continuamente. E para fazer com que este círculo gire continuamente é necessário recorrer às secções da norma, onde nessas secções encontramos um direcionamento de como planear, implementar, monitorizar e ajustar continuamente. Claro que tudo isto de uma forma completa mostrando quais são os requisitos e objetivos de controlo para a liderança, por exemplo, de forma a estruturar todas as etapas e em menores detalhes [5].

Abordando a mais recente versão da norma ISO/IEC 27001 – 2013 temos a seguinte estrutura que é apresentada na Figura 3.

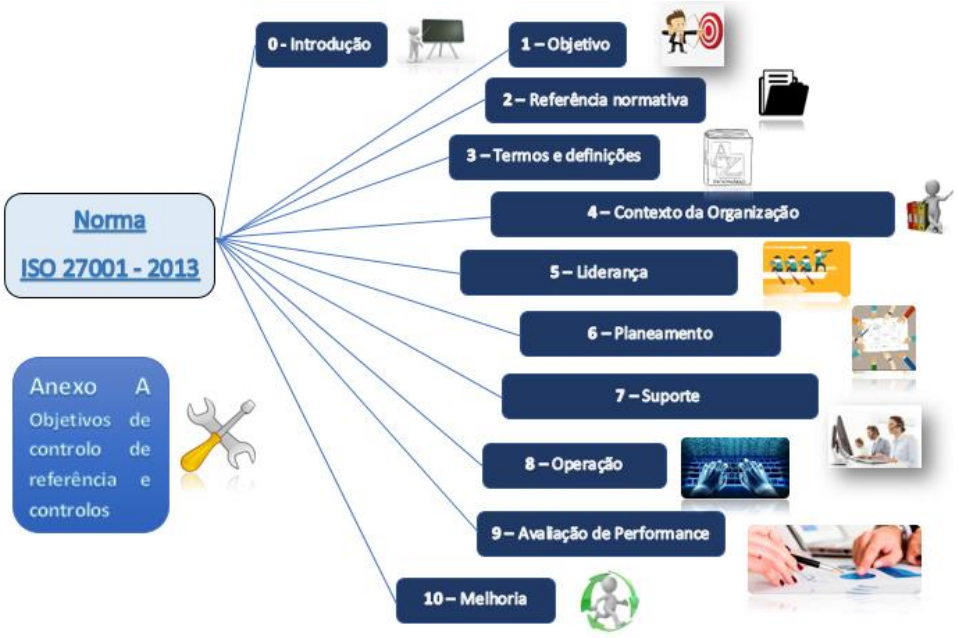


Figura 3 – Visualização geral da estrutura da norma ISO/IEC 27001 – 2013 [20].

Na "**Introdução"** encontra-se explicado o propósito da norma e a sua compatibilidade com outras normas de gestão. Na secção "**Objetivo**" é onde encontra-se a explicação da norma ser aplicável a qualquer tipo de organização. Quanto à secção "**Referência Normativa**" e "**Termos e Definições**" as mesmas referem-se à ISO 27000 como uma norma onde são dados os termos e definições.

No “**Contexto da Organização**” é a secção onde é necessário haver um entendimento da empresa e do seu contexto de forma a haver uma maior compreensão das necessidades e expectativas das partes interessadas, e determinar o âmbito do SGSI. Na secção “**Liderança**” é onde se abordam a liderança e o compromisso, as políticas e as funções organizacionais, responsabilidades e autoridades que a empresa tem que cumprir. Na secção “**Planeamento**” é onde se abordam as ações para abordar os riscos e oportunidades, a avaliação do risco de segurança da informação, o tratamento do mesmo e os objetivos da segurança da informação e o seu planeamento para os alcançar. Na secção “**Suporte**” é onde devem ser atribuídos recursos adequados e competentes, um grau de consciência aumentada e a documentação deve ser preparada e controlada. Na secção “**Operação**” é onde tem um maior detalhe sobre a avaliação e tratamento de riscos de informação, e onde tem de haver uma gestão de mudanças e documentação de coisas para que possam ser auditados pelos auditores de certificação. Quanto à secção “**Avaliação de Performance**” a mesma explica o que a empresa deve fazer para monitorizar, medir, analisar, avaliar, auditar e rever os controlos de segurança da informação, processos e sistemas de gestão de forma a melhorar sistematicamente as coisas quando necessário. Por fim, a secção “**Melhoria**” explica o que deve ser feito quando uma não-conformidade e uma ação corretiva ocorrer. Relativamente ao “**Anexo A**” é um anexo onde estão listados todos os controlos e objetivos de controlos. Este anexo é então constituído por 14 secções, várias categorias e 114 controlos [21].

Numa outra perspetiva, a Figura 4 ilustra as várias secções da norma numa estrutura global que permite observar o processo, o funcionamento e a aplicabilidade dos requisitos num sistema SGSI, onde é facilmente destacado o PDCA na estrutura da norma.

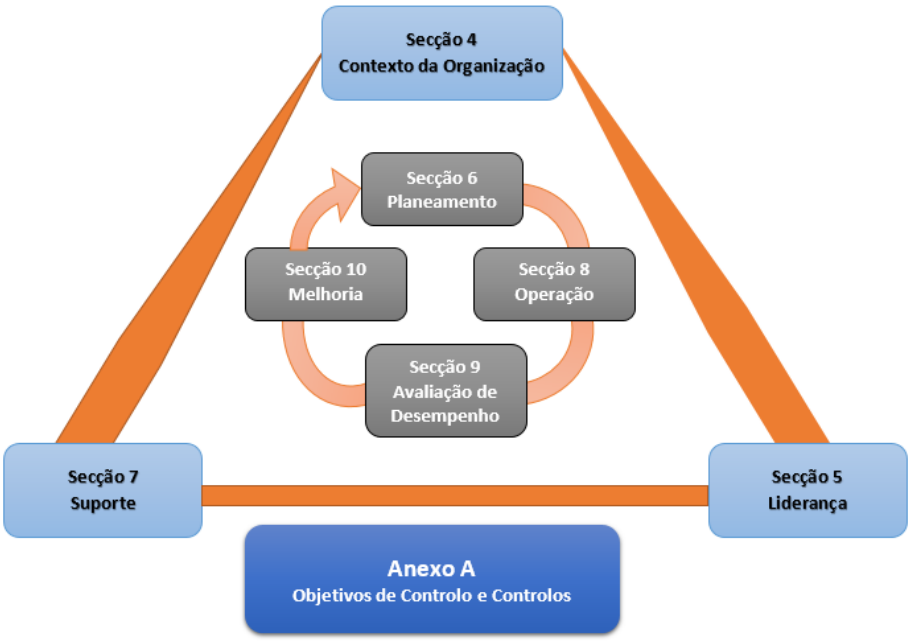


Figura 4 - Estrutura global da norma [22].

Abordando agora as duas componentes da norma, na primeira componente, referente às secções da mesma, encontram-se definidas as regras e os requisitos de cumprimento da mesma onde devem ser aplicáveis e não é aceitável a exclusão de quaisquer dos requisitos especificados nas secções 4 a 10, para uma organização que reivindica a sua conformidade face à norma. A Figura 5 ilustra esta mesma componente.

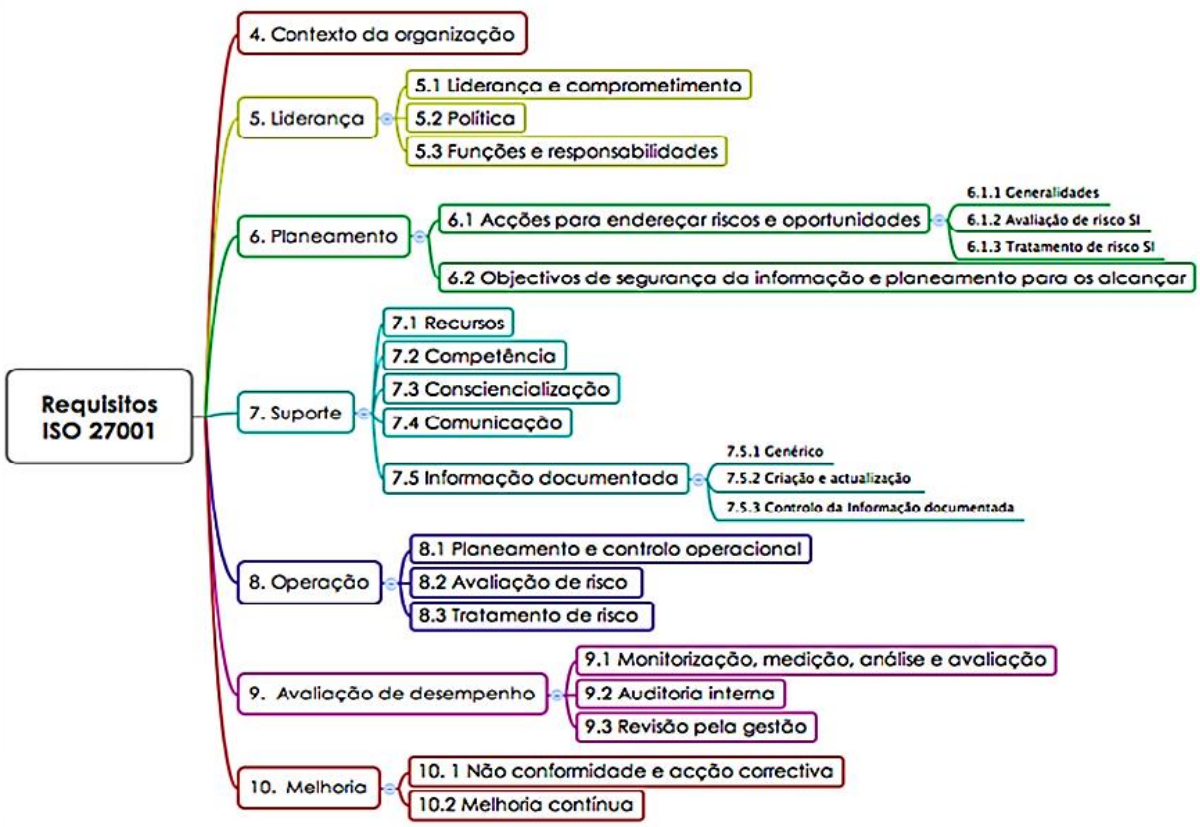


Figura 5 - Diagrama dos requisitos genéricos da norma ISO/IEC 27001 - 2013 [22].

Quanto à segunda componente da norma, o Anexo A, é onde se encontram especificados os objetivos de controlo e os controlos de referência, de A.5 a A.18, que de igual forma também se encontram alinhados com os listados na ISO/IEC 27002 – 2013, nas secções 5 a 18.

É de salientar que estes objetivos de controlo e controlos listados neste anexo, não são exaustivos, o que quer dizer que podem ser necessários objetivos de controlo adicionais, conforme a necessidade da empresa.

A Tabela 4 demonstra as várias secções, as correspondentes descrições do controlo de referência, quantas alíneas possuem (número de categorias) e quantos controlos contêm, sempre em cada secção.

Tabela 4 - Quadro demonstrativo das secções, descrições, categorias e controlos da norma [22].

Secção	Descrição do Controlo de Referência (Anexo A)	Nº Categorias	Nº Controlos
A.5	Políticas 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

Pegando num exemplo de uma secção, a **A.12**, que corresponde à **Segurança de Operações**, a mesma possui **sete categorias** (A.12.**1**; A.12.**2**; A.12.**3**; A.12.**4**; A.12.**5**; A.12.**6** e A.12.**7**) e em cada categoria temos um conjunto de controlos, por exemplo, a categoria A.12.1 é constituída por quatro controlos (A.12.1.**1**; A.12.1.**2**; A.12.1.**3**; A.12.1.**4**;).
Ou seja, cada secção tem um determinado número de categorias principais de segurança da informação, onde cada categoria principal contém: a) um objetivo de controlo que define o que deve ser alcançado; b) um ou mais controlos que podem ser aplicados de forma a alcançar o objetivo de controlo.

Agora para cada prática de cada secção da norma, onde agir? Quais os tipos de controlos, de práticas para, por exemplo, gestão de acesso? Quais são as diretrizes para fazer a política de segurança? As respostas a estas questões serão respondidas mais à frente, na norma ISO/IEC 27002.

Tendo em conta que a norma é responsável por definir os requisitos para um Sistema de Gestão de Segurança da Informação fazendo com que a empresa/organização adote um SGSI que permita mitigar os riscos de segurança atribuídos aos seus ativos e adequar as necessidades à área de negócio, é importante destacar os benefícios desta.

Os benefícios gerais passam pela redução do risco de responsabilidade pela não implementação ou determinação de políticas e procedimentos, redução de custos, oportunidade de identificar e corrigir os pontos fracos, confiança aos parceiros comerciais, aos clientes e às partes interessadas, melhor organização e sobretudo a conformidade com requisitos legais, etc.

Mas é óbvio que existem outros benefícios que demonstram a preocupação e a importância da escolha não só da norma como da sua certificação, que são eles:

I. Demonstração de compromisso da administração/executivos da empresa para com a segurança da informação, na medida em que uma das grandes preocupações hoje em dia é efetivamente a confiança no tratamento adequado da informação mais sensível da empresa, que por muitas vezes acaba por ser o seu maior ativo, quando falamos em organizações ou instituições.
II. Atribuição à empresa de ferramentas que demonstram o cumprimento do ou dos regulamentos no tratamento e circulação de dados pessoais.
III. Aumento da fiabilidade e da segurança da informação e dos sistemas, no que diz respeito aos três pilares da segurança da informação, a confidencialidade, disponibilidade e integridade.
IV. Confirmação da realização de investimentos mais eficientes e orientados ao risco.
V. Incrementação dos níveis de sensibilidade, participação e motivação dos colaboradores da empresa para com a segurança da informação.
VI. Identificação e endereçamento de forma continuada oportunidades para melhorias, tendo em conta que se trata de ser um processo com melhoria contínua.
VII. Aumento da confiança e satisfação não só dos clientes como também das entidades, parceiros, utentes e demais pessoas ligadas direta ou indiretamente à empresa, providenciando um elevado compromisso com a proteção da informação, demonstrando assim um maior conforto para quem interage com as entidades que processam e arquivam os dados pessoais.
VIII. Implementação dos controlos que são provenientes da norma e da análise de risco, que não só melhora o desempenho operacional das empresas como também potencia a realização de um número considerado de negócios e maior poder negocial [22].

Quanto à certificação, a ISO/IEC 27001 é a norma para a qual é possível submeter uma empresa, dizendo que está certificada em gestão de segurança da informação conforme a norma. Uma empresa certificada só o é se atender aos requisitos da norma e se a conclusão da auditoria for bem-sucedida.

Normalmente quando uma empresa ou organização pretende ser certificada, a mesma já possui todo o hardware e software instalado, mas apenas está utilizando de forma insegura os mesmos. Desta forma a implementação desta norma passa por definir as regras organizacionais (políticas de segurança) que são necessárias de modo a prevenir falhas de segurança. Uma vez que esta implementação irá requerer a gestão de várias políticas, procedimentos, funcionários, etc… a mesma descreve como enquadrar todos estes elementos de forma coerente no sistema de gestão de segurança da informação.

A gestão de segurança da informação não é só estar atento à segurança TI (Antivírus, Firewalls, etc…), é preciso ter em conta a gestão de processos, os recursos humanos, a proteção física, ambiental, a proteção legal, etc…

Para implementar a norma ISO/IEC 27001 numa empresa/organização é necessário:

1) Obter o apoio/autorização dos diretores/responsáveis pela empresa/organização;
2) Definir o âmbito do SGSI;
3) Fazer um inventário de ativos;
4) Avaliar ativos (processo que foi acrescentado e que será abordado mais à frente no capítulo 4);
5) Identificar os riscos (constituido pela identificação das ameaças e das vulnerabilidades);
6) Analisar os riscos;
7) Avaliar os riscos;
8) Preparar o plano de tratamento de risco;
9) Preparar a declaração de aplicabilidade;
10) Desenvolver o programa de implementação do SGSI;
11) Implementação do programa SGSI;
12) Sistema de Gestão de Segurança da Informação – demonstração;
13) Realizar todas as operações diárias prescritas pela documentação do SGSI;
14) Realizar auditoria interna;
15) Rever a conformidade;
16) Aplicar medidas corretivas;
17) Realizar pré-avaliação de certificação;
18) Realizar auditoria de certificação;
19) Projeto é dado como finalizado;
20) Operação de rotina do SGSI;
21) Realizar auditoria anual de vigilância.

A Figura 6 ilustra todos os passos (processos), abordados anteriormente, a implementar para a obtenção da certificação pela norma ISO/IEC 27001.

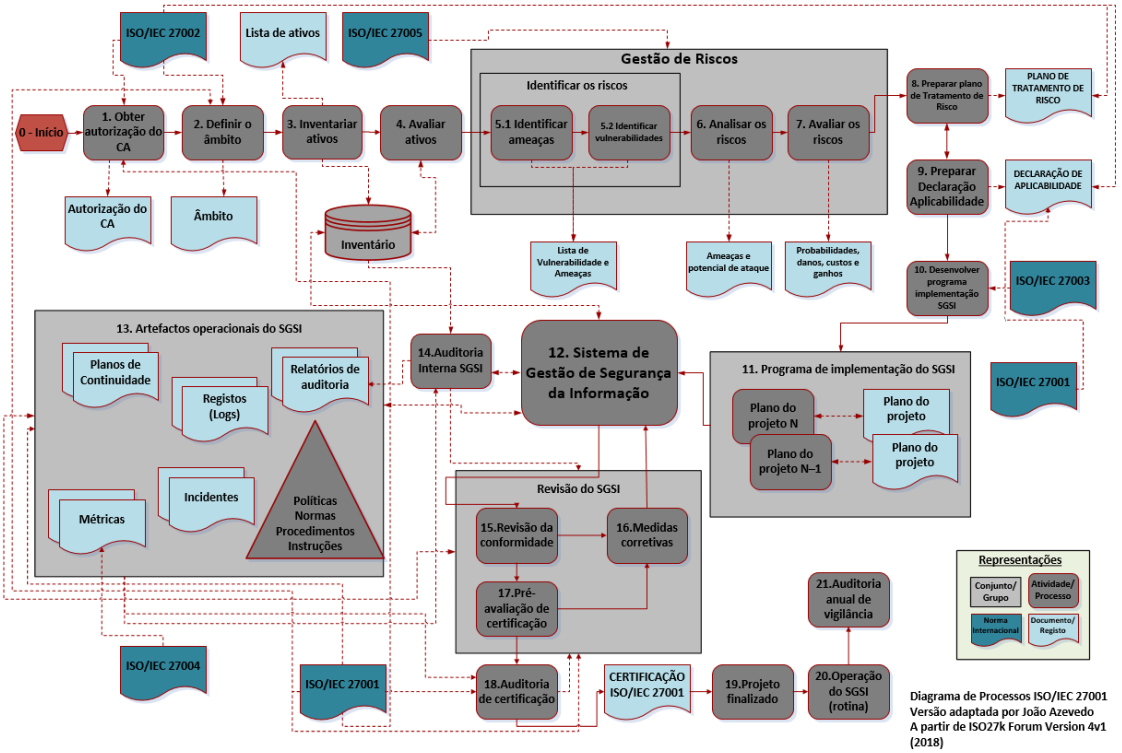


Figura 6 - Diagrama de Processos, adaptado de ISO27k Forum, versão 4.1, 2018 [23].

Este diagrama proporciona todos os requisitos para estabelecer, implementar, manter e melhorar de forma contínua um sistema de gestão de segurança da informação. O mesmo pode ser visto, com melhor nitidez, no Anexo A – Diagrama de processos de um SGSI (ISO/IEC 27001).

2.2.4 Norma ISO/IEC 27002

Com a rápida expansão da TI aliada à constante preocupação em garantir a integridade das informações, na década de 90 surgiram normas capazes de garantir a segurança da informação. Não muito mais tarde, esta expansão, originou um enorme interesse internacional nessas normas de segurança da informação que permitiu a criação da norma ISO 17799. Ora a ISO/IEC 17799 foi atualizada para ISO/IEC 27002 em julho de 2007, mas a sua versão original, foi publicada em 2000, que por sua vez era uma cópia fiel da norma britânica BS 7799-:1999 [24].

A norma ISO/IEC 27002 é uma norma internacional que estabelece um código de boas práticas com um conjunto completo de controlos que auxiliam a implementação do SGSI na empresa. Código de boas práticas quer dizer que é baseado em boas práticas do mercado, ou seja, boas práticas que eram utilizadas por diversas pessoas, entidades ou até organizações como a ISO que chegaram a um certo ponto e juntaram-se para definir uma única lista de boas práticas em que fosse possível todos seguirem a mesma para a mesma área até com objetivos semelhantes, resultante da colaboração e conhecimento de todo esse meio envolvente, profissional e entendido na matéria [25].

A mesma baseia-se essencialmente na norma 27001 (que especifica 114 controlos que podem ser utilizados para reduzir os riscos de segurança) e disponibiliza detalhes sobre como implementar ou estabelecer estes controlos, onde estes devem ser escolhidos com base numa avaliação de riscos dos ativos relevantes da empresa. Ou seja, é recomendável que a ISO/IEC 27002 seja utilizada em conjunto com a ISO/IEC 27001 pois os controlos da norma ISO/IEC 27002 auxiliam a empresa a alcançar os requisitos da norma ISO/IEC 27001, tendo em conta que a empresa pretende ser certificada quer seja numa ou noutra norma [26].

Tendo em atenção a secção quatro da norma ISO/IEC 27002, a mesma explica que toda a norma, especificamente, está distribuída em objetivos de controlo, controlos e diretrizes. Os controlos são todo o tipo de medidas, ações, que podem incluir ações de monitorização, ações de acompanhamento, etc… E esta norma vai descrever os diversos controlos genéricos que poderão ser utilizados para poder adaptar à empresa. Só que não basta ter os controlos para termos um guia, por isso é que a norma contém também um pouco mais que isso. Contém algumas diretrizes, que estão sempre abaixo dos controlos da norma, para explicar um pouco mais como é que se leva para a prática. E por fim os objetivos de controlo basicamente são responsáveis por descrever qual o objetivo de a empresa estar a seguir todos os controlos específicos. Estes objetivos de controlos são defendidos nas seções da norma e aparecem sempre abaixo da secção/domínio da norma, como mostra a Figura 7.

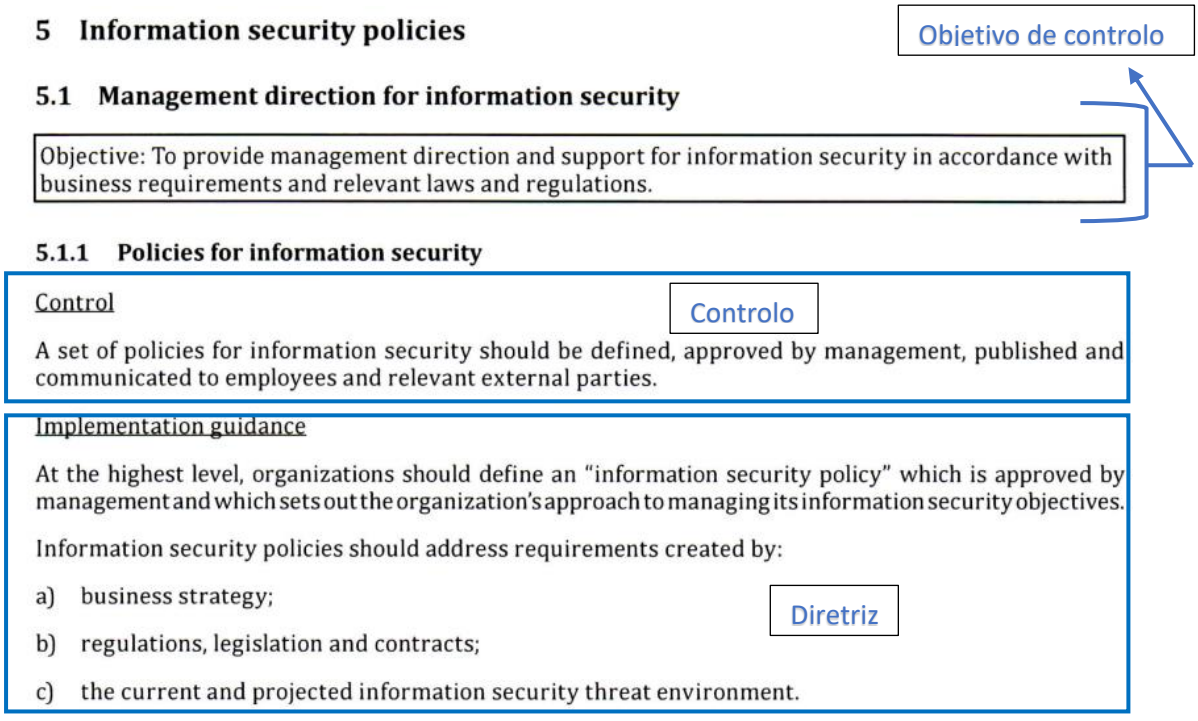


Figura 7 – Excerto (foto) da norma ISO/IEC 27002:2013, retirado a parte da secção "Política de segurança da informação" de forma a demonstrar objetivo de controlo, controlos e diretriz [6].

Quanto às duas versões (2005 e 2013) que existem da norma, não houve uma grande revolução, mas sim algumas alterações que permitiram atualizar não só a norma como também abranger um maior número de secções e de controlos de forma a englobar

mais áreas e de facto ser mais fácil a aplicação da norma. A Figura 8 mostra quais as diferenças e semelhanças entre elas de forma superficial.

Secção/Domínio	ISO/IEC 27002:2005	Secção/Domínio	ISO/IEC 27002:2013
5	Política de Segurança da Informação	5	Política de Segurança da Informação
6	Organização da Segurança da Informação	6	Organização da Segurança da Informação
7	Gestão de Ativos	7	Gestão de Ativos
8	Segurança de Recursos Humanos	8	Segurança de Recursos Humanos
9	Segurança Física e do Ambiente	9	Controlo de Acesso
10	Segurança das Operações e Comunicações	10	Criptografia
11	Controlo de Acesso	11	Segurança Física e do Ambiente
12	Aquisição, Desenvolvimento e Manutenção de S.I.	12	Segurança das Operações
13	Gestão de Incidentes de Segurança da Informação	13	Segurança das Comunicações
14	Gestão da Continuidade do Negócio	14	Aquisição, Desenvolvimento e Manutenção de S.I.
15	Conformidade	15	Relacionamento com o Fornecedor
		16	Gestão de Incidentes de Segurança da Informação
		17	Aspetos da Segurança da informação na GCN*
		18	Conformidade

*GCN – Gestão de Continuidade do Negócio

Figura 8 - ISO/IEC 27002 2005 vs ISO/IEC 27002 2013 [27].

Relativamente à estrutura da norma ISO/IEC 27002:2013 a Figura 9 ilustra as secções constituintes da norma.

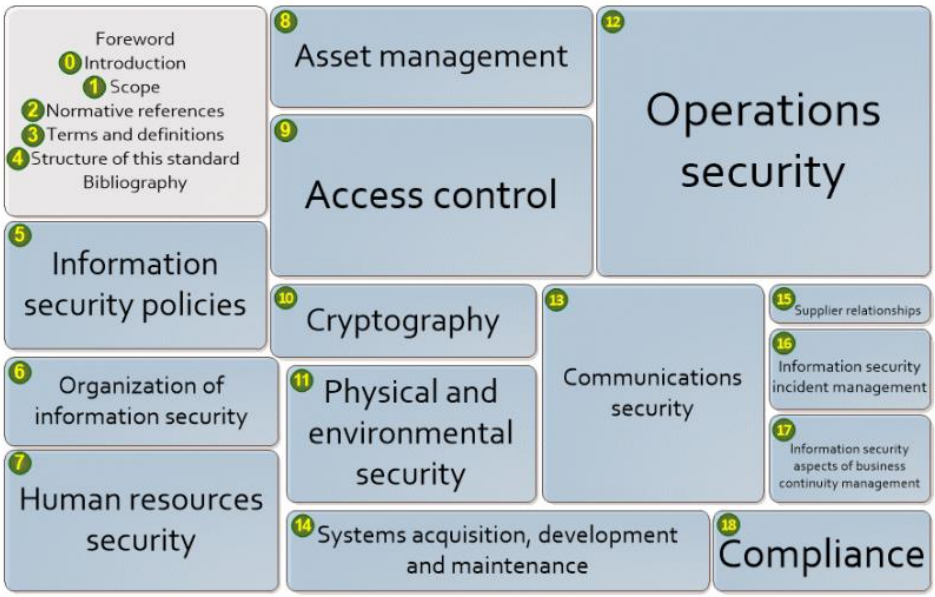


Figura 9 - Estrutura da norma ISO 27002:2013 - Secções [28].

0. Introdução – Explica o propósito da norma e a sua compatibilidade com outras normas de gestão;

1. Objetivo – Explica que a norma é aplicável a qualquer tipo de organização;

2. Referência Normativa – Refere-se à ISO 27000 como uma norma onde são dados os termos e definições;

3. Termos e Definições – Refere-se à ISO 27000;

4. Estrutura da Norma – Indica que a norma contém as cláusulas de controlo de segurança (14), categorias principais de segurança (35) e o número de controlos (114). Ou seja, cada cláusula, que define os controlos de segurança, contém uma ou mais categorias principais de segurança. Cada categoria principal de segurança contém um objeto de controlo declarando o que deve ser alcançado; E um ou mais controlos que podem ser aplicados para atingir o objetivo do controlo.

5. Política de Segurança da Informação – Refere como deve ser criado o documento sobre a política de segurança da informação, onde deve conter os conceitos de segurança da informação, uma estrutura para estabelecer os objetivos e as formas de controlo, o comprometimento da direção com a política, etc…;

6. Organização da Segurança da Informação – Refere que para uma implementação de segurança da informação numa empresa/organização é necessário estabelecer uma estrutura para geri-la da maneira mais adequada. As atividades de segurança da informação devem ser coordenadas por representantes da empresa/organização que devem ter responsabilidades bem definidas e proteger as informações de caráter sigiloso;

7. Segurança de Recursos Humanos – Refere que antes da contratação de qualquer funcionário ou fornecedor é importante que esse seja devidamente analisado, principalmente se o mesmo tiver um cargo que lide com informações sigilosas. Esta secção tem como objetivo a mitigação do risco de roubo, fraude ou mau uso dos recursos;

8. Gestão de Ativos – Aborda a definição de ativo, segundo a norma, e refere que os mesmos devem ser identificados e classificados de forma que um inventário possa ser estruturado e posteriormente mantido;

9. Controlo de Acesso – Refere que é importante limitar o acesso às informações e ao processamento das mesmas impedindo assim o acesso a qualquer utilizador, funcionário ou terceiro que não tenha autorização para tal. E que em caso de autorização de acesso, os mesmos são responsabilizados pelos seus atos e responsabilizados pela proteção das suas informações de autenticação;

10. Criptografia – Refere que é relevante garantir a utilização adequada e eficaz da criptografia de forma a proteger a confidencialidade, autenticidade e a integridade das informações bem como desenvolver e implementar uma política sobre a proteção de utilização de controlos criptográficos para a proteção de informação e tempo de vida das chaves criptográficas;

11. Segurança Física e do Ambiente – Refere que todos os equipamentos e instalações de processamento de informação críticas ou sensíveis devem ser mantidas em locais seguros, com níveis e controlos de acesso apropriados com proteção contra ameaças físicas e ambientais;

12. Segurança das Operações – É necessário a definição dos procedimentos e responsabilidades pela gestão e operação de todos os recursos de processamento das informações. Está incluído a gestão de serviços de terceiros, o planeamento dos recursos dos sistemas minimizando o risco de falhas e a criação de procedimentos para a geração de cópias de segurança (backups);

13. Segurança das Comunicações – Refere-se à forma como assegurar a proteção da informação nas redes e nas suas instalações de processamento de informações;

14. Aquisição, Desenvolvimento e Manutenção de Sistemas – Nesta secção os requisitos de segurança dos sistemas de informação devem ser identificados e acordados antes do seu desenvolvimento e da sua implementação para que possam ser protegidos visando a manutenção da sua confidencialidade, autenticidade e integridade por meios criptográficos;

15. Relacionamento com Fornecedores – O objetivo nesta secção passa por garantir a proteção dos ativos da empresa/organização que são acessíveis por fornecedores e manter um nível acordado de segurança da informação e prestação de serviços de acordo com os acordos de fornecedores;

16. Gestão de Incidentes de Segurança da Informação – Nesta secção devem ser estabelecidos procedimentos formais de registo e escalonamento, os funcionários, os fornecedores e terceiros devem estar conscientes dos procedimentos para notificação dos eventos de segurança da informação de forma a assegurar que eles sejam comunicados o mais rápido possível e corrigidos no mais curto espaço de tempo;

17. Gestão da Continuidade do Negócio – Nesta secção devem ser desenvolvidos e implementados os planos de continuidade do negócio de forma a impedir a interrupção das atividades do mesmo e assegurando que as operações essenciais sejam recuperadas o mais rápido possível;

18. Conformidade – Tem como objetivo evitar violações obrigacionais, por estatuto, regulamentares ou obrigações contratuais e de quaisquer requisitos de segurança da informação.

Seguir os princípios da certificação da ISO/IEC 27002 é um passo relevante, para garantir a segurança da informação nas empresas. Neste sentido é deveras importante as empresas, organizações e instituições possuírem profissionais certificados nas suas equipas de segurança, de forma a auxiliar no processo de implementação das boas práticas relacionadas com a norma, assim como a obtenção da certificação ISO/IEC 27001 [29].

2.2.5 Norma ISO/IEC 27005

Os riscos de segurança da informação representam uma verdadeira e considerável ameaça para as empresas devido à possibilidade de perdas ou danos financeiros, perda

de serviços de rede essenciais e/ou perda de reputação. A gestão de riscos é um dos principais elementos-chave na prevenção de fraudes online, roubos de identidade, perda de dados pessoais e muitos outros incidentes. Desta forma, as organizações, sem uma sólida estrutura de gestão de riscos, expõem-se a muitos tipos de ameaças cibernéticas.

A norma ISO/IEC 27005 – Tecnologia de Informação – Técnicas de Segurança – Gestão de Risco de Segurança da Informação, como o próprio nome indica, fornece as diretrizes para a gestão de riscos de segurança da informação. A norma suporta os conceitos gerais especificados na ISO/IEC 27001 e auxilia a implementação satisfatória da segurança da informação, baseada numa abordagem de gestão de risco. Para além de poder ser utilizada por todo o tipo de empresas, organizações e ou instituições (por exemplo, entidades governamentais, empresas comerciais, instituições universitárias, etc…), que tenham por objetivo gerir riscos que possam comprometer a sua segurança da informação, é fundamental ter o conhecimento dos conceitos, modelos, processos e terminologias descritos na ISO/IEC 27001 e ISO/IEC 27002, para uma compreensão completa da ISO/IEC 27005.

Este tipo de gestão de risco consiste essencialmente num processo contínuo de observação do contexto, de identificação, de avaliação e de tratamento dos riscos.

Quanto à estrutura da norma, esta encontra-se dividida em 12 secções, onde contêm as informações do processo e das atividades necessárias para a sua execução, e em anexos, onde contêm informações adicionais e alguns exemplos de aplicação e/ou implementação. Da primeira à quarta secção encontram-se as referências e a estrutura da norma, a quinta e a sexta secções apresentam a visão geral do processo de gestão de riscos e as restantes secções tratam especificamente do processo de gestão de riscos.

A estrutura da norma é a seguinte:

0. Introdução – Explica o propósito da norma e a sua compatibilidade com outras normas de gestão;

1. Objetivo – Explica que a norma é aplicável a qualquer tipo de organização;

2. Referência Normativa – Refere-se à ISO 27000 como uma norma onde são dados os termos e definições;

3. Termos e Definições – Refere-se à ISO 27000 e onde constam os termos e definições referentes à norma;

4. Estrutura da Norma – Indica que a norma contém a descrição do processo de gestão de riscos de segurança da informação e das suas atividades, que contém da 7ª secção à 12ª, todas as atividades de gestão de risco e que nos anexos encontram-se as informações adicionais para essas mesmas atividades de gestão de risco.

5. Contextualização – Indicam quais os contributos do cumprimento dos processos para as organizações.

6. Visão geral do processo de gestão de riscos de segurança da informação – Indica a visão geral de alto nível do processo de gestão de riscos, onde apresenta esquemas de forma a demonstrar como a norma se aplica ao processo de gestão de riscos.

7. Definição do contexto – Fornece as considerações gerais, os critérios básicos, os objetivos e limites e também os papéis e responsabilidades que a organização tem que ter em conta para a definição do contexto.

8. Processo de avaliação de riscos de segurança da informação – Faz numa primeira fase a descrição geral do processo e posteriormente apresenta e descreve as atividades do processo de avaliação de riscos (identificação dos riscos; análise de riscos; avaliação de riscos).

