POLITÉCNICO DE LEIRIA | ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Relatório Prático

Mestrado em Cibersegurança e Informática Forense

Análise de Risco e Políticas para uma Clínica Médica Hipotética

Filipe Henriques, 2180066

Jéssica Pedrosa, 2180067

Patrícia Silva, 2180068

Tiago Martins, 2182716

Leiria, janeiro de 2019

Resumo

Para a realização deste trabalho, foi criado um cenário hipotético de uma clínica localizada em Portugal, encontrando-se inserida num grupo clínico privado. Esta clínica presta serviços médicos gerais e especializados tais como enfermagem, oftalmologia ou ainda fisioterapia. Apresenta ainda um departamento de investigação direcionada à área de cardiologia e um departamento de autópsias.

A clínica possui uma estrutura empresarial de modo a se dividir e organizar as atividades realizadas na mesma. Para além disso, tem também uma estrutura referente à sua administração empresarial que expõe os cargos existentes na clínica e a sua posição na hierarquia dos mesmos. Existem um conjunto de entidades, de diversos setores de atividade, com as quais a clínica estabelece parcerias que têm como objetivo as entidades envolvidas atingirem interesses comuns.

Como qualquer entidade nos dias de hoje, a clínica terá de recolher e organizar, um conjunto de dados em formato físico ou digital, tais como dados dos pacientes ou dados da clínica em si. De modo a otimizar o seu funcionamento interno e o serviço prestado aos seus clientes, a clínica faz uso de diferentes *software*/aplicações.

Antes de se dar início à análise de riscos propriamente dita do cenário criado, foi efetuada a identificação dos ativos, das ameaças e ainda das vulnerabilidades. A análise de riscos teve em consideração as identificações mencionadas anteriormente e permitiu também identificar alguns riscos da clínica, de diferentes níveis de gravidade. Alguns destes serão mitigados através de controlos enquanto que outros terão de ser aceites pela entidade.

Para a realização deste trabalho foram levados em consideração um conjunto de elementos legislativos e normativos nomeadamente a ISO/IEC 27001, a ISO/IEC 27002, a ISO/IEC 27005, a Lei da Segurança do Ciberespaço 46-2018 e, por sua vez, a Diretiva UE 2016/1148 Nível comum de segurança das redes e ainda o Regulamento Geral da Proteção dos Dados.

Palavras-chave: Clínica, riscos, controlos, ativos, vulnerabilidades.

Esta página foi intencionalmente deixada em branco

Lista de Figuras

Lista de Acrónimos

AC – Autoridade de Controlo

CNPD – Comissão Nacional de Proteção de Dados

CNCS – Centro Nacional de Cibersegurança

CSSC – Conselho Superior de Segurança do Ciberespaço

ENSC – Estratégia Nacional de Segurança do Ciberespaço

EPD – Encarregado de Proteção de Dados

ISO/IEC – *Organization for Standardization and the International Electrotechnical Commission*

PDCA – *Plan, Do, Check, Act*

RGPD – Regulamento Geral de Proteção de Dados

SGSI – Sistema de Gestão da Segurança de Informação

UE – União Europeia

Índice

1. Introdução

No âmbito da unidade curricular de Políticas e Análise de Risco na Segurança de Informação, do curso de Mestrado Cibersegurança e Informática Forense da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria, foi elaborado o presente relatório de modo a elaborar uma análise de risco e estabelecimento de políticas e controlos de segurança numa clínica médica hipotética.

Segurança da informação tem sido um tópico nas organizações no qual é prestado menos importância do que devia existir, por isso, é importante que seja mostrado justificações e provas de que o aumento da segurança na informação é uma necessária ação para reduzir prejuízos causados por ameaças. As análises de risco numa organização ajudam precisamente nesta temática, pelo que é possível identificar e classificar riscos, vulnerabilidades e ameaças tendo em conta as estratégias de negócio e financeira da organização. Esta análise ajuda a identificar os possíveis prejuízos numa organização caso não sejam tomadas medidas para combater os riscos analisados. Com isto, poderá ser possível justificar a implementação de controlos e políticas de segurança para combater os riscos que devem ser resolvidos.

Considerando os factos acima referidos, para este projeto foi produzido um cenário hipotético de uma clínica médica. Assim foi descrita a arquitetura do seu sistema de informação, de modo a efetuar uma análise de risco e também para estudar as implicações do novo Regulamento Geral da Proteção de Dados da União Europeia (UE) e da Lei nº 46/2018 nesta organização. Depois serão desenvolvidos e implementados os controlos de segurança necessários para combater os riscos mais pertinentes da organização.

O presente relatório está dividido em seis capítulos, sendo que o capítulo 2 consiste no enquadramento do tema do projeto proposto, que é a abordagem dos vários temas pertinentes à segurança e privacidade da informação na organização.

O capítulo 3 é composto pela caracterização de um ambiente empresarial da hipotética clínica médica, sendo especificadas as estruturas empresariais e administrativas da empresa, a caraterização física e os principais ramos de atividade da clínica e também o seu enquadramento com o mundo digital.

No capítulo 4 é exposta a arquitetura do sistema de informação utilizada, como também as tecnologias e os dados que são recolhidos, organizados, protegidos e distribuídos na clínica hipotética.

No capítulo 5 é realizada uma análise de risco no qual são identificados os riscos, vulnerabilidades e ameaças sobre a clínica, como também uma classificação destes riscos relativos à importância estratégica e financeira. É também abordado a implicação que o novo Regulamento Geral da Proteção de Dados, bem como, as possíveis consequências que a Diretiva 2016/1148 e, por sua vez, a Lei nº46/2018 terão sobre a empresa. Também são identificados os controlos e as políticas de segurança do sistema do SGSI, sendo estes baseados na classificação dos riscos elaborada no capítulo anterior.

E por fim, no capítulo 6, o relatório termina com a conclusão, em que é feito um balanço geral da análise dos riscos e da implementação dos respetivos controlos de segurança escolhidos.

2. Enquadramento

Uma vez que a temática do presente trabalho se prende com o planeamento e análise crítica da segurança e privacidade dos dados de uma organização, neste capítulo, pareceu relevante tratar os tópicos de gestão de risco e políticas de segurança, os requisitos e recomendações para o desenvolvimento e operação de um SGSI, o enquadramento da legislação, o regulamento geral da proteção de dados, a Diretiva UE 2016/1148 Nível comum de segurança das redes e ainda a Lei da Segurança do Ciberespaço 46-2018.

2.1 Gestão de risco e políticas de segurança

No que toca à segurança de informação, existem três princípios fundamentais, a confidencialidade, a integridade e a disponibilidade.

A confidencialidade diz respeito ao facto de que toda a informação deve ser protegida de acordo com o seu grau de sigilo, limitando o seu acesso apenas quando necessário.

A integridade passa por garantir que a informação se mantenha na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-la contra alterações indevidas, intencionais ou acidentais.

A disponibilidade visa que toda a informação partilhada por um indivíduo ou instituição, esteja sempre disponível aos seus utilizadores.

Estando este cenário enquadrado na área da saúde, muitos dos dados abordados necessitam de ter um elevado grau de confidencialidade, assim como um igual cuidado quanto à integridade e disponibilidade. O risco da fuga de informação pode ser elevado se as devidas precauções não forem tomadas.

Uma vulnerabilidade é uma fragilidade na segurança que pode ser utilizada pelas ameaças de modo a causar danos aos ativos de uma organização. O facto de existir uma vulnerabilidade não significa que esta venha a ser explorada, no entanto devem-se tomar as devidas precauções.

Uma ameaça é composta por uma vulnerabilidade, um ator e uma motivação, podendo o ator ser um funcionário, um externo à organização ou uma organização concorrente, e a motivação ser financeira, política ou nenhuma no caso de um erro ou acidente. Segundo a norma ISO/IEC 27005, todas as ameaças devem ser identificadas genericamente e por tipo.

O Impacto é o resultante da ação bem sucedida de uma ameaça, e tem uma ordem de magnitude consoante os ativos afetados. Segundo a norma ISO/IEC 27005, os impactos devem de ser especificados em torno do nível de danos ou custos causados à organização.

Esta norma define que o risco é o efeito da incerteza nos objetivos e está associado ao potencial das ameaças explorarem as vulnerabilidades de um ativo ou grupo de ativos. Deve-se tratar os riscos sempre de forma preventiva, de forma a minimizar o impacto caso os mesmos se venham a concretizar.

A norma ISO/IEC 27005 estipula o processo de gestão de riscos. Este é um processo iterativo e contém várias etapas.

A primeira etapa é a definição do contexto, onde é estabelecida toda a informação relevante à análise e gestão de risco. Seguidamente são identificados os riscos, o que envolve a identificação de fontes, eventos causas e potenciais consequências. Depois estes são analisados, onde é compreendida a natureza dos mesmos e determinando o nível de risco. Seguidamente os riscos são avaliados, fazendo a distinção de prioridade de tratamento para cada um e são consequentemente tratados. O processo de tratamento contém 4 partes, a avaliação do tratamento já realizado, no caso de risco residual, a verificação se este é tolerável, no caso de não o ser, a definição e implementação de um novo tratamento, e a avaliação e eficácia desse tratamento. Posteriormente no caso da existência de risco residual após análise e tratamento dos mesmos, terá de existir uma aceitação do risco. [1]

2.2 Requisitos e recomendações para o desenvolvimento e operação de um SGSI

A informação tem vindo a ganhar maior importância nos ativos de organizações e estes dados são atualmente, em muitas organizações, a forma como são realizados muitos dos seus negócios. Os sistemas de gestão de segurança da informação vêm assim resolver a necessidade de garantir a proteção da informação da organização, como também a proteção do próprio negócio e assegurar a sua continuidade.

