Licenciatura em Sistemas e Tecnologias de Informação

Plano de Continuidade de Negócio

Análise de um Estudo de Caso

Projeto Final de Licenciatura

Elaborado por Ricardo Saragoça

Aluno nº 20121638

Orientador: Professor Doutor Sérgio Nunes

Barcarena

Junho 2015

Universidade Atlântica

Licenciatura em Sistemas e Tecnologias de Informação

Plano de Continuidade de Negócio

Análise de um Estudo de Caso

Projeto Final de Licenciatura

Elaborado por Ricardo Saragoça

Aluno nº 20121638

Orientador: Professor Doutor Sérgio Nunes

Barcarena

Junho 2015

O autor é o único responsável pelas ideias expressas neste relatório

Agradecimentos

A toda a minha família que sempre me apoiou nesta jornada, em especial à minha mãe que sempre me fez acreditar que com esforço e dedicação é possível alcançar todos os objetivos que nos propomos, ao meu pai que sempre me incentivou e apoiou a ir mais longe acreditando sempre que vale a pena o sacrifício e à minha esposa que esteve sempre ao meu lado durante esta viagem, suportando a minha ausência e sempre com uma palavra de apoio e incentivo.

Ao meu orientador o professor Doutor Sérgio Nunes, pela pronta disponibilidade, pela paciência e apoio na elaboração deste trabalho.

A todos os meus colegas pelo apoio e companheirismo ao longo destes três anos em que partilhamos esta viagem e a tornaram mais fácil e entusiasmante.

À organização que me permitiu efetuar este estudo de caso, pois sem a sua permissão não seria possível elaborar este trabalho.

A todos vos o meu mais sincero obrigado.

Resumo

Plano de Continuidade de Negócio Análise de um Estudo de Caso

As empresas estão cada vez mais dependentes das tecnologias de informação para a realização de negócio, e os incidentes disruptivos são uma ameaça constante, que em casos extremos podem levar ao desaparecimento da empresa. Para aumentar a sua resiliência e garantir a continuidade do negócio, as empresas optam por implementar planos de continuidade de negócio, mas como pode ser operacionalizado um plano de continuidade de negócio?

Para responder a esta questão foi desenvolvido este trabalho de pesquisa metodológica de estudo de caso. Que após um processo de revisão da literatura relevante apurou um conjunto de boas práticas a seguir num plano de continuidade de negócio. De modo a avaliar como é operacionalizado um plano de continuidade de negócio num contexto real, social e económico específico, foi construído um estudo de caso sobre uma instituição financeira a operar no mercado português, que criou e implementou o seu próprio plano de continuidade de negócio, explorando o processo, as opções tomadas e tecnologia utilizada.

Para avaliar o plano de continuidade da organização, foi feita uma análise ao processo de operacionalização face às boas práticas apuradas e à norma ISO 22301, após o qual se conclui que a organização se encontra num nível de *compliance* de cerca de 68.3%. Face a este resultado foi elaborado um conjunto de recomendações com o objetivo de elevar o nível de *compliance* da organização para cerca de 100% do ISO 22301.

Palavras-chave: Plano de continuidade de negócio, BIA, Gestão da continuidade, ISO 22301, Estudo de caso, Virtualização, Alta disponibilidade, Recuperação de desastres

Abstract

Business Continuity Plan Analysis of a Case Study

Companies are increasingly dependent on information technology for conducting business, and disruptive incidents are a constant threat, in extreme cases can lead a company to extinction. To increase their resilience and ensure business continuity, companies choose to implement business continuity plans, but how can a business continuity plan be operationalized?

To answer this question was developed this methodological research case study. That after a relevant literature review process, found a set of good practices to follow in a business continuity plan. In order to assess how a business continuity plan can be operationalized on a real and specific social and economic context, a case study is built on a financial institution operating in the Portuguese market that has created its own business continuity plan, exploring the process , the choices made and technology used.

To assess the organization's business continuity plan, an analysis was made of the process in the face of good practice and the ISO 22301, after which to conclude that the organization is in a compliance level of about 68.3%. To tackle this result was drafted a set of recommendations in order to raise the compliance level to about 100%.

Keywords: Business continuity management, business impact analysis, ISO 22301, case study, virtualization, high availability, Disaster Recovery.

Índice

Índice de figuras

Índice de tabelas

Lista de abreviaturas e siglas

PCN – Plano de continuidade de negócio.

BIA – Business impact analysis.

PECB – Professional Evaluation and Certification Board.

DR - Disaster Recovery.

TI – Tecnologias de informação.

INE – Instituto Nacional de Estatística.

A/C – Ar Condicionado.

MTTR – Mean Time to Repair.

MTBF – Mean Time Between Failures.

NIST - National Institute of Standards and Technology.

MTD - Maximum Tolerable Downtime.

RTO - Recovery Time Objective.

RPO - Recovery Point Objective.

CPD – Centro de Processamento de Dados.

Introdução

Atualmente as organizações têm a sua atividade assente em sistemas de informação, e dependem deles para a realização de negócio, segundo o (INE, 2014) em 2014 95% das empresas tem ligações é internet de banda larga, demostrando uma tendência crescente de cerca de 10% desde o início da década, sendo já de 100% em empresas com mais de 250 colaboradores, revelando a importância que as empresas atribuem à ligação à internet para o seu negócio. Cerca de 66% das empresas em Portugal vão mais longe dotando os seus colaboradores com meios de ligação à internet através de banda larga móvel (INE, 2014).

A aposta na ligação à internet nas empresas vai ganhando um papel central sendo utilizada por 39% das empresas para a angariação de clientes através das redes sociais (INE, 2014), e para o acesso a serviços contratados na *cloud*, sendo que 13% das empresas em Portugal utilizam serviços deste tipo em 2014 (INE, 2014).

As quebras de serviço representam perda de volume de negócio, podendo em casos extremos levar à extinção da organização, segundo o estudo efetuado pela entidade independente *Vanson Bourn* para a EMC (EMC, 2014) que analisou 3300 empresas de 24 países de todos os continentes com mais de 250 colaboradores, dando assim uma visão a nível global dos impactos dos períodos de *downtime* e perca de dados.

Segundo o estudo (EMC, 2014) que estima que os custos com perda de dados e inatividade nas organizações cheguem em média a 1.7 mil milhões de dólares num ano, 754$ milhões com perca de dados e 954$ milhões com *downtime*. Sendo que 64% das empresas do estudo experienciaram períodos de *downtime* no último ano, levando a uma perda de receita de cerca de 36% e ao atraso de desenvolvimento dos seus produtos em cerca de 34%.

Apesar destes resultados apenas 51% das empresas do estudo tem um plano de *disaster recovery* e 71% do pessoal do TI não confia na sua capacidade de recuperar informação após um incidente (EMC, 2014).

O estudo (EMC, 2014) conclui ainda que as empresas que não têm uma estratégia de alta disponibilidade, estão duas vezes mais propensas a perdas de dados e disrupções do que as restantes.

Devido à crescente importância dos sistemas de informação para a realização de negócio e tendo em conta os impactos das disrupções, os sistemas de *disaster and recovery*, os planos de continuidade do negócio e os sistemas de alta disponibilidade ganham uma importância vital para as empresas no sentido de aumentar a taxa de disponibilidade dos seus sistemas e de assegurar a continuidade do negócio evitando elevadas perdas em caso disrupção do serviço.

1. Título Revisão da Literatura

1.1. Gestão da continuidade de negócio

Segundo a ISO 22301 (ISO 22301, 2012) a gestão de continuidade de negócio é um processo holístico que identifica potenciais ameaças à organização e os seus impactos nas operações, e fornece um *framework* para a construção de organizações mais resilientes com capacidade efetiva de resposta que salvaguarde os interesses dos seus *stakeholders*, a sua reputação, marca e atividades de criação de valor.

Já para o BCM *Institute* (BCMInstitute, 2014) é uma disciplina que envolve toda a organização e um conjunto de processos que identifica potenciais impactos que ameaçam a organização. Proporciona uma capacidade de resposta eficaz que salvaguarda os principais interesses dos *stakeholders* e a sua reputação.

Segundo a norma ISO 22301 (ISO 22301, 2012) a gestão de continuidade de negócio deve ter em conta a importância dos pontos da tabela abaixo.

Ponto	Descrição
Ponto 1	Compreender as necessidades da organização e a necessidade para a criação de um plano de continuidade de negócio as suas políticas e objetivos.
Ponto 2	Implementar controlos e métricas de forma a medir a capacidade global da organização de resposta a incidentes disruptivos.
Ponto 3	Monitorizar a performance e a efetividade do plano de continuidade de negócio.
Ponto 4	Melhoria continua baseada na avaliação dos objetivos.

Tabela 1- Pontos-chave de um plano de continuidade de negócio

Fonte: (ISO 22301, 2012)

A gestão da continuidade do negócio só consegue atingir o sucesso se tiver o apoio da gestão de topo da organização, a melhor maneira de conseguir esse apoio é focar os benefícios de ter um processo de gestão de continuidade de negócio eficaz. Hoje em dia uma boa gestão de continuidade de negócio não é ter de tomar ações para endereçar questões externas mas sim, reconhecer o valor acrescentado que as boas práticas de gestão de continuidade de negócio trazem para a organização (St-GERMAIN)

- Proteção do valor da organização beneficiando os acionistas.
- Maior compreensão do negócio como resultado da análise de riscos.
- Resiliência operacional resultante da redução de risco.

- Redução de *downtime* através da identificação de *workarounds* para mitigar as disrupções.
- Podem ser identificadas questões de conformidade para outros processos.
- Registos relevantes para a organização podem ser mantidos e protegidos.
- As questões da legislação, de saúde e segurança são consideradas.
- Melhoria operacional através da reengenharia de processos de negócio.
- Proteção dos ativos físicos e do conhecimento do negócio.
- Preservação dos mercados garantindo a continuidade da atividade.
- Melhoria da segurança global

1.2. Business Impact Analysis (BIA)

Segundo a ISO 22301 (ISO 22301, 2012) o BIA é o processo de analisar as atividades e o efeito que um evento disruptivo possa ter sobre elas.

Segundo o NIST (Swanson, Bowen, Phillips, Gallup, & Lynes, 2010) o principal objetivo do BIA é entender que processos são vitais para a operação e perceber quais os impactos de eventos disruptivos no negócio. Para isso é necessário relacionar os sistemas com os processos e serviços críticos do negócio, e com base nessa informação caracterizar as consequências de um evento disruptivo. Os resultados do BIA são o centro da política de continuidade do negócio.

Regra geral um BIA pode ser dividido em três objetivos (Swanson, Bowen, Phillips, Gallup, & Lynes, 2010):

- Determinar os processos críticos para o negócio e criticidade de recuperação – Neste ponto são identificados os processos críticos e os sistemas que os suportam e é determinado o impacto de uma disrupção do serviço de suporte aos processos identificados, assim como o *downtime* máximo tolerável para a organização de modo a conseguir continuar com a sua missão após um evento disruptivo. O downtime pode ser identificado se vários modos:
    - MTD (*Maximum Tolerable Downtime*) – O MTD representa o tempo máximo total de *downtime* de um sistema \ processo crítico para o negócio até colocar a continuidade da organização em risco.
    - RTO (*Recovery Time Objective*) – O RTO define o tempo máximo que um sistema pode estar indisponível até criar impactos graves noutros sistemas / processos críticos para o negócio.
    - RPO (*Recovery Point Objective*) – O RPO representa o tempo máximo de perda de dados em caso de desastre.
- Identificação de recursos – Neste ponto são identificados os recursos para recuperar os processos críticos e as suas dependências o mais rápido possível após um evento disruptivo. Devem ser avaliados todos os recursos necessários

(Instalações, pessoal, equipamento, software, dados, componentes do sistemas como comunicações, etc.).

- Identificar prioridades de recuperação – Neste ponto são criadas prioridades de recuperação com base no levantamento efetuado nos pontos anteriores.

Segundo (Swanson, Bowen, Phillips, Gallup, & Lynes, 2010) quanto maior for a duração de uma disrupção maior é o custo para a organização. Por outro lado quanto menor o RTO mais caras são as soluções de *backup* e replicação. O ideal é encontrar um ponto de equilibro entre os custos de recuperação e os custos de *downtime*, este ponto difere de organização para organização dependendo das restrições orçamentais e requisitos funcionais.

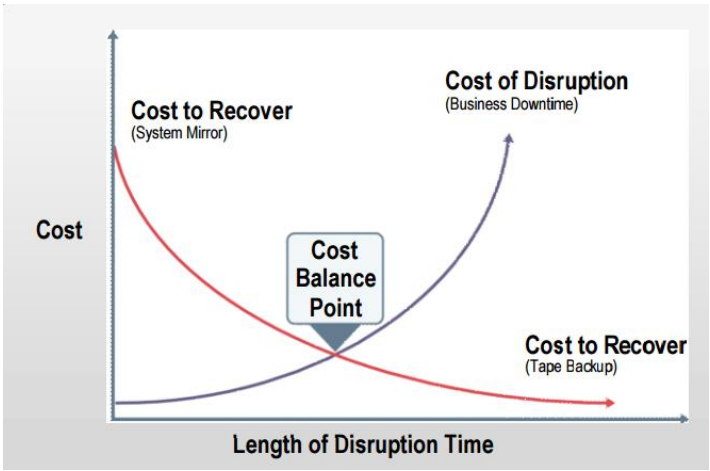


Fig. 1 – Ponto de equilíbrio custo *downtime* vs. Custo recuperação.

Fonte: (Swanson, Bowen, Phillips, Gallup, & Lynes, 2010)

1.3. Disaster and recovery

Segundo o BCM *institute* (BCMInstitute, 2014) DR é a capacidade de uma organização de fornecer serviços críticos de TI e telecomunicações após o seu normal funcionamento ter sido interrompido por um incidente, emergência ou desastre. DR recupera os recursos de TI e telecomunicações, assegurando que as funções críticas do negócio continuam a funcionar no menor espaço de tempo possível ou num *timing* predefinido pela organização.

Para (Schmidt, 2006) *disaster recovery* é a capacidade de continuar a fornecer serviços no caso de graves incidentes disruptivos, muitas vezes com capacidade e desempenho reduzidos, normalmente as atividades de recuperação exigem atividades manuais.

Normalmente o *disaster recovery* é ativado quanto as operações não podem ser retomadas no mesmo sistema ou local. Assim é ativado um sistema \ local de *backup* onde possam continuar as operações. Este sistema \ local de *backup* pode ser no mesmo *site* do sistema primário mas é aconselhável um *site* alternativo distante, uma vez que uma grande falha pode afetar um *site* ou região. A reposição do serviço pode não acontecer de forma

imediata, mas deve respeitar os parâmetros RPO, RTO e MTD descritos no BIA (Schmidt, 2006).

1.4. ISO 22301

A norma ISO 22301 é uma norma internacional desenvolvido pela ISO – *International Organization for Standardization*.

As normas ISO são documentos cridos por grupos de especialistas que determinem os requisitos, especificações, características e guias que podem ser utilizados para assegurar que materiais, produtos, processos e serviços são desenvolvidos com qualidade para os seus propósitos. Deste modo é possível assegurar que os produtos ou serviços são seguros e têm qualidade e fiabilidade. Para as empresas as normas ISO são ferramentas para reduzir custos, minimizando desperdícios e erros, aumentando a produtividade. (International Organization for Standardization - Standards, 2014)

A ISO 22301 surge como uma norma internacional de referência no seguimento da norma Britânica BS25999 (Whitcher, 2009), e especifica os requisitos para planear, estabelecer, implementar, operar, monitorizar, rever e manter o processo de melhoria contínua e um plano de continuidade de negócio de modo a que as organizações possam recuperar de eventos que provoquem a disrupção da atividade. Assim a ISO 22301 é uma norma genérica com princípios aplicáveis a todas as organizações. (St-GERMAIN)

Segundo a ISO 22301 (ISO 22301, 2012) uma gestão de continuidade de negócio contribui para uma sociedade mais resiliente. E deve conter os componentes chave descritos na tabela abaixo

Componente	Descrição
C1	Política.
C2	Responsabilidades bem definidas.
C3	Gestão do processo relativo a: • Política • Planeamento • Implementação e operação • Performance • Gestão das revisões • Melhoria
C4	Documentação com evidências auditáveis.

C5	Um plano de continuidade de negócio relevante para a organização.

Tabela 2 - Componentes chave da gestão de continuidade de negócio

Fonte: (ISO 22301, 2012)

A ISO 22301 utiliza um modelo "*Plan-Do-Check-Act*" mantendo a coerência com as normas ISO de gestão de sistemas (ISO 22301, 2012).

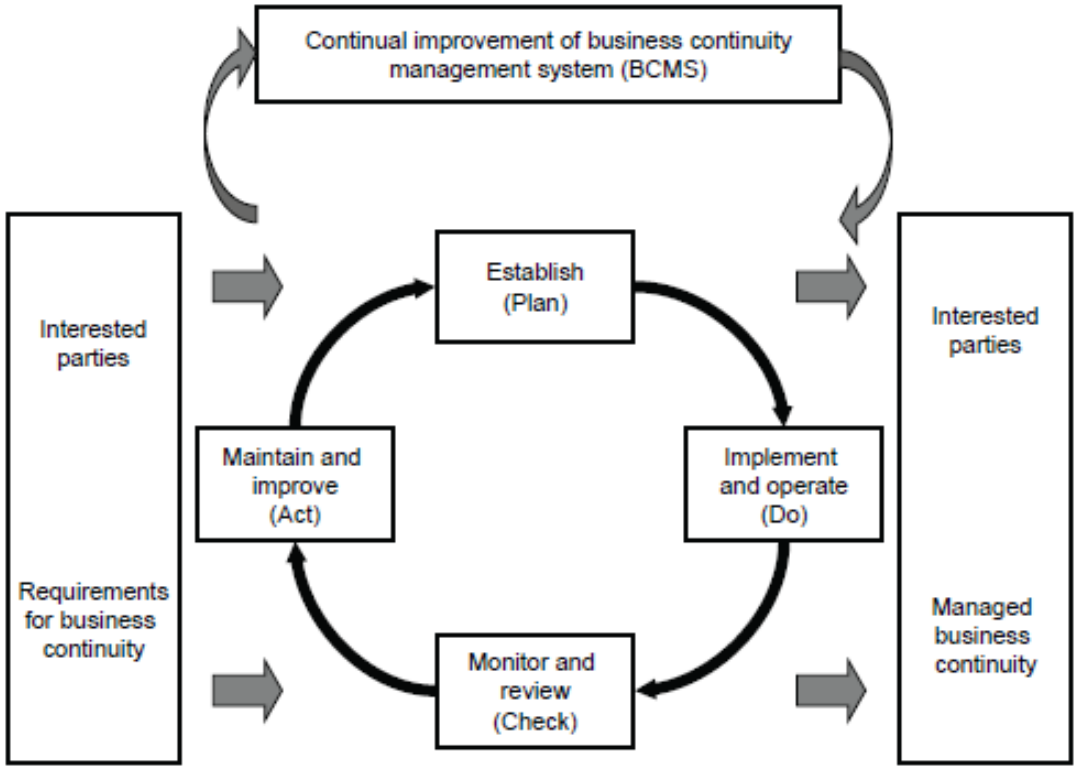


Fig. 2 - Modelo PDCA aplicado ao plano de continuidade de negócio.

Fonte: (ISO 22301, 2012)

Este modelo assenta no processo de melhoria continua através de quatro atividades como apresentado da tabela abaixo.

Atividade	Descrição
Planear (*Establish (plan)*)	Estabelecer o plano de continuidade de negócio contendo as políticas, objetivos, objetos, controlos, processos e procedimentos relevantes de modo a atingir resultados alinhados com as políticas e objetivos da organização.
Implementar (*Implement and operate*	Implementar as politica, controlos, processos e procedimentos definidos na atividade anterior.

(do))	
Verificar (*Monitor and review (Check)*)	Monitorizar e avaliar a performance face aos objetivos e politicas definidas e reportar os resultados para revisão da gestão que deverão determinar e autorizar as ações de melhoria.
Atuar (*Maintain and improve (Act)*)	Manter e melhorar o plano de continuidade da atividade através de ações corretivas baseadas na atividade de revisão, readaptando o plano, as politica e os objetivos.

Tabela 3 - Atividades do modelo PDCA

Fonte: (ISO 22301, 2012)

1.4.1. Contexto da organização

Segundo a PECB (St-GERMAIN) o objetivo desde tema é determinar todas as questões internas e externas relevantes para o resultado do PCN tais como:

- As atividades, funções, serviços, produtos, parcerias, cadeias de abastecimento, relações com as partes interessadas e impacto potencial dos incidentes disruptivos.
- Ligação entre o PCN e os objetivos da organização e as suas políticas.
- A apetência da organização pelo risco.
- As necessidades e expectativas das partes interessadas.
- Requisitos legais e regulatórios aplicáveis ao contexto da organização.

Assim é necessário identificar o âmbito do PCN tendo em conta os objetivos estratégicos do negócio, os produtos e serviços chave, a tolerância ao risco, obrigações legais e regulatórias e obrigações contractuais (St-GERMAIN).

Fig. 3 - Alinhamento do PCN com os objetivos da organização

Fonte: (St-GERMAIN)

A organização deve determinar todas as questões importantes para o PCN, considerando tanto as questões internas como externas e deve criar um documento identificando os seguintes pontos (ISO 22301, 2012)

- Identificação das atividades, funções, serviços, produtos, parcerias, fornecedores. Impacto para estas atividades de um evento disruptivo.
- Pontos de ligação entre as políticas de continuidade do negócio e os objetivos e políticas da organização incluindo a estratégia global de risco.
- A apetência ao risco da organização.

No seu contexto a organização deve:

- Articular os seus objetivos com o plano de continuidade de negócio.
- Definir os fatores internos e externos que potenciam o risco.
- Definir o critério de risco tendo em conta a apetência ao risco da organização.
- Definir o propósito do PCN.

Na criação de um PCN a organização deve determinar:

- Todas as partes interessadas para o PCN.
- Os requisitos de todos os interessados.

A organização deve de ter em conta os requisitos legais e regulatórios da sua atividade na criação e implementação do PCN. Deve ser criado um documento e mantido atualizado com os requisitos legais e regulatórios da sua atividade no que diz respeito à continuidade de negócio, operações, produtos ou serviços (ISO 22301, 2012)

Antes da criação do PCN a organização deve definir o âmbito do plano, deixando bem claro qual a aplicabilidade e o seu campo de ação, ao definir o âmbito deve ter em conta os fatores identificados nos pontos anteriores. No documento de definição de âmbito a organização deve (ISO 22301, 2012)

- Determinar as áreas da organização a incluir no PCN.
- Estabelecer os requisitos do PCN, considerando a missão, objetivos, obrigações internas e externas da organização.
- Identificar produtos e serviços e todas as atividades relacionadas dentro do âmbito do PCN.
- Ter em conta as necessidades e interesses de todas as partes como clientes, investidores, acionistas, cadeia de fornecimento, necessidades da comunidade, expectativas dos interessados.
- Definir o âmbito do PCN em termos da natureza, tamanho, complexidade da organização.

1.4.2. Papel da Gestão, liderança

A gestão de topo deve demostrar compromisso com o PCN. Através da liderança e ações, a gestão de topo deve criar um ambiente em que os diferentes atores se envolvam e consigam operar de modo eficaz para a concretização dos objetivos. Assim a gestão de topo é responsável por (St-GERMAIN):

- Assegurar que o PCN é compatível com a estratégia da organização.
- Integrar os requisitos do PCN nos processos da empresa.
- Disponibilizar os recursos necessários.
- Comunicar a importância do PCN.
- Assegurar que o PCN atinge os resultados esperados.
- Dirigir e suportar o processo de melhoria continua.
- Estabelecer e comunicar a política de continuidade de negócio.
- Assegurar que os objetivos e planeamento do PCN são efetuados.
- Assegurar que as responsabilidades dos principais papéis são atribuídas.

A gestão de topo deve demostrar liderança e compromisso com o PCN (ISO 22301, 2012):

Assegurar que as políticas e objetivos estabelecidos para o PCN são compatíveis com a estratégia da gestão para a organização.

- Assegurar a integração dos requisitos do PCN no processo de negócio da organização.
- Assegurar a disponibilidade dos recursos necessários para o PCN.
- Comunicar a importância do PCN.
- Assegurar que o PCN atinge os objetivos definidos.
- Orientar e apoiar as pessoas envolvidas com o PCN.
- Promover a melhoria continua.
- Apoiar outras áreas de gestão demostrando liderança e compromisso com o PCN.

A gestão de topo deve assegurar que as responsabilidades para papéis relevantes são atribuídas e comunicadas à organização (ISO 22301, 2012)

- Definir critérios de aceitação para riscos e definir quais os níveis aceitáveis de risco.
- Participar altivamente nos testes.
- Assegurar que são efeituadas auditorias ao PCN.
- Demostrar o seu empenho na melhoria continua.

A gestão de topo deve assegurar que a política definida compra os seguintes requisitos (ISO 22301, 2012)

- A política deve ser apropriada à atividade da organização.
- A política deve definir uma *framework* para definir os objetivos da continuidade de negócio.
- A política deve satisfazer os requisitos definidos.
- A política deve enfatizar a melhoria contínua do PCN.

A política do PCN deve (ISO 22301, 2012):

- Estar disponível como documento.
- Ser comunicada à organização.
- Estar disponível a todas as partes interessadas.
- Ser revista em intervalos definidos ou caso exista uma mudança significativa.

1.4.3. Planeamento

Esta fase é uma fase crítica para o PCN uma vez que é nesta fase que são estabelecidos os objetivos estratégicos e os princípios gerais do PCN. Os objetivos do PCN são uma expressão das intenções da organização de tratar os riscos identificados. Os objetivos identificados devem (St-GERMAIN):

- Ser consistentes com a política de continuidade de negócio.
- Ter em conta o nível mínimo de serviço aceitável para a organização.
- Ser mesuráveis.
- Ter em conta os requisitos.
- Ser monitorizados e atualizados sempre que necessário.

Na criação do planeamento para o PCN as organizações devem ter em conta os requisitos levantados nos pontos anteriores e determinar os riscos e oportunidades (ISO 22301, 2012).

- Assegurar que pode atingir os objetivos propostos.
- Prevenir ou reduzir efeitos indesejados.
- Atingir a melhoria continua.