9. Tratamento do risco de segurança da informação – Faz numa primeira fase a descrição geral do processo, apresentando a atividade de tratamento do risco e depois especifica cada opção de tratamento do risco (modificação do risco; retenção do risco; ação de evitar o risco; partilha do risco;)

10. Aceitação do risco de segurança da informação – Fornece as diretrizes para a implementação da aceitação do risco.

11. Comunicação e consulta do risco de segurança da informação – Fornece as várias razões bem como os benefícios da perceção do risco.

12. Monitorização e análise crítica de riscos de segurança da informação – Refere a importância da monitorização contínua de forma a detetar as várias mudanças que ocorrem nas diversas fases de vida das organizações e indica quais os elementos que devem ser monitorizados continuamente.

Anexos (A, B, C, D, E, F e G) Definição do âmbito e dos limites do processo de gestão de risco de segurança da informação, Identificação e valorização dos ativos e avaliação do impacto, Exemplos de ameaças comuns, Vulnerabilidades e métodos de avaliação de vulnerabilidades, Abordagens para o processo de avaliação de riscos de segurança da informação, Restrições para a modificação do risco e Restrições para a modificação do risco – Resumidamente, ambos os anexos fornecem vários exemplos e os vários passos para completar as atividades.

O processo de gestão de riscos de segurança da informação, da norma ISO/IEC 27005:2011, como mostra a Figura 10, consiste, essencialmente, em:

- **Estabelecimento do contexto (secção 7)**: descrição de como definir o contexto da organização e como estabelecer os critérios de aceitação do risco residual;
- **Identificação de riscos (secção 8)**: determinar quais são os acontecimentos que possam causar perda de confidencialidade, integridade e disponibilidade;
- **Análise de riscos (secção 8)**: descreve as metodologias de forma a dar a escolher ao gestor qual a melhor opção para efetuar a análise segundo a probabilidade e o impacto;

- **Avaliação de risco (secção 8)**: indica os níveis de risco a que uma organização está exposta, através de escalas e permite definir a prioridade de intervenção e o prazo adequado para a realização da intervenção;
- **Tratamento de riscos (secção 9)**: estabelece quatro opções para o tratamento do risco (modificar, aceitar, evitar e partilhar o risco) e permite a elaboração de um plano de tratamento do risco.

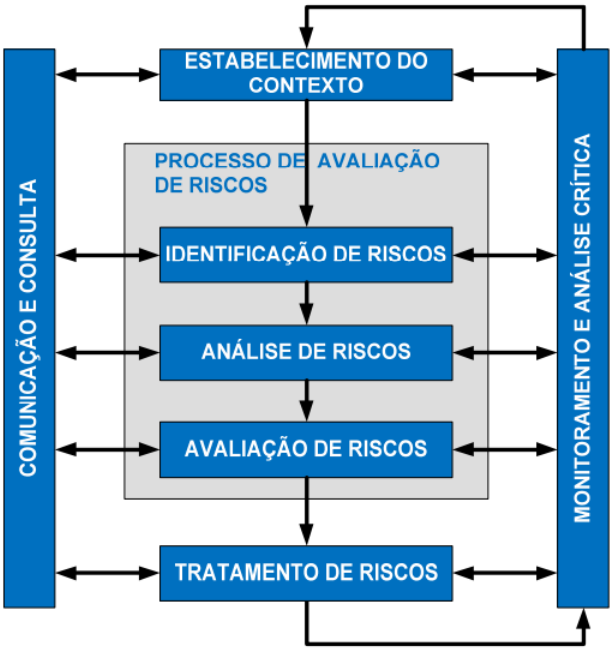


Figura 10 - Processo de Gestão do Risco da norma ISO/IEC 27005:2011 [8].

No entanto, a norma não fornece nenhuma metodologia específica, mas sim uma abordagem genérica. Cabe a cada empresa, organização ou instituição definir a sua abordagem, dependendo, por exemplo, do âmbito do SGSI, com base no contexto da gestão de riscos ou do sector industrial.

2.3 Outras normas relacionadas

Após alguma pesquisa sobre as normas, já identificadas previamente, a ISO/IEC 27001 e a ISO/IEC 27002, tornou-se evidente que para a elaboração de um SGSI 100% funcional requer sempre algo a mais, requer principalmente o envolvimento de mais normas pois a ISO/IEC 27001, por si só, é limitada. Desta forma, e apenas por terem feito parte da investigação realizada ao longo do trabalho, por terem uma relação próxima à norma ISO/IEC 27001 e por também terem a importância que têm, optou-se por mencioná-las no estado da arte, ainda que, de forma muito breve.

A norma **ISO/IEC 27003 – Tecnologia da informação – Técnicas de Segurança - Orientação de implementação de um SGSI** tem como objetivo providenciar um conjunto de diretrizes para a implementação de Sistemas de Gestão de Segurança da

Informação, numa empresa, organização e ou instituição, baseada na norma ISO/IEC 27001. Esta norma contém informações de como fazer uso do modelo "Plan-do-Check-Act" e também dos seus requisitos e as suas diferentes fases. De uma forma geral, através desta norma, uma organização é capaz de desenvolver um processo para a gestão da segurança da informação, fornecendo às partes interessadas uma garantia de que os riscos, aos ativos de informação, são continuamente mantidos dentro dos limites de segurança conforme definido pela empresa/organização [7].

A norma **ISO/IEC 27004 – Tecnologia da Informação – Técnicas de Segurança – Gestão de Segurança da Informação – Monitorização, medição, análise e avaliação**, fornece diretrizes destinadas a auxiliar as organizações na avaliação do desempenho em segurança da informação e na eficácia de um SGSI, a fim de atender aos requisitos da secção 9.1 da norma ISO/IEC 27001. Assim sendo, a norma estabelece:

- Monitorização e medição do desempenho da segurança da informação;
- Acompanhamento e medição da eficácia de um SGSI, incluindo os seus processos e controlos;
- Análise e avaliação dos resultados da monotorização e medição.

É uma norma que incide sobre as métricas e relatórios de um SGSI pois é responsável pela especificação de métricas e técnicas de medição aplicáveis de forma a determinar a eficácia do SGSI, os objetivos de controlo e todos os controlos utilizados para implementação e gestão da segurança da informação. As métricas são utilizadas para medir os componentes da fase "Check" e "Act" do ciclo Plan-Do-Check-Act [30].

Gerir riscos deve ser uma parte integrante de qualquer empresa, organização e/ou instituição. Embora não faça parte da família ISO 27000, a **ISO 31000 – Gestão de Riscos – Diretrizes** é uma norma de gestão de riscos e ao fornecer diretivas e princípios abrangentes, auxilia as organizações nas suas análises e avaliações de riscos. É uma norma que não tem como objetivo a certificação, mas, as recomendações de melhores práticas desta norma foram desenvolvidas para melhorar as técnicas de gestão e garantir a segurança no local de trabalho em qualquer situação. Com esta norma é possível conhecer os riscos e saber quais as consequências da não eliminação ou mitigação dos riscos e prevenir futuros eventos. A norma, relativamente ao processo de avaliação de riscos, fornece a estrutura para identificar e analisar o risco para o conhecimento das consequências e das suas probabilidades, para uma tomada de decisão especifica caso seja necessário [31].

A norma **ISO 9001 – Sistema de Gestão de Qualidade – Requisitos** é responsável por estabelecer os critérios para um sistema de gestão da qualidade e é a única norma na família (9000) que pode ser certificada. Apesar de gestão de qualidade não ter muito a ver com gestão de segurança da informação, cerca de 25% dos requisitos da norma ISO/IEC 27001 fazem parte da norma ISO 9001, ou seja, uma organização que tenha implementada a norma ISO 9001, poderá mais facilmente implementar a norma ISO/IEC 27001 [32].

2.4 Certificação

A Certificação é uma ferramenta útil e que permite garantir uma maior credibilidade na medida em que demonstra que o produto ou o serviço atende às expetativas do cliente da empresa ou da organização em causa. Esta certificação em algumas empresas ou instituições pode ser mesmo uma exigência legal ou contratual concedendo assim uma maior fiabilidade ao cliente de que a empresa garante segurança.

Tendo em conta que quem faz as certificações é um organismo de certificação externo, e não a ISO, é importante então saber como é que a empresa ou a organização pode escolher o organismo para obter a certificação que pretende.

Ao escolher um organismo de certificação, a empresa em causa deve:

- Avaliar os vários organismos de certificação;

- Verificar se o organismo de certificação utiliza o correspondente padrão CASCO (Committee on conformity assessment) que quer dizer Comissão de avaliação da conformidade;

- Verificar se está acreditado [33].

A próxima lista indica as etapas que uma empresa de certificação normalmente segue.

1. Entrar em contacto com o cliente (discussão de qual a norma a implementar…);
2. Elaborar uma proposta (informação do detalhe da proposta, o custo e o tempo necessário para a auditoria formal ser feita);
3. Dar a conhecer à equipa de auditoria os objetivos do cliente;
4. Efetuar uma pré-auditoria onde permita identificar eventuais omissões ou fraquezas da empresa ou organização;
5. É realizada a auditoria, dependendo da norma escolhida e é feita a aplicação em várias fases;
6. Certificar a empresa ou organização, emitindo o certificado;
7. Nomeação de um gestor de forma a este poder realizar ao longo de um determinado tempo, constantes auditorias de forma a atualizar a segurança da empresa (conformidade) [34].

2.5 Auditoria de Segurança

Hoje em dia, não se torna suficientemente seguro apenas cumprir com as normas de segurança impostas pela própria empresa. A mesma tem que provar mesmo que estão a ser cumpridas as normas de segurança através de auditorias regulares que produzem os relatórios com as melhores práticas de segurança. O que quer dizer que é importante compreender que uma auditoria de segurança é um processo contínuo que deve conceder uma melhoria contínua para qualquer empresa.

A auditoria de segurança é um processo específico e que é destinado a avaliar os riscos de segurança que uma Organização/Empresa/Instituição enfrenta, avaliar o controlo ou as contramedidas adotadas pela empresa de forma a mitigar esses riscos. Ou seja, uma auditoria de segurança deve determinar o nível de auditoria apropriado para o ambiente de determinada empresa. Deve identificar os ataques (com ou sem êxito) que constituem uma ameaça para a rede da empresa, bem como os ataques contra os recursos que tenham sido identificados como valiosos na avaliação de riscos. E também avaliar a administração do sistema, a consciência dos funcionários, os controlos de gestão e a conformidade com as normas de segurança. Esta é uma ferramenta valiosa para dar uma visão geral precisa ao administrador [35].

Efetuar uma auditoria é tipicamente um processo humano que é gerido por uma equipa de "auditores" que possuem elevados conhecimentos técnicos e específicos na área de tecnologia de informação.

Estas equipas são então encarregues de entrevistar todo o pessoal interveniente na empresa, de conduzir avaliações de vulnerabilidades, políticas de segurança existentes, e de analisarem os sistemas de tecnologias de informação abrangidos pelo âmbito da auditoria. Na maioria dos casos, uma equipa depende fortemente de ferramentas de tecnologia para realizar a auditoria.

De seguida encontram-se alguns exemplos de questões a que normalmente uma auditoria de segurança deve responder:

- Os Logs de acesso existem (para ver quem acede aos dados)?

- Os computadores pessoais são regularmente verificados quanto ao malware?

- Quem tem acesso aos ficheiros de backup?

- A rede tem listas de controlo de acesso?

- Quão difíceis são as passwords?

Devido em alguns casos as políticas de segurança tornarem-se obsoletas, dado ao exponencial aparecimento de novas tecnologias, uma auditoria não só deve avaliar o cumprimento das políticas de segurança, mas também deve avaliar a própria natureza, a qualidade e saber controlá-las. É muito importante realçar que as auditorias de segurança fazem parte de um processo contínuo da definição e da manutenção eficazes das políticas de segurança [36].

Alguns dos principais benefícios de uma auditoria de segurança são a possibilidade de detetar falhas de segurança graves, detetar as falhas de segurança não graves que podem ser melhoradas e a indicação de quais as medidas corretivas de forma a melhorar a segurança.

2.6 Avaliação quantitativa e qualitativa

A **avaliação quantitativa** é um método que é utilizado quando existem dados que são confiáveis de eventos ocorridos, quando a probabilidade pode ser medida em valores numéricos ou quando se pode calcular o valor de uma consequência gerada pelo risco. É uma avaliação que traz números para a equação, com análises baseadas na probabilidade de manifestação de ameaças específicas e escalas de medição pré-determinadas, utilizadas para estabelecer os riscos ou as perdas associadas a essas ameaças, onde são necessários dados mensuráveis e objetivos para determinar o valor de cada ativo da empresa e para calcular probabilidades e valores de risco [37]. Essencialmente recorre à utilização de dois elementos fundamentais, a probabilidade de um evento ocorrer e a perda associada à ocorrência do evento, fazendo uso de uma figura produzida à custa destes elementos, denominada por "Expectativa Anual de Perda" (ALE – Annual Loss Expectancy) ou "Custo Anual Estimado" (EAC – Estimated Annual Cost). Esta figura é calculada para cada evento, multiplicando-se a perda potencial associada ao mesmo pela probabilidade de ocorrer, permitindo, posteriormente, ordenar os eventos por ordem de grandeza de risco e tomar as decisões baseadas nessa lista [1]**.** Como objetivo desta avaliação, destaca-se a capacidade de associação de uma quantia financeira específica a cada risco que é identificado, representando a perda potencial para a empresa em caso desse mesmo risco existir realmente. Em caso de ocorrência de um ataque ou violação de dados, permite à empresa o poder de estabelecer facilmente o impacto financeiro do incidente [37].

No que toca a desvantagens, prende-se essencialmente com a ausência de realidade e de objetividade dos dados. Porque a probabilidade de um evento ocorrer raramente é exata e pode, em alguns casos, promover complacência.

A **avaliação qualitativa** é uma avaliação que é utilizada para identificar os principais riscos enfrentados por uma empresa, quando os dados não se encontram disponíveis ou quando estão incompletos. Ao invés de serem utilizados números, são utilizadas palavras para descrever os riscos, a sua probabilidade de ocorrência e as consequências que os mesmos poderão gerar [1]. O que quer isto dizer que não são utilizados dados probabilísticos, mas apenas a perda potencial estimada. Esta análise baseia-se em qualidades essencialmente subjetivas atribuídas a cada risco, que indicam o seu mérito ou de outra forma em relação um ao outro. Como por exemplo o facto de poder avaliar o risco como baixo, médio ou alto [37].

Num contexto de segurança da informação, uma análise envolve uma descoberta e uma revisão dos ativos da empresa (hardware, software, processos, recursos humanos, etc…) para fraquezas conhecidas em relação a uma base de dados de vulnerabilidades potenciais. Onde, cada risco é medido em relação a escalas relativas de forma a estabelecer a probabilidade de que uma determinada ameaça possa explorar essa vulnerabilidade [37].

Uma desvantagem, talvez relevante, para esta avaliação qualitativa, é a sua natureza, que produz resultados inconsistentes. Tendo em conta que este método não utiliza ferramentas como a matemática e a estatística para modelar o risco, o resultado deste método depende muito das ideias de quem conduz a análise de risco, pelo facto de ser um método subjetivo [38].

3. CARACTERIZAÇÃO DA UNIVERSIDADE DA MADEIRA

A Universidade da Madeira, UMa, é uma instituição de ensino superior público, localizada no Funchal, na Região Autónoma da Madeira, que foi fundada a 13 de setembro de 1988 e que é constituída por três edifícios que se encontram em diferentes pontos geográficos. São eles o edifício da Penteada (Campus Universitário da Penteada), o edifício da Reitoria (no Colégio dos Jesuítas) e o edifício Sede onde funcionam a maior parte dos serviços de ação social e onde encontra-se a residência (na Rua de Santa Maria, nº253) [39] [40] [41].

A universidade integra diferentes áreas de conhecimento dividindo-se atualmente em quatro faculdades (Artes e Humanidades; Ciências Exatas e da Engenharia; Ciências Sociais; Ciências da Vida) e duas escolas superiores (Tecnologias e Gestão; Saúde). Na Faculdade de Artes e Humanidades existem três departamentos (Arte e Design; Línguas, Literaturas e Culturas; Psicologia) onde a mesma tem por missão a realização de atividades de ensino de licenciatura (1º ciclo), mestrado (2º ciclo) e doutoramento (3º ciclo). Na Faculdade de Ciências Exatas e da Engenharia existem seis departamentos (Física; Engenharia Civil e Geologia; Engenharia Eletrotécnica; Engenharia Informática e Design de Media Interativos; Matemática; Química A) onde a mesma tem por missão a realização de atividades de ensino de licenciatura (1º ciclo), mestrado (2º ciclo), doutoramento (3º ciclo) e investigação. Na Faculdade de Ciências Sociais existem três departamentos (Ciências da Educação; Educação Física e Desporto; Gestão e Economia) onde a mesma tem por missão a realização de atividades de ensino de licenciatura (1º ciclo), mestrado (2º ciclo), doutoramento (3º ciclo) e Pós-Graduação. Na Faculdade de Ciências da Vida existem dois (Biologia e Medicina) onde a mesma tem por missão a realização de atividades de ensino de licenciatura (1º ciclo) e ciclo básico para a medicina, mestrado (2º ciclo) e doutoramento (3º ciclo). Na Escola Superior de Tecnologias e Gestão existem nove cursos técnicos superiores profissionais, apenas um curso de licenciatura (1º ciclo) e um curso de pós-graduação. Por fim, na Escola Superior de Saúde existe um curso de licenciatura (1º ciclo), e um curso de mestrado (2º ciclo) [42].

Para termos uma noção do número de pessoas que frequentam ou podem frequentar diariamente a Universidade da Madeira, após consulta na página oficial da mesma, observemos a Tabela 5.

Tabela 5 - Levantamento do número de docentes e não docentes por departamento, em 2016 [43].

Faculdades	Docentes	Não docentes
Artes e Humanidades	61	0
Ciências Exatas e da Engenharia	78	6
Ciências Sociais	62	1
Ciências da Vida	20	5
Escola Superior	**Docentes**	**Não docentes**
Tecnologias e Gestão	-	-
Saúde	-	-
TOTAL	221	12

Tendo em conta o diretório de contactos disponível no site oficial da UMa, dispostos por departamentos, número de telefone e email, constam 564 pessoas docentes, não docentes, etc… dentro da universidade. Somando o número de alunos que nestes últimos anos a universidade tem acolhido, embora haja algum decréscimo, conta com sensivelmente entre 3000 a 3500 alunos e a contar com as pessoas que entram na universidade pelas mais variadas razões, desde reuniões, palestras, organizações de eventos, etc…. É possível concluir que a universidade movimenta um número igual ou superior a 4000 pessoas por ano, o que é demasiado importante e relevante destacar a elevada capacidade de segurança que a mesma deve ter.

3.1 Missão

A UMa visa encontrar soluções adequadas, num quadro de responsabilidade, equidade e sustentabilidade, que contribuam para o desenvolvimento e afirmação da Madeira e do país num mundo globalizado e dinâmico.

A Universidade prossegue, entre outros, os seguintes fins:

a) A realização de atividades de investigação científica, promovendo a difusão e valorização social e económica do conhecimento e da inovação tecnológica;
b) A formação humana ao mais alto nível, nos seus aspetos cultural, científico, artístico, técnico e profissional, realizando ciclos de estudos conferentes de grau académico, CTeSP e outros cursos não conferentes de grau académico de interesse para a RAM, procurando preparar os seus estudantes para os desafios da sociedade global e da formação ao longo da vida, transmitindo-lhes conhecimento científico, competência técnica e uma formação transversal que os transforme em cidadãos do mundo, criativos e empreendedores, responsáveis e profissionais, tolerantes e atentos aos desafios ambientais, culturais e humanos duma sociedade que se pretende sustentável e equitativa;
c) A promoção e o apoio a ações e programas que contribuam para a inserção dos seus diplomados no mundo do trabalho e que fomentem o seu espírito de iniciativa e de empreendedorismo, bem como a mobilidade de estudantes e diplomados, nomeadamente no espaço europeu do ensino superior.

3.2 Visão

A UMa pretende preparar os seus estudantes para serem cidadãos técnica e cientificamente competentes, cultos, inovadores e atuando com base nos valores da transparência, justiça, igualdade, fraternidade e do desenvolvimento sustentável do planeta, e, através do seu caráter empreendedor, da qualidade da sua investigação e formação e do seu espírito de serviço, pretende ser um ator indispensável no desenvolvimento social, cultural e económico da RAM e na sua internacionalização.

3.3 Estrutura organizacional da UMa – Unidades Funcionais

No quadro da autonomia de gestão da instituição, em especial no da organização dos serviços, compete, nos termos do disposto no art. 62º/4 dos Estatutos da Universidade da Madeira, ao Reitor a definição da sua estrutura funcional, delimitando as unidades funcionais, as suas designações, os seus objetivos, as suas competências e dependências e articulações funcionais, sendo que da competência do Conselho Geral a sua aprovação. – cfr. art. 62º/5 do Estatutos [44].

As unidades funcionais da Universidade compreendem as unidades de apoio à Reitoria e as unidades gerais comuns a toda a Universidade:

1. Unidades de Apoio à Reitoria:
    a. Assessoria Jurídica;
    b. Gabinete de Apoio à Reitoria;
    c. Gabinete de Controlo da Qualidade;
    d. Gabinete de Imagem e Relações Públicas;
    e. Secretariado Externo.
2. Unidades Gerais:
    a. Direção de Serviços Financeiros e Patrimoniais, constituída por:
        i. Unidade de Aprovisionamento e Património;
        ii. Unidade Económica e Financeira.

    b. Direção de Serviços de Infraestruturas e Equipamentos, constituída por:
        i. Unidade de Infraestruturas e Instalações;
        ii. Unidade de Equipamentos e Recursos Físicos.
    c. Arquivo;
    d. Biblioteca;
    e. Unidade de Assuntos Académicos, constituída por:
        i. Gabinete de Gestão Académica;
        ii. Gabinete de Apoio ao Estudante.
    f. Unidade de Comunicações e Informática, constituída por:
        i. Gabinete de Desenvolvimento de Aplicações Informáticas;

ii. Gabinete de Redes e Sistemas Informáticos.

g. Unidade de Projetos e Cooperação;

h. Unidade de Recursos Humanos [43].

A Figura 11 ilustra a hierarquia das unidades funcionais referidas anteriormente.

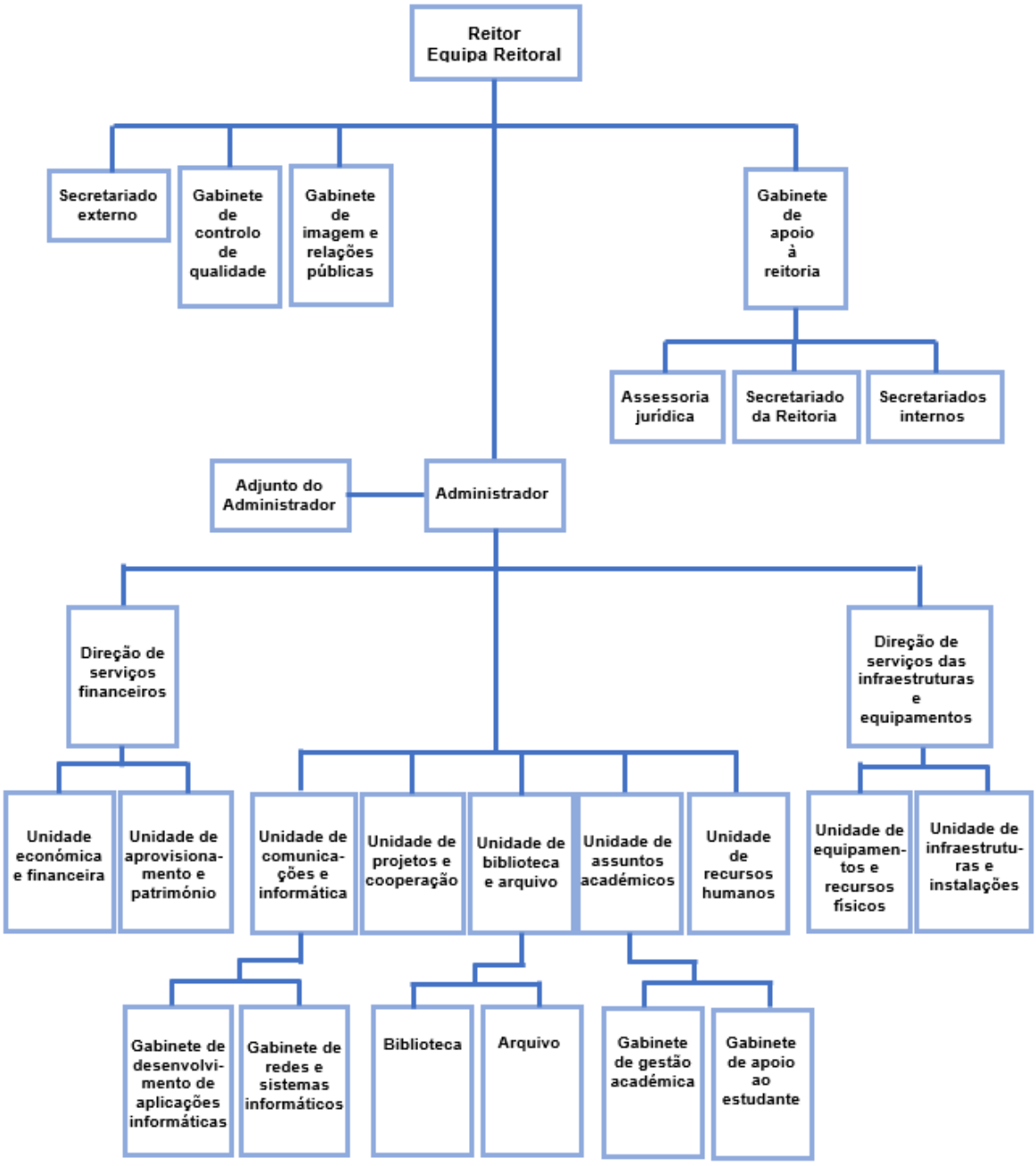


Figura 11 - Organigrama da estrutura organizacional da Universidade da Madeira [44].

Quanto aos órgãos da Universidade, a mesma é composta por:

- Conselho geral;
- Reitor;
- Conselho de Gestão.

3.4 Descrição da evolução da estrutura da rede da UMa

O edifício da Penteada, localizado no Campus Universitário da Penteada, foi construído em meados da década de 90 onde o mesmo abriu portas às atividades letivas a partir do ano de 1998. Diz-se que no projeto inicial do edifício já existia uma rede estruturada, instalada em calhas e espaços próprios e já suportada por zonas técnicas definidas para o efeito. Nessa rede estruturada destacavam-se os espaços que foram deixados, em cada piso, para a colocação dos bastidores de equipamentos ativos e as ligações de dados e voz, onde estava destacado o piso 0, sendo a zona de maiores dimensões com o propósito de servir como ponto central dessa mesma estrutura da rede [45].

A Figura 12 ilustra a estrutura atual da rede da instituição, simplificada, onde se encontram apenas as principais ligações da rede (denominadas de Backbone de edifício) juntamente com os bastidores.

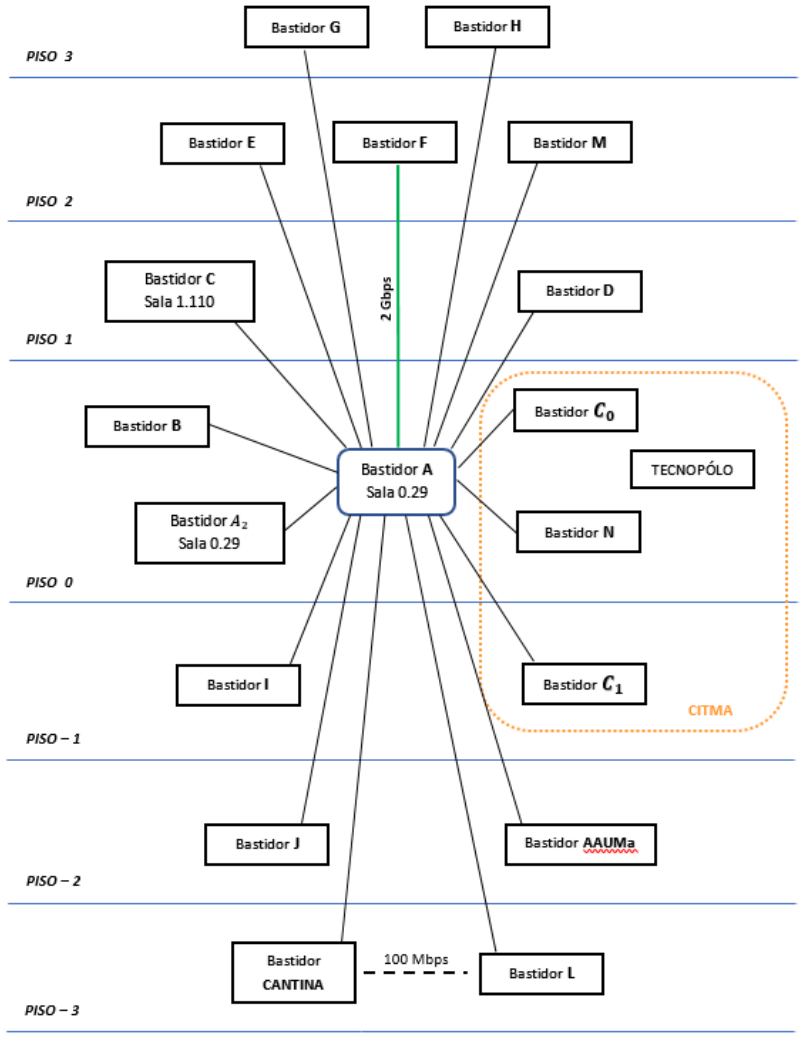


Figura 12 - Backbone do edifício da Penteada – Estrutura simplificada da rede da UMa [45].

Como é possível observar, o bastidor A, encontra-se praticamente a meio de todos os outros pois é o bastidor principal do edifício, o ponto onde todas as cablagens

convergem, servindo de interligação com todos os restantes bastidores, denominados de bastidores de piso. No início, apenas foram instalados no máximo 2 bastidores por piso que continham os equipamentos ativos que interligavam os gabinetes dos docentes e dos funcionários onde também permitiam o acesso às impressoras e aos servidores web, mail e entre outros, da instituição, e à internet. Existiam muito poucas ou quase nenhumas tomadas para cada sala sendo as salas do piso 0 as que ainda continham 2 ou 3 tomadas a mais que as restantes, para dados e voz que nem eram utilizadas. Até nos gabinetes dos docentes tinham entre 1 a 3 tomadas. Desde então houve uma necessidade enorme de passar novas cablagens e acrescentar um maior número de tomadas às salas de maior capacidade que tinham maior número de equipamentos terminais ligados à rede, principalmente os laboratórios de informática [45].

Como foi possível observar na figura anterior, houve a necessidade de acrescentar mais bastidores, essencialmente no piso 0 (piso central constituído pelo bastidor central e restantes) e no piso 2 (laboratório de informática e salas de computadores), pois são os pisos onde há uma maior afluência de equipamentos terminais ligados à rede [45].

Quanto às ligações da rede, desde o inicio, as mesmas são todas implementadas em cobre, com cabos de UTP e de categoria 5, existindo diversas evoluções nas zonas que foram renovadas recentemente. Ou seja, existiam ainda zonas de rede em categoria 5, categoria 5E e categoria 6, suportando diferentes velocidades e diferentes qualidades de transmissão. Mais tarde, em 2005, com o investimento feito ao abrigo do programa Madeira Digital, foi possível evoluir com as redes wi-fi onde foram instalados, no edifício, 120 pontos de acesso, distribuídos por todos os pisos, permitindo a ligação aos portáteis dos docentes, dos alunos e de visitantes na instituição. Com o decorrer da evolução e das mais recentes instalações, o número de serviços suportados pela instituição foram aumentando, ao longo do tempo, assim como a sua complexidade, destacando-se o aparecimento na rede interna do suporte à videoconferência, a interligação e partilha de serviços com outras universidades, entre outros [45].

Numa fase inicial da rede, os equipamentos ativos instalados nos diversos bastidores eram hubs (repetidores) a 10Mbits/s e switchs (comutadores) a 100Mbits/s. Mais tarde, em toda a rede, foram globalmente atualizados para switchs (comutadores) com velocidade de 100Mbits/s [45].

Atualmente, a ligação entre bastidores ainda é feita a 1Gbit/s à exceção de apenas um troço que é feito a 2Gbits/s, como foi possível confirmar na figura anterior [45].

Com o investimento realizado em 2005, houve um aumento exponencial da velocidade e permitiu a integração de novas tecnologias para gestão mais avançada da rede, VLAN – IEE 802.1Q, suportando assim um maior número de novos serviços [45].

Quanto à ligação a outras redes universitárias e à Internet, a partir de 2010 a transferência máxima passou de 512Kbits/s para 100Mbits/s estando a ligação atualmente, e desde 2015, com transferência máxima de 200Mbits/s [45].

Quanto ao pessoal técnico, responsável pela manutenção e gestão da rede da instituição inicialmente, evoluiu e aumentou exponencialmente. Na altura em que a instituição abriu portas às atividades letivas, existiam seis elementos no Sector de Comunicações e Informática (SCI) onde apenas três deles tinham responsabilidade na manutenção e gestão da rede. E só um deles tinha um perfil de técnico superior na área das redes e sistemas. Atualmente a equipa cresceu e já conta com cinco pessoas com responsabilidade na manutenção e gestão da rede entrando recentemente um técnico com formação superior [45].

3.5 Descrição da arquitetura da rede da UMa

Neste subcapítulo pretende-se clarificar as características da estrutura da rede em termos físicos (equipamento passivo – cabos; equipamento ativo – switchs, routers, Firewalls, servidores de rede, etc…) e em termos lógicos (sub-redes) de forma a poder complementar a informação abordada anteriormente.

3.5.1 Arquitetura Física

Como demonstrado anteriormente, a arquitetura física e simplificada da rede encontra-se ilustrada Figura 12, figura anterior, embora não esteja incluída:

- A zona de servidores, por ter uma dimensão e complexidade consideradas devido aos variados serviços existentes na instituição;
- As zonas das diferentes faculdades;
- A rede com os terminais dos docentes, funcionários e laboratórios de informática;
- Toda a extensão para a rede WI-FI já integrada na rede existente, atualmente [45].

A arquitetura da rede é essencialmente em estrela surgindo algumas subdivisões para novas estrelas, de menor dimensão, em alguns troços da rede. As exceções são as redes para os outros dois edifícios, o edifício da reitoria e o edifício do SASUMa, onde o número de postos e serviços têm alguma dimensão para serem considerados segmentos particulares. É no edifício da Reitoria que estão centralizados os serviços da reitoria, os serviços administrativos, os serviços de recursos humanos e o Gabinete de Desenvolvimento de Aplicações Informáticas. Daí localizar-se alguns dos servidores importantes, por exemplo, os servidores web, a base de dados de docentes e alunos, e algumas plataformas que existem na academia [45].

A interligação entre bastidores está implementada, atualmente, em fibra ótica multimodo, com dois cabos de fibra a interligar cada bastidor existentes nos vários pisos ao bastidor principal do piso 0, os quais seguem caminhos diferentes por questões de redundância a falhas [45].

Nas ligações entre o bastidor principal e os restantes bastidores, implementadas sobre fibra ótica multimodo, encontram-se as interligações de maior capacidade, 1Gbit/s. Na cablagem que liga os equipamentos nos bastidores aos equipamentos terminais, assenta em cabos UTP de categoria 5, suportando ligações a 100Mbits/s. Quanto aos servidores, estes, na sua maior parte são servidos com rede a 1Gbit/s assentes em cabo de categoria 6. A ligação mais recente e de maior capacidade é a ligação ao Sistema Blade e opera a 10Gbit/s [45].

No que diz respeito à ligação à Internet, a mesma é fornecida pela operadora NOS e permite uma velocidade máxima contratada de 200Mbits/s. Um dos pontos negativos da rede é que não existe redundância neste circuito, que liga a UMa à Internet e que tem ligação física no edifício da Penteada (Campus da Penteada) [45].

A Figura 13 ilustra o cenário geral, atualmente, da rede da Universidade da Madeira.

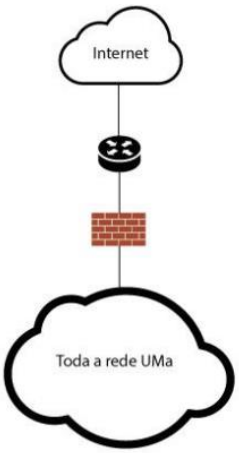


Figura 13 – Cenário geral da rede da Universidade da Madeira [46].