Sendo estes sistemas essenciais para a continuidade do negócio, foram criados requisitos para ajudar a desenvolver e a operar um SGSI, de forma a possibilitar uma melhor base onde organizações poderão seguir e construir o seu sistema de gestão da segurança da informação. As normas ISO/IEC 27001 e 27002 vêm ajudar o processo de criação e manutenção do sistema. Estas normas fazem parte da família de normas de segurança de informação ISO/IEC 27000, pelo que estas duas em especial, fornecem um conjunto de regras e de boas práticas da segurança na informação com o fornecer de requisitos para estabelecer, implementar, manter e melhorar de forma contínua um SGSI. [2]

Para este fim, a norma ISO/IEC 27001 introduz o modelo PDCA, que é a base na qual as recomendações e requisitos para o desenvolvimento e operação do SGSI estão estruturadas. [3] Apesar do modelo PDCA não ser referido na introdução da versão 2013 da norma, a utilização do modelo é visível nas suas principais cláusulas.

O passo *Plan* refere-se às cláusulas: "O Contexto da organização" que ajuda a compreender o contexto da organização de modo a determinar as questões internas e externas mais significativas para os objetivos do SGSI; "A Liderança", esta cláusula sugere a os objetivos e a forma de como a gestão de topo deve lidar com os aspetos funcionamento da organização e dos seus empregados ligados ao SGSI; "O Planeamento", aqui é exposta a necessidade de elaborar planos e os aspetos que devem ser planeados relativos aos riscos e oportunidades de segurança que devem ser avaliados; E "O Suporte", cujo o objetivo insere-se na necessidade de documentar todas as ações e processos desenvolvidos para o SGSI e os seus processos de comunicação. O passo *Do* refere à cláusula "Operação", que explica o que deve ser efetuado para a implementação

e funcionamento do SGSI, o que, por sua vez, envolve planear, implementar e controlar processos para responder aos requisitos e objetivos de segurança da informação, e também implementar ações para responder a esses requisitos e objetivos. O passo *Check* refere-se à cláusula "Avaliação do desempenho", sendo exposta a forma e os pontos essenciais de como deve ser avaliado o desempenho do SGSI. É importante determinar quais processos e controlos de segurança que terá de monitorizar, e a forma como será medido, analisado e avaliado os resultados no desempenho. E o passo *Act* refere-se à cláusula "Melhoria", este refere-se na forma de atuar considerando os resultados do desempenho do SGSI. [2] [3]

2.3 Regulamento Geral da Proteção de Dados O novo Paradigma dos Dados Pessoais

O uso da internet já nada tem a haver com o que era há uns anos e a legislação encontrava-se desatualizada perante esta nova realidade. Assim, para colmatar as necessidades sentidas, foi criado o RGPD. Afinal, a Internet é usada para quase tudo fazendo, cada vez mais, parte do quotidiano das pessoas e até mesmo das empresas. As empresas tiveram de evoluir para permanecer ativas numa época em que para conseguirem entrar no mercado, ter vantagens e fazer concorrência é preciso fazer parte do mundo digital. Para além disso, não se pode ignorar o facto de que as empresas tinham cada vez mais dados pessoais, mas por outro lado, não apresentavam muita preocupação nos dados que recolhiam. Vivemos numa época em que mais dados é sinónimo de melhor, mesmo que esses dados não sejam necessários agora, não se sabe o dia de amanhã. O regulamento veio mudar este aspeto.

No fim de maio de 2016 o novo regulamento geral da proteção de dados, da UE, entrou em vigor em todos os Estados-Membros, criando um novo paradigma dos dados pessoais, no entanto só se tornou aplicável no fim de maio de 2018. Este regulamento veio substituir a diretiva europeia, Diretiva 95/46 / CE, estabelecida em 1995 e revogar o Decreto Legislativo nº196/2003.

O RGPD aplica-se a todas as empresas da UE e todas aquelas que, não estando na UE, tratam de dados de residentes da UE ou pessoas que estejam a viajar na UE. Esse

tratamento de dados serviu para oferecer serviços ou monitorizar o comportamento dessas pessoas. Em relação à aplicação material, o regulamento aplica-se a todas as formas de tratamento, incluindo as automatizadas.

Com o novo RGPD houve uma implementação e reforço de vários princípios como o da lealdade, o da transparência, o do consentimento e o da responsabilidade. São 11 princípios e todos eles devem estar implementados no mundo dos negócios e, consequentemente, nas empresas/organizações.

Para além dos princípios, o RGPD também apresentou, de forma geral, 7 direitos aos titulares dos dados, como o direito ao acesso, à retificação, à limitação de tratamento e à oposição. Os titulares têm agora mais direitos, estando esses regulamentados e os titulares devem e têm de os conhecer, podendo usufruir deles em qualquer altura. Também possuem sempre o direito a que os seus dados pessoais se encontrem em segurança e devidamente protegidos, podendo prestar queixa a uma autoridade de controlo (AC) caso vejam os seus direitos a serem violados. A autoridade de controlo em Portugal é a Comissão Nacional de Proteção de Dados (CNPD).

O regulamento também define bem o conceito de responsável pelo tratamento, de encarregado de proteção dos dados (EPD) e o de subcontratante. O certo, é que as empresas têm agora mais responsabilidades e com o RGPD têm de ser capazes de autorregularem-se e de autorresponsabilizarem-se. Tal deve-se ao facto de caber a cada empresa garantir que o RGPD se encontra aplicado, ou seja, que a sua empresa se encontre em conformidade com o regulamento. A empresa tem de conseguir provar, perante uma AC, que o regulamento está devidamente implementado. O responsável pelo tratamento tem essa responsabilidade e também, a de garantir que a empresa está em conformidade com o RGPD, garantindo que os dados que o mesmo utilize, de titulares, para efeitos de tratamento, têm o consentimento desse titular (quando aplicável); que o titular tem conhecimento dos direitos que possuí; de responder perante uma solicitação desses direitos ao titular; de garantir a proteção dos dados e muitas outras tarefas. Caso ocorra uma violação dos dados pessoais, o responsável pelo tratamento deve notificar a AC, sem demoras injustificadas e, caso necessário, os titulares dos dados.

Em alguns casos, pode ser necessário que a empresa/organização contrate um encarregado da proteção dos dados. Esses casos vão desde empresas que tratem de dados sensíveis em grande escala a empresas que façam controlo regular e sistemático dos

titulares dos dados em grande escala. Também a maioria dos organismos públicos devem ter um EPD. O EPD deve garantir a conformidade no seio da organização e deve informar os problemas que encontrar, bem como sugerir resoluções e envolver-se na sua implementação. Deve estar envolvido em todas as questões relacionadas com os dados pessoais. Este encarregado não pode ser penalizado nem destituído pelo facto de exercer as suas funções, que vão desde aconselhar o pessoal que trate dos dados, até à função de cooperar com a AC e ser o ponto de contacto com a mesma.

O RGPD também prevê os casos em que uma transferência de dados para países terceiros é ou não permitida, entre muitas outras situações. O que se pode dizer, é que com o novo regulamento há uma nova mudança de paradigma, as empresas têm uma maior gama de responsabilidades e caso não cumpram o regulamento, terão de pagar as consequências. A coima, em casos menos graves, pode ir até 10 milhões ou 2% do volume de negócio a nível mundial, em casos graves, pode ir até 20 milhões ou 4% do volume de negócio anual a nível mundial, tudo isto dependendo do valor mais alto.

Este novo regulamento é sem dúvida uma mudança no paradigma dos dados. É visível uma implementação e reforço nos princípios e nos direitos. Ele foi pensado para a segurança dos titulares, ou mais concretamente, dos seus dados pessoais, e com isto veio dar mais direitos aos titulares, pois os dados são propriedade dos mesmos. Ele obriga a que haja uma relação de maior transparência entre as empresas e os titulares, pois os últimos têm o direito de saber para o que é que os seus dados estão a ser recolhidos, quem os irá tratar e de que modo, quanto tempo serão guardados e quem posteriormente poderá ter acesso aos mesmos, entre outros tópicos. [4]

2.4 Diretiva UE 2016 1148 Nível comum de segurança das redes e a Lei da Segurança do Ciberespaço 46-2018

O volume de negócios e a comunicação entre os vários Estados-Membros da UE encontra-se em constante crescimento. Atualmente, praticamente qualquer organização ou empresa possui um sistema de informação, do qual se encontra bastante dependente. Contudo, não se pode ignorar o facto de o crescimento da internet e a evolução

exponencial da tecnologia, também aumentarem os riscos e as ameaças. A exploração destes mesmos riscos com o objetivo de provocar um ataque, quando é bem-sucedida, faz com que ocorra o que se designa de incidente. Seja em grande ou pequena escala, um incidente poderá ter sido motivado por diversas razões, realizado de diversas formas e pode ainda prejudicar vários ativos das entidades como também, em certos casos, colocar em risco a privacidade dos cidadãos. Com este cenário atual de alto risco presente também na UE, esta decidiu assumir uma posição e tentar, de alguma forma, proteger os seus cidadãos. Deste modo, a UE criou a Diretiva 2016/1148 cujo principal objetivo passa por conferir aos sistemas de informação e redes dos Estados-Membros segurança e proteção, para, por conseguinte, melhorar o funcionamento do mercado interno. Esta diretiva será aplicada em todo e qualquer Estado-Membro da UE, contudo unicamente a dois grupos de entidades – os operadores de serviços essenciais e os prestadores de serviços digitais. No que diz respeito aos prestadores de serviços digitais, existem três tipos – mercados em linha, motores de pesquisa em linha e os serviços de computação em nuvem. Já os operadores de serviços essenciais, de acordo com o serviço disponibilizado, são classificados em setores específicos, cada um dos mesmos com os seus devidos e diferenciados requisitos de segurança.

