INSTITUTO DE ESTUDOS SUPERIORES MILITARES

CURSO DE PROMOÇÃO A OFICIAL SUPERIOR

2009/2010

TII

O TEXTO CORRESPONDE A TRABALHO FEITO DURANTE A FREQUÊNCIA DO CURSO NO IESM SENDO DA RESPONSABILIDADE DO SEU AUTOR, NÃO CONSTITUINDO ASSIM DOUTRINA OFICIAL DA FORÇA AÉREA PORTUGUESA.

PLANO DE CONTINUIDADE DE SERVIÇOS, NO ÂMBITO DOS SISTEMAS DE INFORMAÇÃO DA FAP

JOSÉ MANUEL DA SILVA TRABULA

CAPITÃO TINF

INSTITUTO DE ESTUDOS SUPERIORES MILITARES

PLANO DE CONTINUIDADE DE SERVIÇOS, NO ÂMBITO DOS SISTEMAS DE INFORMAÇÃO DA FAP

CAP/TINF José Manuel da Silva Trabula

Trabalho de Investigação Individual do CPOS/FA

Pedrouços 2010

INSTITUTO DE ESTUDOS SUPERIORES MILITARES

PLANO DE CONTINUIDADE DE SERVIÇOS, NO ÂMBITO DOS SISTEMAS DE INFORMAÇÃO DA FAP

CAP/TINF José Manuel da Silva Trabula

Trabalho de Investigação Individual do CPOS/FA

Orientador: TCOR/Nav António Eugénio

Pedrouços 2010

Agradecimentos

Aos meus camaradas de curso, pela amizade e apoio sempre presentes.

A todos os que se disponibilizaram para as entrevistas realizadas, contribuindo decisivamente com os seus conhecimentos e experiência para o resultado obtido.

À Major Ana Telha pela disponibilidade e informação fornecida.

Ao Major José Gorgulho pelo constante apoio, revisão do trabalho e espírito crítico sempre necessário num trabalho de investigação.

Por fim, mas o mais importante, à minha mulher Amélia e ao meu filho João por todo o apoio, encorajamento, paciência, motivação e muita tolerância ao longo destes últimos meses.

Índice

Índice de Figuras

Índice de Tabelas

Resumo

Um dos aspectos mais importantes em qualquer organização é o acesso aos seus Sistemas de Informação.

Espera-se desses sistemas uma elevada disponibilidade, segurança, fiabilidade e que forneçam atempadamente a informação necessária, credível e actualizada.

A Força Aérea não possui um plano que garanta a continuidade de serviços, no âmbito dos Sistemas de Informação, de modo a que o acesso à informação seja retomado num prazo aceitável.

Um dos objectivos desta investigação é o de indicar uma metodologia que permita elaborar um Plano de Continuidade de Serviços, para os Sistemas de Informação, de modo a preparar a Organização para situações de ruptura, quer sejam originadas por desastres naturais, por intervenção humana ou por falhas técnicas.

Neste trabalho discute-se a importância da análise e caracterização dos Sistemas de Informação e da infra-estrutura de Tecnologias de Informação que os suportam, avaliando-se a actual situação e o impacto provocado em caso de indisponibilidade.

Foram efectuadas entrevistas aos responsáveis pelas diversas áreas que permitiram, através da análise dos dados obtidos e de acordo com um quadro conceptual, testar as hipóteses apresentadas.

Decorrente da investigação fica demonstrado, através da análise de impacto realizada, que há uma grande dependência dos Sistemas de Informação e que não existem, na maior parte dos casos, procedimentos alternativos definidos ou devidamente testados, pelo que a inexistência de um Plano de Continuidade de Serviços tem um elevado impacto na organização.

Em relação à infra-estrutura de Tecnologias de Informação, verifica-se que esta não garante a continuidade de serviços, comprometendo a disponibilidade dos Sistemas de Informação.

Nas conclusões apresentadas reforça-se a importância e a necessidade de se implementar uma solução que permita a continuidade dos serviços a partir de outro local, numa perspectiva de garantia da disponibilidade pela capacidade de recuperação dos Sistemas.

Abstract

One of the most important aspects in any modern organization is the access to its Information Systems.

Those systems are expected to be highly available, secure, reliable and able to supply all the necessary information on time, in a credible and updated way.

The Air Force doesn't have any plan to guarantee ongoing services of the Information Systems, so that the essential functions can become operational again within an acceptable timing.

One of the objectives of this research is to indicate a methodology, which can allow the creation of an Ongoing Services Plan for the Information Systems, so that the organization can be prepared for any rupture, caused by any natural disaster or human or technical failure.

In this work, it is discussed the importance of analysis and characterization of the Information Systems and of the structure of the Information Technologies that support them by evaluating the current situation and the impact caused in case of non-availability.

Interviews were made to the people responsible for several different areas, which allowed to test the different presented hypothesis, through the analysis of the data we got from that and accordingly to previously set concepts.

With this research, through the impact analysis done, it can be seen that there is a huge dependence of the Information Systems and that, in most cases, there aren't any defined alternative procedures nor any appropriated tested ones, so the non-existence of any Ongoing Services Plan has a huge impact in the organization.

In what the Information Technologies Infrastructure is concerned, it was shown that it doesn't guarantee the ongoing services, compromising the Information Systems availability.

In the presented conclusions, it is reinforced the importance and the necessity of implementing a solution which allows the ongoing services to work from another place, guaranteeing availability through the capacity of system recovery.

Palavras-chave

Análise de Impacto, Continuidade de Serviços, *Recovery Point Objective*, *Recovery Time Objective*, Sistemas de Informação, Tecnologias de Informação.

Lista de Abreviaturas

AFA – Academia da Força Aérea

BA – Base Aérea

CA – Comando Aéreo

CDA – Centro de Dados Alternativo

CDP – Centro de Dados Principal

CIMFA – Centro de Informação Meteorológica da Força Aérea

CLAFA – Comando da Logística da Força Aérea

DAT – Direcção de Abastecimento e Transportes

DCSI – Direcção de Comunicações e Sistemas de Informação

DFFA – Direcção de Finanças da Força Aérea

DI – Direcção de Infra-Estruturas

DIVCSI – Divisão de Comunicações e Sistemas de Informação

DMSA – Direcção de Manutenção de Sistemas de Armas

DP – Direcção de Pessoal

DTC – *Data Transfer Card*

EMFA – Estado-Maior da Força Aérea

FA – Força Aérea

FAP – Força Aérea Portuguesa

HFA – Hospital da Força Aéea

IGP – Inspecção Geral das Pescas

IM – Instituto de Meteorologia

METAR – *Meteorological Aerodrome Report*

NATO – *North Atlantic Treaty Organization*

NC3B – NATO *Consultation, Command and Control Board*

PCS – Plano de Continuidade de Serviços

PDSIFA – Plano Director dos Sistemas de Informação da Força Aérea

PGS – *Portugese Ground Station*

RFA – Regulamento da Força Aérea

RIGFA – Rede Interna Geral da Força Aérea

RPO – *Recovery Point Objective*

RTO – *Recovery Time Objective*

SGH – Sistema de Gestão Hospitalar

SI – Sistemas de Informação

SIAGFA – Sistema Integrado de Apoio à Gestão da Força Aérea

SIAGFA-GM – Sistema Integrado de Apoio à Gestão da Força Aérea – Módulo de Gestão de Material

SIAGFA-MGM – Sistema Integrado de Apoio à Gestão da Força Aérea – Módulo de Gestão de Manutenção

SIAGFA-MGO – Sistema Integrado de Apoio à Gestão da Força Aérea – Módulo de Gestão Operacional

SIAGFA-RH – Sistema Integrado de Apoio à Gestão da Força Aérea – Módulo de Recursos Humanos

SICOM – Sistema Integrado de Comunicações Militares

SIGAP – Sistema de Informação de Gestão da Área de Pessoal

SIGMA – Sistema de Informação de Gestão de Manutenção e Abastecimento

SIINFRAS – Sistema de Informação de Infra-Estruturas

SIPAV – Sistema de Informação de Processamento Automático de Vencimentos

SLA – *Service Level Agreements*

TAF – *Terminal Aerodrome Forecasts*

TI – Tecnologias de Informação

UPS – *Uninterruple Power Supply*

Introdução

A Informação é um recurso organizacional de vital importância para a Força Aérea.

A gestão da informação é uma responsabilidade fundamental, exigindo uma estrutura organizacional definida, procedimentos normalizados e o envolvimento de toda a cadeia hierárquica.

Os Sistemas de Informação (SI) são um dos pilares de sustentação do processo de tomada de decisão numa organização moderna. Espera-se que contribuam, aos diversos níveis e em tempo oportuno, com a Informação necessária, suficiente, credível e actualizada.

As organizações precisam de adoptar estratégias que lhes permitam salvaguardar a Informação, dado o seu potencial valor, assim como os SI que a armazenam, processam e transmitem, através de medidas de protecção, detecção, reacção e recuperação.

A dependência cada vez maior dos SI dita que a Organização deverá desenvolver um plano de gestão de continuidade para a sua protecção e garantia de cumprimento da missão.

No centro do planeamento de gestão de continuidade está uma importante capacidade tecnológica, conjuntamente com todos os procedimentos que asseguram a protecção da Informação e das pessoas, de forma a garantirem uma total disponibilidade da Informação e, assim que necessário, uma rápida recuperação dos SI e das funções críticas e vitais da Organização.

A decisão de se implementar uma solução de continuidade de serviços depende da análise do impacto na Organização, decorrente da indisponibilidade dos seus SI. Após esta análise, torna-se necessário identificar e recomendar o conjunto de medidas destinadas a proteger os SI e garantir a sua disponibilidade.

Durante esta investigação serão analisados e caracterizados os SI operacionais ou transaccionais considerados prioritários na Força Aérea Portuguesa (FAP) em termos de recuperação e garantia de disponibilidade. As conclusões deste trabalho de investigação são válidas no âmbito da Força Aérea (FA).

O objectivo deste trabalho é o de contribuir, através de um conjunto de orientações e a indicação de uma metodologia, para a elaboração de um plano que garanta a continuidade de serviços, no âmbito dos SI da FAP.

Neste trabalho foi seguido o método de investigação em Ciências Sociais de Raymond Quivy e Luc Van Campenhoudt (2008). Foi identificada uma pergunta de partida

que traduz aquilo que se procura saber e servirá, ao longo da investigação, como referência orientadora:

- Que metodologia deve ser adoptada pela Força Aérea que permita assegurar, em caso de interrupção de serviços, a disponibilidade dos Sistemas de Informação?

A partir desta pergunta inicial derivam as seguintes perguntas a que se procurará dar resposta:

- Qual o impacto na Força Aérea em caso de indisponibilidade dos seus Sistemas de Informação?
- Poderá a actual infra-estrutura de Tecnologias de Informação da Força Aérea comprometer a continuidade de serviços?

Este trabalho apresenta no primeiro capítulo a problemática da indisponibilidade dos SI na FA. Salienta a importância dos SI nas organizações e refere os aspectos que devem estar presentes na elaboração de um Plano de Continuidade de Serviços, através de um quadro teórico de referência.

O segundo capítulo faz uma análise e caracterização dos SI e da infra-estrutura de Tecnologias de Informação (TI) que os suportam, avaliando a actual situação com base no modelo conceptual definido no primeiro capítulo.

No terceiro capítulo efectua-se a análise de resultados, a partir dos dados observados, confrontando-os com os capítulos anteriores, de modo a verificar as hipóteses e desse modo dar resposta às perguntas da investigação. Do resultado desta verificação serão extraídas as conclusões e indicadas algumas recomendações.

A partir da actual situação dos SI/TI da FAP e da relação entre os conceitos, foram formuladas as seguintes hipóteses que serão verificadas durante esta investigação:

- A inexistência de um plano de continuidade de serviços, para os Sistemas de Informação, tem um elevado impacto na Força Aérea.
- A actual infra-estrutura de Tecnologias de Informação da Força Aérea garante a continuidade de serviços.

A fim de verificar as hipóteses acima referidas, foram efectuadas diversas entrevistas aos responsáveis dos SI e da infra-estrutura de TI.

A construção do modelo de análise[1] implicou a identificação de conceitos fundamentais à problemática em estudo, articulando-os em dimensões, componentes e

[1] Anexo A – Modelo de Análise

indicadores. No decorrer deste trabalho, para além da terminologia disponível no Glossário, serão utilizados os seguintes conceitos:

Análise de Impacto: Processo analítico em que as organizações definem com rigor quais os SI críticos, através da atribuição de um grau de prioridade de recuperação, da identificação dos responsáveis pelos SI, da identificação dos tempos máximos de recuperação e do impacto da indisponibilidade desses SI (*Business Continuity Institute).*

Tecnologias de Informação: Refere-se especialmente à tecnologia, isto é, *Hardware*, *Software* e rede de comunicações. São compostas por recursos tangíveis (servidores, PC, *routers*, *switches*) e intangíveis (*software*). Facilitam a aquisição, processamento, armazenamento, entrega e partilha da informação e outros conteúdos digitais (Peppard & Ward, 2003).

Continuidade de Serviços: Procedimentos que uma organização põe em prática para assegurar que as funções essenciais estão disponíveis após uma interrupção não planeada. Visa evitar a interrupção de serviços estabelecendo as medidas que permitam, de uma forma rápida e eficaz, aceder às funções consideradas críticas (*Business Continuity Institute*).

Sistemas de Informação: É o meio através do qual as pessoas e as organizações, utilizando a tecnologia, recolhem, processam, armazenam, utilizam e difundem informação (Peppard & Ward, 2003).

1. Continuidade de Serviços no âmbito dos Sistemas de Informação

A Força Aérea não possui um Plano de Continuidade de Serviços (PCS), no âmbito dos seus SI.

Em qualquer organização a indisponibilidade de serviços e a perda de dados são inaceitáveis. Deve ser considerada, ao mais alto nível, a existência de um plano que garanta o acesso à informação vital e cuja recuperação e disponibilidade sejam consideradas prioritárias.

O Plano Director de Sistemas de Informação da Força Aérea (PDSIFA) refere que um dos pilares de sustentação do processo de tomada de decisão, numa organização moderna e estruturada como a FA, é o conjunto de SI que a suporta. Apesar da reconhecida importância dos SI, não existe um PCS (Damásio, 2009).

Um dos factores mais importantes na disponibilidade de serviços é a infra-estrutura tecnológica de suporte aos SI. Na FA existem 17 Centros de Dados que apoiam igual número de redes internas que formam a Rede Interna Geral da Força Aérea (RIGFA). Contudo, não existe definido um Centro de Dados Alternativo.

Neste capítulo será indicada uma classificação dos Centros de Dados que permita avaliar os seus níveis de disponibilidade. De seguida, apontar-se-á os aspectos mais importantes que devem estar presentes no que diz respeito à continuidade de serviços. Reforça-se a importância de um PCS e serão descritos dois aspectos fundamentais na sua elaboração: a realização de uma análise de impacto e a identificação das técnicas de recuperação de dados.

a. Infra-estrutura de Tecnologias de Informação

Antes de se equacionar o planeamento da continuidade de serviços deve garantir-se uma infra-estrutura de TI resiliente. Os aspectos mais importantes e críticos das TI estão relacionados com a fiabilidade e a disponibilidade da sua infra-estrutura.

Para Boggs et. al. (2009) os componentes críticos da infra-estrutura de TI – servidores, unidades de armazenamento, *software* e elementos activos de rede (*switches* e *routers*) – deverão ser constantemente actualizados e monitorados, originando uma redução de 43% na indisponibilidade de serviços.

No desenho, concepção e implementação de um Centro de Dados deverão ser observados aspectos tão importantes como a redundância dos sistemas de

fornecimento de energia e refrigeração, controlo de acesso às instalações, sistemas anti-fogo e soluções tecnológicas tolerantes a falhas, ou seja, servidores em *Cluster* partilhando unidades de armazenamento (Lourenço, 2009).

Os SI são considerados resistentes e seguros quando os pontos de falha são minimizados ou totalmente eliminados.

Nos Centros de Dados deverão ser adoptadas medidas que os tornem tolerantes a falhas, seja por motivo humano, técnico ou natural. Neste contexto é reconhecida internacionalmente a classificação em *Tiers* elaborada pelo *Uptime Institute*[2] e que mede a tolerância a falhas.

Tabela 1 – Classificação dos Centros de Dados

Classificação *Uptime Institute*	**Caracterização**
TIER **I** Infra-Estrutura Básica	Caminho único para a distribuição de energia e ar condicionado; Sem componentes redundantes; **Até 28.8 H de indisponibilidade/ano (99.671% de disponibilidade)**
TIER **II** Infra-Estrutura de componentes com redundância	Caminho único para a distribuição de energia e ar condicionado; Componentes redundantes; **Até 22 H de indisponibilidade/ano (99.741% de disponibilidade)**
TIER **III** Infra-Estrutura mantida concorrentemente	Múltiplos caminhos para a distribuição de energia e ar condicionado, mas só um activo; Componentes redundantes; Manutenção concorrente; **Até 1.6 H de indisponibilidade/ano (99.982% de disponibilidade)**
TIER **IV** Infra-Estrutura com tolerância a falhas	Múltiplos caminhos activos para a distribuição de energia e ar condicionado; Componentes redundantes; Tolerância a falhas; **Até 0.4 H de indisponibilidade/ano (99.995% de disponibilidade)**

(Fonte: Adaptado de *Uptime Institute - Data Center Site Infrastructure Tier Standard: Topology*)

A análise dos Centros de Dados mediante as classificações *Tier* é feita atribuindo-se o menor valor *Tier* de um determinado sistema. Um Centro de Dados com sistemas de distribuição eléctrica classificados como *Tier* II e com redundância de encaminhamentos de rede classificados como *Tier* III receberá uma classificação geral de *Tier* II. No Anexo B – Classificação dos Centros de Dados - são analisadas em pormenor as classificações atribuídas pelo *Uptime Institute*.

Pela caracterização utilizada, verifica-se que a disponibilidade dos Centros de Dados limita a disponibilidade geral da infra-estrutura de TI e consequentemente os SI.

Pode-se concluir que no centro de um PCS está uma importante capacidade tecnológica que, em conjunto com os procedimentos alternativos que asseguram a protecção da informação e das pessoas, garante uma total disponibilidade da informação e uma rápida recuperação dos SI.

[2] O *Uptime Institute* é uma organização focada nos assuntos de alta disponibilidade dos Centros de Dados.

b. Continuidade de Serviços

Quando se refere a continuidade de serviços estão presentes, segundo Jardim (2007), diversos factores e processos tais como políticas de *backup*, arquitecturas redundantes de alta disponibilidade e tolerantes a falhas, técnicas de recuperação de dados e a existência de um Centro de Dados Alternativo, fundamental em qualquer metodologia de continuidade de serviços.

Jardim (2007) refere ainda a relação existente entre continuidade de serviços e gestão dos níveis de serviço (*Service Level Agreements* – SLA). Estes são desenvolvidos e implementados de acordo com as necessidades e os vários níveis de criticidade dos SI. A gestão da continuidade de serviços deve suportar estes SLA para que os procedimentos de recuperação possam implementar com sucesso o que está definido.

A alta disponibilidade é um dos factores mais importantes na continuidade de serviços. Para Piedad & Hawkins (2000), citado por Jardim (2007), "o termo alta disponibilidade significa uma redução no *downtime* aplicacional, planeado ou não, que é sentido pelos utilizadores". Para Weygant (2001), a alta disponibilidade caracteriza um SI que é desenhado de forma a evitar perda de serviços, reduzir falhas e ao mesmo tempo minimizar a indisponibilidade dos Sistemas.