A organização deve planear:

- As ações para endereçar os riscos e oportunidades.
- Integrar e implementar as ações no processo de continuidade de negócio.
- Avaliar a aplicação dessas ações.

A gestão de topo deve assegurar que os objetivos são estabelecidos e comunicados a todas as funções e níveis relevantes da organização. (ISO 22301, 2012)

Os objetivos devem:

- Ser consistentes com a política de continuidade de negócio.

- Ter em conta o nível mínimo de produção ou serviço que é aceitável apara a organização.
- Ser mensuráveis.
- Ter em conta os requisitos definidos.
- Ser monitorizados e atualizados.

A organização deve manter os objetivos documentados. Para criar o documento de objetivos da continuidade da atividade deve determinar (ISO 22301, 2012)):

- Quem é o responsável.
- O que vai ser feito.
- Quais os recursos necessários.
- Quando irá ficar completo.
- Como vão ser avaliados os resultados.

1.4.4. Suporte

A gestão eficiente do PCN no dia-a-dia assenta na utilização dos recursos adequados para cada tarefa. Esses recursos incluem pessoal competente e com formação adequada, o suporte dos serviços, comunicação, e recursos suportados por documentação eficiente. Tanto a comunicação interna como externa devem ser consideradas nesta área, incluindo o formato, o conteúdo e o *timing* (St-GERMAIN).

A organização deve determinar e fornecer os recursos necessários para a criação, implementação, manutenção e melhoria contínua do PCN, para isso a organização deve (ISO 22301, 2012)

- Determinar as competências necessárias das pessoas que irão executar o PCN.
- Assegurar que essas pessoas são competentes e tem a educação, formação e experiencia adequada.
- Quando aplicável tomar ações de forma a adquirir competências e avaliar o resultado dessas ações.
- Manter a documentação apropriada como evidencia das competências.

As pessoas que efetuam trabalho sobre o controlo da organização devem ter conhecimento (ISO 22301, 2012)

- Da política de continuidade do negócio.
- O seu papel e contributo para o PCN.
- As implicações de não seguir o PCN.
- Seu papel em caso de incidente disruptivo.

A comunicação assume um papel de relevo em caso de ocorrência de um incidente disruptivo. A organização deve determinar a relevância da comunicação interna e externa incluindo (ISO 22301, 2012):

- O que deve ou não ser comunicado.
- Quando comunicar.
- A quem comunicar.

A organização deve criar, implementar e manter um procedimento para (ISO 22301, 2012):

- Comunicar internamente às partes interessadas e aos empregados da organização.
- Comunicar externamente aos clientes, parceiros, comunidade local, e outras partes interessadas como a comunicação social.
- Receber, documentar e responder a comunicação das partes interessadas.
- Adaptar ou integrar um sistema de alerta de ameaças regional ou nacional.
- Assegurar a disponibilidade dos meios de comunicação durante um evento disruptivo.
- Comunicar com as autoridades.
- Operar e testar o plano de comunicação a utilizar em caso de evento disruptivo.

O PCN deve incluir (ISO 22301, 2012)

- A documentação referida nesta ISO.
- Toda a documentação que a organização considere pertinente para o sucesso do PCN, esta documentação pode variar segundo:
    - O tamanho da organização e o seu tipo de atividades, processos, produtos e serviços.
    - A complexidade dos processos e as suas interações.
    - A competência das pessoas envolvidas.

Na criação do documento a organização deve assegurar (ISO 22301, 2012)

- A identificação e descrição do documento (Titulo, data, autor, e/ou numero de referencia)
- Formato (linguagem, versão software, etc.) e media (formato eletrónico, papel, etc.)

Toda a documentação deve ser controlada para assegurar (ISO 22301, 2012):

- A sua disponibilidade.
- A proteção adequada (perca de informação, confidencialidade, integridade).

Para controlar a informação do documento a organização endereçar as seguintes atividades sempre que aplicável (ISO 22301, 2012)

- Distribuição, acesso, recuperação e utilização.
- Preservação.
- Controlo de alterações.
- Recuperação e utilização.
- Preservação da sua legibilidade (o documento deve ser de leitura clara).
- Preservação de utilização de informação obsoleta.

1.4.5. Operação

Depois do planeamento a organização deve operacionalizar o PCN, esta fase inclui (St-GERMAIN):

- *Business Impact Analysis* (BIA) – Identificação dos processos e serviços críticos para a organização, as interdependências entre processos assim como os recursos mínimos necessários para operar os processos identificados.
- Avaliação do Risco – O objetivo desta fase é criar, implementar e manter um documento formal que identifique e analise o rico de incidentes disruptivos de forma sistemática.
- Estratégia de continuidade de negócio – Depois de estabelecidos os requisitos e através do BIA e da avaliação do risco, podem ser desenvolvidas estratégias para proteção e recuperação das atividades críticas tendo em conta a tolerância ao risco da organização e respeitando os *timings* de recuperação.
- Procedimentos de continuidade de negócio – a organização deve documentar os procedimentos de recuperação de modo a assegurar a recuperação das atividades e a gestão de incidentes disruptivos, os procedimentos devem:
    - Estabelecer o protocolo de comunicação interno e externo.
    - Ser específicos com paços claros a serem executados durante o incidente disruptivo.
    - Ser flexíveis de modo a responderem a ameaças inesperadas.
    - Devem se focar no impacto dos eventos disruptivos.
    - Devem ser desenvolvidos com atenção as interdependências.
    - Devem ser eficazes a minimiar as consequências e conter estratégias de mitigação adequadas.
- Teste – de forma a assegurar que os procedimentos de continuidade de negócio são eficazes e alinhados com os objetivos de continuidade, a organização deve promover testes periódicos. Os testes são uma forma de validar os planos e estratégias de continuidade de negócio são adequados para responder de forma eficaz aos incidentes e dentro dos *timings* definidos.

A organização deve planear implementar e controlar o processo, para implementar as ações descritas nos pontos anteriores a organização deve (ISO 22301, 2012)

- Estabelecer um critério para os processos.

- Implementar um mecanismo de controlo de processos com base nos critérios definidos.
- Manter um registo na medida do necessário para ter confiança que os processos têm sido executados conforme definido.

A organização deve estabelecer, implementar e manter um processo formal e documentado para o *business impact analysis and risk assessment* que (ISO 22301, 2012):

- Estabeleça o contexto de avaliação, definição de critério e a avaliação do impacto potencial de um evento disruptivo.
- Tenha em conta os requisitos legais e outros que a organização considere relevantes.
- Inclua uma análise sistemática, priorização de tratamento do risco e dos custos relacionados.
- Definir os requisitos de output do *business impact analysis and risk assessment.*
- Especifique os requisitos para que a informação seja atualizada e permaneça confidencial.

A organização deve estabelecer, implementar, e manter um processo formal e documentado para determinar as prioridades, os objetivos e objetos de recuperação. Este processo deve incluir a avaliação dos impactos dos eventos disruptivos nos produtos e serviços da organização (ISO 22301, 2012)

O BIA deve incluir o seguinte:

- Identificar as atividades que suportam o negócio.
- Avaliar os impactos nas atividades ao longo do tempo.
- Determinar prazos para retomar as diversas atividades dentro de um nível mínimo aceitável, tendo em conta o prazo máximo a partir do qual não é aceitável para o negócio.
- Identificar dependências e os recursos essenciais para as atividades incluindo, fornecedores, parceiros, e outras partes relevantes.

A organização deve criar, implementar e manter um processo de avaliação de riscos formalmente documentado que sistematicamente identifique, analise e avalie o risco de eventos disruptivos para a organização (ISO 22301, 2012)

A organização deve:

- Identificar os riscos de eventos disruptivos para as atividades, processos, sistemas, informação, pessoas, bens, parceiros, e outros recursos que os suportem.
- Analisar os riscos de forma sistemática.
- Avaliar que eventos disruptivos querem intervenção.

- Identificar ações compatíveis com os objetivos de continuidade de negócio e a apetência da organização pelo risco.

A estratégia de continuidade do negócio deve basear-se nos outputs do *business impact analysis and risk assessment*. A organização deve determinar a estratégia apropriada para: (ISO 22301, 2012)

- Proteger as atividades com maior relevância para o negócio.
- Estabelecer, continuar, retomar as atividades priorizadas e as suas dependências, suportes e recursos.
- Mitigar, respondendo e gerindo os impactos.

A organização deve determinar os requisitos e recursos para implementar as estratégias escolhidas, os tipos de recursos a considerar devem ser os seguintes entre outros que a organização considere relevantes (ISO 22301, 2012)

- Pessoas.
- Informação e dados.
- Edifícios, ambiente de trabalho.
- Instalações, equipamento e consumíveis.
- Sistemas e tecnologias de informação e comunicação.
- Transporte.
- Budget.
- Parceiros e fornecedores.

Para tratamento dos riscos identificados as organizações devem considerar as seguintes medidas proactivas (ISO 22301, 2012)

- Reduzir a probabilidade de disrupção.
- Reduzir o período de disrupção.
- Limitar o impacto das disrupções nos produtos e serviços chave da organização.

A organização deve criar, implementar e manter procedimentos de continuidade da atividade para gerir os incidentes disruptivos e continuar as atividades baseado nos objetivos de recuperação identificados no BIA (ISO 22301, 2012).

Os procedimentos devem:

- Estabelecer o protocolo de comunicação interno e externo.
- Ser específicos e claros com os passos necessários para retomar a atividade em caso de disrupção.
- Ser flexíveis para responder a ameaças imprevistas e mudanças das condições internas e externas.

- Ser focados no impacto dos eventos disruptivos.
- Ser desenvolvidos com base em prossupostos estabelecidos e na análise de interdependências.
- Deve ser eficaz para minimizar as consequências, através de estratégias de mitigação adequadas.

A organização deve criar, documentar e implementar procedimentos e uma estrutura para responder a incidentes disruptivos através de pessoal com a responsabilidade, autoridade e competência para gerir o incidente (ISO 22301, 2012)

A estrutura de resposta deve:

- Identificar o *threshold* que justifique o início da resposta formal.
- Avaliar a natureza e extensão do incidente disruptivo e o seu potencial impacto.
- Ativar a resposta de continuidade do negócio apropriada.
- Ter processos e procedimentos para a ativação, operação, coordenação e comunicação.
- Ter recursos disponíveis para suportar o processo e os procedimentos de gestão de incidentes disruptivos de forma a minimizar o impacto.
- Comunicar com as partes interessadas, autoridades e a média.

Devem existir procedimentos atualizados para:

- Detetar um incidente.
- Monitorizar um incidente.
- Comunicação interna com a organização documentada.
- Comunicação documentada com as entidades nacionais ou regionais de aviso de riscos.
- Assegurar os meios de comunicação durante um incidente disruptivo.
- Estrutura definida de comunicação com as entidades de emergência.
- Registo de informação vital sobre o incidente, ações e decisões tomadas.
    - Alerta das partes interessadas do impacto potencial do incidente.
    - Assegurar a interoperabilidade das organizações e ou pessoal envolvido na resposta ao incidente.
    - Assegurar o funcionamento dos meios de comunicação.

A organização deve estabelecer procedimentos documentados de reposta a incidentes disruptivos e de como recuperar as atividades afetadas num espaço de tempo predefinido. Estes procedimentos devem endereçar os requisitos de quem os vai executar (ISO 22301, 2012).

O PCN deve:

Definir os papéis e responsabilidades das pessoas e equipas que tem autoridade durante um incidente.

- Definir um processo para ativar a resposta.
- Detalhar como gerir as consequências imediatas de um incidente:
    - O bem-estar os indivíduos.
    - A estratégia e opções operacionais para responder ao incidente.
    - Prevenção de indisponibilidade futura das atividades prioritárias.
- Detalhar como e em que circunstancias a organização irá comunicar com os funcionários.
- Como a organização irá recuperar as suas atividades prioritárias dentro do tempo período definido.
- Detalhes de como a organização deve responder à comunicação social apos um incidente, incluindo.
    - Estratégia de comunicação.
    - Interface com a comunicação social.
    - Guia ou *template* para escrever uma comunicação para a comunicação social.
    - Definir as pessoas que podem comunicar com a comunicação social.

Cada plano deve definir:

Propósito e âmbito.

- Objetivos.
- Critérios e procedimentos de ativação.
- Procedimentos de implementação.
- Papéis, responsabilidades e autoridades.
- Procedimentos e requisitos de comunicação.
- Interdependências internas e externas.
- Requisitos de recursos.
- Fluxo de informação e processos de documentação.

A organização deve ter documentados os procedimentos de *restore* e retoma da atividade depois das medidas temporárias aplicadas após um incidente, de forma a retomar o seu normal funcionamento (ISO 22301, 2012)

A organização deve testar com regularidade os procedimentos de continuidade de negócio de modo a assegurar a seu alinhamento com os objetivos definidos (ISO 22301, 2012).

A organização deve promover testes que:

- Sejam consistentes e no âmbito do PCN.
- Sejam baseados em cenários apropriados, bem planeados e com objetivos bem definidos.

- Feitos ao longo do tempo validem juntos o plano num todo, devem envolver todas as partes interessadas.
- Devem minimizar o risco de disrupções na normal atividade.
- Devem produzir relatórios com os resultados, recomendações e ações para implementar possíveis melhorias.
- Os testes devem de ser revistos num processo de melhoria continua.
- Os testes devem ser feitos em intervalos planeados ou sempre que existam alterações significativas na organização ou no ambiente onde opera.

Tipo de Teste	O que fazer	Benefícios	Desvantagens
Checklist	Distribuir planos para revisão	Assegura que os planos endereção todas as atividades	Não aborda a eficácia
Passo a passo	Verificar cada passo do PCN	Assegura que as atividades planeadas estão bem descritas no PCN	Baixo valor em provar as capacidades de resposta
Simulação	Cenário para testar procedimentos de recuperação	Sessão de prática	Quando os subconjuntos são muito diferentes
Paralelo	Teste total sem parar o *site* primário	Assegura elevados níveis de fiabilidade sem interromper o normal funcionamento	Dispendioso uma vez que todo o pessoal esta envolvido
Disrupção	Simulação de desastre com disrupção do serviço	Teste mais confiável ao PCN	Elevado risco

Tabela 4 - Tipos de teste ao PCN, benefícios e desvantagens

Fonte (St-GERMAIN)

1.4.6. Avaliação de performance

Uma vez implementado o PCN o ISO 22301 defende que deve existir uma monitorização permanente assim como testes periódicos, de modo a rever e melhorar a operação (St-GERMAIN)

- Monitorizar se as políticas de continuidade de negócio estão a ser cumpridas.
- Medir a performance dos processos, procedimentos, funções e verificar a conformidade com a ISO 22301.
- Monitorizar o histórico de evidências de performance do PCN.
- Promover auditorias internas periódicas.

Segundo a ISO 22301 (ISO 22301, 2012) a organização deve determinar:

- O que deve ser monitorizado e medido.
- Os métodos de monitorização, medida, análise e avaliação, de modo a assegurar resultados validos.
- Quando a monitorização e medição devem ser efetuados.
- Quando os resultados da monitorização devem ser analisados e avaliados.

A organização deve:

- Tomar uma ação sempre que necessário para endereçar os resultados, antes que ocorra uma não conformidade.
- Guardar todos os documentos que sejam evidencia.

Os procedimentos de monitorização devem fornecer:

- Um conjunto de métricas apropriadas à organização.
- Monitorizar em que medida o PCN e os seus objetivos são cumpridos.
- Indicadores de performance dos processos, procedimentos e funções que protegem as atividades prioritárias.
- Monitorizar a conformidade dos objetivos de continuidade de negócio com a ISO 22301.
- Monitorizar as evidências históricas de deficiências do PCN.
- Guardar os resultados do processo de monitorização e avaliação de forma a facilitar as ações corretivas.

Avaliação dos procedimentos do PCN (ISO 22301, 2012):

- A organização deve promover avaliações aos procedimentos do PCN de forma a assegurar a sua adequação e efetividade.
- As avaliações devem ser feitas através de revisões periódicas, exercidos, testes, relatórios pós incidente e indicadores de performance. Alterações significativas devem ser refletidas nos procedimentos.
- A organização deve avaliar periodicamente o cumprimento legal e regulatório assim como a aplicação das melhores práticas da indústria e a conformidade com os seus próprios objetivos de continuidade de negócio.

- A organização deve promover avaliações periódicas ou quando exista uma alteração significativa.

A organização deve promover auditorias internas em intervalos planeados para avaliar o sistema de continuidade de negócio (ISO 22301, 2012). Verificar se o sistema de continuidade da atividade está conforme:

- Os requisitos da organização para o PCN.
- Os requisitos da ISO 22301.
- Verificar se o sistema está implementado e mantido atualizado.

A organização deve:

- Planear, estabelecer, implementar e manter um programa de auditoria, incluindo a sua frequência, os seus métodos, responsabilidades, requisitos de planeamento e relatório. O programa de auditoria deve ter em consideração a importância dos resultados das auditorias anteriores.
- Definir os critérios e âmbito de auditoria.
- Selecionar os auditores e conduzir as auditorias de modo a garantir objetividade e imparcialidade em todo o processo.
- Assegurar que os resultados das auditorias são entregues a todos os gestores relevantes para o processo.
- As evidências devem ser guardadas como prova da implementação do plano de auditoria.

A gestão de topo deve rever o PCN, em períodos pré estabelecidos para assegurar que o PCN continua adequado (ISO 22301, 2012).

A revisão deve incluir as seguintes considerações:

- O estado das ações de revisões anteriores.
- Alterações internas e externas relevantes para o PCN.
- Indicadores de performance do PCN, incluindo:
    - Não conformidades e ações corretivas.
    - Avaliação de resultados do processo de monitorização e avaliação.
    - Resultados de auditorias.
- Oportunidade de melhoria continua.

A revisão deve considerar a performance da organização incluindo:

- O acompanhamento de ações de revisões prévias.
- A necessidade de alteração do PCN incluindo politica e objetivos.
- Oportunidade de melhoria.
- Resultados de auditorias e revisões ao PCN.

- Técnica, produtos ou procedimentos que possam ser utilizados na organização para melhorar o PCN.
- Estado das ações corretivas.
- Resultados dos testes.
- Riscos não endereçados corretamente na avaliação de risco.
- Alterações que possam afetar o PCN sejam internas ou externas.
- Verificar se a politica continua adequada.
- Recomendações de melhoria.
- Lições aprendidas e ações resultantes de incidentes disruptivos.
- Novas boas práticas.

O resultado da revisão deve incluir decisões de melhoria continua e possíveis necessidades de alteração ao PCN e devem incluir o seguinte sempre que aplicável (ISO 22301, 2012):

- Alterações ao âmbito do PCN.
- Melhorias na eficácia do PCN.
- Atualização da avaliação de risco, BIA, PCN e procedimentos relacionados.
- Modificação de procedimentos e controlos para responder a eventos internos e externos que possam impactar o PCN incluindo:
    - Requisitos operacionais e de negócio.
    - Requisitos de segurança e redução de risco.
    - Processos operacionais.
    - Requisitos legais e regulatórios.
    - Obrigações contractuais.
    - Níveis de risco e critérios de aceitação de riscos.
    - Recursos necessários.
    - Requisitos de budget.
- Eficácia dos controlos e medidas.

Toda a documentação deve ser guardada como evidencia e os resultados da revisão devem ser comunicados às partes interessadas, e devem ser tomadas as ações apropriadas para implementar as ações necessárias (ISO 22301, 2012)

1.4.7. Melhoria

A melhoria contínua pode ser definida como as ações que a organização toma para aumentar a eficácia e eficiência dos processos e controlos, de forma a alcançar benefícios para a organização e para os *stakeholders*. A organização pode melhorar de forma contínua, aumentado a eficiência do PCN através da sua política de continuidade de negócio, objetivos, resultados de auditorias, análise dos eventos monitorizados, indicadores, ações corretivas e revisão do processo de gestão (St-GERMAIN)

Sempre que existam não conformidades a organização deve (ISO 22301, 2012):

- Identificar a não conformidade.
- Reagir à não conformidade.
    - Tomar ações corretivas de modo a eliminar a não conformidade.
    - Lidar com as consequências.
- Avaliar a necessidade das ações para eliminar as causas da não conformidade.
    - Rever a não conformidade.
    - Determinar as causas da não conformidade.
    - Verificar se existem não conformidades idênticas.
    - Avaliar a necessidade de ações corretivas de forma a assegurar que a não conformidade não volta a ocorrer no PCN.
    - Determinar e implementar as ações corretivas.
    - Rever a eficácia das ações implementadas.
    - Alterar o PCN de necessário.
- Implementar as ações necessárias.
- Rever a eficácia das ações corretivas implementadas.
- Altear o PCN sempre que necessário.

A organização deve guardar todos os documentos como evidencia de:

- Não conformidades e das ações corretivas implementadas.
- Resultados das ações corretivas implementadas.

1.5. Alta disponibilidade

Quando falamos em alta disponibilidade, falamos na capacidade de recuperar de falhas num curto espaço de tempo e de forma automática. As falhas podem dar-se no equipamento, ambiente ou ser resultado de erro humano, o importante é recuperar no menor espaço de tempo possível (Schmidt, 2006).

Para (Janssen, 2014) Alta disponibilidade refere-se a sistemas duráveis que operam de forma contínua sem falhas durante um longo período de tempo. O termo implica que as partes do sistema foram testadas e em muitos casos existem existe tolerância a falha através de componentes redundantes.

Segundo (Weygant, 2001) a alta disponibilidade caracteriza um sistema desenhado para evitar a perca de serviço, reduzindo ou gerindo as falhas, assim como minimizando os períodos de *downtime* planeados no sistema. É esperado que um serviço seja de alta disponibilidade quando a vida, saúde e bem-estar, incluindo o bem-estar da empresa dependem dele.

Em muitos negócios a disponibilidade dos sistemas informáticos é tão importante como a eletricidade. Os sistemas de alta disponibilidade são desenhados para operar com o mínimo *downtime* planeado e não planeado (Weygant, 2001).

De um modo geral um sistema de alta disponibilidade pode ser definido como um sistema capaz de assegurar um elevado nível de disponibilidade num determinado período de tempo (Microsoft, 2008).

Taxa de *Uptime*	*Downtime* Anual
99%	87 *hours* 36 *minutes*
99.9%	8 *hours* 46 *minutes*
99.99%	*52 minutes 34 seconds*
99.999%	5 *minutes* 15 *seconds*

Tabela 5 - Taxa de *uptime* vs. *Downtime* anual

Fonte (Microsoft, 2008)

1.5.1. Disponibilidade

Para melhor compreender a alta disponibilidade temos de a definir e quantificar.

A disponibilidade é a medida da quantidade de tempo que um sistema ou componente está disponível (Schmidt, 2006).

A taxa de disponibilidade é expressa em percentagem de tempo que o sistema está disponível. Por exemplo um sistema com uma taxa de disponibilidade de 99,9% durante um ano significa que o sistema teve um *downtime* aproximado de 8.75h, ou de outra forma, para atingir uma disponibilidade de 99,9% o sistema só pode estar indisponível 40 min a cada quatro semanas (Microsoft, 2008).

Para calcular a disponibilidade de um sistema é utilizado o rácio de *uptime* sobre o tempo total (*Uptime+downtime*) (Schmidt, 2006).

$$\text{availability} = \frac{\text{uptime}}{\text{uptime} + \text{downtime}}.$$

Fig. 4 - Fórmula de disponibilidade

Fonte (Schmidt, 2006)

1.5.2. Mean Time Between Failures

Outro indicador importante é o MTBF (mean time between failures), com este indicador podemos medir a fiabilidade de um componente do sistema (Weygant, 2001).

O MTBF é o tempo médio que decorre desde um estado sem falha ate à ocorrência de uma falha (Cisco Systems, Inc., 2004).

O MTBF é a média entre duas falhas de um componente.

$$\text{MTBF} = \frac{\text{Total Operating Time}}{\text{Total Number of Failures}}$$

Fig. 5 - Fórmula de cálculo do MTBF

Fonte (Weygant, 2001)

1.5.3. Mean Time To Repair

Este indicador dá o tempo médio de recuperação de uma determinada disrupção. (Schmidt, 2006),

Por outras palavras é o tempo medio necessário para diagnosticar e resolver um problema, de forma manual ou automática (Cisco Systems, Inc., 2004).

O MTTR (Mean Time To Repair) pode ser calculado da seguinte forma:

MTTR = (Total down time) / (number of breakdowns)

A disponibilidade também pode ser calculada utilizando a seguinte fórmula:

$$\text{availability} = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}.$$

Fig. 6 - Fórmula de cálculo de disponibilidade utilizando MTBF e MTTR

Fonte (Weygant, 2001)

Esta fórmula demostra a importância de reduzir o MTTR para o aumento da disponibilidade (Schmidt, 2006).

Fatores que influenciam o MTTR numa rede (Cisco Systems, Inc., 2004):

- Falta de mecanismos de suporte e de técnicos com conhecimento da rede.

- Falta de documentação sobre a topologia e configuração da rede.
- Tamanho da rede pode dificultar a determinação da causa do problema.
- Alterações não documentadas e feitas sem respeitar o processo de *change management*.

1.5.4. Arquitetura

De modo a conseguir uma rede de alta disponibilidade é necessário pensar em todos os pontos possíveis de falha, e encontrar alternativas de modo a colmatar essas falhas.

Um dos principais aspetos a ter em conta ao desenhar uma arquitetura de sistemas de alta disponibilidade é a alimentação elétrica e a refrigeração dos equipamentos, assim de modo a providenciar um ambiente adequado devem ser aprovisionados UPS redundantes com gerador e A/C redundantes.

Segundo (Barroso, Clidaras, & Hölzle, 2013) os *datacenters* podem ser classificados numa escala de 1 a 4 segundo a distribuição de fontes de energia, UPS, dispositivos de refrigeração e redundância:

- *Tier* I - *Datacentres* com um único ponto de distribuição de energia, UPS única e um único sistema de refrigeração, sem componentes redundantes.
- *Tier* II – Adição de componentes redundantes ao *Tier* I (N+1) aumentando a disponibilidade.
- *Tier* III – *Datacentres* com uma fonte de energia ativa e uma alternativa. Cada caminho tem os seus componentes redundantes, providenciando redundância mesmo durante manutenções.
- *Tier* IV – *Datacenters* com duas fontes de energia e dois dispositivos de refrigeração ativos com componentes redundantes capazes de fornecer tolerância a falhas de quaisquer componentes sem impacto na capacidade.

