POLITÉCNICO DE LEIRIA | ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Relatório Prático

Mestrado em Cibersegurança e Informática Forense

Gestão de continuidade de negócio numa Clínica Médica Hipotética

Filipe Henriques, 2180066

Jéssica Pedrosa, 2180067

Patrícia Silva, 2180068

Tiago Martins, 2182716

Leiria, junho de 2019

Resumo

O presente trabalho prende-se com a gestão de continuidade de negócios de uma organização. Deste modo, 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.

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. Estas parcerias 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 gestão de continuidade de negócios da clínica, foi efetuado uma análise de riscos no qual envolveu 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. Consoante os riscos mitigados e aceites, foram criados as políticas e planos necessários para preparar a clínica no caso destes riscos acontecerem.

Para a realização deste trabalho foram levados em consideração um conjunto de elementos legislativos e normativos nomeadamente a NIST *Special Publication* 800-34 Rev. 1, a ISO/IEC 27001, 27002, a 27005 e 27031 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: Continuidade, negócio, riscos, incidentes, ativos.

Esta página foi intencionalmente deixada em branco

Lista de Figuras

FIGURA 1 - ESTRUTURA EMPRESARIAL DA CLÍNICA 3

FIGURA 2 - ESTRUTURA DE ADMINISTRAÇÃO DA CLÍNICA 5

FIGURA 3 - PROCESSO DE ANÁLISE DO RISCO 11

Esta página foi intencionalmente deixada em branco

Lista de Tabelas

TABELA 1 - PRINCIPAIS PARCEIROS E SETORES DE ATIVIDADE 4

TABELA 2 - LISTA DE PROCESSOS DO SISTEMA DE INFORMAÇÃO..... 26

TABELA 3 - CLASSIFICAÇÃO DE IMPACTOS NOS PROCESSOS..... 29

TABELA 4 - ESTIMATIVA DOS TEMPOS DE INATIVIDADE..... 30

TABELA 5 - COMPONENTES/RECURSOS DO SISTEMA DA CLÍNICA..... 32

TABELA 6 - IDENTIFICAÇÃO DE PRIORIDADE DOS RECURSOS 33

Lista de Acrónimos

BCP – *Business Continuity Plan*

CNPD – Comissão Nacional de Proteção de Dados

CNCS – Centro Nacional de Cibersegurança

DRP – *Disaster Recovery Plan*

EPD – Encarregado de Proteção de Dados

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

MTD - *Maximum Tolerable Downtime*

NAS - *Network-attached storage*

NIST – *National Institute of Standards and Technology*

RGPD – Regulamento Geral de Proteção de Dados

RPO - *Recovery Point Objective*

RTO - *Recovery Time Objective*

SIEM – *Security Information and Event Management*

SGSI – Sistema de Gestão da Segurança de Informação

UE – União Europeia

WRT - *Work Recovery Time*

Índice

Resumo i

Lista de Figuras iii

Lista de Tabelas v

Lista de Acrónimos vi

Índice vii

1. Introdução 1

2. Caracterização do ambiente hipotético 3

3. Arquitetura do Sistema de Informação 7

4. Análise de Risco 11

4.1 Identificação dos Ativos 11

4.2 Identificação das Ameaças 13

4.3 Identificação das Vulnerabilidades 15

4.4 Tabelas de Identificação dos Riscos 17

4.5 Avaliação dos Riscos 21

5. Gestão de continuidade de negócios 22

5.1. Políticas de continuidade de negócio 22

5.2. Business Impact Assessement 25

5.2.1. Determinação dos processos de negócio e da criticidade da recuperação 25

5.2.2. Identificação dos requisitos de recursos 31

5.2.3. Identificação das prioridades de recuperação para os recursos de sistema 33

5.3. Identificação de controlos preventivos 35

5.4. Estratégias de contingência 47

5.5. Desenvolvimento dos planos BCP e DRP 50

5.5.1. Plano BCP 51
5.5.2. Plano DRP 53
5.6. Exercícios, testes e simulacros 61
5.6.1. Testes 61
5.6.2. Treino 62
5.6.3. Exercícios 62
5.7. Manutenção dos planos 64
6. Conclusão 65
Referências 67
Anexos i
Anexo 1 – Análise de Riscos i
Anexo 2 – Riscos Residuais v

1. Introdução

No âmbito da unidade curricular de Tratamento de Incidentes de Segurança Informática, do curso de Mestrado Cibersegurança e Informática Forense da Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria, foi redigido o presente relatório de modo a elaborar uma gestão de continuidade de negócios numa clínica médica hipotética.

Segurança da informação tem sido um tópico nas organizações tendo vindo a ganhar mais relevância na atualidade. Desta forma é importante que sejam identificados e justificados quais os ativos mais importantes numa organização que devem ser mais, ou menos, protegidos contra certas ameaças. A análise de risco é uma área da segurança da informação que ajuda nesta atividade de identificação de ativos nas organizações, e também na classificação de riscos, vulnerabilidades e de ameaças tendo em conta as estratégias de negócio e estratégias financeiras da organização. Esta análise ajuda a identificar os possíveis prejuízos numa organização, caso não sejam tomadas medidas para combater os riscos analisados. Outro aspeto importante da segurança da informação envolve a gestão de continuidade de negócios contra acontecimentos/desastres inesperados. Este aspeto procura preparar ou precaver, consoante o plano definido, as organizações contra desastres, ao desenvolver medidas e planos para estas estarem preparadas e cientes no que devem fazer numa situação de desastre. Assim, é possível recuperar e voltar à normalidade o mais rápido possível.

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 uma gestão de continuidade de negócios nesta organização.

Para a realização deste trabalho foram levados em consideração um conjunto de elementos legislativos e normativos nomeadamente a NIST *Special Publication* 800-34 Rev. 1, a ISO/IEC 27001, 27002, a 27005 e 27031, 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.

O presente relatório está dividido em seis capítulos, sendo que o capítulo **Error! Reference source not found.** 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 3 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 4 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.

No capítulo 5 é efetuada a gestão de continuidade de negócios no qual envolve a definição de políticas para esta, realização do *Business Impact Assessement* (BIA), identificar controlos preventivos, definição de estratégias de contingência, o desenvolvimento dos planos BCP e DRP, planeamento dos exercícios de teste e de melhoria, e por fim, a definição do modo de manutenção dos planos anteriormente desenvolvidos.

Por último, no capítulo 6, o relatório termina com a conclusão, em que é feito um balanço geral de todos os aspetos mencionados anteriormente.

2. Caracterização do ambiente hipotético

O cenário hipotético para este projeto diz respeito a uma clínica médica que está inserida num grupo privado. Esta clínica tem a finalidade da prestação de serviços médicos gerais e especializados. A clínica hipotética apresenta uma estrutura empresarial na qual existem vários departamentos, como o departamento administrativo da clínica, que contém o conselho administrativo que mantém a gestão dos departamentos dentro da clínica, nomeadamente: Organismo médico, Recursos Humanos, Gestão e Finanças, Administração Informática e Serviço Informático (Serviço Externo). Como se pode visualizar na Figura 1 - Estrutura empresarial da clínica, as áreas gerais e especializadas da clínica que constitui o organismo médico são a clínica geral, enfermagem, oftalmologia, cardiologia e fisioterapia.

É importante realçar que a clínica em causa não trata de casos urgentes, nem críticos, de modo que, mesmo os pacientes da enfermaria não são pacientes críticos ou urgentes. A clínica também não possuí horário de 24 horas por dia, sendo que abre das 8 horas às 20:00 horas e fecha aos feriados e fim-de-semana.

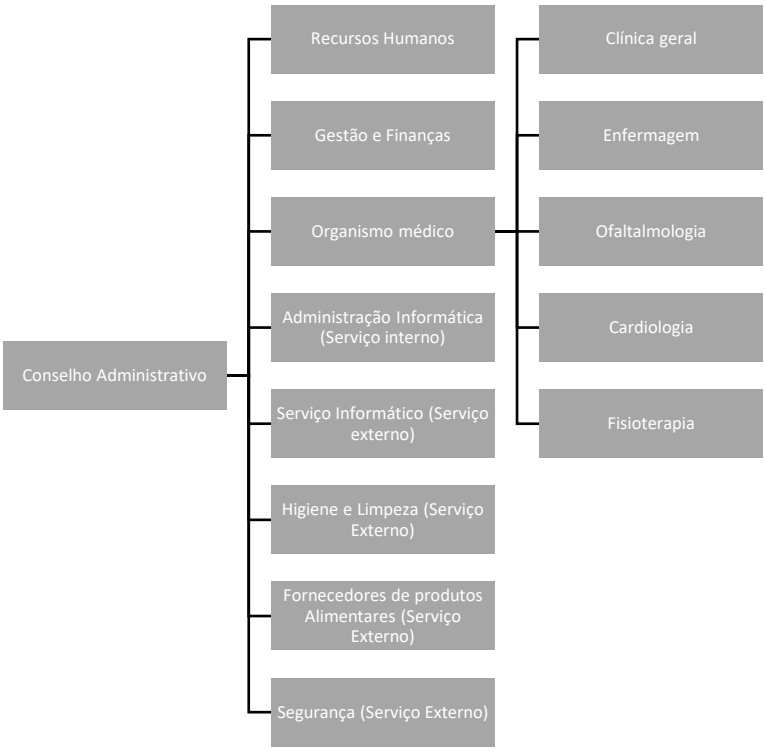

Figura 1 - Estrutura empresarial da clínica

Esta clínica hipotética localiza-se na cidade de Leiria, em Portugal, e atua no ramo de atividade ligado aos serviços médicos. O edifício da clínica é constituído por 4 pisos, em que o acesso entre eles é feito por escadas ou elevadores. O primeiro piso (piso -1) é o local onde reside a administração informática da clínica e é também, onde são armazenados os servidores dedicados que guardam os dados desta 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 se situam as salas 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*

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 clínica, 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.

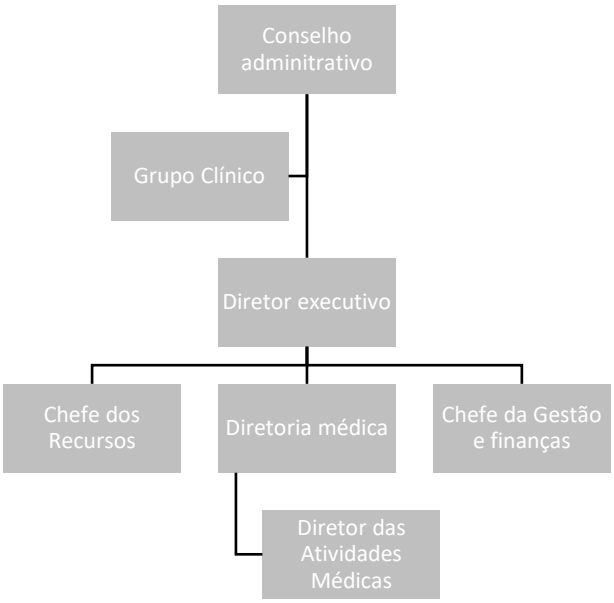

Figura 2 - Estrutura de administração da clínica

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 que todos estes dados são de acesso livre nas clínicas do mesmo grupo clínico. Os fornecedores interagem maioritariamente com o grupo, sendo que apenas alguns interagem com 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 (*software*/aplicações à medida) e a uma empresa para os serviços de higiene e limpeza e de produtos alimentares.