Enquanto que esta diretiva é aplicada a todo e qualquer prestador de serviços digitais, no que diz respeito aos operadores de serviços essenciais, estes são identificados através da realização de um processo de seleção.

Por consequência da criação desta diretiva, a UE teve de criar um grupo de cooperação que tem como principal função analisar a informação que é recolhida de cada Estado-Membro da UE.

Já no que toca a cada Estado-Membro, a adoção desta diretiva também representa um conjunto de consequências para os mesmos. Os Estados-Membros da UE, de modo a garantir a segurança no seu território, têm de adotar uma estratégia nacional de segurança das redes e sistemas de informação que, por sua vez, define medidas políticas e regulamentares e ainda os objetivos estratégicos.

Para além disso, cada Estado-Membro terá ainda de nomear três entidades para três papeis distintos – a autoridade nacional competente (uma ou várias), o ponto de contacto único e a equipa de resposta a incidentes de segurança informática (CSIRT). A principal tarefa da autoridade nacional competente passa por controlar a execução da Diretiva. Já

relativamente ao ponto de contacto único, cada país membro da UE nomeia uma entidade para este papel que é responsável pelos assuntos relacionados com a segurança, tendo ainda de garantir a cooperação entre as partes envolvidas na execução da Diretiva. Relativamente à rede de equipas de resposta a incidentes de segurança informática – a rede CSIRT – cada Estado-Membro terá também de possuir uma. A CSIRT tem a responsabilidade resolver os incidentes e riscos e assegurar, entre os vários Estados-Membros da UE, a cooperação e a confiança.

A Diretiva apresenta um procedimento geral para a notificação de incidentes constituído por diversas etapas. Neste, pontos de contactos únicos, autoridades nacionais competentes e as CSIRT, desempenham, cada uma, um dado papel. É de mencionar que, só a fase inicial deste processo é comum tanto para operadores de serviços essenciais como para prestadores de serviços digitais, divergindo entre as duas categorias de entidade a partir de um dado momento.

Portugal, como Estado-Membro da UE, teve que efetuar a transposição da Diretiva para a sua legislação sendo que, para tal, criou a Lei nº46/2018, publicada em Diário da República de modo a que a Diretiva passe a ter efeitos em território nacional. A Lei nº46/2018 define os critérios e medidas necessárias para garantir a segurança nas redes e sistemas de informação; é aplicada à Administração Pública, aos operadores de infraestruturas críticas, aos operadores de serviços essenciais, aos prestadores de serviços digitais e a qualquer entidade que utilize redes e sistemas de informação. Esta lei apresenta os requisitos de segurança a cumprir, sendo que estes variam consoante o tipo de entidade em causa. Esta lei apresenta o processo a executar, caso ocorra um incidente, em território nacional.

A Lei nº46/2018 define ainda que é necessário proceder a fiscalizações de modo a se encontrarem incumprimentos. As infrações poderão ser de três níveis de gravidade – muito graves, graves e negligência – sendo sancionadas através de coimas de valor variável. Esta lei refere o Conselho Superior de Segurança do Ciberespaço (CSSC) que tem como objetivo controlar, executar e rever a Estratégia Nacional de Segurança do Ciberespaço (ENSC). Em Portugal, o Centro Nacional de Cibersegurança (CNCS) é a autoridade nacional competente e o ponto de contacto único; o CNCS terá que, por exemplo, identificar os operadores de serviços essenciais portugueses. Já o CERT.PT, em Portugal, corresponde à Equipa de Resposta a Incidentes de Segurança Informática Nacional e é o representante nacional na rede CSIRT Europeia.

A UE ao criar a Diretiva e a adoção dessas normas europeias pela legislação portuguesa, levou a que a ANACOM como autoridade reguladora das comunicações em Portugal sentisse a necessidade de também refletir as suas preocupações, tendo elaborado o Aviso n.º 11948/2018. Este apresenta obrigações específicas que as empresas têm de cumprir e apresenta ainda, com bastante detalhe, o que as empresas devem fazer em caso de incidente.

A UE, perante o cenário atual de tantos riscos e ameaças, tomou a atitude correta ao criar a Diretiva, cuja transposição é obrigatória em cada Estado-Membro. Deste modo, torna-se evidente que a UE pretende, acima de tudo, garantir a segurança no ciberespaço para todos os seus cidadãos. [5]

3. Caracterização do ambiente hipotético

O cenário hipotético para este projeto diz respeito a uma clínica médica que está inserida num grupo privado. Esta clínica para além da prestação de serviços médicos gerais e especializados, tem ainda um departamento de investigação direcionada à área de cardiologia e de autópsias. A clínica hipotética apresenta uma estrutura empresarial no qual existem o corpo administrativo da clínica, Concelho administrativo, que mantém os 4 grupos principais na clínica: Organismo médico e de investigação; Recursos Humanos; Gestão e Finanças; Informático (Serviço Externo). Como se pode visualizar na Figura 1 - Estrutura empresarial da clínica as áreas gerais e especializadas da clínica são a clínica geral, enfermagem, oftalmologia, cardiologia e fisioterapia.

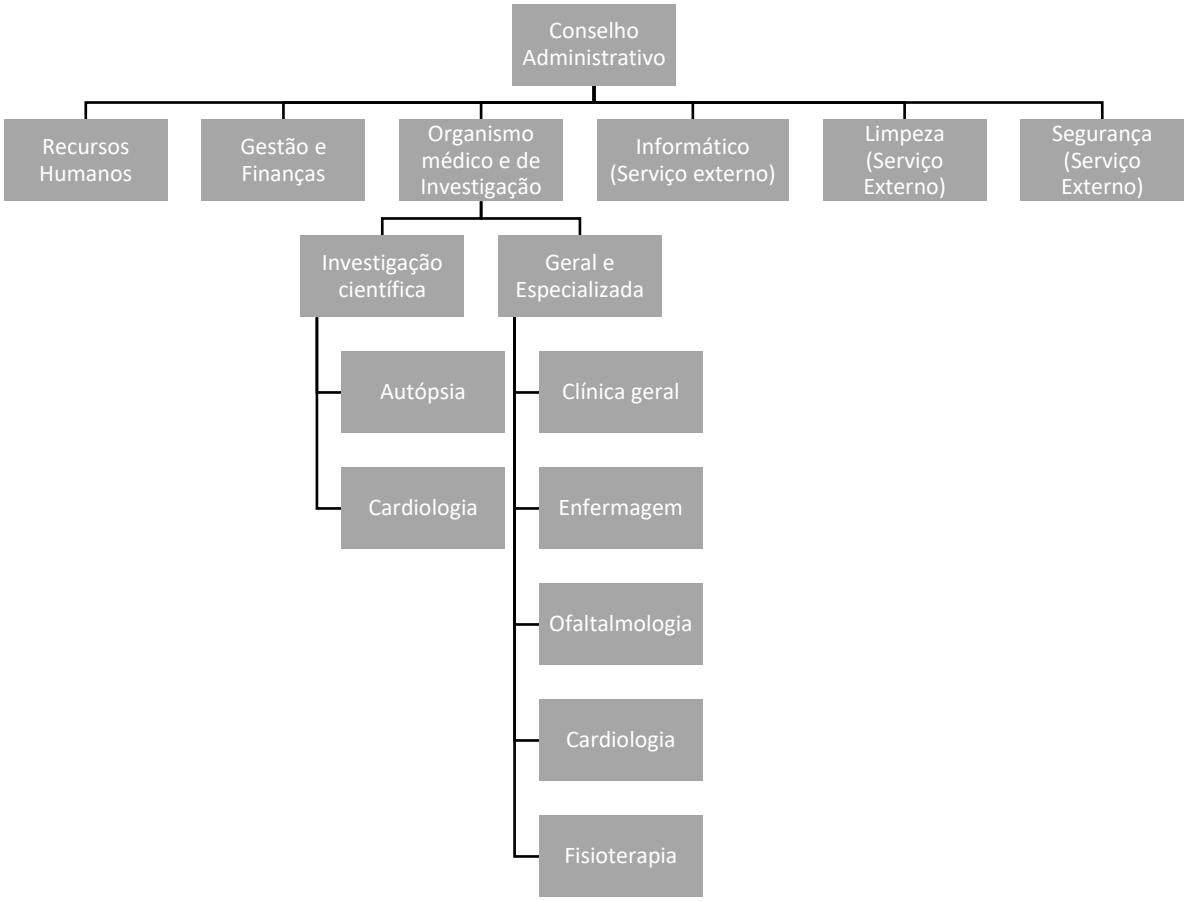

Figura 1 - Estrutura empresarial da clínica

Esta Clínica hipotética localiza-se na cidade de Leiria, em Portugal, e atua no ramo de atividade ligado aos serviços médicos e nos ramos de Investigação científica. O edifício da clínica é constituída por 4 pisos, em que o acesso entre eles é feito por escadas ou elevadores. O primeiro piso (piso -1) é dedicado à realização de autópsias, e também o local onde são armazenados os servidores dedicados que guardam dados relativos a esta clínica. O segundo piso (piso 0) é onde se encontra a receção, a sala de espera, a clínica geral e enfermagem, a oftalmologia, os gabinetes dos recursos humanos, e da gestão e finanças, e por fim o refeitório. O terceiro piso (piso 1) contém os quartos, a cardiologia e a fisioterapia. No último piso (piso 2) é onde reside o departamento de investigação, a sala de reuniões, os gabinetes do diretor executivo e da administração. Na Tabela 1, podem ser visualizados os principais parceiros de negócio da clínica e os seus setores de atividade empresarial.