Outro princípio básico é a redundância de equipamentos e *links* dentro da rede, e *links* redundantes de acesso ao exterior.

No que diz respeito aos *links* para o exterior devem sempre que possível, ser utilizados dois operadores diferentes com caminhos destintos e equipamentos redundantes de *routing* (Cisco Systems, Inc., 2004).

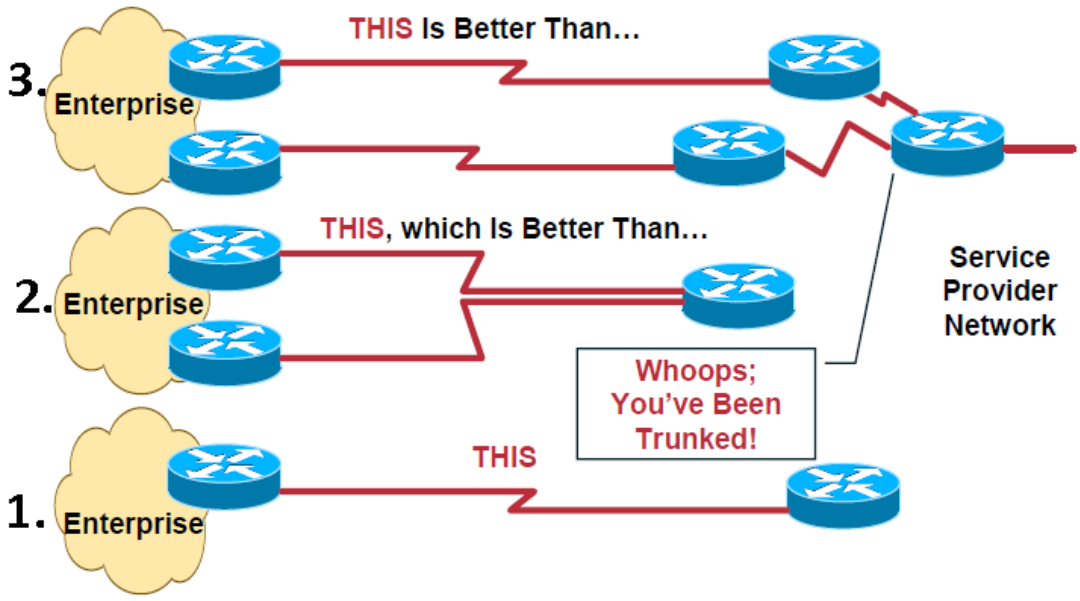


Fig. 7 - Redundância de *Links*

Fonte (Cisco Systems, Inc., 2004)

A imagem a cima representa três cenários de ligações ao exterior (Cisco Systems, Inc., 2004) :

- 1 – Um *router* único de saída ligado por um *link* único a um único operador. Este cenário não apresenta redundância logo representa um ponto de falha.
- 2 – Dois *routers* de saída ligados por dois *links* do mesmo operador ligados ao mesmo *endpoint* do operador. Neste cenário já existe redundância de equipamentos e *links* mas existe uma dependência excessiva do operador.
- 3 - Dois *routers* de saída ligados por dois *links* de operadores diferentes a *endpoints* diferentes, providenciando redundância de equipamentos, *links* e operadores, no entanto devido ao subaluguer de infraestruturas pelos operadores podemos encontrar pontos únicos de falha, no entanto este tipo de arquitetura é o que dá mais garantias de continuidade em caso de falhas.

Da mesma forma que devemos promover uma arquitetura redundante para as ligações exteriores, devemos promover o mesmo princípio dentro da rede, assim os equipamentos e caminhos devem de ser redundantes de modo a garantir que em caso de avaria ou quebra de conectividade o serviço não é comprometido.

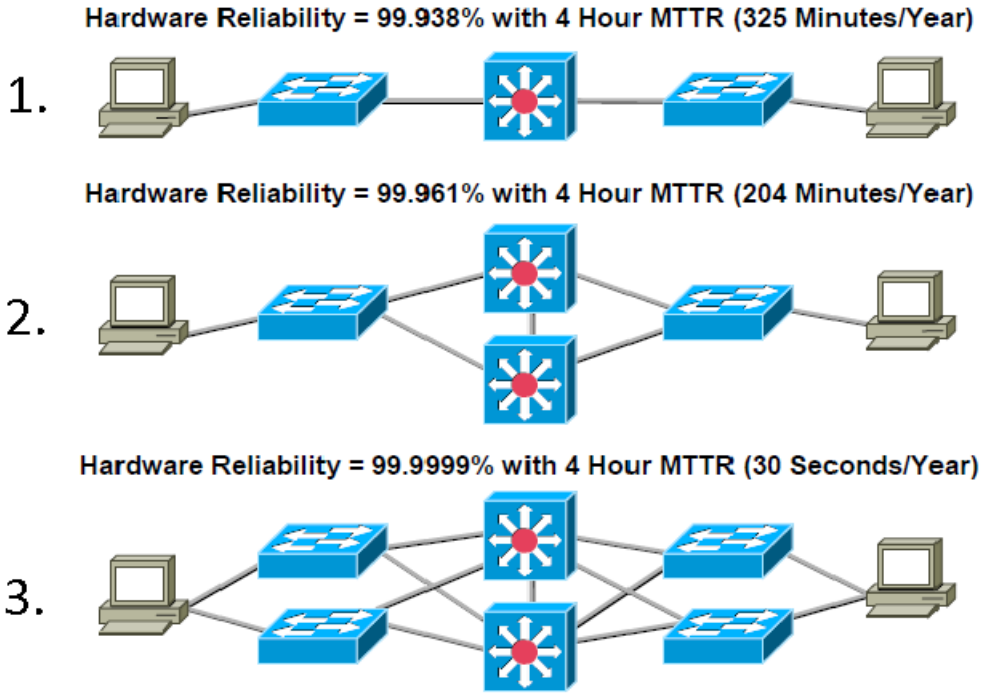


Fig. 8 - Topologias vs. *Uptime*

Fonte (Cisco Systems, Inc., 2004)

A imagem a cima mostra três cenários diferentes com os respetivos níveis de *uptime* esperado com um MTTR de 4 horas (Cisco Systems, Inc., 2004):

- 1 – Arquitetura simples sem redundância de equipamentos e *links*, neste cenário podemos esperar um *uptime* aproximado de 99,938%.
- 2 – Neste cenário é introduzida a redundância ao nível dos *switch* core e redundância de ligação dos *switch's* de piso, continuando a ser utilizado um *link* único para interligar *hosts* e equipamentos, este cenário apenas fornece redundância do *switch* core, a taxa de *uptime* aproximada com este tipo de arquitetura é de 99.961%.
- 3- Neste cenário é adicionada redundância dos *switchs* de piso e *links*. Assim temos caminhos alternativos em caso de quebra de *links* ou avaria de equipamentos atingindo um cenário *de full redundancy* onde podemos esperar uma taxa de *uptime* aproximada de 99.9999%.

Assim a chave para uma arquitetura de alta disponibilidade é a redundância, não só a redundância de equipamentos mas também de caminhos de rede e energia.

1.6. Virtualização

Para (Schmidt, 2006) a virtualização é a construção de uma camada de abstração dos recursos físicos. Este conceito é importante independentemente da tecnologia utilizada.

A virtualização é crucial para a implementação de redundância, fornecendo liberdade em relação aos recursos físicos permitindo troca-los conforme a necessidade ou alocando o serviço a outros componentes físicos.

Ao introduzir componentes redundantes na arquitetura com o objetivo de lidar com as potenciais falhas de um componente, não devemos vincula-los a uma instância específica, pois em caso de falha dessa instância todo o sistema ficaria comprometido, para evitar estas situações devemos criar um componente virtual que fornece serviço de forma independente do componente físico, podendo utilizar um qualquer componente físico para atribuir serviço.

Este conceito é aplicado não só a componentes de *hardware* mas também a componentes de *software*, assim o conceito de abstração pode ser aplicado a componentes de sistemas operativos como processos ou serviços, a bases de dados logicas ou web *services*, assim podemos ver a virtualização como um princípio básico em TI que permite um *design* de arquiteturas aplicáveis a alta disponibilidade e *disaster recovery* (Schmidt, 2006).

Segundo (Kusnetzky, 2011) com a virtualização podemos criar um ambiente artificial onde vários computadores são vistos com um computador, ou onde um computador físico pode conter vários computadores virtuais, o mesmo se passando com o *storage*, onde um bloco de *storage* grande pode ser apresentado como vários blocos de *storage* pequeno ou vários blocos pequenos de *storage* podem ser apresentados com um bloco de grandes dimensões.

Para (Kusnetzky, 2011) existem vários motivos para uma organização optar por virtualização, entre os quais:

- Permitir a qualquer *device* de rede aceder a qualquer aplicação através uma qualquer rede, mesmo quando a aplicação não foi desenhada para trabalhar com este tipo de *devices*.
- Isolamento de aplicações de modo a aumentar a segurança.
- Isolamento de aplicações do sistema operativo permitindo o seu funcionamento independentemente do sistema operativo base.
- Aumentar o número de pedidos suportados pela aplicação, criando varias instâncias em máquinas diferentes a correr de modo simultâneo.
- Diminuir o tempo que uma aplicação leva a correr, segmentando os dados ou a própria aplicação por vários sistemas.
- Otimização da utilização de um sistema único, permitindo uma maior carga.
- Aumentar a disponibilidade de uma aplicação, através de redundância.

2. Questão e objetivos de investigação

Tendo em conta a revisão da literatura surge a seguinte questão de investigação:

- Como pode ser operacionalizado um plano de continuidade de negócio?

Para responder à questão de investigação foram identificados alguns objetivos.

- O1 - Determinar o processo de implantação.
- O2 - Determinar as tecnologias utilizadas e a sua implantação.
- O3 - Determinar os processos de monitorização.
- O4 - Determinar a envolvência da gestão de topo no projeto.
- O5 - Verificar de que forma esta estratégia está alinhada com a atividade.

3. Metodologia

Para (Sekaran & Bougie, 2013) a investigação é um processo para encontrar soluções para problemas complexos apos o estudo e análise dos seus diversos fatores.

Segundo (Sekaran & Bougie, 2013) para produzir conhecimento científico é necessário aplicar um método com técnicas que assegurem a precisão do conhecimento produzido, assim torna-se necessário seguir uma metodologia apropriada de modo a garantir um trabalho de qualidade, neste trabalho foi utilizada a cebola de investigação de (Saunders, Lewis, & Thornhill, 2009) como guia metodológico.

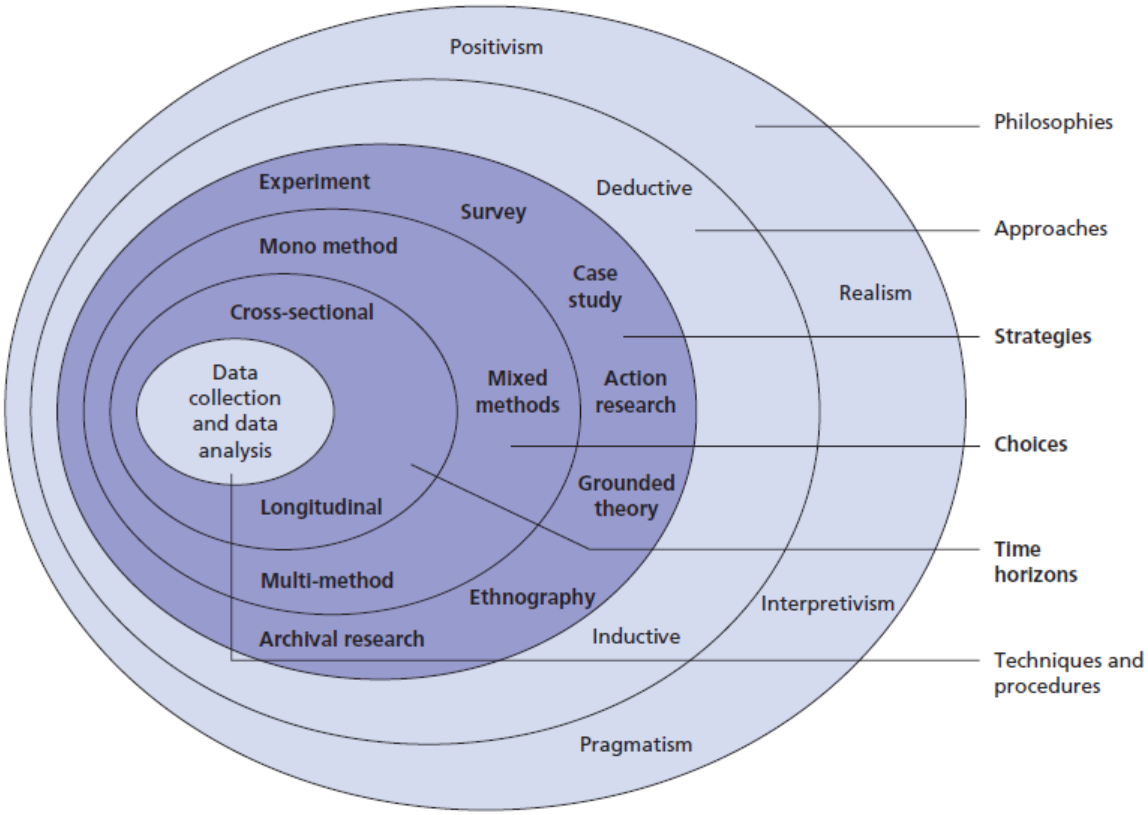


Fig. 9 - The research onion, the Research methods for business students

Fonte: (Saunders, Lewis, & Thornhill, 2009)

3.1. Filosofia

O primeiro passo para definir a metodologia é a filosofia de investigação. A forma como o investigador perceciona o mundo e o desenvolvimento de conhecimento determina o tipo de investigação a seguir (Saunders, Lewis, & Thornhill, 2009)

De acordo com (Saunders, Lewis, & Thornhill, 2009), existem quatro tipos de filosofias em investigação: positivismo, realismo, pragmatismo e interpretativíssimo. O positivismo advém das ciências naturais \ exatas, uma metodologia estruturada que facilita a sua replicação, observações e conclusões com base em casos que se comportam do mesmo modo e fundamentados em bases estatísticas.

Segundo (Saunders, Lewis, & Thornhill, 2009) o realismo é uma filosofia que tem na sua base a convicção que a realidade existe independentemente das ideias e crenças humanas. O realismo defende que os objetos da vida real têm uma existência independentemente da mente humana.

O Interpretativismo é a filosofia mais utilizada nas ciências sociais e considera variáveis que podem ter alterações em função do contexto onde estão inseridas e procura compreender a realidade de um determinado contexto sob investigação tentando encontrar explicações para as ações, motivos e intenções. (Saunders, Lewis, & Thornhill, 2009)

Já no pragmatismo o investigador adapta a sua visão da realidade permitindo obter a resposta à questão de investigação e considera validos os fenómenos observáveis assim como os seus significados, mais focado na investigação prática, integrando diversas perspetivas que ajudam a interpretar os dados, utiliza múltiplos métodos e abordagens da recolha de dados para a investigação. (Saunders, Lewis, & Thornhill, 2009)

Considerando que a investigação é um estudo de caso e a visão do investigador, a filosofia aplicada é o realismo, pois o objetivo é observar um fenómeno dentro do seu contexto.

Dentro do realismo existem dois caminhos a seguir, o realismo direto e o realismo crítico, enquanto o realismo direto defende uma visão em que o mundo é relativamente estável o realismo crítico tem uma visão mais abrangente, defendendo um estudo a vários níveis pois considera que a forma como interagem as estruturas, os processos e procedimentos têm influência na perceção do fenómeno de estudo. (Saunders, Lewis, & Thornhill, 2009)

Devido à complexidade do meio que envolve o fenómeno em estudo a filosofia adotada é o realismo crítico que defende que como investigadores só somos capazes de entender um fenómeno se compreendermos as estruturas sociais que deram origem ao fenómeno de estudo. (Saunders, Lewis, & Thornhill, 2009)

3.2. Abordagem de investigação

Quanto à abordagem da investigação existem dois caminhos possíveis, o método dedutivo e o método indutivo.

Segundo (Saunders, Lewis, & Thornhill, 2009) o método dedutivo assenta numa teoria ou conjunto que hipóteses e a investigação decorre no sentido de validar a teoria ou hipóteses. Já no método indutivo são recolhidos dados e observados fenómenos e a teoria surge da análise dos dados e observações, mais indicada para a compreensão do contexto onde ocorrem os factos, por este facto por norma as suas conclusões não são generalizadas.

Dedução	Indução
Princípios científicos	Entender o envolvimento da variável humana nos eventos estudados
Partir da teoria para os dados	Entendimento profundo do contexto dos eventos estudados
Necessidade de explicar relações casuísticas entre variáveis	Recolha de dados qualitativos
Recolha de dados quantitativos	Estrutura de estudo mais flexível com enfâse na evolução da investigação
Aplicação de controlos para validar os dados	Entendimento que o investigador é parte da investigação
Aproximação altamente estruturada	O principal intuito não é a generalização
Investigador é independente ao tema do estudo	
Necessidade de grande recolha de dados para poder generalizar	

Tabela 6 - Método Dedutivo vs. Indutivo

Fonte: (Saunders, Lewis, & Thornhill, 2009)

Após analisar as principais diferenças entre os dois métodos e sendo este trabalho um estudo de caso onde se pretende extrair conhecimento específico de um acontecimento no

seu contexto e o resultado não pretende ser generalizado a abordagem escolhida foi a indução.

3.3. Estratégia de investigação

De acordo como as estratégias de investigação disponíveis, este trabalho segue o estudo de caso, indicado para examinar um fenómeno no seu contexto natural, aplicando multi métodos de recolha de dados de modo a obter informação de várias entidades (Pessoas, grupos, organizações). (Benbasat, Goldstein, & Mead, 1987)

Segundo (Yin, 2013) o estudo de caso está indicado para investigações focadas em responder ao Como? e Porquê? de um determinado fenómeno, onde o investigador é confrontado com situações complexas que dificultam a identificação de variáveis importantes, quando o investigador procura encontrar relações entre fatores e quando o objetivo é analisar ou descrever o fenómeno.

Já para (Bell, 2014) o estudo de caso é um termo que abrange um grupo de métodos de pesquisa que têm como principal preocupação a interação entre fatores e eventos.

Para (Benbasat, Goldstein, & Mead, 1987) o estudo de caso deve ter as seguintes características:

- O fenómeno deve ser observado no seu ambiente natural.
- Dados recolhidos através de diversos métodos.
- Uma ou mais entidades são analisadas.
- A complexidade da unidade é estudada aprofundadamente.
- Pesquisa dirigida aos estágios de exploração, classificação e desenvolvimento de hipóteses do processo de construção do conhecimento.
- Não utiliza formas experimentais de controlo ou manipulação.
- O investigador não tem de especificar antecipadamente o conjunto de variáveis dependentes e independentes.
- Os resultados dependem do poder de integração do investigador.
- Podem se feitas mudanças na seleção do caso ou dos métodos de recolha de dados no decorrer da investigação.
- Responde a questões como? E porque?
- Focos em eventos contemporâneos.

3.4. Horizonte temporal

Segundo (Saunders, Lewis, & Thornhill, 2009) uma investigação científica pode-se caracterizar no que diz repito ao horizonte temporal por, *cross-sectional* onde a investigação é feita num ponto do tempo, ou longitudinal onde a investigação decorre ao longo do tempo.

Embora o estudo de caso tenha decorrido ao longo de um período de tempo a análise é focada nos resultados obtidos num determinado momento o que leva a escolher o horizonte temporal *cross-sectional*.

3.5. Recolha e análise de dados

Segundo (Bell, 2014) os métodos de recolha de informação são escolhidos de acordo com a tarefa a levar a cabo.

Segundo (Yin, 2013) a utilização de várias fontes na construção do estudo de caso, além de permitir um conjunto maior de tópicos de análise, permite corroborar os dados.

O que faz com que utilize uma técnica *multi method* que utiliza dados qualitativos e quantitativos (Saunders, Lewis, & Thornhill, 2009).

Segundo (Creswell, 2003) numa abordagem *multi methods* o investigador utiliza estratégias que envolvem a recolha de dados de forma sequencial ou em simultâneo, para melhor compreender os problemas da pesquisa, a recolha de dados envolve dados numéricos por exemplo de instrumentos de medida, como dados de texto como exemplo os recolhidos de entrevistas, de forma a ter uma base de dados final para análise com dados qualitativos e quantitativos.

Assim para a elaboração do caso de estudo foram utilizados os seguintes métodos (Yin, 2013):

- Documentação – Material escrito em forma de memorando, jornal, relatório formal.
- Arquivos gravados – Gráficos da organização, registos de pessoal, financeiros ou de serviço.
- Entrevistas – Com perguntas fechas e ou abertas.
- Observação direta – Absorvendo ou anotando detalhes, ações ou subtilezas no campo de estudo.
- Artefactos físicos – Dispositivos e outputs de ferramentas.

De forma a criar um conjunto de dados completo que permitam estudar como uma organização no seu contexto natural responde às possíveis ameaças à sua atividade.

4. Estudo de caso

O estudo de caso foi elaborado recorrendo à experiencia do investigador como membro técnico da equipa de projeto, através da análise da documentação técnica e dos procedimentos respeitantes à continuidade de negócio em vigor na organização. Foram ainda realizadas entrevistas não estruturadas informais cujo conteúdo não foi registado a pedido dos intervenientes por razões de confidencialidade.

A pedido da organização será preservado o seu nome assim como todos os detalhes confidenciais.

4.1. Caracterização da organização

A organização em estudo é a sucursal portuguesa de uma empresa multinacional europeia do ramo financeiro, especializada no crédito ao consumo à distância, tendo na sua carteira soluções de crédito clássico, *revolving*, consolidado e automóvel. Não possuindo uma rede de balcões físicos, opera essencialmente pelos canais à distância como internet e telefone.

Neste momento a empresa conta com cerca de 465 colaboradores na sua sede em lisboa divididos por sete direções e tem em carteira mais de 340 mil clientes com um volume de negócio de cerca de 115.531.592€, tendo um papel importante na economia e emprego nacional.

Neste modelo de negócio a componente de TI tem uma importância fundamental, pois todo o contacto com o cliente é feito à distância, sendo que qualquer *downtime* tem um impacto imediato no negócio e na imagem transmitida ao cliente.

A empresa está presente em Portugal desde 1996. No início da sua atividade em Portugal a organização não contava com informática própria, utilizando um sistema IBM AS400 alojado numa empresa financeira concorrente, levantando uma serie de questões de concorrência, confidencialidade e flexibilidade.

Desde cedo ficou claro para a gestão de topo que a organização tinha de ser informaticamente independente, assim foi criado um departamento de informática com desenvolvimento de sistemas próprios à medida “dentro de casa”, de modo a preencher os requisitos do negócio, as aplicações de negócio foram desenvolvidas com recurso a tecnologia *web base* facilitando o acesso às aplicações através de um simples *browser*.

Paralelamente ao desenvolvimento do novo sistema foi adotado o modelo ITIL como referencia para os processos de gestão de TI, garantindo a qualidade do serviço prestado ao negócio.

4.2. Infraestrutura inicial

De modo a alojar a infraestrutura foi criado um CPD a partir de uma sala comum com as seguintes características:

- Paredes falsas em madeira.
- Chão falso.
- Duas unidades de A/C de insuflação de ar frio através do chão falso.
- Sistema de deteção e extinção de incêndios.

Devido ao facto de não ser um CPD construído de raiz, mas sim uma adaptação numa sala comum, apresentava vários problemas entre os quais:

- O material das paredes não é resistente ao fogo.
- Mau isolamento térmico.
- O chão falso é demasiado baixo impossibilitando a correta circulação do ar frio, provocando problemas de refrigeração.

O CPD alojava um conjunto de cerca de 38 servidores físicos de suporte às aplicações de negócio e infraestrutura:

- IIS de suporte às aplicações de negócio.
- *Cluster* SQL de dois nós com as bases de dados transacionais.
- *Mail server*.
- Um *domain controller.*
- *Proxy server*.
- *Fax Server*.
- Mail *Relay*.
- *FTP Server*.

Equipamento de suporte

- Sistema de controlo de acessos.

Infraestrutura de rede

- Core *switch*.
- *Firewall*.
- 2 *Switchs* de apoio.

Rede pisos

- Um *switch* em cada fração.

Sistema de armazenamento.

- SAN com duas controladoras.
- 1 *Array* de discos.
- 2 *Switchs* de fibra.

Sistema de *backup* para tapes armazenadas no local e executado manualmente.

A imagem abaixo representa o esquema logico implementado:

- Um *switch* core ligado aos *switchs* de piso, com uma *vlan* por piso

- Duas DMZ para os serviços com comunicação ao exterior
- Uma DMZ para a infraestrutura do *website* com ligação ao exterior dedicado por dois operadores diferentes através de BGP.
- Uma ligação ao sistema *lagacy*.
- Duas ligações dedicadas a *contact center* com serviços contractados.
- Ligações através de um *link* partilhado com o acesso à internet corporativo para:
    - Gráfica responsável pelas comunicações físicas através de VPN.
    - Seguradora parceira através de VPN.
    - Serviço de informação de crédito utilizado no processo de análise por túnel SSH.
    - Serviço contabilístico remoto através de VPN
    - SMS-C das operadoras para envio de SMS.
- Todos os canais de comunicação e energia utilizavam o mesmo caminho físico de entrada no edifício.