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 da clínica ou até mesmo para dar consultas remotas.

Existe também o sistema de alarme e videovigilância, sendo que as câmaras se encontram no piso -1, no piso 0 na área da receção, no piso 2 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.

A clínica emprega para a administração dos seus sistemas informáticos e da rede informática da clínica 2 administradores. Estes administradores para além das duas funções de administração, eles estão também encarregues na gestão dos processos de *backup* de dados dos servidores da clínica, verificação e testagem dos *backups*.

É de realçar que o serviço de informática externo existe apenas para fornecer manutenção adicional nos *software*/aplicações à medida da clínica.

3. Arquitetura do Sistema de Informação

O negócio da presente clínica hipotética baseia-se na prestação de serviços de saúde. Os serviços de saúde são constituídos pelas áreas de:

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

Nos serviços de prestação de cuidados de saúde, existem vários processos como, o processo de gestão da conta de cliente, o processo de gestão de conta do colaborador, o processo de gestão de consultas, o processo para pagamento de serviços prestados, o processo para as atividades de telemedicina, o processo de gestão dos dados recolhidos nos vários processos, o processo de gestão de eventos, o processo de gestão dos recursos humanos, o processo de gestão dos serviços externos de higiene e de produtos alimentares, o processo da gestão de segurança, o processo relativo a comunicações, o processo relativo a auditorias e o processo de notificações relativas a licenças, atualizações e contratos. Mais ligado à área administrativa, existem os processos de *backup* incremental diário dos dados, de *backup* completo semanal dos dados, testes e validação dos *backups*. Os *backups* totais não têm todos a mesma data, sendo que, para alguns processos, um *backup* total é feito na segunda-feira, para outros processos é na terça-feira, e assim sucessivamente, de forma a que o custo para os fazer seja distribuído durante a semana.

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

- dados pessoais do cliente:
    - nome;
    - idade;
    - morada;
    - número de telefone;

    - credenciais de saúde;
    - histórico médico:
        - consultas;
        - exames médicos.
- dados dos funcionários;
- dados da clínica;
- dados das consultas:
    - paciente;
    - médico;
    - tipo de consulta;
    - data;
    - resultados médicos.

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

- dados pessoais dos clientes;
- dados dos funcionários;
- dados médicos;
- 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 pessoais dos clientes referentes às consultas pelo grupo clínico de forma a outras clínicas do mesmo grupo poderem obter melhor informação dos clientes e, caso estes utilizem os serviços das outras clínicas.

A clínica utiliza duas aplicações/*software* à medida, uma para gerir os negócios 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 usa também aplicações/*software* generalistas, nomeadamente:

- o SIEM *Wazuh* para motorizar a atividade de *logs* nos vários *hardwares*, como os computadores físicos da clínica e *software*, como as *firewalls* na rede da clínica;
- o *Primavera* da *Primavera BSS* para gerir toda a parte de gestão e faturação da clínica.

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 das consultas e exames dos pacientes serão partilhados com outras clínicas pertencentes ao mesmo grupo clínico. 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. Os dados financeiros estão apenas acessíveis tanto ao diretor executivo e restantes cargos superiores como também pela gestão dos recursos humanos e 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. O servidor da clínica é utilizado não só para alojar a aplicação *web* para os clientes e o servidor do SIEM *Wazuh*, mas também para armazenar as bases de dados de cada aplicação que são os dados mais importantes da clínica. 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 o servidor está presente 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.

4. 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 2 e 3.

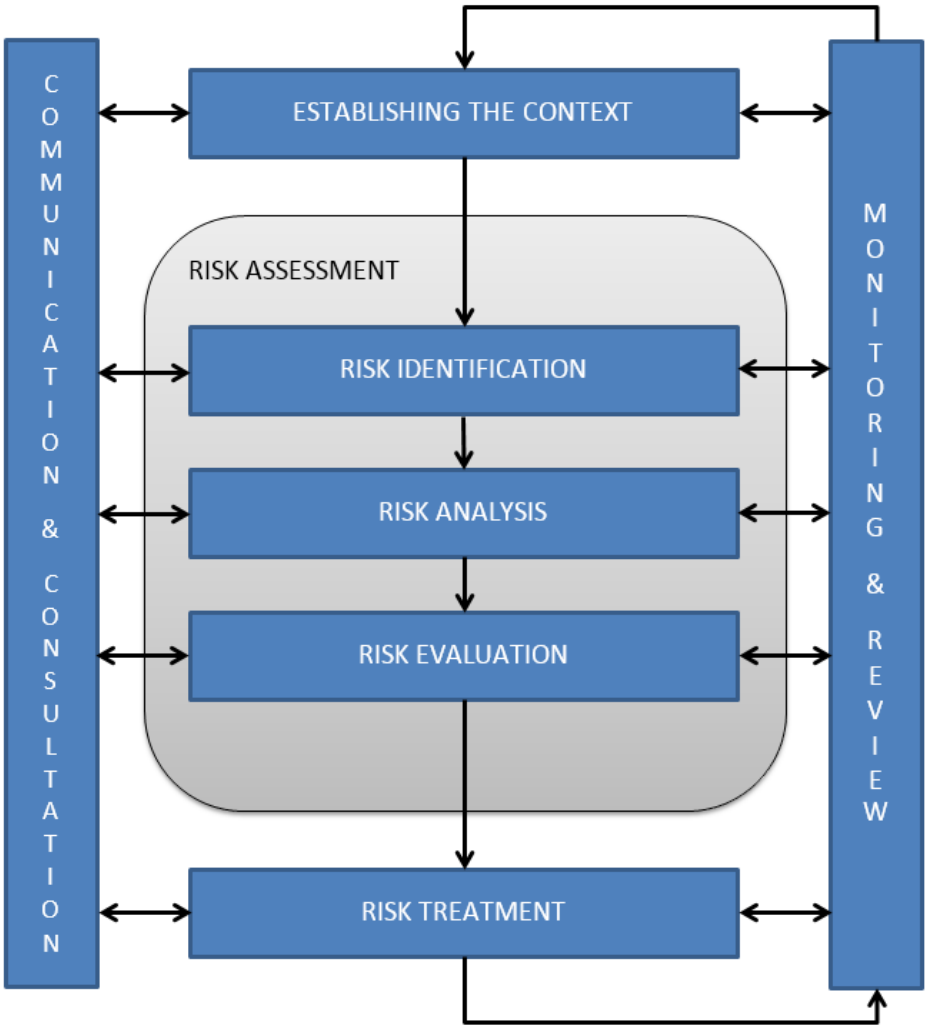

Figura 3 - Processo de análise do risco [1]

4.1 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, o SIEM e o *software Primavera*;

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

4.2 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:

- 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:

- Roubo de informação;
- 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*;
- Coimas por incumprimento de legislação e regulamentos.

4.3 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 de equipamentos periódica;
- 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;
- Má alocação dos direitos de acesso;
- Fraca gestão de *password*;
- *Software* à medida novo e imaturo.

Vulnerabilidades de rede:

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

Vulnerabilidades relacionadas a pessoal interno:

- Ausência de pessoal;
- Treino de segurança inadequados;

- Uso incorreto de *software* e *hardware*;
- Falta de consciência em relação à segurança;
- Trabalho não supervisionado por empresas de terceiros.

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 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 nº 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 informáticos como por exemplo, ataques do tipo *Denial of Service*, ataques *zero-day*, *eavesdropping*, entre outros.

4.4 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 no Anexo 1 – Análise de Riscos.

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.

Relativamente à ameaça dos *malwares*, esta pode ocorrer por diversas fontes como, por exemplo, falta de sensibilidade na equipa para conceitos de segurança informática o que pode levar à exposição da clínica a ataques com sucesso, sendo um exemplo o ataque de *phishing* direcionado a um dado membro da equipa. Para além dos ataques de *phishing*, os membros da equipa também poderão navegar em sítios pouco seguros e até mesmo instalar *software* ilegítimo podendo levar ao comprometimento de ativos da empresa como, por exemplo, impressoras, computadores físicos, portátil, os próprios programas utilizados pela clínica, entre outros. Outra fonte desta ameaça serão pessoas com intenções maliciosas tentarem aceder ao sistema fazendo, para isso, utilização de *malware*. A falta de sensibilidade na equipa para conceitos de segurança informática poderá levar ao comprometimento de ativos com um grau de probabilidade de ocorrência superior do que pessoas com intenções maliciosas tentarem aceder ao sistema. Dado que os ataques maliciosos acabam por ser mais elaborados, e, como a clínica tem *software* à medida e utiliza o sistema operativo *Windows 10 Enterprise* que, por sua vez, sofre atualizações regularmente, acaba por ser uma tarefa mais complicada.

A ameaça de erro no uso pode ter como fonte a má utilização do *software* por parte das pessoas que o utilizam devido à falta de conhecimento e formação relativa ao mesmo. Com esta ameaça pode ocorrer comprometimento do sistema, por exemplo, os sistemas e *firmwares* de impressoras e de computadores bem como o comprometimento da informação, nomeadamente os dados privados que a empresa possui.

Já a ameaça de falhas técnicas de *software* pode ocorrer por *bugs* e qualquer outro tipo de falha nos *software* feitos à medida devido à falta de testes a que os mesmos foram submetidos. Relativamente a falhas técnicas no próprio sistema operativo utilizado na

clínica ou até mesmo o *software Primavera*, a probabilidade da ocorrência de falhas técnicas nestes é baixa. Isto devido ao facto de sofrerem atualizações periódicas e, até mesmo, o facto de serem submetidos a uma fase de testes mais rigorosa pela entidade que os fornece.

A ameaça de comprometimento de informação pode ter vários tipos de fontes e o seu impacto pode depender da informação que for comprometida. Por exemplo, esta ameaça pode ter origem de ataques realizados por pessoas com intenções maliciosas que acabam por obter informação, seja através de *malware* ou até mesmo de outras técnicas de ataque. No entanto, pelas razões já mencionadas aquando a referência à ameaça de *malware*, a probabilidade da ocorrência é baixa. Já no que diz respeito à falta de sensibilidade para conceitos de segurança por parte dos utilizadores, esta tem uma probabilidade de ocorrência muito mais elevada sendo que, inconscientemente os utilizadores podem acabar mesmo por comprometer informação da clínica, nomeadamente, os dados privados desta. Podem existir incidentes – como por exemplo, desastres naturais - que levem à destruição de equipamento que poderão levar à perda de dados privados da clínica e até mesmo documentos. Também poderão ocorrer incidentes de segurança que sejam do conhecimento do público sem o prévio conhecimento da clínica, o que poderá levar ao comprometimento da informação. No entanto, a probabilidade de tal ocorrer é baixa. É também importante ter consideração o facto da possibilidade de ocorrer comprometimento da informação no grupo e não na clínica, ter um impacto elevado na clínica, sendo que a probabilidade de ocorrer comprometimento da informação no grupo e não na clínica é mais elevado.