Tabela 1 - Principais parceiros e setores de atividade

Parceiros	Setores
Indústria Farmacêutica	Farmacêutico
Óticas	Serviço Ótico
Seguradoras	Serviços de Seguros
Institutos / Universidades	Educação
Fabricante de SI	Administração, desenvolvimento e manutenção de *Software*
Polícia Judiciária	Jurídico

A presente clínica hipotética, segue a estrutura de administração empresarial ilustrada na Figura 2, que consiste no conselho administrativo, o qual toma as decisões na clínicas, depois tem-se o diretor executivo, o qual executa as decisões realizadas pelo conselho administrativo. Por fim existem os vários chefes de cada grupo e de cada departamento da clínica.

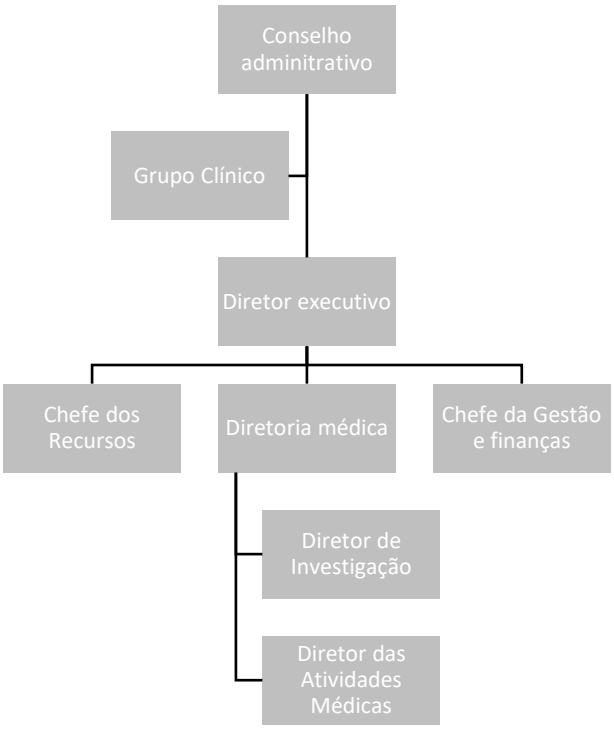

Figura 2 - Estrutura de administração da clínica

A Clínica apresenta uma relação com os pacientes e fornecedores. Esta armazena informações como os dados pessoais, análises e exames, dados de pagamento dos pacientes, sendo todos estes dados são de acesso livre nas clínicas do mesmo grupo clínico. Cada clínica especializa-se em diversas áreas de investigação onde os resultados das pesquisas são partilhados entre o grupo. No caso da presente clínica, esta presta serviços de autópsia à polícia judiciária, pelo que estes dados apenas estão disponíveis na própria clínica e na polícia judiciária. Os fornecedores interagem maioritariamente com o grupo, sendo que apenas alguns interagem com a esta clínica como os fornecedores de produtos alimentares e serviços de higiene e limpeza.

A clínica apresenta uso de *outsourcing*, pois esta recorre a uma empresa externa para a manutenção dos serviços informáticos e a uma empresa para os serviços de higiene e limpeza.

Esta clínica hipotética faz uso de sistemas para facilitar a prestação de serviços aos clientes, tais como um *website* da clínica. Nestes serviços existe uma área pessoal *online* onde o cliente pode marcar consultas, aceder a exames e análises médicas pessoais. A clínica também possui um serviço de telemedicina para quando é necessário um ou mais indivíduos remotos participarem numa atividade médica ou científica da clínica.

Existe também sistema de alarme e videovigilância, sendo que as câmaras se encontram no piso -1, piso 0 na área da receção, no piso 2, na área da investigação e nos corredores. Esse sistema pertence a uma empresa, com a qual se tem contrato, que trata de toda a logística.

Considera-se hipoteticamente que a clínica foi identificada pelo CNCS como operador de serviços essenciais do setor da saúde e, por conseguinte, do subsetor das instalações de prestação de cuidados de saúde. Deste modo, a clínica fica sujeita às obrigações impostas pela Lei nº 46/2018.

4. Arquitetura do Sistema de Informação

O negócio da presente clínica hipotética baseia-se na prestação de serviços de saúde e serviços de autópsia a entidades autoritárias. Os serviços de saúde são:

- Enfermagem;
- Consultas médicas gerais;
- Consultas e tratamentos médicos especializados na:
- Cardiologia;
- Oftalmologia;
- Fisioterapia;

Também são efetuadas investigações científicas no ramo da cardiologia, para fins não lucrativos e para prestígio clínico. Nos serviços de prestação de cuidados de saúde, existem vários processos tais como, o processo para a criação da conta de cliente, o processo de marcação de consultas nos vários serviços prestados, o processo para gestão de consultas, o processo para finalizar as consultas (pagamento), o processo para as atividades de Telemedicina e o processo de armazenamento dos dados recolhidos nos vários processos.

Os dados que são recolhidos e organizados são os dados utilizados nos vários processos de negócio da clínica, sendo estes:

- os dados pessoais do cliente:
    - nome;
    - idade;
    - morada;
    - número de telefone;
    - credenciais de saúde;
    - histórico médico:
        - consultas;
        - exames médicos;
- dados das consultas:
    - paciente;
    - médico;

        - tipo de consulta;
        - data;
        - resultados médicos;
    - dados das investigações científicas;
    - dados das autópsias.

No que toca aos dados mais sensíveis e por consequência estão mais protegido:

- dados pessoais dos clientes;
- dados das investigações;
- dados das autópsias;
- dados das transações financeiras;

No entanto é de notar que todos os dados se encontram protegidos através de diferentes técnicas, segundo o seu grau de sensibilidade.

Por fim, serão distribuídos os dados relativos às investigações científicas e os dados pessoais dos clientes referentes às consultas.

A clínica utiliza duas aplicações à medida, uma para gerir os negócios, as investigações e as autópsias e outra para a interação com os clientes (por exemplo a área de cliente na aplicação). Estas duas aplicações têm integração de serviços de modo à aplicação principal da clínica poder aceder aos dados da aplicação do cliente. Deste modo, serão mantidas duas bases de dados separadas, uma com os dados da aplicação *web* e outra com os dados da aplicação da clínica. A clínica também utiliza um *software* à medida para a telemedicina juntamente com o seu próprio equipamento de *streaming*. Também usa o *software Primavera* da *Oracle* para gerir toda a parte de gestão e faturação. Isto tudo corre em sistemas operativos da *Microsoft*, mais especificamente no *Windows 10 Enterprise*.

Relativamente ao fluxo de informação, a aplicação *web* dos clientes apenas tem acesso à sua base de dados, enquanto que a aplicação da clínica tem acesso à sua base de dados e também à da aplicação dos clientes. Apenas os dados relativos às investigações científicas e os dados das consultas e exames dos pacientes serão partilhadas com outras clínicas pertencentes ao mesmo grupo clínico. Os dados relativos às autópsias serão apenas acessíveis aos clientes desses serviços e aos especialistas que o efetuam. Cada cliente terá acesso apenas às suas informações na base de dados da aplicação *web*. A clínica em si terá acesso a todos os dados dos clientes recolhidos, mas apenas o conselho executivo, o diretor executivo e investigadores têm acesso aos dados das investigações

científicas na presente clínica. Os dados financeiros estão apenas acessíveis tanto ao diretor executivo e restantes cargos superiores como também pela gestão de finanças.

Todo o equipamento informático da clínica é fixo, exceto o portátil do diretor executivo. São também utilizados vários tipos de equipamentos tecnológicos para as várias áreas de saúde dos serviços disponibilizados. Um cliente poderá utilizar qualquer tipo de sistema operativo para utilizar o *software* dedicado ao mesmo, pois este é uma aplicação *web* acessível pelo *browser*. É utilizado um *Ubuntu Server* como sistema operativo dos servidores da clínica, e na clínica existem 3 *Access Points*, cada um no piso 0, 1 e 2. Existem 2 redes *wireless*, uma para uso público e outra para a clínica. Os servidores da clínica são utilizados não só para alojar a aplicação *web* para os clientes, mas também para armazenar os dados das aplicações da clínica e as bases de dados. Para efeitos de comunicação entre funcionários da clínica é usado um serviço de *webmail*, *Microsoft*.