Quanto à ligação entre os três edifícios, o edifício da Penteada (Campus da Penteada) liga-se ao edifício da Reitoria (Colégio dos Jesuítas), através de fibra ótica multimodo, num cabo subterrâneo com 1Gbit/s de largura de banda. Sendo o edifício da Reitoria um dos que contém serviços essenciais a toda a universidade, devido a essa importância o mesmo tinha uma ligação que permitia redundância na ligação com o edifício da Penteada, que existiu até 2010, altura em que foi quebrada após o temporal de 20 de fevereiro. Relativamente à ligação entre o edifício da Reitoria e o edifício Sede (SASUMa) a mesma é feita igualmente por fibra ótica com largura de banda de 10Mbits/s. Por fim a ligação entre o edifício Sede (SASUMa) e a residência é feita através de um cabo UTP. É de salientar que as ligações entre cada um não contêm redundância o que significa que se um dos circuitos falhar os edifícios a jusante ficam sem acesso à Internet, como é possível comprovar na Figura 14 [46].

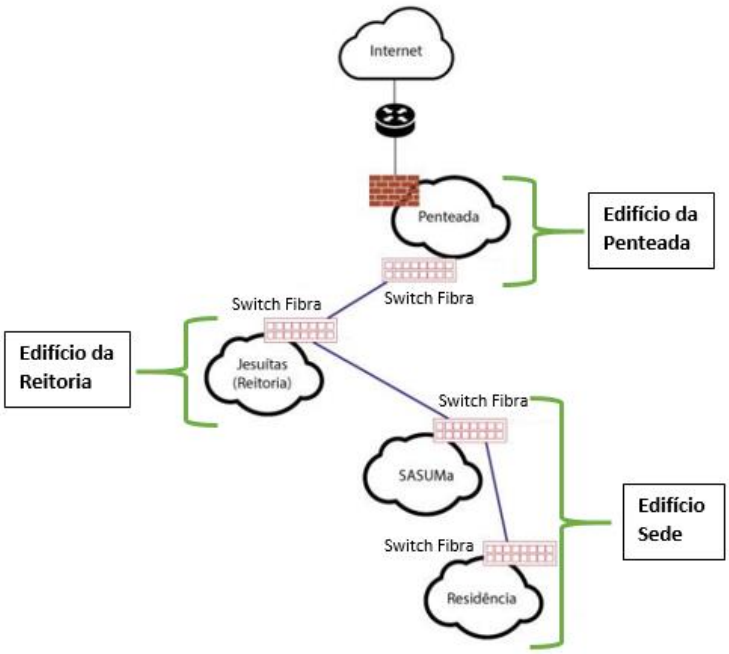


Figura 14 - Ligações entre cada edifício [46].

Destaca-se ainda o alargamento do serviço Voice over IP (VoIP) que se encontra ainda em fase de implementação.

No fim do Anexo B – Recolha de informação da rede da UMa encontra-se a lista completa dos equipamentos ativos atualmente em operação em cada bastidor e os equipamentos principais da rede Wi-FI.

Quanto ao estado atual da rede no que diz respeito às limitações e fragilidades, é de referir que:

- No bastidor principal (piso 0) existem equipamentos de diferentes fabricantes para as mesmas funções (exemplo: switchs) o que dificultam a gestão e fazem com que haja uma maior probabilidade de incompatibilidades;
- Existem ainda equipamentos que maioritariamente já têm mais de dez anos, ou seja, muito antigos;
- Apesar de a rede WI-FI consistir num número elevado de pontos de acesso (120) não existe um controlador que facilite a monitorização e configuração dos mesmos;
- Existe um elevado número de queixas constantes dos utilizadores devido a problemas de cobertura de rede [45].

Existem problemas na capacidade dos pontos de acesso conseguirem suportar o elevado número de dispositivos existentes, sobretudo em zonas de maior densidade de utilizadores [45].

3.5.2 Arquitetura Lógica

Atualmente a rede da instituição utiliza a Virtual LAN, mais conhecida por VLAN, para dividir uma rede local em mais de uma rede, ou seja, dividir o tráfego entre diferentes perfis de utilização. Neste caso são utilizadas para separar as redes dos funcionários (docentes e não docentes) da rede dos alunos. Existem outras VLAN's próprias para por exemplo a gestão de equipamentos, segmentos particulares da rede (sala de videoconferência, sistema Blade, entre outros). A Tabela 6 apresenta algumas das vinte VLAN's existentes e configuradas da rede da instituição onde seis delas encontram-se inativas [45] [46].

Tabela 6 - Lista de VLANs da rede da Universidade da Madeira [46].

VLANs	Designação da Rede	Destinatários
VLAN1	Funcionários e servidores	Docentes e funcionários UMa e SASUMa
VLAN2	Alunos	Alunos UMa
VLAN3	IP válidos escritório	Router, servidor DNS externo, etc…
VLAN4	INATIVA	
VLAN5	Rede wireless rWauma	Labs, salas informátic, WPA Pre-shared key
VLAN6	Infraestrutura WI-FI (APs)	APs Wireless
VLAN7	INATIVA	
VLAN8	e-U Wireless UserRoaming	Utilizadores em roaming na rede e-U
VLAN9	Associação académica (AAUMa)	Utilizadores da AAUMa
VLAN10	INATIVA	
VLAN11	VoIP	Docentes e funcionários da UMa
VLAN12	Administração VoIP	Gestão de equipamentos VoIP
VLAN13	INATIVA	
VLAN14	INATIVA	
VLAN15	INATIVA	
VLAN16	Controlos de acessos interno SALTO e externo NET2	Controlos de acesso interno e externo UMa Posto receção Parque do Colégio dos Jesuítas
VLAN17	Sistema Blades – Rede de Gestão	Gestão dos servidores Blade, Fabric Interconnect e Storage NetApp
VLAN18	Sistema Blades	VLAN Iscsi/vMotion
VLAN19	Sistema Blades	VLAN vMotion/Iscsi
VLAN20	Sistema Blades	VLAN Hosts de VMware

A Figura 15 ilustra o cenário das VLANs existentes na Instituição.

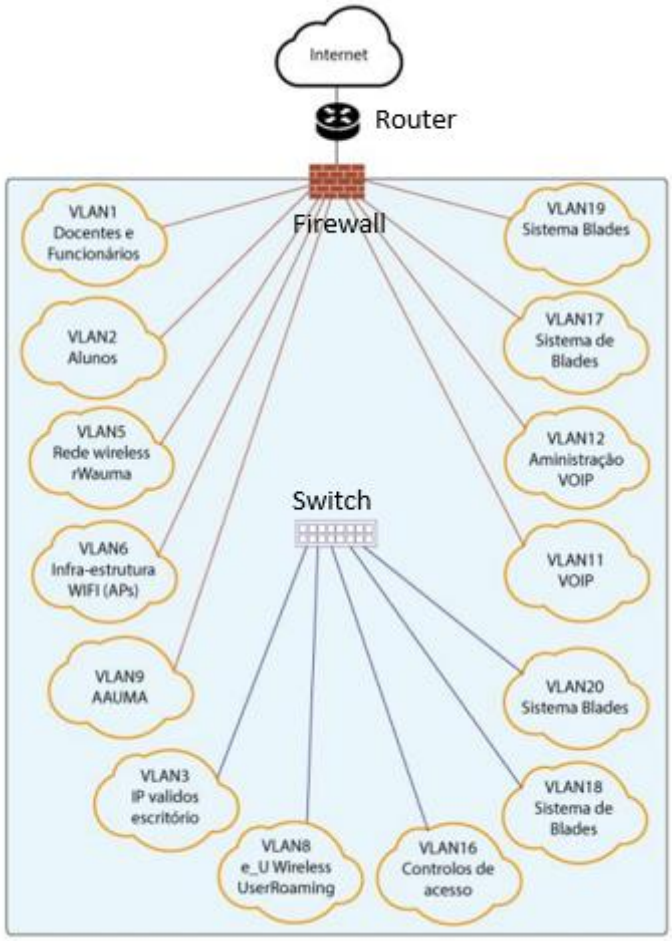


Figura 15 - Cenário atual das VLANs da rede da Universidade da Madeira [46].

Como é possível observar existem VLANs que se encontram ligadas diretamente à Firewall, de forma a orientar a gestão das mesmas, e as restantes VLANs encontram-se ligadas aos switchs para acessos internos.

O facto de poder-se utilizar VLANs torna-se numa solução flexível na medida em que permite que qualquer serviço possa estar disponível em qualquer ponto da rede do edifício, mas tem como condicionamento ter um ponto central que condensa todas as funções de encaminhamento, filtragem e segurança. Pode ser pouco resiliente a falhas e ter limitações de desempenho.

3.6 Situação atual

A própria estrutura organizacional da UMa, bem como a atuação dos serviços em áreas completamente distintas como por exemplo a área administrativa, a área financeira, a área social, etc…, resultam numa tamanha variedade e num grande volume de produção e circulação de informação, seja a maior parte dela no formato digital.

Como abordado anteriormente, toda a rede da UMa encontra-se dispersa em 3 edifícios, geograficamente dispersos uns dos outros, daí haver um cenário complexo no que toca

a sistemas de comunicação e de segurança da informação que é transmitida entre os mesmos.

De forma a perceber e compreender em que ponto se encontra a segurança da rede do campus da universidade da Madeira, mais concretamente, quais são os principais desafios e problemas que a segurança da rede da UMa enfrenta, procedeu-se a uma primeira análise da situação atual. A forma com que a informação foi obtida foi única e exclusivamente através da realização de várias entrevistas estruturadas e/ou semiestruturadas com os responsáveis da gestão da rede da UMa e através de consulta de documentos da instituição, culminando assim numa mais rápida e eficaz identificação de problemas de segurança críticos e/ou vitais da rede da UMa.

Os documentos com as questões que foram elaboradas para as entrevistas encontram-se em anexo (Anexo B – Recolha de informação da rede da UMa) onde as mesmas foram baseadas em vários documentos de referências bibliográficas utilizadas para a realização deste trabalho ([11], [45], [47]).

Obtidas então as respostas às questões, procedeu-se ao agrupamento das mesmas, com especial atenção à existência de processos relacionados com a segurança da informação que foram definidos e implementados nos seguintes contextos:

No contexto da **segurança organizacional** da empresa, foram abordados os aspetos relacionados com a política de segurança e as funções e responsabilidades sobre os ativos.

Quanto à **segurança física e ambiental,** foram abordadas as condições de segurança física das instalações da universidade bem como das áreas onde se encontram equipamentos de rede e das áreas e/ou zonas específicas onde é feito o tratamento e onde é guardado toda a informação.

Relativamente à **segurança de equipamentos e serviços,** procedeu-se à identificação e avaliação de todos os equipamentos existentes (servidores, máquinas, todos os dispositivos existentes, etc…) bem como quem os manuseia e qual a segurança que os mesmos têm, tendo em conta que a maioria deles são ativos. Em relação aos serviços analisou-se a segurança dos mesmos.

No contexto da **segurança da rede de dados**, a análise baseou-se essencialmente na segurança das comunicações.

Quanto à **segurança aplicacional**, procedeu-se ao levantamento de todo o tipo de programas e /ou aplicações desenvolvidas e/ou utilizadas, de como é feito o armazenamento e registos de log.

Relativamente à **segurança de recursos humanos**, analisou-se as funções e responsabilidades dos ativos no que toca à segurança no início e término da relação contratual e à formação técnica dos mesmos.

Quanto à **conformidade**, analisou-se muito por alto, visto ser ainda muito recente, o cumprimento ou não dos requisitos legais (regulamentação em vigor até à data) e

contratuais, nomeadamente o Regulamento Geral de Proteção de Dados (RGPD) e outras leis em vigor, relacionadas com a proteção dos dados pessoais.

3.6.1 Segurança Organizacional

Um dos pontos fundamentais desta área é a política de segurança. Ora a política de segurança tem como principal objetivo possibilitar a gestão da segurança numa empresa/organização/instituição. Trata-se de um documento formal e vital que reflete a disposição da administração de dirigir a empresa de forma mais segura e controlada e onde o mesmo deve ser disponibilizado a todos os funcionários, colaboradores, etc… e ainda deve ser revisto sempre que surjam novos requisitos e/ou algum objetivo de controlo que não seja validado. Ou seja, uma empresa ou instituição que possua este documento formal, onde este tenha sido escrito e esteja implementado, só trará benefícios a nível de segurança e irá fortalecer a segurança, em todos os níveis.

A UMa não possui o documento formal de política de segurança, logo por aqui já é possível afirmar que não existe um documento em que estejam escritas as regras e boas práticas relacionadas ao uso seguro dos dados, apesar de dispor de alguns procedimentos de segurança estabelecidos, de forma informal. Com isto verificou-se que não existe documento algum disponível para consulta de todos os colaboradores sobre qualquer procedimento de segurança estabelecido, traduzindo-se no completo desconhecimento de regras e boas práticas.

O estado atual da segurança da informação é desconhecido pois não existe formação por parte dos utilizadores, investigadores, técnicos, etc… que evitem e que tenham certos cuidados com as suas atividades. Ou seja, não existe um documento a informar os cuidados a ter e a evitar.

Não existe um documento formal em que esteja definido quem é o responsável por quê, o que tem que fazer e etc.... apenas as funções encontram-se razoavelmente distribuídas e são atribuídas a cada um dos elementos da equipa, ou seja, a pessoa "x" está responsável por "X" servidor e em segunda linha tem a pessoa "y" que está responsável pelo mesmo.

Relativamente ao pessoal da gestão da rede, existem três equipas, uma equipa de redes e sistemas informáticos que é constituída por dois técnicos superiores e cinco técnicos, uma segunda equipa para desenvolvimento de aplicações que é constituída por sete técnicos superiores com diferentes competências e por fim uma terceira equipa de unidade de instalações de equipamentos que é constituída por seis técnicos. Quanto à administração da rede, é constituída por um engenheiro e por outros dois técnicos, delegados pelo anterior.

Verificou-se que nunca foi efetuada qualquer auditoria formal, apenas aconteceu uma, mas meramente informal. Neste momento não existe planeamento para auditorias nem nada do género.

Desta forma, e tendo em conta este contexto, constatou-se a ausência do documento (política de segurança) e de uma grande lacuna na descrição de processos formalmente definidos, o que quer dizer que não se encontram estabelecidas regras nos vários domínios da segurança da informação, nem muito menos se encontra definido os cargos e responsabilidades associadas.

3.6.2 Segurança Física e Ambiental

No que diz respeito à segurança física, e de uma forma geral, todas as instalações da UMa cumprem parcialmente as exigências de segurança. Abordando sempre o edifício da Penteada (instalações da UMa), verifica-se a existência de um perímetro de segurança física e sistema de vigilância (câmaras localizadas e apontadas para as portas de acesso do interior para o exterior do edifício, sistema que é gerido e observado constantemente por um funcionário). O acesso físico à universidade pode ser feito pela porta principal (onde não há relativamente controlo algum, todos entram) e pode ser feito pelas restantes portas pois só dão acesso através de cartão pessoal. Existem ainda umas portas que dão acesso à universidade, através do Tecnopolo (edifício ao lado ao da universidade) mas essas portas encontram-se fechadas pelo lado do Tecnopolo. Existe uma exceção apenas na porta principal de acesso à universidade que é controlada apenas aos fins de semana e nos dias de semana a partir de uma determinada hora, por um segurança.

O acesso físico às salas onde se encontram os equipamentos de rede e etc… (zonas/áreas técnicas) é feito única e exclusivamente por chaves. Quem tem as chaves são os elementos da equipa da unidade de comunicações de informática e alguns elementos da equipa de equipamentos e instalações onde estes últimos apenas necessitam da mesma para a manutenção do ar condicionado. Ainda para mais existem chaves mestras que dão completo acesso a qualquer sala, onde as chaves encontram-se sem muita proteção, na receção da UMa. As zonas, que podem ser muito bem caracterizadas por zonas críticas, não são controladas nem por sistemas de vigilância nem por outro sistema de segurança. Não é possível obter registos nenhuns de quem entra ou quem sai, ou seja, não há nada que possa comprovar a entrada ou saída de pessoas nessas zonas. Relativamente ao controlo de acesso físico das salas, não existe documento de política de segurança que defina quem tem acesso e quem não tem. Inicialmente houve alguns despachos, mas nunca foram divulgados de forma correta, visível e clara. Verifica-se também que o acesso físico à sala onde são guardados todos os dados dos alunos e restantes funcionários, é feito por chave tradicional, ou seja, não existe registo.

Quanto à segurança ambiental, algumas das salas (zonas/áreas técnicas), devido à falta de espaço nas mesmas, são utilizadas como arrumos, prejudicando a qualidade ambiental das salas.

Desta forma, e tendo em conta este contexto, constatou-se que a implementação de pelo menos um sistema de controlo de acesso (por cartão) é uma necessidade evidente

para um maior e melhor controlo no acesso às salas (zonas/áreas técnicas) bem como a definição de uma política de acessos.

3.6.3 Segurança de Equipamentos e Serviços

Desde 2005, altura em que a rede da UMa sofreu uma enorme evolução, com o investimento feito ao abrigo do programa Madeira Digital, onde houve uma vasta aquisição de equipamentos mais sofisticados, a todo o nível. Posteriormente a essa fase, a última vez que a rede sofreu nova evolução mais específica foi entre 2010 e 2015, altura em que a capacidade de resposta de todos os equipamentos e a nível de ligações de rede tornou-se mais rápida. De 2015 até hoje a rede tem sofrido algumas alterações pontuais, tanto a nível de aquisição um ou outro equipamento assim como software com características adequadas às exigências de processamento e de segurança da informação.

Apesar de alguma evolução naquelas épocas em grande número de aquisição de equipamentos de rede, verifica-se que houve uma significativa diminuição na aquisição e atualização de equipamentos mais importantes para maior segurança e gestão da rede. Apenas algumas aquisições foram feitas variando algumas marcas e modelos, fazendo reduzir a fiabilidade e tornando a gestão de rede mais complexa devido às compatibilidades.

Embora todos os equipamentos adquiridos, como ativos físicos tecnológicos, se encontrarem identificados e registados, não há um documento formal que conste toda a informação dos mesmos desde as várias aquisições como das várias alterações de tudo o que existe até à data.

Quanto ao manuseamento e às operações técnicas de manutenção e etc… é tudo efetuado por pessoal técnico e devidamente habilitado com as competências informáticas, desde técnicos de manutenção subcontratados, como os próprios engenheiros e técnicos superiores da universidade. Verifica-se que não existe uma política de operações que garanta a normalização dos mecanismos de segurança aplicados e de todo o trabalho que é realizado. Verifica-se ainda que na maioria dos casos as intervenções técnicas encontram-se, no geral, ao critério de cada técnico, embora o engenheiro esteja sempre a par das intervenções, quando não presente, pois não existindo documentação dos procedimentos nem muito menos políticas bem definidas e especificas para as operações, podem incorrer em lapsos nas configurações.

Muitos dos equipamentos, adquiridos em 2005, ainda se encontram no ativo, embora já em completo fim de ciclo e totalmente obsoletos e até à data muitos não foram substituídos. Verifica-se que atualmente a única firewall central é a mesma que foi instalada desde a primeira aquisição de equipamentos, ou seja, encontra-se de alguma forma obsoleta, o que torna o sistema inseguro.

Não existe algum tipo de inspeção periódica feita aos equipamentos (layer 2 – camada de ligação de dados e layer 3 – Camada de rede) nas salas técnicas, no sentido de verificar por exemplo se as configurações de routers, switchs, etc… foram ou não alteradas. Nem todos os bastidores se encontram fechados à chave, devido ao mau planeamento de instalação dos mesmos que impede a correta arrumação dos cabos e restantes equipamentos.

De uma forma geral, todos os equipamentos de rede encontram-se devidamente protegidos e só quem tem acesso à chave das salas técnicas é que os pode aceder (técnicos de manutenção, técnicos de operações e funcionária da limpeza).

3.6.4 Segurança da Rede de Dados

A UMa, como abordado no subcapítulo 3.5, possui uma infraestrutura de rede de dados bem estruturada embora não garanta redundância principalmente nas ligações entre os três edifícios que juntos formam toda a rede da UMa. Inicialmente existia redundância entre o edifício da reitoria (onde constam os serviços essenciais a toda a universidade) e o edifício do campus da Penteada, mas que foi quebrada devido ao temporal de 20 de fevereiro. Desta forma, se um dos circuitos falhar, os edifícios a jusante ficarão sem acesso à internet. Verifica-se também que não existe redundância da ligação de rede no exterior (operador).

De 2005 para cá a rede da instituição utiliza a Virtual LAN, mais conhecida por VLAN, que serve para dividir o tráfego entre diferentes perfis de utilização. Neste caso são utilizadas para separar as redes dos funcionários (docentes e não docentes) da rede dos alunos onde também existem outras VLAN's próprias para por exemplo a gestão de equipamentos, segmentos particulares da rede (sala de videoconferência, sistema Blade, entre outros). O facto de serem utilizadas as VLANs torna-se numa solução flexível na medida em que permite que qualquer serviço possa estar disponível em qualquer ponto da rede do edifício, mas tem como condicionamento ter um ponto central que condensa todas as funções de encaminhamento, filtragem e segurança. Daí poder ser pouco resiliente a falhas e ter limitações de desempenho.

Quanto ao estado atual da rede, no que diz respeito às limitações e fragilidades, verifica-se que:

a) No bastidor principal (piso 0) existem equipamentos de diferentes fabricantes para as mesmas funções (exemplo: switchs) o que dificultam a gestão e fazem com que haja uma maior probabilidade de incompatibilidades;
b) Existem ainda equipamentos que maioritariamente já têm mais de dez anos, ou seja, muito antigos;
c) Apesar de a rede WI-FI consistir num número elevado de pontos de acesso (120) não existe um controlador que facilite a monitorização e configuração dos mesmos;

d) Existe um elevado número de queixas constantes dos utilizadores devido a problemas de cobertura de rede pois em zonas de maior densidade de utilizadores os pontos de acesso acabam por não suportar o elevado número de dispositivos existentes;
e) Os principais fatores de falha de acesso à eduroam são por falha momentânea do sistema de autenticação (durante alguns minutos), por problemas de drivers (drivers desatualizados o que impede a correta ligação à rede wireless) ou por má configuração da rede wireless, por parte dos utilizadores;
f) Os pontos de falha máxima na rede, observados, localizam-se no circuito, no router e na firewall, e acontecem por diversos motivos. O nó da rede que corresponde às salas de conferência, é um nó muito sensível e que é um dos que enfrentam maior risco de falha.

Abordando o acesso tanto à rede local como à rede wireless da UMa, verifica-se que o acesso à rede wireless é feito com autenticação que se baseia nos dados dos alunos, funcionários e docentes, que são obtidos na altura que entram na instituição, ou seja, neste caso só acede quem tem as credenciais (identidade – número de aluno e password). O acesso à rede local já qualquer pessoa pode aceder onde não existe controlo, mas a ligação encontra-se limitada pelas VLANs. Por exemplo, se uma pessoa se ligar à rede por cabo, a mesma tem acesso de imediato à rede embora o acesso seja limitado no que a VLAN permitir. Existe documentação que diz o que é feito nas VLANs. Um ponto preocupante é que a VLAN1 se encontra na VLAN por defeito. Neste momento o router não permite mais atribuições à ligação ao exterior pois as ligações ao exterior encontram-se todas cheias e em utilização. Quanto às pessoas que se deslocam à universidade para eventos (palestras, conferências, etc…) ou outros motivos, também têm forma de acesso à rede wireless. se são alunos ligados a uma instituição anterior, já têm conta associada a uma “eduroam” e só basta redefinir a rede para ter acesso. Noutra situação existem contas Guest que são atribuídas às restantes pessoas onde ficam registados e onde são controladas as suas entradas e saídas (dia e hora). Nesta situação são pedidos os dados pessoais dados estes que são obrigatórios para as contas Guest (nome completo e o email). Existe um outro caso, quando uma pessoa que vem dar um workshop (por exemplo) e pretende que todas as pessoas presentes tenham acesso à rede wireless. Aí essa pessoa tem que requerer esse acesso no local próprio e a mesma fica responsável por essa atribuição. Todos estes procedimentos estão informatizados no office 365, mas não se encontram documentados, ou seja, carece de uma política bem definida.

O desempenho da rede wireless, devido ao facto de ser acedida por várias dezenas de utilizadores e pelos mais variados dispositivos móveis, revela a necessidade não só de maior velocidade como também de adquirir provavelmente um maior número de APs de forma a melhor o desempenho atual da ligação e de forma a haver uma maior disponibilidade da mesma.

É de igual forma importante haver um investimento na redundância das várias ligações e a definição de uma política de rede.

3.6.5 Segurança Aplicacional

Nunca é demais lembrar, que de pouco importa que o investimento de segurança seja exclusivamente direcionado para a segurança das infraestruturas de comunicação (rede), se esse mesmo investimento é descurado ao nível aplicacional. Se por um lado as empresas têm conhecimento das ameaças existentes no mundo online e dos perigos que estas representam para o seu correto funcionamento, por outro existe ainda uma clara falta de informação sobre as consequências de um ataque. Nem sempre as empresas sabem o que pode acontecer em caso de infeção ou de um ataque bem-sucedido. O que representa para a infraestrutura? Qual o período de downtime (caso ele exista)? Como se consegue repor a situação de operacionalidade e principalmente qual o custo para a empresa? Estas são perguntas simples onde as respostas nem muitas empresas as sabem dar: uma lacuna de informação que dificulta a justificação de investimentos nesta área, área esta onde hoje em dia a simples firewall já não é suficiente.

A UMa possibilita o desenvolvimento interno de programas informáticos à medida das necessidades de forma a obter soluções para as diversas áreas funcionais. Apesar de serem realizadas algumas avaliações aos requisitos de desempenho, à exigência computacional, verifica-se a inexistência de política de segurança para o levantamento de requisitos para a documentação obrigatória de todas as aplicações desenvolvidas.

Quanto ao armazenamento de dados, verifica-se que o mesmo é feito, fisicamente, em dois locais geograficamente afastados. Um é feito no edifício da Penteada (universidade) o outro é feito no edifício do colégio dos jesuítas (reitoria). Os sistemas utilizados para efetuar os backups no Windows é o nativo do mesmo (destino unidade exterior), NAS para o destino do backup, baseado em raid de forma a garantir maior consistência dos dados que são guardados e o Linux que também é o nativo do mesmo. Constata-se que a decisão de efetuar backup é da responsabilidade da pessoa que está responsável pelo serviço. Tanto as bases de dados, os ficheiros, as aplicações, os sites e os emails locais são as áreas que são tidas em consideração para efetuar backup onde em caso de ataques, por exemplo, aos sites, são repostos os backups dos mesmos e depois então em offline são analisados os sites de forma a melhorarem a segurança a esses ataques. De uma forma geral são feitos backups ao sistema integrado (de forma pontual) tornando possível a recuperação completa do sistema, em caso de falha. São feitos backups aos dados de forma periódica, mas não do sistema completo, o que implicaria uma maior capacidade de armazenamento, o que não está disponível. Nos serviços, os backups são feitos muito raramente. Em caso de situações que não tenham o backup do sistema é reconstruído criando uma nova máquina.

Neste momento, a nível de políticas de atualizações, estão a testar um serviço que funciona também para servidores que permite a distribuição e controlo das atualizações dos sistemas Windows. Este permite criar categorias de máquinas, como por exemplo,

pode ser dividido em 2 classes onde na classe 1 (de terminais) é definido que a atualização será feita e na classe 2 (de servidores) e definido que a atualização seja semanalmente. Com este novo serviço será possível separar os sistemas críticos ou de segurança, dos restantes. Outro dos grandes benefícios deste serviço é relativamente à ligação da internet, pois quanto maior for o número das máquinas nesse serviço, menor será a carga na ligação à internet para ir buscar as atualizações, pois são consumidas internamente. Todavia, este sistema tem um custo de desempenho enorme pois a máquina tem que ter uma elevada capacidade de RAM, um bom processador e um disco razoavelmente grande.

De uma forma geral verifica-se também que:

I. As atualizações de aplicação da rede são feitas apenas quando não há muito movimento na universidade;
II. Existem máquinas antigas que não estão devidamente atualizadas. A estratégia que é utilizada para as atualizações é tão banal e é feita de forma manual que acaba por não dar uma boa garantia de atualização. Primeiro é tirado um printscreen à versão atual/anterior e depois é feita a nova atualização. Caso aconteça alguma coisa de anormal é feito o downgrade à versão anterior, recorrendo novamente ao printscreen;
III. Outro problema é possuírem ainda máquinas com Windows XP na área dos docentes onde nessas existem pastas partilhadas. Alguma que esteja infetada e ligada à rede interna é um potencial risco na rede;
IV. Não existe software de monitorização de ataques;
V. Já existem algumas plataformas para a agregação da informação sobre o estado da rede, mas ainda não monitorizam todos os equipamentos e serviços, nem estão configuradas para oferecer relatórios úteis e ajustados às necessidades;
VI. Alguns dos servidores ainda se encontram em HTTP (máquinas/serviços antigos);
VII. As ligações de acesso normalmente são encriptadas. SSH. Têm uma política de passwords FORTE. As passwords não são mudadas com muita frequência. Relativamente aos servidores, nem todos utilizam HTTPS. Num serviço interno não existe esse cuidado de usar HTTPS. Foi recentemente atualizado um serviço que é utilizado na biblioteca (koha) pois foi necessário encriptá-lo. Houve também uma atualização no serviço de correspondência pois estava a ser utilizada a ligação HTTP, e mesmo sendo utilizado predominantemente a nível interno, decidiram reforçar a segurança para HTTPS. A nível de serviços externos, geralmente todos têm ligação por HTTPS;
VIII. Não existe políticas de criptografia e gestão de chaves no armazenamento.

Há uma evidente necessidade de definir uma política de segurança para este âmbito, essencialmente nos backups e nas atualizações quer das máquinas quer dos servidores e quer da rede. Verificou-se que apesar da maioria das aplicações efetuarem registos de logs e eventos de segurança, estas funcionalidades ainda não se encontram implementadas em todos os sistemas.

3.6.6 Segurança de Recursos Humanos

Este contexto é um dos mais sensíveis e importantes para o completo funcionamento de uma empresa ou instituição na medida em que todos os utilizadores, colaboradores, funcionários, fornecedores, etc… de uma empresa, organização e/ou instituição é que fazem a segurança da informação. Porque, por de trás dos controlos de segurança, até mesmo dos mais sofisticados, estão sempre pessoas, profissionais responsáveis pela configuração, pelo uso e pela manutenção desses controlos. Por mais que se pense que depois de aplicados todos os mecanismos de segurança é sinal que está tudo seguro, não é verdade. Está comprovado que atualmente, seja com intenção maliciosa ou falta de cuidado, os funcionários, colaboradores, etc… continuam a ser a principal causa de violação da segurança de informação (dados). Em ambientes corporativos, é comum os utilizadores, colaboradores, funcionários, etc… ficarem muito confiantes no sistema de segurança da informação e nos recursos de informática. Estes não compreendem que o sistema de TI também oferece riscos e que cabe a eles uma parcela de responsabilidade para garantir a segurança das informações da empresa. Para isso é importante que a política de segurança da informação aborde a segurança em recursos humanos, ou seja, a mesma deve determinar como será feita a consciencialização dos empregados para a importância da segurança da informação e garantir que os mesmos assumam as suas responsabilidades nesse processo, que pode custar a "vida" à empresa e consequentemente os seus empregos.

É importante que antes de ter acesso aos sistemas de informação da organização, o contratado assine um termo onde diz concordar com a política de segurança da informação, com as suas responsabilidades para com essa política e com as possíveis penalidades caso ele não cumpra o que foi estabelecido em contrato. Dentre as obrigações do novo contratado, devem estar o bom uso dos recursos de TI, o sigilo de informações sensíveis (mesmo após o término do contrato), a correta classificação das informações e a adoção de outros procedimentos de segurança pré-definidos pela organização. Cabe também à direção garantir que todos os colaboradores recebam a formação adequada, pelo menos uma vez por ano, e que os conhecimentos adquiridos sejam colocados em prática, inclusive pela própria direção.

Na UMa verifica-se que existe um documento formal em que consta as responsabilidades dos contratados (funcionários, colaboradores, docentes, não docentes) mas não se encontra definido na política de segurança. Ou seja, verifica-se a falta de um plano de atividades de sensibilização para a segurança da instituição, que contemple os principais aspetos da segurança (confidencialidade, integridade, disponibilidade e não repúdio).

Verifica-se ainda que, no que toca ao processo de registo dos alunos, o mesmo é feito de forma correta, embora o processo de revogação do registo, após a saída dos alunos (conclusão do ensino), não o seja, o que leva a um maior gasto, embora não muito alto, pelo facto de a universidade ter que manter as contas dos mesmos. Isto é, um aluno ao ingressar na universidade, após efetuar o seu registo, é lhe atribuído automaticamente

uma conta de email, no office 365, onde tem direito a cinco instalações do office sem qualquer custo para o próprio. Caso as contas dos alunos que já não têm vínculo com a instituição, não sejam revogadas, e à medida que os anos passam e mais alunos entram para a mesma, são sempre aquelas contas que terão que ser mantidas a mais enquanto não houver revogação. Tudo isto está a ser gerido especialmente pela equipa do GDAE pois são eles que recebem os dados para a criação das contas. No caso dos emails é gerido pelo departamento de informática onde é também feita a gestão do acesso à rede wireless. Quanto aos acessos através do cartão, de cada aluno, é gerido por uma pessoa do gabinete de Unidade de Equipamentos e Instalações.

Para uma estratégia eficaz de segurança da informação, é preciso que haja cooperação de todos os funcionários e isso exige um empenho na consciencialização coletiva por parte do departamento de Recursos Humanos. É preciso fazer a distinção de um utilizador ativo e não ativo da rede, ou seja, há uma necessidade evidente de implementar o processo de revogação das contas dos alunos que já não se encontram vinculados à instituição.

3.6.7 Conformidade

Este ponto não será aprofundado neste trabalho apenas pelo facto de não haver tempo suficiente para o abordar pelo facto de ser um tema que atualmente está em evolução. Trata-se da legislação do Regulamento Geral de Proteção de Dados, RGPD, que será um tema muito importante para posteriormente incluir e desenvolver.

3.7 Conclusões

Resumidamente, a análise à situação atual mostra que a UMa, apesar de ter feito um forte investimento em equipamentos e na infraestrutura da rede apenas naqueles anos e em essencialmente duas fases, a partir dessa altura houve uma grande redução na melhoria dos equipamentos, da infraestrutura. No âmbito da segurança da informação, a forma de atuação revela-se ainda muito reativa. O estado atual da segurança da informação é completamente desconhecido, ou seja, não existe formação por parte dos utilizadores, técnicos, investigadores e etc… que evitem e que tenham certos cuidados com as suas atividades. Há, também, uma enorme falta de processos formais estabelecidos de aplicação de metodologias, orientados por requisitos de segurança e monitorizados para a deteção de falhas. Os processos informais que existem, nem sempre são aplicados na totalidade pois não há uniformização de procedimentos, por exemplo, quando dois técnicos realizam uma tarefa idêntica e ambos não seguem rigorosamente uma determinada ordem de planeamento, execução e implementação, acabam por criar e causar, com essas ações, um acréscimo de vulnerabilidades à instituição.

Claramente existe a necessidade de melhoria nos serviços de gestão de redes e serviços pois os métodos de gestão ainda se encontram dimensionados para uma rede mais simples e com menor número de equipamentos o que permite colocar maior pressão nos serviços e pouca flexibilidade e possibilidades na prevenção e resolução de diferentes situações, seja um problema ou o aparecimento de um novo requisito ou de um novo serviço.

Há uma necessidade lógica e evidente em definir uma política de segurança formal bem como documentar os processos para os vários contextos pois, até hoje, é inexistente.

É factual que de certa forma não há satisfação com a solução que têm implementada atualmente, a nível geral.

4. METODOLOGIA E ANÁLISE

Feita a caracterização à UMa, no capítulo anterior, principalmente à situação atual da rede da UMa, é possível comprovar que, apesar dos investimentos realizados ao longo dos anos, que se tornaram importantes para a evolução e atualização da rede, não houve um acompanhamento no estabelecimento e na implementação, quer de processos de segurança da informação, quer na definição das políticas de segurança. O que direta ou indiretamente contribui para uma maior ocorrência de vulnerabilidades e consequentemente a possibilidade de ocorrência de prejuízo para a UMa.

Tendo em conta a informação já obtida e identificada, achou-se por bem efetuar uma análise mais formal e mais concisa de forma a obter resultados mais fidedignos e objetivos. Desta forma foi realizada uma investigação na área de análise de segurança e análise dos riscos de segurança da informação com o propósito de encontrar um processo ou um procedimento que já tenha sido implementado, ou que seja conhecido e que possa ser seguido de forma a apresentar uma análise clara e objetiva dos principais riscos que a rede da UMa enfrenta.