No que diz respeito à ameaça de abusos de direitos, os direitos podem estar mal distribuídos para os vários perfis criados tendo em consideração os cargos ocupados pelo funcionário em causa. Uma outra fonte pode ser pessoas mal-intencionadas que abusem dos direitos que possuem. Ambas as fontes mencionadas anteriormente levam ao comprometimento tanto de informação privada e de documentos como também de sistemas como, por exemplo, computadores. O abuso de direitos também pode ter impacto na credibilidade na clínica, apesar de esta ameaça apresentar uma probabilidade de ocorrência baixa.

A ameaça de ações não autorizadas está relacionada com, por exemplo, o facto de um funcionário ser despedido e no seu contrato estar definido que a partir desse momento

perde os direitos que têm na clínica. No entanto, perante o sistema ainda consegue realizar ações, que nesta situação, serão não autorizadas. Assim, este ex-funcionário poderá acabar por comprometer informação, entre outros, prejudicando os ativos da clínica, mas o impacto real que irá existir dependerá das intenções do ex-funcionário em causa. Uma outra fonte possível relativa a esta ameaça passa por problemas de *software* que possam levar a que um utilizador tenha mais direitos no sistema do que o devido. Mais uma vez, a falta de sensibilidade para conceitos de segurança por parte dos funcionários poderá ser uma outra fonte tendo como exemplo um utilizador deixar o seu posto de trabalho com a sessão iniciada no dispositivo e alguém aceder à mesma.

Já a ameaça de falta de disponibilidade para o trabalho encontra-se relacionada com a probabilidade de ocorrência de greves, ou até mesmo de epidemias ou de outros problemas que impeçam os funcionários de se apresentarem no seu posto de trabalho. É de referir que, de entre outras as fontes mencionadas, a probabilidade de ocorrência de greves acaba por apresentar uma probabilidade mais elevada de ocorrer.

A ameaça relativa a *hackers* ou *crackers* está relacionada com pessoas mal-intencionadas que realizem um ataque. É de ter em atenção que as intenções de um *hacker* e de um *craker* são distintas, logo, as consequências do ataque realizado também poderão ser diferentes. A ocorrência desta ameaça poderá levar também ao comprometimento tanto de informação privada e de documentos como também de sistemas como, por exemplo, computadores. Pode ainda ser comprometido o normal funcionamento da clínica.

Relativamente à ameaça de falhas técnicas de *hardware*, uma fonte para esta ameaça é o facto de algum do *hardware* deixar de funcionar corretamente levando ao mau funcionamento do(s) equipamento(s) em causa. Tal ameaça poderá levar ao comprometimento da prestação de serviços por parte da empresa e ainda o comprometimento parcial dos dados da clínica.

A ameaça de coimas por incumprimento de legislação e regulamentos tem como fonte o facto de a clínica não estar em conformidade com o que a Lei nº46/2018 e o RGPD que lhes exigem. Caso esta ameaça se concretize, se o ocorrido for comunicado aos *media*, esta poderá levar à perda de credibilidade da empresa.

A ocorrência da ameaça de perda de serviços essenciais pode ter várias fontes dependendo do serviço essencial em causa. Assim, possíveis fontes para esta ameaça são

o corte energético, corte de água ou até mesmo a perda de acesso à Internet, sendo que estas fontes podem ter como causa, por exemplo, um desastre natural ou um incidente não intencional. É de referir que, tendo em conta a localização da clínica, há uma maior probabilidade da ocorrência de um incidente não intencional do que de um desastre natural.

Já a ameaça de distúrbio devido à radiação está relacionada com o equipamento que a clínica necessita, equipamento esse que emite algum tipo de radiação. As fontes desta ameaça poderão ser alguma falha técnica no equipamento ou até mesmo um erro na atualização do *firmware* do equipamento. É de ter em conta que a probabilidade da ocorrência de uma falha técnica no equipamento é superior à de um erro na atualização do *firmware* do equipamento.

Por fim, no que diz respeito às ameaças físicas e/ou naturais, esta está relacionada, por exemplo, com a ocorrência de desastres naturais. Também pode ter como fonte um incidente não intencional ou um incidente intencional como a danificação de um equipamento da clínica por parte de um funcionário ou cliente. A probabilidade da ocorrência de um incidente não intencional é superior à de um incidente intencional ou até mesmo de um desastre natural.

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. Um exemplo deste risco é o comprometimento da informação porque, como a clínica se insere no grupo e também detém informação do mesmo, a ocorrência deste risco poderá afetar a clínica em específico e o grupo.

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.

4.5 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 da falta na disponibilidade de pessoal para o trabalho. 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, 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. Gestão de continuidade de negócios

O plano BCP (*Business continuity planing*) foca-se em sustentar as operações e proteger a viabilidade do negócio desde a identificação de um desastre até ao normal funcionamento do negócio. Assim, este plano pode ser um plano de longo termo. Neste plano também consta o plano DRP (*disaster recovery plan*) que tem como principal objetivo minimizar os efeitos de um desastre e de dar os passos necessários para assegurar que os recursos, pessoal e processos de negócio conseguem retomar as operações dentro de um tempo definido. Este é um plano de curto termo. De forma geral, o BCP pode ser visto como "Aconteceu um desastre. Como se pode continuar o negócio até alguém pôr tudo de volta à normalidade?", enquanto o DRP pode ser visto como "Aconteceu um desastre. Como se pode minimizar o seu efeito? E como repor o funcionamento normal?".

Os planos de contingência são constituídos por atividades abrangentes com o objetivo de sustentar e recuperar os serviços de sistemas críticos após um evento de emergência. Este tipo de planeamento enquadra-se num esforço mais abrangente, no esforço da segurança e na gestão da emergência que incluí o BCP, o DRP e a gestão de incidentes. [2]

5.1. Políticas de continuidade de negócio

Na organização existe um plano de contingência para cada sistema de informação, plano esse que será acionado na ocorrência de um incidente que tenha impacto ao nível do funcionamento destes. É da responsabilidade do coordenador do BCP no grupo e do coordenador da área de segurança da clínica, tanto a elaboração do BCP e do DRP da clínica, bem como a devida atualização destes de 18 em 18 meses. É também da responsabilidade destes dois coordenadores mencionados, a documentação de todos os planos.

Só o coordenador da área de segurança da clínica pode declarar estado de desastre, contudo, no caso da ausência deste coordenador, a declaração poderá ser efetuada ou pelo diretor da clínica ou por um membro da direção da clínica ou até mesmo pelo coordenador dos planos no grupo. Qualquer pessoa dentro da clínica pode ativar o estado de

emergência, contudo, a ativação deste não leva à declaração de desastre dado que essa declaração só poderá ser efetuada pelas pessoas descritas acima.

Como a organização em questão insere-se na área da saúde, e, por conseguinte, como esta trata de uma elevada quantidade de dados privados de extrema importância, a clínica tem de garantir a devida proteção, confidencialidade, integridade e disponibilidade dos seus dados, mesmo no caso da ocorrência de eventos disruptivos. Também no caso de ocorrerem eventos disruptivos, a organização terá de proteger todos os seus ativos e as pessoas relacionadas de alguma forma com a clínica (sejam pacientes ou colaboradores da clínica). Em caso de ocorrência de eventos adversos que causem algum tipo de disrupção nos sistemas, deve ser priorizado o retorno dos sistemas mais críticos da clínica, de forma a que os mesmos possam voltar ao seu normal funcionamento, de acordo com o seu nível de criticidade. Todos os procedimentos necessários e descritos nos planos devem ser devidamente testados e atualizados quando necessário. Todos os colaboradores têm a obrigação de seguir os planos e as ordens dadas pela equipa que está a executar os planos de contingência. Está ao encargo do grupo assegurar os recursos necessários para garantir a viabilidade de todos os procedimentos abrangidos pelos planos.

Em relação às equipas que executam os planos, parte do pessoal provêm do grupo, sendo que os mesmos têm os conhecimentos e treinos necessários para dar resposta a disrupções nos serviços dos quais os mesmos sofreram treino. Assim, um conjunto do pessoal tem como foco dar resposta a disrupções relacionadas com o servidor, enquanto outro tem foco a dar resposta a disrupções relacionadas com as comunicações da clínica. A área em que os membros da equipa vão trabalhar, está assim, diretamente relacionada para o foco do seu treino e preparação. As equipas também possuem membros da própria clínica, membros esses que executam funções semelhantes àquilo que irá ser feito pela equipa para recuperar o sistema. Apesar das funções que eles normalmente fazem estarem relacionadas com o que terão de fazer para recuperar o sistema, ainda recebem treino para a recuperação efetiva do próprio sistema. Para os vários tipos de disrupções existem equipas especificas, responsáveis por implementar os planos de contingência. As equipas são a de gestão (onde o coordenador dos planos se encontra integrado), de disrupção de serviços essenciais, de tecnologias e sistemas de informação (recuperação do servidor, da base de dados, da rede e de sistemas operativos), de aplicações, de comunicações e, por último, de relações públicas e situações legais. Nestas equipas existe o líder que tem o poder para tomar decisões.

Devem ser executados *backups* cifrados com diferentes níveis de frequência, dependendo da criticidade e impacto que os dados desses *backups* têm para o negócio. Os *backups* devem ser transportados para as instalações fora da clínica (instalações essas preparadas para receber e dar suporte a *hardware* e a alguns serviços informáticos da clínica), segundo um agendamento pré-definido.

Se devido a qualquer problema e/ou disrupção de serviços, e sempre que existir atrasos ou interrupções temporárias nas prestações dos serviços, os colaboradores devem ser educados e cordiais com os pacientes, pedindo a sua compreensão. Se for necessário fechar as instalações e enviar os clientes para outras clínicas, os colaboradores devem ser compreensivos e auxiliar tanto quanto possível, de modo a garantir que os pacientes terão continuidade nos seus cuidados de saúde noutra clínica.

5.2. Business Impact Assessement

O processo de BIA tem como objetivo, a identificação e priorização de componentes de um sistema, através da sua correlação com os processos de negócio que os sistemas de informação suportam. Deve-se utilizar esta informação para caraterizar o impacto dos processos caso o sistema se verifique indisponível. Este processo é composto por três fases distintas:

1. **Determinação dos processos de negócio e da criticidade da recuperação**.
2. **Identificação dos requisitos de recursos**;
3. **Identificação das prioridades de recuperação para os recursos de sistema**.

É de ter em consideração, que sendo um cenário hipotético, é possível que falte alguns processos necessários ao negócio da clínica. Também em relação às categorias de impacto, só foram consideradas categorias qualitativas, mas num cenário real seria necessário e extremamente importante definir medidas quantitativas.

5.2.1. Determinação dos processos de negócio e da criticidade da recuperação

O primeiro passo para realizar o BIA passa pela enumeração dos processos de negócio da clínica, identificação dos níveis de impacto nesses processos, e na determinação dos tempos que os processos podem estar indisponíveis.

Os processos existentes no sistema de informação desta clínica hipotética foram definidos no capítulo 3, mas, é possível visualizar a sua listagem na Tabela 2.