Todos os ativos tecnológicos e de informação estão localizados na clínica, isto significa que os servidores estão presentes no edifício da clínica, mais especificamente no piso -1 do edifício. Se necessário, as aplicações podem pedir dados a outros servidores do grupo e vice-versa.

5. Análise de Risco

A análise de risco é constituída por várias etapas representadas na Figura 3. A Definição do Contexto já foi explicada nos capítulos 3 e 4.

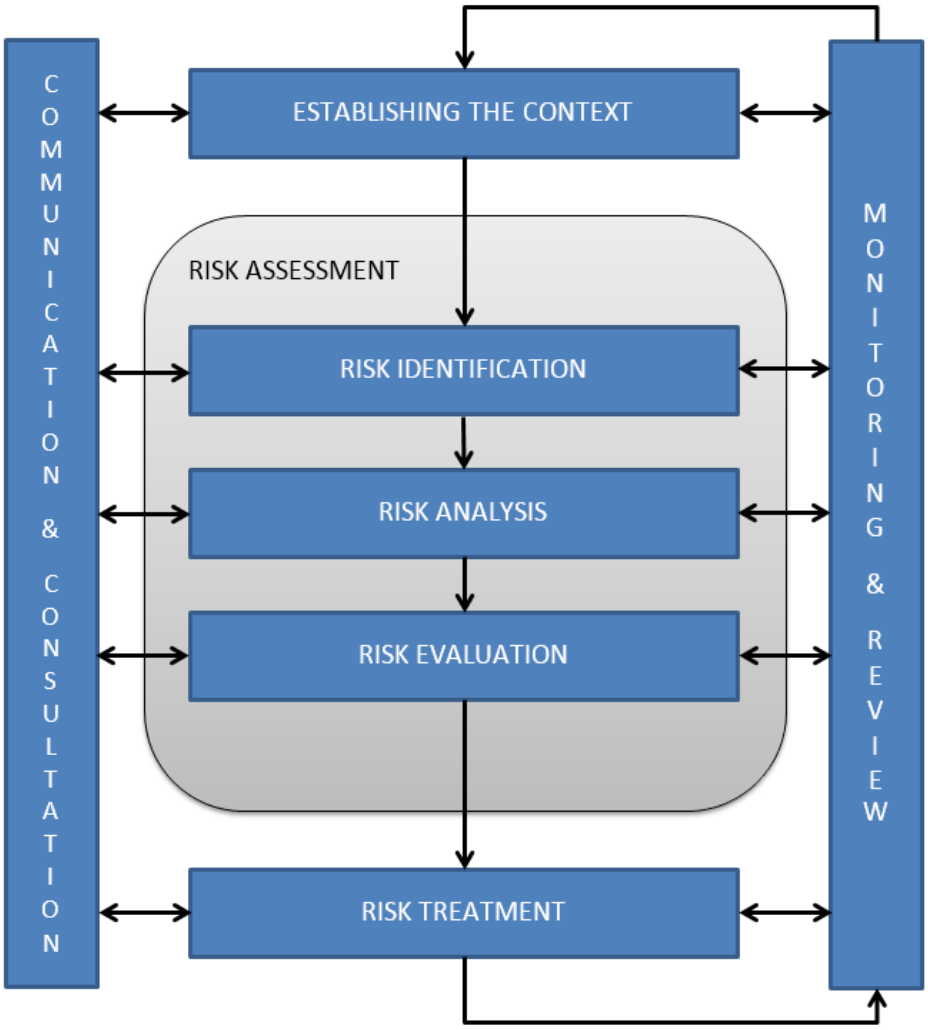

Figura 3 - Processo de análise do risco [1]

5.1 Identificação dos ativos

A clínica conta com vários ativos que têm de ser protegidos. De seguida são listados os ativos da clínica.

- As aplicações que a clínica usa, nomeadamente a aplicação *web*, a da clínica, a aplicação da telemedicina e o *software Primavera*

- Computadores fixos espalhados pela clínica, em áreas de trabalho como nos gabinetes e na área de investigação
- *Access Points*, *router*, *switch* e cabos *Ethernet*
- Quadros elétricos e geradores
- Servidores, encontram-se no piso -1
- Dados privados e/ou confidenciais, nomeadamente dos clientes, da clínica e do grupo
- Portátil pessoal do diretor
- Equipamento médico
- Telefones fixos
- Cartões de acesso
- Equipamento de segurança da empresa contratada
- Documentos
- Impressoras

5.2 Identificação das Ameaças

De seguida são apresentadas várias listas de potenciais ameaças que podem prejudicar os ativos da clínica.

Ameaças físicas:

- Fogo;
- Danos por água;
- Acidente maior;
- Destruição do equipamento.

Ameaças naturais:

- Inundações;
- Sismos;
- Fenómenos climatéricos;
- Fenómenos meteorológico.

Perdas de serviços essenciais:

- Falha de energia;
- Falha dos sistemas de ar-condicionado e água;
- Falha de telecomunicações.

Distúrbio devido a radiação:

- Radiação eletromagnética;
- Pulsos eletromagnéticos.

Comprometimento da informação:

- Espionagem Industrial (local ou remota);
- Escutas;
- Roubo de informação;
- Roubo de equipamento;
- Aproveitamento do equipamento descartado;
- Divulgação de informação confidencial ou privada;
- Modificação do *software* e *hardware*.

Falhas técnicas:

- Falha de equipamento;
- Mau funcionamento do equipamento;
- Saturação dos sistemas de informação;
- Mau funcionamento do *software*.

Ações não autorizadas:

- Uso não autorizado de equipamento e de *software*;
- Corrupção dos dados.

Comprometimento de funções:

- Erro no uso;
- Abuso de direitos;
- Falha na disponibilidade de pessoal para o trabalho.

Muitas das ameaças ditas acima podem ser de fonte humana, para além dessas ainda há:

- *Hackers* ou *crackers*;
- Informante;
- Coimas por incumprimento de legislação e regulamentos.

5.3 Identificação das Vulnerabilidades

Serão listadas várias vulnerabilidades detetadas, consoante o tipo.

Vulnerabilidades de *hardware*:

- Manutenção insuficiente e falha na instalação de dispositivos;
- Planos de substituição equipamentos periódica;
- Suscetibilidade a poeiras, humidade, entre outros;
- Suscetibilidade à radiação e pulsos eletromagnéticos;
- Suscetibilidade às mudanças de temperatura;
- Suscetibilidade a variações de energia;
- Armazenamento desprotegido;
- Falta de cuidado no despacho de equipamentos de armazenamento;
- Cópia descontrolada.

Vulnerabilidades de *software*:

- Testes insuficientes aos *software* feitos à medida;
- Falhas bem conhecidas no *software Primavera* e *Windows*;
- Utilizadores do sistemas não fazerem *logout*;
- Falta de cuidado na reutilização de equipamentos de armazenamento;
- Inexistência de auditorias;
- Má alocação dos direitos de acesso;
- Falta de documentação nos *software* feitos à medida;
- Definição incorreta de parâmetros de input nos *software* à medida;
- Inexistência de mecanismos de autenticação e identificação;
- Tabelas de *password* desprotegidas;
- Fraca gestão de *password*;
- *Software* à medida novo e imaturo;

- Não controlo de *downloads* e uso de *software*;
- Falta de *backups* e testes de *backups*;
- Falta de proteção física do edifício;
- Produção ineficiente de relatórios.

Vulnerabilidades de rede:

- Linhas de comunicação desprotegidas;
- Tráfego de dados desprotegidos;
- Ponto único de falha;
- Arquitetura de rede insegura;
- Transferência de *passwords* em texto;
- Conexões à rede pública desprotegidas;

Vulnerabilidades relacionadas a pessoal interno:

- Ausência de pessoal;
- Procedimentos de recrutamento inadequados;
- Treino de segurança inadequados;
- Uso incorreto de *software* e *hardware*;
- Falta de consciência em relação à segurança;
- Falta de mecanismos de monitorização;
- Trabalho não supervisionado por empresas de terceiros.

Vulnerabilidades do local físico:

- Falta de controlo ao acesso físico ao edifício e áreas do mesmo;
- Falta de proteções físicas em áreas sensíveis.

Vulnerabilidades da organização:

- Falta de procedimento para registo ou revogação de utilizadores;
- Falta de preocupações de segurança aquando os contratos com terceiros;
- Serviço de resposta de manutenção inadequado;
- Falta de políticas de utilização de *email*;
- Falta de procedimentos para tratamento e manipulação de informação confidencial;
- Falta de procedimentos disciplinares definidos em caso de incidente de segurança da informação;

- Falta de política formal da utilização de portáteis;
- Falta de políticas de "*clear desk*" ou "*clear screen*";
- Falta de controlo de ativos para fora da clínica;
- Falta de mecanismos de monitorização estabelecidos para quebras de segurança;
- Falta de procedimentos para reportar problemas de segurança;
- Não conformidade com o RGPD;
- Não cumprimento das obrigações a que está sujeita como operador de serviços essenciais presentes na lei n 46/2018.

Para além de todas as vulnerabilidades e ameaças mencionadas, como se usa alguns *software* feitos à medida, estes são mais suscetíveis a ataques do tipo *Denial of Service*, ataques *zero-day*, *eavesdropping*, entre outros.