Nem todos os eventos que provocam interrupção de serviços necessitam que se active o PCS. Um ambiente de produção (aplicações, bases de dados, sistemas e infra-estrutura) implementado numa plataforma tecnologicamente redundante, que garanta a disponibilidade dos serviços na ordem dos 99,95% (quatro horas de indisponibilidade/ano) a 99,995% (25 minutos/ano), permite que os vários tipos de indisponibilidade sejam controlados e minimizados.

A necessidade de um PCS deve então ser entendida como uma extensão da disponibilidade de serviços. Caso um sistema fique indisponível por um período de tempo superior ao definido, a situação poderá evoluir de um problema de disponibilidade para um problema de continuidade de serviços.

c. Importância de um Plano de Continuidade de Serviços

A disponibilidade, segurança, fiabilidade e o acesso atempado à informação são factores essenciais para o normal funcionamento de uma organização.

Um PCS é um processo que auxilia as organizações a prepararem-se para situações de ruptura, quer sejam originadas por desastres naturais, por intervenção humana ou por falhas técnicas.

Os cenários de risco evoluíram das catástrofes naturais para cenários mais diversificados e abrangentes, desde a falta de energia que afecta toda uma região geográfica até à concretização de ataques terroristas.

O objectivo de um PCS é o de garantir que os serviços críticos sejam retomados num prazo aceitável, minimizando o impacto e assegurando que os SI e a infra-estrutura tecnológica são recuperados e restabelecidos.

Numa perspectiva organizacional, a crescente dependência dos SI/TI, o impacto na organização provocado pela indisponibilidade dos sistemas e a obrigação de cumprimento de requisitos legais reforçam a importância da implementação de um PCS.

O sucesso de uma metodologia de continuidade de serviços está fortemente dependente da infra-estrutura de TI, das políticas de segurança de informação (através de *backup* e replicação de dados) e da elaboração da análise do impacto causado na organização em caso de indisponibilidade total ou parcial dos SI.

O documento AC/35-D/1039 de 08 de Outubro de 2008 da NATO, que complementa o AC/322-D(2007)0043, de 30 de Agosto de 2007 do NC3B, "*Supporting Document on the Availability Aspects of Security*", inclui uma secção de continuidade de serviços e refere que "Deve ser estabelecido um plano de continuidade de serviços sempre que a análise de impacto na organização identifique requisitos de alta disponibilidade em relação à informação e aos sistemas que a suportam".

Os RFA 390 – 1 (A), 3 e 4 estabelecem que devem ser observados os princípios da garantia de informação como condição única para a salvaguarda da Informação e dos SI que a armazenam, processam e transmitem, ou seja, deve ser estabelecido um conjunto de medidas que deverão incluir a capacidade de restauração dos SI, incorporando medidas de protecção, detecção, reacção, recuperação e localização alternativa.

d. Análise de Impacto

Uma das tarefas iniciais e mais críticas na elaboração de um PCS consiste na realização de uma análise de impacto. Com base no modelo a seguir

apresentado, efectuaram-se entrevistas aos responsáveis da área técnica e funcional dos SI/TI da FAP que permitiram ter um conhecimento mais profundo da actual realidade e que é transversal à Organização.

Para Toigo (2003) a análise de impacto deve, numa primeira fase, relacionar os SI com as TI que os suportam. Após a recolha destes dados, procede-se à identificação das vulnerabilidades dos SI/TI que podem originar interrupção de serviços e avaliar o impacto provocado pela indisponibilidade dos SI.

Segundo Jardim (2007:32) "Não faz sentido o desenvolvimento de um plano de continuidade se a própria organização tiver demasiadas exposições que à partida podem ser prevenidas ou minimizadas.".

O sucesso de um PCS está dependente de uma análise de impacto em que as organizações definem com rigor quais os SI críticos, através da atribuição de um grau de prioridade de recuperação, e da identificação do impacto na organização em função do tempo de indisponibilidade.

A análise de impacto permite caracterizar os SI do seguinte modo:

- TI que o suportam;
- Identificação das vulnerabilidades dos SI/TI;
- Atribuição do grau de prioridade de recuperação;
- Identificação do impacto na organização em caso de indisponibilidade;
- Atribuição do grau de criticidade;
- Identificação de procedimentos alternativos;
- Identificação das interdependências entre os SI;
- Indicação do *Recovery Point Objective* (RPO): refere-se à quantidade máxima aceitável de perda de dados que não é possível recuperar ou que poderão ser reintroduzidos no sistema. Este parâmetro reflecte o tempo máximo necessário ao sincronismo dos dados (Batista, 2010);
- Indicação do *Recovery Time Objective* (RTO): indica o período de tempo máximo aceitável de indisponibilidade, isto é, o tempo decorrido entre a interrupção de serviços e a sua total recuperação, correspondendo ao tempo que os processos da organização podem funcionar sem suporte dos SI. Para Batista (2010), o valor de RTO mais baixo irá determinar o tempo máximo de recuperação de todos os serviços disponíveis - disponibilidade total do Centro de Dados.

e. Técnicas de Recuperação de Dados

As organizações têm necessidade de salvaguardar os seus dados de modo a permitir a sua recuperação em caso de ocorrência de um evento que provoque uma interrupção de serviços. Este objectivo pode ser alcançado através de diversas técnicas, desde a mais básica e simples que consiste em procedimentos de *backup* e *restore* até técnicas mais complexas de replicação de dados.

O *backup/restore* baseia-se na cópia dos dados para *tape* e na sua reposição no mesmo local ou num local alternativo. Possui um elevado tempo de recuperação (RTO de 24 a 72 horas), devido à necessidade de aplicar o último *backup* e efectuar as configurações dos sistemas. Em termos de perda de dados depende da última cópia efectuada, normalmente um dia. Este é o método mais simples e com menor impacto no desempenho das aplicações (Gorgulho, 2010).

A replicação consiste na transferência dos dados da unidade de armazenamento para outro equipamento similar localizado num Centro de Dados Alternativo. Esta replicação pode ser feita em tempo real (síncrona) ou desfasada no tempo (assíncrona) e está fortemente dependente das comunicações (Batista, 2010).

Segundo Lourenço (2009), para os SI cuja perda de dados aceitável vai desde alguns minutos até às duas horas, a replicação assíncrona é a mais apropriada. A replicação síncrona é indicada para os sistemas em que não é admissível perder dados e seja exigida uma rápida disponibilidade.

O *backup* é útil para efectuar a reposição dos dados tal como se encontravam num determinado momento no tempo, em que a perda de dados não seja considerada crítica. A replicação é usada para garantir que os dados, e as alterações efectuadas durante o dia, estão sempre disponíveis mesmo quando ocorre a interrupção de serviços. É a técnica aconselhada para SI e dados considerados críticos (Batista, 2010), referindo que "sem uma solução de *backup* eficaz, não existe continuidade de serviços".

Remete-se para o Anexo C – Técnicas de Recuperação**,** uma análise comparativa destas técnicas, de modo a clarificar em que consiste cada uma delas e a evidenciar as suas diferenças**.**

Se a organização tiver capacidade de replicar os seus dados para um local geograficamente diferente garantirá, segundo Fonseca (2004), a disponibilidade dos dados, o acesso aos SI e a continuidade de serviços.

Qualquer que seja a técnica utilizada, é fundamental a existência de um Centro de Dados Alternativo, que representa o mais elevado nível de protecção dos SI de uma organização (Betan, 2010). Este Centro deve estar localizado numa zona geográfica diferente da do Centro de Dados Principal. Em termos de comunicações deverão estar assegurados circuitos redundantes entre os dois Centros.

Como foi referido, as organizações dependem cada vez mais dos seus SI. Um PCS procura garantir as condições de acesso à informação em caso de indisponibilidade total ou parcial dos SI.

O sucesso desse plano depende da existência de uma infra-estrutura de TI redundante e tolerante a falhas, da definição de uma política de segurança dos dados e da existência de um Centro de Dados Alternativo. A metodologia a adoptar depende da elaboração de uma análise que permita avaliar o impacto que a indisponibilidade dos SI provoca na organização.

2. Os Sistemas de Informação e as Tecnologias de Informação na Força Aérea

Actualmente existem 117 SI em exploração na Força Aérea. Nesta investigação serão caracterizados apenas os que são considerados mais prioritários (Prioridade 1) pela Divisão de Comunicações e Sistemas de Informação (DIVCSI), no âmbito das suas competências e com base numa análise preliminar sujeita a aprovação superior. No Anexo D – Sistemas de Informação da Força Aérea - estão identificados todos os sistemas e as prioridades atribuídas pela DIVCSI.

Neste capítulo, apresentar-se-á o resultado da informação obtida através das entrevistas efectuadas aos responsáveis pelos SI/TI e orientadas de modo a responder aos pontos principais da análise de impacto. Os SI analisados foram agrupados em três áreas funcionais: Pessoal, Logística e Operacional.

a. Caracterização dos Sistemas de Informação da Área de Pessoal

- **SIGAP**: Sistema de Informação de Gestão da Área de Pessoal;
- **SIAGFA-RH**: Sistema Integrado de Apoio à Gestão da Força Aérea - Módulo de Recursos Humanos;
- **SGH**: Sistema de Gestão Hospitalar;
- **PICIS**: Sistema de Informação de Cuidados Críticos;

- **CLINIDATA XXI**: Sistema de Gestão do Laboratório de Patologia Clínica do HFA;
- **SIPAV**: Sistema de Informação de Processamento Automático de Vencimentos;
- **SIPAV-CONTBANC**: Pagamentos por Conta Bancária.

Tabela 2 – Sistemas de Informação da Área de Pessoal

Sistema de Informação	EPR	PRI (0 a 5)	IMP (0 a 5)	CRI (0 a 5)	Processo Alternativo	DEP	RTO	RPO
SIGAP e SIAGFA-RH	DP	5	5	5	Não Existe	X	48 horas	48 horas
SGH	HFA	5	5	5	Alguns	X	45 min.	12 horas
PICIS	HFA	5	5	4	Papel	SGH	12 horas	24 horas
CLINIDATA XXI	HFA	5	5	5	Não Existe	SGH	2 horas	12 horas
SIPAV e SIPAV-CONTBANC	DFFA	5	5	5	Não Existe	SIGAP	24 horas	24 horas

EPR – Entidade Primariamente Responsável
PRI – Prioridade de Recuperação (**0** – Baixa a **5** – Elevada)
IMP – Impacto em caso de indisponibilidade (**0** – Baixo a **5** – Elevado)
CRI – Criticidade do Sistema (**0** – Baixa a **5** – Elevada)
DEP – Dependência de outros Sistemas de Informação
RTO – *Recovery Time Objective*
RPO – *Recovery Point Objective*

(Fonte: Elaborado pelo autor)

No SIGAP e SIAGFA-RH, para uma indisponibilidade superior a dois dias (RTO), o impacto nos processos de gestão é elevado (Nunes, 2009). Neste período, a actividade normal será comprometida e a capacidade de resposta limitada. Perde-se a capacidade de produção dos indicadores necessários ao planeamento de pessoal e haverá impacto noutros SI.

Por motivos legais, existe suporte em papel para a maior parte dos dados registados no SIGAP. O RPO indicado é de dois dias devido à possibilidade de reintrodução dos dados, obrigando ao reforço de pessoal.

A indisponibilidade dos SI de Saúde (SGH, PICIS e CLINIDATA XXI) tem um elevado impacto na missão do Hospital da Força Aérea (HFA), uma vez que prejudicam a prestação eficaz dos actos médicos (Cordeiro, 2010).

No SGH a indisponibilidade traduz-se em atrasos na realização de actos médicos podendo impedir a sua concretização devido à impossibilidade de consultar o processo clínico electrónico. No caso do módulo de enfermagem, os enfermeiros deixam de ter acesso a dados importantes como a prescrição de medicamentos.

Na maioria dos módulos existem processos alternativos, embora pouco expeditos e sem rotinas devidamente testadas.

A indisponibilidade do PICIS tem como consequência a incapacidade de fornecer, em tempo útil, informação acerca do doente. Foi estabelecido um RTO de 12 Horas e um RPO de 24 Horas (Cordeiro, 2010). Embora inadequado a uma unidade de recobro, existe um procedimento manual alternativo em papel e o SGH pode ser utilizado, com limitações, para aceder a alguma informação dos doentes.

Segundo Costa (2010), a indisponibilidade do CLINIDATA XXI afecta gravemente o funcionamento do laboratório, sendo totalmente inviável atender os utentes. Por este motivo o RTO é de duas Horas.

Actualmente, pelo número de doentes e pela sofisticação dos equipamentos laboratoriais, já não são viáveis os procedimentos manuais. A transferência manual é hoje inaceitável pelos riscos que lhe são inerentes, estabelecendo-se um RPO de 12 Horas (Costa, 2010). Segundo a Chefe do Serviço de Patologia Clínica, sem sistema, o impacto na actividade do laboratório de análises será elevado. O CLINIDATA XXI depende do SGH para aceder à inscrição e dados dos utentes.

Na área financeira, a indisponibilidade do SIPAV e do SIPAV-CONTBANC tem um impacto elevado (Passos, 2009). A inexistência de procedimentos alternativos provocará a incapacidade para o processamento dos vencimentos. O período máximo aceitável sem acesso aos sistemas é de um dia (RTO).

Não houve capacidade para indicar a quantidade aceitável de dados perdidos (RPO), assumindo-se um dia devido à actual política de *backup* destes sistemas.

b. Caracterização dos Sistemas de Informação da Área de Logística

- **SIGMA-ABAST**: Sistema de Informação de Gestão de Manutenção e Abastecimento;
- **SIAGFA-GM**: Sistema Integrado de Apoio à Gestão da Força Aérea - Módulo de Material;
- **SIAGFA-MGM e SIAGFA-MGM-C**: Sistema Integrado de Apoio à Gestão da Força Aérea - Módulos de Gestão de Manutenção;
- **PGS**: *Portuguese Ground Station*;
- **SIINFRAS**: Sistema de Informação de Infra-Estruturas.

Tabela 3 – Sistemas de Informação da Área Logística

Sistema de Informação	EPR	PRI (0 a 5)	IMP (0 a 5)	CRI (0 a 5)	Processo Alternativo	DEP	RTO	RPO
SIGMA-ABAST e SIAGFA-GM	DAT	5	5	5	Papel	SIAGFA-GM depende do SIGMA-ABAST	48 horas	48 horas
SIAGFA-MGM e SIAGFA-MGM-C	DMSA	5	4	4	Não Existe	SIGAP e SIGMA-ABAST	24 horas	24 horas
PGS	DMSA	4	5	5	Existe	Não tem	1 Sem	24 horas
SIINFRAS	DI	5	5	5	Não Existe	Não tem	72 horas	2 horas

EPR – Entidade Primariamente Responsável
PRI – Prioridade de Recuperação (**0** – Baixa a **5** – Elevada)
IMP – Impacto em caso de indisponibilidade (**0** – Baixo a **5** – Elevado)
CRI – Criticidade do Sistema (**0** – Baixa a **5** – Elevada)
DEP – Dependência de outros Sistemas de Informação
RTO – *Recovery Time Objective*
RPO – *Recovery Point Objective*

(Fonte: Elaborado pelo autor)

Em caso de indisponibilidade dos sistemas SIGMA-ABAST e SIAGFA-GM durante determinados períodos (exercícios, número de alertas ou elevado índice de manutenção inopinada), a utilização do processo alternativo torna-se insustentável a partir do terceiro dia. Este procedimento consiste em listagens das existências do material disponível (local e central) que, devido ao elevado número de movimentos, rapidamente ficam desactualizadas correndo-se o risco de ser indicada a existência de um artigo crítico e este já ter sido consumido sem ter havido reposição. Por este motivo, os indicadores RTO e RPO definidos são de 48H.

Sem acesso a estes sistemas o impacto na actividade aérea será elevado (Gomes, 2010), podendo afectar a taxa de prontidão dos meios aéreos ou mesmo impedir o cumprimento de determinadas missões.

O SIAGFA-MGM e SIAGFA-MGM-C apoiam a manutenção de aeronaves. A indisponibilidade destes sistemas terá impacto na configuração, no controlo de potenciais e principalmente na situação operacional das aeronaves, podendo comprometer algumas missões (incluindo alertas).

O impacto será maior se a interrupção de serviços ocorrer durante um período em que esteja a ser pedido um esforço suplementar de missões ou durante exercícios (Silva, 2009).

O RPO definido é de 24 Horas porque o registo dos consumos de potencial são feitos na caderneta do avião (horas de voo, horas de funcionamento próprio, ciclos de trem, etc.), sendo actualizados posteriormente no sistema.

Assumindo-se que as aeronaves continuarão a operar, apesar do sistema estar indisponível, perder-se-á a visibilidade do potencial remanescente tanto das aeronaves como dos componentes. O RTO indicado é de 24 Horas.

Os helicópteros EH-101 têm um SI dedicado à gestão de manutenção. O PGS possui sistemas e processos alternativos que apresentam algumas limitações porque só permitem a visualização da informação, não se podendo registar as actividades de manutenção nem descarregar os dados dos voos (Guerreiro, 2010).

Uma semana é o tempo indicado como RTO, sendo possível operar com os métodos alternativos. De acordo com a política de *backup* deste sistema, é estabelecido um RPO de um dia. Existe a capacidade de reintrodução dos dados dos helicópteros através da utilização do *Data Transfer Card* (DTC), que armazena os dados gerados pelos sistemas internos do helicóptero.

A missão da Repartição de Património da Direcção de Infra-Estruturas (DI) é apoiada pelo SIINFRAS. A indisponibilidade deste sistema impede o cumprimento dessa missão porque não podem ser introduzidos ou analisados novos processos, nem consultados os já existentes (Salvado, 2010).

Com um RPO de duas horas e um RTO de três dias, este sistema não tem alternativa.

c. Caracterização dos Sistemas de Informação da Área Operacional

- **SIAGFA-MGO**: Sistema Integrado de Apoio à Gestão da Força Aérea - Módulo de Gestão Operacional;
- **Winventus**: Informação Meteorológica.

Tabela 4 – Sistemas de Informação da Área Operacional

Sistema de Informação	EPR	PRI (0 a 5)	IMP (0 a 5)	CRI (0 a 5)	Processo Alternativo	DEP	RTO	RPO
SIAGFA-MGO	CA	5	5	5	SIM	SIGAP SIAGFA-RH, SIAGFA-MGM , SIAGFA-GM e SIGMA-ABAST	72 horas	72 horas
WINVENTUS	CIMFA	4	4	5	SIM	Não tem	6 horas	3 horas

EPR – Entidade Primariamente Responsável
PRI – Prioridade de Recuperação (**0** – Baixa a **5** – Elevada)
IMP – Impacto em caso de indisponibilidade (**0** – Baixo a **5** – Elevado)
CRI – Criticidade do Sistema (**0** – Baixa a **5** – Elevada)
DEP – Dependência de outros Sistemas de Informação
RTO – *Recovery Time Objective*
RPO – *Recovery Point Objective*

(Fonte: Elaborado pelo autor)

Sem acesso ao SIAGFA-MGO é comprometida a capacidade de planeamento das missões, consulta e extracção de informação.

As missões serão sempre efectuadas porque existe um procedimento alternativo ao seu planeamento. É possível efectuar reserva de *airtasks* e fazer manualmente o *tasking*, inserindo-se posteriormente essa informação. Os dados do modelo 1M serão inseridos após o processamento das missões no sistema.