Tabela 2 - Lista de processos do sistema de informação

Processo	Descrição
Gestão de conta de cliente	Processo executado aquando um novo cliente/paciente pretende usufruir de algum serviço associado à clínica, ou, sempre que haja alterações nas informações que constem na conta de um cliente, ou ainda, sempre que for necessário a eliminação da conta do mesmo.
Gestão de consultas	Processo executado aquando uma nova marcação de consulta, ou, sempre que haja alterações nas consultas já marcadas, ou ainda, quando existe eliminação de uma consulta previamente marcada.
Pagamento de serviços prestados	Processo de pagamento por parte dos clientes a serviços prestados pela clínica, como por exemplo, consultas.
Atividades de telemedicina	Processo associado à prestação de serviços de saúde à distância, como por exemplo, a realização de consultas de clínica geral.
Gestão de dados recolhidos	Processo que consiste na realização de toda a gestão inerente aos dados recolhidos pelos vários processos. Este processo é responsável pelo armazenamento dos dados, pela disponibilização dos dados e/ou alteração dos mesmos de acordo com o que é solicitado, pela normalização dos dados e pela eliminação efetiva dos dados.
Gestão de *backups*	Processo relativo à criação periódica de *backups*. Também é o responsável pela eliminação dos *backups*, quando solicitado, tendo em conta as restrições legais relacionadas com a preservação dos dados.

Processo	Descrição
Gestão de conta do colaborador	Processo executado aquando um novo colaborador é contratado pela clínica, ou, sempre que haja alterações nas informações que constem na conta do mesmo, ou ainda, sempre que for necessário a eliminação da conta desse colaborador devido, por exemplo, ao despedimento do mesmo. Esta conta está associada a perfis e privilégios do colaborador de acordo com o cargo exercido.
Gestão de recursos humanos	O processo responsável por toda a gestão dos recursos humanos, desde a procura de candidatos (por exemplo, os concursos de seleção) e sua contratação até à renovação dos contratos e/ou despedimentos dos colaboradores. Também é responsável pela gestão dos estagiários enviados pelo grupo.
Gestão de serviços externos de higiene e limpeza e de fornecedores de produtos alimentares	Processo relativo a serviços externos, sendo esses relativos aos serviços de fornecedores de produtos alimentares e de higiene e limpeza.
Comunicações	Processo responsável pela comunicação e gestão da relação para com os fabricantes de SI. A manutenção e notificação de erros relativos aos *software* são alguns exemplos relativos a este processo. O processo também é relativo ao grupo, nomeadamente, aos pedidos e respostas a solicitações entre a clínica e o grupo, bem como a gestão dos serviços externos que estão à responsabilidade do grupo como os serviços farmacêuticos, os seguros e a ótica. As comunicações podem ser via *e-mail* ou telefone e podem servir para outros contactos necessários ao negócio, como por exemplo, as comunicações dentro da clínica.

Processo	Descrição
Gestão da segurança	Processo relativo aos serviços de segurança implementados na clínica. Serviços como as câmaras fazem parte deste processo.
Notificações relativas a licenças, atualizações e contratos	Processo responsável pelo aviso aquando a aproximação do período de finalização de licenças e contratos, bem como pelo aviso de novas atualizações disponíveis para *software* utilizado pela clínica. Também permite gerir os avisos.
Gestão de eventos	Processo relativo ao SIEM, em que existe recolha de *logs*, análise, e visualização dos dados. Permite detetar incidentes de segurança
Auditoria	Processo relativo a auditorias feitas por parte do administrador do sistema e por pessoal exterior à clínica

Com os processos listados, é necessário analisar o impacto das falhas de disponibilidade destes processos. Para tal, foram classificadas para cada um dos processos o seu impacto, na Tabela 3, consoante as seguintes categorias de impacto definidas em baixo.

Categoria de Impacto: **Reputação**

Valores de impacto da categoria:

- Severo = Existe perda de reputação para a clínica e para grupo
- Moderado = Existe perda de reputação para a clínica
- Mínimo = Não existe perda de reputação

Categoria de Impacto: **Cuidados aos pacientes**

Valores de impacto da categoria:

- Severo = Põe em perigo a vida ou saúde do paciente

- Moderado = Interferência nos cuidados normais de saúde do paciente
- Mínimo = Não interfere nos cuidados de saúde do cliente

Categoria de Impacto: **Qualidade na prestação de serviços**

Valores de impacto da categoria:

- Severo = Impossibilidade de prestação de serviços
- Moderado = Interferência na eficácia da prestação de serviços
- Mínimo = Não existe interferência na eficácia da prestação de serviços

Tabela 3 - Classificação de impactos nos processos

Processo	**Categoria de Impacto**			
	Reputação	**Cuidados aos pacientes**	**Qualidade na prestação de serviços**	**Impacto**
Gestão de conta de cliente	Moderado	Severo	Moderado	Moderado
Gestão de consultas	Moderado	Severo	Moderado	Moderado
Pagamento de serviços prestados	Mínimo	Mínimo	Moderado	Mínimo
Atividades de telemedicina	Mínimo	Moderado	Moderado	Mínimo
Gestão de dados recolhidos	Severo	Severo	Severo	Severo
Gestão de *backups*	Severo	Mínimo	Mínimo	Moderado
Gestão de conta do colaborador	Mínimo	Mínimo	Moderado	Mínimo
Gestão de recursos humanos	Moderado	Mínimo	Mínimo	Mínimo
Gestão de serviços externos de higiene e limpeza e de fornecedores de produtos alimentares	Severo	Severo	Moderado	Severo
Comunicações	Severo	Moderado	Moderado	Moderado
Gestão da segurança	Moderado	Mínimo	Mínimo	Moderado

Processo	Categoria de Impacto			
	Reputação	**Cuidados aos pacientes**	**Qualidade na prestação de serviços**	**Impacto**
Notificações relativas a licenças, atualizações e contratos	Mínimo	Mínimo	Mínimo	Mínimo
Gestão de eventos	Severo	Moderado	Moderado	Severo
Auditoria	Moderado	Mínimo	Mínimo	Moderado

Por fim, como última análise a realizar na fase de determinação dos processos de negócio e da criticidade das suas recuperações, deve ser determinado para cada processo a estimativa dos tempos de inatividade. Na Tabela 4, serão determinados os tempos de:

- ***Recovery Point Objective*** **(RPO)** indica a perda máxima de dados que uma organização está disposta a perder depois de um desastre.
- ***Recovery Time Objective*** **(RTO)** indica a duração necessária para voltar a repor os sistemas críticos *online*.
- ***Work Recovery Time*** **(WRT)** indica a duração necessária para recuperar os dados perdidos (baseado no RPO) e para introduzir os dados gerados manualmente.
- ***Maximum Tolerable Downtime*** **(MTD)** representa o tempo total que os líderes da organização estão dispostos a aceitar no caso de uma disrupção de um processo de negócio. Este é baseado nos tempos de RTO mais WRT.

Tabela 4 - Estimativa dos tempos de inatividade

Processo	RPO	RTO	WRT	MTD
Gestão de conta de cliente	0 horas	8 horas	10 horas	18 horas
Gestão de consultas	12 horas	8 horas	12 horas	20 horas
Pagamento de serviços prestados	24 horas	20 horas	36 horas	56 horas

Processo	RPO	RTO	WRT	MTD
Atividades de telemedicina	48 horas	72 horas	24 horas	96 horas
Gestão de dados recolhidos	-	5 horas	8 horas	13 horas
Gestão de *backups*	-	12 horas	16 horas	28 horas
Gestão de conta do colaborador	18 horas	18 horas	12 horas	30 horas
Gestão de recursos humanos	24 horas	20 horas	14 horas	34 horas
Gestão de serviços externos de higiene e limpeza e de fornecedores de produtos alimentares	12 horas	6 horas	6 horas	12 horas
Comunicações	-	6 horas	12 horas	18 horas
Gestão da segurança	12 horas	8 horas	12 horas	20 horas
Notificações relativas a licenças, atualizações e contratos	48 horas	36 horas	72 horas	108 horas
Gestão de eventos	6 horas	8 horas	8 horas	16 horas
Auditoria	24 horas	12 horas	14 horas	26 horas

5.2.2. Identificação dos requisitos de recursos

A identificação dos requisitos dos recursos é importante para efetuar a sua avaliação, de forma a obter os esforços realísticos para a recuperação e o resumo dos processos de negócio o mais rápido possível. Estes recursos podem ser qualquer componente no sistema de informação da clínica, como *hardware*, *software* ou mesmo ficheiros de dados importantes. Para iniciar esta segunda etapa do BIA, devem ser identificados todos os recursos essenciais para suportar os processos de negócio anteriormente definidos e para o funcionamento da clínica (ver Tabela 5).

Tabela 5 - Componentes/Recursos do sistema da clínica

Componentes/Recursos do Sistema	**Plataforma/SO/Versão (se aplicável)**	**Descrição**
Servidor	*Threadripper* 2990WX, 128GB RAM/CentOS/7	Componente de *hardware* responsável pelo alojamento das aplicações à medida da clínica e das bases de dados.
Network-attached storage (NAS)	HPE MSA 2040 ES SAN DC SFF *Storage*, 48TB	Componente física responsável pelo armazenamento dos dados da clínica.
Routers	Cisco SF350-48MP 48-port 10/100 *POE Managed Switch*	Componente física responsável pela rede tanto dos clientes como dos colaboradores da clínica.
Desktops	Computador Acer Aspire AXC-885 i5-8400 8GB/*Windows 10 Enterprise*	Componente física utlizada pelos colaboradores da clínica para usufruírem das aplicações à medida. Alguns também possuem a aplicação *Primavera*, nomeadamente, os *desktops* de gestão.
Aplicação à medida (Cliente)	Máquina virtual 1 CentOS 7	Aplicação *web* destinada para a interação dos clientes com a clínica.
Aplicação à medida (Clínica)	Máquina virtual 2 CentOS 7	Aplicação destinada para a interação dos colaboradores com a clínica.

Primavera	Não aplicável	Aplicação responsável pela gestão de contabilidade e de recursos humanos.
Telefones	Não aplicável	Componente utilizado para possíveis comunicações do pessoal da clínica para pessoas da própria clínica ou externas.
Serviço *Outlook*	*Exchange*	Componente utilizado para possíveis comunicações do pessoal da clínica para pessoas da própria clínica ou externas.

5.2.3. Identificação das prioridades de recuperação para os recursos de sistema

A terceira e última etapa do BIA, é baseada nos resultados das análises anteriores dos processos e recursos de negócio e sistema. Aqui são usados os recursos identificados para serem interligados com os processos de negócio do sistema. Desta forma, os níveis de prioridade poderão ser estabelecidos para organizar a ordem de recuperação das atividade e recursos. A Tabela 6 lista a ordem de recuperação dos recursos do sistema da clínica. Esta tabela também define um tempo expectado (RTO) para a recuperação dos recursos depois de uma grave disrupção (no qual seja necessário efetuar a reconstrução/reparação completa ou troca do recurso).