5.4 Tabelas de Identificação dos Riscos

Para a identificação dos riscos recorreu-se a um ficheiro com tabelas intitulado de "Análise de Risco.xls" disponibilizadas na página da unidade curricular da Plataforma de *eLearning* 2018.19. As tabelas de identificação dos riscos encontram-se em anexo.

Os riscos foram identificados através das vulnerabilidades e das ameaças anteriormente identificadas para este cenário hipotético, tendo-se ainda recorrido como auxílio à ISO 27005. Da totalidade de riscos identificados, alguns apresentam uma menor granularidade de modo a abranger o maior número de casos possíveis que estejam correlacionados entre si.

Alguns dos riscos identificados apresentam uma maior preocupação uma vez que afetam não só a clínica, mas também o grupo no seu todo e, possivelmente, em alguns casos, os parceiros. Exemplos destes riscos são o comprometimento da informação porque como a clínica se insere no grupo e também detém informação do mesmo, assim a ocorrência deste risco poderá afetar a clínica em específico e o grupo; como a clínica

tem uma área voltada para a investigação, se a informação deste departamento ficar comprometida, o seu parceiro, nomeadamente a indústria farmacêutica, também poderá ser implicado. Para além disso, se existir comprometimento da informação na área das autópsias, este poderá afetar severamente uma investigação policial.

Relativamente às coimas por incumprimento de legislação e regulamentos, estas, no caso do cenário hipotético criado para este trabalho, referem-se às coimas que a clínica poderá sofrer por incumprimento do RGPD e da Lei nº46/2018. É de mencionar não só o facto de cada um dos elementos se referir a aspetos legislativos divergentes como também o facto de aplicarem coimas diferentes e por razões distintas.

5.5 Avaliação dos Riscos

No subcapítulo anterior, a ordem pela qual as tabelas foram apresentadas foi de acordo com o nível de gravidade dos riscos, mais especificamente, por ordem decrescente. Assim, decidiu-se que se irá tentar mitigar todos os riscos identificados com a exceção dos informadores e da falta na disponibilidade de pessoal para o trabalho. Em relação aos informadores, este não é um risco que será mitigado uma vez que se considerou que o custo inerente à mitigação deste risco comparativamente à probabilidade do mesmo ocorrer não compensa o investimento. Deste modo, será um risco que a entidade irá aceitar. Já relativamente à falta na disponibilidade de pessoal para o trabalho, este risco será aceite dado que não existe qualquer controlo ou medida de mitigação para o mesmo.

Os riscos identificados que se tentarão mitigar são nomeadamente os *malwares*, erro no uso, falhas técnicas de *software*, comprometimento da informação, abuso de direitos, ações não autorizadas, furto de equipamento, falta na disponibilidade de pessoal para o trabalho, *hackers* ou *crackers*, falhas técnicas de *hardware*, coimas por incumprimento de legislação e regulamentos, perda de serviços essenciais, distúrbio devido a radiação e ameaças físicas e/ou naturais. Todos estes riscos identificados serão mitigados uma vez que o custo da sua mitigação comparativamente com as vantagens que se obtêm da sua mitigação, compensa.

O objetivo da mitigação de todos estes riscos passa por tentar manter a credibilidade e segurança na clínica e garantir o seu funcionamento no que toca aos serviços prestados, redes e sistemas de informação.

No que diz respeito ao risco referente às coimas por incumprimento de legislação e regulamentos, é importante a clínica tentar mitigar o mesmo uma vez que tais incumprimentos poderão se tornar de conhecimento público, nomeadamente dos *media*, prejudicando a sua credibilidade, que, por sua vez, corresponde a uma consequência grave para o negócio em si.

5.6 Políticas e controlos de segurança dos sistemas de informação

Todos estes controlos antes de serem implementados serão discutidos pelo conselho administrativo e executados, depois, pelo diretor executivo. Isto é, o diretor executivo será o responsável por comunicar com as entidades e serviços apropriados para implementar os controlos de segurança aqui definidos e escolhidos pelo conselho administrativo.

Ameaça: *Malware*.

Medidas de controlo:

- **Política de dispositivos móveis**

Políticas:

  - "Não devem ser utilizados dispositivos móveis nas instalações da clínica que não estejam presentes no registo de dispositivos permitidos";
  - "Para os dispositivos permitidos, não deve ser instalado *software* de fontes desconhecidas ou não confiáveis";
  - "Todos os dispositivos móveis da clínica devem ser protegidos, isto é, não devem ser deixados em zonas inseguras e de forma não protegida contra acesso físico por outros indivíduos não autorizados".

Estas políticas são afetas a toda a clínica.

- **Acesso a redes e a serviços de rede**

Política:

  - "Não devem ser usados dispositivos da clínica para aceder a redes ou serviços não pertencentes à clínica ou não confiáveis".

Esta política afeta a toda a clínica.

- **Controlos contra código malicioso**

Para além do que já foi estabelecido sobre a instalação de *software* não conhecido ou confiável, será também imposto que os equipamentos estarão devidamente atualizados com as medidas de segurança mais recentes nos dispositivos informáticos.

Serão também bloqueados quaisquer *websites* desnecessários para o funcionamento da clínica na rede privada, e na rede publica serão bloqueados apenas os *websites* conhecidos/identificados como perigosos.

Estas medidas de segurança serão garantidas pelo serviço informático.

- **Restrições sobre a instalação de *software***

Qualquer *software* não conhecido ou confiável não será permitido ser instalado nos equipamentos e dispositivos de trabalho da clínica.

Caso seja necessário instalar algum *software*, tal deverá ser permitido pelos serviços informáticos, que, por sua vez, avaliam o *software* e executam a instalação se necessário.

Ameaça: Erro no uso.

Medidas de controlo:

- **Consciencialização, educação e formação em segurança da informação**

Irá ser disponibilizada formação na utilização dos *software* usados na clínica e nas boas práticas de segurança da informação. Estas formações estão disponíveis apenas a novos funcionários da clínica.

Serão também iniciadas ações de consciencialização da segurança da informação e dos dispositivos da clínica uma vez a cada seis meses. Estas ações afetam toda a clínica.

Ameaça: Falhas técnicas de *software*.

Medidas de controlo:

- **Teste de aceitação de sistemas**

O serviço informático está responsabilizado pelo desenvolvimento de testes de aceitação nos *software* da clínica de modo a analisar possíveis vulnerabilidades nas aplicações resultantes de novas atualizações noutros sistemas e no próprio *software* à medida da clínica.

Ameaça: Comprometimento da informação.

Medidas de controlo:

- **Gestão de suportes de dados amovíveis**

Ao reutilizar um suporte, este deverá ser sujeito a um *software* de formatação e limpeza da informação lá guardada.

Ao terminar a utilização do suporte, este deverá ser guardado num lugar seguro.

Cada suporte está ou deverá ser registado, como também catalogado o registo dos funcionários que utilizaram o determinado suporte.

Cada suporte deverá usar encriptação do conteúdo, isto é, dependendo do dispositivo este deverá usar um método adequado para a encriptação da informação.

- **Eliminação de suportes de dados**

Ao descartar um suporte, este deverá ser devidamente destruído.

Anualmente será feita uma auditoria nos suportes de dados amovíveis para identificar os suportes sujeites a troca por um novo.

Qualquer suporte que armazene informação sensível será registado e monitorizado.

- **Restrição de acesso à informação**

Como será referido no controlo "Papéis e responsabilidades de segurança da informação", os direitos de acesso serão de acordo com as responsabilidades por cada ativo já estabelecidas, e baseados nos controlos de acesso na clínica.

Os acessos dentro dos sistemas informáticos serão geridos pelo serviço informático.

- **Política sobre a utilização de controlos criptográficos**

Políticas e implementações:

  - "Todos os dados a circular pela rede *Wi-Fi* privada da clínica devem ser encriptados e seguros pelo *WPA2-enterprize*";
  - "Na transmissão dos dados da clínica para o grupo clínico pela rede pública (Internet), deverá ser usado uma camada segura para enviar os dados, nomeadamente, a última versão do protocolo *TLS/SSL*".

- **Política de secretária limpa e ecrã limpo**

De modo a evitar falhas na segurança da informação, a gestão e responsáveis de cada departamento serão responsáveis por formar e consciencializar os funcionários da clínica a manter o seu ambiente de trabalho limpo e livre de informação confidencial exposta ao olho nu.

- **Acordos de confidencialidade ou não divulgação**

Como a clínica lida com vários dados sensíveis, deverá ser garantida a implementação de acordos de confidencialidade e não divulgação a todos os membros e parceiros da clínica. Estes acordos definem também as responsabilidades, ações e consequências caso uma falha na segurança de informação aconteça.

Ameaça: Abuso de direitos.

Medidas de controlo:

- **Papéis e responsabilidades de segurança da informação**

No organismo médico e de investigação:

  - O departamento de investigação e o departamento médico estão responsáveis pelos dados e informação derivados das suas atividades;
  - O serviço informático está responsável pelos processos e funcionamento das aplicações da clínica.

O serviço de segurança é responsável pela segurança física dos ativos físicos da clínica.

A gestão é responsável pelas informações dos funcionários da clínica.

O conselho administrativo é responsável pela informação proveniente das outras clínicas e do grupo.