A investigação ao estado da arte permitiu identificar duas normas, internacionalmente conhecidas e desenvolvidas, especificamente para a segurança da informação e gestão de risco que sugere e recomenda uma série de processos quer de planeamento, quer de verificação quer de implementação e quer de melhoria contínua, fundamentais para a segurança e proteção da informação, numa organização. São elas a norma ISO/IEC 27001:2013 – Sistema de gestão de segurança da informação – Requerimentos [5] e a norma ISO/IEC 27005:2011 – Gestão de risco de segurança da informação [8]. A norma ISO/IEC 27001:2013 especifica os requisitos para o estabelecimento, a implementação, a manutenção e a melhoria contínua de um SGSI. Para além de outros benefícios, a aplicação da mesma permite determinar e avaliar os riscos de segurança da informação a que a organização esteja sujeita, implementando procedimentos e mecanismos que permitam preservar a confidencialidade, a integridade e a disponibilidade da informação. A norma ISO/IEC 27005:2011 não providencia um método específico, mas fornece as diretrizes para o processo de gestão de riscos.

Em simultâneo, foi possível associar e complementar o processo das normas, de análise de segurança/risco, com um processo semelhante, encontrado no livro “Engenharia de Redes Informáticas” de Edmundo Monteiro e Fernando Boavida [3], num documento publicado online por Paulo Silva da UCEFF [48] e num outro documento “Implementação de uma Metodologia de Análise de Risco baseada na BS7799-3” de Tulio Valentim [49].

A análise de segurança e/ou análise dos riscos à rede da UMa não pode ser iniciada sem que antes se demonstre quais foram os processos baseados para a escolha e apresentação do processo que foi seguido.

4.1 Processos e análise

A norma ISO/IEC 27001:2013, abordada no estado da arte, sugere uma determinada sequência de processos de planeamento, implementação, avaliação e melhoria contínua, como ilustra a Figura 6, enunciada no estado da arte. Nela é possível verificar os vários processos necessários para a implementação e certificação de um SGSI e quais as normas correspondentes a esses mesmos processos.

Visto o principal objetivo do trabalho não ser preparar a UMa para ser certificada na norma ISO/IEC 27001, tendo obrigatoriamente que seguir todos os processos presentes na Figura 6, mas sim efetuar uma análise de segurança/risco à rede da UMa. Assim sendo, foram escolhidos os processos que se encontram na Figura 16. O motivo para a escolha desses processos, abaixo indicados, e que partiu da análise dos vários documentos, resultantes da investigação ao estado da arte ([3], [48] e [49]), para além das normas já mencionadas, foi o facto de haver a necessidade de encontrar casos em que já estivesse sido implementado algo semelhante.

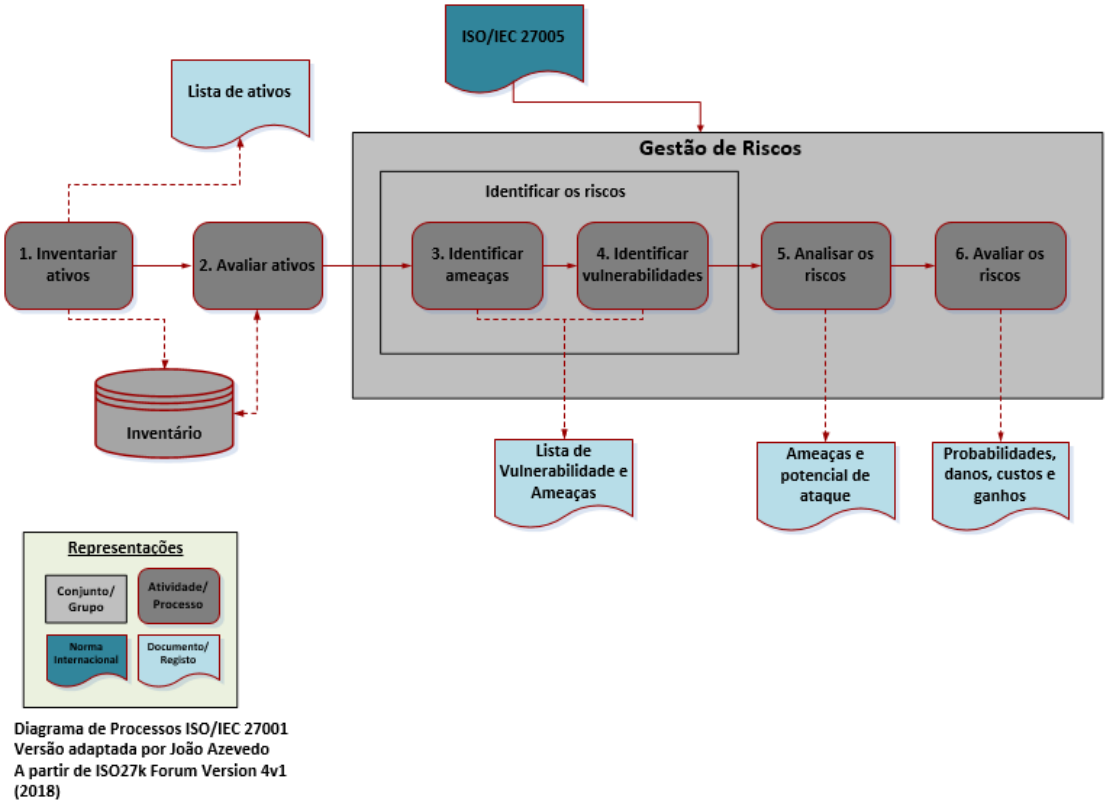


Figura 16 - Excerto do diagrama de processos (Anexo A – Diagrama de processos de um SGSI (ISO/IEC 27001)) correspondente aos processos da gestão de risco e restantes utilizados para a análise.

O primeiro processo consiste na realização de um **inventário dos ativos**, ou seja, consiste na identificação dos ativos da instituição, quanto ao tipo, e na demonstração de qual foi a metodologia utilizada na recolha dessa informação. O segundo processo, **avaliação dos ativos**, apesar de não fazer parte do diagrama de processos da norma ISO/IEC 27001, original, foi adicionado de forma a ser possível, mais à frente,

enquadrado na análise de impacto. Este processo pode ser feito segundo os seguintes parâmetros: custo de reparação, custo de recuperação, tempo de reparação, tempo de recuperação ou segundo o impacto sob os aspetos: confidencialidade, integridade e disponibilidade. Os seguintes encontram-se dentro do processo da norma ISO/IEC 27005 e não podem ser seguidos enquanto os dois anteriores não forem concluídos. O processo de gestão de riscos é constituído pela identificação dos riscos, associados à identificação das ameaças (terceiro processo) e à identificação das vulnerabilidades (quarto processo), pela **análise dos riscos**, associados à análise dessas ameaças e vulnerabilidades (quinto processo) e pela **avaliação dos riscos**, associados às probabilidades de ocorrência e ao impacto estimados (sexto processo).

Embora a próxima fase, tratamento do risco, correspondente ainda à parte da Gestão de riscos, da norma ISO/IEC 27005:2013, seja importante para o decorrer dos processos, escolheu-se não a abordar pois o principal objetivo era apenas a análise de segurança/risco à rede da UMa.

Desta forma, enumerados os processos escolhidos para a realização da análise de segurança/risco à rede da UMa, segue-se então a definição e a especificação dos mesmos, bem como a análise referente à UMa.

4.1.1 Inventário (identificação) dos ativos

Antes de abordar como deve ser seguido este processo, inventário dos ativos, é importante compreender "o que é um ativo?" e saber a sua dimensão no contexto da segurança da informação.

Um ativo, de acordo com a ISO/IEC 27001 e a ISO/IEC 27002, é qualquer coisa que tenha valor para a organização [5]. Ou seja, um ativo é caracterizado por todo o objeto, tangível ou intangível que uma empresa pode controlar. É qualquer coisa onde um incidente possa causar prejuízos tais como, perda de confidencialidade, perda de integridade e/ou perda de disponibilidade.

A norma ISO/IEC 27001:2013 clarifica que, na secção A.8.1.1 da mesma," os ativos associados às informações e aos recursos de processamento de informações devem ser identificados e deve ser elaborado e mantido um inventário desses ativos", na secção A.8.1.2, "os ativos registados nesse inventário devem ter um responsável" e na secção A.8.1.3, "as regras para o uso aceitável dos ativos devem ser identificadas, documentadas e implementadas", como mostra a Figura 17.

A.8	Asset management	
A.8.1	Responsibility for assets	
Objective: To identify organizational assets and define appropriate protection responsibilities.		
A.8.1.1	Inventory of assets	*Control* Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.
A.8.1.2	Ownership of assets	*Control* Assets maintained in the inventory shall be owned.
A.8.1.3	Acceptable use of assets	*Control* Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.

Figura 17 - Excerto retirado do Anexo A, tabela A.1, correspondente à secção A.8 Gestão dos Ativos [5].

De igual forma, a norma ISO/IEC 27005:2011 [8], no Anexo B, mais precisamente na página 33, apresenta o exemplo de identificação dos ativos, onde diz que existem dois tipos de ativos que podem ser distinguidos em: ativos primários e ativos de suporte e infraestrutura. Nos **ativos primários** encontram-se os processos e atividades de negócio e a informação. Os processos e atividades de negócios podem compreender: processos cuja interrupção, mesmo que parcial, impossibilite a organização de prosseguir com o seu negócio ou a sua missão; processos que contêm procedimentos secretos ou que envolvam tecnologia proprietária; processos que, em caso de modificação, podem afetar significativamente o cumprimento do negócio ou da missão da organização; processos necessários para que a organização fique em conformidade com os requisito contratuais, legais ou regulatórios. Quanto à informação pode compreender: a informação vital para o exercício das atividades da organização; a informação de caráter pessoal, como as definidas em leis nacionais de privacidade; a informação estratégica necessária para o alcance dos objetivos determinados pelo direcionamento estratégico; a informação de alto custo, cuja recolha, armazenamento, processamento e transmissão demanda um longo tempo ou incorre num alto custo de aquisição. Nos **ativos de suporte e infraestrutura** encontram-se o hardware, o software, a rede, os recursos humanos, as instalações físicas e a estrutura da organização.

Antes de efetuar o inventário dos ativos (lista dos ativos) foi necessário primeiro proceder à recolha de informação que tornasse possível a elaboração da lista dos ativos. Para isso houve a necessidade de aplicar as técnicas de análise documental e essencialmente a realização de entrevistas semiestruturadas, como já mencionadas no capítulo anterior. A justificação para o uso dessas técnicas prende-se com o facto de, posteriormente à investigação de quais as técnicas deveriam ser utilizadas para melhor corresponder aos objetivos propostos e ao tempo definido para a realização do trabalho, estas foram as que mais reuniam as melhores condições para a recolha da informação. É importante salientar a importância do detalhamento destas informações sobre os ativos. Neste caso foram apenas recolhidas e serão também demonstradas as informações que na altura foram pertinentes, com certeza existiriam muitas mais.

Procedendo-se então ao processo de inventário dos ativos da UMa, posteriormente à recolha de informação, obteve-se os seguintes resultados.

Quanto aos ativos primários, relativamente a:

Processos e atividades de negócio

- Sistema Financeiro;
- Sistema Documental.

Informação

- Sistema de Informação Académico.

Quanto ao inventário dos ativos de suporte e infraestrutura, da UMa, efetuou-se uma generalizada e mais discreta identificação de ativos:

Hardware (todos os elementos que dão suporte aos processos)

- Todos os servidores, todos os computadores fixos utilizados nas instalações da UMa, todos os computadores portáteis pessoais (funcionários, docentes, alunos…), impressoras, discos de rede, unidades de disco amovíveis e cartões de memória;

Software (todos os programas que contribuem para a operação de um sistema de processamento de dados)

- Todos os sistemas operativos, todos os programas de serviço, de manutenção ou de administração, todos os programas para gestão de base de dados, todos os programas de diretório e de servidores web, todos os programas de contabilidade e todos os programas desenvolvidos na UMa;

Rede (todos os dispositivos de telecomunicação utilizados para interligar computadores ou quaisquer outros elementos remotos de um sistema de informação)

- O suporte a cablagem, todos os equipamentos e interfaces de rede (routers, switches, modems, repetidores, access points), todos os protocolos que permitem a interligação dos sistemas de informação, e todos os serviços de assistência remota e videoconferência;

Recursos humanos (todas as classes de pessoas envolvidas com os sistemas de informação)

- Todos os administradores e dirigentes responsáveis pelos ativos primários (todo o quadro de administração desde o reitor aos administradores da rede), todos os utilizadores que têm acesso aos sistemas para tratamento da informação (pessoal dos recursos humanos, da secretaria, dos vários gabinetes como o Gabinete de apoio ao aluno), toda equipa de desenvolvimento de sistemas e toda equipa de técnicos que tem acesso privilegiado aos sistemas de forma a poder desempenhar as suas funções nas várias áreas (manutenções);

Instalações físicas (todos os locais e meios físicos necessários para as operações)

- Todo o ambiente externo onde as medidas de segurança da instituição não podem ser aplicadas (instalações, edifícios, prédios exteriores ao edifício da

instituição), todas as zonas internas limitadas por linhas de proteção física que criam partições dentro das instalações (salas, gabinetes dos docentes, laboratórios e gabinetes das diversas áreas de gestão), todo o serviço essencial (energia elétrica), todos os serviços de comunicação (fibra ótica da operadora) e todos os serviços de infraestrutura (ar condicionado, agua, saneamento e esgoto);

Estrutura da organização (descrição da estrutura da organização, compreendendo as hierarquias de pessoas que executam as tarefas e os procedimentos que controlam essas hierarquias)

- Todas as autoridades do corpo administrativo da UMa, toda a estrutura organizacional da instituição (reitor, pessoal do secretariado, etc…), toda a estrutura de organização de projetos e todas as entidades subcontratadas para os mais diversos fornecimentos de serviços e recursos (serviço de assessoria, serviços de manutenção ar condicionado, etc…);

A lista de todos os ativos identificados e que foram possíveis recolher encontram-se no Anexo C – Lista de ativos da UMa.

Toda esta lista de ativos carece, em grande parte dos ativos apresentados, de definição de responsáveis por ativo ou grupo de ativos. Dessa forma e para completar o processo de inventário de ativos, falta apenas a definição de responsabilidades onde existem três elementos a definir: um **proprietário**, um **custodiante** e um **administrador**. O proprietário deve ser o gestor de nível mais alto envolvido com o ativo, na medida em que é responsável por tomar decisões pelo ativo, é responsável pela classificação e é responsável por responder pelo ativo na organização. O custodiante, que pode ser considerado um guarda do ativo, é geralmente um subordinado direto do proprietário e tem como funções receber a responsabilidade do proprietário, responder pelo ativo, após o proprietário e é a pessoa que está mais diretamente relacionado com o ativo em questão. Já o administrador é considerado um utilizador do ativo, embora com mais responsabilidades pois é quem faz a manutenção do ativo, é responsável por manter o correto funcionamento do ativo, mas, é a pessoa que não decide nem responde pelo ativo.

Assim sendo, a pessoa que supostamente atribuirá esses três cargos, na UMa, provavelmente será o máximo responsável pela rede da UMa.

A Tabela 7 indica de que forma podem ser atribuídos os cargos e os responsáveis pelos ativos.

Tabela 7 - Exemplo de definição de cargos e responsabilidades para cada ativo.

Tipo de Ativo	Subtipo	Designação do Ativo	Local do Ativo	Cargo	Responsável
Primário	Informação	Base dados de ficheiros dos alunos	Sala 2.20	Administrador	Tiago José
Suporte e Infraestruturas	Software	Sistema operacional - Linux	Sala 1.10	Proprietário	João P. Silva

Na tabela consta o "tipo de ativo", que pode ser primário ou de suporte e infraestruturas, o "subtipo" que corresponde aos elementos de cada tipo de ativo, por exemplo, o tipo de ativo pode ser primário, mas tanto pode corresponder a processos e atividades de negócio como a informação. Mais, o tipo de ativo pode ser de suporte e infraestruturas e pode corresponder a hardware, ou a software, ou a rede, ou a recursos humanos, ou a instalações físicas ou a estrutura de organização. A terceira coluna corresponde à designação do ativo, nesta parte convém ser uma designação única e específica de forma a não confundir com outros ativos. A quarta coluna corresponde à localização do ativo, ou seja, em qual sala, laboratório, ou até andar o ativo se encontra. A quinta coluna corresponde ao cargo da pessoa que será responsável pelo ativo, poderá ser administrador, custodiante ou proprietário. A sexta e última coluna corresponde à identificação da pessoa que será responsável pelas funções atribuídas. Poderá haver repetição dos nomes caso a mesma pessoa tenha cargos diferentes e consequentemente mais ativos atribuídos.

Para este efeito, e visto que a equipa de gestão e administração da rede é constituída por sensivelmente sete pessoas (engenheiros, técnicos superiores e técnicos), e que as restantes equipas das mais variadas áreas são pequenas, considerou-se como responsável por um ativo a pessoa que exerce operações e que está em contacto direto com esse mesmo ativo ou grupo de ativos. Ou seja, se um determinado ativo for utilizado por várias pessoas (técnicos e/ou engenheiros), a responsabilidade irá cair sempre sobre o gestor do ativo.

4.1.2 Avaliação dos ativos

O processo seguinte, após a identificação dos ativos da UMa, é determinar a escala de medida a ser utilizada e os critérios que permitam associar um ativo a um valor nessa escala. Ou seja, o próximo passo passa pela realização da avaliação dos ativos enumerados anteriormente com o objetivo de se obter o nível de risco associado a cada um deles. Poderiam ter sido utilizados vários critérios que se encontram, alguns deles, mencionados no anexo B da norma ISO/IEC 27005:2011 [8], onde são sugeridos os seguintes:

- **Custo de aquisição**, tendo em conta o investimento realizado;
- **Custo de reparação**, tendo em conta o valor que é necessário investir para a sua substituição ou arranjo;
- **Custo de recuperação**, tendo em conta o valor que é necessário gastar (gastos operacionais) na contratação da equipa para fazer o trabalho;
- **Tempo de reparação**, tendo em conta o tempo que demora a efetuar manutenção do ou dos equipamentos;
- **Tempo de recuperação**, tendo em conta o tempo que demora os equipamentos a estarem operacionais (tempo que leva a ser detetado uma falha somado ao tempo que leva a equipa a concluir o trabalho);
- **Reputação da instituição**, tendo em conta a sua imagem institucional perante os restantes (parceiros, fornecedores e restantes entidades).

O administrador ou outra pessoa responsável pelo ou pelos ativos, deve efetuar a avaliação de um ou mais ativos baseando-se pelo menos em um ou mais critérios de forma a poder, posteriormente, justificar o porquê do resultado obtido.

Devido à diversidade dos ativos que possam ser encontrados na organização, é provável que alguns deles, aqueles que possuam um valor monetário conhecido, possam ser avaliados através do valor monetário em euros, mas outros, aqueles com um valor expresso em termos qualitativos, talvez tenham que ser avaliados através de uma lista de valores a serem selecionados, por exemplo numa escala: "muito baixo", “muito alto”, etc…. A decisão de ser utilizada uma escala qualitativa ao invés de uma escala quantitativa ou vice-versa, depende da preferência da instituição ou do responsável ou administrador do ou dos ativos, porém, convém que seja pertinente, aos ativos em avaliação, porque ambos os tipos de avaliação podem ser utilizados para se determinar o valor de um mesmo ativo.

Embora houvesse a possibilidade de aplicar uma escala nesta situação, optou-se por representar essa avaliação dos ativos em texto, com o intuito de ser mais específico quanto ao valor dos ativos e o impacto que tem para a instituição. Essa avaliação encontra-se no Anexo D – Avaliação dos ativos.

A avaliação dos ativos, realizada com recurso aos dados quantitativos, permitiu chegar à conclusão que em caso de algum incidente, os ativos de maior valor possam ter um impacto maior no bom funcionamento da instituição.

4.1.3 Identificação das ameaças (Identificação do Risco)

A maior parte dos sistemas (principalmente os sistemas de informação) das empresas estão vulneráveis a diversas ameaças que podem causar danos aos ativos da empresa como roubos eletrónicos, sabotagem, espionagem, inundação, incêndio e ataques de hackers e crackers. Só o facto de a informação ser, hoje em dia, um ativo de fundamental importância para qualquer empresa ou organização, a mesma está constantemente sob

ameaças. Às vezes só o simples facto de as sabermos identificar, monitorizar e amenizá-las com controlos, evitamos a exposição principalmente para o exterior. Daí ser importante ter em conta o conceito e conhecimento adequado para tentar minimizar todo o risco que uma ameaça pode provocar.

A norma ISO/IEC 27000, no capítulo correspondente aos termos e definições, termo com a identificação 2.83, indica que "uma ameaça é uma causa potencial de um incidente indesejado, que pode resultar em danos num sistema ou organização". Ou seja, uma "simples" ameaça pode ser qualquer ação, acontecimento ou entidade que age sobre um ativo ou até sobre uma pessoa, através de uma ou mais vulnerabilidades e que consequentemente gera um determinado impacto na organização.

De acordo com a norma ISO/IEC 27005:2011 [8], no oitavo capítulo, ponto 8.2.3, refere que "as ameaças podem ser de origem natural, origem humana e podem ser acidentais ou intencionais". A mesma refere ainda que deve ser criada uma lista de ameaças com a identificação do tipo e da origem das ameaças.

Desta forma, a Tabela 8, exemplifica como devem ser identificadas as ameaças.

Tabela 8 - Exemplo de identificação de ameaças.

Tipo	Ameaça	Origem (*)
Falha técnica	Saturação do sistema de informação	A, I
Comprometimento da informação	Indisponibilidade de recursos humanos	A, I, N
Ação não autorizada	Apropriação indevida de informação	I

A Tabela 8 contém três exemplos de ameaças típicas que as organizações enfrentam, onde na mesma é mencionado o tipo de ameaça, a descrição da ameaça e qual a sua origem. A terceira coluna da tabela diz respeito à origem da ameaça, onde no qual pode ser A (acidental), I (Intencional) ou N (natural). A letra A é utilizada para indicar as ações de origem humana que podem comprometer acidentalmente os ativos, a letra I é utilizada para indicar as ações intencionais direcionadas contra os ativos e a letra N é utilizada para todos os incidentes que não são provocados por ação humana.

A título de exemplo, e de forma a entender qual a origem das ameaças, a Tabela 9 mostra exemplos de ameaças causadas por seres humanos, de forma intencional, onde encontram-se representadas a fonte de ameaça, a motivação e as possíveis consequências das mesmas.

Tabela 9 - Tabela de exemplo da origem de ameaça intencional, motivação e consequências.

Fontes de ameaça	Motivação	Consequências
Hacker/Cracker	Desafio Dinheiro Protesto Rebelia	Hacking Negação de serviço Acesso não autorizado Invasão de sistemas
Espiões	Vantagem competitiva Espionagem económica	Garantir uma vantagem política Exploração económica Engenharia social Invasão de privacidade Furto de informações
Pessoas: sem formação, insatisfeitas, negligentes, demitidas, etc…	Curiosidade Egocentrismo Ganhos financeiros Vingança	Chantagem Busca de informação sensível Roubo de ativos Corrupção de dados Desvio de informação Acessos não autorizados a sistemas

Quanto à identificação das ameaças aos ativos da UMa, a Tabela 10, representa algumas ameaças identificadas relativamente a um dos ativos definidos no Anexo C – Lista de ativos da UMa, Sistema Financeiro, onde esta identificação resultou da recolha de informação através de entrevistas semiestruturadas e de questionários realizados, presentes no Anexo B – Recolha de informação da rede da UMa, aos responsáveis e administradores da rede da UMa.

Tabela 10 - Identificação das ameaças aos ativos (exemplo para o ativo escolhido - Sistema Financeiro).

Ativo	Tipo de ameaça	Ameaça	Origem (*)
Sistema Financeiro	Evento Natural	Tsunami	N
		Erupção vulcânica	N
	Ameaça Física	Corte no acesso à internet	A, I
		Acidente com equipamento	A, I
	Ação não autorizada	Destruição equipamento	I
		Processamento ilegal de dados	I
	Comprometimento da informação	Destruição de registos	A, I
		Engenharia social	I
	Falha técnica	Saturação do sistema de informação	A, I
		Falha no equipamento	A
	Comprometimento de funções	Indisponibilidade de recursos humanos	A, I, N
		Repúdio de ações	I

(*) A (acidental), I (intencional) e N (natural)

De forma a simplificar ao máximo o processo da identificação das ameaças utilizou-se a representação da Tabela 11 onde mostra um exemplo aplicado a um dos ativos identificados como relevante, o sistema de informação académico.

Tabela 11 - Exemplo utilizado para a representação das ameaças aos ativos, neste caso ao Sistema de Informação Académico..

Ativo	Ameaça
Sistema de Informação Académico	Avaria de equipamento (servidor)
	Ataque informático (ex.: DoS)
	Perda de informação
	Sabotagem
	Ataque através de software (ex.: vírus)
	Corte na rede local
	Corte no acesso à internet
	Acidente com equipamento
	Sobrecarga de corrente
	Avaria de equipamento (ar condicionado)
	Acesso não autorizado
	Erros Programas (configurações)

A continuação da Tabela 11 encontra-se no Anexo E – Tabela das ameaças aos ativos escolhidos.

É importante salientar que apesar da identificação feita aos ativos (sistema financeiro, sistema documental e sistema de informação académica) como relevantes, os mesmos envolvem, internamente, outros ativos de dimensão mais baixa. Isto para dizer que o sistema financeiro engloba não só o uso de equipamento (hardware) como também aplicações (software) onde estas também acabam por ser ativos.

4.1.4 Identificação das vulnerabilidades (Identificação do Risco)

A identificação das vulnerabilidades da UMa passou, numa primeira fase, pela compreensão da definição de "vulnerabilidade" no contexto da segurança da informação.

Recorrendo à norma ISO/IEC 27000, vulnerabilidade é "uma fraqueza de um ativo ou de um controlo que pode ser explorada por uma ou mais ameaças". Dito por outras palavras, uma vulnerabilidade é uma fragilidade ou falha num ativo que pode ser explorada por uma ou mais ameaças que afeta diretamente a confidencialidade, a integridade e a disponibilidade. O facto de existir uma vulnerabilidade por si só não causa prejuízo por esta ser um elemento passivo, no entanto, no caso de haver uma ameaça presente já irá haver prejuízo. É importante realçar que uma vulnerabilidade é uma propriedade do ativo e não uma ação ou um evento. O próximo exemplo, ilustrado na figura seguinte, permite compreender o conceito de vulnerabilidade assim como de

ameaça. Na Figura 18 encontra-se uma parede que está a servir de barreira entre a água e o homem, ou seja, a água, à esquerda da parede, é uma ameaça para o homem que se encontra à direita da parede. Perante esta situação é possível observar que existe duas possibilidades: a água pode subir, podendo transbordar a parede; ou então pode ficar abaixo da altura da parede, fazendo com que esta se parta. Desta forma, a ameaça de dano é o potencial para o homem se molhar, magoar-se ou afogar-se. Enquanto a parede estiver intacta, a ameaça não é concretizada.

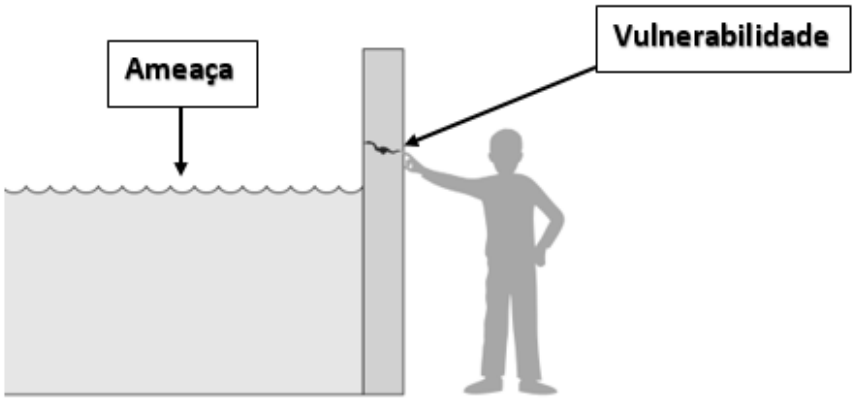


Figura 18 – Vulnerabilidade vs Ameaça [50].

No entanto, é possível observar que existe uma pequena fenda na parede, que representa uma vulnerabilidade, e que esta ameaça a segurança do homem. Desta forma, em caso de o nível da água subir ou ultrapassar a fenda, a mesma irá explorar a vulnerabilidade e consequentemente prejudicará o homem.

As vulnerabilidades podem ser classificadas como:

- **Físicas** – Exemplos: a não implementação de câmeras de vigilância, a não implementação de alarmes, extintores, detetores de fumo, a não garantia de seguro, etc…
- **Naturais** – Exemplos: a falta de prevenção para a humidade, acumulação de poeira, inundações.
- **Hardware** – Exemplos: a má utilização de equipamentos, a falta de manutenção, o erro de instalação, o desgaste de peças ou materiais, etc…
- **Software** – Exemplos: erros de configuração, defeitos de software, falta de requisitos de segurança, a não atualização de software, etc…
- **Humanas** – Exemplos: falta de formação, a falta de consciencialização, os erros ou omissões dos técnicos, o não executar procedimentos de segurança, as greves, etc…
- **Organizacionais** – Exemplos: a indefinição de responsabilidades, a inexistência de controlos físicos, a inexistência de monitorização, a inexistência de políticas de segurança, a inexistência de auditorias, a inexistência de análises críticas, a inexistência de planos de continuidade, etc…

Relativamente ao processo propriamente dito de identificação de vulnerabilidades, o mesmo pode ser feito por meio de duas técnicas: técnica de identificação através da tecnologia e técnica de identificação através da gestão.

A **técnica de identificação através da tecnologia** indica que a identificação pode ser feita com recurso a: ferramentas automatizadas de vulnerabilidades, testes de invasão, análise da segurança de sistemas, entre outros.

A **técnica de identificação através da gestão** indica que a identificação pode ser feita com recurso a: entrevistas com os administradores e gestores, questionários de segurança, inspeção física, análise de documentos, entre outros.

A técnica de identificação de vulnerabilidades utilizada foi através da gestão, com recurso a entrevistas com os administradores e gestores da rede da UMa e também com recurso a alguns questionários, onde esses documentos, desenvolvidos e utilizados para as entrevistas e questionários, encontram-se no Anexo B – Recolha de informação da rede da UMa.

Escolhida a técnica de identificação de vulnerabilidades resta apenas elaborar uma tabela na qual estejam representados os ativos, as ameaças a esses ativos e as vulnerabilidades associadas a esses ativos. Desta forma, segue na Tabela 12 um exemplo das vulnerabilidades afetas às ameaças definidas para o ativo escolhido (sistema de informação académico).

Tabela 12 - Identificação das vulnerabilidades dos ativos - Exemplo.

Ativo	Ameaças	Vulnerabilidades
Sistema de Informação Académico	Acesso não autorizado	Controlos de acesso inadequados
		Não aplicação de políticas
		Equipamento desatualizado
		Mecanismo de acesso simples
	Erros Programas (configurações)	Falta de procedimentos
		Falta de conhecimento
		Parâmetros incorretos
		Inexistência de cópias
	Ataque (vírus)	Falta de conhecimento
		Falta de planeamento de contingência
		Falta de política de segurança
		Bugs em aplicações

Na Tabela 12 encontram-se representadas algumas ameaças ao ativo escolhido para o exemplo, sistema de informação académico, de forma a demonstrar as vulnerabilidades que os mesmos apresentam. A restante tabela encontra-se no Anexo F – Tabela das vulnerabilidades aos ativos escolhidos.

É importante referir que a identificação das vulnerabilidades externas não é suficiente, é de extrema relevância proceder também à identificação das vulnerabilidades internas.

A Fortinet, empresa multinacional da califórnia que desenvolve e comercializa software, produtos e serviços de Cibersegurança como firewalls, antivírus, entre outros diz que "cerca de 80% dos incidentes de Cibersegurança industrial que ocorrem nas organizações com infraestruturas críticas são provocados por questões internas como erros humanos involuntários na configuração de software ou no funcionamento inadequado de protocolos de rede." [51].

4.1.5 Análise dos riscos

Indica a norma ISO/IEC 27005:2011 [8], na secção 8.3.4, precisamente no inicio da página trinta, que uma análise do risco é responsável por designar "valores para a probabilidade e para as consequências de um risco" e que "o risco estimado é uma combinação da probabilidade de um cenário de incidente e das suas consequências". Desta forma, antes de determinar a probabilidade e o impacto é necessário definir qual das metodologias, qualitativa ou quantitativa, a aplicar para definir a escala da probabilidade e/ou do impacto.

Neste processo de análise do risco, optou-se pela metodologia quantitativa, de forma a poder demonstrar uma maior precisão na análise e facilitar a tomada de decisão, embora também possam ser utilizadas em simultâneo as duas metodologias.

A norma ISO/IEC 27005:2011 [8], na secção 8.3.2, precisamente no inicio da página vinte e nove, indica que "convém que as consequências expressas em tempo e valor financeiro sejam medidas com a mesma abordagem utilizada para a probabilidade da ameaça e das vulnerabilidades" a mesma refere ainda que "a consistência deve ser mantida em respeito à abordagem quantitativa ou qualitativa". Assim sendo, foram definidas as seguintes escalas com valores numéricos, indicando valores monetários, de forma a facilitar a tomada de decisão.

Para a **probabilidade de ocorrência** foi estabelecida a escala da seguinte forma: quanto maior for a probabilidade de ocorrência, maior será a classificação.

Para o **impacto** foi estabelecida a escala em termos de custo/danos/ganho da seguinte forma: quanto maior for o impacto, maior será a classificação.

Desta forma, a Tabela 13 e a Tabela 14, apresentadas de seguida, representam as escalas de probabilidade de ocorrência e de impacto, definidas para o efeito.

Tabela 13 - Escala de probabilidade de ocorrência.

Classificação	Probabilidade de ocorrência
1	1 vez em 10000 anos
2	1 vez em 1000 anos
3	1 vez em 100 anos
4	1 vez em 10 anos
5	1 vez por ano

6	1 vez por mês
7	1 vez por semana
8	1 vez por dia
9	1 vez por hora
10	1 vez por minuto

Tabela 14 - Escala de impacto (custo/dano/ganho).

Classificação	Impacto (custo/dano/ganho)
1	0 €
2	1 €
3	10 €
4	100 €
5	1.000 €
6	10.000 €
7	100.000 €
8	1.000.000 €
9	10.000.000 €
10	danos totais

O processo de análise do risco combina a estimativa da probabilidade de ocorrência com o impacto resultante. Assim sendo, para a realização da análise do risco, considerou-se a Tabela 8Tabela 10, elaborada na identificação das ameaças, e construiu-se a Tabela 15 como exemplo.

Tabela 15 - Análise do risco (exemplo).

Tipo	Ameaça	Origem (*)	Probabilidade/Impacto
Falha técnica	Saturação do sistema de informação	A, I	5/5
Comprometimento da informação	Indisponibilidade de recursos humanos	A, I, N	6/5
Ação não autorizada	Apropriação indevida de informação	I	7/4

(*) A (acidental), I (intencional) e N (natural)

Da tabela anterior, verifica-se que, a probabilidade de ocorrência de uma falha técnica, como é o caso da saturação do sistema de informação, ainda que pouco provável, pois o histórico de falhas deste género, tanto a nível intencional como a nível acidental, desta forma tem um custo na ordem dos mil euros.

Quanto à indisponibilidade dos recursos humanos, embora tenha um custo na casa dos mil euros, já tem a tendência de ocorrer mais vezes em relação à ameaça anterior.

Relativamente à apropriação indevida de informação, a probabilidade de ocorrência já é maior pois pelo historial é uma das ameaças que normalmente qualquer empresa enfrenta semanalmente ou até diariamente e, por não ter muita importância, visto não dar para fazer muita coisa com o tipo de informação, o custo acaba por ser baixo.

A continuação da análise do risco encontra-se no Anexo G – Tabela da Análise do risco.

Através da análise do risco a instituição fica assim a conhecer o nível de risco de modo a posteriormente ter a oportunidade de decidir o que vai fazer em relação a cada risco: reduzir, aceitar, evitar e/ou transferir.

4.1.6 Avaliação dos riscos

Com os resultados obtidos nos processos anteriores, já é possível iniciar o processo de avaliação dos riscos, processo que é responsável por ordenar os riscos por prioridade, de acordo com os critérios de avaliação de riscos definidos. É importante salientar que o processo de avaliação dos riscos é fundamental para o gestor de segurança pois é através dos resultados deste processo que será baseado o planeamento de segurança.

A norma ISO/IEC 27005:2011 [8], na secção 8.4, mais precisamente na página 30, diz que "a avaliação dos riscos usa o entendimento do risco obtido através da análise de riscos para a tomada de decisões sobre ações futuras" e que para a avaliação dos riscos pode-se fazer uso dos "métodos ou abordagens selecionados abordados no Anexo E".

Assim sendo, e com recurso ao "Anexo E" da norma, utilizou-se a matriz de risco apresentada na "Tabela E.1 b)" de forma a poder avaliar os resultados da análise do risco, processo anteriormente abordado. A Tabela 16 representa assim a matriz de risco, onde mostra a relação entre a probabilidade de ocorrência e o impacto estimado, na escala quantitativa.