Tabela 6 - Identificação de prioridade dos recursos

Prioridade	**Componente/Recurso de Sistema**	**Recovery Time Objective**
Servidor	*Threadripper* 2990WX, 128GB RAM/CentOS/7	8 horas para reparar ou trocar

Prioridade	**Componente/Recurso de Sistema**	**Recovery Time Objective**
Network-attached storage (NAS)	HPE MSA 2040 ES SAN DC SFF *Storage*, 48TB	8 horas para reparar ou trocar
Routers	Cisco SF350-48MP 48-port 10/100 *POE Managed Switch*	6 horas para reparar ou trocar
Desktops	Computador Acer Aspire AXC-885 i5-8400 8GB/*Windows 10 Enterprise*	24 horas para reparar ou trocar
Aplicação à medida (Cliente)	Máquina virtual 1 CentOS 7	12 horas para reparar / comunicar aos fabricantes de SI
Aplicação à medida (Clínica)	Máquina virtual 2 CentOS 7	18 horas para reparar / comunicar aos fabricantes de SI
Primavera	Não aplicável	18 horas para reparar / comunicar à entidade responsável pelo serviço
Telefones	Não aplicável	6 horas para reparar ou trocar
Outlook	*Exchange*	10 horas para reparar / comunicar à *Microsoft*

5.3. Identificação de controlos preventivos

Todos os 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.

É de ter em consideração que algumas medidas poderão influenciar outras ameaças de forma direta ou indireta, ajudando na sua mitigação.

Ameaça: *Malware*.

Processos: Gestão de conta de cliente, gestão de consultas, pagamento de serviços prestados, atividades de telemedicina, gestão de dados recolhidos, gestão de conta do colaborador e gestão de recursos humanos.

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 pública 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.

Processos: Gestão de conta de cliente, gestão de consultas, pagamento de serviços prestados, atividades de telemedicina, gestão de dados recolhidos, gestão de *backups*, gestão de conta do colaborador, gestão de recursos humanos, comunicações, gestão da segurança, notificações relativas a licenças, atualizações e contratos, gestão de eventos e auditoria.

Medidas de controlo:

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

Irá ser disponibilizada formação na utilização dos *software* utilizados 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*.

Processos: Gestão de conta de cliente, gestão de consultas, pagamento de serviços prestados, atividades de telemedicina, gestão de dados recolhidos, gestão de conta do colaborador e gestão de recursos humanos.

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.

Processos: Gestão de conta de cliente, gestão de consultas, pagamento de serviços prestados, atividades de telemedicina, gestão de dados recolhidos, gestão de *backups*, gestão de conta do colaborador e gestão de recursos humanos.

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.

- ***Backup* de informação**

Já existem procedimentos de *backup* implementados na clínica, contudo, os *backups* diários não respondem de forma eficiente para cada prioridade dos processos de negócio. Os *backups* são armazenados em discos magnéticos e são efetuados automaticamente segundo um agendamento previamente definido. É de ter em conta que para os processos cujo RPO não é aplicável não possuem *backups*. Desta forma, serão definidos períodos diferentes de *backup* de informação incremental para cada processo:

  - Gestão de conta de cliente: 4 horas
  - Gestão de consultas: 12 horas
  - Pagamento de serviços prestados: 20 horas
  - Atividades de telemedicina: 24 horas
  - Gestão de conta do colaborador: 18 horas
  - Gestão de recursos humanos: 20 horas
  - Gestão de serviços externos de higiene e de produtos alimentares: 12 horas
  - Gestão da segurança: 12 horas
  - Notificações relativas a licenças, atualizações e contratos: 24 horas
  - Gestão de eventos: 6 horas
  - Auditoria: 24 horas

Ameaça: Abuso de direitos.

Processos: Gestão de conta de cliente, gestão de consultas, pagamento de serviços prestados, atividades de telemedicina, gestão de dados recolhidos, gestão de *backups*, gestão de conta do colaborador, gestão de recursos humanos, gestão da segurança, gestão de eventos e auditoria.

Medidas de controlo:

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

O departamento médico está responsável pelos dados e informação derivados das suas atividades.

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.

Processos: Gestão de conta de cliente, gestão de consultas, pagamento de serviços prestados, atividades de telemedicina, gestão de dados recolhidos, gestão de *backups*, gestão de conta do colaborador, gestão de recursos humanos, comunicações, gestão da segurança, gestão de eventos e auditoria.

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, identificado 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 têm acesso ao piso 2; apenas os serviços de administração informática 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: *Hacker* ou *crackers*.

Processos: Gestão de conta de cliente, gestão de consultas, pagamento de serviços prestados, atividades de telemedicina, gestão de dados recolhidos, gestão de *backups*, gestão de conta do colaborador, gestão de recursos humanos, comunicações, gestão da segurança, notificações relativas a licenças, atualizações e contratos, gestão de eventos e auditoria.

Medidas de controlo:

- **Contacto com autoridades competentes**

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

- Autoridade jurídica;
- CNCS;
- Grupo Clínico;
- CNPD.

Ameaça: Falhas técnicas *hardware*.

Processos: Gestão de conta de cliente, gestão de consultas, pagamento de serviços prestados, atividades de telemedicina, gestão de dados recolhidos, gestão de *backups*, gestão de conta do colaborador, gestão de serviços externos de higiene e limpeza e de fornecedores de produtos alimentares, gestão de recursos humanos, comunicações, gestão da segurança, notificações relativas a licenças, atualizações e contratos, gestão de eventos e auditoria.

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. Os serviços externos fazem manutenção do seu próprio equipamento.

Existe, numas instalações externas à clínica, algum *hardware* que poderá ser utilizado no caso de ser necessário trocar *hardware* estragado. Existe também documentação relativa ao *hardware* disponível para troca.

- **Espelhamento e *Striping***

Será implementado o RAID 10 no servidor principal. Este RAID irá ajudar a que não se percam dados, em caso de destruição de discos, devido ao espelhamento. Para além

disso, o *striping* permitirá uma escrita mais rápida, de forma a que exista uma maior eficácia nos processos.

Ameaça: Coimas por incumprimento de legislação e regulamentos.

Processos: Gestão de conta de cliente, gestão de consultas, pagamento de serviços prestados, atividades de telemedicina, gestão de dados recolhidos, gestão de *backups*, gestão de conta do colaborador, gestão de recursos humanos, gestão de serviços externos de higiene e limpeza e de fornecedores de produtos alimentares, gestão da segurança, notificações relativas a licenças, atualizações e contratos, gestão de eventos e auditoria.

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 encarregado da proteção dos dados, 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.

Processos: Gestão de conta de cliente, gestão de consultas, pagamento de serviços prestados, atividades de telemedicina, gestão de dados recolhidos, gestão de *backups*, gestão de conta do colaborador, gestão de recursos humanos, gestão de serviços externos de higiene e limpeza e de fornecedores de produtos alimentares, comunicações, gestão da segurança, notificações relativas a licenças, atualizações e contratos, gestão de eventos e auditoria.

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 e uma segunda fonte de energia suplementar.

- **Serviço suporte alternativo**

Existe um servidor secundário, nas instalações fora da clínica, para a eventualidade de o servidor primário deixar de conseguir dar a resposta necessária ao negócio. Assim, este servidor secundário previne que a maioria dos serviços digitais da clínica parem completamente de forma a que não seja possível continuar o negócio.

Ameaça: Ameaças físicas e/ou naturais.

Processos: Gestão de conta de cliente, gestão de consultas, pagamento de serviços prestados, atividades de telemedicina, gestão de dados recolhidos, gestão de *backups*, gestão de conta do colaborador, gestão de recursos humanos, gestão de serviços externos de higiene e limpeza e de fornecedores de produtos alimentares, comunicações, gestão da segurança, notificações relativas a licenças, atualizações e contratos, gestão de eventos e auditoria.

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.

Após a implementação dos controlos, voltou-se à análise de riscos para perceber até que ponto os riscos eram mitigados. Assim, foi efetuado o cálculo do risco residual para cada ameaça, Anexo 2 – Riscos Residuais. Após a análise detetou-se que os controlos implementados para o caso das coimas por incumprimento de legislação e regulamentos eram os suficientes, de forma que não será necessário criar o plano BCP para este caso.

5.4. Estratégias de contingência

***Malwares*, erro no uso, falhas técnicas de *software*, comprometimento da informação, abuso de direitos, ações não autorizadas, *hackers* ou *crackers*, falhas técnicas de *hardware* e ameaças físicas e/ou naturais:**

Sempre que ocorrer perda ou alteração indevida nos dados, os mesmos devem ser repostos com o último *backup* adequado disponível.

Uma outra estratégia consiste em ter um servidor secundário nas instalações fora da clínica. Isto permite que, se por algum motivo o servidor principal deixar de responder, o servidor secundário consegue dar resposta continuando a ser possível a atividade normal do negócio, apesar de poder existir uma menor eficácia nos processos de negócio. Este servidor secundário é um espelho parcial do servidor principal. Assim, o servidor secundário consegue dar respostas às aplicações da clínica e do cliente continuando a gerir os dados relativos a estas aplicações. No entanto, este servidor não dá resposta ao serviço de telemedicina.

Falhas técnicas de *hardware* e ameaças físicas e/ou naturais:

O servidor principal utiliza uma solução RAID de forma a garantir redundância de dados e a sua segurança. Assim, os dados encontram-se replicados, de forma a que, se algum disco se danificar, não se perde os dados do mesmo e o servidor continua a ser capaz de dar resposta relativa a esses dados. A RAID abrange os dados mais críticos e utilizados pela clínica, sendo que os outros dados não possuem uma solução RAID. Desta forma, efetua-se o espelhamento dos dados e o *striping*.

Caso algum equipamento apareça danificado, o equipamento deve ser substituído por um igual ou semelhante, de forma a que se consiga dar continuidade ao negócio. Deve ser observada a documentação do equipamento armazenado na mesma localização que o servidor secundário, e, caso exista um equipamento equivalente ao danificado, deve-se proceder à sua troca. Caso não se encontre um equipamento semelhante na documentação, deve-se contactar o grupo para que o mesmo encaminhe para as instalações da clínica hipotética, um equipamento semelhante.

Ameaças naturais e/ou físicas e falta de disponibilidade de pessoal para o trabalho:

Em caso de algum desastre que impossibilite o funcionamento ou até mesmo a abertura da clínica ao público, a clínica passará a encaminhar os seus pacientes para os cuidados de uma clínica próxima, até o grupo formalizar qualquer outro tipo de solução para a clínica hipotética. Para os pacientes da enfermaria, a clínica disponibiliza transporte para os mesmos, até à clínica do grupo mais próxima. Caso não haja transporte disponível, a clínica chamará um táxi e pagará a prestação de tal serviço.

Perda de serviços essenciais e ameaças físicas e/ou naturais:

Em caso de falha de energia, será utilizado um gerador secundário que a instalação tem disponível. Em caso de problemas no fornecimento de água, utiliza-se um tubo redundante, para o fornecimento da mesma, que se encontra numa rede com localização diferente.

Perda de serviços essenciais, ameaças físicas e/ou naturais, falha técnica de *hardware*, *malwares* e *hackers* ou *crackers*:

Se houver problemas com a internet e/ou a rede telefónica, que a substituição de equipamentos não resolva, deve-se notificar as operadoras dos respetivos serviços, de forma a que as mesmas resolvam a situação.

***Malwares*, erro no uso, falhas técnicas de *software*, ações não autorizadas, abuso de direitos e *hackers* e *crackers*:**

Caso haja alguma disrupção nos *software* feitos à medida que impossibilite ou dificulte a sua utilização e, por isso, a utilização dos serviços providenciados pelos mesmos, os fabricantes de SI devem ser contactados para que estes procedam à resolução do problema em causa. No entanto, caso as aplicações fiquem em baixo, deve-se proceder primeiro ao reiniciar das mesmas e caso não resulte deve-se proceder à notificação.