Uma paragem superior a três dias pode originar erros na recuperação da informação (Saraiva, 2009).

Para Ramos (2010), Chefe do Centro de Informação Meteorológica da Força Aérea (CIMFA), no caso de indisponibilidade do Winventus os dados armazenados localmente ficam desactualizados, o que reduzirá a qualidade e fiabilidade da informação prestada às tripulações e que no extremo poderá levar ao cancelamento das missões. Devido a esta situação foi definido um RPO de três horas e um RTO de seis horas.

O Winventus está preparado para tratar automaticamente os dados que tenham ficado retidos na fonte. Quando o sistema estiver disponível torna-se necessário informar o Instituto de Meteorologia (IM) de modo a proceder-se ao envio da informação aí retida.

Como alternativa existe a utilização do telefone e fax, o que requer um aumento dos recursos humanos implicando que este processo apenas possa ser utilizado durante algumas horas.

Este SI é considerado crítico devido à possibilidade de algumas missões serem canceladas. A validação das previsões - *Terminal Aerodrome Forecasts* (TAF) - tem que ser feita pelas observações - *Meteorological Aerodrome Report* (METAR). Sem esta última informação em tempo útil o TAF tem que ser cancelado e sem TAF válido as tripulações não descolam.

d. Infra-estrutura de Tecnologias de Informação na Força Aérea

Em 2007 iniciou-se o projecto de reestruturação de sete Centros de Dados (EMFA, CA, BA5, BA6, BA11, HFA e AFA), com o objectivo de dotá-los dos mais modernos sistemas de arrefecimento (ar condicionado) e de fornecimento de energia através de *Uninterruple Power Supply* (UPS), dois componentes fundamentais para o funcionamento dos equipamentos informáticos.

De acordo com Gorgulho (2010), este projecto teve início devido à necessidade de substituição de servidores e do exponencial crescimento de espaço para armazenamento de informação.

Uma das características dos novos Centros de Dados é a capacidade de monitorização remota 24H/7 permitindo uma actuação pró-activa. Todos têm capacidade de funcionamento redundante: 2N para os sistemas de frio (existem dois sistemas iguais sendo necessário apenas um para sustentar o funcionamento) e N+1 para os sistemas de energia (o sistema tolera a falha de um dos módulos que o constituem).

Com este projecto foi possível dotar os Centros de Dados com uma solução de alta disponibilidade, para alguns SI, que consiste na utilização de servidores que fornecem o mesmo serviço partilhando um equipamento de armazenamento de dados. No caso de um dos servidores parar, por motivo de avaria ou de intervenção técnica, o serviço manter-se-á disponível. Esta solução caracteriza-se pela sua flexibilidade em termos de dimensionamento e configuração e ainda pela uniformização da tecnologia que permite a troca de componentes, a uniformização da formação, da administração e da operação.

Na Tabela 5 estão identificados os Centros de Dados, onde os SI em análise estão instalados, apresentando-se as vulnerabilidades identificadas e as medidas de controlo existentes.

Tabela 5 – Vulnerabilidades dos SI/TI e Medidas de Controlo

Centro de Dados	SI	Vulnerabilidades	Medidas de Controlo
EMFA	SIGAP SIAGFA-RH SIPAV SIPAV-CONTBANC SIGMA-ABAST SIAGFA-GM SIAGFA-MGM SIAGFA-MGM-C SIAGFA-MO SIINFRAS	• *Switch* central (ponto único de falha); • Sistema de arrefecimento através de um circuito de água; • Não existe redundância do servidor aplicacional (SIGAP e SIINFRAS); • Não existe redundância do servidor de Base de Dados (SIINFRAS).	• Monitorização 24H/7; • Contrato de suporte de Hardware 24x7x4H; • *Backup* Diário/Semanal/Mensal e Anual; • Controlo de Acessos; • Sistema Anti-fogo; • Controlo de Humidade e temperatura; • Distribuição energia N+1; • Ar-condicionado 2N; • Grupo gerador dedicado ao Centro de Dados; • Sistemas de detecção de inundação e de válvulas de corte do circuito de água; • Servidores com fontes de alimentação redundantes; • Manutenção preventiva (distribuição Energia e ar-condicionado).
CA	WINVENTUS	• Ar condicionado N; • UPS não redundante; • Sala dos Servidores inadequada.	• Contrato de suporte de Hardware 24x7x4H; • Servidores com fontes de alimentação redundantes; • Servidores com funções redundantes; • Grupo Gerador.

Centro de Dados	SI	Vulnerabilidades	Medidas de Controlo
HFA	SGH PICIS CLINIDATA XXXI	• Base única de instalação dos servidores (ponto único de falha); • *Switch* central (ponto único de falha); • Não existe redundância do servidor de Base de Dados(PICIS e CLINIDATA XXI) • Não existe redundância do servidor aplicacional (PICIS).	• Contrato de suporte de Hardware 24x7x4H; • *Backup* Diário/Semanal/Mensal e Anual; • Ar condicionado 2N; • Sistema Anti-fogo; • Servidores com fontes de alimentação redundantes; • Grupo Gerador.
BA6	PGS	• Não existe redundância do servidor de Base de Dados; • *Switch* central (ponto único de falha); • Base única de instalação dos servidores (ponto único de falha).	• Contrato de suporte de Hardware 24x7x4H; • *Backup* Diário/Semanal/Mensal e Anual; • Ar condicionado 2N; • Sistema Anti-fogo; • Servidores com fontes de alimentação redundantes; • Monitorização remota.

(Fonte: Elaborado pelo autor)

O Centro de Dados do EMFA é o principal Centro da FA. É a partir daí que é efectuada a monitorização 24H/7 dos Centros de Dados intervencionados. Possui um grupo gerador de energia dedicado, que alimenta todos os componentes do Centro e permite a autonomia necessária em caso de falha prolongada de energia eléctrica.

Apesar da intervenção efectuada nos sete Centros de Dados, existem alguns pontos únicos de falha, nomeadamente a existência de um único *switch* central que liga os servidores à RIGFA. Em caso de falha os SI ficam indisponíveis.

e. Rede de comunicações

Para a implementação de uma solução de continuidade de serviços terá que existir redundância em termos de comunicações e uma largura de banda que permita a transferência de dados (Lourenço, 2009).

A RIGFA é uma rede que assenta numa topologia em estrela com um ponto central (*router*) no Comando Aéreo (CA) utilizando, basicamente, a rede de comunicações de micro-ondas da FA e a rede do Sistema Integrado de Comunicações Militares (SICOM), ver Anexo F – Rede de comunicações para voz e dados.

A estrela começa a ter algumas pontas ligadas entre si, não com a intenção de aumentar a largura de banda mas com o objectivo da redundância (Oliveira, 2010). Um dos pontos críticos é o *router* central do CA. Em caso de avaria o acesso à RIGFA fica indisponível. Outra das falhas que se pode identificar na RIGFA é a falta de monitorização dos equipamentos que a constituem (*routers*, *switches*). Não

existe qualquer mecanismo de alerta que permita actuar de uma forma pró-activa evitando interrupções.

Efectuada a análise de impacto e a caracterização dos SI e da infra-estrutura de TI que os suporta, está-se em condições de, no próximo capítulo, validar as hipóteses que orientam esta investigação e responder à pergunta central.

3. Análise de Resultados

Construído o modelo teórico e apresentados os conceitos estruturantes, procedeu-se à elaboração do modelo de análise que procura caracterizar os conceitos sob a forma de dimensões, componentes e indicadores (Anexo A – Modelo de Análise), constituindo uma ferramenta de suporte à investigação.

Nesta fase, enquadrada na etapa de verificação, é importante confrontar o modelo de análise com os dados obtidos ao longo da investigação através da pesquisa bibliográfica, da observação directa e das entrevistas realizadas aos responsáveis pelos SI e TI.

Após a análise empírica destes dados e da caracterização dos SI/TI apresentada no capítulo anterior, proceder-se-á agora ao teste e verificação das hipóteses formuladas, no sentido de responder às perguntas derivadas e à pergunta central que norteia a presente investigação.

A definição de uma metodologia que assegure a continuidade de serviços implica a realização de uma análise de impacto que permita caracterizar os SI e a infra-estrutura de TI que os suporta.

Em relação à primeira hipótese é importante identificar qual o impacto na FA em caso de indisponibilidade total ou parcial dos seus SI.

Um dos primeiros aspectos a considerar é a identificação dos SI considerados críticos. Dos 117 SI em exploração na FAP, a DIVCSI considerou 15 como sendo os mais prioritários (Prioridade 1), em termos de recuperação e disponibilidade. Esta informação permitiu concentrar a investigação apenas nestes sistemas e procurar obter junto dos seus responsáveis os indicadores que contribuissem para os caracterizar, procurando avaliar o impacto que a sua indisponibilidade tem na Organização.

Quanto à existência de processos alternativos, dos sete sistemas analisados da área de pessoal só dois (SGH e PICIS) é que os têm definidos, embora pouco expeditos, sem rotinas testadas e, no caso do PICIS, pouco adequado a uma unidade de recobro. Na áera de logística, apenas o PGS e o SIGMA-ABAST/SIAGFA-GM têm alternativa. No

primeiro apenas para visualização, no segundo baseada em listagens em papel que rapidamente ficam desactualizadas. Por último, na área operacional, os dois SI têm processos alternativos. No SIAGFA-MGO esses procedimentos alternativos não estão escritos; no Winventus o processo alternativo é baseado na utilização do telefone e do fax o que requer um aumento dos quantitativos de pessoal.

Da análise destes resultados pode concluir-se que há uma grande dependência dos SI. Os processos alternativos ou não existem ou são ineficazes, traduzindo-se numa incapacidade de resposta que, nalguns casos, compromete o cumprimento da missão.

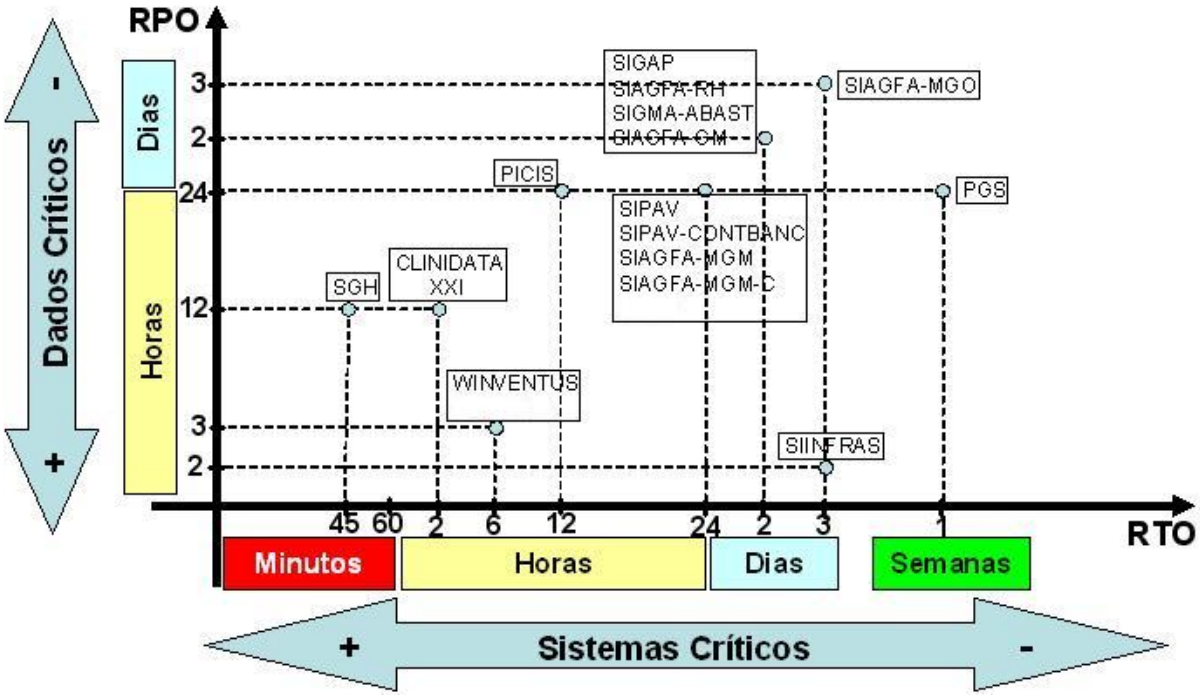
Outro dos aspectos importantes da análise de impacto realizada está relacionado com a percepção que os responsáveis têm da criticidade dos SI. Para medir este valor contribuem, principalmente, dois indicadores: RTO e RPO. O primeiro corresponde ao tempo que os processos da organização conseguem funcionar sem suporte dos SI, ou seja, os sistemas críticos que necessitam de uma resposta rápida em termos de recuperação e disponibilidade. O segundo corresponde à quantidade máxima aceitável de perda de dados, isto é, os considerados críticos e para os quais pode, ou não, existir capacidade de reintrodução.

Dos resultados verificados na área de pessoal, o sistema mais crítico é o SGH e os menos críticos são o SIGAP e o SIAGFA-RH. Quanto aos dados, o CLINIDATA XXI, de apoio ao laboratório de análises do HFA, é o sistema com mais elevada criticidade considerando-se aceitável a perda de dados das últimas 12H (com capacidade de reintrodução).

Na área de logística, os dois módulos de apoio à manutenção de aeronaves do SIAGFA são os mais críticos, enquanto que o PGS é o menos crítico devido à alternativa existente, que permite continuar a dar resposta até uma semana após a indisponibilidade do sistema. Em relação aos dados, o SIINFRAS, com apenas duas horas, é o mais crítico.

Por último, na área operacional, o Winventus é o mais crítico quer quanto ao sistema quer quanto aos dados.

A Figura 1 – Sistemas Críticos x Dados Críticos permite-nos ter uma visão global e integrada dos indicadores RTO e RPO.



(Fonte: Elaborado pelo autor)

Figura 1 – Sistemas Críticos x Dados Críticos

Em termos gerais, o sistema mais crítico é o SGH com apenas 45 minutos de RTO. Sendo um sistema composto por vários módulos e que permite efectuar a gestão dos utentes do HFA, o impacto na gestão da actividade hospitalar é elevado. Quanto aos dados, os mais críticos são os do SIINFRAS, com apenas duas horas de janela de tempo.

Após esta caracterização dos SI estão criadas as condições que permitem responder à pergunta derivada "Qual o impacto na Força Aérea em caso de indisponibilidade dos seus Sistemas de Informação?". Pela análise efectuada pode concluir-se que, em caso de indisponibilidade dos SI, o impacto provocado na Organização é elevado.

Este impacto traduz-se na incapacidade de responder às necessidades das diversas áreas, devido à inexistência de processos alternativos aos SI e à criticidade dos dados e dos próprios sistemas.

Como não existe definido um Plano de Continuidade de Serviços, no âmbito dos SI, e foram identificados requisitos de alta disponibilidade em relação à informação e aos sistemas que a suportam, conclui-se que a primeira hipótese "A inexistência de um plano de continuidade de serviços, para os Sistemas de Informação, tem um elevado impacto na Força Aérea" está assim confirmada.

Para a verificação da segunda hipótese torna-se importante analisar a infra-estrutura tecnológica de suporte aos SI.

Como resultado da análise de impacto foram identificadas as TI que suportam os SI em estudo, assim como as vulnerabilidades que apresentam e as medidas de controlo existentes.

Em primeiro lugar, importa classificar o Centro de Dados do EMFA de acordo com as classificações *Tier* do *Uptime Institute*, que são interpretadas como níveis de disponibilidade e confiabilidade dos serviços disponibilizados.

Em termos de distribuição de energia e do circuito de ar condicionado, o Centro de Dados apresenta um nível de redundância que permite classificá-lo de *Tier IV* (infra-estrutura tolerante a falhas). No entanto, apresenta alguns pontos únicos de falha como, por exemplo, o *switch* central que interliga todos os servidores do Centro de Dados à RIGFA. Isto significa que se o *switch* avariar os serviços serão interrompidos, provocando indisponibilidade dos SI. Este facto, de acordo com as regras de classificação, faz com que o Centro de Dados do EMFA seja classificado como *Tier III* (manutenção simultânea), o que equivale a uma disponibilidade de 99,982% (indisponibilidade de 1,6H/Ano).

Apesar do esforço desenvolvido em dotar os sistemas com capacidade de alta disponibilidade, existem cinco SI (SIGAP, PGS, SIINFRAS, PICIS e CLINIDATA XXI) que são suportados apenas por um servidor de base de dados e/ou aplicacional, o que se traduz num ponto único de falha.

Por outro lado, alguns SI identificados como tendo um elevado impacto, estão alojados em Centros de Dados que não apresentam os requisitos de alta disponibilidade e resiliência de acordo com a sua criticidade. Estão nesta situação o Winventus (no CA), o PGS (na BA6) e o SGH, PICIS e CLINIDATA XXI (no HFA).

Em todos os Centros de Dados, excepto o do EMFA, existe apenas um suporte para a instalação dos servidores (ponto único de falha).

Quanto à RIGFA, apesar das melhorias introduzidas, largura de banda e redundância na rede de comunicações, o facto da sua topologia ser em estrela com um ponto central no CA faz com que exista um ponto único de falha. Deste modo, a ligação entre o Centro de Dados Principal e o Centro de Dados Alternativo será comprometido caso o ponto central no CA avarie.

A presença 24H/7 de um operador especializado no Centro de Dados do EMFA permite monitorar os componentes críticos da infra-estrutura TI e actuar prontamente em caso de ocorrência de alguma anomalia, que possa comprometer a disponibilidade de serviços.

Estão também implementadas outras medidas de controlo, nomeadamente sistemas de anti-fogo, controlo de humidade e temperatura, servidores com fontes de alimentação redundantes, contratos de suporte de *hardware* 24x7 com 4 horas de resposta e são realizadas diariamente cópias de segurança.

Após a análise à infra-estrutura tecnológica da FAP estão criadas as condições para responder à segunda pergunta derivada "Poderá a actual infra-estrutura de Tecnologias de Informação da Força Aérea comprometer a continuidade de serviços?". Resulta dessa análise a evidência de que na presença de um evento que afecte os Centros de Dados ou os seus equipamentos não redundantes, haverá uma interrupção dos serviços disponibilizados.

Assim, a hipótese "A actual infra-estrutura de Tecnologias de Informação da Força Aérea garante a continuidade de serviços." é refutada.

A análise anterior permite, através de um método dedutivo, responder à pergunta central desta investigação: "Que metodologia deve ser adoptada pela Força Aérea que permita assegurar, em caso de interrupção de serviços, a disponibilidade dos Sistemas de Informação?".

Como se verificou, a inexistência de um PCS tem um elevado impacto na Organização. Ficou demonstrado que há uma grande dependência dos SI e que não existem, nalguns casos, procedimentos alternativos definidos ou devidamente testados.

Da análise de impacto efectuada foi possível avaliar os dois indicadores extremamente importantes para a definição da metodologia a adoptar em caso de interrupção de serviços: RTO e RPO, que permitem saber quais os dados e sistemas mais críticos.

De acordo com as técnicas de recuperação identificadas no capítulo um, o método de *backup* é indicado para sistemas que permitem perda de dados superior a um dia e para aplicações consideradas não críticas, com tempos de recuperação entre as 24 e as 72 horas. A replicação síncrona é indicada para sistemas em que não é admissível a perda de dados (*Zero Data Lost*). A replicação assíncrona é para os SI cuja perda de dados varia entre alguns minutos e as duas horas.