Tabela 16 - Matriz de Risco.

		Impacto									
		1	2	3	4	5	6	7	8	9	10
Probabilidade de ocorrência	1										
	2										
	3										
	4										
	5										
	6										
	7										
	8										
	9										
	10										

Nesta tabela, o risco resultante foi medido numa escala de 1 a 10 onde esta escala de risco foi posteriormente convertida numa classificação simples e mais genérica, com o propósito de identificar bem os níveis de risco, obtendo-se o seguinte:

- Nível de risco baixo (a verde): 1 – 6
- Nível de risco médio (a laranja): 7 – 8
- Nível de risco alto (a vermelho): 9 – 10

Definiu-se ainda, na Tabela 17, a prioridade de intervenção, para esses níveis de risco, assim como estabeleceu-se também um prazo genérico, meramente representativos, sendo que esses prazos e prioridades requerem sempre a aprovação do ou dos gestores da rede e/ou da administração da instituição.

Tabela 17 - Atribuição da prioridade de intervenção e do prazo, em relação aos níveis de risco.

Nível de Risco	Intervenção	Prazo
Baixo	Não prioritária	6 meses
Médio	Programada	3 meses
Alto	Prioritária	Imediato

Segundo a norma ISO/IEC 27005:2011, na secção 8.1, mais precisamente no fim da página 21, o processo de avaliação de risco termina quando é obtida "uma lista de riscos avaliados e ordenados por prioridade, de acordo com os critérios de avaliação de riscos".

A avaliação dos riscos da UMa encontra-se no Anexo H – Avaliação do risco.

Finalizado o processo de avaliação é possível especificar as ações necessárias para a mitigação dos riscos, seguindo a priorização qualitativa. Identificado o nível de risco e a sua prioridade, antes de prosseguir para a próxima fase é importante referir que é necessário reavaliar os riscos periodicamente, independentemente de haver alterações ou não.

Identificados os problemas da UMa e analisados e avaliados, optou-se por escolher os que mais se destacam, não só pelo nível de risco que apresentam, mas por terem sido primeiramente abordados e de certa forma assinalados quando decorreram as entrevistas. A lista que apresenta os problemas que deverão ser resolvidos para que o nível de risco da instituição seja o mais baixo possível, encontra-se no Anexo I – Lista dos Problemas da UMa relevantes.

4.2 Conclusões

Neste capítulo foi proposta e implementada uma metodologia (conjunto de processos) para a análise de segurança/riscos, baseada essencialmente na norma ISO/IEC 27005 e na norma ISO/IEC 27001. Com o objetivo de avaliar todos os problemas e desafios da rede da UMa, para posteriormente tentar solucionar alguns ou a maior parte deles, esta metodologia, identificou ativos, ameaças e vulnerabilidades através da recolha de informações, por meio de entrevistas e questionários. Desta forma, e perante os dados recolhidos, as estimativas dos riscos refletem alguma confiabilidade na análise e avaliação efetuadas, permitindo deduzir os níveis de risco que a instituição enfrenta, priorizando-os. Esta não é uma metodologia científica que possa ser realizada através do uso de fórmulas matemáticas – é de natureza mais subjetiva.

Todos os processos apresentados, pela forma e pela sequência que foi proposta, não devem ser encarados como processos únicos para a obtenção dos resultados obtidos, embora a maior parte dos processos derivem de normas standard, de segurança da informação. Isto porque a decisão e a avaliação dos processos devem ser sempre as mais adequadas, apropriadas e adaptadas a cada situação e/ou cenário, por dependerem dos objetivos que cada organização pretende atingir e por dependerem muito da pessoa que realiza a análise e a avaliação, do seu domínio e do seu conhecimento na área. Não obstante, a metodologia proposta é constituída por seis processos dependentes uns dos outros que no final constituem uma ferramenta de medição para o próximo passo que é a implementação de políticas de segurança propostas para colmatar os problemas/desafios relevantes e identificados da rede da UMa.

5. PROPOSTA DE IMPLEMENTAÇÃO DA POLÍTICA DE SEGURANÇA

Nos capítulos anteriores, para além da caracterização da rede da UMa, procedeu-se à identificação dos desafios/problemas onde posteriormente foi apresentada uma análise e metodologia, a esses mesmos problemas, de forma a tentar resolvê-los. Posteriormente à fase de investigação, optou-se por utilizar as normas ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27005 por serem normas globalmente aceites e por se enquadrarem no tema abordado neste trabalho.

Tendo em consideração essas normas e através de outras referências, correlacionou-se os métodos e/ou processos utilizados em cada um, obtendo-se o conjunto de processos, proposto e utilizado, para a análise e para a avaliação dos desafios/problema da reda da UMa.

Posteriormente à identificação, análise e avaliação feita aos problemas da UMa, constatou-se que havia a necessidade de implementar controlos de forma a mitigá-los. Desta forma, foram analisados e associados aos domínios da norma ISO/IEC 27002 e controlos da norma ISO/IEC 27001, com o intuito de apresentar a proposta de melhoria para a rede, que consiste na criação de um documento de política de segurança.

Dos 14 domínios existentes na referida norma, e por serem aqueles os problemas escolhidos, optou-se por abordar apenas quatro (política de segurança da informação; organização de segurança da informação; controlo de acesso; segurança física e ambiental) pelo facto de não só serem os domínios mais próximos como solução aos problemas apresentados, mas também pelo facto de o tempo para a sua completa implementação (restantes domínios) exceder largamente o prazo definido para este trabalho. Estes domínios correspondem, respetivamente, às secções A.5, A.6, A.9 e A.11 da mesma norma.

Nos seguintes subcapítulos são abordados: o conceito de política de segurança e a importância que tem para uma organização; intenção da política de segurança; os controlos abordados em cada um dos subcapítulos correspondentes às secções da norma e por fim a conclusão ao capítulo.

5.1 Conceito

O termo “política” ou até “política de segurança” tem vários significados totalmente diferentes uns dos outros, dependendo do contexto a que é aplicado. Por exemplo, no contexto político, uma política é um plano ou curso de ação, de um governo ou partido político, destinado a influenciar e determinar decisões, ações e outros assuntos. No contexto deste trabalho, uma política de segurança é um conjunto de regras estabelecidas que fornecem orientação na proteção dos ativos de uma organização. Ou

seja, é a base de tudo o que esteja relacionado com a proteção dos bens de uma organização e a sua conceção é essencial para a segurança da informação em todas as áreas de uma organização, uma vez que é ela que define as normas, processos, procedimentos e responsabilidades a serem adotadas a fim de garantir o controlo da segurança da organização. É importante referir que o principal objetivo da segurança da informação é a proteção da confidencialidade, integridade e disponibilidade da informação e do sistema de informação, seja no processamento, na transição ou no armazenamento da mesma, através de vários elementos como por exemplo a aplicação de políticas, programas educacionais e/ou formações de consciencialização.

Para além de definir regras, processos e procedimentos, é um documento que deve incluir procedimentos disciplinares no caso da violação das regras definidas na política, pela organização.

A política de segurança deve ser considerada como um documento vivo pelo facto de as mesmas exigirem constantes modificações e manutenções conforme as necessidades da organização. E é escrita com o propósito de apoio à missão, visão e planeamento estratégico de cada organização [52].

Uma boa política é aquela que contém regras, processos, procedimentos bem enquadrados, bem explícitos, que é breve, clara, objetiva e concisa. Deve ser fácil de ler e de interpretar assim como deve ser o mais simples possível de forma a poder ser compreendida por todos.

Entendido o conceito, a importância e o objetivo da política de segurança, é importante sabê-la como implementar. Os passos para uma boa implementação da política de segurança são: planeamento, elaboração, aprovação e formação.

No **planeamento** deve haver inicialmente uma reunião entre principalmente os gestores e as equipas técnicas de TI de forma a realizar-se a recolha e/ou levantamento completo de toda a informação e dados produzidos pela organização e utilizadores, afetos a ela, que devem ser protegidos. Em caso de existir algum tipo de documento semelhante a uma política, deve ser efetuada uma análise às falhas e aos pontos que sejam necessários aperfeiçoar para diminuir os riscos. Posteriormente, é fundamental que a diretoria e o conselho de administração da organização tenham conhecimento e aprovem o planeamento.

Na **elaboração**, é o momento em que as equipas especializadas delimitam as normas, os processos e os procedimentos, onde também são estabelecidas sanções e punições para quem as viole. Por exemplo, estabelecimento de regras e/ou limites para o acesso à internet, uso de emails e todas as demais medidas que todos (funcionários, colaboradores, entidades subcontratadas, etc…) devem seguir.

Na **aprovação**, passo posterior à elaboração da política, é o momento em que o documento, que contém a política da organização, deve ser submetido à aprovação da gestão de topo, podendo variar estas regras dependendo de cada organização.

Sinteticamente é o passo em que o documento deve ser aprovado por todas as entidades superiores (recursos humanos, diretoria e conselho de administração).

O último passo trata-se da **formação** e consciencialização de todos os intervenientes da organização (funcionários, colaboradores, entidades subcontratadas, etc…), isto porque são estes que estarão envolvidos direta e indiretamente com todas as regras contidas no documento. É importante, num primeiro momento, criar canais de comunicação com todos os intervenientes a fim de tirarem as suas dúvidas e estarem cientes e conscientes das regras que constam no documento.

5.2 Intenção da Política

Tendo em conta as atividades já realizadas nos capítulos anteriores, o levantamento dos problemas e desafios, situação atual, da rede da UMa (capítulo 3) e a análise feita aos mesmos (capítulo 4), a solução encontrada, e proposta, foi a de elaborar e implementar um documento de políticas de segurança de forma a poder mitigar o nível de risco que a instituição enfrenta.

Uma política de segurança deve ser criada com o objetivo de estabelecer regras a serem seguidas por todos, na UMa, que utilizam os recursos de informática disponíveis, de forma a que todos estejam conscientes sobre a importância da segurança da informação, contribuindo assim para o sucesso da instituição.

A investigação ao estado da arte permitiu identificar os vários domínios da norma ISO/IEC 27001 e da ISO/IEC 27002, assim como os controlos correspondentes. Posteriormente, foi feita a análise baseada nos contextos de segurança, abordados nos capítulos, anteriormente referidos, e optou-se por escolher quatro domínios para a elaboração das políticas. Foram escolhidos os seguintes:

Política de Segurança da Informação (correspondente ao domínio/secção A.5) – Atendendo à necessidade de proporcionar regras e apoio da gestão para a segurança da informação, de acordo com os requisitos da instituição.

Organização de Segurança da Informação (correspondente ao domínio/secção A.6) – Atendendo à necessidade de estabelecer um modelo de referência de gestão para iniciar e controlar a implementação e operação da segurança da informação dentro da instituição.

Controlo de Acesso (correspondente ao domínio/secção A.9) – Atendendo à necessidade de assegurar o acesso de utilizadores autorizados e prevenir o acesso não autorizado a sistemas e serviços.

Segurança Física e Ambiental (correspondente ao domínio/secção A.11) – Atendendo à necessidade de prevenir o acesso físico não autorizado principalmente às salas com material e equipamento sensível.

Nos subcapítulos seguintes são abordados os desafios/problemas pelo qual foram enquadrados no domínio correspondente onde também são detalhados os passos que levaram à elaboração do documento final de política de segurança, presente no Anexo J – Documento de Políticas de Segurança.

5.3 Política de Segurança da Informação

Tendo em conta a lista dos problemas da UMa, presente no Anexo I – Lista dos Problemas da UMa relevantes, os que se enquadram neste domínio são os seguintes:

- Inexistência de documento formal de política de segurança;
- O atual estado da segurança da informação ser desconhecido por não haver formação por parte dos utilizadores, investigadores, técnicos, funcionários, docentes e não docentes, etc…;
- Inexistência de realização de auditoria regular de forma a verificar o estado da segurança da informação da rede bem como de toda a instituição, embora esteja atualmente a ser realizada uma auditoria específica.

As principais situações anteriormente descritas, apesar de haverem outras, mas menos relevantes, foram tidas em consideração na elaboração da política de segurança, que se encontra no documento presente no Anexo J – Documento de Políticas de Segurança.

Desta forma, a definição da política de segurança da informação foi elaborada tendo em consideração as normas ISO/IEC 27001 e ISO/IEC 27002 e os controlos nelas contidos para corresponder às situações descritas anteriormente.

Os controlos utilizados para cobrir as situações descritas foram:

- A.5.1.1 – "Um conjunto de políticas para a segurança da informação deve ser definido, aprovado pela gestão, publicado e comunicado aos colaboradores e partes externas relevantes";
- A.5.1.2 – "As políticas para a segurança da informação devem ser revistas em intervalos planeados ou quando ocorrerem alterações significativas de modo a assegurar a sua contínua aplicabilidade, adequabilidade e eficácia".

No primeiro controlo contém as diretrizes para a **definição de segurança da informação**, os **objetivos** e **princípios** para orientar as atividades relacionadas à segurança da informação e a atribuição de **responsabilidades** gerais e específicas para a gestão de segurança da informação, para funções definidas.

No segundo controlo contém as diretrizes para a atribuição dos cargos afetos ao próprio documento de política de segurança, por exemplo, quem fica como proprietário da política, quem deve efetuar as revisões e quem deve aprovar.

Para a elaboração, propriamente dita, da política de segurança da informação assim como do documento, a investigação ao estado da arte permitiu identificar as normas ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27003 onde esta última, juntamente com a consulta de outras políticas institucionais, foram as responsáveis pela estrutura escolhida e proposta na definição da política onde, as restantes normas contribuíram com os controlos (definidos anteriormente para este caso).

A estrutura da política de segurança, realizada, é composta por:

- **Introdução** – apresenta uma breve contextualização sobre o tema.
- **Âmbito** – descreve os elementos abrangidos pela instituição.
- **Objetivos** – descreve o objetivo da instituição com a política.
- **Princípios** – descreve dos princípios que a instituição segue para alcançar os objetivos.
- **Referências Normativas** – descreve quais foram as normas utilizadas na elaboração da política.
- **Termos e Definições** – apresenta os termos e as suas definições fundamentais e a maior parte aplicados ao documento.
- **Revisão da Política** – descreve qual o prazo e quem é responsável pela revisão.
- **Diretrizes Gerais** – descreve as regras gerais da instituição.
- **Responsabilidades** – descreve as responsabilidades das várias unidades que a instituição possui.
- **Violação e Penalidades** – descreve quais são as penalidades em caso de incumprimento e/ou violação das políticas.
- **Vigência** – informa a altura em que as políticas entram em vigor.
- **Referências** – enumera quais as referências utilizadas neste documento.

Desta forma o documento final de política de segurança da informação, proposta para os problemas identificados da instituição, encontra-se no Anexo J – Documento de Políticas de Segurança.

5.4 Organização de Segurança da Informação

Tendo em conta a lista dos problemas da UMa, presente no Anexo I – Lista dos Problemas da UMa relevantes, os que se enquadram neste domínio são os seguintes:

- Inexistência de documento de atribuição de responsabilidades e funções;
- Existência de máquinas com Windows XP (sistema operativo antigo), pelo menos na área dos docentes, onde encontram-se pastas partilhadas. Um computador infetado ligado à rede interna é um potencial risco na rede.

A definição da política – Organização de Segurança da Informação, foi elaborada tendo em consideração as normas ISO/IEC 27001 e ISO/IEC 27002 e os controlos nelas contidos para corresponder às situações descritas anteriormente.

Os controlos utilizados para cobrir as situações descritas foram:

- A.6.1.1 – "Todas as responsabilidades de segurança da informação devem ser definidas e alocadas";
- A.6.1.3 – "Devem ser mantidos contactos apropriados com as autoridades competentes que sejam relevantes";
- A.6.2.1 – "Deve ser adotada uma política e as respetivas medidas de segurança para gerir os riscos introduzidos pela utilização de dispositivos móveis".

No primeiro controlo são definidas as responsabilidades de segurança da informação onde é também apresentado um organograma de forma a identificar bem os cargos mais importantes e decisivos.

No segundo controlo é abordado a importância de manter contactos com as entidades competentes de forma a garantir uma maior segurança dos ativos, em caso de não cumprimento das leis ou até em caso de ataques aos ativos.

No terceiro e último controlo constam as diretrizes da política de dispositivos móveis onde para este mesmo controlo foi elaborada uma política, à parte desta, embora relacionada com esta.

Desta forma a política – Organização de Segurança da Informação, proposta para os problemas identificados da instituição, encontra-se no Anexo J – Documento de Políticas de Segurança.

5.5 Controlo de Acesso

Tendo em conta a lista dos problemas da UMa, presente no Anexo I – Lista dos Problemas da UMa relevantes, o que se enquadra neste domínio é o seguinte:

- Inexistência de processo de revogação dos alunos. Os antigos alunos continuam a pertencer aos "utilizadores ativos";

A definição da política – Controlo de Acesso, foi elaborada tendo em consideração as normas ISO/IEC 27001 e ISO/IEC 27002 e os controlos nelas contidos para corresponder às situações descritas anteriormente.

O controlo utilizado para cobrir a situação descrita foi:

- A.9.2.1 – "Deve ser implementado um processo formal de registo e cancelamento de utilizadores para assegurar a atribuição de direitos de acesso";

Nesse controlo são abordadas as diretrizes para o registo, cancelamento dos utilizadores assim como a restrição ou a permissão de acesso dos sistemas, serviços e/ou aplicação aos utilizadores.

Desta forma a política – Controlo de Acesso, proposta para os problemas identificados da instituição, encontra-se no Anexo J – Documento de Políticas de Segurança.

5.6 Segurança Física e Ambiental

Tendo em conta a lista dos problemas da UMa, presente no Anexo I – Lista dos Problemas da UMa relevantes, os que se enquadram neste domínio são os seguintes:

- Não implementação de medidas de segurança física, eficientes, para as salas que contêm material sensível;
- Inexistência de registos de acesso às salas com material sensível, por estes serem feitos por chave tradicional, ou seja, não controlando quem entra e/ou sai;
- A existência de chaves mestras para o acesso às salas com material sensível;
- Utilização de algumas salas que contêm equipamento sensível como arrumos o que prejudica a qualidade do ambiente;
- Inexistência de apoio técnico ou política para auxiliar os alunos ou professores a encriptar os seus dados ou onde deixar os seus dados mais confidenciais.

A definição da política – Segurança Física e Ambiental, foi elaborada tendo em consideração as normas ISO/IEC 27001 e ISO/IEC 27002 e os controlos nelas contidos para corresponder às situações descritas anteriormente.

Os controlos utilizados para cobrir as situações descritas foram:

- A.11.1.1 – "Devem ser definidos e utilizados perímetros de segurança para proteger as áreas que contenham informação sensível ou crítica e recursos de processamento de informação";
- A.11.1.2 – "As áreas seguras devem ser protegidas através de controlos de entrada apropriados que assegurem que apenas é permitido o acesso a pessoas autorizadas";
- A.11.1.3 – "Devem ser concebidas e aplicadas medidas de segurança física para escritórios, salas e instalações";
- A.11.2.1 – "Os equipamentos devem ser colocados e protegidos de forma a reduzir os riscos de ameaças e perigos ambientais, e as oportunidades para acesso não autorizado";
- A.11.2.9 – "Deve ser adotada uma política de secretária limpa de papéis e suportes de dados amovíveis e uma política de ecrã limpo para os recursos de processamento de informação.

No primeiro controlo são definidas as diretrizes para a definição do perímetro de segurança de forma a proteger as instalações que contenham essencialmente informações sensíveis ou críticas e instalações de processamento de informação.

No segundo controlo são definidas as diretrizes com os controlos de entrada a utilizar de forma a proteger as áreas seguras e apenas permitir o acesso a pessoas autorizadas.

No terceiro controlo são definidas as diretrizes para a proteção das instalações, salas, escritórios onde para além dos controlos de acesso abordados, são também abordadas as medidas para a monitorização dos acessos.

No quarto controlo são definidas as diretrizes para a proteção dos equipamentos de forma a reduzir os riscos de ameaças, perigos ambientais e oportunidades de acesso não autorizado.

No quinto e último controlo são definidas as diretrizes da política de mesa limpa e ecrã limpo onde para este mesmo controlo foi elaborada uma política, à parte desta, embora relacionada com esta.

Desta forma a política – Segurança Física e Ambiental, proposta para os problemas identificados da instituição, encontra-se no Anexo J – Documento de Políticas de Segurança.

5.7 Conclusões

Identificados, analisados e avaliados os problemas e desafios da UMa, verificou-se que o normal funcionamento da instituição está cada vez mais dependente dos seus sistemas de informação, o que faz com que haja uma necessidade de maximizar a segurança dos mesmos. Claramente existe uma necessidade de uma solução para monitorizar e mitigar esses problemas.

Neste capítulo foi proposto e elaborado, como solução aos problemas identificados da UMa, um documento de políticas de segurança da informação. Este conjunto de políticas surge com o propósito de colmatar alguns dos problemas que foram identificados, na instituição, como por exemplo a inexistência de políticas (diretrizes/regras/processos/procedimentos) que servirão de base para um acertado planeamento, uma acertada implementação, monitorização, manutenção e melhoria do sistema de gestão de segurança da informação, da instituição.

Com o estudo realizado ao estado da arte, referente às normas ISO/IEC 27001 e ISO/IEC 27002, e tendo em conta os problemas que foram listados, foi possível identificar os domínios/controlos que mais se adequaram a esses mesmos problemas por forma a mitigá-los. Visto o tempo para a sua completa implementação exceder largamente o prazo definido para este trabalho, foram apenas abordados quatro dos catorze domínios. Os domínios abordados foram: Política de Segurança da Informação; Organização de Segurança da Informação; Controlo de Acesso; Segurança Física e Ambiental. Estes domínios correspondem, respetivamente, aos capítulos 5, 6, 9 e 11 da norma ISO/IEC 27002. O estudo feito a esses domínios permitiu identificar vários controlos que contribuíram para o desenvolvimento e elaboração das políticas. Apesar da elaboração das políticas ter-se baseado não só nos problemas identificados, como também nos domínios, não quer dizer que para cada domínio tenha que existir uma, duas ou mais políticas ou vice-versa. Neste caso foram desenvolvidas as políticas

relativamente aos domínios por se ter identificado vários controlos que correspondiam aos vários domínios utilizados, para resolver os problemas identificados.

Desenvolvidas e elaboradas as políticas, baseadas nas normas ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27003, a instituição terá que as aprovar e só depois é que podem ser implementadas. É importante referir que para a obtenção de bons resultados, devem ser divulgadas, devem ser seguidas à risca por toda a comunidade da instituição e deve ser dada formação a esse respeito, a todos os que interagem direta ou indiretamente com os ativos da instituição. Por fim, e após algum tempo de implementação é preciso realizar auditorias de forma a verificar se tudo está a ser cumprido rigorosamente. Prevê-se, através da aplicação das políticas, que a UMa obtenha:

- Uma melhor e mais acertada definição das responsabilidades distribuídas pelos ativos;
- Um aumento da consciencialização relativamente à segurança da informação;
- Uma otimização de planos e processos de gestão da informação, através da normalização de processos;
- As políticas de segurança desenvolvidas podem também ser utilizadas como um auxílio na antecipação do risco e na garantia da continuidade do negócio da instituição.

Um dos objetivos de indicar esta proposta (política de segurança) baseou-se essencialmente no facto de a principal causa e fonte de ameaças e vulnerabilidades presentes numa organização ser o próprio utilizador, o ser humano. Isto deve-se ao facto de não haver sobretudo uma consciencialização das pessoas na instituição.

6. CONCLUSÃO

Neste capítulo são apresentadas as conclusões que foram obtidas no decorrer da realização deste trabalho onde também são referidas algumas indicações de trabalhos futuros que possam vir a ser realizados mais tarde, de forma a complementar não só o atual estado físico e lógico da rede assim como também mantê-la o mais segura e precavida possível.

6.1 Conclusão geral

Este trabalho, numa primeira fase, incidiu numa vasta pesquisa teórica sobre conceitos ligados direta e indiretamente ao tema – Segurança da Informação, que se revelou eficaz e muito útil, tendo sido adquiridos alguns novos conceitos e esclarecidos outros conceitos fundamentais não só para a área da Informática como também para todas as outras áreas que indiretamente utilizam-nos. Foram consultados alguns livros presentes na biblioteca da Universidade da Madeira, alguns casos de estudo pesquisados na Internet, foram consultadas ainda algumas dissertações no repositório científico e digital da Universidade da Madeira, que mostraram a sua utilidade na preparação e abordagem ao tema. Foram ainda consultadas inúmeras normas referentes ao tema com o intuito de achar a ou as que mais se enquadrariam com os objetivos propostos. Optou-se por escolher preliminarmente a família de normas ISO/IEC 27000, pois embora cada uma das normas tenha uma função específica, todas elas têm como grande objetivo, implementar um SGSI capaz de fornecer um modelo para o estabelecimento, a implementação, a operacionalização, a monitorização, a revisão, a manutenção e a melhoria contínua da proteção dos ativos de informação de uma organização. Foi através do estudo da maior parte das normas a essa família que surgiram como normas base para a realização deste trabalho, a ISO/IEC 27001, a ISO/IEC 27002, a ISO/IEC 27003 e a ISO/IEC 27005. Estas normas eram as únicas que permitiriam desenvolver todo o processo de identificação, análise, avaliação e resolução dos problemas e desafios da instituição.

Numa segunda fase, com uma possível metodologia em vista e já abordando o primeiro objetivo, resultante do estudo ao estado da arte, houve a necessidade de proceder à observação, ao conhecimento e investigação das características da rede da Universidade da Madeira de forma a poder interpretar e observar o estado atual da rede e as necessidades que a mesma tem, no que diz respeito ao grau de segurança, manutenção e gestão da rede. Esta foi uma tarefa um pouco complexa devido às grandes dimensões da rede, mas que foi de certa forma minimizada através da marcação de várias reuniões e entrevistas, com os técnicos e responsáveis pela gestão dos serviços da UMa, com o intuito de auxiliarem e acompanharem na interpretação da estrutura e composição da rede. O que possibilitou um levantamento de necessidades e problemas existentes essencialmente na área de gestão e monitorização da rede e dos serviços da

Universidade da Madeira. Desse acompanhamento resultaram alguns documentos com o levantamento das necessidades e dos problemas da rede que foram mais tarde analisados e introduzidos num único documento cujo propósito passou por posteriormente aplicar uma metodologia que fosse possível avaliar o nível de risco que a UMa enfrenta, atualmente.

Recorrendo ainda às normas estudadas e abordadas no estado da arte, através da ISO/IEC 27001 e em simultâneo com outras referências, desde livros, dissertações e documentos académicos foi possível definir uma metodologia para proceder à identificação, análise e avaliação aos problemas da UMa. Recorreu-se ao diagrama de processos de um SGSI, referente à norma ISO/IEC 27001, e definiu-se todos os passos/processos necessários e utilizados para proceder à identificação, análise e avaliação dos problemas da UMa, alcançando o segundo objetivo estabelecido para este trabalho. Todos os processos, desde a identificação dos ativos, avaliação dos ativos, identificação das ameaças e vulnerabilidades, a análise do risco e posteriormente a avaliação do risco permitiram definir o nível de risco que a instituição enfrenta, para cada problema abordado. Com esta metodologia foi possível não só avaliar o risco como também priorizá-lo de forma a entender qual a sua influência e impacto na instituição. Ou seja, verificou-se a eficiência da metodologia utilizada bem como a sua flexibilidade de aplicação a este caso, por esta metodologia permitir uma melhoria e continuidade do "negócio" da instituição, no que ao nível de risco de uma organização diz respeito. Com base nessa metodologia definida, foi possível afirmar que o normal funcionamento da instituição está cada vez mais dependente dos sistemas de informação, o que intensifica a necessidade de maximizar a segurança dos mesmos, e que existem soluções tecnológicas e ou procedimentais com potencial para mitigar e/ou eliminar esses níveis de risco obtidos.

A proposta, para colmatar esses problemas da UMa, associados a níveis de risco médio, foi a definição e elaboração de um documento de políticas que permitirá melhorias no funcionamento dos sistemas de informação da instituição. Foi escolhida esta proposta por a maior parte dos problemas da UMa, identificados, demonstrarem a inexistência de normas, processos e procedimentos que indiquem os caminhos ou uma orientação a seguir. Um dos outros objetivos para esta proposta (política de segurança) baseou-se também pelo facto de a principal causa e fonte de ameaças e vulnerabilidades presentes numa organização ser o próprio utilizador, o ser humano. Isto deve-se ao facto de não haver sobretudo uma consciencialização das pessoas na instituição, porque a segurança não passa apenas por proteger os sistemas, mas também pela consciencialização dos utilizadores para a sua necessidade, tornando-se necessária a definição de políticas adequadas a cada organização. Onde essas políticas de segurança devem ser alinhadas com os objetivos estratégicos da organização por forma a manter e/ou melhorar o seu valor.

Tendo em conta, novamente, as normas estudadas e abordadas no estado da arte, a ISO/IEC 27001 e a ISO/IEC 27002, e sabendo que ambas abrangem num total catorze domínios, por motivos de limitação de tempo para a realização deste trabalho, optou-

se por abordar apenas quatro domínios (Política de Segurança da Informação, Organização de Segurança da Informação, Controlo de Acesso e Segurança Física e Ambiental) pelo facto de também os problemas identificados e definidos como relevantes enquadrarem-se nesses mesmos domínios. Dessa forma foram aplicados, num total, onze controlos com o intuito de elaborar as políticas para que fosse possível mitigar ao máximo o nível de risco dos problemas identificados da instituição. Elaboradas as políticas é ainda necessário garantir o cumprimento dos últimos passos: aprovação e formação. Escrito o documento de políticas de segurança, resta esse mesmo documento ser aprovado pelo conselho de administração da instituição. Caso seja aprovado, deve ser de imediato divulgado por vários meios, confirmando que toda a comunidade tem acesso às políticas a si destinadas. Por fim, o último passo para a conclusão do processo das políticas passa pela formação e educação de toda a comunidade para que sejam cumpridas todas as regras definidas a fim de garantir a segurança dos ativos da instituição. Apesar de não fazer parte, diretamente, do processo para a elaboração e implementação das políticas, é necessário realizar posteriormente uma auditoria de modo a que seja possível verificar se estão a ser cumpridas todas as regras, normas, processos e/ou procedimentos para a segurança da informação, da instituição.

Apesar de não ter sido possível apresentar resultados comprovados, face à solução proposta, onde seria necessário no mínimo entre seis a doze meses para os conseguir, de forma clara, face aos objetivos traçados, desde o momento inicial, este trabalho tornou-se exequível e demonstrou que é possível prever que com esta proposta implementada na instituição resultará essencialmente numa maior otimização de planos e processos de gestão da informação, um aumento da consciencialização interna relativo à segurança da informação e o comprometimento com a aplicação das políticas. Estou convicto que a sua aplicação terá forçosamente impacto nos objetivos e exigências da organização, acabando por se tornar numa opção estratégica. Será uma árdua tarefa, implementar e seguir tudo à risca, mas, na minha opinião, as vantagens resultantes da implementação desta proposta recompensam todo o esforço que toda a comunidade, principalmente os utilizadores que contêm mais privilégios (funcionários, docentes, não docentes, estagiários, etc.) da instituição terão que fazer.

Ao longo da realização deste trabalho foram encontradas diversas dificuldades nomeadamente a falta do conhecimento prévio de toda a rede da instituição assim como do conhecimento de todos os sistemas, serviços, entidades, etc. que a instituição possui. Alguma dificuldade inicial em como abordar o tema e dar um rumo o mais rigoroso possível. E pelo facto de haver muita informação que não poderia ser disponibilizada por ser confidencial. Todavia, a maior parte dos obstáculos foram ultrapassados com recurso às várias entrevistas e reuniões com os responsáveis pela gestão da rede da instituição assim como às reuniões realizadas com o professor Eduardo e a professora Lina a fim de auxiliar noutras áreas necessárias.

A realização deste trabalho permitiu constatar que para além de todas as medidas e mecanismos que uma organização possa implementar, é necessário ter sempre um

conjunto de políticas bem definidas e implementadas, assim como é necessário ter em conta que nenhuma organização está salvaguardada apenas utilizando todas estas medidas referidas. A segurança de toda a organização só é mantida caso haja uma enorme dedicação e um sério comprometimento de toda a comunidade afeta à organização. Deste modo é claríssimo que tornar um ambiente computacional seguro é uma tarefa bastante complexa, que requer uma enorme gestão, organização e participação de todos.

Apesar de todo este trabalho ser exequível noutras instituições, organizações e ou até em empresas, é importante referir que é sempre necessário haver uma adaptação pois nem todas as organizações são de dimensões semelhantes a esta, por exemplo. Haverá sempre algum ajuste, seja introdução ou substituição de um ou outro elemento.

6.2 Trabalhos futuros

Neste trabalho realizado, apenas foram exploradas estas quatro normas (ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27003 e ISO/IEC 27005) para executar tanto a análise e avaliação dos problemas da UMa como também a elaboração das políticas para mitigar esses mesmos problemas. Mas é completamente evidente que existem outras normas, outras metodologias e outros processos que poderiam dar origem também a uma análise, avaliação e elaboração de políticas.

Para além dos problemas mencionados neste capítulo e para o qual foram desenvolvidas as políticas, baseadas nos domínios das normas identificadas no estado da arte, existem outros mais. O caminho está traçado e pode continuar a ser seguido tendo em conta que outras políticas são também necessárias, assim como a criação de procedimentos e processos para alguns dos domínios que não foram mencionados. Desta forma é recomendável que os restantes domínios e restantes políticas sejam de igual forma elaborados (as) e aplicados (as) para que a segurança da informação se torne uniforme e em conformidade com os objetivos da instituição.

Em termos de outro possível trabalho futuro, seria interessante e extremamente importante realizar uma auditoria à rede da Universidade da Madeira, baseada nas normas ISO/IEC 27001 e ISO/IEC 27002 de forma a saber o que está a ser gerido deficientemente e proceder à certificação que corresponda aos objetivos definidos e propostos para a instituição.

O facto de a instituição poder a vir ser certificada pela norma ISO/IEC 27001 só irá ter benefícios e logo a curto-médio prazo pois ainda este ano foi também desenvolvida uma norma para corresponder à nova regulamentação RGPD o que vem beneficiar as organizações que já têm implementado essa regulamentação.

7. REFERÊNCIAS

[1] H. S. Mamede, Segurança Informática nas Organizações, Lisboa: FCA - Editora de informática, 2006.

[2] "Público - Cibersegurança," [Online]. Available: https://www.publico.pt/2018/12/27/tecnologia/noticia/doze-meses-ciberataques-falhas-seguranca-1855905#gs.nVjEDqFM. [Acedido em 20 Junho 2017].

[3] E. Monteiro e F. Boavida, Engenharia de Redes Informáticas, Lisboa: FCA - Editora de Informática, 2011.

[4] Roberto, "Gestão de Ativos – A organização nas mãos da TI - Revista Infra Magazine 11," 2013. [Online]. Available: https://www.devmedia.com.br/gestao-de-ativos-a-organizacao-nas-maos-da-ti-revista-infra-magazine-11/27895#ixzz3vcga4erB. [Acedido em 20 fevereiro 2018].

[5] "ISO/IEC 27001:2013(E) - Information technology - Security techniques - Information security management systems - Requirements," 2013. [Online]. Available: https://trofisecurity.com/assets/img/iso27001-2013.pdf. [Acedido em 21 outubro 2017].

[6] ISO/IEC 27002:2013(E) - Information technology - Security techniques - Code of practice for information security controls, Second edition ed., Switzerland: ISO copyright office, 2013.

[7] "ISO/IEC 27003:2017(E) - Information technology - Security techniques - Information security management systems - Guidance," [Online]. Available: https://www.iso.org/standard/63417.html. [Acedido em 20 junho 2017].

[8] "ISO/IEC 27005:2011(E) - Information technology - Security techniques - Information security risk management," [Online]. Available: https://www.iso.org/standard/56742.html. [Acedido em 21 outubro 2017].

[9] SignificadosBr, "Significado de Segurança," [Online]. Available: https://www.significadosbr.com.br/seguranca. [Acedido em 22 Março 2017].

[10] André, "Segurança Informática - Introdução," [Online]. Available: https://www.dei.isep.ipp.pt/~andre/doc/seguranca-introducao.html. [Acedido em 22 Junho 2017].

[11] A. Carneiro, Introdução à Segurança dos Sistemas de Informação, FCA - Editora de Informática, Lda., 2002.

[12] E. Percilia, “Segurança em Redes de Computadores,” [Online]. Available: https://brasilescola.uol.com.br/informatica/seguranca-redes.htm. [Acedido em 20 Junho 2016].

[13] Pedro.CCM, “Introdução à segurança informática,” 3 Julho 2017. [Online]. Available: https://br.ccm.net/contents/623-introducao-a-seguranca-informatica. [Acedido em 20 Junho 2018].