Caso haja alguma disrupção no *software Primavera* ou no *Outlook* deve-se contactar as entidades responsáveis pelo serviço em causa com a maior brevidade possível, sendo estas respetivamente a *PRIMAVERA Business Software Solutions* e a *Microsoft*.

***Malwares*, falhas técnicas de *software*, ações não autorizadas, abuso de direitos, *hackers* e *crackers* e comprometimento da informação:**

Uma outra estratégia associada ao comprometimento de uma máquina/sistema é proceder ao isolamento da mesma e, de seguida, solucionar o problema. Também deve ser notificado o grupo cajo se detete comprometimento da informação.

Caso se detete qualquer tipo de fuga de informação deve-se contactar o grupo.

Distúrbio devido à radiação:

Deve-se contactar a autoridade competente em caso deteção de problemas de radiação.

Abuso de direitos e ações não autorizadas:

Se for detetado algum uso indevido de equipamento/*software*, por parte de algum colaborador, a administração deve ser notificada da ocorrência e tomar medidas. A administração também deve ser notificada se algum ex-colaborador for detetado a realizar algum acesso a *hardware*/*software* da clínica, devido aos seus direitos ainda não terem sido totalmente revogados.

5.5. Desenvolvimento dos planos BCP e DRP

Para cada um destes planos existe um critério de ativação. O critério consiste no tempo necessário para determinar a causa do problema. Se for possível determinar a causa do problema e repor o sistema ou serviço em funcionamento normal dentro de 20 a 30 minutos, não será ativado o plano. Caso não seja possivel, deverá ser notificado o coordenador de planos para que este ative o plano apropriado, e, se este não tiver disponível, segue-se a política relacionada com a ativação dos planos / declaração de desastre.

Nos planos poderá vir a ser necessário contactar entidades, para isso será utilizada uma lista de contactos que contêm as informações necessárias para contactar qualquer serviço essencial para tratar de um problema ou incidente, nomeadamente os contactos:

- GNR – 244 830 150
- PJ - 244 845 222
- PSP – 244 859 859
- Bombeiros - 244 849 700
- Táxis de Leiria – 244 815 900/244 832 555
- Grupo clínico – 938 888 887/244 999 999; grupoclínico@outlook.com
- Serviço externo de higiene e limpeza – 918 888 886; servicoHigieneLimpeza@gmail.com
- Serviço externo de produção de alimentos – 968 888 885; alimentaHealth@outlook.com
- Serviço responsável pelo fornecimento de equipamento médico – 938 888 884
- Autoridade responsável por incidentes de radiação – 918 888 883
- Fabricantes de SI – 938 888 882, fabricantesSI@outlook.com
- Canalizador – 918 888 889
- Eletricista – 918 888 888
- *Microsoft* – 808 223 242; https://support.microsoft.com/pt-pt/supportforbusiness/productselection
- *Primavera* – 919 204 462/253 309 900; https://pt.primaverabss.com/pt/contactos/#contPri

- Administração – 244 888 888/968 888 881

É de ter em conta que após qualquer procedimento em cada plano, os problemas encontrados e a sua resolução devem ser documentados pela equipa.

5.5.1. Plano BCP

Caso ocorra um incidente devido a *malware*, erro no uso, *hacker* ou *cracker*, falhas técnicas de *hardware* e *software*:

- Se afetar o/as servidor/NAS/aplicações à medida:
    - Assim que possível deve-se continuar os processos de negócio a partir do servidor secundário, até o problema do original estar resolvido.
- Se afetar os *desktops*:
    - Caso exista algum *desktop* disponível para utilização, o colaborador deve continuar o seu trabalho nesse *desktop* até o problema relacionado com o *desktop* em causa ser resolvido.
    - Caso não exista nenhum *desktop* disponível, o trabalho deve ser continuado manualmente (com papel e caneta) até existir um *desktop* disponível.
- Se afetar *routers*/telefones/outro tipo de equipamento:
    - Caso seja equipamento médico, deve-se utilizar outro para o mesmo efeito, se não for possível deve-se solicitar que o paciente volte quando o problema se encontrar resolvido.
    - Caso exista algum equipamento suplente, deve-se passar a utilizar esse até que o problema seja resolvido.
- Se afetar o *software Primavera*:
    - Os colaboradores devem passar a fazer os pagamentos manualmente, solicitando pagamento monetário aos pacientes (sendo que os pacientes devem ser avisados previamente de tal inconveniente). Os colaboradores devem apontar tudo com papel e caneta de forma a que, quando o sistema estiver funcional, efetuem

os registos desses mesmos pagamentos, enviando a fatura/recibo para o cliente por *email*.

Caso ocorra um incidente devido ao erro no uso:

- Deve-se aguardar que seja efetuada a reposição dos dados perdidos através dos *backups* respetivos aos processos afetados ou através do *backup* completo dos dados.
- Enquanto se aguarda pela reposição, se não for possível continuar a utilizar a aplicação, deve-se dar continuidade ao trabalho manualmente (com caneta e papel).

Caso ocorra um incidente devido ao comprometimento de informação:

- Os colaboradores devem continuar o seu trabalho sem divulgar qualquer tipo de informação sobre o assunto, até novas ordens da administração e/ou grupo.

Caso ocorra perda de serviços essenciais, falta de disponibilidade de pessoal para trabalho ou ocorra uma ameaça física e/ou natural:

- A clínica, se possível, continua o seu negócio com as fontes alternativas desses serviços.
- Caso os métodos alternativos para os serviços essenciais não sejam suficientes para manter as instalações abertas, deve-se passar os serviços médicos para outras clínicas do grupo e disponibilizar meios de transporte para os pacientes que necessitem.
- Caso se perda as telecomunicações, os colaboradores devem utilizar sempre que possível o *e-mail* e/ou *sites* para continuar o seu trabalho. Caso sejam problemas relativos ao *e-mail*, devem utilizar as telecomunicações sempre que possível. Caso estas duas vias sejam comprometidas, os colaboradores podem utilizar o seu telemóvel pessoal, se possível. Caso

não seja possível devem continuar o seu trabalho, o máximo possível, aguardando que o problema seja resolvido.

- Caso haja uma ameaça natural, como fogo, inundações, sismos e furacões:
    - Todo o pessoal da clínica deve ser imediatamente evacuado das instalações.
- Caso exista falta de pessoal:
    - Pedir auxílio ao grupo por pessoal temporário para continuar a exercer as funções das pessoas em falta na clínica.
    - Caso o grupo não possua pessoal alternativo os serviços médicos devem ser passados para outras clínicas do grupo e disponibilizar meios de transporte para os pacientes que necessitem.

Caso ocorra distúrbios devido a radiação:

- As instalações da clínica devem ser evacuadas e o incidente reportado ao grupo/entidade responsável.
- Os serviços médicos devem ser passados para outras clínicas do grupo e disponibilizados meios de transporte para os pacientes que necessitem.

5.5.2. Plano DRP

Muitas vezes, ao longo do plano, estipula-se a identificação do problema e a resolução do mesmo. Num cenário real, seria necessário que o plano estivesse delineado para cada problema que se pudesse encontrar e a respetiva resolução do mesmo. No entanto, sendo este um cenário hipotético, só se conseguiu identificar alguns problemas apesar de existirem mais. Devido a isto, foi optado por apresentar, de uma forma geral, os problemas e soluções com as quais a clínica se poderia deparar.

Perda de serviços essenciais:

- Falha de energia:
    - O gerador secundário é ligado automaticamente.
        - Se o gerador não se ligar automaticamente, a equipa deve ligá-lo manualmente.

        - Se não for possível ligar manualmente, a administração deve ser notificada.
    - A equipa deve proceder à identificação do problema que causou a falha de energia
        - Se o problema for algum quadro, ou outro componente que se desligou, a equipa deve ligar o componente.
        - Se for um problema que vem do fornecedor de energia, a equipa deve proceder à notificação do problema ao fornecedor.
        - Se for um problema derivado à danificação de algum componente, a equipa deve proceder aos serviços do eletricista cujo contacto se encontra na lista de contactos.
    - Assim que o problema se encontrar resolvido, a equipa deve proceder à ativação da fonte de energia primária e desligar a fonte de energia secundária.
- Falha de água:
    - É utilizado automaticamente o tubo de rede secundário.
    - A equipa deve identificar o problema:
        - Se for o caso de a água estar desligada, a equipa deve ligá-la.
        - Se for um problema derivado do fornecedor, a equipa deve notificar o fornecedor do problema.
        - Se for um outro tipo de problema, a equipa deve contactar o canalizador cujo contacto se encontra na lista de contactos.
    - Assim que o problema se encontrar resolvido, a equipa deve proceder à ativação da fonte de água primária e desligar a fonte de água secundária.
- Falha de comunicações telefónicas:
    - A equipa deve identificar a fonte do problema:
        - Em caso de não identificar a fonte do problema deve contactar imediatamente o fornecedor do serviço para que o mesmo resolva o problema.
        - Em caso de ser alguma avaria de equipamento, deve contactar o fornecedor do serviço e explicar a situação para que o mesmo proceda à reparação ou substituição do equipamento.

        - Em caso de qualquer outra fonte do problema, a equipa deve contactar o fornecedor do serviço e explicar o problema para que o mesmo o possa resolver.
- Falha de internet:
    - A equipa deve identificar a fonte do problema:
        - Se for uma falha de intranet associada ao grupo, deve contactar imediatamente o grupo e expor o problema para o mesmo resolver.
        - Em caso de uma falha na rede local:
            - Se for um problema de *hardware*:
                - A equipa irá à documentação verificar se existe um equipamento igual ou semelhante, na instalação onde se encontra o servidor secundário, se houver é enviada para o adquirir e substituir o equipamento danificado. Se não constar tal equipamento na documentação, a equipa terá de efetuar uma notificação ao grupo para que o mesmo envie para a clínica um equipamento semelhante ou igual. Assim que o equipamento chegar é feita a sua substituição.
                - Após a substituição, a equipa deve proceder à análise da rede para determinar se o problema ficou resolvido. Se não ficou resolvido deve voltar a identificar a fonte do problema e resolvê-lo.
            - Se não for de *hardware*, a equipa, juntamente com o administrador da rede, deve proceder à resolução do problema.
        - Em caso de falha com a rede exterior, deve contactar o fornecedor do serviço e expor o problema para o mesmo resolver.

Falhas técnicas de *hardware,* falhas técnicas de *software*:

- Falha da NAS:

- A equipa deve isolar o equipamento e só depois deve ser ativada a utilização dos processos de negócio a partir do servidor secundário, até o problema do original estar resolvido.
- A equipa deve proceder à identificação do problema:
  - Se for um problema relativo aos discos:
    - A equipa irá à documentação verificar se existe um equipamento igual ou semelhante, na instalação onde se encontra o servidor secundário, se houver é enviada para o adquirir e substituir o equipamento danificado. Se não constar tal equipamento na documentação, a equipa terá de efetuar uma notificação ao grupo para que o mesmo envie para a clínica um equipamento semelhante ou igual. Assim que o equipamento chegar é feita a sua substituição.
    - Após a substituição, a equipa deve proceder à análise determinar se o problema ficou resolvido. Se não ficou resolvido deve voltar a identificar a fonte do problema e resolvê-lo.
  - Se for outro problema:
    - A equipa terá de efetuar uma notificação ao grupo para que o mesmo envie para a clínica um equipamento semelhante ou igual. Assim que o equipamento chegar é feita a sua substituição.