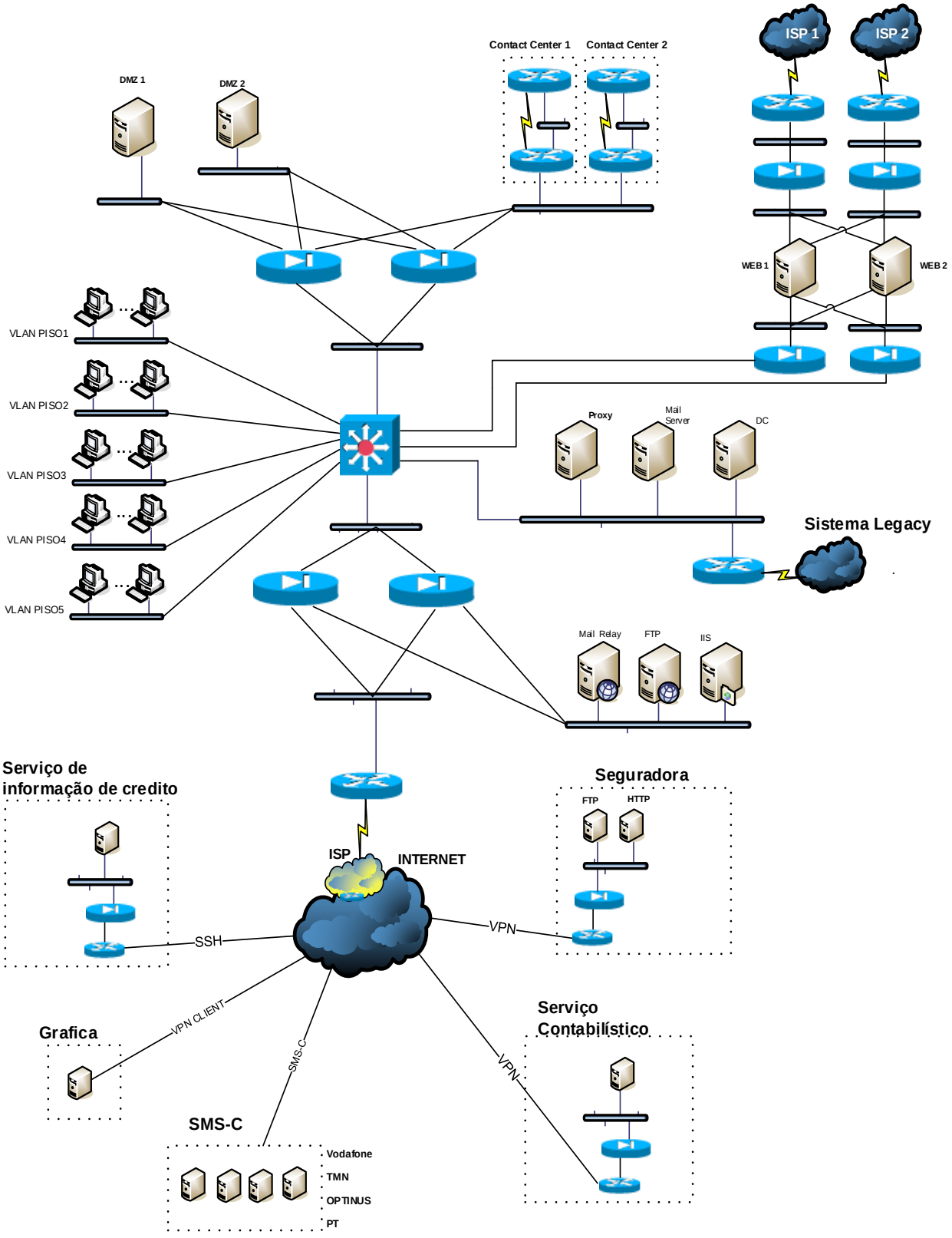


Fig. 10 - Diagrama lógico da rede da organização

Infraestrutura de voz

- Internamente a gestão das chamadas era feita por uma central telefónica digital com componente de *contact center*, ligada à rede pública através de primários de voz para chamadas para a rede fixa, e *comsat* para chamadas de rede móvel, como ilustrado na figura abaixo.

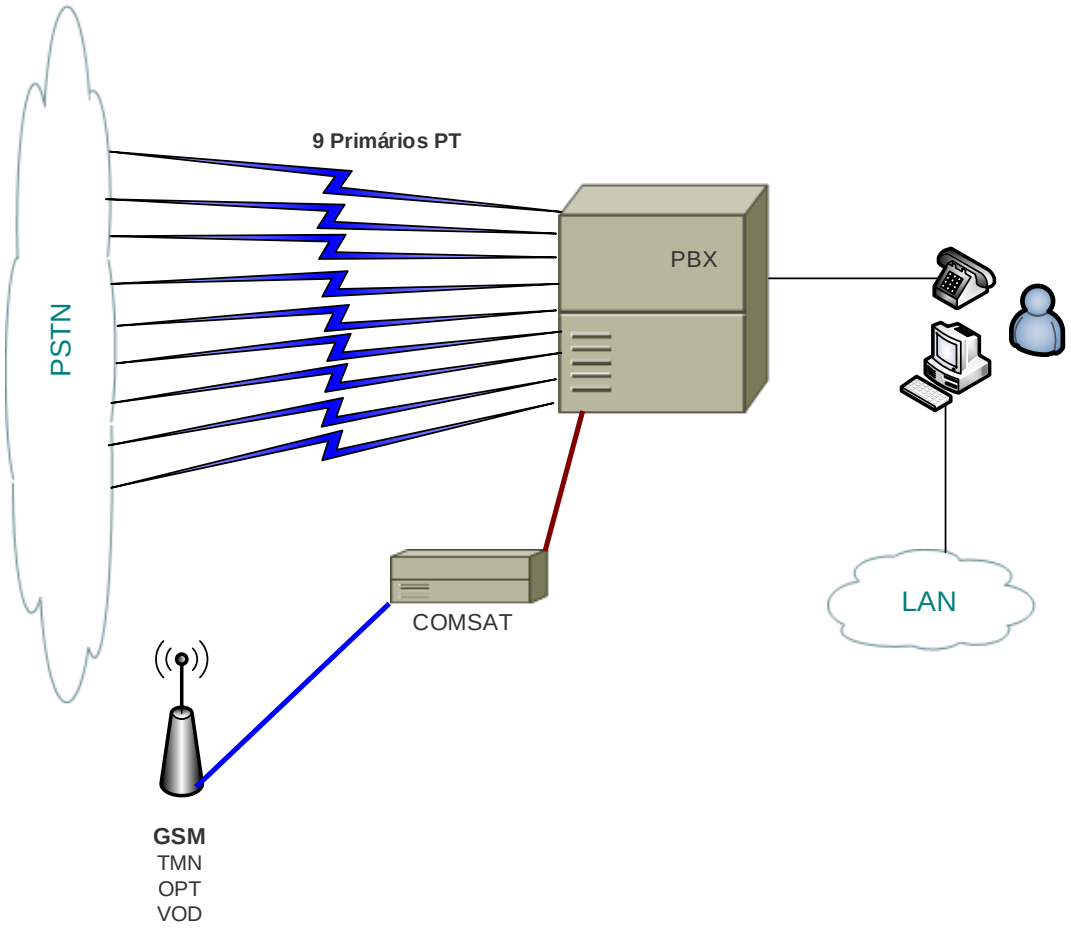


Fig. 11 - Diagrama da rede de voz da organização

4.3. Plano continuidade da atividade

Para a realização do plano de continuidade da atividade foi efetuado um estudo ao negócio e à sua infraestrutura, de forma a levantar os requisitos para uma solução, que garanta a continuidade da atividade do ponto de vista das TI e dos processos de negócio em caso de desastre.

4.3.1. Análise inicial

Para a realização do estudo inicial e para melhorar a compreensão dos processos críticos para a organização foram realizadas as seguintes tarefas:

- Compreensão das necessidades do negócio – Para melhor compreender as necessidades do negócio foram feitas entrevistas a todas as direções, de modo a compreender os processos e a sua criticidade para a cadeia de valor do negócio, assim foram mapeadas:
    - As principais responsabilidades.
    - RTO, RPO, nível de criticidade e número mínimo de postos de trabalho para cada macro processo.
    - Impactos de uma paragem para as várias áreas da direção.
    - Principais interdependências.
    - Aplicações e sistemas de suporte com respetivo RTO e RPO.
    - Momentos críticos.
    - Recursos mínimos.
- Mapeamento das aplicações com a infraestrutura que as suportam e respetivos RTO e RPO tendo em conta o apurado na fase de entrevistas.
- Com o resultado do levantamento efetuado, foi criado um BIA contendo a seguinte estrutura.
    - Enquadramento – Um breve enquadramento do negócio da organização, Missão e valores, informação financeira, governação e estrutura orgânica.
    - Um ponto por cada direção onde é registado:
        - Breve descrição da função da direção.
        - Serviços da direção.
        - Impactos e riscos de paragem.
        - Momentos críticos.
        - Principais interdependências.
        - Número de efetivos.
        - Objetivos de recuperação, recursos humanos, linhas telefónicas e *fax*, equipamento informático, fornecedores externos, aplicações necessárias e respetivos tempos de recuperação, processos manuais alternativos, registos críticos, atividades criticas apos desastre.
        - Resumo da informação condensada de todas as direções.
        - Resumo de todas as aplicações identificadas e respetivo RTO e RPO.
- Análise de risco do centro de dados - Documento de análise aos riscos do CPD existente tendo em conta:
    - Localização.
    - Espaço físico.
    - Sistemas estruturais.
    - Sistemas de proteção de incendio.
    - Sistemas mecânicos.
    - Sistemas elétricos.
    - Sistemas de monitorização.
    - Segurança física.

4.3.2. Conclusões

No final, toda a informação foi condensada num documento com toda a análise efetuada.

Após o enquadramento da organização, da informação financeira e estrutura organizacional, descreve o método e conclusões encontradas, este ponto sumariza as principais conclusões do estudo.

4.3.2.1. Análise de riscos físicos

Na análise de riscos, foram considerados três tipos de desastre como ilustrado na figura abaixo:

Fig. 12 - Tipos de incidentes disruptivos

- Riscos físicos:
  - Localização em zona de risco sísmico.
  - Localização junto a edifícios de habitação e serviço de que desconhece a utilização.
  - O edifício encontra-se no alinhamento de aproximação ao aeroporto da portela.
  - Foi detetada a presença de caixas de cartão no CPD.
  - Existem pontos de acesso ao edifício fáceis de utilizar para fins de intrusão.
  - Equipamento espalhado pela sala não acondicionado em bastidores.
  - Falta de vídeo vigilância no acesso ao CPD.
- Sistemas estruturais
  - A porta de acesso ao CPD é frágil e facilmente violável.

  - Passagem de cabos para o CPD pelo teto de chão por aberturas não seladas com material anti fogo.
  - A sala da UPS apresenta tubagem à vista o que representa risco de inundação.
  - Parte das divisórias do CPD são em vidro o que representa risco de intrusão bem como risco de em caso de incendio ou em caso de ativação do sistema de extinção do vidro partir facilitando a propagação do fogo.
  - Parte das divisórias não tem resistência ao fogo.
  - As paredes são pouco resistentes ao fogo e facilitam a condensação exagerada de água, aumentando os níveis de umidade da sala.
  - O CPD tem teto falso solto em alguns pontos podendo cair em cima de pessoas ou equipamento.
  - A sala da UPS não tem chão falso apresentado risco elevado em caso de inundação.
- Sistemas de proteção de incendio
  - A sala da UPS ao contrário do CPD não possui um sistema de deteção e extinção de incêndios.
- Sistemas mecânicos
  - Nem todos os bastidores possuem aberturas para arrefecimento.
  - Não existe sistema de renovação de ar e de extração de fumos.
  - O CPD e sala da UPS não têm um sistema de deteção de água debaixo do chão falso.
- Sistemas elétricos
  - Quadros elétricos dentro do CPD representam risco de incendio e dificultam o acesso em caso de emergência.
  - A UPS alimenta todo o edifico incluindo o CPD existindo o risco de se ligar um equipamento que cause ruido na rede elétrica numa tomada socorrida.
  - A UPS apresenta uma carga de 92% (No máximo deveria estar a 75% 80%)
  - Não existe gerador *diesel*.
- Monitorização
  - Não existe um sistema central que reúna os alarmes dos detentores de incendio, aguas, A/C.
  - A UPS não esta ligada a um sistema de alarme o que provoca que em caso de alarme ninguém seja avisado ficando o alarme na UPS.
- Segurança Física
  - Não existe sistema de vídeo vigilância no CPD.

4.3.2.2. Análise de impacto no negócio

Devido a questões de confidencialidade os detalhes da análise de impacto no negócio serão omissos.

Nesta fase foram identificados os seguintes pontos:

- Áreas de negócio e respetivos macro processos críticos para o negócio.
- Impacto de falhas nas áreas ou macro processos de negócio críticos.
- Tempo máximo de paragem máximo admissível (RTO).
- Tempo máximo de perda de dados admissível (RPO).
- Níveis de criticidade.

Nível de Criticidade	Critério de seleção dos Processos por Criticidade	Requisitos de Recuperação dos Processos no Plano de Continuidade
NIVEL 1 **(Funções críticas)**	Tempo máximo de indisponibilidade, menor ou igual que 1 Dia. Dimensão do Impacto da Contingência: ALTO Impacto de uma perda de dados ALTO e nível de atualização indeterminado.	**Recuperação da função operacional até 1 Dia.** **Perda de dados aceitável: último *Backup* do guardado fora do *site*. (dia anterior)** **Integridade dos dados garantida**
NIVEL 2	Tempo máximo de indisponibilidade, de 1 dia a 3 Dias. Dimensão do Impacto da Contingência: ALTO-MÉDIO Impacto de uma perda de dados ALTO e nível de atualização indeterminado.	**Recuperação da função operacional entre 2 a 3 Dias.** **Perda de dados aceitável: último *Backup* do guardado fora do *site*. (dia anterior)** **Integridade dos dados garantida.**
NIVEL 3	Tempo máximo de indisponibilidade, 3 A 7 Dias. Dimensão do Impacto da Contingência: MÉDIO-BAIXO	**Recuperação da função operacional entre 4 a 7 Dias.** **Perda de dados aceitável: último *Backup* guardado fora do *site*. (dia anterior)**
NIVEL 4 **(Restantes Funções e Processos)**	**Tempo máximo de indisponibilidade > 7 Dias.** **Dimensão do Impacto da Contingência: BAIXO**	**A recuperação poderia ser feita em mais de 7 dias o poderia não ser recuperado em situação de contingência**

Tabela 7 - Níveis de criticidade

Como resultado foram apurados três serviços com nível de criticidade 1, quatro serviços com nível de criticidade 2, um serviço com nível de criticidade 3 e oito serviços com um

nível de criticidade 4, foram também registados como necessidade de negócio um RTO mínimo de um dia e máximo de 30 dias e um RPO mínimo de 0 dias e máximo de 8 dias.

4.3.2.3. Estratégias de recuperação

Face ao apurado nos pontos anteriores foram equacionados vários cenários de recuperação com base em cenários conceptuais, tendo em conta os *tiers* de recuperação definidos pelo grupo SHARE em 1992 (SHARE Inc, 2007).

Após a divisão das aplicações \ serviços pelos vários *tiers*, conclui-se que existe 28 aplicações *tier* 2-3 e 2 aplicações *tier* 1

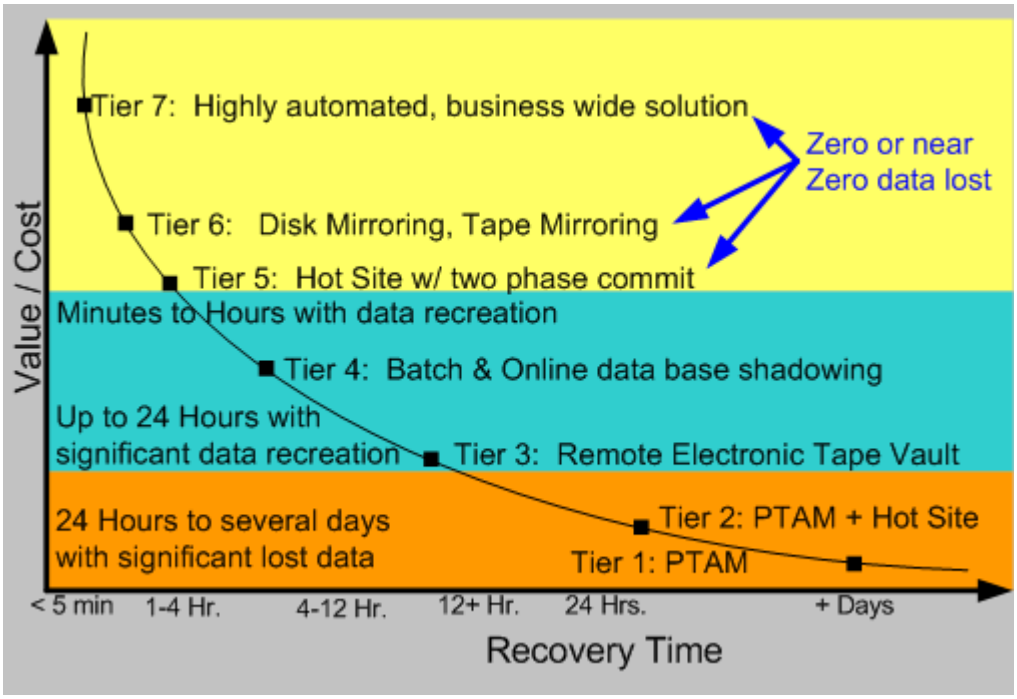


Fig. 13 - *Tiers* de recuperação

Fonte (SHARE Inc, 2007)

4.3.3. Cenários identificados

Fase à analise efetuada e aos requisitos de negócio foram equacionados três cenários possíveis para garantir a continuidade do negócio em caso de desastre.

Na identificação dos cenários foram identificados os recursos críticos de servidores, SAN, LAN e WAN para a recuperação do ambiente de produção da organização.

4.3.3.1. Estratégias de recuperação

Cold Site

Cenário baseado na transferência de *tapes* para um *site* secundário sem infraestrutura instalada.

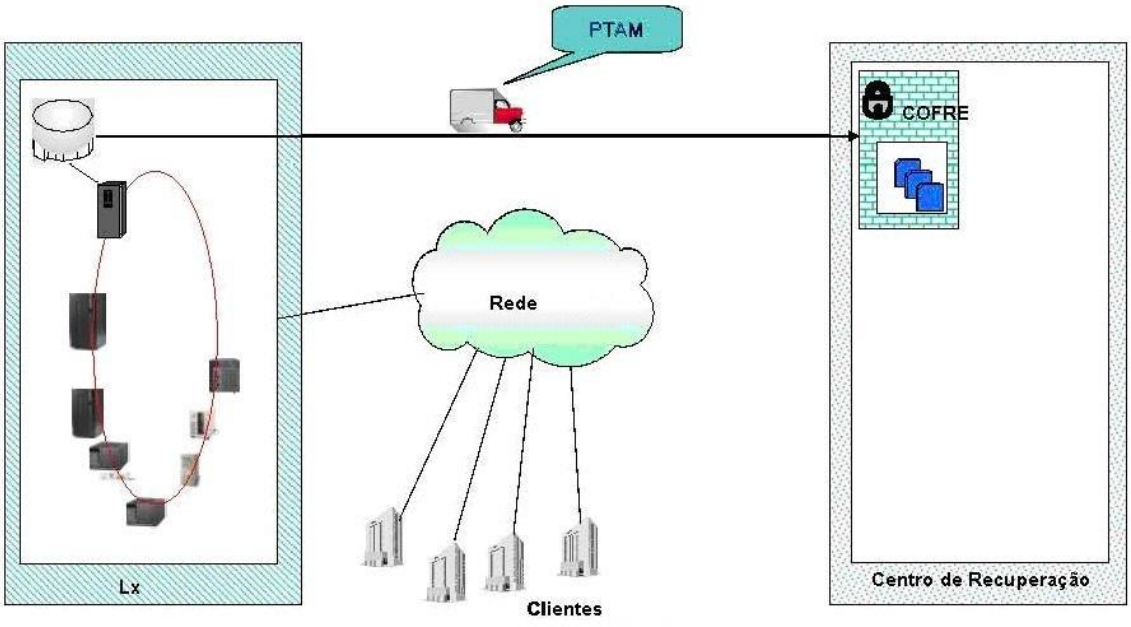


Fig. 14 - Cenário de recuperação *Cold Site*

Recursos necessários

- Local alternativo para recuperação sendo ai armazenadas todas as cópias de dados críticos.
- Equipamento crítico e linhas de comunicação não estão necessariamente disponíveis no local alternativo.

Processo de *backup*

- *Backup* de todos os dados críticos em duplicado, sendo mantida uma cópia no CPD para recuperação local e a segunda cópia é enviada para o centro de recuperação.

Processo de recuperação

- O processo de recuperação poderá ser complexo e de difícil gestão. É necessário envolver a equipa aplicacional para determinar os procedimentos de recuperação das aplicações, o tempo de recuperação poderá ser elevado e difícil de prever, este cenário preenche os requisitos de aplicações *tier* 1.

Warm Site

Cenário baseado na transferência de tapes para um *site* remoto que contem infraestrutura que pode ser iniciada a pedido.

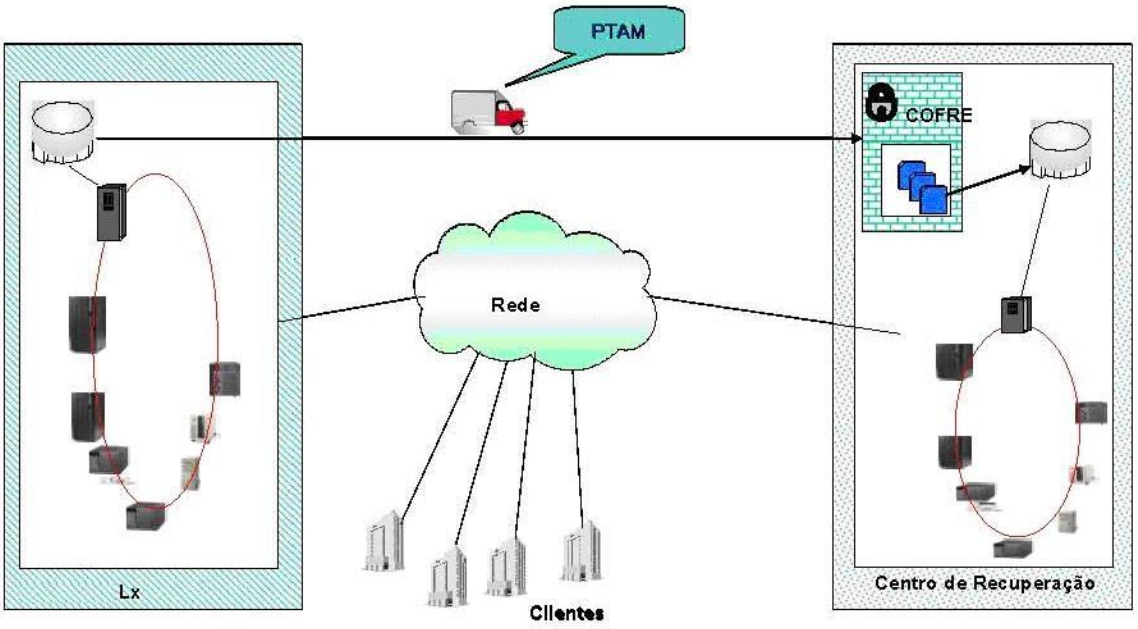


Fig. 15 - Cenário de recuperação *Warm* Site

Recursos necessários

- Local alternativo para recuperação sendo ai armazenadas todas as cópias de dados críticos.
- Equipamento crítico para recuperação do sistema de informação, sendo normalmente partilhado e disponibilizado apos o desastre.
- Linhas de comunicação.

Processo de *backup*

- *Backup* de todos os dados críticos feito em duplicado, sendo mantida uma cópia no CPD para recuperação local e a segunda cópia é enviada para o centro de recuperação.

Processo de recuperação

- Em caso de desastre todos os recursos críticos são imediatamente disponibilizados.
- O processo de recuperação de dados é semelhante ao executado localmente em normal operação pelas equipas de suporte.

- O processo de recuperação poderá ser complexo e de gestão difícil. Deverá ser necessário o envolvimento do pessoal das aplicações para determinar e aplicar os procedimentos corretos de recuperação. No entanto, o facto de os equipamentos estarem disponíveis permite reduzir bastante o tempo de recuperação.

Hot Site

Cenário em que os *backups* são transferidos ou executados em tempo real para um site remoto que contem toda a infraestrutura operacional.

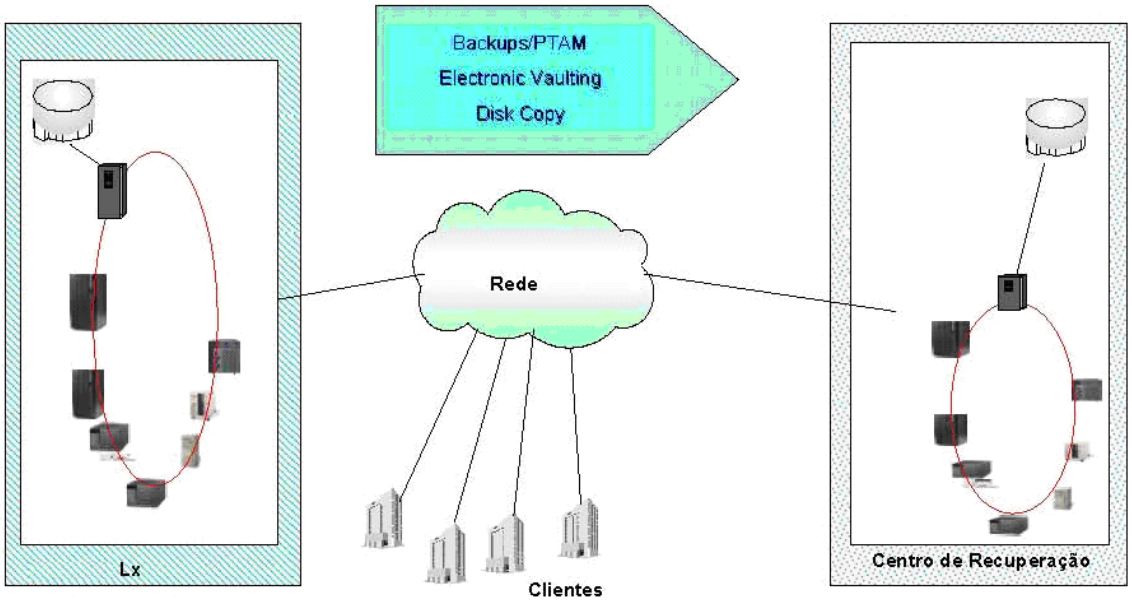


Fig. 16 - Cenário de recuperação *Hot* Site

Recursos necessários

- Um local alternativo para recuperação sendo ai guardadas todas as cópias dos dados críticos, identificado como centro de recuperação em caso de desastre.
- Equipamento crítico para recuperação do Sistema de informação, sendo normalmente dedicado e devendo estar pronto a entrar em atividade.
- Linhas de comunicação para continuidade de negócio e para transferência de dados entre os dois centros.
- *Tape drives* e *cartridges* adicionais, conforme o caso.