[14] M. Â. Mendoza, “Cibersegurança ou segurança da informação? Explicando a diferença,” 17 Janeiro 2017. [Online]. Available: https://www.welivesecurity.com/br/2017/01/17/ciberseguranca-ou-seguranca-da-informacao/. [Acedido em 22 Junho 2017].

[15] “Serviços Partilhados do Ministério da Saúde - A segurança da informação,” Novembro 2017. [Online]. Available: http://ciberseguranca.spms.min-saude.pt/wp-content/uploads/2018/03/eSIS_Flyer_Seguranca_da_Informacao.pdf. [Acedido em 22 Junho 2018].

[16] BSIGroup, “O que é uma norma e como elas afetam seu negócio?,” [Online]. Available: https://www.bsigroup.com/pt-BR/Normas/Informacoes-sobre-normas/O-que-e-uma-norma/. [Acedido em 20 Março 2018].

[17] M. Muller, “Quais são e para quê servem as normas de segurança da informação?,” 30 Março 2017. [Online]. Available: https://www.anyconsulting.com.br/normas-de-seguranca-da-informacao/. [Acedido em 20 Junho 2018].

[18] “Wikipedia - ISO/IEC 27000-series,” [Online]. Available: https://en.wikipedia.org/wiki/ISO/IEC_27000-series. [Acedido em 6 Junho 2016].

[19] ISO/IEC 27000:2016(E) - Information technology - Security techniques - Information security management systems - Overview and vocabulary, Switzerland: ISO copyright office, 2014.

[20] F. Palma, “Portal GSTI - ISO 27001 em 5 minutos | O que é a ISO 27001?,” 2017. [Online]. Available: https://www.youtube.com/watch?v=68cphWTnsmw.

[21] D. Vasile, “ISO 27001 Domains, Control Objectives and Controls,” 2011. [Online]. Available: https://www.pentest.ro/iso-27001-domains-control-objectives-and-controls/. [Acedido em 22 Novembro 2017].

[22] C. M. R. Correia, “Plano de Implementação da Norma ISO/IEC 27001 no INEM. Dissertação Mestre em Gestão de Informação. Universidade Nova de Lisboa-Instituto Superior de Estatística e Gestão de Informação.,” Lisboa, 2016.

[23] “ISO27k,” [Online]. Available: http://www.iso27001security.com/html/toolkit.html. [Acedido em 30 Novembro 2018].

[24] F. Sir, “ebah - ISO 17799,” 2002. [Online]. Available: http://www.ebah.pt/content/ABAAAe6B8AF/iso-17799. [Acedido em 20 outubro 2017].

[25] F. Palma, “Portal GSTI - ISO 27002 em 5 minutos | O que é ISO 27002?,” 2017. [Online]. Available: https://www.youtube.com/watch?v=fa4A-OBe67E.

[26] F. Palma, “Portal GSTI - Quais os objetivos das ISO 27001 e ISO 27002,” 2011. [Online]. Available: https://www.portalgsti.com.br/2011/05/iso-27001-e-iso-27002.html. [Acedido em 20 Março 2018].

[27] EXIN, “Slideshare - O que mudou com a revisão da norma ISO 27002:2005 para a versão 2013.,” 2014. [Online]. Available: https://pt.slideshare.net/Exin/o-que-mudou-com-a-reviso-da-norma-iso-270022005-para-a-verso-2013. [Acedido em 28 Julho 2018].

[28] Noticebored, “ISO/IEC 27002:2013 — Information technology — Security techniques — Code of practice for information security controls (second edition),” Fevereiro 2018. [Online]. Available: http://www.iso27001security.com/html/27002.html. [Acedido em 10 Setembro 2018].

[29] W. Pandini, “Ostecblog - 30 dez ISO 27002: Boas práticas para gestão de segurança da informação,” 2016. [Online]. Available: https://ostec.blog/padronizacao-seguranca/iso-27002-boas-praticas-gsi. [Acedido em 10 Setembro 2018].

[30] “ISO/IEC 27004:2016(E) - Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and evaluation,” [Online]. Available: https://www.iso.org/standard/64120.html. [Acedido em 20 junho 2017].

[31] “ISO 31000 – Gestão de Riscos – Diretrizes,” [Online]. Available: https://www.iso.org/iso-31000-risk-management.html. [Acedido em 20 junho 2017].

[32] “ISO 9001 – Sistema de Gestão de Qualidade – Requisitos,” [Online]. Available: https://www.iso.org/standard/62085.html. [Acedido em 20 junho 2017].

[33] ISO, “ISO - The facts about certification,” [Online]. Available: https://www.iso.org/certification.html. [Acedido em 3 Junho 2016].

[34] BSIGroup, “Conheça os procedimentos para obter sua certificação,” [Online]. Available: http://www.bsigroup.com/pt-BR/Nossos-servicos/Certificacao/Como-obter-a-certificacao/. [Acedido em 6 Junho 2016].

[35] OptimalRisk, “Security Surveys and Audits,” [Online]. Available: http://www.optimalrisk.com/Risk-Security-Consulting/Security-Surveys-and-Audits. [Acedido em 6 Junho 2016].

[36] R. Srivastava, “It Security Audit Process,” 10 Fevereiro 2010. [Online]. Available: https://pt.slideshare.net/rsrivastava91/it-security-audit-process. [Acedido em 6 Junho 2016].

[37] “Cybersecurity Risk Assessment – Qualitative vs Quantitative Assessments,” [Online]. Available: https://blog.finjan.com/cybersecurity-risk-assessment-qualitative-vs-quantitative/. [Acedido em 12 Março 2018].

[38] B. Karabacak e I. Sogukpinar, “ISRAM: information security risk,” em *Computers & Security*, vol. 24, 2005, pp. 147 - 159.

[39] Wikipedia, “Universidade da Madeira,” [Online]. Available: https://pt.wikipedia.org/wiki/Universidade_da_Madeira. [Acedido em 24 Junho 2017].

[40] “Universidade da Madeira - UMa,” [Online]. Available: https://www.uma.pt/sobre/historia/. [Acedido em 24 Junho 2017].

[41] SASUMa, “SASUMa,” [Online]. Available: http://www.sasuma.pt/portal/index.php?id=sasuma. [Acedido em 24 Junho 2017].

[42] “Universidade da Madeira - Faculdades e Escolas,” [Online]. Available: https://www.uma.pt/sobre/faculdades-e-escolas/. [Acedido em 24 Junho 2017].

[43] “Universidade da Madeira - Relatório de Gestão Consolidado 2016,” [Online]. Available: http://conselhogeral.uma.pt/index.php?option=com_docman&task=doc_download&gid=766&Itemid=80&lang=pt. [Acedido em 10 Fevereiro 2018].

[44] “Universidade da Madeira - Regulamento orgânico da Universidade da Madeira,” 2013.

[45] *Proposta Melhoria Rede UMa: Fase 1 - Documento fornecido pelos Serviços Técnicos da UMa.,* 2017.

[46] R. Ruel, “Desenho e Implementação de uma Plataforma Integrada para Monitorização e Gestão da Rede da UMa - Projeto de Mestrado em Engenharia Informática,” 2016.

[47] L. Rodríguez, *Segurança em Sistemas de Comunicação - 2ª Aula Prática - Análise de Risco e Potencial Alvo de Ataque.,* 2011.

[48] P. Silva, “Análise de Riscos de Segurança da Informação,” [Online]. Available: http://www.ifc-camboriu.edu.br/~nildo/si/An%E1lise%20de%20Riscos.pdf. [Acedido em 8 outubro 2018].

[49] T. Valentim, “Implementação de uma Metodologia de Análise de Risco baseada na BS7799-3 - Universidade Federal do Rio de Janeiro - Escola Politécnica - Departamento de Eletrónica e de Computação,” Rio de Janeiro, 2008.

[50] C. P. Pfleeger, S. L. Pfleeger e J. Margulies, Security in Computing 5th edition, Massachusetts: Prentice Hall, 2015.

[51] S. Marvão, “B!Tmagazine,” [Online]. Available: https://www.bit.pt/10-passos-para-mitigar-vulnerabilidades-nas-infraestruturas-criticas/. [Acedido em 17 dezembro 2018].

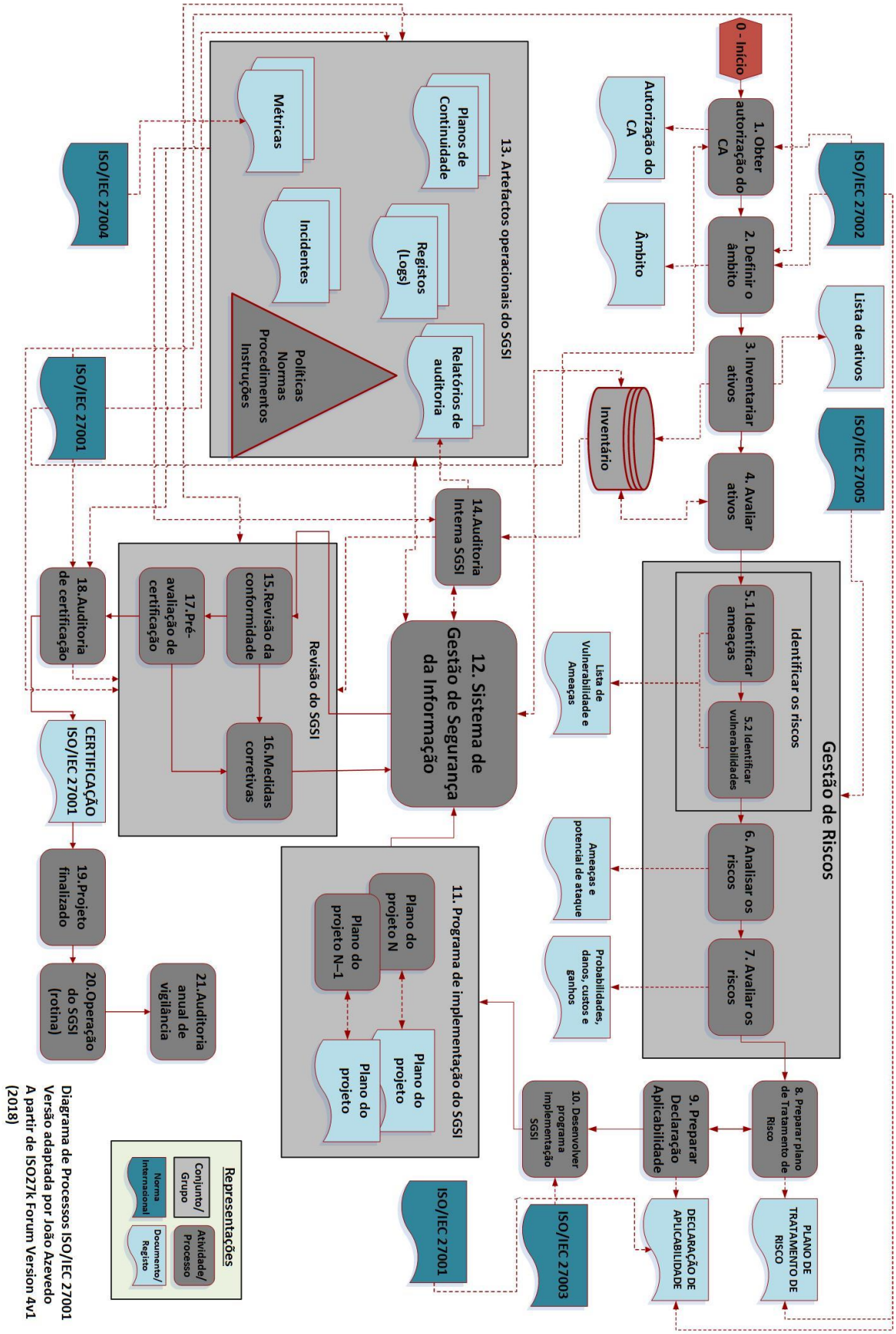
[52] D. W. Straub, G. Seymour e B. L. Richard, Information Security Policy, Processes and Practices, M. E. Sharpe, 2008.

[53] L. Rodríguez, *Capítulo 1 - Introdução - Segurança em Sistemas de Comunicação,* 2011.

[54] E. Marques, *Análise de Risco da Universidade da Madeira - Segurança em Sistemas de Comunicação,* 2014.

ANEXOS

Anexo A – Diagrama de processos de um SGSI (ISO/IEC 27001)



Anexo B – Recolha de informação da rede da UMa

Neste anexo encontram-se os documentos, informais, que foram elaborados para as reuniões (entrevistas), com o objetivo de saber o estado atual da rede e quais os pontos negativos identificados, até então.

A.1 Documentos elaborados na primeira reunião

1º Documento: Questões – Análise de Segurança

Segurança no Controlo de Acesso

- Qual o estado atual das políticas de segurança. Existe algum documento do género?
- Que ganhos poderá ter quem atacar os recursos informáticos?
- Quais são os acessos existentes ao exterior?
- Quais são os mecanismos de segurança que utilizam?
- Existe um processo formal de registo de utilizador que atribui e revoga o acesso e os direitos de acesso a sistemas e serviços, e os direitos de acesso são revistos regularmente e removidos após a saída do utilizador (aluno…)?

Segurança Autenticação e Encriptação

- Quais são os mecanismos de autenticação existentes?
- Existe uma política para o uso de criptografia e gestão de chaves?
- Quais as políticas de passwords que têm? (na camada rede e na camada de ligação)

Segurança da Informação

- Qual o estado atual de segurança da informação e dos esforços de formação?
- A Segurança da Informação tem grande relevância para a rede da universidade?

Segurança na Organização

- Qual o estado atual de sensibilização dos níveis superiores de gestão da organização?
- Quantos são e quem são os responsáveis pelo departamento de informática ou pela sala dos servidores?
- Os papéis/funções/responsabilidades encontram-se claramente definidas/atribuídas?

Restantes questões:

- É feita ou já alguma vez foi feita alguma auditoria?
- De que forma os visitantes podem/têm acesso à rede/internet, na universidade?
- Como é que é dado acesso nesses casos?
- Quando é adicionada uma máquina o que é feito (a nível de políticas de atualizações)?
- Quanto às máquinas antigas como estão a ser efetuadas as políticas de atualizações?
- Quais os mecanismos de segurança que os servidores têm? Abordando apenas os mais importantes.
- Quanto ao sistema que usam para efetuar os backups, como funciona e se está bem protegido?
- O quê que está a ser feito de backups? sistemas, serviços...
- Quais são as áreas que são necessárias para fazer backup?
- Quais são os custos de reparação/recuperação em horas/dias (em caso de ocorrência de uma falha/ataque ou algo do género) dos vários serviços e recursos (os mais importantes)?
- Existe número limite máximo de dispositivos que se podem ligar a cada AP dos vários andares?
- Qual a segurança que os AP's têm, para além da física (cadeado aplicado de forma à não remoção do cabo)?
- Quando fazem alguma manutenção ou mudança/alteração de cabos, todos os utilizadores ou a maior parte são informados?
- Como são feitas as filtragens da Firewall, da firewall central, como também dos servidores? (por porta, por IP)
- Levantamento de serviços internos e externos (mais relevantes) e como está a ser feito a segurança dos mesmos?

Questões por Camadas de Segurança (2º documento)

Segurança no meio físico:

- A nível de equipamento de Redes o que têm, onde está localizado e se está protegido e assegurado?
- Qual o nível de segurança que tem a sala? Quem pode aceder e como pode aceder?
- Que tipo de segurança/abertura utiliza a porta?
    - Chave;
    - Eletrónica;
- Existe algum registo de quem entra e sai da sala?
- Todas as ligações por rede (ex.: cabos, fichas, dispositivos periféricos e etc…) são revistas ou inspecionadas periodicamente?

Segurança na Ligação:

- Quais os protocolos existentes?
- Como está a ser feito o controlo das portas e do tráfego?
- Existe algum limite de quantidade de endereços que uma porta pode "aprender"?
- Existe algum controlo de MAC's?
- Quanto ao equipamento, é inspecionado periodicamente?

Segurança na rede e transporte

- Qual a segurança que os servidores têm?
- Quais são as políticas de atualização?
- Quais são os mecanismos de segurança que utilizam?
- Nesta altura, o que é que pode estar a ser deficientemente gerido, em toda a rede?
- Qual é o risco máximo admissível que a rede da universidade pode aceitar?
- Quais são os custos de reparação/recuperação (em caso de ocorrência de um ataque ou algo semelhante)?
- Há satisfação com a solução que têm implementada?

Segurança na Aplicação

- Qual o estado atual de segurança das aplicações de rede?
- Quais são os mecanismos de firewall existentes?
- Existe proteção contra malware, está atualizada?
- A informação, o software e os sistemas estão sujeitos a cópias de segurança e a testes regulares?

Segurança no Controlo de Acesso

- Qual o estado atual das políticas de segurança. Existe algum documento do género?
- Que ganhos poderá ter quem atacar os recursos informáticos?
- Quais são os acessos existentes ao exterior?
- Quais são os mecanismos de segurança que utilizam?
- Existe um processo formal de registo de utilizador que atribui e revoga o acesso e os direitos de acesso a sistemas e serviços, e os direitos de acesso são revistos regularmente e removidos após a saída do utilizador (aluno…)?

Segurança Autenticação e Encriptação

- Quais são os mecanismos de autenticação existentes?
- Existe uma política para o uso de criptografia e gestão de chaves?

Segurança da Informação

- Qual o estado atual de segurança da informação e dos esforços de formação?
- A Segurança da Informação tem grande relevância para a rede da universidade?

Segurança na Organização

- Qual o estado atual de segurança do sistema como um todo?
- Qual o estado atual de sensibilização dos níveis superiores de gestão da organização?
- Quantos são e quem são os responsáveis pelo departamento de informática ou pela sala dos servidores?
- Os papéis/funções/responsabilidades encontram-se claramente definidas/atribuídas?

Segurança Geral

- É feita ou já alguma vez foi feita alguma auditoria?

A.2 Documentos elaborados na segunda reunião

Análise de Risco da Universidade (1º documento)

- ✓ **Descrição do cenário**
  - Utilizadores:
    - Número de alunos, docentes, funcionários, pessoas que estão inscritas/têm acesso não só à rede como também, fisicamente, à universidade?
    - É possível ter essa informação por andar (ex.: Piso -2 tem normalmente x utilizadores), por grupos (ex.: docentes, alunos, associados, funcionários…) ou por áreas (ex.: faculdade de ciências ou cursos)?

NOTA: O objetivo nesta parte é ter uma estimativa da quantidade de utilizadores que utilizam ou têm acesso não só à universidade como também à rede da mesma, e se possível dividi-los em grupos de forma a futuramente prevenir alguma situação de risco.

  - Rede local:
    - Número de ligações existentes, ativas ou não, (ex.: fichas, tomadas, cabos)?
    - Número de VLANs existentes e se encontram-se bem divididas/organizadas?
    - Existe algum bastidor?
    - Existe algum diagrama ou esquema de rede (atualizado) que demonstre todas as ligações até à data?

NOTA: O objetivo nesta parte é ter uma estimativa da quantidade de ligações entre a rede e outros dispositivos que se possam ligar à própria de forma a poder ter uma ideia do risco que pode apresentar e de saber se as VLANS encontram-se bem distribuídas e por grupos/áreas ou pisos.

  - Acesso à internet:
    - Quais são os tipos de ligações existentes?
    - Quem pode aceder à internet e como pode?

NOTA: O objetivo nesta parte é ter uma estimativa da quantidade de ligações existentes e de quem pode ou está autorizado a aceder à internet a partir da universidade…

  - Acesso comutado:
    - Existe algum acesso por ISDN ou PSTN? Se sim quantos e se estão bem implementados e monitorizados.

NOTA: O objetivo nesta parte é saber se existe algum tipo de acesso e se sim quais e se encontram-se protegidos e se são monitorizados.

- Servidores:
  - Quantos?
  - Quais os existentes e se estão devidamente identificados?
  - Algum exposto à internet?
  - Quem tem acesso?
  - Quem faz a manutenção?

NOTA: O objetivo nesta parte é ter uma estimativa de quantos servidores existem, quais são e quem tem acesso, se são feitas vistorias aos mesmos de forma a evitar ataques e quais os que contêm informações relevantes que requeiram um nível de segurança mais apertado. É importante também ter um esquema dos endereçamentos e tipos de encaminhamentos de IP…

- Computadores pessoais:
  - Existe algum programa ou software que permita identificar/quantificar ou até monitorizar o número de computadores pessoais existentes no interior da Universidade e que tenham acesso à rede?
  - No departamento de informática ou na sala onde contém os equipamentos de rede, existe algum computador pessoal?
  - É permitido o uso de computadores pessoais no interior das salas onde constem equipamentos da rede da Universidade?

NOTA: O objetivo nesta parte é poder proteger ao máximo o uso de computadores pessoais no interior da sala de bastidores ou departamento de informática de forma a minimizar o risco de "ataques" internos ou de acessos mal-intencionados.

- Mecanismos de segurança:
  - Quais são os tipos de mecanismos de segurança existentes?
  - Qual o nível de segurança que têm?
  - Quanto a hardware, existe firewall e proxies?
  - A autenticação é centralizada?
  - Que tipos de mecanismos são utilizados nos acessos do exterior?
  - Existem mecanismos de monitorização?
  - Câmaras de vigilância nas entradas/saídas do departamento?

NOTA: O objetivo nesta parte é entender se existe mecanismos de segurança implementados, se sim quais são, … de forma a poder perceber o nível de segurança que a rede apresenta.

- Equipa técnica:
  - Como é formada a equipa (ex.: quantos gestores, quantos técnicos, quantos administradores)?
  - Quem tem privilégios e acessos a quê?

NOTA: O objetivo nesta parte é perceber se existe uma hierarquia e se a mesma é respeitada, bem como quem é responsável pelo quê, ou seja, quais são as suas funções e se todos os encargos são cumpridos.

- ✓ **Bens a proteger**
  - Hardware:
    - Quantos computadores?
    - Quantos servidores?
    - Quantas impressoras?
    - Equipamento de comunicações…
      - VALOR TOTAL INVESTIDO em hardware = ?

NOTA: O objetivo nesta parte é perceber a quantidade de equipamento de rede (em funcionamento ou não) que a universidade possui e qual o seu investimento para posteriormente fazer uma análise de forma a minimizar os riscos de segurança.

  - Software
    - Sistemas operativos?
    - Office's?
    - Ambientes de desenvolvimento…
      - VALOR TOTAL INVESTIDO em software = ?

NOTA: O objetivo nesta parte é perceber a quantidade de software de rede existente (em funcionamento ou não) que a universidade possui, se está atualizado e qual o seu investimento para posteriormente fazer uma análise de forma a minimizar os riscos de segurança.

  - Informação
    - Administrativa
    - Documentos pessoais
    - Trabalhos académicos
    - Trabalhos científicos
      - VALOR TOTAL INVESTIDO em informação = ?

NOTA: O objetivo nesta parte é perceber qual o tipo de informação que existe, qual o grau de privacidade que corresponde e se está a ser respeitado e se a privacidade está assegurada.

  - Tempo
    - Tempo de paragem das atividades:
      - Custo de aulas teóricas/práticas, de realização de avaliações e de docentes, em caso de falha ou ataque a um determinado sistema ou servidor…
        - VALOR TOTAL = ?
    - Tempo de reparação
      - Custo da equipa técnica
        - VALOR TOTAL = ?

NOTA: O objetivo nesta parte é entender que o tempo que leva a recuperação de um equipamento, um sistema ou uma rede a estar novamente segura é relevante para o perigo que a universidade pode enfrentar. Também em caso de falha ou ataque a um determinado recurso pode implicar imensos danos não só físicos como também orçamentais.

- Outros bens
  - Equipamentos laboratoriais
  - Recursos financeiros
  - Secretaria
  - Má preparação dos alunos
    - VALOR TOTAL = ?
- Valor global dos bens a proteger
  - Fazendo as contas de tudo, a universidade/departamento de informática "sobrevive" a uma perda total no SI? [47], [53], [54]

A.3 Documentos com as respetivas questões respondidas

Análise de Risco da Universidade (1º documento)

✓ **Descrição do cenário**

- Utilizadores:
  - Número de alunos, docentes, funcionários, pessoas que estão inscritas/têm acesso não só à rede como também, fisicamente, à universidade?

Número de alunos: 2800

Número de docentes: 253

Número de não docentes: 12

Número de funcionários: 150

AAUMa, SASUMa, Colégio dos Jesuítas, outras entidades…

Restantes pessoas: Todos têm acesso fisicamente à universidade, pela porta principal.

  - É possível ter essa informação por andar (ex.: Piso -2 tem normalmente x utilizadores), por grupos (ex.: docentes, alunos, associados, funcionários…) ou por áreas (ex.: faculdade de ciências ou cursos)?

Não existe indicadores para o número de pessoas, por andar. Possivelmente por áreas é possível.

NOTA: O objetivo nesta parte é ter uma estimativa da quantidade de utilizadores que utilizam ou têm acesso não só à universidade como também à rede da mesma, e se possível dividi-los em grupos de forma a futuramente prevenir alguma situação de risco.

- Rede local:
  - Número de ligações existentes, ativas ou não, (ex.: fichas, tomadas, cabos)?

Existem sensivelmente cerca de 50 fichas/tomadas no piso 3 (distribuídas entre as salas de aulas, gabinetes de professores, laboratórios e sala servidores). Cerca de 90 fichas/tomadas no piso 2 (distribuídas entre as salas de computadores, as salas de estudo, a sala de informática, gabinetes de professores e laboratórios). Cerca de 40 fichas/tomadas no piso 1 (distribuídas entre as salas de aulas, gabinetes de professores e laboratórios). Cerca de 80 fichas/tomadas no piso 0 (distribuídas entre as salas de aulas, gabinetes de professores, laboratórios, sala de servidores). Cerca de 50 fichas/tomadas no piso -1 (distribuídas entre as salas de aulas, laboratórios, sala de servidores, AAUMa). Cerca de 60 fichas/tomadas no piso -2 (distribuídas entre as salas de aulas, laboratórios, sala de servidores). E por fim cerca de 20 fichas/tomadas no piso -3 (distribuídas entre as salas de aulas e parte da cantina).

Um total sensivelmente de 400 fichas/tomadas de redes e restantes 600 tomadas de eletricidade.

  - Número de VLANs existentes e se encontram-se bem divididas/organizadas?

Existem sensivelmente 15 VLANs e encontram-se razoavelmente organizadas/definidas e delineadas.

VLANs	Designação da Rede
VLAN1	Funcionários e servidores
VLAN2	Alunos
…	…

  - Existe algum bastidor/quantos?

Existem 18 bastidores, todos eles divididos por pisos. Média 2 por piso.

  - Existe algum diagrama ou esquema de rede (atualizado) que demonstre todas as ligações até à data?

Sim.

NOTA: O objetivo nesta parte é ter uma estimativa da quantidade de ligações entre a rede e outros dispositivos que se possam ligar à própria de forma a poder ter uma ideia do risco que pode apresentar e de saber se as VLANS encontram-se bem distribuídas e por grupos/áreas ou pisos.

- Acesso à internet:
  - Quais são os tipos de ligações existentes?

Existem 2 tipos de ligações existentes: Rede local (cabo) e wireless (eduroam).

- Quantos pontos de acesso existem?

Existem cerca de 120 pontos de acesso à rede wireless (eduroam) onde os mesmos têm capacidade de gestão remota, mas não possuem um controlador que possa facilitar a monitorização e configuração deles.

NOTA: O objetivo nesta parte é ter uma estimativa da quantidade de ligações existentes e de quem pode ou está autorizado a aceder à internet a partir da universidade…

- Acesso comutado:
  - Existe algum acesso por ISDN ou PSTN? Se sim quantos e se estão bem implementados e monitorizados.

Existem acessos por ISDN e PSTN onde os mesmos apenas são utilizados para voz. Possui sistema RDIS para acesso primário para o exterior, 30 canais de voz.

NOTA: O objetivo nesta parte é saber se existe algum tipo de acesso e se sim quais e se encontram-se protegidos e se são monitorizados.

- Servidores:
  - Quantos?

Na sala de servidores existe 1 grande bastidor (Blade) constituído por 3 servidores físicos e dezenas (50) para serviços variados, com máquinas virtuais. Tem 10 máquinas distintas e antigas e 1 bastidor CEE com sensivelmente 7 máquinas físicas (15 máquinas virtuais).

Nos Jesuítas tem cerca de 15 máquinas onde esse parque informático tem sensivelmente 3 anos de existência.

A solução é substituir as 10 máquinas antigas para evitar perda desnecessária de energia.

- Quais os existentes e se estão devidamente identificados?

Existem os servidores de email, DHCP, web, restantes serviços disponíveis.

- Algum exposto à internet?

Muitos encontram-se expostos à internet.

- Quem tem acesso?

Responsáveis pelos servidores, sensivelmente 5 a 6 pessoas, incluindo o Dr. Gilberto e Eng. João Matos.

- Quem faz a manutenção?

Quem efetua a manutenção por vezes é a equipa de manutenção da universidade como também poderá ser uma do exterior.

NOTA: O objetivo nesta parte é ter uma estimativa de quantos servidores existem, quais são e quem tem acesso, se são feitas vistorias aos mesmos de forma a evitar ataques e quais os que contêm informações relevantes que requeiram um nível de segurança mais apertado. É importante também ter um esquema dos endereçamentos e tipos de encaminhamentos de IP…

- Computadores pessoais:
  - Existe algum programa ou software que permita identificar/quantificar ou até monitorizar o número de computadores pessoais existentes no interior da Universidade e que tenham acesso à rede?

Não é relevante.

  - No departamento de informática ou na sala onde contém os equipamentos de rede, existe algum computador pessoal?

Não é regra.

  - É permitido o uso de computadores pessoais no interior das salas onde constem equipamentos da rede da Universidade?

Não existe política para uso de computadores pessoais dos docentes.

NOTA: O objetivo nesta parte é poder proteger ao máximo o uso de computadores pessoais no interior da sala de bastidores ou departamento de informática de forma a minimizar o risco de "ataques" internos ou de acessos mal-intencionados.

- Mecanismos de segurança:
  - Quais são os tipos de mecanismos de segurança existentes?

Firewall e proxies, Autenticação centralizada através do LDAP e Federated Services, Kerberos, Radius para os acessos do exterior, mecanismos de monitorização, mecanismos de auditoria e a nível físico, possui câmaras de vigilância (apenas na entrada do departamento).

  - Qual o nível de segurança que têm?
  - Quanto a hardware, existe firewall e proxies?

Existe apenas 1 firewall, o que torna todo o sistema inseguro.

  - A autenticação é centralizada?

Sim.

  - Que tipos de mecanismos são utilizados nos acessos do exterior?

Por fibra dedicada pelo operador (NOS).

  - Existem mecanismos de monitorização?

Sim, quer a nível físico como da rede. Embora o físico seja de baixo nível.

  - Câmaras de vigilância nas entradas/saídas do departamento?

Não existe nada que possa comprovar a entrada ou saída de pessoas nessa zona/área.

NOTA: O objetivo nesta parte é entender se existe mecanismos de segurança implementados, se sim quais são, … de forma a poder perceber o nível de segurança que a rede apresenta.

- Equipa técnica:
  - Como é formada a equipa (ex.: quantos gestores, quantos técnicos, quantos administradores)?

Existem 3 equipas técnicas:

- Redes e Sistemas composta por 5 técnicos e 2 técnicos superiores;

- Desenvolvimento e Aplicações composta por 7 técnicos superiores;

- Unidade de Instalações e Equipamentos composta por 5 a 6 técnicos.

Administrador é essencialmente o Dr. Gilberto e possivelmente 1 a 2 engenheiros/técnicos delegados pelo Dr. Gilberto.

  - Quem tem privilégios e acessos a quê?

Quem de mais privilégios tem é o Dr. Gilberto, de seguida Eng. João Matos e Eng. Duarte Costa.

NOTA: O objetivo nesta parte é perceber se existe uma hierarquia e se a mesma é respeitada, bem como quem é responsável pelo quê, ou seja, quais são as suas funções e se todos os encargos são cumpridos.

✓ **Bens a proteger**

- Hardware:
  - Quantos computadores?

Computadores funcionários: 100 (funcionários) x 700 € (preço médio de cada PC) = 70 000 euros;

Computadores docentes: 253 (docentes) x 500 € (preço médio de cada PC) = 126 500 euros;

Computadores do Piso 0 e 2: 120 (PC's) x 500 € (preço médio de cada PC) = 60 000 euros;

  - Quantos servidores?

1 blade custa sensivelmente 35 000 euros

1 servidor custa sensivelmente 2 000 euros

Existem sensivelmente 40 servidores, logo total = 80 000 euros

  - Quantos switch's?

1 Switch custa sensivelmente 400 euros

Existem sensivelmente 40 switches, logo total = 16 000 euros

- Quantas impressoras?

1 impressora simples custa sensivelmente 300 euros

Existem sensivelmente 20 impressoras de baixo custo, logo total = 6 000 euros

1 impressora Canon C2020 + contrato de manutenção custa sensivelmente 3 000 euros

Existem sensivelmente 20 impressoras C2020, logo total = 60 000 euros

- Equipamento de comunicações…

Em telefones/telemóveis ligados em rede têm um custo total = 40 000 euros

1 Projetor custa sensivelmente 200 euros

Existem sensivelmente 20 Vídeo projetores com um custo total = 4 000 euros

- **VALOR TOTAL INVESTIDO em hardware** = **500 mil euros**

NOTA: O objetivo nesta parte é perceber a quantidade de equipamento de rede (em funcionamento ou não) que a universidade possui e qual o seu investimento para posteriormente fazer uma análise de forma a minimizar os riscos de segurança.

- Software
  - Sistemas operativos?

4 500 euros Anuais em SQL Servers e outras licenças.

- Office's?

20 000 euros Anuais em Contas office 365

- Ambientes de desenvolvimento…

400 euros Anuais em ambientes Windows, Visual Studio e 6 ferramentas.

- **VALOR TOTAL INVESTIDO em software** = **valor na ordem dos 30 mil euros.**

NOTA: O objetivo nesta parte é perceber a quantidade de software de rede existente (em funcionamento ou não) que a universidade possui, se está atualizado e qual o seu investimento para posteriormente fazer uma análise de forma a minimizar os riscos de segurança.

- Informação
  - Administrativa (contratos, ofícios, etc…)

Parte da gestão da universidade = ordem dos 200/300 000 euros

- Documentos pessoais

Informação pessoal de base de dados = valor indefinido

- Trabalhos académicos

O custo dos trabalhos académicos tem a ver com a não aprovação da cadeira, o que por sua vez implica ao aluno permanecer mais 1 ano, ou não. Daí também não dar para ter um valor em concreto.

- Trabalhos científicos

Valor Qualitativo, ou seja, inestimável.

- **VALOR TOTAL INVESTIDO em informação** = **valor muito elevado, na ordem dos milhões, talvez.**

NOTA: O objetivo nesta parte é perceber qual o tipo de informação que existe, qual o grau de privacidade que corresponde e se está a ser respeitado e se a privacidade está assegurada.

- Tempo
  - Tempo de paragem das atividades:
    - Custo de aulas teóricas/práticas, de realização de avaliações e de docentes, em caso de falha ou ataque a um determinado sistema ou servidor…

Média de ganhos de docente: 2 000 euros por mês/ 28 000 euros por ano (14 meses).

Existem 253 docentes logo total: 506 000 euros por mês/ 7 084 000 euros por ano (14 meses).

Média de ganhos de funcionários: 1000 euros por mês/ 14 000 euros por ano (14 meses).

Existem 150 funcionários logo total: 150 000 euros por mês/ 2 100 000 euros por ano (14 meses).

Custo de uma aula teórica (2 horas): 42 euros (por hora) x 2 = 84 €

Custo de salário do professor a dividir por 4 (4 semanas = 1 mês) a dividir por 12 (12 horas por semana de aulas). De seguida é só multiplicar pelo número de horas de aula.

Custo de uma aula prática (3 horas): 42 euros (por hora) x 3 = 126 €

- VALOR TOTAL = **valor na ordem dos milhões (ano).**
  - Tempo de reparação
    - Custo da equipa técnica

O custo das equipas técnicas irá variar devido às suas funções e contratos. Uma equipa técnica (2 técnicos), por exemplo, responsáveis pela manutenção do ar condicionado pode ter um custo de 2600 euros por mês. Existem cerca de 4 equipas técnicas onde cada equipa tem em média 5 a 6 técnicos.

- VALOR TOTAL = **valor na ordem de meio milhão de euros.**

NOTA: O objetivo nesta parte é entender que o tempo que leva a recuperação de um equipamento, um sistema ou uma rede a estar novamente segura é relevante para o perigo que a universidade pode enfrentar. Também em caso de falha ou ataque a um determinado recurso pode implicar imensos danos não só físicos como também orçamentais.

- <u>Outros bens</u>
  - Equipamentos laboratoriais

Em equipamento na área de Redes existe uma quantia aproximada de 100 mil euros.