Na FA existem quatro SI em que a perda de dados admissível se situa entre as duas e as doze horas. Em termos de indisponibilidade há quatro sistemas que requerem uma recuperação inferior a doze horas (o SGH apenas 45 minutos).

De acordo com estas necessidades, conclui-se que a técnica de recuperação mais adequada aos SI da FA é a replicação assíncrona entre o Centro de Dados Principal, no EMFA, e um Centro de Dados Alternativo.

No entanto, como a infra-estrutura de TI não assegura a continuidade de serviços, para que seja implementada uma metodologia que garanta a disponibilidade dos SI deverão primeiro ser criadas as condições necessárias, ou seja, identificação e preparação, num local geograficamente distante de Alfragide, de um Centro de Dados Alternativo num dos Centros de Dados intervencionados.

Neste capítulo, que se enquadra na fase de verificação, de acordo com a metodologia de investigação seguida, foram analisados os resultados obtidos através das entrevistas efectuadas aos diversos responsáveis pelos SI/TI da FAP.

Verificou-se que há uma grande dependência dos SI, que a inexistência de um Plano de Continuidade de Serviços tem um elevado impacto na Organização e que a actual infra-estrutura de TI não garante a continuidade de serviços, comprometendo a disponibilidade dos SI.

Conclusões

A continuidade de serviços, no âmbito dos SI, tem actualmente uma grande importância para as organizações. A dependência de um recurso vital como é a informação, releva a necessidade dos sistemas que a armazenam, processam e transmitem estejam permanentemente disponíveis.

A FAP, como uma Organização moderna e dependente dos seus SI, não possui um plano que garanta o acesso à informação em caso de interrupção de serviços que provoque a indisponibilidade desses sistemas.

As conclusões deste trabalho visam contribuir, através de um conhecimento mais aprofundado sobre esta problemática, com um conjunto de orientações e a indicação de uma metodologia que sirvam de base à elaboração de um PCS.

Esta investigação seguiu as várias fases das etapas do procedimento metodológico proposto: elaboração da pergunta de partida, fase exploratória, definição da problemática, construção do modelo de análise, observação, análise de resultados e conclusões.

Na fase inicial foi criado o quadro teórico de referência para tratamento do problema identificado, estabelecendo-se os conceitos estruturantes relativos à pergunta de partida. O modelo de análise caracteriza esses conceitos sob a forma de dimensões, componentes e indicadores que serviram de orientação para a recolha de informação, de modo a validar as hipóteses.

No primeiro capítulo enquadrou-se o tema quanto à problemática em estudo, salientando a importância de um PCS. Foi referido que, antes de se equacionar o planeamento, deve garantir-se uma infra-estrutura de TI resiliente. Medidas como a redundância dos sistemas de fornecimento de energia e refrigeração, a definição de uma política de segurança de informação, a existência de equipas de monitorização e a implementação de soluções tecnológicas tolerantes a falhas deverão ser observadas de modo a aumentar a disponibilidade dos SI. Foram apresentados os parâmetros definidos pelo *Uptime Institute* e que permitem classificar os Centros de Dados quanto à sua disponibilidade e tolerância a falhas.

Pela caracterização dos Centros de Dados quanto à sua disponibilidade, concluiu-se que esta limita a disponibilidade geral da infra-estrutura de TI e, por conseguinte, os SI.

De seguida verificou-se que nem todos os eventos que provocam uma interrupção de serviços necessitam que se active o PCS. A alta disponibilidade, assente numa plataforma tecnologicamente redundante, permite, por si só, que os vários tipos de

indisponibilidade sejam minimizados e garante o cumprimento dos SLA estabelecidos. Só em caso de um sistema ficar indisponível por um período superior ao definido é que a situação poderá evoluir de um problema de indisponibilidade para um problema de continuidade de serviços.

Segundo os autores consultados, uma das tarefas iniciais de um PCS é a elaboração da análise de impacto. Os SI deverão ser caracterizados de acordo com vários indicadores, nomeadamente, as TI que os suportam, a identificação das vulnerabilidades (SI/TI), o impacto na organização em caso de indisponibilidade e, principalmente, o indicador que permite quantificar a perda de dados máxima admissível (RPO) e o indicador que define o período de tempo máximo aceitável de indisponibilidade (RTO).

Por último, foram caracterizadas as técnicas de recuperação de dados, de acordo com a criticidade dos sistemas e dos dados.

Essas técnicas baseiam-se, fundamentalmente, na cópia dos dados para *tape* (e posterior reposição no mesmo local ou num local alternativo) e na replicação para um Centro de Dados Alternativo, através da cópia dos dados de uma unidade de armazenamento para outro equipamento similar. A primeira é a mais simples de implementar mas tem grandes desvantagens como, por exemplo, a grande quantidade de dados perdidos (normalmente um dia) e o elevado tempo de recuperação, tipicamente 24 a 72 horas. A replicação poderá ser de dois tipos: síncrona (em tempo real) ou assíncrona (desfasada no tempo), dependendo apenas da quantidade aceitável de dados perdidos, zero para a síncrona e de minutos a poucas horas no caso da assíncrona.

Os dados obtidos através das entrevistas efectuadas aos responsáveis pelos SI/TI foram apresentados no capítulo dois. Com base na análise de impacto e nas classificações *Tier* do *Uptime Institute* foi recolhida a informação necessária à caracterização dos SI e TI.

Existem na FAP 117 SI em exploração. Nesta investigação apenas foram analisados os que a DIVCSI considerou, no âmbito das suas competências e sujeito a aprovação superior, como os mais críticos (Prioridade 1) e cuja indisponibilidade poderá ter um maior impacto na Organização. Estes SI foram agrupados em três áreas: Pessoal (sete), Logística (seis) e Operacional (dois).

Em relação à infra-estrutura TI, existem 17 Centros de Dados interligados entre si através da RIGFA. Destes, sete foram intervencionados e reestruturados de modo a dotá-los com os mais modernos sistemas de arrefecimento e fornecimento de energia. Possuem a capacidade de funcionamento redundante, 2N para os sistemas de frio (existem dois sistemas iguais sendo necessário apenas um para sustentar o funcionamento) e N+1 para os

sistemas de energia (o sistema tolera a falha de um dos vários módulos que o constituem). Foi também instalada uma solução de alta disponibilidade, para alguns SI, que consiste na utilização de servidores que fornecem o mesmo serviço partilhando um equipamento de armazenamento de dados. Os SI em estudo estão instalados em quatro destes Centros de Dados (EMFA, CA, HFA e BA6).

Para a implementação de um PCS deverá existir uma rede de comunicações redundante e uma largura de banda que permita a transferência de dados.

As redes de comunicações de micro-ondas da FAP e do SICOM servem de suporte à RIGFA, que assenta numa topologia em estrela com um ponto central (*router*) no CA. Esta estrela tem algumas pontas ligadas directamente entre si, não com a intenção de aumentar a largura de banda mas com o objectivo da redundância.

No capítulo três, tendo como objectivo a verificação das hipóteses, realizou-se uma análise empírica dos dados observados, obtidos através das diversas entrevistas efectuadas aos responsáveis pelos SI/TI.

Dessa análise resultou a confirmação da primeira hipótese e a resposta à primeira pergunta derivada: o impacto provocado na Organização, em caso de indisponibilidade dos SI, é elevado. Este impacto traduz-se na incapacidade em dar resposta às necessidades das diversas áreas, devido à inexistência de processos alternativos e à conclusão de que os dados e os sistemas são considerados críticos, de acordo com os indicadores apurados.

Como não existe definido um PCS para os SI e foram identificados requisitos de alta disponibilidade em relação à informação e aos sistemas que a suportam, concluiu-se que a primeira hipótese “A inexistência de um plano de continuidade de serviços, para os Sistemas de Informação, tem um elevado impacto na Força Aérea” estava confirmada.

Para a verificação da segunda hipótese e resposta à segunda pergunta derivada, foi possível concluir que da análise efectuada resultou a evidência de que na presença de um evento que afecte os Centros de Dados ou os seus equipamentos não redundantes, haverá uma interrupção dos serviços disponibilizados.

Existem várias vulnerabilidades na infra-estrutura de TI, nomeadamente vários pontos únicos de falha, que não garantem a redundância e alta disponibilidade necessárias à continuidade de serviços. Assim, foi refutada a hipótese “A actual infra-estrutura de Tecnologias de Informação da Força Aérea garante a continuidade de serviços.”.

A utilização de um método dedutivo permitiu responder à pergunta central desta investigação: “Que metodologia deve ser adoptada pela Força Aérea que permita

assegurar, em caso de interrupção de serviços, a disponibilidade dos Sistemas de Informação?".

Da análise efectuada, verificou-se que a inexistência de um PCS tem um elevado impacto na Organização. Ficou demonstrado que existe uma grande dependência dos SI e que não existem procedimentos alternativos definidos ou devidamente testados.

Foram avaliados dois indicadores extremamente importantes para a definição da metodologia a adoptar: RTO e RPO. Na FAP existem quatro SI em que a perda de dados admissível se situa entre as duas e as doze horas. Em termos de indisponibilidade há quatro sistemas que requerem uma recuperação inferior a doze horas.

De acordo com estas necessidades, conclui-se que a técnica de recuperação mais adequada aos SI da FAP é a replicação assíncrona entre o Centro de Dados Principal, no EMFA, e um Centro de Dados Alternativo.

No entanto, e como a infra-estrutura de TI da FA não assegura a continuidade de serviços, para que seja implementada uma metodologia que garanta a disponibilidade dos SI deverão ser criadas as condições necessárias, ou seja, a identificação e preparação de um Centro de Dados Alternativo, num local geograficamente distante de Alfragide.

Para fazer face a esta situação, torna-se necessário implementar uma solução que permita a continuidade dos serviços a partir de outro local, numa perspectiva de garantia da continuidade de serviços pela capacidade de recuperação dos sistemas e dos dados, pelo que se recomendam as seguintes linhas de acção, que representam um conjunto de orientações para a elaboração de um Plano de Continuidade de Serviços, no âmbito dos Sistemas de Informação da FAP:

a. Estado-Maior

(1) Elaborar documentação doutrinária para a criação de um plano de continuidade de serviços, no âmbito dos SI da Força Aérea;

(2) Promover a elaboração e actualização contínua da Análise de Impacto aos SI, sempre que existam novos sistemas ou que se alterem os pressupostos de exploração dos existentes;

(3) Promover, junto dos responsáveis pelos SI, a definição de procedimentos alternativos, onde aplicável, que permitam minimizar o impacto da indisponibilidade dos SI.

b. CLAFA/DCSI

(1) Identificar e instalar um Centro de Dados Alternativo, geograficamente distante de Alfragide;

(2) Centralizar no Centro de Dados do EMFA os SI críticos;

(3) Eliminar ou minimizar os vários pontos únicos de falha existentes na infra-estrutura de TI de modo a aumentar a disponibilidade dos SI;

(4) Garantir a redundância de comunicações e largura de banda suficientes para a transferência de dados entre o Centro de Dados do EMFA e o Centro de Dados Alternativo.

O trabalho efectuado permitiu constatar que há uma grande dependência nos SI e que a inexistência de um Plano de Continuidade de Serviços tem um elevado impacto na Organização. Por outro lado, a actual infra-estrutura de TI não garante a continuidade de serviços, comprometendo a disponibilidade dos SI e o acesso atempado à informação necessária de uma forma credível e actualizada.

Esta investigação pretende também ser um contributo, e de algum modo um alerta, para a particular acuidade da problemática da continuidade de serviços. Não é imaginável que uma organização como a Força Aérea corra riscos que possam comprometer as suas operações e missão, motivadas pela indisponibilidade da informação e dos seus sistemas.

Deve ser considerada, ao mais alto nível, a existência de um plano que garanta o acesso à informação vital e cuja recuperação e disponibilidade sejam consideradas prioritárias.

A Força Aérea tem os mecanismos e, mais importante, as pessoas com a competência técnica e o profissionalismo necessários para a implementação de um Plano de Continuidade de Serviços, no âmbito dos seus Sistemas de Informação.

Glossário

Backup: Processo que consiste na cópia de segurança de dados para um dispositivo de armazenamento.

Cluster: Conjunto de máquinas interligadas via rede que cooperam entre si para atingir um objectivo comum. O objectivo é alta disponibilidade e alto desempenho.

Dados: Representação da informação sob uma forma convencional adequada à comunicação, à interpretação ou ao processamento.

Hardware: Totalidade ou parte dos componentes físicos de um sistema de processamento de informação, (ex: Computadores, Servidores, Periféricos).

Informação: Significado atribuído aos dados por meio de convenções utilizadas na sua representação. É o resultado do processamento, manipulação e organização de dados, de tal forma que represente uma modificação (qualitativa ou quantitativa) no conhecimento do sistema que a recebe.

Largura de Banda: Capacidade para se transferir informação através de uma rede. Medida em bits por segundo.

Ponto Único de Falha: Qualquer componente da infra-estrutura tecnológica sem redundância ou meios de controlo e que em caso de avaria pode representar um interrupção total de serviços.

Replicação: Consiste na cópia dos dados de um disco ou conjunto de discos, para outro equipamento similar dedicado a armazenar exactamente os mesmos dados.

Replicação Assíncrona: Replicação de dados desfasada no tempo.

Replicação Síncrona: Replicação de dados em tempo real.

Resiliência: Capacidade de superar ou recuperar de adversidades.

Restore: Reposição dos dados a partir de uma cópia de segurança.

Router: Unidade funcional que estabelece um caminho através de uma ou mais redes de computadores.

Sistemas Cooperativos ou de "*Workgroup*": Permitem a execução de tarefas típicas de ambiente de escritório. Neste segmento enquadram-se as ferramentas de correio electrónico, gestão documental, folhas de cálculo, processamento de texto, entre outras (Alter, 1999).

Sistemas Estratégicos: Sistemas que fornecem informação estratégica para apoio à tomada de decisão, através de indicadores obtidos pela conjugação de diversas variáveis de informação. Privilegiam o processamento de elevadas quantidades de informação, em

detrimento de tempos de resposta ou elevada disponibilidade. Destinam-se ao nível de topo da organização (Alter, 1999).

Sistema de Informação Crítico: Um Sistema de Informação é considerado crítico porque, independentemente da duração da indisponibilidade e da altura do mês em que ocorra, não existe processo alternativo ou é incipiente ou não está devidamente testado. A criticidade é extensível à infra-estrutura de Tecnologias de Informação que o suporta (Toigo, 2003).

Sistemas de Informação de Gestão: Permitem efectuar a análise dos dados disponíveis, convertendo-os em informação para apoio ao nível de decisão intermédio (Alter, 1999).

Sistemas Operacionais ou Transaccionais – Sistemas que suportam as operações diárias da organização. Permitem a execução de tarefas específicas, com base em regras e procedimentos bem definidos, suportando grandes volumes de transacções. Apresentam como requisitos desempenho e disponibilidade elevadas. São sistemas vitais ao funcionamento da organização (Alter, 1999).

Software: Totalidade ou parte dos programas, dos procedimentos, das regras e da documentação associada, pertencentes a um sistema de processamento de informação.

Switch: Unidade funcional que liga dois ou mais equipamentos terminais de processamento de dados, e permite a utilização exclusiva de um circuito de dados entre eles, até terminar a conexão.

Unidades de Armazenamento: é um dispositivo capaz de gravar (armazenar) informação (dados).

Vulnerabilidade: A vulnerabilidade é uma falha na concepção de um sistema, na sua execução ou nos controlos que existem para o proteger e que pode resultar em danos quando é accionada acidentalmente, ou intencionalmente explorada.

Bibliografia

Livros

– ALTER, S. (1999). *Information systems*: *A Management Perspective*. 3th ed. Addison Wesley.

– JARDIM, Nuno, SERRANO, António (2007). *Disaster Recovery*: Um paradigma na Gestão da Continuidade. FCA Editora de Informática, LDA.

– PEPPARD, Joe, WARD, John (2003). *Strategic Planning for Information Systems*. 3th ed. UK. John Wiley & Sons, LTD.

– PIEDAD, F. & HAWKINS, M. (2000). *High Availability: Design, Techniques and Processes*, Prentice Hall PTR.

– QUIVY, Raymond; CAMPENHOUDT, Luc Van. (2008). Manual de Investigação em Ciências Sociais. 5ª ed. Lisboa: Gradiva.

– TOIGO, Jon William (2003). *Disaster Recovery Planning: preparing for the unthinkable*. 3th ed. USA. Prentice Hall.

– WEYGANT, P.S. (2001). *Clusters for High Availability: A Primer of HP Solutions*.

Publicações Militares

– Plano Director dos Sistemas de Informação da Força Aérea de 3 de Julho de 2009. Alfragide: DIVCSI.

– RFA 390-1 (A) (2000). Política de Sistemas de Comunicações e de Informação da Força Aérea. Alfragide: FAP.

– RFA 390-3 (2008). Política de Segurança da Informação e dos Sistemas de Informação e Comunicações na Força Aérea. Alfragide: FAP.

– RFA 390-4 (2009). Organização e Estrutura de Segurança dos Sistemas de Informação e Comunicações da Força Aérea. Alfragide: FAP.

Internet

– BETAN, Harvey (2010). *How to determine the appropriate failover disaster recovery site: hot, cold or warm*, [referência de 8 de Março de 2010]. Disponível na Internet em: <http://searchdisasterrecovery.techtarget.com>.

– BOGGS, Raymond, BOZMAN, Jean S., PERRY, Randy (2009). *Reducing Downtime and Business Loss: Addressing Business Risk with effective Technology*, IDC White Paper

[em linha], [referência de 15 de Dezembro de 2009]. Disponível na Internet em <http://www.hp.com/hpinfo/newsroom/press_kits/2009/CompetitiveEdge/ReducingDowntime.pdf>.

– FONSECA, Francisco (2004). Plano de Continuidade de Negócio. Semanário Económico [em linha], [referência de 23 de Novembro de 2009] Disponível na Internet em <http://www.compromissoportugal.pt/docs/ficheiros/Plano_de_Continuidade_de_Negocio.pdf>.

– Business Continuity Institute. Promoting the art and science of Business Continuity Management worldwide, [referência de 14 de Novembro de 2009]. Disponível na Internet em <http://www.thebci.org/>.

– Business Continuity Management Institute. The Institute for Business Continuity, [referência de 17 de Novembro de 2009]. Disponível na Internet em <http://www.bcm-institute.org/bcmi10/>.

– Business Standards, [referência de 5 de Janeiro de 2010]. Disponível na Internet em <http://www.businessstandards.com/index.xalter>.

– Conducting a Business Impact Analysis, [referência de 5 de Janeiro de 2010]. Disponível na Internet em <http://www.training-hipaa.net/template_suite/BIA_guide.htm>.

– Data Center Knowledge, [referência de 3 de Dezembro de 2009]. Disponível na Internet em <http:// www.datacenterknowledge.com/>.

– Disaster Recovery Planning, [referência de 5 de Janeiro de 2010]. Disponível na Internet em <http://www.drplanning.org/portal/>.

– Federal Financial Institutions Examination Council. *Information Security* [em linha], [referência de 27 de Dezembro de 2009]. Disponível na Internet em http://www.ffiec.gov/ffiecinfobase/booklets/information_security/infosec_toc.htm>.

– Global Security. Reliable Security Information, [referência de 17 de Novembro de 2009]. Disponível na Internet em <http://globalsecurity-whitepapers.tradepub.com/>.

– Government Information Security, [referência de 17 de Novembro de 2009]. Disponível na Internet em <http://www.govinfosecurity.com/articles.php?art_id=1725>.