Processo de *backup*

- Estão disponíveis diversas tecnologias de *backup*.
- No caso de se usarem processos como *Disk Copy*, Alta Disponibilidade, etc., poderá ser possível fazer o *backup* da informação existente no Centro de Recuperação, evitando assim a realização de *backups* duplicados no Centro de Produção e o respetivo transporte.

Processo de recuperação

- Em caso de desastre, todos os recursos críticos deverão estar disponíveis para utilização.
- O processo de recuperação dependerá do cenário utilizado.
- No caso de *Disk Copy* os sistemas são inicializados como se seria feito no Centro de Produção em caso de falta de eletricidade (havendo que recuperar somente os dados em falta).
- No caso de *mirroring* seria necessário um tratamento idêntico com a vantagem de não ser preciso recuperar dados.
- Nos casos de alta disponibilidade poderia ter os sistemas em atividade quase automaticamente.

4.3.4. Documentação do plano continuidade da atividade

Após a análise inicial foram criados e mantidos atualizados os seguintes documentos de suporte à continuidade da atividade:

- Modelo de gestão do plano de continuidade da atividade – Este documento descreve o método de gestão dos documentos que integram o plano de continuidade da atividade.
- Plano de gestão de crise – descreve toda a estratégia de recuperação, situações de ativação, responsabilidades e ações macro a desenvolver.
- Plano de recuperação de negócio – Descreve com detalhe os procedimentos a seguir para a gestão de crise pelos *managers* e respetivas equipas de recuperação com vista à célere reativação da atividade.
- Plano de recuperação dos sistemas de informação – Descreve com detalhe os procedimentos a seguir pelas equipas técnicas para a recuperação dos sistemas core.
- Plano de testes – Descreve os testes a serem efetuados a fim de aferir a eficácia dos planos de recuperação e identificar lacunas que devam ser endereçadas.
- BIA – Documento de *Business Impact Analysis* com informação pormenorizada dos impactos e necessidades de recuperação para cada área \ processo critica.

Estes documentos são revistos anualmente.

Para acompanhar e garantir a continuidade da atividade foi criado um comité de crise responsável pela análise, aprovação e formalização dos planos individuais das diversas áreas.

O comité de crise abrange toda a direção da organização e o responsável da continuidade da atividade.

Anualmente ou sempre que se justifique é feito um ponto de situação junto da direção geral sobre a evolução do plano e resultado dos testes.

4.4. Primeira fase de implementação

Face aos cenários de recuperação propostos e à necessidade de aumentar a resiliência e a disponibilidade, a organização decidiu avançar para uma solução *hot site*, assim foi construído um novo CPD de raiz no edifico contiguo ao do CPD existente com as seguintes características:

- Proteção contra incendio ate 1090cº, F90 segundo norma EN1363
- Proteção contra jato de água IP X6 segundo a norma EN60529
- Proteção contra poeira IP5X segundo a norma EN60529
- Proteção contra gases inflamáveis corrosivos DIN 18095
- Proteção contra intrusão classe 3 segundo a norma EN 1627/1630
- Proteção contra choque de 200kg de uma altura de 1.5 m apos tempo de flamabilidade de 30 min.
- Proteção contra entrada e saída de radiações de alta frequência comprovada pela universidade politécnica de Aachen, Alemanha.

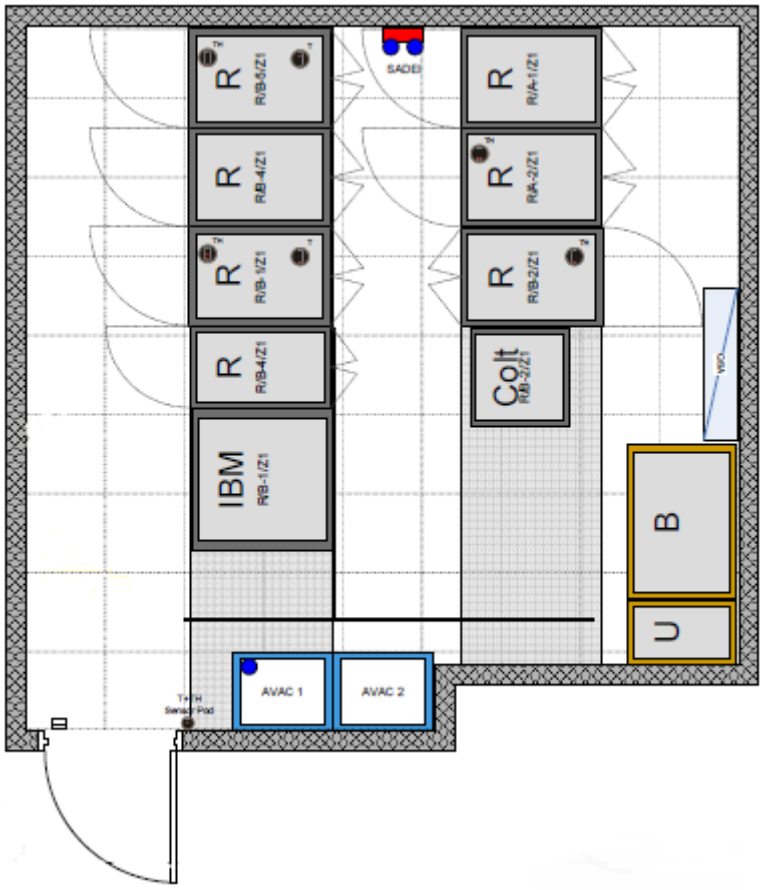


Fig. 17 - CPD *site* principal

Com a construção do novo CPD foi adotada uma filosofia de alta disponibilidade em que as comunicações passaram a entrar por dois pontos distintos do edifício e com caminhos diferentes dentro da rede do operador, assim como a instalação de um novo ponto de entrada de energia para o novo CPD proveniente de um ramal diferente do fornecedor, assim as ligações ao exterior ficaram redundantes, ficando cada um dos CPD com pontos de comunicação com o exterior diferenciados.

No novo CPD foi adicionada uma nova UPS com capacidade para 1.5h de autonomia e foi feito um *upgrade* às baterias da UPS existente aumentado a autonomia para 4h.

Todos os equipamentos instalados possuem fontes de alimentação redundantes ficando cada fonte ligada a uma UPS, garantindo redundância de alimentação energética.

De forma a garantir alta disponibilidade de servidores foi adotada a virtualização, passando de uma abordagem de servidores físicos para uma abordagem de servidores virtuais distribuídos por dois chassis alojados cada um no seu CPD, que utilizando a tecnologia *Vmotion* podem correr em qualquer *host* sem quebra de serviço, sendo que a infraestrutura foi dimensionada para que a totalidade dos servidores virtuais consiga correr num único chassis. De fora da virtualização ficaram os servidores das bases de dados, tendo sido criados três *cluster* SQL com dois nós de modo a permitir a redundância.

De forma a suportar os dados, foram instaladas duas SAN com baias de discos, apoiados por dois *switchs* de fibra distribuídos pelos dois CPD, de modo a garantir disponibilidade dos dados em caso de falha das SAN's principais, foram instaladas duas SANs no CPD antigo e configuradas em *mirror* das SANs principais, sendo necessário reconfigurar as zonas de acesso aos dados em caso de indisponibilidade das SANs principais permitindo assim o acesso aos dados.

De forma a garantir a redundância de rede foi instalado um *switch* core no novo CPD, ligado por fibra ao *switch* core do CPD antigo. Nos *switchs* de piso foram configurados trunks em fibra para cada um dos *switchs* core com *spanning tree* ativo.

Assim a infraestrutura ficou estruturada da seguinte forma:

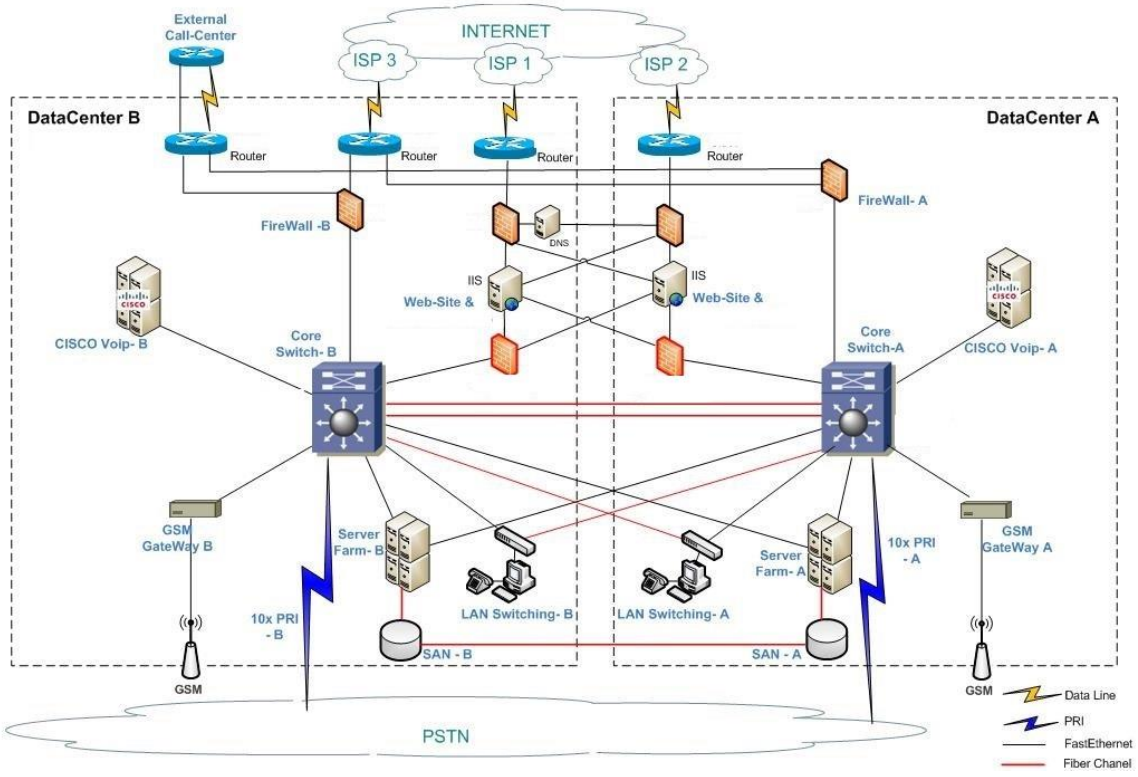


Fig. 18 - Diagrama logico da rede primeira fase de implementação

A infraestrutura de voz foi renovada passando para um sistema *VoIP* com componentes redundantes, foram também instalados dois conjuntos de primários, que asseguram as comunicações de voz com a rede fixa e dois *comsat* divididos pelos dois CPD que asseguram as comunicações com a rede móvel.

A imagem abaixo representa a estrutura de voz distribuída pelos dois CPD.

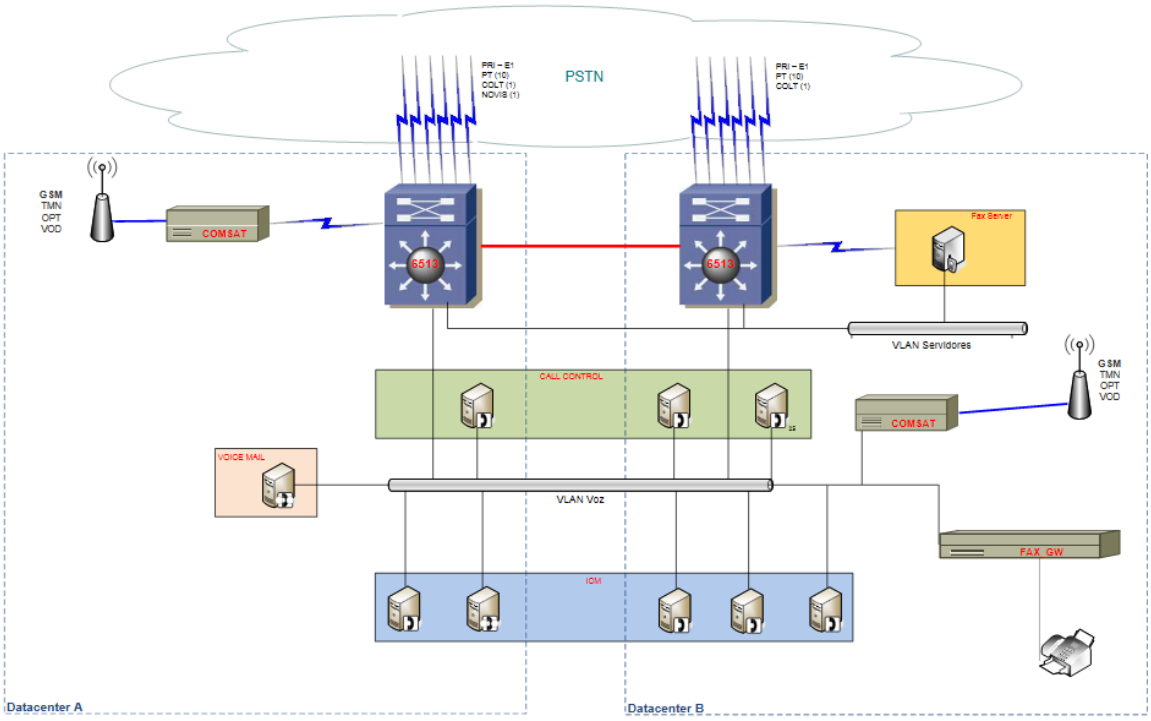


Fig. 19 - Diagrama da rede voz primeira fase de implementação

De modo a assegurar a disponibilidade da informação em caso desastre ou eliminação acidental, foi instalado um robot de *backups* com duas *pools* de *tapes*, uma residente no robot e outra externa que corresponde à cópia da primeira *pool*. Para assegurar a disponibilidade dos dados no caso da indisponibilidade do *site* principal foi contractado um serviço de *tape vaulting* em que a segunda pool era enviada para um cofre a 300km de distância com uma periocidade semanal.

4.5. Segunda fase de implementação

Apesar da solução implementada ser de alta disponibilidade não assegura uma proteção contra desastres de nível 3, assim a solução encontrada passou pela criação de um espaço na região de Oeiras com 120 postos de trabalho e um novo CPD de forma a albergar a infraestrutura redundante que se encontrava no CPD mais antigo passando este a ser considerado uma sala técnica, ao executar esta fase foram efetuadas algumas alterações à infraestrutura.

4.5.1. CPD redundante

De forma a assegurar proteção contra desastres do tipo 3 foi construído um novo CPD com as seguintes características:

- Proteção contra incendio ate 1090cº, F90 segundo norma EN1363
- Proteção contra jato de água IP X6 segundo a norma EN60529

- Proteção contra poeira IP5X segundo a norma EN60529
- Proteção contra gases inflamáveis corrosivos DIN 18095
- Proteção contra intrusão classe 3 segundo a norma EN 1627/1630
- Proteção contra choque de 200kg de uma altura de 1.5 m apos tempo de flamabilidade de 30 min.
- Proteção contra entrada e saída de radiações de alta frequência comprovada pela universidade politécnica de Aachen, Alemanha.

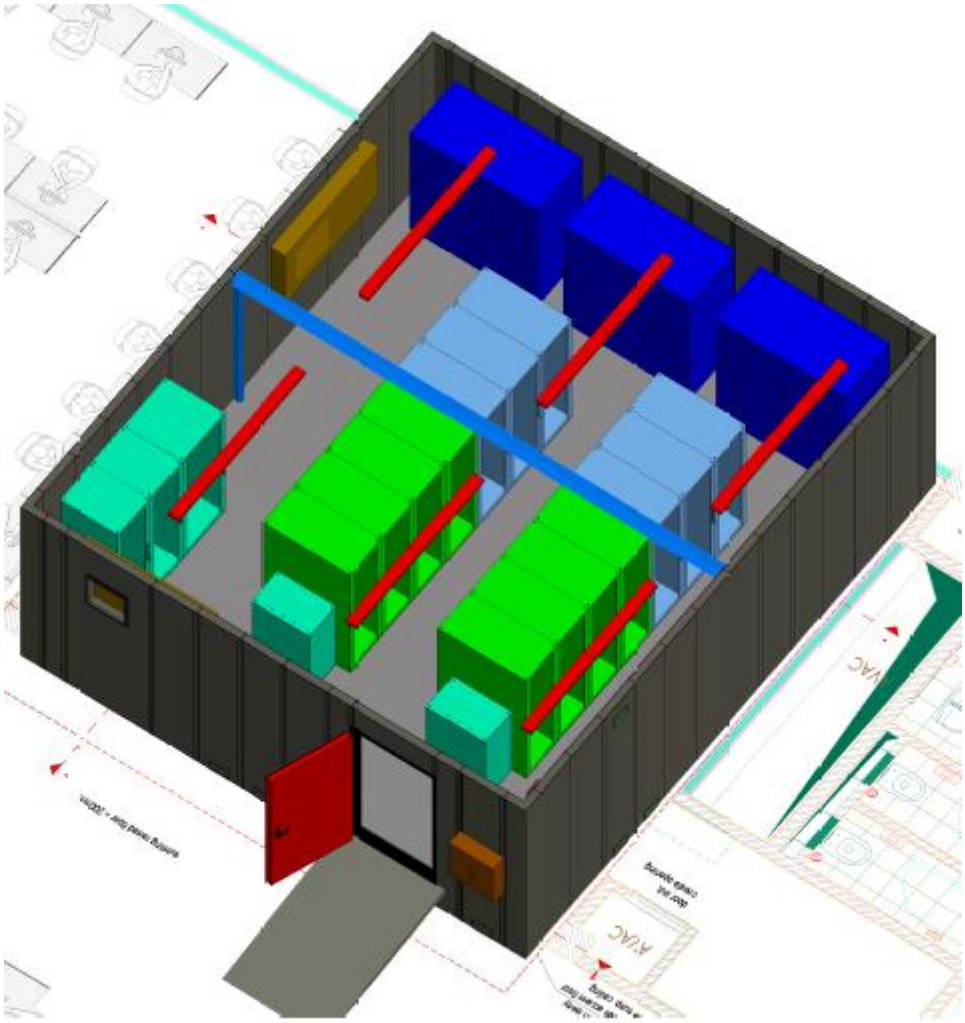


Fig. 20 - Imagem 3D do CPD redundante

Foi instalado ainda no novo CPD um sistema de deteção e extinção de incendio com sensores de fumo e temperatura instalados ao nível do teto e debaixo do chão falso assim como uma nova UPS e baterias com capacidade para 2 horas.

O CPD antigo passou a sala técnica com um *switch* core para redundância e *switch* de distribuição de rede para o piso.

4.5.2. Infraestrutura de rede

A topologia de rede passou a utilizar tecnologia VSS para agregar os chassis do *site* principal e *portchannels* para interligar equipamentos de rede, com estas tecnologias conseguiu-se aumentar os níveis de estabilidade, de redundância e diminuir a dependência de STP.

Infraestrutura de rede do *site* principal

Core switch

- Passam a utilizar dois módulos de supervisão em cada *switch* core.
- Os *switchs* core do *site* principal são agregados em VSS garantindo performance e redundância.

Switch de acesso

- Passam a utilizar *portchannels* com um membro em cada chassis, tirando partido da tecnologia VSS aumentando a largura de banda de 1 Gbps para 2 Gbps e ficam menos dependentes da componente de STP

Infraestrutura de rede do *site* secundário

Core switch

- Um core *switch* com dois módulos de supervisão.

Switch acesso

- À semelhança do *site* principal utilizam *portchannel* para a ligação ao *switch* core.

Os dois *sites* estão ligados em *portchannel* obtendo assim redundância e maior largura de banda que pode chegar a 20Gbps com os dois *links*, e maior estabilidade devido a não utilização de STP.

Alterações à configuração global

Layer 2

- Tecnologia VTPv3 que permite a propagação de *vlans* no *extended-range* e propagação da configuração 802.1s.
    - Ambos os *cores* estão em modo *server*.
    - Todos os equipamentos estão em modo cliente.
- Foi aplicada a tecnologia STP 802.1s para resolver o problema de instâncias de STP, evoluindo assim para a versão mais recente da tecnologia.

- A *root bridge* das instâncias de 802.1s tem como sequencia, primário *core site* principal, secundário *site* secundário.

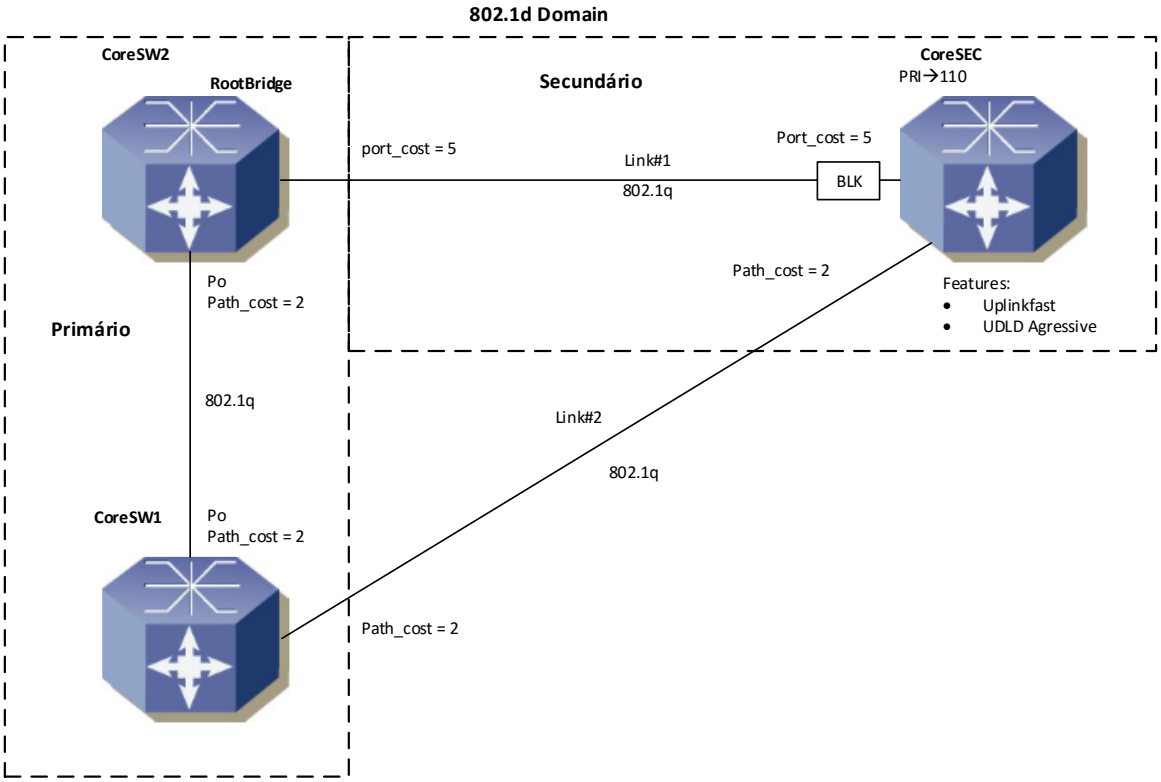


Fig. 21 - Domínio 802.1

Layer 3

- Utilização de HSRP v2 em que o primário é o *site* primário e secundário o *site* secundário.

Firewall

- De modo a manter a redundância foram instaladas *firewall* nos dois *sites* funcionando em modo *ativo*/*standby*, e utilizando instância virtuais.

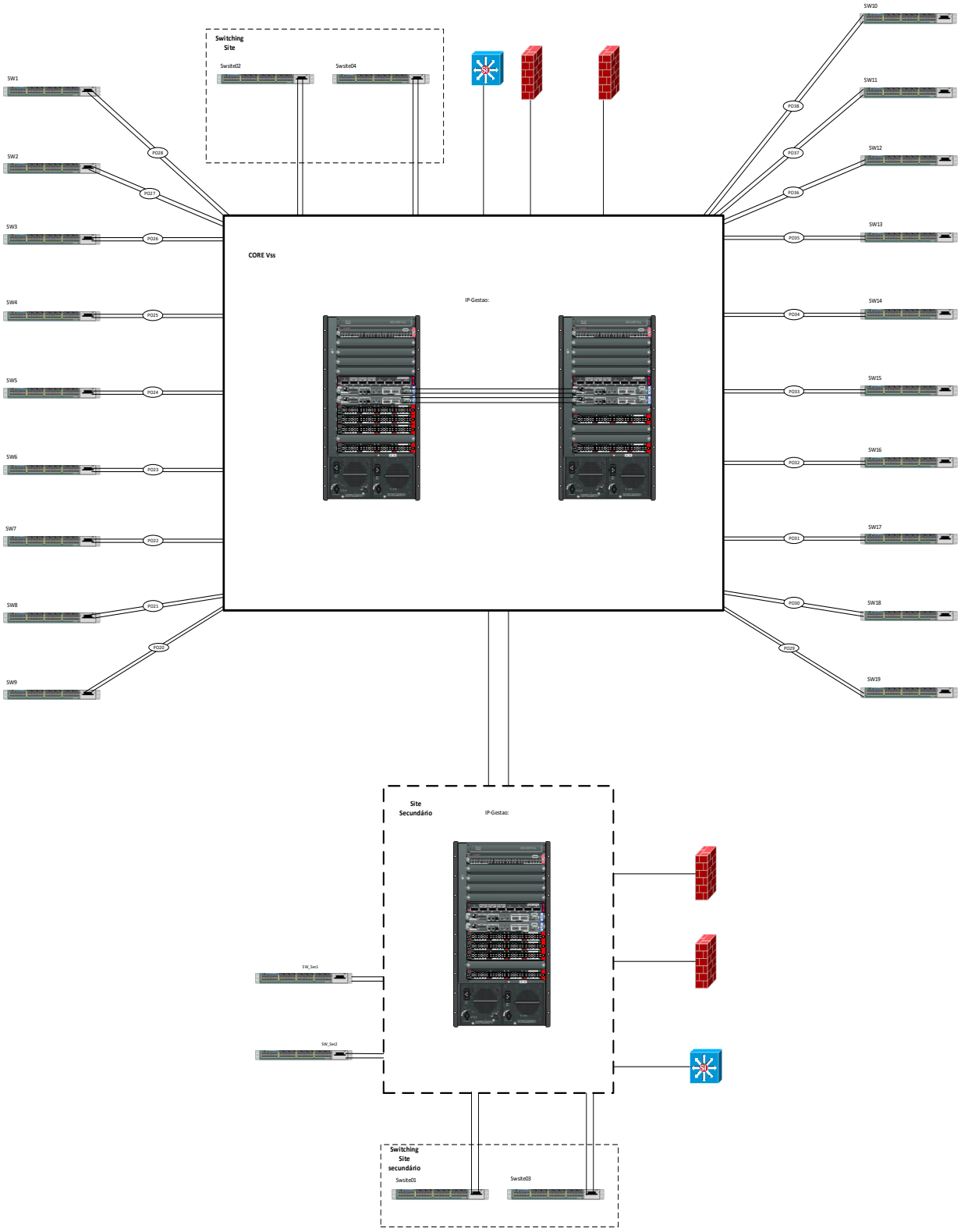


Fig. 22 - Diagrama da rede segunda fase

4.5.3. Infraestrutura de servidores

Para a infraestrutura de servidores, foram adquiridos três novos chassis, dois *fabric-interconnect* e dois MDS para cada CPD, assim a solução foi dividida em dois *fabrics* por cada *site*, os *fabric-interconnect* estão configurados em modo *end-host* não participando na eleição da *root bridge* do domínio de STP, o mecanismo de *mac-learning* esta desativado e é eleito um *uplink* para processar todo o trafego de *multicast* e *broadcast*.