Em equipamento na área de Eletrónica existe uma quantia aproximada de 100 mil euros.

Com as restantes áreas, existe num total (todas as áreas) 500 000 euros.

  - Recursos financeiros
  - Secretaria
  - Má preparação dos alunos

A má preparação dos alunos poderá ir, no máximo, à repetição de 1 ano de curso. Ou seja, o pagamento das propinas + alimentação + deslocação.

Por aluno o valor andaria por volta dos 2 700 euros.

- VALOR TOTAL = **valor na ordem de um milhão de euros.**

- <u>Valor global dos bens a proteger</u>
  - Fazendo as contas de tudo, a universidade/departamento de informática "sobrevive" a uma perda total no SI?

2º Documento: Tabela para identificação do tempo/custo de reparação/recuperação

	Tempo de Reparação (hh:mm)	Tempo de Recuperação (hh:mm)	Custos de Reparação (€)	Custos de Recuperação (€)
Avaria de servidor **4/5 vezes por ano**	2h a 8h	30 minutos a 3h	100 € a 500 €	0 € a 100 €
Ataque DoS **15/20 vezes por ano**	1h a 4h	1h a 2h	20 € a 100 €	20 € a 50 €
Sabotagem **15/20 vezes por ano**	Poucos casos/simples	10 minutos a 1h	0 € a 50 €	-
Ataque vírus **30/40 vezes por ano**	1h a 20h	2h	40 € a 60 €	-
Avaria de hardware **30/40 vezes por ano**	1h a 3h	10 minutos a 1h	30 € a 180 €	0 € a 30 €
Corte na rede local **2/3 vezes por ano**	1h a 2h	30 minutos	40 € a 60 €	10 € a 20 €
Corte no acesso à Internet **1 vez por ano**	1h	1h	-	-
Sobrecarga de corrente **1/2 vezes por ano**	1h a 2h	2h a 4h	0 € a 4000 €	0 € – 500 €
Avaria de Ar condicionado	3h a 6h	1h	600 €	10 € a 50 €
Erros Programas **20/30 vezes por ano**	30 minutos a 2/3 dias	1 a 2 dias	20 € a 3000 €	0 € a 1500 €
Erro Humano	-	-	-	-
Inundações	-	-	-	-
Incêndio	-	-	-	-

Exemplos para identificar o tempo/custo de reparação/recuperação

Exemplo1: um site que fique em baixo, quanto tempo demora a recuperar? Uma hora? Um dia? E qual o seu custo?

Exemplo2: Suponhando que houve um ataque externo, quanto tempo leva a repor o último backup e o seu custo?

Exemplo3: Se for apanhado um computador com vírus, quanto tempo é que leva a repor um sistema e o seu custo?

Exemplo4: Avariou um servidor, quanto tempo leva a sua recuperação e o seu custo?

Exemplo5: Houve uma perda de informação, quanto tempo leva a sua recuperação e o seu custo?

Exemplo6: Uma máquina de hardware antiga que avariou, se for recuperável qual é o tempo que vai ficar desligada até receber a peça? etc… depois por estimativa, quantas máquinas avariam por ano?

Exemplo7: Falha uma máquina de email, supondo que falha durante 5 horas. Se os emails forem críticos perdem-se. Mas se não forem críticos e se chegarem com 5 horas de atraso, não têm grande impacto nem custo algum. Apenas existe custo do pessoal técnico a reparar alguma coisa.

A.3 Documentos com as respetivas questões respondidas

A Lista abaixo indicada enumera todos os equipamentos ativos, atualmente, em cada bastidor e equipamentos principais da rede WI-FI. [45]

Lista de equipamentos de rede do Campus da UMa

- ✓ **Equipamentos Comutadores (Switchs):**

32 3Com SS3 Switch 4400 24 portas

2 3Com SuperStack3 Switch 4050

2 3Com 4800G 24-port

1 SMC 8024L2

2 3Com SS3 Switch 4500

2 3Com Baseline Switch 2924 - PWR Plus (POE)

2 3Com 3300XM 24 portas

1 3Com SS3 Switch 3300 24 portas

1 3Com SuperStack 3 Switch 3300 TM

1 3Com SuperStack II Dual Speed Hub 500 de 12 portas

1 Cisco Catalyst 2960-X-24TS-LL (LAN Lite) com 24 portas 10/100/1000

2 Cisco SF300-24 com 24 portas FE e 4 GE

4 TP-LINK T1700G-28TQ 24GE + 4 Uplink (3 são da AAUMa)

2 TLP-Link TL-SG1024D

6 TLP-Link TL-SG1024DE

6 TLP-Link TL-SG1024DE POE novos

✓ **<u>Equipamentos de Segurança (Firewall):</u>**

1 Cisco PIX 535 Security Appliance Unrestricted Software License (Ref: PIX-535-UR-BUN) – PIX 535-UR Bundle (Chassis, Unrestricted SW, 2 FE, VAC+) com: 1 Cisco PIX 66-MHz four-port 10/100 Fast Ethernet int. card, RJ45 (Ref: PIX-4FE-66) & 3 Cisco PIX 66-MHz Gigabit Ethernet int, card, Multimode (SX) SC (Ref: PIX-1GE-66)

- ✓ **Equipamentos de Encaminhamento (Router):**

1 Cisco 7206VXR com NPE-G1 (IOS v. 12.4) com 1 porta FastEthernet e 2 portas série (2 circuitos ATM 2Mbps Fx-Lx)

- ✓ **Equipamentos de Rede Sem Fios (Access Points):**

120 Cisco Aironet 1100 Series Access Points 802.11g, Single MPCI Radio, Int Ant (112 na Penteada e 8 no Colégio dos Jesuítas)

120 Power Injector for 1100 Series

8 Cisco Aironet 350 Series Bridge 2.4GHz Wireless Building-to-Building Kit (Ligação Penteada – Hotel S. João, Hotel S. João- Colégio dos Jesuítas)

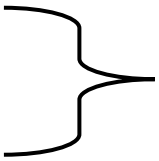
Anexo C – Lista de ativos da UMa

Neste anexo encontram-se todos os ativos que foram possíveis apurar, resultantes da recolha das informações feitas por meio das entrevistas e questionários.

Lista de Ativos da UMa

Recursos Humanos

- ✓ 2800 Alunos
- ✓ 253 Docentes
- ✓ 12 Não Docentes
- ✓ 150 Funcionários



Número total de utilizadores com acesso à rede ≥ **3215**

- ✓ Utilizadores da AAUMa (Associação Académica da Universidade da Madeira)
- ✓ Utilizadores do SASUMa (Serviço de Ação Social da Universidade da Madeira)
- ✓ Utilizadores do Colégio dos Jesuítas
- ✓ Utilizadores do Centro de Investigação
- ✓ Utilizadores do CITMA (Centro de Ciência e Tecnologia da Madeira)

Hardware

- ✓ 500 computadores fixos
- ✓ 2000 portáteis
- ✓ 20 impressoras de secretária
- ✓ 20 impressoras Canon C2020
- ✓ 20 projetores
- ✓ 400 telefones fixos
- ✓ 30 UPS (Uninterruptible Power Supply – Fonte de Alimentação Ininterrupta)

Software

- ✓ Sistemas operativos (Linux/Windows)
- ✓ Contas Office 365
- ✓ Base de dados
- ✓ Ambientes de desenvolvimento

Rede

- ✓ 1 servidor blade
- ✓ 15 servidores HP
- ✓ 1 firewall (CISCO PIX)
- ✓ 120 access point's

- ✓ 40 switches
- ✓ 1 router CISCO
- ✓ 1 servidor web
- ✓ 25 servidores Linux/Windows

Instalações físicas

- ✓ 25 salas de aula
- ✓ 4 salas de estudo
- ✓ 10 anfiteatros
- ✓ 1 sala senado
- ✓ 70 laboratórios
- ✓ 160 gabinetes
- ✓ 1 Bar
- ✓ 1 Cantina
- ✓ Biblioteca
- ✓ Parque estacionamento interno
- ✓ Parque estacionamento externo
- ✓ Armazéns
- ✓ Oficinas
- ✓ Residência universitária

Estrutura organizacional

- ✓ Conselho geral
- ✓ Reitor
- ✓ Conselho de gestão
- ✓ Conselho pedagógico

NOTA: De toda esta lista, os ativos considerados mais relevantes para a UMa foram o **sistema financeiro**, o **sistema documental** e o **sistema de informação académica**.

O Sistema Documental é constituído essencialmente por documentos de trabalho (cursos, atas, disciplinas, processos, etc…) e por versões finais de regulamentos e despachos, baseado no sharepoint (Windows). É neste sistema que consta todo o processo interno que gere os documentos e que produz os ficheiros para o sistema de documentação. O Sistema de Informação Académico é constituído por todos os dados dos alunos, dos cursos, dos planos e das avaliações. Os trabalhos não costumam estar nesta plataforma. Basicamente é um sistema onde centra-se na parte administrativa registando todo o percurso do aluno, incluindo os pagamentos e as inscrições. O Sistema Financeiro é constituído por todos os documentos ligados à parte financeira.

Efetuada a recolha de informação, verifica-se que o Sistema Financeiro e o Sistema de Informação Académico, não apresentam redundância, por serem sistemas enormes o que por sua vez, em caso de uma falha, por exemplo num servidor, os sistemas correm o risco de só estarem disponíveis dias depois, devido ao facto de ser tudo feito manualmente e por possuírem sistemas de alarme antigos.

Anexo D – Avaliação dos ativos

Neste anexo encontra-se a lista de ativos aos quais foram possíveis apurar os seus valores estimados e que resultaram da recolha de dados através das entrevistas e questionários elaborados para o efeito.

- ✓ **Hardware**:
  - Custo computadores?

Computadores dos funcionários: 100 (funcionários) x 700 € (preço médio de cada PC) = 70 000 €;

Computadores dos docentes: 253 (docentes) x 500 € (preço médio de cada PC) = 126 500 €;

Computadores do Piso 0 e 2: 120 (PC's) x 500 € (preço médio de cada PC) = 60 000 €;

Total = 256 500 €

  - Custo servidores?

1 servidor blade com 3 lâminas custa sensivelmente 35 000 €

1 servidor custa sensivelmente 2 000 €

Existem sensivelmente 40 servidores, logo total = 80 000 €

Total = 115 000 €

  - Custo switch's?

1 Switch custa sensivelmente 400 €

Existem sensivelmente 40 switches, logo total = 16 000 €

Total = 16 000 €

  - Custo impressoras?

1 impressora secretária custa sensivelmente 300 €

Existem sensivelmente 20 impressoras de secretária, logo total = 6 000 €

1 impressora Canon C2020 + contrato de manutenção custa sensivelmente 3 000 €

Existem sensivelmente 20 impressoras Canon C2020, logo total = 60 000 €

Total = 66 000 €

  - Custo de equipamento de comunicações e etc…?

Em telefones/telemóveis ligados em rede têm um custo total = 40 000 €

1 Projetor custa sensivelmente 200 €

Existem sensivelmente 20 Vídeo projetores com um custo total = 4 000 €

Total = 44 000 €

- **VALOR TOTAL INVESTIDO em hardware** = **1 milhão de euros**

✓ **Software**:

- Custo em sistemas operativos?

4 500 € anuais em SQL Servers e outras licenças.

- Custo em contas Office 365?

20 000 € anuais

- Custo em ambientes de desenvolvimento…

400 € anuais em ambientes Windows, Visual Studio e 6 ferramentas.

- **VALOR TOTAL INVESTIDO, por ano, em software** = **valor na ordem dos 30 mil euros.**

✓ **Informação**:

- Custo administrativo (contratos, ofícios, etc…)

Parte da gestão da universidade está na ordem dos 200 000 € a 300 000 €

- Custo em documentos pessoais

Informação pessoal de base de dados foi considerado um valor indefinido

- Trabalhos académicos

O custo dos trabalhos académicos tem a ver com a não aprovação da cadeira, o que por sua vez implica ao aluno permanecer mais 1 ano, ou não. Daí também não dar para ter um valor em concreto.

- Trabalhos científicos

O custo dos trabalhos de investigação desenvolvidos na UMa tem um valor qualitativo, ou seja, inestimável. O valor quantitativo seria talvez na ordem dos milhares de milhões de euros

- **VALOR TOTAL INVESTIDO em informação** = **valor muito elevado, provavelmente na ordem dos biliões.**

- ✓ **<u>Tempo</u>**:
  - Tempo de paragem das atividades:

Custo de aulas teóricas/práticas, de realização de avaliações e de docentes, em caso de falha ou ataque a um determinado sistema ou servidor:

Média de ganhos de docente: 2 000 € por mês que equivale a 28 000 € por ano.

Existem 253 docentes logo total: 506 000 € por mês que equivale a 7 084 000 € por ano.

Média de ganho de um funcionário: 1000 € por mês que equivale a 14 000 € por ano.

Existem 150 funcionários logo total: 150 000 € por mês que equivale a 2 100 000 € por ano.

Custo de uma aula teórica (2 horas): 42 € (por hora) x 2 horas = 84 €

Custo do salário do professor a dividir por 4 (4 semanas = 1 mês) a dividir por 12 (12 horas por semana de aulas) e multiplicando pelo número de horas de aula.

Custo de uma aula prática (3 horas): 42 € (por hora) x 3 = 126 €

É possível ainda existirem outros custos, desta forma simplificou-se ao máximo e atribuiu-se um valor total na ordem dos milhões.

  - VALOR TOTAL = **valor na ordem dos milhões.**
  - Tempo de reparação

Custo da equipa técnica

O custo das equipas técnicas irá variar devido às suas funções e contratos. Uma equipa técnica (2 técnicos), por exemplo, responsáveis pela manutenção do ar condicionado pode ter um custo de 2600 € por mês. Existem cerca de 4 equipas técnicas onde cada equipa tem em média 5 a 6 técnicos.

  - VALOR TOTAL = **valor na ordem de meio milhão de euros.**
- ✓ **Custo de outros ativos**
  - Equipamentos laboratoriais

Em equipamento na área de Redes existe uma quantia aproximada de 100 000 €.

Em equipamento na área de Eletrónica existe uma quantia aproximada de 100 000 €.

Com as restantes áreas, existe num total 500 000 €.

  - Recursos financeiros
  - Secretaria
  - Má preparação dos alunos

A má preparação dos alunos poderá ir, no máximo, à repetição de 1 ano de curso. Ou seja, o pagamento das propinas juntamente com o pagamento de alimentação e pagamento de passe para deslocação.

Por aluno o valor andaria por volta dos 2 700 €.

- VALOR TOTAL = **valor na ordem de um milhão de euros.**

Perante estes resultados, o valor final de todos os ativos da UMa é praticamente incalculável na medida em que é óbvio que em caso de uma perda total no Sistema Informático, a universidade não "sobrevive".

Anexo E – Tabela das ameaças aos ativos escolhidos

A tabela seguinte contém algumas das ameaças identificadas dos ativos escolhidos.

Ativo	Ameaça
Sistema Financeiro	Avaria de equipamento (servidor)
	Ataque informático (ex.: DoS)
	Perda de informação
	Sabotagem
	Ataque através de software (ex.: vírus)
	Corte na rede local
	Corte no acesso à internet
	Acidente com equipamento
	Sobrecarga de corrente
	Avaria de equipamento (ar condicionado)
	Acesso não autorizado
	Erros Programas (configurações)
Sistema Documental	Avaria de equipamento (servidor)
	Ataque informático (ex.: DoS)
	Perda de informação
	Sabotagem
	Ataque através de software (ex.: vírus)
	Corte na rede local
	Corte no acesso à internet
	Acidente com equipamento
	Sobrecarga de corrente
	Avaria de equipamento (ar condicionado)
	Acesso não autorizado
	Erros Programas (configurações)
Sistema de Informação Académico	Avaria de equipamento (servidor)
	Ataque informático (ex.: DoS)
	Perda de informação
	Sabotagem
	Ataque através de software (ex.: vírus)
	Corte na rede local
	Corte no acesso à internet
	Acidente com equipamento
	Sobrecarga de corrente
	Avaria de equipamento (ar condicionado)
	Acesso não autorizado
	Erros Programas (configurações)

Anexo F – Tabela das vulnerabilidades aos ativos escolhidos

A tabela seguinte contém algumas das vulnerabilidades identificadas aos ativos escolhidos. No fim da tabela encontram-se alguns ativos que neste momento estão numa fase crítica.

Ativo	Ameaça	Vulnerabilidade
Sistema de Informação Académico	Acesso não autorizado	Controlos de acesso inadequados
		Não aplicação de políticas
		Equipamento desatualizado
		Mecanismo de acesso simples
		Falha na gestão de credenciais acesso
	Erros Programas (configurações)	Falta de procedimentos
		Falta de conhecimento
		Parâmetros incorretos
		Inexistência de cópias
	Ataque (vírus)	Falta de conhecimento
		Falta de planeamento de contingência
		Falta de política de segurança
		Bugs em aplicações
	Perda de informação	Planeamento de contingência ineficaz
	Falha/avaria de equipamento	Falta de redundância
		Inexistência de Backups
Sistema Financeiro	Acesso não autorizado	Controlos de acesso inadequados
		Não aplicação de políticas
		Equipamento desatualizado
		Mecanismo de acesso simples
		Falha na gestão de credenciais acesso
	Erros Programas (configurações)	Falta de procedimentos
		Falta de conhecimento
		Parâmetros incorretos
		Inexistência de cópias
	Ataque (vírus)	Falta de conhecimento
		Falta de planeamento de contingência
		Falta de política de segurança
		Bugs em aplicações
	Perda de informação	Planeamento de contingência ineficaz
	Falha/avaria de equipamento	Falta de redundância
		Inexistência de Backups
Sistema Documental	Acesso não autorizado	Controlos de acesso inadequados
		Não aplicação de políticas
		Equipamento desatualizado
		Mecanismo de acesso simples
		Falha na gestão de credenciais acesso

	Erros Programas (configurações)	Falta de procedimentos
		Falta de conhecimento
		Parâmetros incorretos
		Inexistência de cópias
	Ataque (vírus)	Falta de conhecimento
		Falta de planeamento de contingência
		Falta de política de segurança
		Bugs em aplicações
	Perda de informação	Planeamento de contingência ineficaz
	Falha/avaria de equipamento	Falta de redundância
		Inexistência de Backups
Firewall	Falha em todo o sistema rede	Firewall obsoleta
		Inexistência de Política de atualização
Sala servidores	Acesso não autorizado	Políticas de controlo de acesso inexistentes
		Falta de mecanismos de registos de acesso
Máquinas (Windows)	Falha em equipamento	Política de atualização inexistente
…	…	…

Anexo G – Tabela da Análise do risco

Na tabela seguinte consta a análise do risco que foi realizada tendo em conta as ameaças identificadas aos ativos da UMa, onde combina a probabilidade de ocorrência com o impacto resultante.

Tipo	Ameaça	Origem (*)	Probabilidade/Impacto
Ameaça física	Acidente com equipamento	A, I	6/3
	Sabotagem	A, I	6/4
	Corte na rede local de dados	A, I	5/4
	Corte no acesso à internet	A, I	5/3
	Sobrecarga de corrente	A, I, N	5/5
Comprometimento da informação	Ataque servidor	I	6/4
	Vírus	A, I	7/4
Falha técnica	Saturação do sistema de informação	A, I	5/5
	Erros software	A	6/5
	Falha de equipamento	A	7/3
Comprometimento de funções	Indisponibilidade de recursos humanos	A, I, N	6/5
	Erros humanos	A, I	4/3
Ação não autorizada	Apropriação indevida de informação	I	7/4

Anexo H – Avaliação do risco

Neste anexo encontra-se a maior parte dos desafios/problemas da UMa, por contexto, onde se encontram referenciados consoante o nível de risco que possuem, atualmente.

1. Segurança Organizacional

Relativamente à segurança organizacional, o risco é médio, atendendo ao seguinte:

a) Não existe nenhuma política de segurança;
b) Não foi feita nenhuma auditoria de forma a poder verificar o atual estado da rede, bem como da própria instituição, no que diz respeito à segurança da informação;
c) Não existe um documento de atribuição de responsabilidades e funções;
d) As equipas das mais diversas áreas são de número reduzido.

Perante qualquer ameaça mais pormenorizada levará a uma lenta resposta de atuação o que acabará por poder afetar o correto funcionamento dos serviços e sistemas da instituição.

2. Segurança Física e Ambiental

Relativamente à segurança física e ambiental, o risco é médio, atendendo ao seguinte:

- Não estão implementadas medidas se segurança física, eficiente, para as salas que contêm material sensível;
- Os acessos às salas com material sensível são feitos por chave tradicional, ou seja, não há registos de quem entra e/ou sai;
- A existência de chaves mestras para o acesso às salas com material sensível;
- Utilização de algumas salas que contêm equipamento sensível como arrumos o que prejudica a qualidade do ambiente;
- Não há apoio técnico ou política para auxiliar os alunos ou professores a encriptar os seus dados ou onde deixar os seus dados mais confidenciais.

Em caso de alguma pessoa, com maldade, pedir a chave na receção para aceder à sala "x" que contém determinado tipo de material informático e dizer que vem da parte do administrador, tem logo acesso à mesma.

3. Segurança de Equipamentos

Relativamente à segurança de equipamentos, o risco é baixo, atendendo ao seguinte:

a) Manuseamento e as operações técnicas de manutenção são feitas por pessoal técnico e devidamente habilitado;

b) Não existe uma política de operações que garanta a normalização dos mecanismos de segurança;
c) As intervenções técnicas encontram-se ao critério de cada técnico;
d) Nem todos os bastidores encontram-se bem protegidos devido ao mau planeamento de instalação que impede a arrumação dos cabos e equipamentos.

Em caso de falha ou avaria de algum equipamento, na maior parte das vezes são detetadas logo e o processo de recuperação, geralmente, é relativamente rápido. Mas em caso de uma avaria ou falha num serviço ou sistema mais grave, a recuperação pode ser demorada atendendo ao facto da inexistência de processos de manutenção eficazes.

4. Segurança da Rede

Relativamente à segurança da rede, o risco é baixo atendendo ao seguinte:

a) Não existe redundância na ligação de rede nos três edifícios da instituição;
b) Existência de alguns equipamentos de rede de vários fabricantes para as mesmas funções que dificultam a gestão e provocam incompatibilidades;
c) Existência de equipamentos de rede obsoletos;
d) Não existe um controlador que facilite a monitorização e configuração dos AP's;
e) Não existe política definida para atribuição de acessos à rede wireless a que pessoas que venham visitar ou realizar atividades na instituição e precisem de acesso.

Em caso da existência de algumas ameaças, tais como, falhas em equipamentos, cortes no acesso á rede e etc… tendo em conta a probabilidade de ocorrência e o impacto, acaba por não ser tão significante o risco.

5. Segurança Aplicacional

Relativamente à segurança aplicacional, o risco é baixo atendendo ao seguinte:

a) Os backups são realizados de forma adequada e periodicamente;
b) Encontra-se neste momento, em fase de testes, um serviço de política de atualizações que permite a distribuição e controlo das atualizações;
c) Existem algumas máquinas que não se encontram devidamente atualizadas;
d) Existem algumas máquinas com sistemas operativos antigos, na área dos docentes;
e) Não existe software de monitorização de ataques;
f) Não existe políticas de criptografia e gestão de chaves no armazenamento.

Em caso de infeção de alguma máquina com sistema operativo antigo e/ou obsoleto que esteja ligada à rede é um potencial risco na rede.

6. Segurança de Recursos Humanos

Relativamente à segurança de recursos humanos, o risco é baixo atendendo ao seguinte:

a) Existe um documento formal em que constam as responsabilidades dos contratados (funcionários, colaboradores, docentes e não docentes) mas, não se encontra definido na política de segurança;
b) O processo de registo dos alunos é feito adequadamente;
c) O processo de revogação dos alunos é inexistente. Os antigos alunos continuam a pertencer aos "utilizadores ativos";
d) Não há consciencialização nem formação dos funcionários.

A falta de consciencialização, formação e alinhamento com as políticas de segurança da instituição pode levar a que um colaborador possa cometer vandalismo ou sabotagem.

7. Conformidade

Relativamente à conformidade, o risco é baixo tendo em conta que este tema está em desenvolvimento apesar de se encontrar numa fase já posterior à implementação.

Anexo I – Lista dos Problemas da UMa relevantes

Neste anexo encontra-se a lista dos problemas da UMa que foram escolhidos de forma a serem tratados e mitigados.

- Inexistência de documento formal de política de segurança;
- O atual estado da segurança da informação ser desconhecido por não haver formação por parte dos utilizadores, investigadores, técnicos, funcionários, docentes e não docentes, etc…;
- Inexistência de realização de auditoria regular de forma a verificar o estado da segurança da informação da rede bem como de toda a instituição, embora esteja atualmente a ser realizada uma auditoria específica;
- Inexistência de documento de atribuição de responsabilidades e funções;
- Existência de máquinas com Windows XP (sistema operativo antigo), pelo menos na área dos docentes, onde encontram-se pastas partilhadas. Um computador infetado ligado à rede interna é um potencial risco na rede;
- Inexistência de processo de revogação dos alunos. Os antigos alunos continuam a pertencer aos “utilizadores ativos”;
- Não implementação de medidas de segurança física, eficientes, para as salas que contêm material sensível;
- Inexistência de registos de acesso às salas com material sensível, por estes serem feitos por chave tradicional, ou seja, não controlando quem entra e/ou sai;
- A existência de chaves mestras para o acesso às salas com material sensível;
- Utilização de algumas salas que contêm equipamento sensível como arrumos o que prejudica a qualidade do ambiente;
- Inexistência de apoio técnico ou política para auxiliar os alunos ou professores a encriptar os seus dados ou onde deixar os seus dados mais confidenciais.

Anexo J – Documento de Políticas de Segurança

Neste anexo encontram-se as seis políticas que foram propostas para minimizar os riscos obtidos através da identificação, análise e avaliação dos problemas e desafios da rede da UMa.

1. Política de Segurança da Informação

Documento de Política de Segurança

UNIVERSIDADE da MADEIRA

Campus Universitário da Penteada

Madeira, Funchal 9020 – 105

291 705 000

info@mail.uma.pt

Controlo de Versões e Aprovação

Histórico de alterações

Data	Versão	Autor	Comentários	Aprovação
15/01/2019	1.0	João Azevedo	Elaboração do documento	Em aprovação

Classificação do Documento

Classificação	Autorização de Distribuição
Pública	Este documento deve ser exposto nos locais próprios e de acesso público à UMa. Este documento deve ser publicado no site https://www.uma.pt/ (sharepoint) Qualquer alteração a esta definição de Autorização de Distribuição tem de ser aprovada pelo Conselho de Administração.

Responsabilidades do Documento

ELABORAÇÃO, ATUALIZAÇÃO	Administrador da Segurança da Informação*
APROVAÇÃO	Conselho de Administração (CA)*
REVISÃO	(a definir)*

*(identificar a pessoa ou as pessoas responsáveis)

Glossário

PSI – Política de Segurança da Informação

ISO – International Organization for Standardization

IEC – International Electrotechnical Commission

UMa – Universidade da Madeira

Índice

1. Introdução

Hoje em dia, a informação, os processos e os sistemas com ela relacionados, as redes e as pessoas envolvidas no seu manuseamento, são fundamentais para o negócio das empresas/instituições e/ou organizações e, tal como outros ativos, requerem proteção contra vários riscos a que possam estar sujeitos. Verifica-se, cada vez mais, que na UMa, existe uma dependência do normal funcionamento dos sistemas de informação e infraestruturas de comunicações, pelo que as ameaças informáticas são também uma ameaça regular ao normal funcionamento da instituição.

Tanto a informação como os restantes ativos da UMa estão sujeitos a ameaças deliberadas e acidentais, enquanto que os processos, sistemas, redes e pessoas relacionadas possuem vulnerabilidades, o que por sua vez faz com que os riscos à segurança da informação estejam sempre presentes. A aplicação de uma política de segurança da informação fará com que o nível de risco seja o mais baixo possível, protegendo a UMa das ameaças e vulnerabilidades, reduzindo o impacto aos seus ativos. Isto é, a segurança da informação pode ser obtida a partir da implementação de um conjunto de controlos adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Esses controlos necessitam de ser estabelecidos, implementados, monitorizados, revistos e aprimorados, quando necessário, para garantir que os objetivos específicos de segurança e negócios da instituição sejam atendidos.

De forma a limitar a probabilidade de uma ameaça atingir a confidencialidade, a integridade e a disponibilidade dos ativos de informação, como por exemplo, a fraude, o vandalismo, a sabotagem, entre outros, a UMa preocupa-se com a segurança da informação.

Deste modo, por meio de esforços contínuos e geridos, criou-se os alicerces para a proteção dos ativos de informação, assegurando a redução dos riscos, a redução do custo, de certa forma, o atendimento aos requisitos legais e a imagem e reputação da UMa.

2. Âmbito

Esta PSI é aplicável a toda a instituição, ou seja, a todos os que direta ou indiretamente possuam acesso à UMa.

3. Objetivos

O principal objetivo desta política de segurança é a definição essencialmente dos princípios e regras básicas de gestão de segurança da informação, na Uma. Mas também:

- ✓ Contribuir com iniciativas relativas à segurança da informação;
- ✓ Auxiliar na salvaguarda dos ativos da UMa – pessoas, propriedade, finanças e reputação;
- ✓ Prestar assistência e melhorar a qualidade da tomada de decisões em toda a UMa;
- ✓ Atender aos requisitos legais e/ou estatutários.

4. Princípios

A segurança da informação deve ser entendida como uma responsabilidade coletiva. Assim sendo, o conjunto de regras que possui esta PSI guiar-se-á pelos seguintes princípios:

a) **Confidencialidade**: garantia de que a informação não esteja ou seja disponível ou revelada a pessoas, sistemas, órgãos ou entidades não autorizadas pela UMa;
b) **Integridade**: garantia de que a informação não foi modificada ou destruída de forma não autorizada ou até de forma acidental, quer na origem, no transporte e/ou no seu destino;
c) **Disponibilidade**: garantia de que a informação esteja acessível, a pessoas, sistemas, órgãos ou entidades, autorizadas pela UMa, sempre que for necessário;
d) **Autenticidade**: garantia de que a informação é contruída por pessoas, sistemas, órgãos ou entidades com permissão para tal;
e) **Não repúdio**: garantia de que o emissor da informação não negue posteriormente a autoria da mesma;
f) **Conhecimento**: garantia de que todos os funcionários, colaboradores, docentes, não docentes e entidades prestadoras de serviço tenham formação e competências que permitam a execução das suas funções, mas também tenham formação na segurança da informação;
g) **Responsabilidade**: todos os indivíduos, sem exceção, que participam de alguma forma na produção, manuseamento, transporte e destruição da informação, devem ser responsáveis pela mesma.
h) **Privacidade:** garantia ao direito coletivo e pessoal, à intimidade e ao sigilo da correspondência e comunicações individuais.

5. Referências Normativas

A presente PSI encontra-se baseada nas recomendações da norma ISO/IEC 27001:2013 [3] e da norma ISO/IEC 27002:2013 [4], reconhecidas mundialmente como a norma para um sistema de gestão de segurança da informação e o código de práticas para a gestão de segurança da informação, respetivamente, além de estar de acordo com o Regulamento Geral de Proteção de Dados e outras leis vigentes.

6. Termos e Definições

Para efeitos desta política de segurança deve-se definir vários conceitos que estão intimamente ligados à Segurança da Informação. São estes:

Ativo – qualquer bem, tangível ou intangível, que tenha valor para a instituição.

Ameaça – causa potencial de um incidente indesejado, que pode resultar em danos num sistema ou organização.

Ataque – tentar destruir, expor, alterar, desativar, roubar ou obter acesso não autorizado ou fazer uso não autorizado de um recurso.

Autenticação – garantia de que uma característica reivindicada de uma entidade é correta.

Autenticidade – propriedade que uma entidade é o que afirma ser.

Confidencialidade – garantia de que a informação não é disponibilizada ou divulgada a indivíduos, entidades, ou processos não autorizados.

Conformidade – cumprimento de um requisito.

Controlo – medida que está a modificar o risco.

Controlo de acesso – controlo de entrada e/ou saída para uma área por qualquer meio (mecânico ou eletrónico).

Disponibilidade – garantia de que qualquer informação esteja disponível sempre que utilizadores autorizados necessitem.

Diretrizes – são as regras de alto nível que representam princípios básicos que a instituição resolveu incorporar a sua gestão de acordo com a visão estratégica da alta direção. Servem como base para que as normas e os procedimentos sejam criados.

Eficácia – até que ponto as atividades planeadas são realizadas e os resultados planeados alcançados.

Evento – ocorrência ou alteração de um conjunto particular de circunstâncias.

Evento Segurança da Informação – ocorrência identificada de um sistema, serviço ou estado de rede indicando uma possível violação da política de segurança da informação ou falha de controlo ou uma situação anteriormente desconhecida que pode ser relevante para a segurança.

Integridade – garantia de que a informação estará disponível de forma correta e completa, sem alterações.

Incidente de segurança – qualquer evento adverso relacionado à segurança de sistemas de informação levando ao comprometimento de um ou mais princípios básicos de segurança da informação.

Melhoria contínua – atividade recorrente para melhorar o desempenho.

Norma – conjunto de regras que devem ser seguidas por um grupo.

Nível de risco – magnitude de um risco expresso em termos da combinação de consequências e da sua probabilidade.

Não conformidade – não cumprimento de um requisito.

Não repúdio – capacidade de provar a ocorrência de um evento reivindicado ou ação e suas entidades de origem.

Processo – conjunto de atividades interrelacionadas ou interativas que transforma entradas em saídas.

Política de segurança da informação – conjunto de princípios que norteiam a gestão da segurança da informação e que devem ser observados pelo corpo técnico e gestor da instituição, bem como pelos seus utilizadores internos e externos, a fim de garantir que os ativos estejam assegurados.

Quebra de segurança – ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações.

Risco – efeito da incerteza sobre os objetivos.

Risco de segurança da informação – potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da instituição.

Segurança da informação – preservação da confidencialidade, integridade e disponibilidade da informação.

Sensibilização – atividade de ensino que tem como objetivo orientar sobre o que é segurança da informação, fazendo com que os participantes possam perceber na sua rotina pessoal e profissional ações que precisam de ser corrigidas.

Vulnerabilidade – fraqueza de um ativo ou controlo que pode ser explorada por uma ou mais ameaças.

7. Revisão da Política

A política de segurança deverá ser revista anualmente ou em caso de ocorrência de alguma alteração de forma a garantir a conformidade, pertinência e efetividade contínuas.

A revisão deve ser efetuada por um ou mais elementos dos serviços de informática. Nesta revisão deve ser efetuada uma análise crítica dos serviços e sistemas de informação, onde podem também ser incluídas oportunidades de melhoria bem como ter em consideração a evolução tecnológica e as condições legais.

Posteriormente à fase de revisão, a política deve ser submetida ao Reitor da UMa, para que as alterações sejam aprovadas e posteriormente comunicadas a quem de respeito (comunidade da UMa ou a intervenientes a quem de respeito).

8. Diretrizes Gerais

I. É protegida a confidencialidade da informação dos alunos, estagiários, funcionários, colaboradores, docentes e não docentes, entidades externas, propriedade intelectual e quaisquer dados sensíveis.
II. É mantida a integridade de toda a informação armazenada nas bases de dados.
III. É assegurada a disponibilidade da rede de dados da UMa e dos sistemas e serviços associados.
IV. Os requisitos de segurança da informação decorrentes de imposições regulamentares Nacionais e Europeias aplicáveis e as atividades de coordenação entre as diferentes autoridades serão implementados e cumpridos.
V. A segurança da informação será gerida de acordo com os princípios do menor privilégio, necessidade de saber e segregação de deveres.
VI. Serão produzidos planos de resposta a incidentes de segurança da informação tendo em vista a prossecução da continuidade do negócio e recuperação de desastres.
VII. Os riscos de segurança da informação são compreendidos e tratados de acordo com o nível de risco aceite pela UMa.
VIII. Todos os eventos que coloquem em causa o nível de segurança da informação, serão monitorizados e serão tomadas medidas corretivas.
IX. São tomadas medidas de segurança apropriadas contra a destruição, perda, modificação, acesso ou a difusão acidental ou não autorizada da informação.
X. São desenvolvidas iniciativas de sensibilização, treino e formação sistemática dos funcionários, colaboradores, docentes e não docentes, estagiários, alunos e restantes intervenientes, em matérias de segurança da informação.

XI. Deverão ser disponibilizados relatórios do estado de segurança da informação aos responsáveis.
XII. Todos os alunos, funcionários, docentes e não docentes, estagiários, técnicos e entidades subcontratadas são responsáveis pela segurança da informação utilizada no desempenho das suas funções.
XIII. É responsabilidade de cada um comunicar as falhas de segurança da informação de que tenha tido ou venha a ter conhecimento.
XIV. É responsabilidade de cada aluno, docente, não docente, estagiário, funcionário e restantes intervenientes o bom uso e confidencialidade das credenciais de acesso.
XV. É responsabilidade de cada um aderir, cumprir com as normas e procedimentos publicados no âmbito desta política.
XVI. Não são permitidas situações que possam colocar a instituição perante violação da lei e dos regulamentos aplicáveis à mesma.