A gestão e o conselho administrativo são responsáveis pela informação económica e financeira do negócio da clínica.

- **Segregação de funções**

Como está definido no controlo "Papéis e responsabilidades de segurança da informação", os ativos só poderão ser utilizados por quem necessite dos mesmos para desempenhar as suas funções e que, por sua vez, tenha permissões para fazer uso desses mesmos ativos; ao utilizá-los esses funcionários tornam-se responsáveis pelos ativos em causa.

Ameaça: Ações não autorizadas.

Medidas de controlo:

- **Remoção de ativos**

Quaisquer ativos deverão permanecer na clínica, apenas com a exceção do portátil do diretor executivo no qual terá segurança criptográfica no disco e consciencialização do diretor para evitar deixar este ativo em locais desprotegidos.

Para a eventualidade de existir uma remoção de um ativo devidamente justificada, esta será registada: o quando será removido e quando será devolvido, identificada o responsável, e também processado um acordo de responsabilidade por tal ativo.

Este processo será da responsabilidade da gestão da clínica.

- **Procedimento disciplinar**

Nos casos de incidentes sobre a segurança da informação, caso seja identificado e confirmado um ator responsável pelo incidente pertencente à clínica, este será sujeito a um procedimento disciplinar com base na natureza e gravidade do incidente.

- **Política de controlo de acesso**

Políticas:

  - "Cada responsável pelo seu ativo estará também responsável por definir as formas e restrições para outro elemento da clínica poder aceder a esse ativo";
  - "No acesso físico, os clientes apenas têm acesso aos pisos 0 e 1; apenas os membros do conselho administrativo e membros do departamento de investigação têm acesso ao piso 2; apenas os serviços informáticos e os responsáveis pelas autópsias têm acesso ao piso -1. Os seguranças têm acesso a qualquer piso do edifício, e os funcionários do serviço de limpeza têm acesso total ao edifício, mas com acesso condicionado nos pisos -1 e 2, onde serão acompanhados por um segurança".

- **Gestão de direitos de acesso privilegiado**

A gestão de direitos de acesso físico é executada pelo serviço de segurança. A gestão dos direitos de acesso privilegiado nos ativos será mantida pela gestão da clínica.

Ameaça: Furto de equipamento.

Medidas de controlo:

- **Perímetro de segurança físico**

Como a clínica tem áreas no edifício onde ocorrem atividades com dados sensíveis, estas devem ser devidamente identificadas e protegidas:

  - Todo o piso -1 deverá ter o máximo de segurança possível;
  - Todo o piso 2 deverá ter o máximo de segurança possível;
  - As áreas de trabalho da gestão e gabinetes nos pisos 0 e 1 devem ter pelo menos segurança física mínima com controlo de acesso apenas para os funcionários da clínica e outros autorizados;

- **Controlos de entrada física**

Os controlos de entrada física serão garantidos implementando um sistema de cartões de identificação para permitir acesso a diferentes pisos e salas do edifício.

Este controlo de acesso será implementado pelo serviço informático e gerido pelo serviço de segurança.

- **Colocação e proteção de equipamentos**

Como a clínica disponibiliza vários equipamentos médicos e informáticos. estes devem ser protegidos. Desta forma deverão ser seguidas as seguintes guias:

  - Todo o equipamento médico deverá ser apenas utilizado nas horas de trabalho;
  - Todo o equipamento informático existente nos mesmos pisos que o equipamento médico deverá ser protegido contra possíveis exposições eletromagnéticas.

Ameaça: *Hacker* ou *Crackers*.

Medidas de controlo:

- **Contacto com autoridades competentes**

Sempre que um incidente ocorrer na segurança da informação da clínica deveram ser contactadas as seguintes autoridades:

  - Autoridade jurídica;

- CNCS;
- Grupo Clínico;
- CNPD.

Ameaça: Falhas técnicas *hardware*.

Medidas de controlo:

- **Manutenção de equipamentos**

Para além dos equipamentos de serviços básicos de suporte, será também estabelecido um plano de manutenção para os equipamentos médicos e informáticos.

A manutenção para os equipamentos informáticos será executada pelos serviços informáticos, e a manutenção dos equipamentos médicos será realizada pelos fabricantes dos equipamentos ou por uma empresa competente no serviço de manutenção de equipamento médico.

Ameaça: Coimas por incumprimento de legislação e regulamentos.

Medidas de controlo:

- **Reportar eventos de segurança da informação e das redes e sistema de informação**

Serão implementadas regras sobre o que os funcionários da clínica deverão fazer em caso de falha da segurança de informação.

Sempre que for detetado alguma falha no *software*/*hardware*, esta deve ser notificada aos serviços informáticos de tal ocorrência.

No caso de falhas na expetativa da integridade, confidencialidade e disponibilidade devem ser notificadas à gestão.

Violações de acesso devem ser reportadas ao serviço de segurança.

Falhas derivadas do erro humano devem ser notificadas à gestão.

Incumprimento com as políticas de segurança devem ser reportadas à gestão.

- **Privacidade e proteção de dados pessoais e segurança das redes e sistemas de informação**

Deve ser garantido que exista sempre um especialista sobre o RGPD, nomeadamente um EPD, que analise e mantenha a conformidade da clínica com o regulamento.

Os dados pessoais devem ser protegidos desde o momento em que são obtidos e até terem um fim.

A clínica deve ter mecanismos que permitam implementar a segurança dos dados pessoais, e que permitam garantir os direitos previstos no regulamento para os titulares dos dados.

A clínica, na qualidade de operador de serviços essenciais, deve cumprir tanto a implementação dos requisitos de segurança previstos na lei como também as instruções de cibersegurança emitidas pelo CNCS.

Para além disso, a clínica na eventualidade de sofrer um incidente que afete o funcionamento e a segurança das suas redes e sistemas de informação deve-o notificar à CNCS.

Se ocorrer falhas de segurança que comprometam os dados confidenciais e/ou privados e/ou as redes e sistemas de informação da clínica, caso seja caso disso, deverão ser notificadas, dentro dos prazos limites, as autoridades competentes. Essas autoridades, dependendo do caso, poderão ser a CNPD e a CNCS, garantindo assim que os regulamentos e legislação a que a clínica está sujeita são devidamente cumpridos.

Ameaça: Perda de serviços essenciais.

Medidas de controlo:

- **Segurança da cablagem**

No edifício da clínica, os cabos da rede e os cabos de comunicações da clínica serão separados para evitar possíveis interferências.

Toda a cablagem deverá estar instalada nas instalações de modo a permanecer escondida e de difícil acesso. Apenas os terminais estarão visíveis e protegidos com um mecanismo de controlo de acesso de modo a que só os indivíduos com autorização dada pelo diretor e/ou segurança possam aceder.

- **Serviços básicos de suporte**

De modo a combater avarias nos serviços básicos de suporte, será criado um plano para efetuar a manutenção periódica dos equipamentos relativos a estes serviços na clínica.

Para a eventualidade de ocorrer uma falha externa à clínica, deverão ser estabelecidos serviços básicos de suporte alternativos, isto é, uma segunda fonte de água potável, uma segunda fonte de energia suplementar e uma segunda fonte de gás.

Ameaça: Ameaças físicas e/ou naturais.

Medidas de controlo:

- **Proteção contra ameaças externas e ambientais**

De modo a evitar danos causados pelos incidentes externos ou ambientais, será contratado um especialista nesta área de trabalho para ajudar a definir medidas para combater estas ameaças. A clínica terá de ter ainda dispositivos de deteção de incêndios bem como sistema de ar condicionado de modo a controlar a temperatura no interior do edifício.

6. Conclusões e recomendações futuras

Para este trabalho foi concebido para cenário hipotético uma clínica que tem um departamento de investigação médica, uma pareceria com a polícia judiciária para a concretização de autópsias, para além dos cuidados médicos gerais que oferece. Deste modo, esta clínica apresenta uma séria de ativos que devem ser protegidos tais como dados privados e ou confidenciais.

Assim a maior parte da informação que é tratada pela clínica é privada e confidencial, sendo que tem de existir assim uma boa infraestrutura que garanta a segurança da mesma. A informação mais crítica passa pelos dados dos clientes, das investigações, das autópsias e do grupo clínico. Também se tem de ter em consideração o RGPD sendo que o mesmo tem como objetivo a proteção dos dados dos titulares dos mesmo. Para além do RGPD a clínica também foi hipoteticamente identificada como um operador de serviços essenciais, o que obriga a cumprir a lei nº 46/2018 que define um conjunto de regras para garantir a segurança das redes e sistemas de informação em território nacional.

De modo a assegurar a segurança dos ativos, foi feita uma análise de risco que explora grande parte das vulnerabilidades assim como ameaças que possam existir.

Nesta análise é abordada cada ameaça e vulnerabilidade procurando-se mitigar o maior número de riscos possíveis. Os riscos foram identificados e avaliados tendo em consideração a sua probabilidade de ocorrência e o consequente impacto que teriam para a empresa. Exemplos de riscos mais graves passam por *malwares,* erros na utilização de *hardware*/*software*, falhas técnicas de *software*. Riscos menos graves passam por ameaças físicas e/ou naturais, perda de serviços essenciais e incumprimentos de legislação e regulamentos.