Cada *fabric-interconnect* tem um *uplink* para cada nó do sistema VSS e esses *uplinks* estão agregados num *portchannel*.

Em termos topológicos cada *fabric-interconnect* possui um *port-channel* para o *Core* conferindo os mecanismos de redundância necessários. A conectividade com cada chassis efetua-se via quatro canais de 10Gbps por IOM, adicionalmente esses quatro canais encontram-se agregados via o protocolo LACP, na prática a conectividade entre o chassis e os *fabric-interconnect* é efetuada via FCoE.

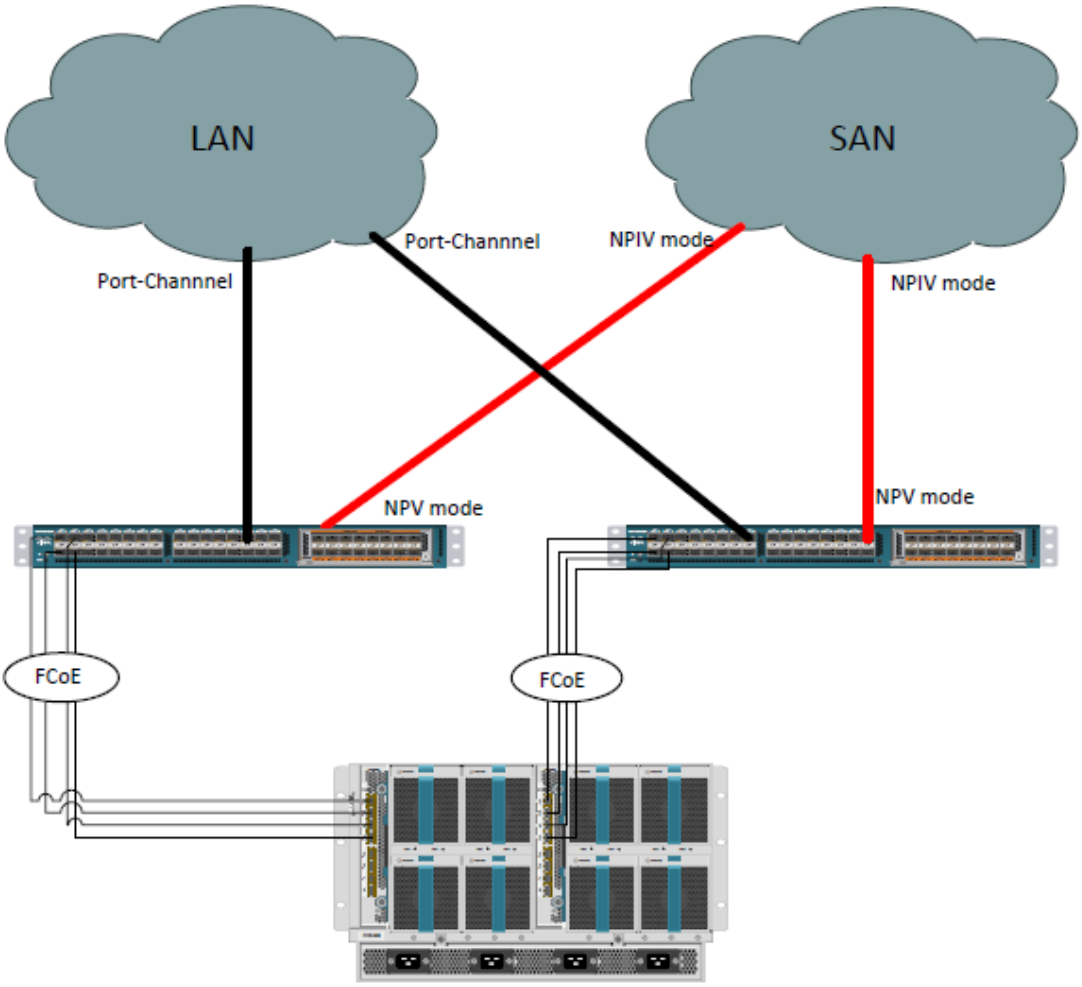


Fig. 23 - **Diagrama conectividade fabric-interconnect**

4.5.4. Infraestrutura SAN

A SAN foi completamente renovada passando a utilizar duas SANs e dois tipos de *storage* com tecnologias distintas.

Duas *storage* uma para cada *site* com as seguintes funcionalidades:

- Disposição dos dados por camadas tendo em conta a performance e histórico de acesso aos dados, três camadas com performance diferentes em que:
  - *Fast cache* de 400Gb em SSD
  - *Tier 1* - SSD servindo 2 % dos dados.
  - *Tier* 2 – SAS servindo 32 % dos dados.
  - *Tier* 3 - NL SAS servindo 66% dos dados.
- Sistema de recuperação dos dados através de componente especifica de *recovery point* que permite a recuperação local ou remota através da replicação dos dados para o *site* secundário.

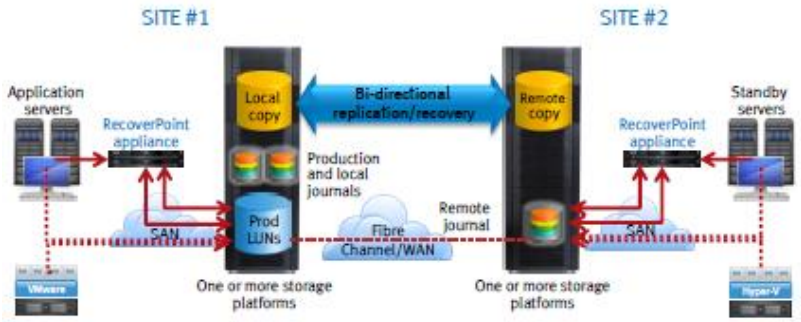


Fig. 24 **- Diagrama SAN A**

Além das funcionalidades descritas a segunda SAN utiliza um sistema em *cluster* em que garante a escrita nos dois *sites* ao mesmo tempo através de volumes distribuídos

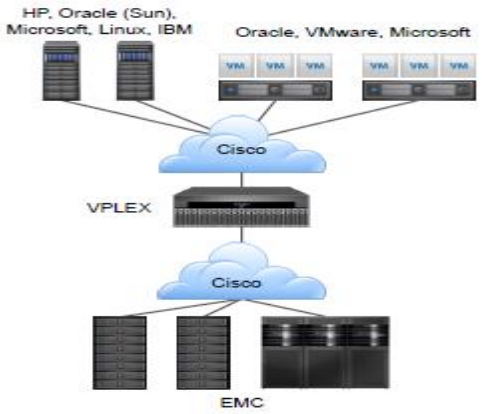


Fig. 25 - Diagrama SAN B

Em baixo o diagrama de SAN com a respetiva replicação de dados

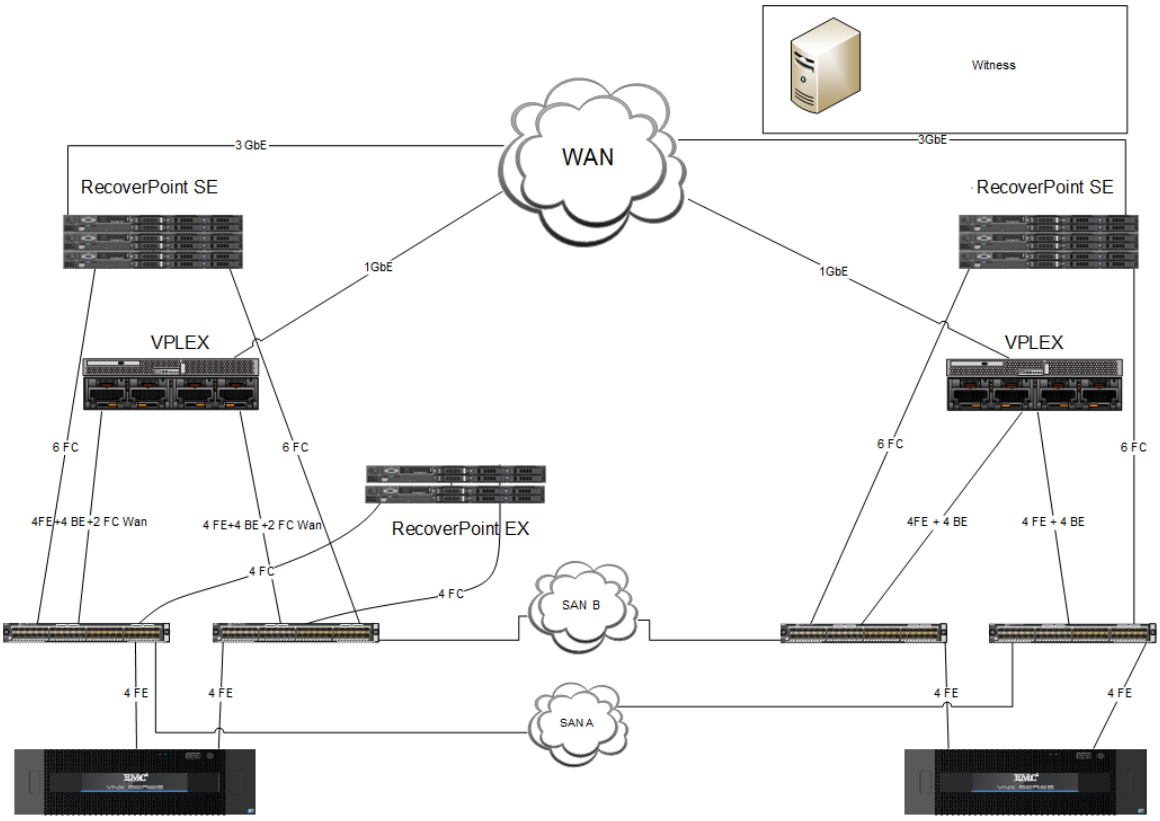


Fig. 26 - Diagrama infraestrutura SAN

4.5.5. Infraestrutura de *backup*

Além do sistema de replicação da SAN, que replica os dados quase em tempo real, garantindo um RPO de minutos, foi instalada uma nova solução de *backup* para disco, esta nova tecnologia permite encurtar de forma drástica os tempos de *backup* diários.

A infraestrutura de *backups* está dividida pelos dois *sites*, o *site* sede e o de recuperação, sendo que o *site* sede é o *site* primário funcionando o *site* secundário como infraestrutura redundante, podendo assumir o papel de primário em caso de necessidade.

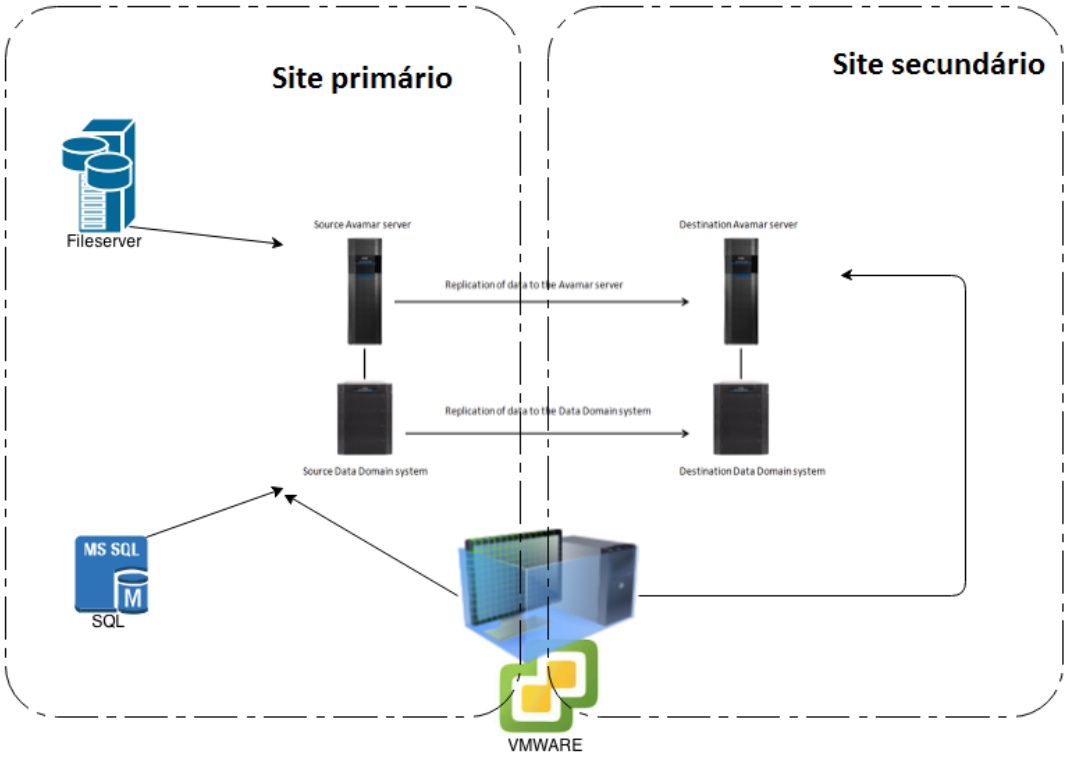


Fig. 27 - Infraestrutura de *backups*

São efetuados *backups* diários de toda a infraestrutura incluindo todas as máquinas virtuais, estes *backups* diários ficam armazenados no sistema de *backup* do *site* principal com uma retenção de 30 dias, paralelamente os *backups* são copiados para o sistema de backup do *site* secundário com retenções diferenciadas:

- Replicação *backup* diário – retenção 1 mês.
- Replicação *backup* semanal – retenção 1 mês.
- Replicação *backup* mensal – retenção 1 ano.
- Replicação *backup* anual – retenção 1 ano.

4.6. Testes

De forma a assegurar a eficácia do plano de continuidade de negócio foi criado um plano de testes aprovado pelo comité de crise e um plano de execução de testes com o detalhe e registo dos resultados.

4.6.1. Plano de teste

O plano de teste pretende assegurar o seguinte:

- A simulação de condições de uma situação de desastre real.

- A verificação que os dados e documentação para a recuperação guardados *off-site* são adequados.
- A capacidade dos membros das equipas de recuperação que participam nos testes de executarem as respetivas tarefas e responsabilidades.
- A capacidade de recuperar as funcionalidades pretendidas.
- O estabelecimento de requisitos válidos para a Recuperação em caso de desastre.

O documento compreende três tipos de teste:

- Percurso estruturado em papel – Simulação em papel de uma ocorrência disruptiva.
- Teste não anunciado – Teste técnico de surpresa que requer a recuperação simulada das operações no CPD de recuperação.
- Teste anunciado – Teste agendado que envolve a recuperação da produção no CPD de recuperação.
- Exercício tático – Simulação de recuperação conduzido num ambiente paralelo.

Os testes devem ser efetuados segundo a seguinte ordem de forma a minimizar o impacto na atividade normal da organização:

- Executar um percurso estruturado em papel logo que o desenvolvimento do plano de continuidade esteja completo.
- Executar um exercício tático para verificar se todos os requisitos estão definidos e se todos os membros das equipas de recuperação compreendem as suas responsabilidades.
- Executar um teste de recuperação anunciado que requeira a ativação simulada de todo o sistema operativo e produtos e de todas as aplicações críticas. Este é um teste para os requisitos básicos e não envolve utilizadores neste ponto. A comunicação de dados não é habitualmente testada no primeiro teste.
- Executar um teste de recuperação anunciado que requeira a ativação de todo o sistema operativo e produtos e de todas as aplicações críticas. Deve ser envolvido pelo menos um utilizador por cada aplicação crítica no CPD de recuperação. Verificar se a comunicação de dados está disponível e pode ser ativada.
- Executar um teste de recuperação anunciado que requeira a ativação de todo o sistema operativo e produtos e de todas as aplicações que devem ser recuperadas. Deve ser envolvido pelo menos um utilizador por cada aplicação crítica no centro de recuperação. Alguma comunicação de dados selecionada deverá ser testada/ligada para verificação
- Executar um teste de recuperação não anunciado que requeira a execução do plano de continuidade e a ativação de todas as comunicações. O teste deve obrigar ao envolvimento de utilizadores para verificação de que a recuperação está completa, e deverão ser executadas operações paralelas com o CPD.

Qualquer plano de teste deve ser organizado e planeado previamente, durante o teste é importante o registo de problemas num log de problemas detalhando os problemas encontrados.

Cenários de teste abrangidos pelo plano de teste da organização:

- Teste à capacidade de tolerância a falhas de energia elétrica (autonomia e plano de ação face a ausência de autonomia).
- Teste à capacidade de recuperação face à indisponibilidade de um sistema CORE, perda de dados ou indisponibilidade de um dos CPD).
- Teste à capacidade de recuperação face à indisponibilidade de uma ou várias áreas de trabalho
- Teste à capacidade de recuperação face à indisponibilidade das comunicações voz e dados.
- Teste à capacidade de recuperação face à indisponibilidade de um fornecedor crítico
- Teste à capacidade de recuperação face à indisponibilidade de recursos humanos.
- Teste à capacidade de recuperação face à indisponibilidade dos dois CPD ou dos três edifícios.

O plano de teste deve incluir:

- Parâmetros do teste
    - Participantes envolvidos.
    - Plano de notificações.
    - *Software* e sistemas a testar.
- Objetivos do teste
    - Listar objetivos primários do teste e resultados esperados.
    - Listar objetivos secundários do teste e resultados esperados.
- Lista de tarefas
    - Selecionar e documentar as tarefas a serem executadas.
    - Estabelecer tempos de início e conclusão por tarefa.
- Medições do teste
    - Registar hora de início e fim das tarefas.
    - Validar dados recuperados.
    - Documentar os problemas encontrados.
    - Registar os desvios do plano de teste.
- Revisão
    - Os parâmetros estavam corretos?
    - Os objetivos foram atingidos?
    - Os critérios de medição estavam corretos?
    - Áreas com problemas, pontos positivos e desvios do plano.

- Recomendações para melhorias.

4.6.2. Plano de execução de testes

O plano de execução de testes tem 13 testes que se dividem em 169 controlos.

Os testes abrangem todos os componentes críticos da infraestrutura:

- Teste à capacidade de tolerância a falhas de Energia Elétrica.
- Teste à capacidade de recuperação face à indisponibilidade de um sistema CORE.
- Teste à capacidade de recuperação face à indisponibilidade de um dos CPD.
- Teste à capacidade de recuperação face à indisponibilidade ou corrupção de dados.
- Teste à capacidade de recuperação face à indisponibilidade de uma ou várias áreas de trabalho.
- Teste à capacidade de recuperação face à indisponibilidade das comunicações voz.
- Teste à capacidade de recuperação face à indisponibilidade das comunicações dados.
- Teste à capacidade de recuperação face à indisponibilidade de um fornecedor crítico.
- Teste à capacidade de recuperação face à indisponibilidade de recursos Humanos.
- Teste à capacidade de recuperação face à indisponibilidade dos três edifícios sede.
- Teste ao Plano de Comunicação.
- Teste à Evacuação.
- Teste à ativação do Plano de Gestão de Crise.

O último teste completo de ativação do CPD de recuperação ocorreu em 2013 e teve uma taxa de sucesso de 98.8% no total dos controlos definidos.

4.7. Monitorização

De modo a monitorizar toda a infraestrutura foram instalados dois sistemas de monitorização, um de controlo ambiental e um de monitorização de sistemas e serviços.

4.7.1. Monitorização ambiental

O sistema de controlo ambiental instalado conta com as seguintes características:

- Vídeo vigilância nos dois CPD.
- Sensores de temperatura e humidade no corredor de ar frio e quente.
- Sensor de inundação colocado debaixo do chão falso.
- Ligação às UPS alertando sem caso de avaria ou passagem para corrente socorrida.

- Ligação ao sistema de deteção de extinção de incendio alertado para avarias ou detenção de fogo e disparo da extinção.

Com este sistema é possível monitorizar os CPD de forma centralizada e receber alertas através de *email* caso ocorra algum problema, caso o problema ocorra fora das horas de expediente o alerta é enviado para a equipa de prevenção de sistemas.

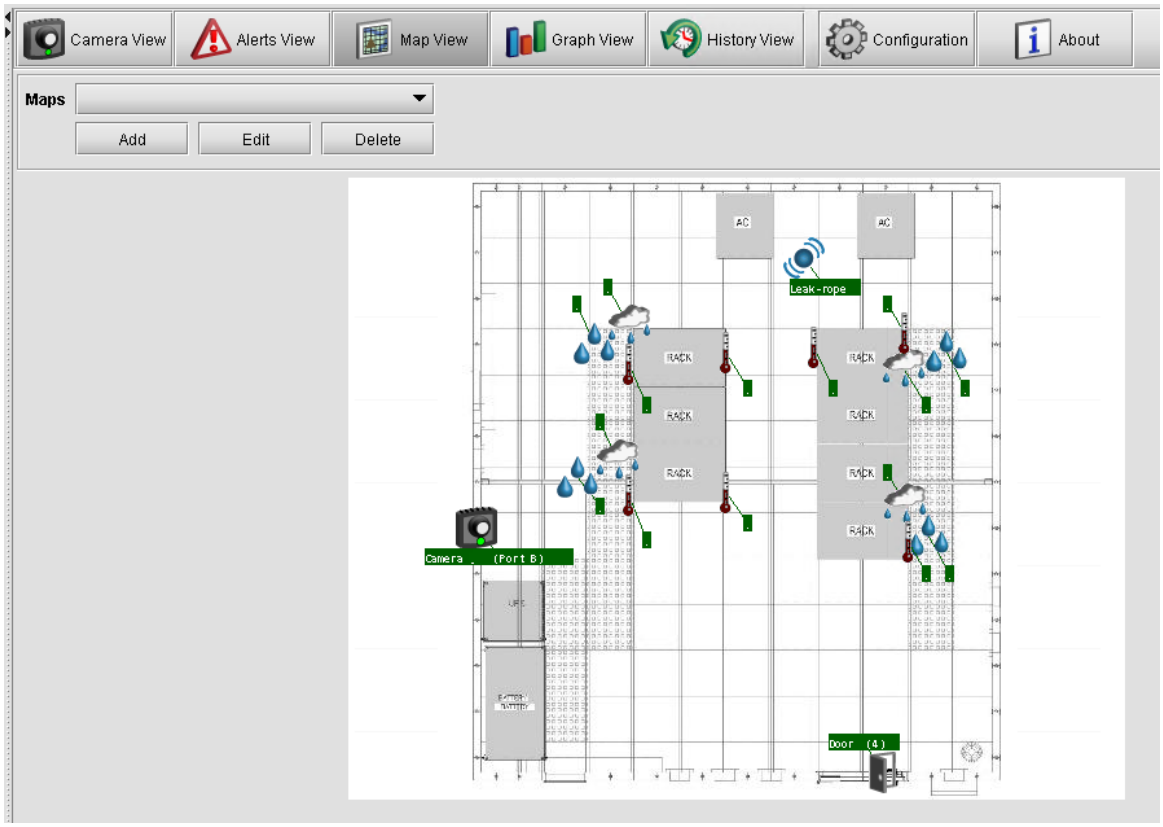


Fig. 28 - Consola de monitorização ambiental

4.7.2. Monitorização de sistemas e serviços

Devido à necessidade de monitorizar os servidores e respetivos serviços foi instalado o sistema de monitorização *System Center Operations Manager*, deste modo é possível monitorizar e recolher alertas sobre o estado da infraestrutura de servidores.

Esta ferramenta fornece uma consola centralizada de alarmes, e utiliza uma abordagem de management packs específicos para cada tipo de serviço, com regras de monitorização que podem ser customizadas conforme as necessidades, fornecendo alarmística, não só do *hardware* ou *software* mas do serviço como um todo.

Os vários serviços podem ser agregados e vistos como componentes de um serviço global, tomado o exemplo de uma aplicação *web*, podemos agregar os componentes de *hardware* e *software* de todos os servidores que intervém no processo de disponibilização

do serviço como *domain controler*, equipamentos de rede, base de dados, serviços de IIS, balanceadores de carga e uma vista da aplicação, onde o sistema de monitorização simula um utilizador a efetuar uma operação na aplicação, e mede a performance da operação disparando alertas em caso de atingir os valores definidos.

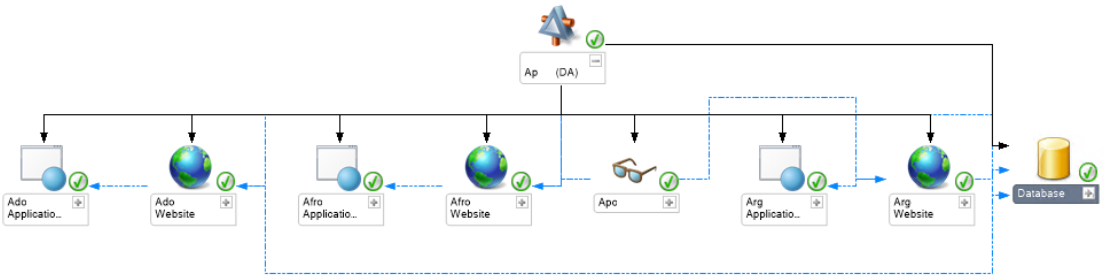


Fig. 29 - Vista estrutura de aplicação

Por sua vez as aplicações criadas como a o exemplo acima, podem ser agregadas em serviços fornecendo uma vista global.