9. Responsabilidades

I. É da responsabilidade de **toda a comunidade** da UMa proteger as pessoas e os ativos da mesma. Toda a comunidade deve apoiar a política de segurança e os procedimentos associados.
II. O **Conselho Geral** é responsável por definir o desenvolvimento estratégico e a supervisão da instituição onde compete, entre outros:
    a. Propor as iniciativas que considere necessárias ao bom funcionamento da Instituição;
    b. Deliberar sobre parcerias e cooperação com outras entidades públicas ou privadas, nas diferentes modalidades previstas na lei, nos casos em que as parcerias e cooperações em causa tenham incidência estratégica ou impacto profundo na Instituição, e com audição prévia do Senado se se tratar de acordos e parcerias internacionais;
    c. Desempenhar as demais funções previstas na lei ou nos Estatutos da Universidade.
III. O **Conselho de Gestão** é responsável por:
    a. Conduzir a gestão administrativa, patrimonial e financeira da instituição e a gestão e contratação dos recursos humanos, no cumprimento da legislação em vigor para os organismos públicos dotados de autonomia patrimonial, administrativa e financeira;
    b. Promover a racionalização e a eficiência dos serviços da Universidade, podendo delegar nos órgãos das unidades orgânicas e nos dirigentes dos serviços as competências consideradas necessárias a uma gestão mais eficiente;

c. Propor ao Conselho Geral a alienação, permuta ou oneração de património ou de participações em associações ou sociedades.

IV. A **Unidade de Assuntos Académicos** é responsável pela:
   a. Gestão administrativa e académica, e de apoio ao estudante.

V. A **Unidade de Aprovisionamento e Património** é responsável por, entre outros:
   a. Organizar os processos de aquisição de empreitadas, bens e serviços de acordo com a legislação em vigor;
   b. Elaborar os contratos de aquisição de bens e serviços;
   c. Coordenar e manter atualizado o inventário dos bens móveis e imóveis da Universidade nos termos da legislação aplicável.

VI. A **Unidade de Infraestruturas e Instalações** é responsável por, entre outros:
   a. Elaborar estudos e projetos gerais, de arquitetura e coordenar os projetos de especialidades, incluindo medições e orçamentos;
   b. Fiscalizar e acompanhar obras, na Universidade;
   c. Elaborar programas preliminares, cadernos de encargos, programas de concursos, procedimentos para adjudicação de projetos, empreitadas de obras públicas, aquisição de serviços ou equipamentos;
   d. Propor medidas tendentes à conservação e manutenção das instalações e equipamentos;
   e. Manter informação sobre inventariação e cadastro do património da Universidade atualizados em articulação com a Direção de Serviços Financeiros e Patrimoniais;
   f. Coordenar os trabalhos dos prestadores externos, nomeadamente manutenção;
   g. Garantir o desenvolvimento e aplicação de planos de prevenção, emergência, contingência, de segurança e higiene e a segurança e vigilância (ativa e passiva).

VII. A **Unidade de Comunicações e Informática** contém os seguintes gabinetes, responsáveis por, respetivamente:
   a. Gabinete de Desenvolvimento de Aplicações Informáticas (GDAI) – desenvolvimento e manutenção de aplicações informáticas que integrem o sistema de informação da UMa;
   b. Gabinete de Redes e Sistemas Informáticos (GRSI) – Assegurar a fiabilidade, a segurança e o desempenho da infraestrutura tecnológica partilhada, incluindo a conectividade entre sistemas.

VIII. A **Unidade de Recursos Humanos** é responsável por:
   a. Gerir os recursos humanos;
   b. Dinamizar ações de formação e reforço de competências.

IX. Todos os restantes intervenientes, **alunos e visitantes**, são responsáveis por:
   a. Respeitar os interesses especiais da instituição que estão contidos nos regulamentos e normas internas e que são essenciais para o funcionamento diário da instituição;
   b. Zelar pela conservação e boa utilização de todos os bens da instituição.
   c.

10. Violação e Penalidades

Os docentes, funcionários, colaboradores, alunos, entidades externas e restantes utilizadores e intervenientes, caso violem a PSI, estarão sujeitos a ações como:

a) Advertência formal;
b) Suspensão;
c) Rescisão de contrato de trabalho;
d) Outra ação disciplinar e/ou processo civil ou criminal.

Deverá ser elaborado um processo disciplinar, pela administração da UMa juntamente com o responsável máximo da área afetada, para apurar as ações a aplicar.

11. Vigência

Estas regras, diretrizes, normas e/ou processos entram em vigor a partir da data de aprovação pelo conselho superior da UMa.

12. Referências

[1] "ISO/IEC 27001:2013(E) Information technology - Security techniques - Information security management systems - Requirements," 2013. [Online]. Available: https://trofisecurity.com/assets/img/iso27001-2013.pdf. [Acedido em 21 outubro 2017].

[2] ISO/IEC 27002:2013(E) - Information technology - Security techniques - Code of practice for information security controls, Second edition ed., Switzerland: ISO copyright office, 2013.

[3] ISO/IEC 27000:2016(E) - Information technology - Security techniques - Information security management systems - Overview and vocabulary, Switzerland: ISO copyright office, 2014.

2. Política – Organização de Segurança da Informação

RESUMO

Para assegurar uma gestão efetiva de segurança da informação deve ser criada uma estrutura responsável pela orientação, planeamento, implementação, manutenção e melhoria das práticas de segurança da informação que garanta que os processos operacionais salvaguardem a confidencialidade, integridade e a disponibilidade da informação, apoiando a tomada de decisões ágil sobre os riscos e investimentos a realizar no âmbito da segurança da informação e na conformidade com os requisitos externos (leis, regulamentares ou contratuais), de forma articulada com processos internos da instituição. Nesta política serão definidos os responsáveis e as suas respetivas funções de forma a manter a segurança da informação, na instituição. Serão abordados os contactos com as autoridades e por fim serão assegurados os cuidados que os colaboradores têm que ter com os dispositivos móveis no local de trabalho.

OBJETIVO

Fornecer um modelo de referência de gestão para iniciar e controlar a implementação e a operação de segurança da informação, dentro da Instituição. Assegurar a segurança na utilização de dispositivos móveis.

ÂMBITO

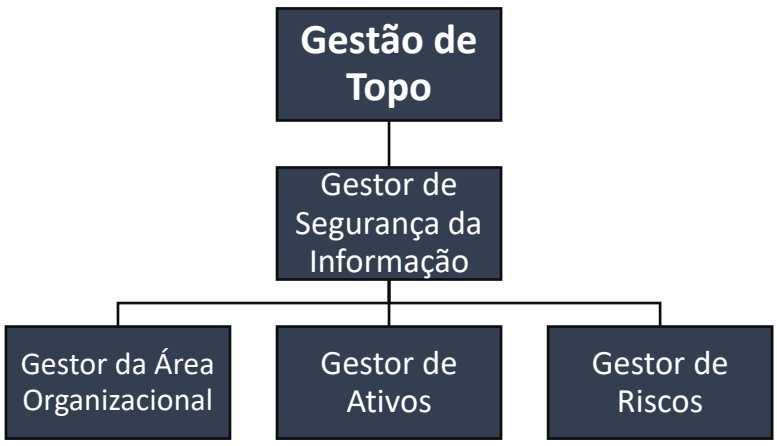
Esta política aplica-se a todos funcionários, docentes, não docentes, estagiários e restantes intervenientes da UMa.

TERMOS E DEFINIÇÕES

Para os propósitos deste documento, os termos e definições fornecidos na política de segurança da informação aplicam-se.

POLÍTICA

I. Para o efetivo cumprimento das regras estabelecidas por esta política, ficam instituídas as seguintes competências e responsabilidades nesta instituição, como mostra o seguinte organograma:



A **Gestão de Topo** da UMa tem a responsabilidade máxima de promover, controlar e monitoriza a segurança da informação da UMa, nomeadamente através da:

- Liderança e compromisso com o sistema de gestão de segurança da informação;
- Aprovação da política de segurança da informação;
- Identificação e nomeação de responsáveis para as funções relevantes para a segurança da informação, assegurando a conformidade da mesma e o registo do desempenho do sistema de gestão de segurança da informação.

O **Gestor de Segurança da Informação** da UMa é responsável por:

- Alinhar os objetivos de Segurança da Informação com os objetivos estratégicos do Departamento de Informática, definindo e mantendo atualizadas as políticas de segurança da informação, apoiando e monitorizando a implementação e melhoria contínua dos procedimentos internos de suporte;
- Desenvolver, implementar e melhorar a segurança da informação na instituição.

O **Gestor da Área Organizacional** da UMa deve ser responsável por:

- Promover, no âmbito das suas competências e valências próprias, o cumprimento das políticas, processos e procedimentos, identificando proactivamente as ameaças e vulnerabilidades que coloquem em risco a segurança da informação da UMa.

O **Gestor dos Ativos** da UMa é responsável por:

- Garantir que são classificados os ativos e que são definidos e implementados controlos adequados à proteção dos mesmos, assegurando a confidencialidade, integridade e disponibilidade dos ativos de informação que suportam.

O **Gestor de Riscos** da UMa é responsável por:

- Garantir a aplicação das medidas (técnicas, materiais, organizativas e procedimentais) adequadas que permitem atenuar, eliminar ou transferir os riscos associados aos ativos de informação, reduzindo a probabilidade de uma ameaça específica explorar as vulnerabilidades que comprometam um ativo;
- Avaliar o impacto das medidas implementadas e em consequência da análise de riscos realizada, periodicamente, reavaliar a necessidade de implementar medidas complementares.

É recomendado à Gestão de Topo da instituição definir outras responsabilidades e papéis adicionais, de acordo com o modelo institucional e requisitos de conformidade a que seja obrigada.

É recomendado à Gestão de Topo da instituição a definição de responsáveis para estabelecer contactos com grupos de interesse especial, associações profissionais ou outros fóruns especializados em segurança da informação.

II. A Gestão de Topo da instituição deve definir os responsáveis para estabelecer contactos com autoridades (por exemplo, entidades regulatórias, entidades policiais, autoridades fiscalizadoras, etc.). Esses responsáveis devem:
   a) Manter contactos adequados com as autoridades civis que permitam assegurar uma resposta atempada das mesmas face a um incidente de grandes dimensões;
   b) Manter uma lista atualizada dos contactos das autoridades relevantes a contactar em caso de necessidade, no âmbito de planos de emergência, nomeadamente com a proteção civil, polícia, bombeiros, segurança das instalações físicas.

III. É garantida a segurança do uso de dispositivos móveis na área de trabalho da UMa (Política de Dispositivos Móveis).

IV. É garantido que todos os materiais confidenciais são removidos do espaço de trabalho (Política de Mesa Limpa e Ecrã Limpo).

CONFORMIDADE

- ✓ **Medição de Conformidade**

A equipa do departamento de informática verificará a conformidade com esta política por meio de vários métodos, incluindo entre outros, acompanhamento periódico e auditorias internas e externas.

- ✓ **Exceções**

Qualquer exceção à política deve ser aprovada pela equipa do departamento de informática, antecipadamente.

- ✓ **Não Conformidade**

Um docente, não docente, funcionário ou colaborador que tenha violado esta política pode estar sujeito a ações disciplinares, incluindo até rescisão de contrato de trabalho.

OUTRAS NORMAS, POLÍTICAS, PROCESSOS RELACIONADOS

Política de Dispositivos Móveis; Política de Mesa Limpa e Ecrã Limpo.

REVISÃO

A política de segurança deverá ser revista anualmente ou em caso de ocorrência de alguma alteração de forma a garantir a conformidade, pertinência e efetividade contínuas.

Posteriormente à fase de revisão, a política deve ser submetida ao Reitor da UMa, para que as alterações sejam aprovadas e posteriormente comunicadas a quem de respeito (comunidade da UMa ou a intervenientes a quem de respeito).

HISTÓRICO DE REVISÕES

Data	Versão	Autor	Comentários
15/01/2019	1.0	João Azevedo	Elaboração do documento

3. Política de Mesa Limpa e Ecrã Limpo

RESUMO

É uma política que pode ser uma ferramenta de importação para garantir que todos os materiais confidenciais/sensíveis sejam removidos do espaço de trabalho de um utilizador e sejam guardados ou fechados quando não estiverem em uso ou quando alguém deixa o escritório ou a sala de trabalho à mercê de outros. É uma das principais estratégias para utilizar ao tentar reduzir o risco de violações de segurança no local de trabalho. Esta política também pode aumentar a consciencialização dos funcionários e ou utilizadores sobre a proteção de informações confidenciais.

OBJETIVO

É uma política que permite estabelecer os requisitos mínimos para a manutenção de uma "mesa limpa" – onde as informações mais sensíveis/críticas, como por exemplo, dados dos funcionários, alunos, etc… estão protegidas em áreas seguras e fora do local. Esta política não é só compatível com a norma ISO/IEC 27001 e ISO/IEC 27002, mas também faz parte dos controlos básicos de privacidade.

ÂMBITO

Esta política aplica-se a todos funcionários, docentes, não docentes, estagiários e restantes intervenientes da UMa.

TERMOS E DEFINIÇÕES

Confidencialidade – garantia de que a informação não é disponibilizada ou divulgada a indivíduos, entidades, ou processos não autorizados.

Norma – conjunto de regras que devem ser seguidas por um grupo.

Não conformidade – não cumprimento de um requisito.

Restrito – que é limitado ou que se destina a algo limitado.

Segurança da informação – preservação da confidencialidade, integridade e disponibilidade da informação.

Sensível – algo que tem muita importância e que pode resultar em perda de vantagem ou do nível de segurança.

POLÍTICA

I. Os intervenientes são obrigados a garantir que todas as informações sensíveis/confidenciais, no formato em papel ou digital, estejam seguras na sua área de trabalho, quer quando estejam presentes ou não nesse local.
II. Os computadores (workstations, portáteis ou computadores de secretária) devem estar bloqueados quando os responsáveis estiverem ausentes.

III. Os computadores (workstations, portáteis ou computadores de secretária) devem ser bloqueados e ou desligados, sempre que possível, ao fim do dia de trabalho.
IV. Qualquer informação restrita ou sensível deve ser removida da secretária e trancada na gaveta ou guardada num outro local seguro, sempre que a mesma não estiver ocupada.
V. As gavetas ou armários que contenham informações restritas ou sensíveis devem-se manter fechados e trancados, sempre que não estiver em uso.
VI. As chaves utilizadas para aceder a esses armários e gavetas não devem ser deixadas em qualquer lado. Devem ser guardadas num local próprio e seguro.
VII. As senhas não podem ser deixadas em etiquetas, papéis ou outro tipo de notificação em ou sob o computador, nem podem ser deixadas num local acessível.
VIII. As impressões, contendo informações restritas ou sensíveis devem ser imediatamente removidas da impressora.
IX. Após a eliminação, esses documentos devem ser triturados nos contentores trituradores próprios.
X. Os quadros "brancos" que contenham informações restritas ou sensíveis devem ser apagados.
XI. Todo e qualquer tipo de documentos (folhas, cadernos, apontamentos, etc…) que contenham informações restritas ou sensíveis e que se encontrem em cima da secretária, mesa, cadeira, estante, etc… devem ser guardados, em sítios próprios, em caso de ausência do proprietário.
XII. Todos os dispositivos portáteis de computação (portáteis, tablets) devem ser bloqueados.
XIII. Todos os dispositivos de armazenamento em massa (CD, DVD, Pen USB, etc…) que contenham informações restritas ou sensíveis devem ser guardados em gavetas ou armários, bem protegidos.

CONFORMIDADE

- ✓ **Medição de Conformidade**

A equipa do departamento de informática verificará a conformidade com esta política por meio de vários métodos, incluindo entre outros, acompanhamento periódico e auditorias internas e externas.

- ✓ **Exceções**

Qualquer exceção à política deve ser aprovada pela equipa do departamento de informática, antecipadamente.

- ✓ **Não Conformidade**

Um docente, não docente, funcionário ou colaborador que tenha violado esta política pode estar sujeito a ações disciplinares, incluindo até rescisão de contrato de trabalho.

OUTRAS NORMAS, POLÍTICAS, PROCESSOS RELACIONADOS

Política de Organização de Segurança da Informação; Política de Controlo de Acesso; Política de Segurança Física e Ambiental; Política de Criptografia.

REVISÃO

A política de segurança deverá ser revista anualmente ou em caso de ocorrência de alguma alteração de forma a garantir a conformidade, pertinência e efetividade contínuas.

Posteriormente à fase de revisão, a política deve ser submetida ao Reitor da UMa, para que as alterações sejam aprovadas e posteriormente comunicadas a quem de respeito (comunidade da UMa ou a intervenientes a quem de respeito).

HISTÓRICO DE REVISÕES

Data	Versão	Autor	Comentários
15/01/2019	1.0	João Azevedo	Elaboração do documento

4. Política de Dispositivos Móveis

RESUMO

Os dispositivos móveis (smartphones, tablets, portáteis e vários outros dispositivos de computação pessoal) estão a se tornar um padrão de implementação no atual ambiente de computação das organizações. O seu tamanho, a sua portabilidade e a sua funcionalidade estão a tornar estes dispositivos cada vez mais desejáveis na substituição de dispositivos de desktop tradicionais. No entanto, a portabilidade oferecida por estes dispositivos também pode aumentar a exposição de segurança para as organizações onde sejam utilizados os dispositivos.

OBJETIVO

O objetivo desta política é estabelecer regras e protocolos para o uso de dispositivos móveis e a sua ligação com a rede.

ÂMBITO

Todos os dispositivos móveis, sejam da propriedade da UMa ou dos "trabalhadores", que tenham acesso aos sistemas e aplicações e a informações sensíveis da Instituição, são regidos por esta política**.**

TERMOS E DEFINIÇÕES

Para os propósitos deste documento, os termos e definições fornecidos na política de segurança da informação aplicam-se.

POLÍTICA

As seguintes diretrizes gerais aplicam-se ao uso de dispositivos móveis:

I. Todos os dispositivos móveis devem ser protegidos por uma password exigida no momento em que o dispositivo é ligado.
II. As passwords devem atender aos requisitos descritos nas políticas de controlo de acesso e de criptografia da UMa.
III. Todos os dados armazenados nos dispositivos móveis devem ser criptografados.
IV. Devem ser utilizados protocolos de segurança e de acesso criptografados em todas as ligações de rede sem fio.
V. Os "trabalhadores" devem abster-se de utilizar ligações de rede públicas ou não seguras ao utilizar os dispositivos móveis do trabalho.
VI. Todos os dispositivos móveis pessoais que exigem conectividade de rede devem estar em conformidade com todos os padrões de uso e configuração da UMa.
VII. Os dispositivos móveis pessoais, utilizados para desenvolver trabalhos com grau de sensibilidade e criticidade para a UMa devem ser identificados, registados e aprovados pelo departamento de informática.
VIII. Os dispositivos móveis sem supervisão devem ser fisicamente protegidos.
IX. Os dispositivos móveis que acedam à rede da UMa devem ter proteção anti-malware e antivírus atualizados.

X. Os dispositivos móveis, perdidos ou roubados, devem ter serviços de localização habilitados e as unidades criptografadas ou limpas de todas as informações, de modo a que elas não possam ser utilizadas até serem recuperadas ou destruídas.

RESPONSABILIDADES

Responsabilidades dos Utilizadores de Dispositivos Móveis

Os procedimentos e requisitos a seguir devem ser seguidos por todos os utilizadores de dispositivos móveis:

I. Devem ser revelados imediatamente quaisquer dispositivos móveis perdidos ou roubados.
II. O acesso não autorizado a um dispositivo móvel ou informações da UMa deve ser imediatamente reportado.
III. Os dispositivos móveis não devem ter software/firmware não autorizado, instalado.
IV. Os utilizadores não devem carregar conteúdo ilegal ou software pirata em qualquer dispositivo móvel.
V. Somente aplicações aprovadas pelo departamento de informática são permitidas nos dispositivos móveis que se liguem à rede da UMa.
VI. Todos os dispositivos móveis e as aplicações neles instaladas, devem-se manter atualizadas.
VII. O sistema operacional e os Patches de aplicações devem ser instalados dentro de 30 dias após o seu lançamento.
VIII. Os dispositivos móveis devem ter um software de proteção anti-malware/vírus ativo e atualizado e um software capaz de encriptar todos os ficheiros e pastas no dispositivo.
IX. Todas as partições de armazenamento físico devem ser criptografadas.
X. Os utilizadores devem utilizar o sistema de email corporativo da UMa ao enviar e receber dados da Instituição.
XI. Os utilizadores são responsáveis por garantir que todos os ficheiros importantes armazenados nos dispositivos móveis sejam armazenados em backup regularmente.

Responsabilidades Administrativas

O departamento de informática ou equipa representante deve assegurar:

I. Definições de configuração específicas devem ser definidas para firewall pessoal e software de proteção contra malware para garantir que este software não seja alterável por utilizadores de dispositivos móveis e/ou de propriedade da UMa.
II. Que a formação anual de segurança é fornecida aos utilizadores de dispositivos móveis. O conteúdo e a forma dessa formação devem ser decididos pelo departamento de informática ou sua equipa.

III. O software “XPTO” é utilizado para gerir riscos, limitar problemas de segurança e reduzir custos e riscos de negócio relacionados a dispositivos móveis. O software incluirá a capacidade de inventariar, monitorizar (por exemplo, instalações de aplicações), emitir alertas (por exemplo, passwords desativadas, categorizar software de sistema (sistemas operacionais) e emitir vários relatórios (por exemplo, aplicações instaladas).

IV. Revisões e atualizações regulares e estratégias de segurança utilizadas em dispositivos móveis.

O departamento de informática deve implementar procedimentos e medidas para limitar estritamente o acesso a dados confidenciais que se deslocam de e para dispositivos móveis, uma vez que esses dispositivos geralmente representam um risco mais alto de incidentes do que os dispositivos não móveis.

CONFORMIDADE

- ✓ **Medição de Conformidade**

A equipa do departamento de informática verificará a conformidade com esta política por meio de vários métodos, incluindo entre outros, acompanhamento periódico e auditorias internas e externas.

- ✓ **Exceções**

Qualquer exceção à política deve ser aprovada pela equipa do departamento de informática, antecipadamente.

- ✓ **Não Conformidade**

Um docente, não docente, funcionário ou colaborador que tenha violado esta política pode estar sujeito a ações disciplinares, incluindo até rescisão de contrato de trabalho.

OUTRAS NORMAS, POLÍTICAS, PROCESSOS RELACIONADOS

Política de Controlo de Acesso; Política de Criptografia.

REVISÃO

A política de segurança deverá ser revista anualmente ou em caso de ocorrência de alguma alteração de forma a garantir a conformidade, pertinência e efetividade contínuas.

Posteriormente à fase de revisão, a política deve ser submetida ao Reitor da UMa, para que as alterações sejam aprovadas e posteriormente comunicadas a quem de respeito (comunidade da UMa ou a intervenientes a quem de respeito).

HISTÓRICO DE REVISÕES

Data	Versão	Autor	Comentários
15/01/2019	1.0	João Azevedo	Elaboração do documento

5. Política – Controlo de Acesso

RESUMO

Esta política é definida para corresponder à falta de controlo de registo e cancelamento de utilizadores (alunos) da UMa bem como do seu acesso.

OBJETIVO

Assegurar o registo e cancelamento dos utilizadores da UMa e assegurar o acesso de utilizadores autorizados e prevenir o acesso não autorizado a sistemas e serviços.

ÂMBITO

Esta política aplica-se a todos os utilizadores, alunos, da UMa.

TERMOS E DEFINIÇÕES

Para os propósitos deste documento, os termos e definições fornecidos na política de segurança da informação aplicam-se.

POLÍTICA

Registo Utilizadores (alunos)

A relação do utilizador com a UMa funda-se no ato de matrícula, enquanto marco constitutivo de direitos e deveres recíprocos.

O registo de utilizador é efetuado em (x) passos:

I. Mediante o perfil de utilizador, os dados devem ser inseridos no sistema de gestão académica onde os responsáveis pela introdução desses dados são os serviços académicos, quando é efetuado o registo.
II. As credenciais devem ser geradas e atribuídas a cada utilizador registado onde devem ser atribuídos o número de aluno e a password.
III. Devem ser permitidos todos os acessos a que o utilizador tem direito, perante a situação do mesmo.
IV. Devem ser facultados, entre outros, contas office 365 aos utilizadores.

Cancelamento Utilizadores (alunos)

I. Em caso de suspensão ou desvinculação de um utilizador:
    a. Devem ser suspensas ou removidas as permissões de acesso a aplicações e sistemas da UMa (infoalunos, plataforma moodle, acesso físico à UMa através do cartão);
    b. Deve ser suspensa ou removida a conta de email office 365 e restantes afins;
    c. Deve ser suspenso ou anulado o registo do utilizador.
II. Devem ser, periodicamente, identificados e removidos ou desabilitados as credenciais de utilizadores redundantes.

III. Deve ser assegurado que as credenciais de utilizadores redundantes não sejam emitidas para outros utilizadores.

RESPONSABILIDADES

Os **Serviços Académicos** são responsáveis:

a) Pela gestão dos utilizadores;
b) Registo e cancelamento dos utilizadores.

O **departamento de informática** é responsável por:

a) Gerar e atribuir as credenciais dos utilizadores;
b) Permitir e restringir os direitos de acesso aos utilizadores dos sistemas e aplicações existentes e necessárias.

CONFORMIDADE

- ✓ **Medição de Conformidade**

Os serviços académicos juntamente com o departamento de informática verificarão a conformidade com esta política por meio de vários métodos, incluindo entre outros, acompanhamento periódico e auditorias internas e externas.

- ✓ **Exceções**

Qualquer exceção à política deve ser aprovada pelos serviços académicos e departamento de informática, antecipadamente.

- ✓ **Não Conformidade**

Em caso de violação desta política está sujeito a ações disciplinares, incluindo até rescisão de contrato de trabalho.

OUTRAS NORMAS, POLÍTICAS, PROCESSOS RELACIONADOS

Nenhuma.

REVISÃO

A política de segurança deverá ser revista anualmente ou em caso de ocorrência de alguma alteração de forma a garantir a conformidade, pertinência e efetividade contínuas.

Posteriormente à fase de revisão, a política deve ser submetida ao Reitor da UMa, para que as alterações sejam aprovadas e posteriormente comunicadas a quem de respeito (comunidade da UMa ou a intervenientes a quem de respeito).

HISTÓRICO DE REVISÕES

Data	Versão	Autor	Comentários
15/01/2019	1.0	João Azevedo	Elaboração do documento

6. Política – Segurança Física e Ambiental

RESUMO

A segurança física e ambiental identifica requisitos para proteger a comunidade e a propriedade da instituição contra acesso não autorizado, perda ou danos causados por ameaças físicas e ambientais. O propósito de identificar requisitos, para a instalação, operação, proteção e manutenção de equipamentos de informática, é preservar a segurança dos sistemas de informações e as informações da instituição.

OBJETIVO

Prevenir o acesso físico não autorizado, danos e interferências nas instalações de processamento de informações e das informações da instituição. Prevenir perdas, danos, roubo ou comprometimento de ativos e interrupção das operações da instituição.

ÂMBITO

Esta política aplica-se a todas as instalações, quer sejam salas, escritórios e ou laboratórios que contenham informações sensíveis e ativos de informação da instituição.

TERMOS E DEFINIÇÕES

Para os propósitos deste documento, os termos e definições fornecidos na política de segurança da informação aplicam-se.

POLÍTICA

Diretrizes Gerais

I. Todos os recursos de tecnologia e informação da instituição devem ter controlos de segurança física e ambiental apropriados, aplicados de acordo com os riscos identificados.
II. A responsabilidade pela segurança física e ambiental dos recursos de informação e tecnologia, da instituição, deve ser partilhada pelos técnicos que utilizam os sistemas, administradores do sistema, responsáveis pela gestão dos sistemas, e pelos elementos das empresas subcontratadas para o efeito.

Perímetro de Segurança Física

Assim como é essencial identificar as informações sensíveis, há também a necessidade de identificar e conceder níveis adequados de proteção a diferentes áreas dentro dos edifícios da instituição onde os requisitos de segurança física para essas áreas dependerão do valor, da sensibilidade e dos ativos de informação a serem protegidos, das ameaças e riscos de segurança prováveis ou associados e das salvaguardas e medidas de proteção existentes.

I. De uma forma geral os sistemas de informação devem ser alojados numa área segura protegida por um perímetro de segurança definido com controlos de entrada. Os servidores devem estar localizados em data centers de serviços de informação.

II. Várias barreiras físicas devem ser criadas através de um plano ou projeto apropriado para garantir a proteção física dos ativos da instituição, essencialmente as instalações (salas com equipamento ou informações sensíveis). Os seguintes objetivos de controlo devem ser cobertos no projeto de instalações seguras:
    a. deve ser definido claramente um perímetro de segurança;
    b. deve ser um perímetro forte o suficiente para resistir à maioria das falhas, com paredes externas sólidas;
    c. as portas externas devem ser protegidas contra acesso não autorizado;
    d. o acesso físico às instalações deve ser controlado por:
        1. uma área de receção;
        2. mecanismos digitais de contro de acesso - cartão de identificação (onde constam a que instalações pode aceder, a identificação do proprietário);
        3. Sistema CCTV.
    e. devem ser utilizados sinais que indiquem que o acesso a instalações mais sensíveis é restrito apenas ao pessoal autorizado;
    f. não devem existir paredes ou tetos falsos a rodear a instalação;
    g. em caso de existirem janelas, as mesmas não devem estar viradas para corredores ou locais de acesso pelo público;
    h. devem ser utilizadas portas corta fogo, no perímetro, onde devem estar "alarmadas" e devem ser monitorizadas periodicamente. O pessoal deve estar ciente de que elas devem ser mantidas fechadas.

Controlos de Entrada Física

I. Todas as áreas seguras devem ser protegidas por controlos de entrada apropriados para garantir que apenas as pessoas autorizadas tenham acesso. Os controlos que se seguem devem ser implementados:
    a. O acesso a áreas onde as informações sensíveis são processadas ou armazenadas deve ser restrito apenas ao pessoal autorizado;
    b. Deve ser utilizado sistema de CCTV para controlar os acessos às salas onde contenham material e/ou informações sensíveis;
    c. Os controlos de autenticação, neste caso o uso do sistema de cartão de controlo de acesso, deve ser utilizado para autorizar e validar o acesso;
    d. A data, a hora, e o nome da pessoa devem ser registadas;
    e. Um registo de auditoria de todo o acesso deve ser mantido durante, no mínimo, seis meses;
    f. Deve ser desenvolvida, aprovada e mantida uma lista de pessoas com acesso autorizado a cada instalação;

g. Deve ser vista e revista a lista das pessoas que têm acesso a cada instalação, periodicamente, no intervalo não inferior a 3 meses;
h. Os direitos de acesso a áreas protegidas devem ser revistos regularmente, no mínimo a cada três meses, e atualizados e revogados sempre que for necessário.

II. Exceto as áreas oficialmente designadas como as de acesso público, a instituição deve manter registos de acesso de visitantes às instalações onde os sistemas de informações residem por, pelo menos dois anos e rever os registos dos visitantes periodicamente, mas não menos do que um mês.
III. O acesso às áreas onde as informações sensíveis (por exemplo, salas de servidores, salas de equipamento sensível) sejam processadas ou armazenadas deve ser controlado e restrito apenas a pessoas autorizadas. Todos os visitantes devem ser acompanhados e supervisionados, a menos que o acesso tenha sido previamente aprovado.
IV. O pessoal das empresas subcontratadas deve ter acesso restrito a áreas seguras ou instalações de processamento de informação somente quando for necessário. Esse acesso deve ser autorizado e monitorizado. Deve ser feito um registo exigindo:
    a. Identificação de quem tem acesso;
    b. Motivo de entrada;
    c. Data e hora de entrada e saída;
    d. Identificação de quem deu o acesso;
V. O pessoal das empresas subcontratadas só terá acesso para fins específicos e autorizados e receberão instruções sobre os requisitos de segurança da área e sobre procedimentos de emergência.
VI. Os controlos de acesso devem ser utilizados para autorizar e validar todo o acesso e deve ser também mantido, com segurança, um registo de auditoria de todo o acesso.
VII. A instituição deve utilizar mecanismos automatizados para facilitar a manutenção e revisão dos registos de acesso.
VIII. Para os casos onde as salas que contenham equipamentos ou informações sensíveis, sejam ainda controladas apenas através de chave/chave mestra, o acesso por meio desse método deve ser registado e deve ser mantido como registo: o nome da pessoa que tem acesso, o motivo, a data, e o período em que a mesma acedeu à ou às salas.

Proteção de Instalações (escritórios, salas e laboratórios)

I. Devem ser levados em conta os regulamentos e normas relevantes de segurança e de saúde ao proteger as instalações.
II. As instalações críticas devem se encontrar em locais estratégicos de forma a evitar facilmente o acesso do público.
III. Os diretórios, listas telefónicas e restantes registos, que identifiquem os locais das instalações de processamento de informação, não devem ser facilmente acessíveis pelo público.

IV. Sistema de CCTV ou outros mecanismos de controlo de acesso devem ser implementados e protegidos para monitorizar o acesso físico individual a instalações sensíveis:
    a. Estes mecanismos devem ser protegidos contra adulteração ou desativação;
    b. Os resultados dos mecanismos devem ser revistos regularmente e correlacionados com outras entradas e informações de contro de acesso;
    c. Os registos dos vários mecanismos devem ser armazenados por pelo menos um ano.
V. Os registos de acesso físico devem ser revistos pelo menos de três em três meses.
VI. Devem ser utilizados mecanismos automatizados de forma a reconhecer possíveis intrusões e iniciar ações de resposta designadas.

Localização e Proteção de Equipamentos

I. Deve ser garantido que as instalações da instituição estejam projetadas de forma a proteger as informações e os ativos da UMa. Deve ser planeada a localização ou o local de determinada ou determinadas instalações onde o ou os sistemas de informação residam tendo em consideração os riscos físicos e ambientais que o espaço acarreta ou pode acarretar.
II. Devem ser implementados controlos para minimizar o risco de potenciais ameaças físicas, incluindo roubos, incêndios, inundações, poeiras, vibrações, interferências elétricas, vandalismos, etc. aos equipamentos.
III. Os equipamentos centralizados, por exemplo, servidores, routers, switches e restantes equipamentos, devem ser localizados numa instalação com acesso restrito apenas àqueles que requerem e podem ter acesso.
IV. Todos os equipamentos que contenham informação sensível, como por exemplo, estações de trabalho, portáteis, mídia digital, dispositivos removíveis e dispositivos de armazenamento devem ser localizados e utilizados numa área que não seja acessível ao público.
V. Todos os equipamentos devem ser localizados e monitorizados através dos vários mecanismos de controlo de acesso, como por exemplo, sistema CCTV, com um determinado ângulo, para que todos os momentos sejam monitorizados.
VI. As condições ambientais, tais como a temperatura e a humidade, devem ser monitorizadas de forma a não afetarem adversamente o bom e correto funcionamento e operação dos ativos.
VII. Equipamentos que requeiram proteção especial devem ser isolados para reduzir o nível geral de proteção exigida.

Política de Mesa Limpa e Ecrã Limpo

I. Além de ser necessário bloquear o ecrã dos computadores (estações de trabalho, portáteis, etc.) todas as restantes áreas de trabalho devem ser mais protegidas. (ver documento – Política de Mesa Limpa e Ecrã Limpo).

CONFORMIDADE

- ✓ **Medição de Conformidade**

As equipas responsáveis (unidade de infraestruturas e instalações) verificarão a conformidade com esta política por meio de vários métodos, incluindo entre outros, acompanhamento periódico e auditorias internas e externas.

- ✓ **Exceções**

Qualquer exceção à política deve ser aprovada pelas equipas responsáveis de infraestruturas e instalações juntamente com o conselho de administração.

- ✓ **Não Conformidade**

Em caso de violação desta política está sujeito a ações disciplinares, incluindo até rescisão de contrato de trabalho.

OUTRAS NORMAS, POLÍTICAS, PROCESSOS RELACIONADOS

Política de Mesa Limpa e Ecrã Limpo.

REVISÃO

A política de segurança deverá ser revista anualmente ou em caso de ocorrência de alguma alteração de forma a garantir a conformidade, pertinência e efetividade contínuas.

Posteriormente à fase de revisão, a política deve ser submetida ao Reitor da UMa, para que as alterações sejam aprovadas e posteriormente comunicadas a quem de respeito (comunidade da UMa ou a intervenientes a quem de respeito).

HISTÓRICO DE REVISÕES

Data	Versão	Autor	Comentários
15/01/2019	1.0	João Azevedo	Elaboração do documento