– IT Governance. Specialist services and solutions for IT governance, risk management, compliance and information security, [referência de 29 de Dezembro de 2009]. Disponível na Internet em <http://www.itgovernance.co.uk/>.

– ITIL: Continuity Management, Contingency Planning, Disaster Recovery, Business Continuity, [referência de 12 de Fevereiro de 2010]. Disponível na Internet em <http://www.itil-itsm-world.com/itil-8.htm>.

– ITSMF the IT Service Management Forum, [referência de 15 de Fevereiro de 2010]. Disponível na Internet em <http://www.itsmf.pt/Inicio/tabid/36/Default.aspx>.

– National Institute of Standards and Technology. Information Technology Laboratory. Computer Security Resource Center, [referência de 12 de Fevereiro de 2010]. Disponível na Internet em <http://csrc.nist.gov/publications/>.

– NATO Computer Incident Response Capability. Technical Center, [referência de 17 de Novembro de 2009]. Disponível na Internet em <http://www.ncirc.nato.int>.

– Nonprofit Risk Management Center. Business Continuity Planning Course [em linha], [referência de 27 de Dezembro de 2009]. Disponível na Internet em <http://nonprofitrisk.org/tools/business-continuity/intro/1.htm>.

– Uptime Institute. The Global Data Center Authority. *Data Center Site Infrastructure Tier Standard: Topology* [em linha], [referência de 27 de Dezembro de 2009]. Disponível na Internet em <http://www.uptimeinstitute.org/index.php?option=com_docman&task=doc_download&gid=82>.

Entrevistas

– Tópico de Entrevista: As Tecnologias de Informação e a Continuidade de Serviços. Com o Sr. Engenheiro João Batista, Director da Novell, em Alfragide, 18 de Novembro de 2009.

– Tópico de Entrevista: As Tecnologias de Informação da Força Aérea. Com o Sr. MGen Germano Carvalho, em Alfragide, 21 de Dezembro de 2009.

– Tópico de Entrevista: Análise de Impacto dos Sistemas de Informação do HFA. Com o Sr. Maj Luís Cordeiro, via *email*, 09 de Fevereiro de 2010.

– Tópico de Entrevista: Análise de Impacto dos Sistemas de Informação do HFA. Com a Sr.ª Dr.ª Lina Costa, via *email*, 21 de Janeiro de 2010.

– Tópico de Entrevista: Os Sistemas de Informação da Força Aérea. Com o Sr. Cor Luís Damásio, em Alfragide, 18 de Novembro de 2009.

– Tópico de Entrevista: Análise de Impacto dos Sistemas de Informação da área de Logística. Com o Sr. Cor Armindo Gomes, em Alfragide, 12 de Fevereiro de 2010.

– Tópico de Entrevista: As Tecnologias de Informação e os Centros de Dados da Força Aérea. Com o Sr. Maj José Gorgulho, em Alfragide, 16 de Fevereiro e 07 de Março de 2010.

– Tópico de Entrevista: Análise de Impacto dos Sistemas de Informação de apoio ao EH-101. Com o Sr. Maj Eduardo Guerreiro, via *email*, 15 de Janeiro de 2010.

– Tópico de Entrevista: A implementação de um Plano de Continuidade de Serviços. Com o Sr. Cor Carlos Lourenço, Director da RNSI do MAI, via *email*, 30 de Outubro de 2009.

– Tópico de Entrevista: Análise de Impacto dos Sistemas de Informação da área de Pessoal. Com o Sr. TCor Luís Nunes, em Alfragide, 06 de Novembro de 2009.

– Tópico de Entrevista: A rede de comunicações da FA e a RIGFA. Com o Sr. Ten António Oliveira, em Alfragide, 25 de Janeiro de 2010.

– Tópico de Entrevista: Análise de Impacto dos Sistemas de Informação da área Financeira. Com a Sr.ª TCor Paula Passos, em Alfragide, 06 de Novembro de 2009.

– Tópico de Entrevista: Análise de Impacto dos Sistemas de Informação do CIMFA. Com o Sr. TCor Francisco Ramos, via *email*, 04 de Fevereiro de 2010.

– Tópico de Entrevista: Análise de Impacto dos Sistemas de Informação da DI. Com o Sr. TCor Joaquim Salvado, em Alfragide, 25 de Janeiro de 2010.

– Tópico de Entrevista: Análise de Impacto dos Sistemas de Informação da área Operacional. Com o Sr. TCor Saraiva, via *email*, 04 de Dezembro de 2009.

– Tópico de Entrevista: Análise de Impacto dos Sistemas de Informação da área de Logística. Com o Sr. TCor Gustavo Silva, em Alfragide, 13 de Novembro de 2009.

– Tópico de Entrevista: Os Sistemas de Informação da Força Aérea. Com a Sr.ª Maj Ana Telha, em Alfragide, 30 de Outubro e 06 de Novembro de 2009.

Anexo A – Modelo de Análise

Conceitos	Dimensões	Componentes	Indicadores
Análise de Impacto	Sistema de Informação	*Software*	Sistemas Operativos
			Bases de Dados
			Aplicações
		Métodos Alternativos	Papel
			Digital
		Janelas de Tempo	*Recovery Point Objective* (RPO)
			Recovery Time Objective (RTO)
		Dependência	Sistemas de Informação
		Recuperação	Prioridade
		Responsável	Entidade Responsável
			Impacto
			Criticidade
			Vulnerabilidades
	Imagem da Organização		Impacto
Infra-estrutura de TI	Centro de Dados	*Hardware*	Servidores
			Unidades de Armazenamento
			Equipamentos de Rede
			Redundância
			Actualizações
		Software	Sistemas Operativos
			Bases de Dados
			Cópias de Segurança
			Actualizações
		Ambiental	Ar condicionado
			Energia Eléctrica
		Classificação	*Tier*
			Vulnerabilidades
	Rede de Comunicações		Topologia
			Largura de Banda
			Vulnerabilidades
Continuidade de Serviços	Política de *Backups*		Periodicidade
			Tipo de *Backup*
			Rotação de *Tapes*
			Armazenamento
	Replicação de Dados		Síncrona
			Assíncrona
	Centro de Dados Alternativo		Localização Geográfica
			Tipo de Centro de Dados
	Arquitectura Redundante	Alta-Disponibilidade	Servidores
			Unidades de Armazenamento
			Service Level Agreements
	Medidas de Controlo	Monitorização	Local
			Remota
			Turnos
			Cópias de segurança
			Controlo de acessos
			Sistemas anti-fogo
			Sistema anti-humidade
			Controlo temperatura

Anexo B – Classificação dos Centros de Dados[3]

A classificação *Tier* adoptada em Centros de Dados (*Data Centers* ou *Sites*) foi desenvolvida pelo *Uptime Institute*, nos EUA, e é utilizada desde 1995, sendo reconhecida mundialmente. Os níveis de disponibilidade associados às classificações *Tier* foram determinados pelos resultados de análises de disponibilidade a Centros de Dados reais e apresentam valores entre 99,67% e 99,99%.

Estes valores não são estimados e reflectem a operação de Centros de Dados classificados dentro dos quatro níveis *Tier* (I, II, III e IV). A disponibilidade considerada para a determinação desses valores é sensivelmente inferior aos "cinco noves" (99,9999%). Assim, a disponibilidade do Centros de Dados limita a disponibilidade geral dos serviços de TI.

Para uma boa compreensão dos termos usados nas classificações *Tier* de Centro de Dados são importantes algumas definições:

- Componentes reduntantes – São aqueles cuja quantidade é superior ao mínimo necessário para suportar o equipamento de TI. Termos como N+1 e N+2 são normalmente usados nesse caso;
- Capacidade – trata-se de carga máxima com capacidade "N";
- Manutenção simultânea – Significa que qualquer trabalho pode ser executado de forma planeada sem causar impactos nos serviços. Em termos de infra-estrutura, esta característica significa que qualquer elemento pode ser substituído, reparado, testado, configurado, etc. sem causar impacto nos equipamentos de TI.

1. Classificações *TIER*

a. *Tier* I: Básico

É um Centro de Dados sem componentes redundantes e com um ramo de distribuição (eléctrica e outros sistemas) não redundante para atender os equipamentos de TI.

Características:

- Susceptível a interrupções por actividades planeadas e não planeadas;
- Possui um ramo único de distribuição de alimentação eléctrica, bem como para o sistema de climatização, sem componentes redundantes;

[3] Texto adaptado pelo autor a partir de informação disponível em www.uptimeinstitute.org

- Possui distribuição de alimentação eléctrica para os equipamentos de TI e para o sistema de climatização;
- Pode ter ou não UPS e grupos geradores, é um sistema de módulos simples e apresenta vários pontos individuais de falhas;
- Anualmente a infra-estrutura deve ser completamente desligada para realização de serviços de manutenção preventiva e correctiva;
- Erros de operação e falhas espontâneas na infra-estrutura do Centro de Dados podem ocorrer e levarão à interrupção da operação e indisponibilidade de serviços.

b. Tier II: Componentes redundantes para infra-estrutura do site

São Centro de Dados com componentes redundantes e com um ramo único de distribuição (eléctrica e outros sistemas) para atender os equipamentos de TI.

Características:

- Uma falha num componente pode causar impactos na operação dos equipamentos de TI;
- Uma falha no ramo de distribuição eléctrica causará o desligamento dos equipamentos de TI;
- São sites susceptíveis a interrupções por actividades planeadas;
- Módulos UPS redundantes e grupos geradores devem fazer parte da infra-estrutura de alimentação eléctrica desses ambientes;
- Falhas na execução de serviços de manutenção aumentam os riscos de interrupções não planeadas;
- Erros de operação de componentes da infra-estrutura do Centro de Dados podem causar interrupção dos serviços.

c. Tier III: Manutenção simultânea

São Centro de Dados com componentes redundantes e vários ramos de distribuição (eléctrica e outros sistemas) para atender os equipamentos de TI. Normalmente apenas um ramo de distribuição está activo.

Características:

- Cada componente e elemento dos ramos de distribuição de alimentação eléctrica e outros sistemas e subsistemas do site podem ser removidos

conforme planeado sem causar o desligamento de qualquer equipamento de TI;

- O site é susceptível a interrupções por actividades não planeadas;
- A manutenção da infra-estrutura do site pode ser realizada através das capacidades dos componentes redundantes e dos ramos de distribuição;
- Todos os equipamentos de TI precisam de fontes de alimentação redundantes para realização de manutenção simultânea nos sistemas de distribuição eléctrica crítica entre as UPS e os equipamentos de TI;
- Durante as actividades de manutenção o risco de interrupção é elevado;
- Erros de operação ou falhas espontâneas de componentes da infra-estrutura do site podem causar a interrupção dos serviços.

d. Tier IV: Infra-estrutura do site tolerante a falhas

São Centro de Dados tolerantes a falhas com sistemas redundantes e vários ramos de distribuição (eléctrica e outros sistemas) que atendem simultaneamente os equipamentos de TI, que devem ter fontes de alimentação redundantes. Os ambientes *Tier* IV devem ter, pelo menos, dois sistemas de alimentação de energia eléctrica completamente independentes para os equipamentos de TI.

Características:

- Uma falha única de qualquer sistema, componente ou elemento de distribuição não causará a interrupção dos serviços do Centro de Dados;
- Componentes e elementos de distribuição podem ser removidos (ou retirados de serviço) de forma planeada sem causar o desligamento dos equipamentos de TI;
- Sistemas complementares e ramos de distribuição de serviços eléctricos devem ser separados fisicamente para prevenir que eventos isolados causem impactos em ambos os sistemas ou ramos simultaneamente;
- A manutenção da infra-estrutura do site pode ser realizada com as capacidades dos componentes redundantes e dos ramos de distribuição;
- Durante as actividades de manutenção o risco de interrupção dos serviços pode ser elevado;
- A infra-estrutura é mais compatível com os conceitos de alta disponibilidade de tecnologia da informação.

Tabela B1 - Padrões de desempenho por classificação Tier

Elemento	***Tier* I**	***Tier* II**	***Tier* III**	***Tier* IV**
Componente redundante	N	N+1	N+1	N+1 (MÍNIMO)
Ramos de distribuição	1	1	1 Normal e 1 alternativo	2 activos simultaneamente
Separação de sistemas e ramos de distribuição	Não	Não	Sim	Sim
Manutenção simultânea	Não	Não	Sim	Sim
Refrigeração ininterrupta	Não	Não	Talvez	Sim
Pontos únicos de falhas	Vários	Vários	Alguns	Nenhum (excepto incêndio e desligar por emergência)
Tolerante a falhas	Não	Não	Não	Sim
Equipa de Monitorização	Não	Um turno	Um turno	24 X 7 X 365
Manutenção/Reparação	2 x 12h p/ ano	3 intervenções de 2 em 2 anos	-	-
Falhas/ano	1,2 equipamentos ou distribuição	<1 equipamentos ou distribuição	-	-
Impacto anual (h)	28,8	22	1,6	0,4
Disponibilidade (%)	99,67	99,74	99,98	99,99

(Fonte: Adaptado de *Uptime Institute*)

Em resumo, as classificações *Tier* do *Uptime Institute* são definidas pela disponibilidade da infra-estrutura do Centro de Dados, uma vez que as falhas na distribuição podem causar impactos sobre os equipamentos de TI e, consequentemente, interrupção nos serviços. As classificações *Tier* são interpretadas, então, como níveis de disponibilidade e confiabilidade dos serviços oferecidos pelos Centro de Dados. A análise de sites mediante as classificações *Tier*, conforme definidas pelo *Uptime Institute* , é feita atribuindo-se o menor valor *Tier* encontrado para um determinado sistema do Centro de Dados. Assim um Centro de Dados, com sistemas de distribuição eléctrica classificados como *Tier* II e com redundância de encaminhamentos de telecomunicações classificada como *Tier* III, receberá uma classificação geral *Tier* II.

A melhor disponibilidade que se pode obter para a infra-estrutura de distribuição de um Centro de Dados é de 99,99%, para ambientes *Tier* IV.

Anexo C – Técnicas de Recuperação

A elaboração deste anexo é o resultado das seguintes entrevistas:

- Ao Sr. Coronel Carlos Lourenço, Director da Rede Nacional de Segurança Interna do Ministério da Administração Interna, responsável pela recente implementação de uma solução de continuidade de serviços naquele Ministério;
- Ao Sr. Major José Gorgulho, Chefe da Repartição de Tecnologias de Informação da Direcção de Comunicações e Sistemas de Informação;
- Ao Sr. Engenheiro João Batista, Director para a Península Ibérica da empresa de Sistemas Novell, responsável pela indicação e implementação de uma solução de *Disaster* & *Recovery* numa empresa da área de seguros.

Basicamente existem duas técnicas de recuperação de dados:

- Cópias de segurança (Backup);
- Replicação (Síncrona ou Assíncrona).

O *Backup* baseia-se na cópia para uma tape dos dados de um sistema do Centro de Dados Principal (CDP), permitindo o acesso a dados históricos. Por exemplo, se é realizado no sistema um *backup* diário (na FAP é realizado todas as noites) e se for necessário recuperar um ficheiro de há três dias atrás e já não existir no sistema (ex. tiver sido eliminado), é possível recuperá-lo através do *backup* correspondente. Se o sistema falhar, ou um ficheiro for eliminado acidentalmente, ou outro qualquer problema ocorrer, é o *backup* que é muitas vezes utilizado para trazer o sistema e/ou os ficheiros ao seu estado anterior (de funcionamento).

A Replicação de dados consiste na cópia dos dados de uma unidade de armazenamento (*Storage*) para outro equipamento preparado para armazenar o mesmo tipo de dados. Esta replicação pode ser realizada em tempo real (replicação síncrona), ou seja, assim que os dados são modificados no sistema de produção as mesmas modificações são realizadas no sistema de replicação. Desta forma, se um ficheiro é eliminado no sistema de produção, também é eliminado no outro. A ideia é que tudo o que acontece no sistema de produção também aconteça no sistema replicado, seja em tempo real ou com algum atraso(replicação assíncrona).

O *backup* permite repor os dados de um sistema na situação em que se encontravam na altura da cópia de segurança, no entanto todo o trabalho que foi realizado após o último *backup* fica perdido. Já a replicação, num contexto de cópia dos dados do sistema de produção para o sistema de replicação, permite recuperar todos os dados (ou quase todos dependendo do método de replicação) e não perder, por exemplo, os dados produzidos desde o último *backup*.

O *backup* é útil para efectuar a reposição de um sistema em que a perda de dados, desde a última cópia de segurança, não seja considerada crítica. A replicação é usada para garantir que os ficheiros ou alterações de ficheiros realizadas durante o dia, estão sempre disponíveis mesmo quando o sistema for abaixo a qualquer momento.

Caso exista um Centro de Dados Alternativo (CDA), as diferenças entre as técnicas de recuperação estão sistematizadas na seguinte tabela:

Tabela C1 – Comparação das Técnicas de Recuperação

Técnica	Comentários
Backup/ Restore	Neste método de recuperação baseado na técnica *de backup/restore* (*tape*) aplicam-se as seguintes boas práticas: • As *tapes* de *backup*, devem ser armazenadas, em local seguro, perto do CDP, para permitir uma resposta rápida a necessidades operacionais de reposição de configurações/dados. • Adicionalmente, devem ser realizadas cópias das *tapes* e enviadas regularmente (ex. diariamente) para o CDA, de modo a permitir uma mais rápida recuperação em caso de falha do CDP. • Em caso de interrupção de serviços há necessidade de deslocação da equipa do CDP para colocar em funcionamento os sistemas do CDA e aplicar os últimos backups de configurações e dados. • Possui um elevado tempo de recuperação (RTO) (tipicamente 24h a 72h) e perda de dados (RPO) - dependente dos últimos backups disponíveis (tipicamente 1 dia). • Este método está focado na simplicidade.
Replicação Assíncrona	Neste método de recuperação baseada na Unidade de Armazenamento (*Storage*): • Os dados após serem escritos com sucesso na *Storage* do CDP são replicados, por este, para a *Storage* do CDA, não esperando, no entanto, a confirmação de escrita com sucesso nesta última para dar indicação de sucesso de escrita à aplicação. • Desta forma a replicação assíncrona não tem impacto no desempenho das aplicações em produção no CDP. • Neste tipo de replicação pode existir uma diferença (Minutos a poucas Horas) entre os dados da *Storage* do CDP e da *Storage* do CDA, o que se pode traduzir em perda de alguns dados, alguns minutos até duas horas, (impacto nos RPOs) em caso de falha do primeiro. • É necessário garantir que cada alteração das configurações dos sistemas de Produção do CDP é de imediato aplicada nos sistemas do CDA, para minimizar o impacto nos RTOs. dependente fortemente das comunicações – mínimo 200Mbps
Replicação Síncrona	Neste método de recuperação baseada na *Storage*: • Os dados após serem escritos com sucesso na *Storage* local (CDP) são replicados, por este, para a *Storage* remota, aguardando a confirmação de escrita com sucesso na *Storage* remota (CDA) para dar indicação de sucesso de escrita à aplicação. • Desta forma, a replicação síncrona tem impacto no desempenho das aplicações em produção no CDP. • Em caso de erro de escrita na *Storage* remota (CDA) os dados são eliminados na *Storage* local (DC CDP) por forma garantir que as duas *Storages* possuem exactamente os mesmos dados (consistência). • No modelo síncrono em caso de desastre no CDP, o CDA pode ser colocado em produção e o processamento continuar no exacto ponto no tempo em que o CDP caiu. • É necessário garantir que cada alteração das configurações dos sistemas de produção do CDP é de imediato aplicada nos sistemas do CDA, para minimizar o impacto nos RTOs. • Nesta configuração pretende-se ZDL (*Zero Data Lost*) e recuperação imediata (dependente fortemente das comunicações – mínimo 200Mbps).