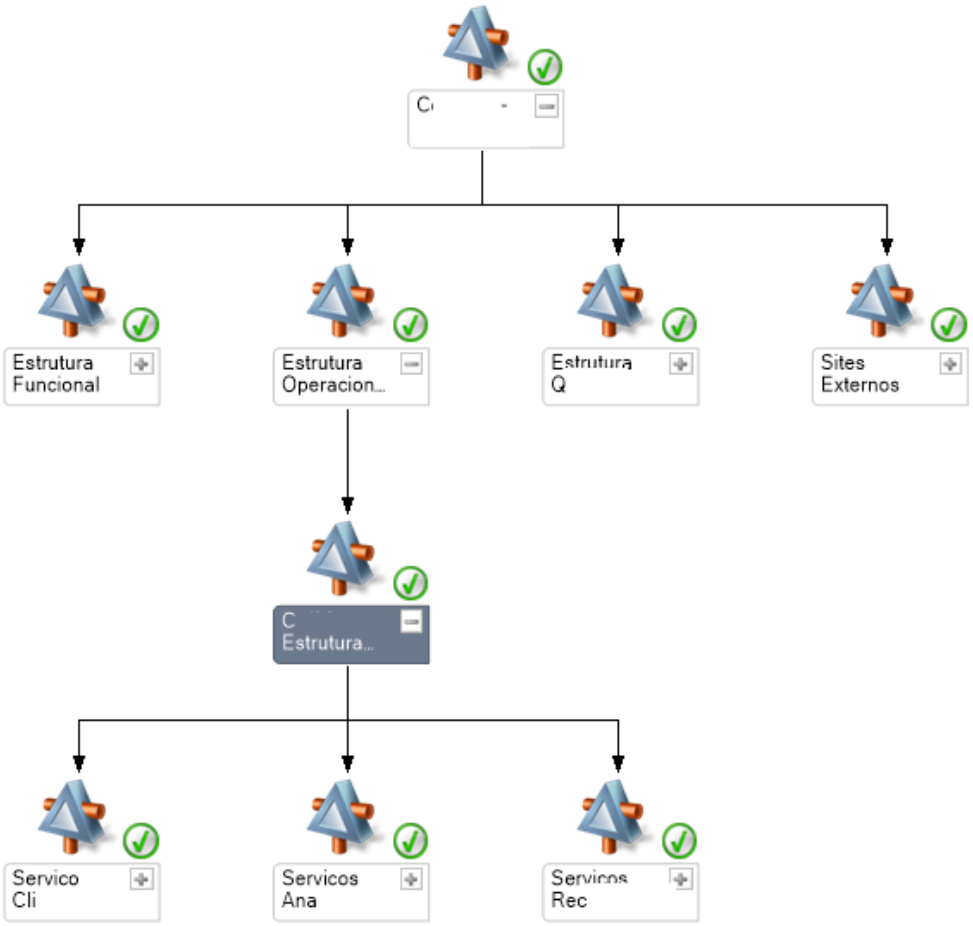


Fig. 30 - Vista estrutura agregação por serviço

Outra das funcionalidades interessantes desta ferramenta é a criação de *dashboards* que mostram a informação de forma sintetizada e percetível aos técnicos de monitorização, facilitando a deteção de problemas de uma forma precoce.

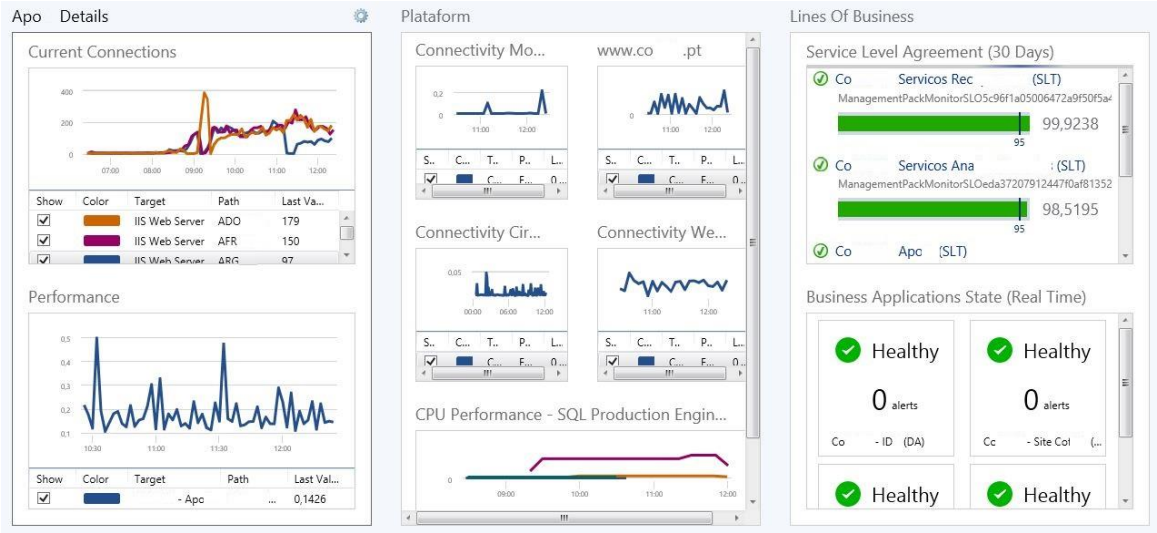


Fig. 31 - *Dashboard* monitorização

Todos os alertas gerados são recebidos pela equipa de operações e monitorização sendo encaminhados para as equipas de prevenção fora do horário de expediente.

5. Análise e discussão de resultados

Neste ponto irá ser efetuada a análise do que foi desenvolvido pela organização face às boas práticas apuradas na revisão da literatura.

De modo a facilitar a leitura e analise irá ser seguido um código de cores em que:

- Objetivo alcançado – Representa que o objetivo em questão foi cumprido pela organização.
- Objetivo alcançado parcialmente – Representa que o objetivo em questão foi cumprido em parte pela organização, no entanto existem pontos a melhorar.
- Objetivo não alcançado - Representa que o objetivo em questão foi não foi cumprido.

Para verificar a percentagem de *compliance* da organização foi criado um sistema de pontos em que:

- Objetivo alcançado – Representa dois pontos.
- Objetivo alcançado parcialmente – Representa um ponto.
- Objetivo não alcançado - Representa zero pontos.

No final será calculada a percentagem de *compliance* para cada conjunto de boas práticas.

5.1. Gestão da continuidade do negócio

Como identificado na revisão da literatura a gestão da continuidade do negócio envolve toda a organização e tem como objetivo identificar ameaças que possam por em causa a continuidade da organização e proporcionar uma capacidade de resposta eficaz contra as ameaças identificadas. Assim existem quatro pontos-chave que devem estar compreendidos na gestão da continuidade de negócio:

1. Compreender as necessidades da organização e a necessidade para a criação de um plano de continuidade de negócio as suas políticas e objetivos.
    a. Objetivo alcançado, uma vez que foram auscultadas todas as áreas e apurados os processos chave e os seus impactos para o negócio.
2. Implementar controlos e métricas de forma a medir a capacidade global da organização de resposta a incidentes disruptivos.
    a. Objetivo alcançado parcialmente, são feitos testes periódicos de avaliação da capacidade da recuperação, mas raramente são envolvidas todas as áreas da organização e existem pontos no plano de teste que nunca foram testados como o teste à capacidade de recuperação face à indisponibilidade de recursos humanos que implica uma restruturação de hierarquias, no entanto existe registo de controlos e métricas no registo de testes que podem ser utilizados para medir a capacidade de resposta da organização a incidentes disruptivos.
3. Monitorizar a performance e a efetividade do plano de continuidade de negócio.
    a. Objetivo alcançado parcialmente, durante os testes periódicos é medida a performance e efetividade do plano, no entanto como referido nem todas as componentes do teste foram testadas e apesar o plano de testes referir que os testes devem ocorrer anualmente a evidência do último teste é de 2013.
4. Melhoria continua baseada na avaliação dos objetivos.
    a. Objetivo alcançado, os documentos que suportam a gestão da continuidade de negócio são revistos e atualizados anualmente mantendo o alinhamento com os objetivos do negócio e tendo em conta os resultados dos testes efetuados com o objetivo de melhorar o processo.

Os objetivos da gestão da continuidade de negócio passam não só pela recuperação em caso de disrupção mas também pelo reconhecer o valor acrescentado que as boas práticas de gestão da continuidade trazem para a organização assim os objetivos da gestão da continuidade do negócio são:

- Proteção do valor da organização beneficiando os acionistas.
    - Objetivo alcançado, através da preservação do negócio e imagem para o cliente aumentado a disponibilidade dos sistemas e criando os mecanismos de continuidade em caso de desastres tipo 3.
- Maior compreensão do negócio como resultado da análise de riscos.

    - Objetivo alcançado, através do BIA onde são mapeados os processos críticos e os seus impactos para o negócio.
- Resiliência operacional resultante da redução de risco.
    - Objetivo alcançado, através de arquiteturas de alta disponibilidade e gestão de TI segundo as boas práticas do ITIL.
- Redução de *downtime* através da identificação de *workarounds* para mitigar as disrupções.
    - Objetivo alcançado, o *downtime* foi reduzido e foram implementados *workarounds* de forma a mitigar as disrupções, de salientar que a maior parte dos *workarounds* é automático conseguido com tecnologias de alta disponibilidade.
- Podem ser identificadas questões de conformidade para outros processos.
    - Objetivo alcançado, tratando-se de uma instituição financeira está abrangida por regulamentação do agente regulador, neste caso o Banco de Portugal e convenções internacionais como o Basileia III, os requisitos impostos pelos regulamentos e convenções foram tidos em conta.
- Registos relevantes para a organização podem ser mantidos e protegidos.
    - Objetivo alcançado, todos os registos relevantes são efetuados em formato eletrónico e armazenados em áreas restritas, e assim como toda a informação crítica está abrangida pela política de *backup*
- As questões da legislação de a saúde e segurança são consideradas.
    - Objetivo alcançado, foram consideradas questões de legislação e regulamentação no desenho do plano de continuidade da atividade e foram tidas em conta as questões de saúde e segurança ao desenhar os novos CPD.
- Melhoria operacional através da reengenharia de processos de negócio.
    - Objetivo alcançado parcialmente, não existem evidências de alterações aos processos de negócio derivadas da gestão de continuidade do negócio, no entanto os processos de negócio estão em constante evolução e encontram-se sem sintonia com a gestão da continuidade.
- Proteção dos ativos físicos e do conhecimento do negócio.
    - Objetivo alcançado o conhecimento do negócio é preservado através da atualização periódica do BIA e os ativos físicos estão protegidos pelas medidas de segurança implementadas na organização.
- Preservação dos mercados garantindo a continuidade da atividade.
    - Objetivo alcançado, a preservação do negócio em caso de desastre é um contributo importante para a preservação do mercado uma

vez que a organização é um importante empregador e desempenha um papel importante na economia.

- Melhoria da segurança global
    - Objetivo alcançado, as politicas e processos implementados assim como as questões de saúde e segurança observados no planeamento dos CPD são um contributo importante para a melhoria da segurança global.

Após a análise da gestão de continuidade da atividade podemos concluir que os objetivos foram atingidos na sua larga maioria e a sua implementação contribuiu para uma organização mais resiliente que salvaguarda os interesses dos seus *stakeholders* da sua reputação, marca e cadeia de valor.

No entanto existe espaço para melhorar, executando o plano de testes com mais regularidade, efetuando a totalidade dos testes e incorporando as lições aprendidas nos processos de negócio.

***Compliance* = 86.6%**

5.2. Business Impact Analysis (BIA)

Como descrito na revisão da literatura o BIA é o processo de analisar as principais atividades e processos da organização e mapear os impactos de eventuais eventos disruptivos no negócio.

Existem três grandes objetivos a alcançar com o BIA:

- Determinar os processos críticos para o negócio e criticidade de recuperação.
    - Objetivo alcançado parcialmente, os processos críticos estão bem definidos assim como o seu impacto para o negócio, no entanto na versão atual do BIA não existe um nível formal de criticidade, no entanto o nível pode ser apurado pelo indicador MTD (*Maximum Tolerable Downtime*) presente em todos os processos \ aplicações e pelo RTO e RPO definidos.
- Identificação de recursos.
    - Objetivo alcançado parcialmente, os recursos humanos estão identificados, no entanto nem todas as áreas indicam os recursos de equipamento, dados, comunicações.
- Identificar prioridades de recuperação.
    - Objetivo não alcançado, não existe registo formal das prioridades de recuperação no BIA, no entanto as prioridades podem ser seguidas pelo MTD mais baixo.

Apos a análise do BIA conclui-se que o BIA esta bem estruturado contendo a avaliação dos impactos de um desastre para o negócio, no entanto não foram encontradas evidências de uma escala de criticidade para os processos e nem todas as áreas indicaram os recursos

necessários à recuperação. Não existe evidência de uma escala de prioridades de recuperação.

***Compliance* = 33.3%**

5.3. Disaster recovery

Como apurado na revisão de literatura, *disaster recovery* é a capacidade de uma organização continuar a fornecer serviço após o normal funcionamento ter sido interrompido por um evento disruptivo.

Objetivo alcançado, a organização criou uma infraestrutura de alta disponibilidade apoiada em dois novos CPD, um principal *tier* IV e um de recuperação *tier* II separados 20Km. Utilizou os princípios de alta disponibilidade para a estrutura de rede, utilizando redundância e caminhos alternativos para todas as ligações ao exterior e entre equipamentos, assim como os princípios da virtualização, tanto para os servidores como para os serviços disponibilizados. Verificou-se também uma política e processos de gestão de continuidade da atividade, que já demostrou através de testes à solução, ser capaz de recuperar a atividade no CPD de recuperação respeitando o MTD, RTO e RPO definido no BIA.

***Compliance* = 100%**

5.4. Análise face à ISO 22301

A norma ISO surge como norma internacional de referência e especifica os requisitos para planear, rever e manter o processo de continuidade de negócio, sendo uma norma genérica com princípios aplicáveis a todas as organizações

5.4.1. Contexto da organização

Neste ponto é necessário identificar o âmbito do PCN tendo em conta os objetivos estratégicos do negócio, os produtos e serviços chave, a tolerância ao risco e as obrigações legais e regulatórias.

A organização deve criar um documento com os seguintes pontos:

- Identificação das atividades, funções, serviços, produtos, parcerias, fornecedores. Impacto para estas atividades de um evento disruptivo.
    - Objetivo alcançado, existe uma identificação de atividades, funções, serviços, produtos, fornecedores e respetivo impacto no BIA.
- Pontos de ligação entre as políticas de continuidade do negócio e os objetivos e políticas da organização incluindo a estratégia global de risco.

    - Objetivo alcançado parcialmente, não existe evidência de um documento que contenha a estratégia global de risco, no entanto o PCN está alinhado com os objetivos da organização.
- A apetência ao risco da organização.
    - Objetivo não alcançado, não existe registo da apetência ao risco.
- Articular os seus objetivos com o plano de continuidade de negócio.
    - Objetivo alcançado, os objetivos da organização estão alinhados com o PCN.
- Definir os fatores internos e externos que potenciam o risco.
    - Objetivo não alcançado, o documento do Plano de gestão de crise descreve os tipos de desastres mas não são especificados os fatores que potenciam o risco.
- Definir o critério de risco tendo em conta a apetência ao risco da organização.
    - Objetivo não alcançado, não existe registo da apetência ao risco
- Definir o propósito do PCN.
    - Objetivo alcançado, o propósito do PCN encontra-se definido no modelo de gestão do PCN
- Todas as partes interessadas para o PCN.
    - Objetivo alcançado, todas as partes interessadas estão envolvidas no PCN ou tem o seu conhecimento.
- Os requisitos de todos os interessados.
    - Objetivo alcançado, foi feito um levantamento de requisitos que é mantido atualizado no BIA.

No documento de definição de âmbito a organização deve:

- Determinar as áreas da organização a incluir no PCN.
    - Objetivo alcançado, as áreas a incluir no PCN estão descritas no documento Plano de Gestão de Crise.
- Estabelecer os requisitos do PCN, considerando a missão, objetivos, obrigações internas e externas da organização.
    - Objetivo alcançado, os requisitos estão definidos no BIA tendo em conta a missão, objetivos e obrigações da organização.
- Identificar produtos e serviços e todas as atividades relacionadas dentro do âmbito do PCN.
    - Objetivo alcançado, os serviços e todas as atividades que os suportam estão presentes no BIA.
- Ter em conta as necessidades e interesses de todas as partes como clientes, investidores, acionistas, cadeia de fornecimento, necessidades da comunidade, expectativas dos interessados.
    - Objetivo alcançado, os interesses dos interessados foram tidos em conta no desenho do PCN.
- Definir o âmbito do PCN em termos da natureza, tamanho, complexidade da organização.

- Objetivo não alcançado, não existe uma definição formal do âmbito do PCN.

Não existe um documento formal de definição de âmbito, no entanto alguns dos pontos são tratados em outros documentos do plano de continuidade de negócio.

No conjunto da documentação não foi encontrado evidências de um documento contendo a informação legal atualizada, existe um parecer do Banco de Portugal sobre planos de continuidade da atividade.

Deve ser criado um documento e mantido atualizado com os requisitos legais e regulatórios da sua atividade no que diz respeito à continuidade da atividade, operações produtos ou serviços.

***Compliance* = 67.8%**

5.4.2. Papel da Gestão, liderança

A gestão de topo deve demostrar liderança e compromisso com o PCN.

A gestão de topo é responsável por:

- Assegurar que o PCN é compatível com a estratégia da organização.
  - Objetivo alcançado, a gestão de topo participa no comité de crise responsável pela definição do PCN.
- Integrar os requisitos do PCN nos processos da empresa.
  - Objetivo alcançado, os processos da empresa foram desenhados tendo em conta o PCN.
- Disponibilizar os recursos necessários.
  - Objetivo alcançado, todos os recursos necessários é definição e implementação do PCN foram disponibilizados.
- Comunicar a importância do PCN.
  - Objetivo alcançado parcialmente, o PCN está presente no desenho de novas soluções ou serviços, mas não existe uma comunicação institucional a reforçar a importância do PCN.
- Assegurar que o PCN atinge os resultados esperados.
  - Objetivo alcançado, é feito um acompanhamento regular dos testes ao PCN.
- Dirigir e suportar o processo de melhoria continua.
  - Objetivo alcançado, como membro do comité de crise apoia o processo de melhoria continua.
- Estabelecer e comunicar a política de continuidade de negócio.

    - Objetivo não alcançado, a política de continuidade está contida no modelo de gestão do PCN.
- Assegurar que os objetivos e planeamento do PCN são efetuados.
    - Objetivo alcançado, existe um acompanhamento regular do planeamento e execução do PCN.
- Assegurar que as responsabilidades dos principais papéis são atribuídas.
    - Objetivo alcançado, o comité de crise atribuiu responsabilidades e papeis na execução do PCN.
- Orientar e apoiar as pessoas envolvidas com o PCN.
    - Objetivo alcançado, através da participação no comité de crise e do acompanhamento aos testes periódicos.
- Apoiar outras áreas de gestão demostrando liderança e compromisso com o PCN.
    - Objetivo alcançado, a gestão de topo demonstra compromisso com o PCN e apoia sempre que necessários as outras áreas de gestão.
- Definir critérios de aceitação para riscos e definir quais os níveis aceitáveis de risco.
    - Objetivo não alcançado, não existe evidência da definição de critérios de risco.
- Participar ativamente nos testes.
    - Objetivo alcançado, participa nos testes, apoia e realça a sua importância junto de todas as áreas de negócio.
- Assegurar que são efetuadas auditorias ao PCN.
    - Objetivo não alcançado, não são feitas auditorias ao PCN.
- A política deve ser apropriada à atividade da organização.
    - Objetivo não alcançado, a política esta dentro do documento Manual de Gestão do PCN não existindo como documento no entanto a política é apropriada à organização.
- A política deve definir uma *framework* para definir os objetivos da continuidade de negócio.
    - Objetivo não alcançado, não existe uma *framework* para definir os objetivos da continuidade de negócio, mas no entanto está patente em todos os documentos que o objetivo principal é recuperar a atividade em caso de desastre.
- A política deve satisfazer os requisitos definidos.
    - Objetivo não alcançado, a política esta dentro do documento Manual de Gestão do PCN.
- A política deve enfatizar a melhoria contínua do PCN
    - Objetivo não alcançado, a política não enfatiza a melhoria contínua do PCN.

A política do PCN deve:

- Estar disponível como documento.

    - Objetivo não alcançado, a política esta dentro do documento Manual de Gestão do PCN.
- Ser comunicada á organização.
    - Objetivo não alcançado, a política esta dentro do documento Manual de Gestão do PCN.
- Estar disponível a todas as partes interessadas.
    - Objetivo alcançado, embora não exista como documento esta no Manual de Gestão do PCN que é disponibilizado a todos os interessados.
- Ser revista em intervalos definidos ou caso exista uma mudança significativa.
    - Objetivo não alcançado, a última alteração registada tem mais de um ano.

Apos a analise deste ponto conclui-se que a gestão de topo está envolvida no PCN, no entanto não existe um documento formal de política de continuidade da atividade, estando a mesma incluída no Manual de Gestão do PCN que não é atualizado há mais de um ano.

***Compliance* = 52.3%**

5.4.3. Planeamento

Na criação do planeamento deve ser tido em conta os requisitos levantados nos pontos anteriores e deve:

- Assegurar que pode atingir os objetivos propostos.
    - Objetivo alcançado, os objetivos de recuperação definidos são alcançáveis.
- Prevenir ou reduzir efeitos indesejados.
    - Objetivo alcançado, o planeamento foi feito no sentido de evitar efeitos indesejados.
- Atingir a melhoria continua.
    - Objetivo alcançado, os documentos são revistos e melhorados com regularidade.

A organização deve planear:

- As ações para endereçar os riscos e oportunidades.
    - Objetivo alcançado, são identificados riscos e oportunidades, as ações são planeadas de forma a mitigar os riscos.
- Integrar e implementar as ações no processo de continuidade de negócio.
    - Objetivo alcançado, as ações de mitigação de riscos são incluídas no processo.
- Avaliar a aplicação dessas ações.
    - Objetivo alcançado, o resultado as ações são avaliados a quando dos testes.

Os objetivos devem:

- Ser consistentes com a política de continuidade de negócio.
    - Objetivo alcançado, os objetivos são consistentes com a política de continuidade de negócio.
- Ter em conta o nível mínimo de produção ou serviço que é aceitável apara a organização.
    - Objetivo alcançado, os objetivos definidos no BIA tem em conta os níveis mínimos de serviço aceitáveis para a organização.
- Ser mensuráveis.
    - Objetivo alcançado, os objetivos de recuperação são concretos e mesuráveis.
- Ter em conta os requisitos definidos.
    - Objetivo alcançado, os objetivos tem em conta os requisitos definidos no BIA.
- Ser monitorizados e atualizados.
    - Objetivo alcançado, os objetivos são atualizados periodicamente no BIA

A organização deve manter os objetivos documentados, para criar o documento de objetivos da continuidade da atividade deve determinar

- Quem é o responsável.
    - Objetivo não alcançado, não existe documento formal de objetivos, embora os objetivos sejam descritos no BIA.
- O que vai ser feito.
    - Objetivo não alcançado, não existe documento formal de objetivos, embora os objetivos sejam descritos no BIA.
- Quais os recursos necessários.
    - Objetivo não alcançado, não existe documento formal de objetivos, embora os objetivos sejam descritos no BIA.
- Quando irá ficar completo.
    - Objetivo não alcançado, não existe documento formal de objetivos, embora os objetivos sejam descritos no BIA.
- Como vão ser avaliados os resultados.
    - Objetivo não alcançado, não existe documento formal de objetivos, embora os objetivos sejam descritos no BIA.

A organização efetuou o planeamento para a recuperação da atividade no entanto não existe um documento formal de objetivos, embora os objetivos aparecem no BIA, é recomendado a criação do documento formal.

***Compliance* = 68.7%**

5.4.4. Suporte

O suporte eficiente do PCN está assente na utilização de recursos adequados para cada tarefa, é importante assegurar que o pessoal tem a formação adequada. Outro aspeto importante é a comunicação.

A organização deve determinar e fornecer os recursos necessários para a criação, implementação, manutenção e melhoria contínua do PCN, para isso a organização deve:

- Determinar as competências necessárias das pessoas que irão executar o PCN.
  - Objetivo alcançado parcialmente, não existe um referencial de competências no PCN no entanto o plano de gestão da crise faz referencias a funções e esta implícito que determinada função possui determinadas competências.
- Assegurar que essas pessoas são competentes e tem a educação, formação e experiencia adequada.
  - Objetivo alcançado parcialmente, a quando da contratação de pessoal são verificados aspetos como educação, formação e experiencia.
- Quando aplicável tomar ações de forma a adquirir competências e avaliar o resultado dessas ações.
  - Objetivo não alcançado, não existem evidências de ações com vista a aumentar as competências desejadas.
- Manter a documentação apropriada como evidencia das competências.
  - Objetivo não alcançado, não é mantido um registo de evidências de competências na documentação do PCN.

As pessoas que intervêm no PCN devem ter conhecimento:

- Da política de continuidade do negócio.
  - Objetivo alcançado, a documentação é disponibilizada a todos os intervenientes no PCN.
- O seu papel e contributo para o PCN.
  - Objetivo alcançado, as pessoas envolvidas no PCN estão cientes do seu papel e contribuído.
- As implicações de não seguir o PCN.
  - Objetivo alcançado, as pessoas envolvidas no PCN estão cientes das implicações de não seguir o PCN.
- Seu papel em caso de incidente disruptivo.
  - Objetivo alcançado, as pessoas envolvidas no PCN estão cinetes do seu papel em caso de incidente disruptivo.

A organização deve determinar a relevância da comunicação interna e externa incluindo:

- O que deve ou não ser comunicado.
    - Objetivo alcançado, o documento de Plano de Gestão de Crise, descreve o que deve ser comunicado.
- Quando comunicar.
    - Objetivo alcançado, o documento de Plano de Gestão de Crise descreve quanto comunicar.
- A quem comunicar.
    - Objetivo alcançado, o documento de Plano de Gestão de Crise descreve a quem comunicar.