Falhas técnicas de *hardware*, falhas técnicas de *software*, *malwares*, *hackers* e *crackers* e erro no uso:

- Falha em massa dos *desktops* da clínica e/ou dispositivos periféricos:
  - É enviada uma equipa para analisar o problema
    - Se o problema for de algum *hardware* que se danificou:
      - A equipa irá à documentação verificar se existe um equipamento igual ou semelhante, na instalação onde se encontra o servidor secundário, se houver é enviada para o adquirir e substituir o equipamento danificado. Se não

constar tal equipamento na documentação, a equipa terá de efetuar uma notificação ao grupo para que o mesmo envie para a clínica um equipamento semelhante ou igual. Assim que o equipamento chegar é feita a sua substituição.

- Após a substituição do equipamento, a equipa deve fazer o equipamento retomar o funcionamento normal.

- Se for detetado qualquer indício de atividade ilegal ou de ataque, a equipa deve notificar a administração e o administrador do sistema para que os mesmos decidam o que devem fazer.
- Se for um outro tipo de problema:
  - A equipa deve analisar o problema e após identificá-lo deve proceder à sua resolução.

- O servidor principal deixa de responder:
  - É enviada uma equipa para analisar o problema
    - Se o problema for de algum *hardware* que se danificou:
      - A equipa irá à documentação verificar se existe um equipamento igual ou semelhante, na instalação onde se encontra o servidor secundário, se houver é enviada para o adquirir e substituir o equipamento danificado. Se não constar tal equipamento na documentação, a equipa terá de efetuar uma notificação ao grupo para que o mesmo envie para a clínica um equipamento semelhante ou igual. Assim que o equipamento chegar é feita a sua substituição.
      - Após a substituição do equipamento, a equipa deve fazer o servidor retomar o funcionamento.
      - Após o servidor estar a funcionar, a equipa deve analisar o servidor de forma a determinar se o mesmo está no seu normal funcionamento. Se o servidor não estiver a funcionar normalmente deve ser analisado o problema e resolvido.
    - Se for detetado qualquer indício de atividade ilegal ou de ataque, a equipa deve notificar a administração e o administrador do sistema para que os mesmos decidam o que devem fazer.

        - Se for um outro tipo de problema:
            - A equipa deve analisar o problema e após identificá-lo deve proceder à sua resolução.

Falhas técnicas de *hardware,* falhas técnicas de *software*, distúrbio devido a radiação e erro no uso:

- Falha no equipamento médico:
    - A equipa deve proceder à identificação do problema e da sua fonte:
        - Se for detetado fuga de radiação:
            - Se for radiação prejudicial ao ser vivo, a equipa deve proceder à imediata evacuação das instalações.
            - Deve proceder à notificação da autoridade competente para que a mesma avalie a situação e proceda à sua resolução.
        - Se for um problema no equipamento:
            - Se for necessário trocar o equipamento:
                - A equipa terá de efetuar uma notificação ao grupo para que o mesmo envie para a clínica um equipamento semelhante ou igual. Assim que o equipamento chegar é feita a sua substituição.
            - Se for um problema relativo ao *software*:
                - A equipa deve notificar o fornecedor do equipamento médico em causa.

Falhas técnicas de *software* e erro no uso:

- Falha no *software* à medida:
    - A equipa deve proceder à identificação do problema e da sua fonte:
        - Se for um problema relativo a uma atualização.
            - Deve ser feito um *rollback* para o último estado estável do sistema.
            - Deve proceder-se à realização da atualização novamente.
        - Se for um problema de compatibilidade de versões:

        - Deve atualizar para as versões mais recentes.
        - Se o problema persistir deve executar *rollback* para o último estado estável do sistema.
    - Se for algum erro critico inesperado:
        - Deve verificar se ocorreu eliminação/alteração dos dados:
            - Se houver, deve-se recuperar os dados perdidos/originais através dos *backups*.
        - Deve verificar o sistema onde a aplicação corre foi corrompido:
            - Se tiver sido corrompido, deve contactar os fabricantes de SI para que os mesmos resolvam o problema.
- Falha dos serviços de terceiros (*Outlook* e *Primavera*):
    - A equipa deve contactar a empresa proprietária do serviço, expondo o problema para que assim, a mesma possa proceder à sua resolução.

Ameaças físicas e/ou naturais:

- Equipamento danificado:
    - A equipa irá à documentação verificar se existe um equipamento igual ou semelhante, na instalação onde se encontra o servidor secundário, se houver é enviada para o adquirir e substituir o equipamento danificado. Se não constar tal equipamento na documentação, a equipa terá de efetuar uma notificação ao grupo para que o mesmo envie para a clínica um equipamento semelhante ou igual. Assim que o equipamento chegar é feita a sua substituição.

Assim que os problemas encontrados estiverem resolvidos deve-se proceder à utilização de *backups* sempre que for necessário recuperar dados. Para isso é necessário que a equipa se desloque às instalações do servidor secundário e recupere os *backups* necessários, volte à clínica e os utilize. É de ter em conta que em qualquer plano no qual

seja utilizado *hardware* que estivesse armazenado nas instalações do servidor secundário, deve-se dar baixa do mesmo assim que o problema estiver resolvido. É também importante, no fim das resoluções dos problemas e possíveis baixas de *hardware*, documentar o problema encontrado e a solução utilizada para a resolução do mesmo.

5.6. Exercícios, testes e simulacros

5.6.1. Testes

De modo a se encontrarem as deficiências ou problemas existentes nos sistemas e por conseguinte, serem realizadas todas as melhorias necessárias, são elaborados testes com diferentes focos. Isto é, são realizados testes para diferentes tipos de disrupções/catástrofes, que podem atingir diferentes componentes dos sistemas. Os testes, assim, acabam por melhorar a resposta aos incidentes. É de ter em conta que os testes devem ser realizados uma vez por ano. Existem diferentes tipos de testes que devem ser implementados e que serão abordados de seguida.

Relativamente aos testes de simulações, devem ser realizados os testes de falha súbita de energia, falha de água, caso de incêndio, falha dos vários tipos de *hardware* que a clínica possuí, nomeadamente, falha no servidor principal, falha em 1, 2 ou mais discos de armazenamento de dados no servidor, falhas no equipamento médico e falha no servidor secundário. Para além dos testes referidos anteriormente, devem ser efetuados testes de falhas de comunicação, desde telefones até *e-mails*, disrupções nos vários *software*, sendo esses a *Primavera* e os *software* feitos à medida para a clínica e para os clientes.

Já os testes do tipo "guião", devem ser executados por cada departamento, em que o pessoal deve rever passo a passo o plano associado ao seu próprio departamento. Assim, no contexto deste cenário serão alvo deste tipo de testes os departamentos de administração, de recursos humanos, de gestão e finanças, de administração informática e o organismo médico.

No fim de cada teste deve-se ter em conta se os planos de contingência são precisos e efetivos e se devem ser impostas e implementadas melhorias nos planos dos vários departamentos. Também tem de se efetuar o balanço e apreciação do que correu bem ou mal de forma a determinar as melhorias.

5.6.2. Treino

O treino do pessoal que constituí as equipas que implementam os planos de contingência, permite garantir que o pessoal esteja preparado para participar nos testes e exercícios que são realizados, e nos eventos de disrupções que podem ocorrer. O objetivo acaba por ser a implementação do plano, numa situação de crise sem que as equipas se tenham de apoiar maioritariamente nos documentos do plano. A formação na responsabilidade e tarefas a executar nos planos de contingência é efetuada sempre que um funcionário entre a serviço da clínica pela primeira vez. Já o treino é um procedimento que para novos funcionários, deve ser realizado aquando a sua entrada na clínica e posteriormente de 6 em 6 meses, até perfazer um ano após o primeiro treinamento efetuado. Já os funcionários que possuem mais de um ano de serviço na clínica realizam um treinamento anual e sempre que algum dos sistemas da clínica e/ou os planos de contingência sofrer alguma alteração, estes receberão um treino focado nas mesmas, se essa alteração for refletida nas suas tarefas. É de referir que cada treino é focado no papel ou função do funcionário no respetivo plano de contingência.

5.6.3. Exercícios

Com o objetivo de validar a viabilidade de um ou mais aspetos do plano são executados exercícios. Existem dois tipos de exercícios que devem ser efetuados para ajudar a garantir o objetivo mencionado, nomeadamente, exercícios *tabletop* e exercícios funcionais.

Relativamente aos exercícios *tabletop*, estes consistem numa discussão de ideias, papeis, tomadas de decisões e responsabilidades no caso de ocorrências de vários cenários possíveis de emergência. Neste cenário, o "instrutor" descreve o cenário e posteriormente faz perguntas, sendo que as pessoas (da equipa) discutem sobre o problema.

Já os exercícios funcionais consistem em o pessoal executar os seus deveres num ambiente simulado e seguro. Neste tipo de exercícios, o conjunto de exercícios que se realizam podem variar de âmbito e complexidade, validando assim diferentes aspetos do plano.

É de ter em conta que o nível de impacto do sistema afeta diretamente o tipo de exercício que será realizado. Por exemplo, o tipo funcional deve ser principalmente empregue em sistemas com nível de impacto alto ou moderado, já os do tipo *tabletop* serão principalmente empregues em sistemas com baixo impacto. Neste cenário deve-se ter em consideração os níveis de impacto já mencionados.

5.7. Manutenção dos planos

Como já se tinha referido, é da responsabilidade do coordenador dos planos de contingência do grupo e do coordenador da área de segurança da clínica tanto a elaboração dos planos de contingência da clínica, bem como a devida atualização deste de 18 em 18 meses. É também da responsabilidade destes dois coordenadores mencionados a documentação de todos os planos de contingência. É de ter em conta que o prazo de 18 meses não será válido quando existirem alterações a nível do negócio (por exemplo, os objetivos do mesmo), atualizações nas tecnologias utilizadas, atualizações nas políticas da clínica e/ou do grupo, mudanças em termos de funcionários e contactos dos mesmos, atualização/término de licenças e/ou contratos de produtos/entidades, bem como alterações de responsabilidades e nas regulamentações e leis, sendo que deve-se proceder à imediata atualização dos planos. Também se tem de rever os planos, na totalidade, sempre que algum elemento dos mesmos sofra alterações significativas. Qualquer atualização dos planos deve ser coordenada e possivelmente sincronizada com todas as entidades que tenham relação com os planos, sendo essas entidades o grupo e os serviços externos como, por exemplo, os fabricantes de SI. A cada nova atualização dos planos, devem ser eliminadas as cópias (tanto digitais como em papel) relativas às versões anteriores, no entanto, deve ser mantido um registo com todas as alterações efetuadas ao longo do tempo. Se a atualização implicar serviços externos ou contratos com qualquer entidade que a clínica possua, as informações relativas a essas entidades devem ser atualizadas e possivelmente poderá vir a ser necessário a notificação e atualização dos contratos. É importante ter em consideração que qualquer alteração significativa nos planos poderá implicar a revisão e possível atualização do BIA.