(Fonte: Elaborado pelo autor)

Anexo D – Sistemas de Informação da Força Aérea[4]

Legenda:

CLS - Classificação

T-Sistemas de Informação Operacionais ou (T)ransaccionais

G - Sistemas de Informação de (G)estão

W-Sistemas de Informação Cooperativos ou de (W)orkgroup

E - Sistemas de Informação (E)stratégicos

PRI – Prioridade de Recuperação

1- Mais Prioritário

3- Menos Prioritário

Tabela D1 – Resumo dos Sistemas de Informação da Força Aérea

Sistema de Informação	Qtd	CLS				PRI		
		T	G	W	E	1	2	3
Área de Pessoal	6	5	1	0	0	2	3	**1**
Área Financeira	11	8	2	0	1	2	4	**5**
Área Logística	20	16	1	0	3	4	5	**12**
Componente Operacional	1	1	0	0	0	1	0	**0**
Inspecção	3	2	1	0	0	0	2	**1**
Entidades Específicas	60	27	0	33	0	0	7	**53**
Adquiridos	16	14	0	2	0	6	4	**5**
Total	**117**	**73**	**5**	**35**	**4**	**15**	**25**	**77**

(Fonte: Elaborado pelo autor)

De acordo com as prioridades de recuperação identificadas pela DIVCSI, no âmbito das suas competências e com base numa análise preliminar sujeita a aprovação superior, apresenta-se, de seguida, uma breve descrição das funcionalidades e potencialidades de cada um desses Sistemas.

De modo a facilitar a compreensão e o potencial impacto que a indisponibilidade desses SI possa ter na Organização, foram agrupados em três áreas funcionais: Pessoal, Logística e Operacional.

1. Descrição dos Sistemas de Informação da Área de Pessoal

Os Sistemas de Informação de Prioridade 1 incluídos nesta área são:

a. SIGAP: Sistema de Informação de Gestão da Área de Pessoal; SIAGFA-RH: Sistema Integrado de Apoio à Gestão da Força Aérea - Módulo de Recursos Humanos

O SIGAP é um sistema de gestão global de dados relativos de pessoal e fornece informação de base a vários SI, numa lógica de integração, partilha e consolidação. O SIAGFA-RH é uma extensão do SIGAP às unidades.

[4] Fonte: DIVCSI

b. SGH: Sistema de Gestão Hospitalar

É um sistema, composto por vários módulos e que permite efectuar a gestão dos utentes do Hospital da Força Aérea (HFA), apoiando a prestação eficaz dos actos médicos.

Estão disponíveis no SGH funcionalidades como a gestão do bloco operatório, pedidos de cirurgias, listas de espera, dados de internamentos, apoio às consultas externas, processo clínico dos doentes, gestão da farmácia do hospital, cuidados de enfermagem e módulo de apoio ao Centro de Medicina Aeronáutica (CMA) para a gestão das revisões do pessoal navegante.

c. PICIS: Sistema de Informação de Cuidados Críticos

O PICIS é um Sistema de Informação integrado para apoio à unidade de cuidados críticos do HFA, nomeadamente anestesia, bloco operatório, recobro e cuidados intensivos.

d. CLINIDATA XXI: Sistema de Gestão do Laboratório de Patologia Clínica do HFA

Este Sistema permite efectuar o registo e controlo de todos os exames realizados pelo Laboratório de Patologia Clínica do HFA. A sua integração com os equipamentos de análise permite a transferência automática de dados, bem como o resultado dos testes efectuados.

e. SIPAV: Sistema de Informação de Processamento Automático de Vencimentos; SIPAV-CONTBANC: Pagamentos por Conta Bancária

Efectuam o processamento automático dos vencimentos dos militares e civis da FA, bem como o seu pagamento através de transferência bancária.

2. Descrição dos Sistemas de Informação da Área de Logística

Nesta área foram identificados seis sistemas de Prioridade 1 que abrangem as áreas de material, manutenção de aeronaves e das infra-estruturas:

a. SIGMA-ABAST: Sistema de Informação de Gestão de Manutenção e Abastecimento; SIAGFA-GM: Sistema Integrado de Apoio à Gestão da Força Aérea - Módulo de Material

O SIGMA-ABAST efectua a componente centralizada de gestão do circuito de abastecimento e controlo de material. Nas unidades operacionais está

disponível o módulo de Gestão de Material do SIAGFA que consiste na extensão do SIGMA-ABAST, permitindo a execução das tarefas do circuito de abastecimento de acordo com as existências locais.

b. SIAGFA-MGM e SIAGFA-MGM-C: Sistema de Informação de Apoio à Gestão da Força Aérea - Módulos de Gestão de Manutenção

O controlo de potenciais de aeronaves e seus componentes, o controlo de configuração de aeronaves, o registo de acções de manutenção, o repositório das cartas de trabalho das Inspecções Programadas de Aeronaves e o controlo de qualificações dos executantes são alguns dos processos do SIAGFA-MGM (módulo local) e SIAGFA-MGM-C (módulo central).

c. PGS: *Portuguese Ground Station*

A PGS é uma aplicação que tem como principal função servir de suporte à Gestão de Configuração do EH101 e controlar o estado dos sistemas instalados no helicóptero.

d. SIINFRAS: Sistema de Informação de Infra-Estruturas

Sistema de informação geográfica na área das infra-estruturas da FA, nomeadamente de servidões, licenciamentos, inventário e arquivo técnico, que disponibiliza informação a todos os órgãos internos que dela necessitem e a entidades civis.

3. Descrição dos Sistemas de Informação da Área Operacional

Existem dois sistemas de Prioridade 1 na componente operacional:

a. SIAGFA-MGO: Sistema Integrado de Apoio à Gestão da Força Aérea - Módulo de Gestão Operacional

Este módulo efectua a gestão da actividade aérea da FA, através das suas vertentes aeronaves, pessoal navegante e missões, produzindo um conjunto de indicadores de gestão. Integra a componente de Autorizações de Sobrevoo e Aterragens (ASA), que tem como objectivo a gestão de autorizações de sobrevoo e aterragens de aeronaves civis em aeródromos militares, bem como o registo de movimentos das mesmas com vista à cobrança de taxas de tráfego. Permite ainda a atribuição de beneficiários da missão, para efeitos de ressarcimento de horas de

voo empregues estando já integrado o processo do cálculo do custo da missão e emissão de facturação.

b. Winventus: Informação Meteorológica

O sistema Winventus recebe, processa e distribui informação meteorológica necessária à actividade da FA e tem ligações a diversos organismos e instituições externas (Instituto de Meteorologia (IM) e Inspecção Geral das Pescas (IGP)).

Nas Tabelas seguintes são apresentados e descritos todos os Sistemas de Informação em exploração na Força Aérea.

Legenda:

EPR – Entidade Primariamente Responsável

CLS - Classificação

T-Sistemas de Informação Operacionais ou (T)ransaccionais

G - Sistemas de Informação de (G)estão

W-Sistemas de Informação Cooperativos ou de (W)orkgroup

E - Sistemas de Informação (E)stratégicos

PRI – Prioridade de Recuperação

1- Mais Prioritário

3- Menos Prioritário

Tabela D2 - SI da Área de Pessoal

Título	Objectivo	E P R	C L S	P R I
SIGAP-Sistema de Informação de Gestão da Área de Pessoal	Gestão global de dados de pessoal, abrangendo áreas como a gestão de carreiras e promoções, cursos, funções, justiça e disciplina e cadastro do indivíduo. É o sistema que fornece a informação de base dos indivíduos a todos os outros sistemas.	DP	T	1
SIGAP-MCR- Módulo de Consulta Rápida do SIGAP	Consulta de informação específica de um indivíduo ou de universos de indivíduos. Produção de indicadores de gestão e mapas de trabalho que servem como base ao processo de tomada de decisão em diferentes níveis. A informação é obtida a partir do SIGAP.	DP	G	2
SIAGFA-RH- Módulo de Recursos Humanos do SIAGFA	Constituindo uma extensão do SIGAP às unidades, o Módulo de Recursos Humanos do SIAGFA fornece um conjunto de funcionalidades destinadas à gestão local de pessoal, efectuando o acompanhamento do indivíduo desde o processo administrativo de apresentação até ao desquite. Dispõe de mecanismos de *workflow* para os processos de emissão de guia de marcha e de licenças, bem como planeamento de férias, controlo da condição física, registo e controlo da execução de testes médicos e vacinas, controlo de efectivos, gestão de escalas de serviço, gestão de planos de mobilização, gestão de sorteios de pessoal para variadas finalidades, gestão de destacamentos e de cursos ministrados na unidade.Integrado com este sistema existe um conjunto de funcionalidades disponibilizadas via *web* para controlo dos alunos da AFA (gestão de marcações	DP	T	1

Título	Objectivo	E P R	C L S	P R I
	de entradas, saídas e refeições).			
SIAMMFA-Sistema de Informação de Avaliação de Mérito dos Militares da FA	Recolha das Fichas de Avaliação Individual (FAI) dos militares e, com base nas mesmas, produção de relatórios destinados a análise em conselho de especialidade ou a processos de renovação de contrato.	DP	T	3
SIAGFA-CRM- Módulo de Recrutamento do SIAGFA	Gestão integrada do recrutamento na Força Aérea, através da recepção de candidaturas (processo efectuado via *web*, através do *site* do Centro de Recrutamento da Força Aérea) e posterior validação, gestão de candidatos, gestão de concursos de admissão à Força Aérea, seriação e ordenação de candidatos/candidaturas e recolha de dados dos candidatos admitidos para posterior disponibilização nos sistemas de gestão de dados de Pessoal.	CRFA	T	2
SIAGFA-SGE- Módulo de Gestão Escolar do SIAGFA	Concebido para suprir as necessidades de gestão de uma unidade de formação específica (o CFMTFA), permite controlar o percurso escolar dos formandos, gerir formadores (disciplinas, faltas, horários), gerir a componente académica (escolas, cursos, turmas), o grupo de formação (áreas, núcleos), elaborar cronogramas e planos curriculares, gerir horários, aulas, turmas e sumários, emitir certificados, diplomas, relatórios, efectuar análise estatística, produzir o calendário escolar e efectuar a gestão logística subjacente à componente escolar (alojamentos, salas de aula, manuais).	DP	T	2

Tabela D3 - SI da Área Financeira

Título	Objectivo	E P R	C L S	P R I
SIPAV-Sistema de Informação de Processamento Automático de Vencimentos	Processamento automático dos vencimentos dos indivíduos, tendo como suporte da informação pessoal dos mesmos o SIGAP.	DFFA	T	1
Complementos de Pensão	Cálculo dos complementos de pensão a abonar a militares da Força Aérea na situação de reserva ou reforma.	DFFA	T	2
SIPAV-CONSHIST- **C**onsulta aos Históricos do SIPAV	Consulta a informação histórica do SIPAV.	DFFA	G	3
SIPAV-CONTBANC Processamento de Pagamentos por Conta Bancária	Processamento do pagamento de vencimentos e ajudas de custo nacionais e estrangeiras por transferência bancária.	DFFA	T	1

Título	Objectivo	E P R	C L S	P R I
ADM-Assistência na Doença aos Militares	Gestão do cadastro dos beneficiários da ADM, bem como dos respectivos pedidos de emissão de cartões.	DP	T	2
HISTADMFA-Consulta de Históricos da ADMFA	Consulta ao histórico de comparticipações aos anteriores beneficiários da ADMFA.	DFFA	G	3
SIPPO-Sistema de Informação do Planeamento, Programação e Orçamento	Elaboração do orçamento anual da Força Aérea por programas, execução da conta-programa, apuramento de desvios e classificação de despesas (vencimentos, ajudas de custo, entre outras).	DFFA	T	2
CORC-Controlo Orçamental das Unidades da Força Aérea	Controlo orçamental, abrangendo orçamentos das Unidades, cabimentos, facturação, pagamentos a fornecedores e transferências interbancárias.	DFFA	T	2
CTB-Contabilidade	Controlo da contabilidade das Unidades e emissão das respectivas contas de gerência. Disponível actualmente apenas para consulta ao histórico.	DFFA	T	3
SICOR-Sistema de Informação de Controlo Orçamental das Direcções Técnicas	Preparação orçamental das Unidades da Força Aérea. Permite ainda a pré-cabimentação das Direcções Técnicas, bem como a obtenção de indicadores de gestão associados à Lei de Programação Militar (LPM).	DFFA	T	3
SIAGFA-PROT-Programação Orçamental Temática	Programação anual da execução orçamental com vista a fornecer Indicadores de Gestão aos órgãos de topo da Força Aérea. Constitui um meio de orientação permanente a quem tem responsabilidades na programação orçamental.	DFFA	E	3

Tabela D4 - SI da Área Logística

Título	Objectivo	E P R	C L S	P R I
CHV-Custo da Hora de Voo	Obtenção, a partir de outros sistemas, dos factores de custo para cálculo do custo da hora de voo e disponibilização destes valores. Disponível apenas para consulta, dado que parte das fontes de dados para o referido cálculo transitou para o SIG.	EMFA DIVREC	E	3
CHV-PC-Custo da Hora de Voo – versão para PC	Obtenção, a partir de outros sistemas, dos factores de custo para cálculo do custo da hora de voo e disponibilização destes valores. Disponível apenas para consulta, dado que parte das fontes de dados para o referido cálculo transitou para o SIG.	EMFA DIVREC	E	3
SIGA-Sistema de Informação de Gestão de Alimentação	Planeamento e controlo do fornecimento de alimentação na Força Aérea.	DAT	T	3

Título	Objectivo	EPR	CLS	PRI
SIGMA-ABAST-Sistema de Informação de Gestão de Manutenção e Abastecimento – Módulo de Abastecimento	Efectuar a componente centralizada de gestão do circuito de Abastecimento e controlo de material, nomeadamente: controlo de artigos e substitutos, controlo de existências nas Unidades e no DGMFA, bem como de consumos por código de aplicação, entre outros.	DAT	T	1
SIGMA-MCR-Módulo de Consulta Rápida do SIGMA	Consulta a informação obtida a partir do SIGMA-ABAST, produzindo indicadores de gestão e mapas de trabalho destinados aos gestores.	DAT	G	3
SIGMA-EMP-Controlo de Reparações e Calibrações de Equip. de Medida e Precisão	Controlo de reparações e calibrações dos equipamentos de medida e precisão, produzindo indicadores de gestão.	DEP	T	2
APL-Códigos de Aplicação	Gestão de códigos de aplicação/equipamento, relacionados com a referência do fabricante.	DAT	T	3
CER-Códigos de Entidades Reparadoras	Gestão de códigos de entidades reparadoras e códigos de fabricantes.	DAT	T	3
SILO-Sistema de Informação Logístico	Gestão de pedidos de consulta para execução em diferido, bem como consultas ao CARDEX e ao histórico de movimentos do SIGMA-ABAST.	DAT	T	3
SIES-Sistema de Informação de Encomendas de Serviço	Gestão de encomendas de serviço efectuadas pelas Direcções técnicas a entidades reparadoras.	DMSA	T	2
SIAO-Módulo de Análise de Óleos do SIAGFA	Gestão de pedidos de análises espectrométricas de óleos de equipamentos que exigem lubrificação, e registo dos respectivos resultados. Este sistema está integrado com o MGM, na medida em que os pedidos de análise que recaem sobre aeronaves da Força Aérea são desencadeados a partir do sistema referido.	DMSA	T	3
SIGAUT-Módulo de Viaturas do SIAGFA	Gestão do parque de equipamentos terrestres, englobando áreas como o controlo de viaturas e equipamentos relacionados, gestão de movimentos (viaturas e condutores), registo de acidentes, gestão de revisões e controlo de custos de manutenção das viaturas.	DAT	T	2
SICOMB-Módulo de Combustíveis e Lubrificantes do SIAGFA	Controlo de combustíveis de viaturas e aeronaves, integrando o ciclo de abastecimento de combustíveis às unidades (identificação da necessidade, requisição de abastecimento, reabastecimento de depósitos e consumos).	DAT	T	2
SIAGFA-GM-Módulo de Gestão de Material do SIAGFA	O Módulo de Gestão de Material consiste na extensão do SIGMA-ABAST às unidades, permitindo a execução das tarefas do circuito de Abastecimento inerentes às mesmas, sendo o órgão gestor dos processos a Esquadra de Abastecimento da Unidade. Engloba as componentes de gestão de material RAMFA8 e RAMFA9.	DAT	T	1
Módulo de Gestão de Equip. de Voo do SIAGFA	Controlo dos equipamentos de voo distribuídos ao pessoal navegante.	DAT	T	3
SIAGFA-MGM-Módulo de	Gestão e controlo de situações, configurações e potenciais de	DMSA	T	1

Título	Objectivo	E P R	C L S	P R I
Gestão de Manutenção do SIAGFA	aeronaves e componentes, bem como registo de acções de manutenção. Este sistema inclui a componente de inspecções programadas a aeronaves, com a abertura automática de cartas de trabalho na execução de uma inspecção.			
SIAGFA-MGM-C-Módulo de Gestão de Manutenção Central do SIAGFA	Efectuar a componente central de gestão e controlo de situações, configurações e potenciais de aeronaves e componentes, bem como o registo de acções de manutenção. Este sistema inclui a componente de inspecções programadas a aeronaves, com a abertura automática de cartas de trabalho na execução de uma inspecção.	DMSA	T	1
RAMFA9-Registo de Existências de Subunidades e Serviços	Controlo de material imobilizado (categoria "P") à carga das Unidades/Órgãos da Força Aérea.	DAT	T	3
SIGMA-PRODIND-Produção de Indicadores de Manutenção	Produção de indicadores a partir do anterior sistema de informação de manutenção de aeronaves (SIGMA-MANUT). Disponível actualmente apenas para consulta.	DMSA		3
INTERF-Ligação POLO com SIGMA-ABAST	Abertura automática de créditos no sistema SIGMA-ABAST e processamento dos mesmos de acordo com a informação enviada pelo POLO.	DAT	T	3

Tabela D5 - SI da Componente Operacional

Título	Objectivo	E P R	C L S	P R I
SIAGFA-MGO-Módulo de Gestão Operacional do SIAGFA	Gestão da actividade aérea através das suas vertentes estruturantes (aeronaves, pessoal navegante e missões), produção de indicadores de gestão. Integra a componente ASA (Autorizações de Sobrevoo e Aterragem), que visa a gestão de autorizações de sobrevoo e aterragem de aeronaves civis em aeródromos militares, bem como o registo de movimentos das mesmas com vista à cobrança de taxas de tráfego.	CA	T	1

Tabela D6 - SI da Inspecção

Título	Objectivo	E P R	C L S	P R I
SIIFA-Sistema de Informação da Inspecção da Força Aérea	Sistema de apoio à Inspecção-Geral da Força Aérea (IGFA) e a todos os órgãos envolvidos no planeamento e controlo de inspecções e na gestão de relatórios e de anomalias. Permite o estabelecimento de uma relação directa entre os níveis de inspecção e de execução.	IGFA	T	2
Módulo de Consulta Estatística do SIIFA	Obtenção de informação estatística e indicadores de gestão a partir dos dados obtidos no SIIFA.	IGFA	G	3

Título	Objectivo	E P R	C L S	P R I
Módulo de Prevenção de Acidentes do SIAGFA	Sistema destinado à participação e gestão de ocorrências relativas a acidentes em voo.	IGFA	T	2