Para a escolha dos controlos para mitigar os riscos não aceites, foram definidos controlos recomendados pelas normas ISO/IEC 27001 e 27002. Neste processo, os controlos escolhidos foram os que se consideravam essenciais e efetivos para tentar mitigar ao máximo o risco associado a uma ameaça.

Sempre que os riscos são mitigados, poderá existir um risco residual pelo que se deve procurar novamente uma forma de os mitigar. No caso de isto não ser possível, é considerada a aceitação do risco, caso os recursos necessários para a sua mitigação não

compensem face à probabilidade e impacto do risco. Exemplos destes riscos são os informadores e a falta de disponibilidade de pessoal para o trabalho. Apenas dois riscos foram aceites dado que o dispêndio para implementar os controlos específicos para combater esses mesmos riscos não irão justificar o valor gasto para os resolver. Desta forma, estes dois riscos foram aceites como vulnerabilidades; possivelmente, serão tratados no futuro, quando existirem formas mais eficientes de se o fazer.

Com a análise feita verificou-se que é impossível ter em conta todas as vulnerabilidades e ameaças possíveis, mas a maior parte são abordadas. Também se verificou que vão existir sempre riscos que não se poderão mitigar, tendo de se considerar a sua aceitação.

Determinou-se que uma boa política de segurança seria fazer-se análises de risco periodicamente pois as ameaças estão constantemente a surgir e/ou mudar, pelo que se têm de atualizar as medidas de mitigação constantemente. Como trabalho futuro deverá observar-se o funcionamento da clínica em contexto real, de forma a determinar se as medidas de mitigação aplicadas são eficientes e viáveis ou se surgem mais riscos que não foram tidos em consideração nesta análise.

7. Referências

[1] NP ISO/IEC 27005:2011, Tecnologia de informação - Técnicas de segurança - Gestão de Riscos de Segurança da Informação.

[2] NP ISO/IEC 27001:2013, Tecnologia de informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos.

[3] Dejank, "Is ISO 27001:2013 based on PDCA cycle?," muut.com, 12 1 2016. [Online]. Available: https://muut.com/i/advisera/27001academy:is-iso-270012013-based-on.

[4] J. Pedrosa, "Regulamento Geral da Proteção de Dados O Novo Paradigma dos Dados Pessoais," Leiria, 2018.

[5] P. Silva, "Diretiva UE 2016/1148 Nível comum de segurança das redes e a Lei da Segurança do Ciberespaço 46-2018," Leiria, 2018.

1. Anexo

Ameaça	*Malwares*		
Impacto Resultante	Impacto médio. A ocorrência pode representar uma anomalia localizada na organização. Uma fonte desta ameaça serão os dispositivos pessoais ligados à rede.	Vulnerabilidade	3
		Aviso prévio	2
		Duration	2
		Valor do Impacto(V+E+D)	7
			Médio
Probabilidade de Ocorrência	Devido ao uso da internet e dispositivos conectados à rede, a probabilidade de ocorrência é elevada.	Probabilidade de Ocorrência	3
			Elevado
Risco Inerente			Elevado

Erro no uso		
Impacto elevado. A má utilização dos equipamentos / *software*, poderá implicar o comprometimento do sistema ou perda total /parcial dos ativos.	Vulnerabilidade	3
	Aviso prévio	2
	Duration	3
	Valor do Impacto(V+E+D)	8
		Elevado
A probabilidade de um erro acontecer na utilização dos ativos é moderada.	Probabilidade de Ocorrência	2
		Moderado
		Elevado

Falhas técnicas *software*		
Impacto médio. Algum do *software* utilizado na empresa é feito à medida, pelo que podem existir *bugs* no mesmo, provocando mau funcionamento. Isto poderá afetar a prestação dos serviços ou até a perda de dados parcial ou total	Vulnerabilidade	3
	Aviso prévio	2
	Duration	2
	Valor do Impacto(V+E+D)	7
		Médio
A probabilidade de um *bug* ou congestionamento no sistema é elevado. Devido à falta de testes efetuados em *software* à medida.	Probabilidade de Ocorrência	3
		Elevado
		Elevado

Comprometimento da informação		
Impacto elevado. Poderá ocorrer na empresa ou no grupo. Poderá existir perda de credibilidade da empresa e terceiros. Poderá ter impacto negativo no negócio.	Vulnerabilidade	3
	Aviso prévio	2
	Duration	3
	Valor do Impacto(V+E+D)	8
		Elevado
A probabilidade de comprometimento é baixa.	Probabilidade de Ocorrência	1
		Baixo
		Moderado

Abuso de direitos		
Impacto médio. Os direitos podem estar mal distribuidos pelos vários perfis levando a que se tenham mais previlégios do que os necessários para exercer o cargo. Também poderá ocorrer abuso de direitos devido a más intenções de um ator, o que poderá implicar o comprometimento do sistema ou perda total /parcial dos ativos.	Vulnerabilidade	2
	Aviso prévio	2
	Duration	3
	Valor do Impacto(V+E+D)	7
		Médio
A probabilidade de ocorrer o abuso de direitos é moderada.	Probabilidade de Ocorrência	2
		Moderado
		Moderado

Ações não autorizadas		
Impacto médio. As ações dependerão da intenção do ator, mas poderá implicar o comprometimento do sistema ou perda total /parcial dos ativos.	Vulnerabilidade	3
	Aviso prévio	2
	Duration	2
	Valor do Impacto(V+E+D)	7
		Médio
A probabilidade de uma ação não autorizada acontecer é moderada.	Probabilidade de Ocorrência	2
		Moderado
		Moderado

Furto de equipamento		
Impacto médio. Poderá ocorrer dentro e fora do perímetro da organização.	Vulnerabilidade	2
	Aviso prévio	2
	Duration	3
	Valor do Impacto(V+E+D)	7
		Médio
A probabilidade de ocorrer é moderada.	Probabilidade de Ocorrência	2
		Moderado
		Moderado

Falta na disponibilidade de pessoal para o trabalho		
Impacto médio. A falta de pessoal poderá comprometer o funcionamento normal do negócio.	Vulnerabilidade	3
	Aviso prévio	1
	Duration	2
	Valor do Impacto(V+E+D)	6
		Médio
A probabilidade de ocorrer é moderada.	Probabilidade de Ocorrência	2
		Moderado
		Moderado

Hacker* ou *crackers		
Impacto elevado. Poderá existir destruição ou roubo de informação. Poderá existir negação de serviço, entre outros, o que pode comprometer o normal funcionamento da organização.	Vulnerabilidade	3
	Aviso prévio	2
	Duration	3
	Valor do Impacto(V+E+D)	8
		Elevado
A probabilidade de um indivíduo ou organização querer prejudicar a empresa é baixa.	Probabilidade de Ocorrência	1
		Baixo
		Moderado

Falhas técnicas *hardware*		
Impacto médio. Algum do *hardware* poderá deixar de funcionar corretamente, provocando mau funcionamento. Isto poderá afetar a prestação dos serviços ou até perda de dados parcial ou total.	Vulnerabilidade	3
	Aviso prévio	2
	Duration	2
	Valor do Impacto(V+E+D)	7
		Médio
A probabilidade de um disco rígido ou equipamento falhar é reduzida, pois estes dispositivos são extensivamente testados pelos fabricantes.	Probabilidade de Ocorrência	1
		Baixo
		Baixo

Coimas por incumprimento de legislação e regulamentos		
Impacto baixo. Poderá existir perda de credibilidade da empresa no caso de uma coima ser aplicada e esta ser notificada aos *media*.	Vulnerabilidade	1
	Aviso prévio	1
	Duration	3
	Valor do Impacto(V+E+D)	5
		Baixo
A probabilidade de uma autoridade de controlo / fiscalizadora aplicar uma coima é baixa.	Probabilidade de Ocorrência	1
		Baixo
		Baixo

Perda de serviços essenciais		
Impacto médio. Poderá impedir o normal funcionamento da organização.	Vulnerabilidade	3
	Aviso prévio	2
	Duration	2
	Valor do Impacto(V+E+D)	7
		Médio
A probabilidade de uma perda de serviço essencial é baixa.	Probabilidade de Ocorrência	1
		Baixo
		Baixo

Distúrbio devido a radiação		
Impacto baixo. Poderá impedir o normal funcionamento da organização e ou danificar os ativos.	Vulnerabilidade	2
	Aviso prévio	1
	Duration	1
	Valor do Impacto(V+E+D)	4
		Baixo
A probabilidade de uma anomalia ocorrer num equipamento médico é baixa.	Probabilidade de Ocorrência	1
		Baixo
		Baixo

Ameaças físicas e/ou naturais		
Impacto médio. Poderá existir destruição total ou parcial de ativos da empresa.	Vulnerabilidade	3
	Aviso prévio	2
	Duration	2
	Valor do Impacto(V+E+D)	7
		Médio
A probabilidade de uma ameaça física e/ou natural ocorrer é baixa.	Probabilidade de Ocorrência	1
		Baixo
		Baixo

Informadores		
Impacto médio. Poderá existir espionagem industrial visto que a organização tem um departamento de investigação, assim como tem uma parceria com a policia judiciária ao efetuar as autópsias.	Vulnerabilidade	3
	Aviso prévio	2
	Duration	2
	Valor do Impacto(V+E+D)	7
		Médio
A probabilidade de um individuo ou organização querer prejudicar a empresa é baixa.	Probabilidade de Ocorrência	1
		Baixo
		Baixo