As cópias dos planos têm de ser guardadas e armazenadas de forma segura, pois os mesmos poderão conter informação confidencial. Com isto, devem existir cópias em formato digital cifradas e devem existir *backups* dessas cópias na instalação onde se encontra o servidor secundário, para assim garantir a confidencialidade e disponibilidade. Deve ser mantido um registo das alterações dos planos para garantir a *accountability*.

6. Conclusão

Para este trabalho foi implementado o cenário hipotético de uma clínica, cenário esse presente no trabalho de PARSI. Neste trabalho decidiu-se que o cenário iria desempenhar apenas cuidados médicos gerais, não cuidando de casos urgentes ou críticos. A clínica apresenta uma séria de ativos que devem ser protegidos tais como, os dados privados dos pacientes e os dados confidenciais da clínica.

Desta forma, a maior parte da informação que é tratada pela clínica é privada e confidencial, sendo que tem de existir uma boa infraestrutura que garanta a segurança da informação. Deve também existir plano de continuidade do negócio que permita a clínica continuar o seu negócio em caso de ocorrência de algum desastre.

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 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* e falhas técnicas de *software*. Riscos menos graves passam por ameaças físicas e/ou naturais e incumprimentos de legislação e regulamentos.

Foi efetuada a gestão de continuidade de negócios sendo que foi necessário efetuar o BIA, que é uma análise mais orientada ao impacto no negócio do que nos dados. Depois foi necessário correlacionar as duas análises realizadas para definir os controlos preventivos mais importantes para a clínica e para desenvolver estratégias e planos de contingência para possibilitar a continuidade do negócio.

Antes do BIA, foram definidas políticas de continuidade de negócio que servem como regras que a empresa deve seguir, como por exemplo, a regra de que na empresa devem sempre existir planos de contingência atualizados.

Para a escolha dos controlos para mitigar os riscos, 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 e o impacto de negócio existente nos processos de negócio. 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 e devem ser definidas estratégias e planos de contingência para minimizar os danos destes riscos acontecerem.

As estratégias de contingência foram definidas consoante o risco residual, os riscos aceites, e o resultado do BIA. Assim, muitas das estratégias criadas focaram-se nos riscos aceites relativos, por exemplo, à falta de pessoal para o trabalho. Os riscos com maior risco residual como o erro de uso, falhas técnicas de *software* e falta de pessoal para o trabalho. Outras estratégias, para além destas, são as estratégias para a eventualidade da perda de serviços essenciais que, apesar de existirem medidas preventivas, devem também existir estratégias caso os controlos falhem.

Relativamente ao desenvolvimento dos planos de contingência, estes foram desenvolvidos com as estratégias de contingência em mente, as ameaças analisadas, e os ativos importantes para o funcionamento do negócio. Desta forma foi possível definir planos para cada cenário de contingência previsto na clínica.

Com isto mencionado, o trabalho aqui realizado proporcionou compreender a enorme dificuldade que é o desenvolvimento de estratégias e de planos de contingência num ambiente real. Como existe uma enormidade de ameaças presentes numa organização, é necessário que os planos de contingência estejam preparados para qualquer tipo de situação possível dentro de cada ameaça. Isto leva a que o nível de trabalho para elaborar um plano de contingência, como BCP e o DRP, seja um grande desafio não só para desenvolver, mas também para manter atualizados.

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. Para além disso, deve-se testar os planos BCP e DRP de forma a determinar se os mesmos são efetivos ou se é preciso atualizá-los consoante a necessidade da clínica.

Referências

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

[2] M. Swanson, P. Bowen, A. W. Phillips, D. Gallup e D. Lynes, “NIST Special Publication 800-34 Rev. 1,” 2010.

Anexos

Anexo 1 – Análise de Riscos

Ameaça 1	***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

Ameaça 2	**Erro no uso**		
Impacto Resultante	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
Probabilidade de Ocorrência	A probabilidade de um erro acontecer na utilização dos ativos é moderada.	Probabilidade de Ocorrência	2
			Moderado
Risco Inerente			Elevado

Ameaça 3	**Falhas técnicas de** *software*		
Impacto Resultante	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
Probabilidade de Ocorrência	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
Risco Inerente			Elevado

Ameaça 4	Comprometimento da informação		
Impacto Resultante	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
Probabilidade de Ocorrência	A probabilidade de comprometimento é baixa.	Probabilidade de Ocorrência	1
			Baixo
Risco Inerente			Moderado

Ameaça 5	Abuso de direitos		
Impacto Resultante	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
Probabilidade de Ocorrência	A probabilidade de ocorrer o abuso de direitos é moderada.	Probabilidade de Ocorrência	2
			Moderado
Risco Inerente			Moderado

Ameaça 6	Ações não autorizadas		
Impacto Resultante	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
Probabilidade de Ocorrência	A probabilidade de uma ação não autorizada acontecer é moderada.	Probabilidade de Ocorrência	2
			Moderado
Risco Inerente			Moderado

Ameaça 7	Falta na disponibilidade de pessoal para o trabalho		
Impacto Resultante	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
Probabilidade de Ocorrência	A probabilidade de ocorrer é moderada.	Probabilidade de Ocorrência	2
			Moderado
Risco Inerente			Moderado

Ameaça 8	*Hacker* ou *crackers*		
Impacto Resultante	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
Probabilidade de Ocorrência	A probabilidade de um indivíduo ou organização querer prejudicar a empresa é baixa.	Probabilidade de Ocorrência	1
			Baixo
Risco Inerente			Moderado

Ameaça 9	Falhas técnicas de *hardware*		
Impacto Resultante	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
Probabilidade de Ocorrência	A probabilidade de um disco rígido ou equipamento falhar é reduzida, pois estes dispositivos são extensivamente testados pelos fabricantes.	Probabilidade de Ocorrência	1
			Baixo
Risco Inerente			Baixo

Ameaça 10	Coimas por incumprimento de legislação e regulamentos		
Impacto Resultante	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
Probabilidade de Ocorrência	A probabilidade de uma autoridade de controlo / fiscalizadora aplicar uma coima é baixa.	Probabilidade de Ocorrência	1
			Baixo
Risco Inerente			Baixo

Ameaça 11	Perda de serviços essenciais		
Impacto Resultante	Impacto médio. Poderá impedir o normal funcionamento da organização.	Vulnerabilidade	3
		Aviso prévio	2
		Duration	2
		Valor do Impacto(V+E+D)	7
			Médio
Probabilidade de Ocorrência	A probabilidade de uma perda de serviço essencial é baixa.	Probabilidade de Ocorrência	1
			Baixo
Risco Inerente			Baixo

Ameaça 12	Distúrbio devido a radiação		
Impacto Resultante	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
Probabilidade de Ocorrência	A probabilidade de uma anomalia ocorrer num equipamento médico é baixa.	Probabilidade de Ocorrência	1
			Baixo
Risco Inerente			Baixo

Ameaça 13	Ameaças físicas e/ou naturais		
Impacto Resultante	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
Probabilidade de Ocorrência	A probabilidade de uma ameaça física e/ou natural ocorrer é baixa.	Probabilidade de Ocorrência	1
			Baixo
Risco Inerente			Baixo

Anexo 2 – Riscos Residuais

Ameaça: *Malwares*

Avaliação dos controlos	O tipo de controlo deste género de ameaça é preventivo, mas isto não significa que o risco é resolvido com total certeza. Considerando isto e os controlos implementados, o risco residual será bastante baixo.	Valor dos controlos	3 Eficiente
Risco Residual			Baixo

Ameaça: Erro no uso

Avaliação dos controlos	O tipo de controlo deste género de ameaça é razoavelmente preventivo. Considerando isto e os controlos implementados, o risco residual será moderado.	Valor dos controlos	2 Aceitável
Risco Residual			Moderado

Ameaça: Falhas técnicas de *software*

Avaliação dos controlos	O tipo de controlo deste género de ameaça é razoavelmente preventivo. Considerando isto e os controlos implementados, o risco residual será moderado.	Valor dos controlos	2 Aceitável
Risco Residual			Moderado

Ameaça: Comprometimento de informação

Avaliação dos controlos	O tipo de controlo deste género de ameaça é preventivo, mas isto não significa que o risco é resolvido com total certeza. Considerando isto e os controlos implementados, o risco residual será bastante baixo.	Valor dos controlos	3 Eficiente
Risco Residual			Baixo

Ameaça: Abuso de direitos

Avaliação dos controlos	O tipo de controlo deste género de ameaça é preventivo, mas isto não significa que o risco é resolvido com total certeza. Considerando isto e os controlos implementados, o risco residual será bastante baixo.	Valor dos controlos	3 Eficiente
Risco Residual			Baixo

Ameaça: Ações não autorizadas

Avaliação dos controlos	O tipo de controlo deste género de ameaça é preventivo, mas isto não significa que o risco é resolvido com total certeza. Considerando isto e os controlos implementados, o risco residual será bastante baixo.	Valor dos controlos	3 Eficiente
Risco Residual			Baixo

Ameaça: Falta na disponibilidade de pessoal para o trabalho

Avaliação dos controlos	O tipo de controlo deste género de ameaça é muito pouco preventivo. Considerando isto e a baixa probabilidade de isto acontecer, o risco residual será moderado.	Valor dos controlos	1 A Melhorar
Risco Residual			Moderado

Ameaça: *Hackers* ou *crackers*

Avaliação dos controlos	O tipo de controlo deste género de ameaça é razoavelmente preventivo. Considerando isto e os controlos implementados, o risco residual será bastante baixo.	Valor dos controlos	2 Aceitável
Risco Residual			Baixo

Ameaça: Falhas técnicas de *hardware*

Avaliação dos controlos	O tipo de controlo deste género de ameaça é razoavelmente preventivo. Considerando isto e os controlos implementados, o risco residual será bastante baixo.	Valor dos controlos	2 Aceitável
Risco Residual			Baixo

Ameaça: Coimas por incumprimento de legislação e regulamentos

Avaliação dos controlos	O tipo de controlo deste género de ameaça é preventivo, mas isto não significa que o risco é resolvido com total certeza. Considerando isto e os controlos implementados, o risco residual será bastante baixo.	Valor dos controlos	3 Efeciente
Risco Residual			Baixo

Ameaça: Perda de serviços essenciais

Avaliação dos controlos	O tipo de controlo deste género de ameaça é preventivo, mas isto não significa que o risco é resolvido com total certeza. Considerando isto e os controlos implementados, o risco residual será bastante baixo.	Valor dos controlos	3 Efeciente
Risco Residual			Baixo

Ameaça: Distúrbio devido a radiação

Avaliação dos controlos	O tipo de controlo deste género de ameaça é muito pouco preventivo. Considerando isto e a baixa probabilidade de isto acontecer, o risco residual será baixo.	Valor dos controlos	1 A Melhorar
Risco Residual			Baixo

Ameaça: Ameaças físicas e/ou naturais

Avaliação dos controlos	O tipo de controlo deste género de ameaça é razoavelmente preventivo. Considerando isto e os controlos implementados, o risco residual será bastante baixo.	Valor dos controlos	2 Aceitável
Risco Residual			Baixo