Tabela D7 - SI de apoio a entidades específicas

Título	Objectivo	E P R	C L S	P R I
SIAGFA-Sistema Integrado de Apoio à Gestão na Força Aérea	O SIAGFA é um sistema que se assume como um portal de entrada para um conjunto de sistemas, agrupados segundo as duas áreas de apoio da Força Aérea (pessoal e logística), e a componente operacional. Engloba ainda sistemas dedicados ao órgão de inspecção (IGFA) e de apoio ao Estado-Maior. Todos os sistemas acedidos a partir do SIAGFA são apresentados de acordo com a área funcional ou a componente a que se destinam.	DCSI	T	2
AFAP-Gestão de Sócios da Associação da Força Aérea Portuguesa	Controlo dos associados da AFAP, nomeadamente ao nível de dados pessoais e contactos, bem como de quotas e emissão de recibos para contabilidade. Emissão de etiquetas para correspondência e criação de suporte digital para envio à Caixa Geral de Depósitos (CGD) para pagamento automático de quotas.	AFAP	T	3
AHFA-Arquivo Histórico da Força Aérea	Gestão de todo o acervo existente no AHFA (revistas, livros, fotografias, entre outros).	SDFA	T	3
CDA-Controlo de Drogas e Álcool	Gestão administrativa do processo de despiste do consumo de álcool e drogas na Força Aérea.	EMFA DIVINFO	T	3
GESTCRED-Gestão de Credenciações NATO	Controlo de toda a informação relativa a processos de credenciação NATO de pessoal militar e civil da Força Aérea, bem como de outros indivíduos que de alguma forma se relacionam com a organização.	SR OTAN	T	3
GHFA-Grupo de História da Força Aérea	Controlo do processo de levantamento de informação da história da Força Aérea.	AHFA	T	3
STANATO-Controlo de STANAG e de publicações NATO	Controlo dos STANAG em todo o processo anterior à sua ratificação e à gestão da sua distribuição interna. Permite ainda inventariar as publicações NATO directamente relacionadas com os documentos em questão.	SR OTAN	T	3
Módulo de Microfilmagem do SIAGFA	Suporte à actividade do Centro de Microfilmagem do Serviço de Documentação da Força Aérea, destinado à gestão das microfilmagens efectuadas pelo referido Órgão.	SDFA	T	3
Gestão e Controlo de Eventos	Gestão dos eventos em que as Relações Públicas da Força Aérea têm que exercer actividade protocolar.	REL.PÚBL FAP	T	3
Sistema de Informação Contabilística do POLO	Gestão contabilística de todas as verbas atribuídas à delegação portuguesa nos Estados Unidos da América.	CLAFA	T	3
Gestão de Alojamentos	Gestão e seriação de candidatos (militares da Força Aérea) à	SAS	T	3

Título	Objectivo	E P R	C L S	P R I
	utilização de messes/residências militares e à participação em eventos sociais (tais como passeios de barco) organizados pelo Serviço de Acção Social (SAS).			
AJ-DESPACHOS-Gestão de Despachos do CEMFA – Assessoria Jurídica	Gestão dos despachos do CEMFA aprovados e em vigor, a partir do despacho nº 59/77, excluindo contratos de arrendamento, prestação de serviços, avenças, concessões e outros abrangidos por normas específicas.	ASS. JURÍDICA CEMFA	T	3
AJ-PROC_ADMI-Controlo de Processos do CEMFA – Assessoria Jurídica	Controlo de processos administrativos do CEMFA, nomeadamente informações, notas, ofícios, requerimentos, recursos e contencioso.	ASS. JURÍDICA CEMFA	T	3
AJ-PROC_JUDI-Controlo de Processos Judiciais do GABCEMFA – Assessoria Jurídica	Controlo de todos os processo judiciais envolvendo a Força Aérea, efectuando o acompanhamento de todas as fases do processo.	ASS. JURÍDICA CEMFA	T	3
AJ-PROTOCOLOS- Gestão de Protocolos do CEMFA – Assessoria Jurídica	Gestão de todos os documentos de âmbito nacional referentes a protocolos estabelecidos entre qualquer órgão da Força Aérea e entidades externas.	ASS. JURÍDICA CEMFA	T	3
Site Oficial da Força Aérea (com ***backoffice*****)**	Disponibilização de informação institucional com ferramenta de gestão de conteúdos.	GAB CEMFA	W	2
Site Oficial da Academia da Força Aérea (com ***backoffice*****)**	Disponibilização de informação institucional com ferramenta de gestão de conteúdos.	AFA	W	3
Site Oficial do Centro de Recrutamento (com ***backoffice*****)**	Disponibilização de informação institucional com ferramenta de gestão de conteúdos.	CRFA	W	3
Site Oficial do Recrutamento com candidaturas *online* (com ***backoffice*****)**	Disponibilização de informação institucional com ferramenta de gestão de conteúdos. Possibilidade de realização de candidaturas *online*.	CRFA	T	2
Site Oficial do Transporte Aéreo Militar (com ***backoffice*****)**	Disponibilização de informação institucional com ferramenta de gestão de conteúdos. Gestão de informação sobre carga e passageiros, bem como de pedidos de transporte.	CA TAM	T	3
Site Oficial dos Rotores de Portugal	Disponibilização de informação institucional.	GAB CEMFA	W	3
Site de Concursos Públicos	Publicitação de concursos públicos no âmbito da Força Aérea, e disponibilização de informação associada às diversas fases do processo de concurso.	CLAFA ADAL	T	2
Site Oficial da Esquadra 201 (com ***backoffice*****)**	Disponibilização de informação institucional.	GAB CEMFA	W	3
Site Oficial da Esquadra	Disponibilização de informação institucional.	GAB	W	3

Título	Objectivo	E P R	C L S	P R I
301 (com ***backoffice*****)**		CEMFA		
Site Oficial da Esquadra 501 (com ***backoffice*****)**	Disponibilização de informação institucional e loja electrónica, com ferramenta de gestão de conteúdos. Disponibilização de uma área de acesso reservado com informação de utilidade para as tripulações quando se encontram em missão.	GAB CEMFA	W	3
Site Oficial do Arquivo Histórico	Disponibilização de informação institucional.	GAB CEMFA	W	3
Site Oficial da Revista Mais Alto (com ***backoffice*****)**	Disponibilização de informação institucional e gestão de assinaturas, com ferramenta de gestão de conteúdos.	GAB CEMFA	T	3
Site Oficial do Museu do Ar (com ***backoffice*****)**	Disponibilização de informação institucional, marcação de visitas *online* e loja electrónica, com ferramenta de gestão de conteúdos.	GAB CEMFA	T	3
Portal de *E-Learning*	Apoio à formação.	Gab. e-learning CFMTFA	W	3
Portal C295 (com *backoffice*)	Disponibilização de informação e documentação sobre a aeronave C295, com ferramenta de gestão de conteúdos.	GT C295	W	3
Portal Temático do Núcleo de Publicações Técnicas	Disponibilização de informação institucional.	DAT	W	3
Portal Temático da Direcção de Engenharia e Projectos	Disponibilização de informação institucional.	DEP	W	3
Portal Temático do Serviço de Acção Social	Disponibilização de informação institucional.	SAS	W	3
Portal Temático da Repartição de Transportes	Disponibilização de informação institucional.	DAT	W	3
Portal Temático do SIG	Disponibilização de informação institucional.	SIG	W	3
Portal da Intranet da Força Aérea Portuguesa (com ***backoffice*****)**	Disponibilização de informação e serviços no âmbito geral da Força Aérea.	DCSI	W	3
Portais das Unidades da Força Aérea (14 portais distintos**)**	Disponibilização de informação local à Unidade.	DCSI	W	3
Portal Temático da Direcção de Mecânica Aeronáutica	Disponibilização de informação institucional.	DMSA	W	3
Portal Temático de Ensino e Formação	Disponibilização de informação institucional.	CFMTFA	W	3
Portal Temático da Educação Física e Desporto	Disponibilização de informação institucional.	DINST	W	3
Portal Temático da Escola	Disponibilização de informação institucional.	CFMTFA	W	3

Título	Objectivo	E P R	C L S	P R I
de Formação Pedagógica de Formadores				
Portal Temático do Gabinete da DCSI	Disponibilização de informação institucional.	DCSI	W	3
Portal Temático da DCSI/RTI	Disponibilização de informação institucional.	DCSI	W	3
CTRL_TIRO Controlo de Tiro de Aviões	Gestão dos treinos de tiro das esquadras de voo no CTA	DCSI	T	3
Formação *online*	Gestão e execução de testes aleatórios *online*.	DCSI	T	3
Gestão de Aquisições	Gestão de aquisições efectuadas na Central de Compras do Estado.	DAT	T	3
GESTAPLIC-Gestão de Aplicações	Controlo e gestão de todas as aplicações sob a responsabilidade da DCSI (desenvolvidas internamente ou adquiridas a entidades externas).	DCSI	T	3
GPI-Gestão do Parque Informático	Gestão do Parque Informático da Força Aérea.	DCSI	T	3
Inquéritos DINST	Gestão de inquéritos *online* sobre a formação da DINST.	DINST	T	3
Previsão Meteorológica	Disponibilização das previsões meteorológicas para os dias mais próximos.	CIMFA	W	3
Ordens de Serviço	Pesquisa de ordens de serviço do EMFA por diversos parâmetros.	DCSI	W	3
EMFAR	Pesquisas ao EMFAR por diversos parâmetros.	DCSI	W	3
Publicações da Força Aérea	Pesquisas e consultas a diversos tipos de publicações da Força Aérea (RFA, MFA, …)	SDFA	W	3
Terminologia OTAN	Disponibilização de glossário de termos OTAN.	SR OTAN	W	3
Publicações IAEFA/IESM	Consulta *online* de trabalhos académicos do IAEFA e do IESM.	DCSI	W	3
Lista Telefónica RATFA	Consulta da RATFA	CC CA	W	3
Lista de Contactos do EMFA (com ***backoffice*****)**	Gestão dos contactos da rede RATFA, nominais, do complexo de Alfragide.		W	3
OSINT *Open Sources Intelligence*	Consulta e Pesquisa de documentos de *Open Sources Intelligence*, com ferramenta de gestão de conteúdos.	EMFA DIVINFO	W	3
Ementas	Disponibilização de informação sobre as ementas da messe de Alfragide.	GAEMFA	W	3
Meeting Rooms	Reserva de salas de reuniões, serviço de catering e audiovisuais.	DCSI	T	3

Tabela D8 - Sistemas de Informação adquiridos a entidades externas

Título	Objectivo	E P R	C L S	P R I
CDI-Centros de Documentação e Informação	Gestão integrada das bibliotecas da Força Aérea.	SDFA	T	3

Título	Objectivo	E P R	C L S	P R I
APLIDOC-Sistema de Gestão Documental	Gestão e controlo de documentos e processos.	SDFA	T	2
SIGES-Sistema Integrado de Gestão do Ensino Superior	Gestão escolar da Academia da Força Aérea.	AFA	T	3
PGS-***Portuguese Ground Station***	Controlo de configurações e inspecções da frota EH101.	DMSA	T	1
C-IETP-***Compound-Interactive Electronic Technical Publications***	Gestão de publicações técnicas da frota EH101.	DMSA	W	2
EMP-***EH101 Mission Planning***	Apoio à missão da frota EH101.	DMSA	T	2
EMMS-***Engine Maintenance Material System***	Monitorização e controlo dos motores da frota F16 (F100).	DMSA	T	2
LSMS-***Logistical Support Maintenance System***	Controlo da configuração e registo de acções de manutenção da frota C295.	DMSA	T	3
LEMP-Laboratório de Equipamentos de Medida e Precisão	Gestão de equipamentos de medida e precisão.	DMSA	T	2
MAM-***Media Asset Management***	Catalogação do arquivo digital do AHFA.	AHFA	T	3
SIINFRAS-Sistema de Informação de Infra-Estruturas	Sistema de informação geográfica, criado com o objectivo de suportar a informação na área das infra-estruturas da Força Aérea (nomeadamente de servidões, licenciamentos, inventário, arquivo técnico, etc.)	DI	T	1
Site de Informação Aeronáutica			W	3
SGH-Sistema de Gestão Hospitalar	Gestão do processo clínico de pacientes do HFA.	HFA	T	1
PICIS-Sistema de suporte à decisão clínica na área de cuidados intensivos do HFA	Apoio Unidade Cuidados Intensivos e Recobro do HFA	HFA	T	1
CLINIDATA XXI-Gestão global do Laboratório de Patologia Clínica do HFA	Gestão de laboratórios de análises clínicas e de diagnóstico.	HFA	T	1
WINVENTUS	Receber, processar e distribuir informação meteorológica necessária à actividade da FAP	CIMFA	T	1

Anexo E – Análise de Impacto dos Sistemas de Informação de Prioridade 1

Anexo elaborado a partir das entrevistas realizadas aos responsáveis pelos SI / TI

Legenda:

EPR – Entidade Primariamente Responsável
PRI – Prioridade de Recuperação (**0** – Baixa a **5** – Elevada)
IMP – Impacto em caso de indisponibilidade (**0** – Baixo a **5** – Elevado)
CRI – Criticidade do Sistema (**0** – Baixa a **5** – Elevada)
DEP – Dependência de outros Sistemas de Informação
RTO – *Recovery Time Objective*
RPO – *Recovery Point Objective*

Tabela E1 – Análise de Impacto

Área	Sistema de Informação	EPR	PRI (0 a 5)	IMP (0 a 5)	CRI (0 a 5)	Processo Alternativo	DEP	RTO	RPO	Observações
Pessoal	SIGAP e SIAGFA-RH	DP	5	5	5	Não Existe	Não tem	2 dias	2 dias	• O impacto da indisponibilidade dos Sistemas é muito grave ao nível da gestão dos Recursos Humanos.Perde-se a capacidade de produção dos indicadores; • O impacto é maior na primeira e últimas semanas do mês; • Não existem procedimentos definidos para recuperação da informação, após o sistema novamente disponível; • Existe capacidade de recuperação da informação perdida; • A indisponibilidade do SIGAP tem impacto no SIPAV.
	SGH	HFA	5	5	5	Alguns	Não tem	45 m	12 horas	• Na maioria dos módulos existem processos alternativos, embora pouco expeditos e sem rotinas devidamente testadas; • A indisponibilidade dos SI da Saúde tem impacto na missão da FAP, uma vez que prejudicam a prestação eficaz dos actos médicos; • O impacto da indisponibilidade do SI traduz-se, na maioria dos módulos, em atrasos nos atendimentos e realização de actos médicos, devidos a falta de rotinas em activar processos alternativos e, em alguns casos, em impedimentos da realização dos mesmos devido à impossibilidade de consultar o processo clínico electrónico.
	PICIS	HFA	5	5	4	Papel	SGH	12 horas	1 dia	• A indisponibilidade deste Sistema tem como consequência a falta de informação acerca do doente que está no bloco operatório, recobro ou cuidados intensivos; • O impacto da indisponibilidade do PICIS é elevado, perdendo-se a capacidade de fornecer informação em tempo útil.

Área	Sistema de Informação	EPR	PRI (0 a 5)	IMP (0 a 5)	CRI (0 a 5)	Processo Alternativo	DEP	RTO	RPO	Observações
	CLINIDATA XXI	HFA	5	5	5	Não Existe	SGH	2 horas	12 horas	• A transferência manual é hoje inaceitável pelos riscos que lhe são inerentes; • A indisponibilidade deste sistema afectaria gravemente o funcionamento do laboratório, sendo totalmente inviável atender a grande maioria dos utentes.
	SIPAV e SIPAV-CONTBANC	DFFA	5	5	5	Não Existe	SIGAP	1 dia	1 dia	• Inexistência de procedimentos alternativos ao sistema, o que provocará a incapacidade para o processamento dos vencimentos.
Logística	SIGMA-ABAST e SIAGFA-GM	DAT	5	5	5	Papel	O SIAGFA-GM depende do SIGMA-ABAST	2 dias	2 dias	• O SIAGFA-GM está disponível nas unidades, permitindo a execução das tarefas do circuito de Abastecimento de acordo com as existências locais; • A indisponibilidade destes sistemas tem um grande impacto na actividade aérea, podendo afectar a taxa de prontidão dos meios aéreos ou mesmo impedir o cumprimento de determinadas missões; • O impacto é maior em caso de realização de exercícios, elevado indice de manutenções inopinadas e maior número de aeronaves de alerta; • A utilização dos processos alternativos torna-se insustentável a partir do 3º dia; • Em caso de indisponibilidade do Sistema o impacto na missão da Força Aérea é uma realidade.
	SIAGFA-MGM e SIAGFA-MGM-C	DMSA	5	4	4	Não Existe	SIGAP e SIGMA-ABAST	1 dia	1 dia	• Os registos de consumos de potencial são efectuados na Caderneta do Avião (horas de voo, horas de funcionamento próprio, ciclos de trem, etc) e os potenciais serão actualizados no sistema assim que estiver disponível; • A indisponibilidade do sistema tem impacto na configuração das aeronaves, no controlo de potenciais e, principalmente na situação operacional das aeronaves; • Sem ferramenta de controlo algumas missões poderão eventualmente ser afectadas; • Se a falha ocorrer numa situação, por exemplo num destacamento do C-130 em Kabul, em que pode estar a ser pedido à Esquadra um esforço suplementar de missões, perder a ferramenta de controlo tem um impacto muito negativo.
	PGS	DMSA	4	5	5	Existe	Não tem	1 Sem.	1 dia	• Em caso de falha do sistema não se podem fazer os downloads dos voos e acertar as métricas nem registar o trabalho efectuado; • O Processo alternativo é a utilização de um computador onde é instalado o sistema e reposição dos últimos dados disponíveis; • Para o processo alternativo existe uma articulação entre a Secção de Aprontamento e o APC de modo a reagir quando o sistema falha por uma razão qualquer

Área	Sistema de Informação	EPR	PRI (0 a 5)	IMP (0 a 5)	CRI (0 a 5)	Processo Alternativo	DEP	RTO	RPO	Observações
	SIINFRAS	DI	5	5	5	Não Existe	Não tem	3 dias	2 horas	• Em caso de indisponibilidade o impacto é elevado porque não podem ser introduzidos e ou analisados novos processos, nem consultados os já existentes. No entanto, existe a capacidade de consulta de cartas e implantação de polígonos (a consulta de processos relacionados não é viável); • Para algumas tarefas existem procedimentos alternativos definidos, mas não descritos na totalidade; • A não existência do sistema, ou outro similar, impede o cumprimento da missão atribuída à repartição de Património da DI.
Operacional	SIAGFA-MGO	CA	5	5	5	SIM	SIGAP - SIAGFA-RH - SIAGFA-MGM - SIAGFA-GM e SIGMA-ABAST	3 dias	3 dias	• Nas unidades existe sistema alternativo no que respeita a planeamento de missões. Através das reservas de airtasks, efectua-se o tasking manualmente, inserindo-se posteriormente essa informação no sistema. Nas unidades os modelos 1M serão inseridos após a inserção das missões no sistema; • Impacto aceitável até aos três dias, se houver cativação de airtasks; • Em caso de indisponibilidade não existe capacidade de planeamento, consulta e extração de informação. Sendo um período de tempo mais prolongado, implica mais tempo e possibilidades de mais erros, na recuperação dessa informação.
	WINVENTUS	CIMFA	4	4	5	SIM	Não tem	6 horas	3 horas	• Processo alternativo recorrendo à utilização do telefone e fax, mas requerendo um substancial aumento dos recursos humanos; • O CIMFA desenvolveu uma aplicação (NETMET) que poderá temporariamente disponibilizar os dados que teriam que ser recebidos por via telefónica e introduzidos manualmente; • Existem procedimentos alternativos definidos mas só ao nível da transmissão de comunicados tipo TAF's, METAR's. Estes comunicados são transmitidos pelo Centro de Comunicações; • Impossibilidade da realização das missões que envolvam troca de informação entre o CIMFA e as UB´s, porque a validação dos TAF´s (previsões) tem que ser feita pelos METAR´s (observações), sem esta ultima informação em tempo o TAF tem que ser cancelado e sem TAF válido as tripulações não descolam.

(Fonte: Elaborado pelo autor)

Tabela E2 – Relação Sistemas de Informação x Tecnologias de Informação

Sistema de Informação	Software	Hardware	Vulnerabilidades	Medidas de Controlo
SIGAP	• Linguagem de Programação em Mapper • Base de dados Oracle (com Sistema Operativo SUSE Linux) • Sistema Operativo Windows 2000 (servidor Aplicacional)	• 1 Servidor Aplicacional ; • 2 Servidores em *cluster* para a Base de Dados que acedem a uma unidade de armazenamento (EVA3000); • *Switch* central (Nortel 8000); • Circuitos de fibra redundantes (SAN Switches) para ligação à Unidade de Armazenamento.	• Não existe redundância ao nível do servidor aplicacional; • Linguagem de programação e Sistema Operativo obsoletos; • *Switch* central é um ponto único de falha; • Nível de actualização do Sistema Operativo. • Circuito único de entrada de energia para o Centro de Dados; • Sistema de arrefecimento através de um circuito de água.	• Monitorização 24H/7; • Contrato de suporte de *Hardware* 24x7x4H; • *Backup* Diário/Semanal/Mensal e Anual; • Controlo de Acessos; • Sistema Anti-fogo; • Controlo de Humidade e temperatura; • Distribuição energia N+1; • Ar-condicionado 2N; • Grupo gerador dedicado ao Centro de Dados; • Sistemas de detecção de inundação e de válvulas de corte do circuito de água; • Servidores com fontes de alimentação redundantes; • Manutenção preventiva (distribuição Energia e ar-condicionado).
SIAGFA-RH	• Linguagem de Programação em Visual Basic • Base de dados Oracle (com Sistema Operativo SUSE Linux)	• 4 Servidores aplicacionais em c*luster*; • 2 Servidores em *cluster* para a Base de Dados que acedem a uma unidade de armazenamento (EVA3000); • *Switch* central (Nortel 8000); • Circuitos de fibra redundantes (SAN *Switches*) para ligação à Unidade de Armazenamento.	• Linguagem de programação obsoleta; • *Switch* central é um ponto único de falha; • Circuito único de entrada de energia para o Centro de Dados; • Sistema de arrefecimento através de um circuito de água.	• Monitorização 24H/7; • Contrato de suporte de *Hardware* 24x7x4H; • *Backup* Diário/Semanal/Mensal e Anual; • Controlo de Acessos; • Sistema Anti-fogo; • Controlo de Humidade e temperatura; • Distribuição energia N+1; • Ar-condicionado 2N; • Grupo gerador dedicado ao Centro de Dados; • Sistemas de detecção de inundação e de válvulas de corte do circuito de água; • Servidores com fontes de alimentação redundantes; • Manutenção preventiva (distribuição Energia e ar-condicionado).
SGH	• Base de dados Oracle (com Sistema Operativo SUSE Linux) • Software Proprietário da Glint HS	• 2 Servidores em *cluster* para a Base de Dados que acedem a uma unidade de armazenamento (EVA4000); • *Switch* central (Nortel 8000); • 2 Servidores aplicacionais em *cluster*.	• Base única de instalação dos servidores (ponto único de falha); • *Switch* central é um ponto único de falha;	• Contrato de suporte de *Hardware* 24x7x4H; • *Backup* Diário/Semanal/Mensal e Anual; • Ar condicionado 2N; • Sistema Anti-fogo; • Servidores com fontes de alimentação redundantes; • Grupo Gerador.

Sistema de Informação	Software	Hardware	Vulnerabilidades	Medidas de Controlo
PICIS	• Base de dados Oracle (com Sistema Operativo SUSE Linux) • Software Proprietário da Siemens	• 1 Servidor Base de Dados; • *Switch* central (Nortel 8000); • 1 Servidor Aplicacional.	• Não existe redundância ao nível do servidor de Base de Dados; • Não existe redundância ao nível do servidor aplicacional; • Base única de instalação dos servidores (ponto único de falha); • *Switch* central é um ponto único de falha.	• Contrato de suporte de *Hardware* 24x7x4H; • *Backup* Diário/Semanal/Mensal e Anual; • Ar condicionado 2N; • Sistema Anti-fogo; • Servidores com fontes de alimentação redundantes; • Grupo Gerador.
CLINIDATA XXI	• Base de dados Oracle (com Sistema Operativo Windows 2000) • Software Proprietário da MaxData	• 1 Servidor Base de Dados; • Switch central (Nortel 8000).	• Não existe redundância ao nível do servidor de Base de Dados; • Sistema Operativo do Servidor da Base de Dados Obsoleto; • *Switch* central é um ponto único de falha.	• Contrato de suporte de *Hardware* 24x7x4H; • *Backup* Diário/Semanal/Mensal e Anual; • Ar condicionado 2N; • Sistema Anti-fogo; • Servidores com fontes de alimentação redundantes; • Grupo Gerador.
SIPAV SIPAV-CONTBANC SIGMA-ABAST	• Linguagem de Programação em Cobol • Linguagem de Programação em Mapper • Base de dados Oracle (com Sistema Operativo SUSE Linux)	• 2 Servidor Aplicacionais; • 2 Servidores em *cluster* para a Base de Dados que acedem a uma unidade de armazenamento (EVA3000); • *Switch* central (Nortel 8000); • Circuitos de fibra redundantes (SAN *Switches*) para ligação à Unidade de Armazenamento.	• Linguagens de programação obsoletas; • Switch central é um ponto único de falha; • Circuito único de entrada de energia para o Centro de Dados; • Sistema de arrefecimento através de um circuito de água.	• Monitorização 24H/7; • Contrato de suporte de *Hardware* 24x7x4H; • *Backup* Diário/Semanal/Mensal e Anual; • Controlo de Acessos; • Sistema Anti-fogo; • Controlo de Humidade e temperatura; • Distribuição energia N+1; • Ar-condicionado 2N; • Grupo gerador dedicado ao Centro de Dados; • Sistemas de detecção de inundação e de válvulas de corte do circuito de água; • Servidores com fontes de alimentação redundantes; • Manutenção preventiva (distribuição Energia e ar-condicionado).
SIAGFA-MGM SIAGFA-MGM-C SIAGFA-MGO SIAGFA-GM	• Linguagem de Programação em Visual Basic • Base de dados Oracle (com Sistema Operativo SUSE Linux)	• 4 Servidores aplicacionais em *cluster*; • 2 Servidores em *cluster* para a Base de Dados que acedem a uma unidade de armazenamento (EVA3000); • *Switch* central (Nortel 8000); • Circuitos de fibra redundantes (SAN *Switches*) para ligação à	• Linguagem de programação obsoleta; • *Switch* central é um ponto único de falha; • Circuito único de entrada de energia para o Centro de Dados; • sistema de arrefecimento através de um circuito de água.	• Monitorização 24H/7 • Contrato de suporte de *Hardware* 24x7x4H; • *Backup* Diário/Semanal/Mensal e Anual; • Controlo de Acessos; • Sistema Anti-fogo; • Controlo de Humidade e temperatura; • Distribuição energia N+1; • Ar-condicionado 2N; • Grupo gerador dedicado ao Centro de Dados;

Sistema de Informação	Software	Hardware	Vulnerabilidades	Medidas de Controlo
		Unidade de Armazenamento.		• Sistemas de detecção de inundação e de válvulas de corte do circuito de água; • Servidores com fontes de alimentação redundantes; • Manutenção preventiva (distribuição Energia e ar-condicionado).
PGS	• Base de Dados Ingres (com Sistema Operativo Windows 2003) • Software Proprietário da Westland	• 1 Servidor de base de dados ; • *Switch* central (Nortel 8000).	• Não existe redundância ao nível do servidor de Base de Dados; • Base única de instalação dos servidores (ponto único de falha); • *Switch* central é um ponto único de falha.	• Contrato de suporte de *Hardware* 24x7x4H; • *Backup* Diário/Semanal/Mensal e Anual; • Ar condicionado 2N; • Sistema Anti-fogo; • Servidores com fontes de alimentação redundantes; • Monitorização remota 24H/7; • Grupo Gerador;
WINVENTUS	• Software Proprietário da Minisoft	• 2 servidores aplicacionais ;	• Ar condicionado N; • UPS não redundante; • Sala dos Servidores inadequada.	• Contrato de suporte de *Hardware* 24x7x4H; • Servidores com fontes de alimentação redundantes; • Servidores com funções redundantes; • Grupo Gerador.
SIINFRAS	• Base de dados Oracle (com Sistema Operativo SUSE Linux) • Software Proprietário da Stei	• 1 Servidor Base de Dados; • 1 Servidor Aplicacional; • *Switch* central (Nortel 8000); • Circuitos de fibra redundantes (SAN *Switches*) para ligação à Unidade de Armazenamento.	• Não existe redundância ao nível do servidor de Base de Dados; • Não existe redundância ao nível do servidor aplicacional; • *Switch* central é um ponto único de falha; • Circuito único de entrada de energia para o Centro de Dados; • sistema de arrefecimento através de um circuito de água.	• Monitorização 24H/7 • Contrato de suporte de *Hardware* 24x7x4H; • *Backup* Diário/Semanal/Mensal e Anual; • Controlo de Acessos; • Sistema Anti-fogo; • Controlo de Humidade e temperatura; • Distribuição energia N+1; • Ar-condicionado 2N; • Grupo gerador dedicado ao Centro de Dados; • Sistemas de detecção de inundação e de válvulas de corte do circuito de água; • Servidores com fontes de alimentação redundantes; • Manutenção preventiva (distribuição Energia e ar-condicionado).

(Fonte: Elaborado pelo autor)

Anexo F – Rede de comunicações para voz e dados[5]

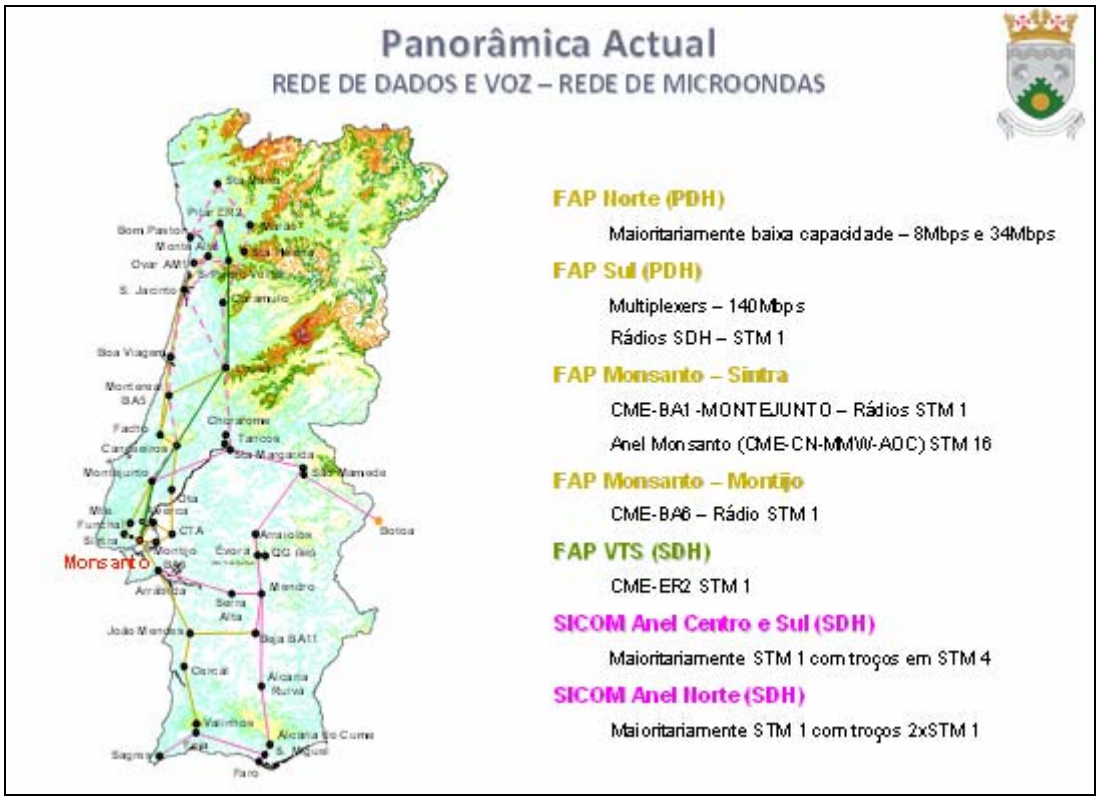


Figura F1 – Rede de Micro-ondas

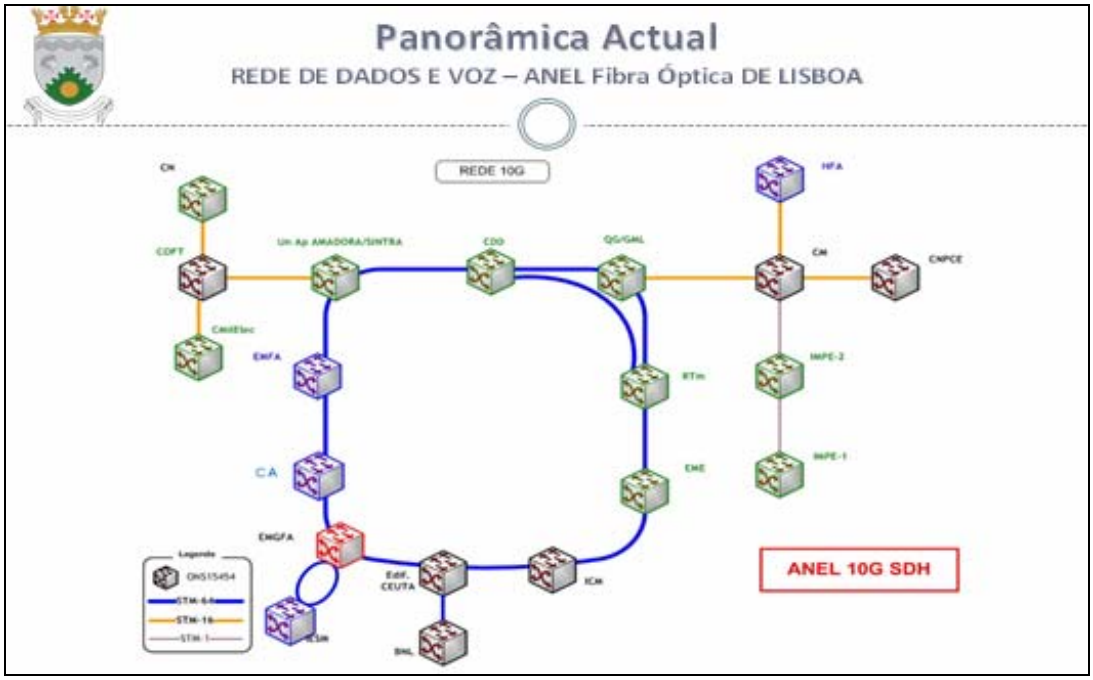


Figura F2 – Anel de Fibra óptica de Lisboa

[5] Fonte: DCSI

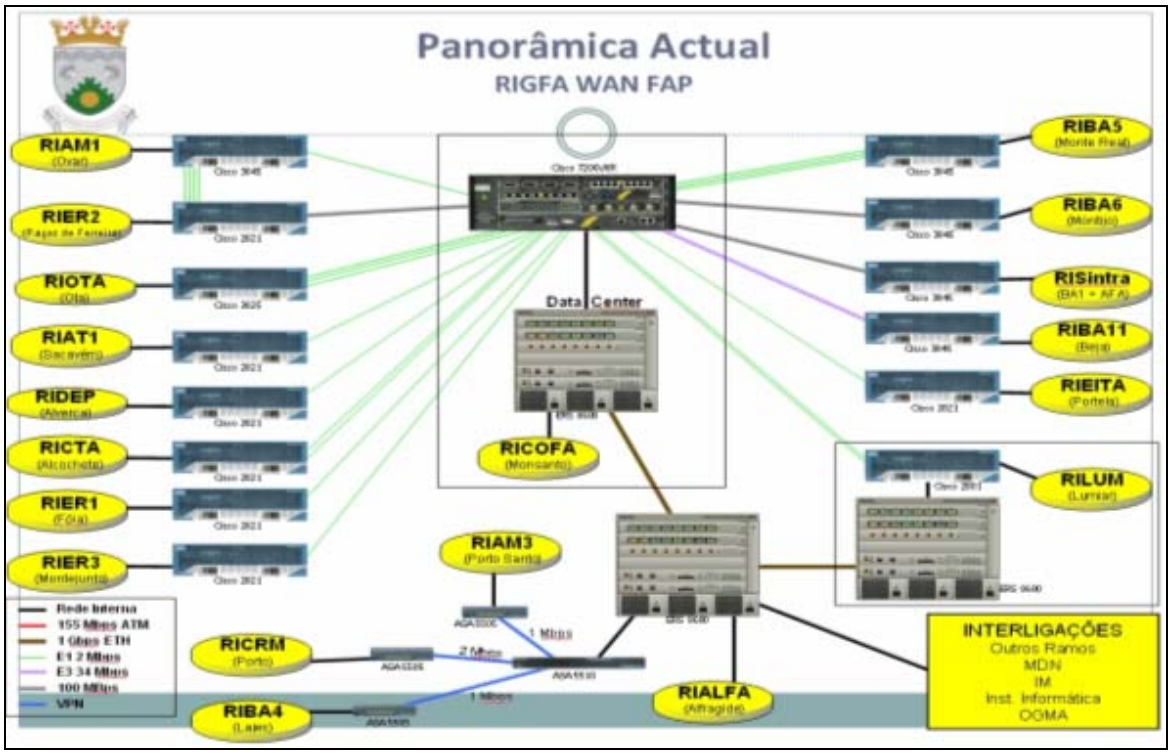


Figura F3 – Topologia da RIGFA

Tabela F1 – Larguras de Banda

De	Para	Largura de Banda (Mbps)	Observações
CA	SINTRA	90	MO (Micro Ondas) - Interface 100 Mb Ethernet
	OTA	6	MO
	AT1	2	MO
	BA5	6	MO
	BA6	90	MO - Interface 100 Mb Ethernet
	BA6	6	MO - Backup
	LUMIAR	6	MO - Backup
	EMFA	1000	Anel margem Norte do SICOM
	BA11	34	MO
	ER2	90	MO Interface 100 Mb Ethernet
	CTA	2	MO
	DGMFA	2	MO
	ER3	2	MO
	ER1	2	MO
	EITA	2	MO
AM1	ER2	6 ou 8	MO
EMFA	AM3	1	Frame Relay Comercial - SICOM
	DNCRFA	4	4Mb para DNCRFA e 1Mb para Internet
	BA4	1	Frame Relay Comercial - SICOM
	LUMIAR	1000	Anel margem Norte do SICOM