A organização deve criar, implementar e manter um procedimento para:

- Comunicar internamente às partes interessadas e aos empregados da organização.
    - Objetivo alcançado, o documento de Plano de Gestão de Crise descreve o procedimento de comunicação interna.
- Comunicar externamente aos clientes, parceiros, comunidade local, e outras partes interessadas como os média.
    - Objetivo alcançado, o documento de Plano de Gestão de Crise descreve o procedimento de comunicação para entidades externas incluindo a comunicação social.
- Receber, documentar e responder a comunicação das partes interessadas.
    - Objetivo não alcançado, não existe evidência de documentos com procedimento para receber, documentar e responder a comunicações das partes interessadas.
- Adaptar ou integrar um sistema de alerta de ameaças regional ou nacional.
    - Objetivo não alcançado, a organização não integra um sistema de alertas de ameaças.
- Assegurar a disponibilidade dos meios de comunicação durante um evento disruptivo.
    - Objetivo alcançado, está previsto a disponibilização de meios de comunicação durante um evento disruptivo.
- Comunicar com as autoridades.
    - Objetivo não alcançado, o documento de Plano de Gestão de Crise que refere os procedimentos de comunicação não faz referência a comunicação com as autoridades.
- Operar e testar o plano de comunicação a utilizar em caso de evento disruptivo.
    - Objetivo alcançado, o plano de execução de testes faz referência a um teste executado com sucesso ao plano de comunicação.

O PCN deve incluir:

- A documentação referida nesta ISO.
    - Objetivo não alcançado, existem documentos na ISO que não estão contemplados no PCN da organização.

- Toda a documentação que a organização considere pertinente para o sucesso do PCN, esta documentação pode variar segundo:
    - Objetivo alcançado, existe documentação acessória no PCN da organização.

Na criação do documento a organização deve assegurar:

- A identificação e descrição do documento (Titulo, data, autor, e/ou numero de referencia)
    - Objetivo alcançado, toda a documentação está devidamente identificada.
- Formato (linguagem, versão software, etc.) e media (formato eletrónico, papel, etc.)
    - Objetivo alcançado, toda a documentação está em formato eletrónico.

Toda a documentação deve ser controlada para assegurar:

- A sua disponibilidade.
    - Objetivo alcançado, a documentação esta em formato eletrónico protegida contra acessos indevidos e é alvo do processo de *backup*.
- A proteção adequada (perca de informação, confidencialidade, integridade).
    - Objetivo alcançado, a documentação esta em formato eletrónico protegida contra acessos indevidos e é alvo do processo de *backup*

Para controlar a informação do documento a organização deve endereçar as seguintes atividades sempre que aplicável:

- Distribuição, acesso, recuperação e utilização.
    - Objetivo alcançado, a documentação esta em formato eletrónico disponível a todos os interessados e protegida contra acessos indevidos e é alvo do processo de *backup*
- Preservação.
    - Objetivo alcançado, a documentação esta em formato eletrónico disponível a todos os interessados e protegida contra acessos indevidos e é alvo do processo de *backup*
- Controlo de alterações.
    - Objetivo alcançado, toda a documentação tem um histórico de versões e alterações.
- Recuperação e utilização.
    - Objetivo alcançado, a documentação esta em formato eletrónico disponível a todos os interessados e protegida contra acessos indevidos e é alvo do processo de *backup*
- Preservação da sua legibilidade (o documento deve ser de leitura clara).

    - Objetivo alcançado, toda a documentação foi elaborada com a sua legibilidade.
- Preservação de utilização de informação obsoleta.
    - Objetivo alcançado, a documentação antiga é retirada para uma pasta de histórico ficando só disponível a documentação atualizada.

No que diz respeito à análise do ponto suporte a, organização demostra possuir os meios de controlo e comunicação, no entanto não existe uma gestão de competências no PCN, o plano de comunicação pode ser melhorado de forma a incluir a comunicação com as autoridades e deve conter um procedimento de receção, registo e resposta no que diz respeito a comunicações externas. Como já referido noutros pontos, o PCN da organização não contem todos os documentos descritos na ISO 22301.

***Compliance* = 76.6%**

5.4.5. Operação

Esta fase compreende a operacionalização do planeamento efetuado nos pontos anteriores.

A organização deve planear implementar e controlar o processo, assim deve:

- Estabelecer um critério para os processos.
    - Objetivo alcançado, existe um critério definido no modelo de gestão do PCN.
- Implementar um mecanismo de controlo de processos com base nos critérios definidos.
    - Objetivo alcançado, existe um circuito de revisão do processo definido no modelo de gestão do PCN.
- Manter um registo na medida do necessário para ter confiança que os processos têm sido executados conforme definido.
    - Objetivo alcançado parcialmente, existem registos de atualização dos documentos, o único registo de execução está no plano de execução de testes.

A organização deve estabelecer, implementar e manter um processo formal e documentado para o *business impact analysis and risk assessment* que:

- Estabeleça o contexto de avaliação, definição de critério e a avaliação do impacto potencial de um evento disruptivo.
    - Objetivo alcançado parcialmente, o BIA contem o impacto potencial de um evento disruptivo para o processo de negócio, mas não estabelece o critério e o contexto.
- Tenha em conta os requisitos legais e outros que a organização considere relevantes.

    - Objetivo alcançado, são tidos em conta todos os aspetos relevantes para a organização.
- Inclua uma análise sistemática, priorização de tratamento do risco e dos custos relacionados.
    - Objetivo alcançado parcialmente, não existe uma priorização do tratamento do risco, mas contem estimativas de custos em alguns processos.
- Definir os requisitos de output do *business impact analysis and risk assessment*.
    - Objetivo alcançado, os outputs estão bem definidos.
- Especifique os requisitos para que a informação seja atualizada e permaneça confidencial.
    - Objetivo alcançado parcialmente, existem requisitos de atualização mas não é referida confidencialidade.

O BIA deve incluir o seguinte:

- Identificar as atividades que suportam o negócio.
    - Objetivo alcançado, estão identificadas as atividades que suportam o negócio.
- Avaliar os impactos nas atividades ao longo do tempo.
    - Objetivo alcançado, estão definidos os impactos para todas as atividades.
- Determinar prazos para retomar as diversas atividades dentro de um nível mínimo aceitável, tendo em conta o prazo máximo a partir do qual não é aceitável para o negócio.
    - Objetivo alcançado, existe um prazo máximo definito para todas as atividades.
- Identificar dependências e os recursos essenciais para as atividades incluindo, fornecedores, parceiros, e outras partes relevantes.
    - Objetivo alcançado, estão identificadas as dependências e recursos para todas as atividades incluindo todas as partes relevantes.

A organização deve criar, implementar e manter um processo de avaliação de riscos formalmente documentado que sistematicamente identifique, analise e avalie o risco de eventos disruptivos para a organização.

A organização deve:

- Identificar os riscos de eventos disruptivos para as atividades, processos, sistemas, informação, pessoas, bens, parceiros, e outros recursos que os suportem.
    - Objetivo alcançado, o documento Plano de Gestão de crise identifica os riscos para a atividade.
- Analisar os riscos de forma sistemática.

    - Objetivo não alcançado, não existe evidência de uma análise sistemática dos riscos.
- Avaliar que eventos disruptivos querem intervenção.
    - Objetivo não alcançado, não existe uma avaliação de que eventos disruptivos requerem intervenção.
- Identificar ações compatíveis com os objetivos de continuidade de negócio e a apetência da organização pelo risco.
    - Objetivo não alcançado, não existe uma avaliação da apetência da organização pelo risco.

A estratégia de continuidade do negócio deve basear-se nos outputs do *business impact analysis and risk assessment.* A organização deve determinar a estratégia apropriada para:

- Proteger as atividades com maior relevância para o negócio.
    - Objetivo alcançado, o PCN foi elaborado com base nos requisitos do BIA de forma a proteger as atividades críticas do negócio.
- Estabelecer, continuar, retomar as atividades priorizadas e as suas dependências, suportes e recursos.
    - Objetivo alcançado, o PCN inclui processos de continuidades das atividades critica e suas dependências definidas no BIA.
- Mitigar, respondendo e gerindo os impactos.
    - Objetivo alcançado, o PCN inclui planos de mitigação dos impactos, seja restabelecendo a atividade no CPD de recuperação seja através de processos manuais.

A organização deve determinar os requisitos e recursos para implementar as estratégias escolhidas, os tipos de recursos a considerar devem ser os seguintes entre outros que a organização considere relevantes

- Pessoas.
    - Objetivo alcançado, este tipo de recurso está identificado no BIA para todos os processos de negócio.
- Informação e dados.
    - Objetivo alcançado, este tipo de recurso está identificado no BIA para todos os processos de negócio.
- Edifícios, ambiente de trabalho.
    - Objetivo alcançado, este tipo de recurso está identificado no BIA para todos os processos de negócio.
- Instalações, equipamento e consumíveis.
    - Objetivo alcançado, este tipo de recurso está identificado no BIA para todos os processos de negócio.
- Sistemas e tecnologias de informação e comunicação.
    - Objetivo alcançado, este tipo de recurso está identificado no BIA para todos os processos de negócio.

- Transporte.
    - Objetivo alcançado, este tipo de recurso está identificado no Plano de Gestão de Crise.
- Budget.
    - Objetivo alcançado, existe um documento acessório com os custos da implementação da solução e os custos mensais estão refletidos no budget da organização.
- Parceiros e fornecedores.
    - Objetivo alcançado, este tipo de recurso está identificado no BIA para todos os processos de negócio.

Para tratamento dos riscos identificados as organizações devem considerar as seguintes medidas proactivas.

- Reduzir a probabilidade de disrupção.
    - Objetivo alcançado, a probabilidade de disrupção é reduzida através de tecnologias de alta disponibilidade e processos de suporte e manutenção.
- Reduzir o período de disrupção.
    - Objetivo alcançado, existe uma estrutura de suporte que inclui equipas de prevenção que atuam no imediato em caso de disrupção.
- Limitar o impacto das disrupções nos produtos e serviços chave da organização.
    - Objetivo alcançado, o impacto é limitado através de tecnologias de alta disponibilidade e redundância de sistemas de suporte às aplicações de negócio.

A organização deve criar, implementar e manter procedimentos de continuidade da atividade para gerir os incidentes disruptivos e prosseguir com as atividades de negócio com base nos objetivos de recuperação identificados no BIA

Os procedimentos devem:

- Estabelecer o protocolo de comunicação interno e externo.
    - Objetivo alcançado, o plano de gestão de crise endereça o protocolo de comunicação.
- Ser específicos e claros com os passos necessários para retomar a atividade em caso de disrupção.
    - Objetivo alcançado, existe um documento de suporte com as ações a tomar para restaurar o serviço no CPD alternativo.
- Ser flexíveis para responder a ameaças imprevistas e mudanças das condições internas e externas.
    - Objetivo alcançado, os procedimentos são flexíveis.
- Ser focados no impacto dos eventos disruptivos.

    - Objetivo alcançado, os procedimentos são focados nos impactos dos eventos disruptivos.
- Ser desenvolvidos com base em prossupostos estabelecidos e na análise de interdependências.
    - Objetivo alcançado, os procedimentos tem em conta as interdependências apuradas no BIA.
- Deve ser eficaz para minimizar as consequências, através de estratégias de mitigação adequadas.
    - Objetivo alcançado, os procedimentos são eficazes e testados com periodicamente.

A organização deve criar, documentar e implementar procedimentos e uma estrutura para responder a incidentes disruptivos através de pessoal com a responsabilidade, autoridade e competência para gerir o incidente.

A estrutura de resposta deve:

- Identificar o *threshold* que justifique o início da resposta formal.
    - Objetivo alcançado, o Plano de gestão da crise endereça esta questão.
- Avaliar a natureza e extensão do incidente disruptivo e o seu potencial impacto.
    - Objetivo alcançado, o Plano de gestão da crise endereça esta questão.
- Ativar a resposta de continuidade do negócio apropriada.
    - Objetivo alcançado, o Plano de gestão da crise endereça esta questão.
- Ter processos e procedimentos para a ativação, operação, coordenação e comunicação.
    - Objetivo alcançado, existem procedimentos para cada fase (Lançamento, Decisão, Ativação, Execução, Recomeço, Recuperação)
- Ter recursos disponíveis para suportar o processo e os procedimentos de gestão de incidentes disruptivos de forma a minimizar o impacto.
    - Objetivo alcançado, existem recursos para suportar o processo.
- Comunicar com as partes interessadas, autoridades e a média.
    - Objetivo alcançado parcialmente, existe procedimento de comunicação mas não inclui a comunicação com as autoridades.

Devem existir procedimentos atualizados para:

- Detetar um incidente.
    - Objetivo alcançado, existe um processo de gestão de incidentes, responsável por detetar incidentes disruptivos.
- Monitorizar um incidente.
    - Objetivo alcançado, existe um processo de gestão de incidentes, responsável por monitorizar incidentes e sendo um incidente disruptivo existe um comité de crise que acompanha a evolução do incidente.
- Comunicação interna com a organização documentada.

    - Objetivo alcançado, existe procedimento para a comunicação interna no plano de gestão de crise.
- Comunicação documentada com as entidades nacionais ou regionais de aviso de riscos.
    - Objetivo não alcançado, não existe procedimento de comunicação com entidades de aviso de riscos.
- Assegurar os meios de comunicação durante um incidente disruptivo.
    - Objetivo alcançado, estão previstos os meios de comunicação em caso de incidente disruptivo.
- Estrutura definida de comunicação com as entidades de emergência.
    - Objetivo não alcançado, não existe procedimento de comunicação com as entidades de emergência.
- Registo de informação vital sobre o incidente, ações e decisões tomadas.
    - Objetivo alcançado, está previsto o registo de todas as ações tomadas e informação vital do incidente.

A organização deve estabelecer procedimentos documentados de reposta a incidentes disruptivos e de como recuperar as atividades afetadas num espaço de tempo predefinido. Estes procedimentos devem endereçar os requisitos de quem os vai executar:

O PCN deve:

Definir os papéis e responsabilidades das pessoas e equipas que tem autoridade durante um incidente.

- Definir um processo para ativar a resposta.
    - Objetivo alcançado, existe um processo definido no Plano de Gestão de Crise e no plano de recuperação de sistemas.
- Detalhar como gerir as consequências imediatas de um incidente:
    - O bem-estar os indivíduos.
        - Objetivo não atingido, não foram encontradas na documentação medidas destinadas ao bem-estar dos indivíduos.
    - A estratégia, tática e opções operacionais para responder ao incidente.
        - Objetivo alcançado, existe um processo definido no Plano de Gestão de Crise e no plano de recuperação de sistemas
- Detalhar como e em que circunstancias a organização irá comunicar com os funcionários.
    - Objetivo alcançado, definido no plano de gestão de crise.
- Como a organização irá recuperar as suas atividades prioritárias dentro do tempo período definido.
    - Objetivo alcançado, definido no plano de gestão de crise.

- Detalhes de como a organização deve responder à comunicação social após um incidente, incluindo.
    - Objetivo alcançado, definido no plano de gestão de crise.

Cada plano deve definir:

Propósito e âmbito.

- Objetivos.
    - Objetivo alcançado, os planos referem os seus objetivos.
- Critérios e procedimentos de ativação.
    - Objetivo alcançado, o plano de gestão de crise estabelece os critérios de ativação dos planos do PCN.
- Procedimentos de implementação.
    - Objetivo alcançado, os planos referem os procedimentos de implementação.
- Papéis, responsabilidades e autoridades.
    - Objetivo alcançado, o plano de gestão de crise estabelece os papéis e responsabilidades.
- Procedimentos e requisitos de comunicação.
    - Objetivo alcançado, o plano de gestão de crise estabelece os requisitos de comunicação.
- Interdependências internas e externas.
    - Objetivo alcançado parcialmente, nem todos os planos referem as interdependências.
- Requisitos de recursos.
    - Objetivo alcançado parcialmente, nem todos os planos tem os requisitos de recursos.
- Fluxo de informação e processos de documentação.
    - Objetivo alcançado parcialmente, nem todos os planos tem fluxo de informação definido.

A organização deve ter documentados os procedimentos de *restore* e retoma da atividade depois das medidas temporárias aplicadas após um incidente de forma a retomar o seu normal funcionamento.

- Objetivo alcançado, o plano de recuperação estipula as ações do período de recuperação.

A organização deve testar com regularidade os procedimentos de continuidade de negócio de modo a assegurar a seu alinhamento com os objetivos definidos:

- Objetivo alcançado, são efetuados testes periódicos.

A organização deve promover testes que:

- Sejam consistentes e no âmbito do PCN.
    - Objetivo alcançado, os testes descritos no plano de teste são consistentes com o âmbito do PCN.
- Sejam baseados em cenários apropriados, bem planeados e com objetivos bem definidos.
    - Objetivo alcançado, os cenários são apropriados e com objetivos definidos.
- Feitos ao longo do tempo validem juntos o plano num todo, devem envolver as partes interessadas.
    - Objetivo alcançado, os testes estão divididos em blocos que no seu conjunto validam o plano num todo.
- Devem minimizar o risco de disrupções na normal atividade.
    - Objetivo alcançado, os testes estão divididos em blocos de modo a ser possível testar as partes sem afetar o todo.
- Devem produzir relatórios com os resultados, recomendações e ações para implementar possíveis melhorias.
    - Objetivo não alcançado, não existem evidências de relatórios formais com recomendações e ações de implementação.
- Os testes devem de ser revistos num processo de melhoria continua.
    - Objetivo alcançado, os testes são revistos a cada execução.
- Os testes devem ser feitos em intervalos planeados ou sempre que existam alterações significativas na organização ou no ambiente onde opera.
    - Objetivo alcançado parcialmente, o plano de testes indica que os testes devem ser efetuados a cada ano, mas as evidências mostram que já decorreu mais de um ano desde os últimos testes.

Após a revisão deste ponto conclui-se que a organização está preparada para suportar o PCN, no entanto existe espaço para melhorar o BIA de forma a cumprir com todos os requisitos do Isso. As evidências sugerem que os documentos do PCN não são atualizados com a frequência definida. Não existe uma análise de riscos de forma sistemática. Os procedimentos de comunicação necessitam de ser revistos de forma a contemplar os requisitos da ISO. Não existem relatórios formais dos testes com recomendações de melhoria e por fim os testes não respeitam a periodicidade definida.

***Compliance* = 83.6%**

5.4.6. Avaliação de performance

Apos a implementação do PCN a norma ISO 22301 defende que deve existir uma monitorização permanente e testes periódicos.

Assim a organização deve determinar:

- O que deve ser monitorizado e medido.

    - Objetivo alcançado parcialmente, a única monitorização está referida no plano de execução de testes.
- Os métodos de monitorização, medida, analise e avaliação, de modo a assegurar resultados validos.
    - Objetivo alcançado parcialmente, o plano de teste refere a medida de avaliação mas não refere aos métodos de monitorização e avaliação.
- Quando a monitorização e medição devem ser efetuados.
    - Objetivo alcançado parcialmente, única monitorização está referida no plano de execução de testes e são efetuados a quando da execução dos testes.
- Quando os resultados da monitorização devem ser analisados e avaliados
    - Objetivo não alcançando, não existe na documentação referência a momentos de monitorização, analise e avaliação.

A organização deve:

- Tomar uma ação sempre que necessário para endereçar os resultados antes que ocorra uma não conformidade.
    - Objetivo não alcançado, não existem evidências de ações tomadas para endereçar resultados antes que ocorra uma não conformidade.
- Guardar todos os documentos que sejam evidencia.
    - Objetivo não alcançado, nem todos os documentos que constituem evidências são guardados.

Os procedimentos de monitorização devem fornecer:

- Um conjunto de métricas apropriadas à organização.
    - Objetivo não alcançado, não existe um procedimento formal de monitorização.
- Monitorizar em que medida o PCN e os seus objetivos são cumpridos.
    - Objetivo alcançado parcialmente, não existe procedimento de monitorização, no entanto existe um acompanhamento do processo e teste por parte do comité de crise.
- Indicadores de performance dos processos, procedimentos e funções que protegem as atividades prioritárias.
    - Objetivo não alcançado, não existem indicadores de performance dos processos, procedimentos e funções definidos.
- Monitorizar a conformidade dos objetivos de continuidade de negócio com a ISO 22301.
    - Objetivo não alcançado, não existe um processo de monitorização formal de conformidade com a ISO.
- Monitorizar as evidências históricas de deficiências do PCN.
    - Objetivo alcançado parcialmente, é mantido um histórico dos testes, mas não existe um procedimento formal de monitorização.

- Guardar os resultados do processo de monitorização e avaliação de forma a facilitar as ações corretivas.
    - Objetivo não alcançado, não existe processo formal de monitorização definido.

Avaliação dos procedimentos do PCN:

- A organização deve promover avaliações aos procedimentos do PCN de forma a assegurar a sua adequação e efetividade.
    - Objetivo alcançado, os procedimentos são revistos e avaliados de forma periódica.
- As avaliações deveram ser feitas através de revisões periódicas, exercidos, testes, relatórios pós incidente e indicadores de performance. Alterações significativas devem ser refletidas nos procedimentos.
    - Objetivo alcançado, são feitas revisões e testes periódicos e os processos e procedimentos são alterados sempre que se justifica.
- A organização deve avaliar periodicamente o cumprimento legal e regulatório assim como a aplicação das melhores práticas da indústria e a conformidade com os seus próprios objetivos de continuidade de negócio.
    - Objetivo alcançado, no processo de revisão periódico é tida em conta a legislação e pareceres regulatórios.
- A organização deve promover avaliações periódicas ou quando exista uma alteração significativa.
    - Objetivo alcançado, os procedimentos são revistos periodicamente e alterados sempre que se haja uma alteração que o justifique.

A organização deve promover auditorias internas em intervalos planeados para avaliar o sistema de continuidade de negócio. Verificar se o sistema de continuidade da atividade está conforme:

- Os requisitos da organização para o PCN.
    - Objetivo não alcançado, não são feitas auditorias ao PCN.
- Os requisitos da ISO 22301.
    - Objetivo não alcançado, não são feitas auditorias ao PCN.
- Verificar se o sistema está implementado e mantido atualizado.
    - Objetivo não alcançado, não são feitas auditorias ao PCN.

A organização deve:

- Planear, estabelecer, implementar e manter um programa de auditoria, incluindo a sua frequência, os seus métodos, responsabilidades, requisitos de planeamento e relatório.
    - Objetivo não alcançado, não são feitas auditorias ao PCN.

- O programa de auditoria deve ter em consideração a importância dos resultados das auditorias anteriores.
    - Objetivo não alcançado, não são feitas auditorias ao PCN.
- Definir os critérios e âmbito de auditoria.
    - Objetivo não alcançado, não são feitas auditorias ao PCN.
- Selecionar os auditores e conduzir as auditorias de modo a garantir objetividade e imparcialidade em todo o processo.
    - Objetivo não alcançado, não são feitas auditorias ao PCN.
- Assegurar que os resultados das auditorias são entregues a todos os gestores relevantes para o processo.
    - Objetivo não alcançado, não são feitas auditorias ao PCN.
- As evidências devem ser guardadas como prova da implementação do plano de auditoria.
    - Objetivo não alcançado, não são feitas auditorias ao PCN.

A gestão de topo deve rever o PCN, em períodos pré estabelecidos para assegurar que o PCN continua adequado.

A revisão deve incluir as seguintes considerações:

- O estado das ações de revisões anteriores.
    - Objetivo alcançado, as revisões ao PCN tem em conta as revisões anteriores.
- Alterações internas e externas relevantes para o PCN.
    - Objetivo alcançado, as revisões ao PCN tem em conta as alterações relevantes para o PCN.
- Indicadores de performance do PCN, incluindo:
    - Não conformidades e ações corretivas
        - Objetivo não alcançado, não existe um plano de auditoria ao PCN.
    - Avaliação de resultados do processo de monitorização e avaliação.
        - Objetivo alcançado parcialmente, não existe um plano de monitorização no entanto são tidos em conta os resultados dos testes ao PCN.
    - Resultados de auditorias.
        - Objetivo não alcançado, não existe um plano de auditoria ao PCN.
- Oportunidade de melhoria continua.
    - Objetivo alcançado, são tidas em conta as oportunidades de melhoria continua.

A revisão deve considerar a performance da organização incluindo:

- O acompanhamento de ações de revisões prévias.
    - Objetivo alcançado, existe o acompanhamento das ações de revisões prévias.

- A necessidade de alteração do PCN incluindo politica e objetivos.
    - Objetivo alcançado, no processo de revisão periódico são avaliadas e alteradas se necessário a política e objetivos.
- Oportunidade de melhoria.
    - Objetivo alcançado, são tidas em conta as oportunidades de melhoria.
- Resultados de auditorias e revisões ao PCN.
    - Objetivo não alcançado, não existe um plano de auditoria ao PCN.
- Técnica, produtos ou procedimentos que possam ser utilizados na organização para melhorar o PCN.
    - Objetivo alcançado, no processo de revisão são avaliados técnicas, produtos ou procedimentos para melhorar o PCN.
- Estado das ações corretivas.
    - Objetivo alcançado, são avaliadas as ações corretivas.
- Resultados dos testes.
    - Objetivo alcançado, os resultados dos testes são revistos e considerados.
- Riscos não endereçados corretamente na avaliação de risco.
    - Objetivo alcançado, os riscos encontrados na avaliação de risco são avaliados e idos em conta.
- Alterações que possam afetar o PCN sejam internas ou externas.
    - Objetivo alcançado, as alterações que possam afetar o PCN são tidas em conta no processo de revisão.
- Verificar se a politica continua adequada.
    - Objetivo alcançado, a política é revista.
- Recomendações de melhoria.
    - Objetivo alcançado, as recomendações de melhoria são tidas em conta no processo de revisão.
- Lições aprendidas e ações resultantes de incidentes disruptivos.
    - Objetivo alcançado, as lições aprendidas com eventos disruptivos são tidas em conta no processo de revisão.
- Novas boas práticas.
    - Objetivo alcançado, as novas boas práticas que são do conhecimento da equipa que procede à revisão são tidas em conta.

O resultado da revisão deve incluir decisões de melhoria continua e possíveis necessidades de alteração ao PCN e devem incluir o seguinte sempre que aplicável:

- Alterações ao âmbito do PCN.
    - Objetivo alcançado, sempre que justificado o âmbito do PCN é revisto.
- Melhorias na eficácia do PCN.
    - Objetivo alcançado, sempre que justificado são introduzidas alterações com vista ao melhoramento da eficácia do PCN.
- Atualização da avaliação de risco, BIA, PCN e procedimentos relacionados.

    - Objetivo alcançado, sempre que justificado os documentos referidos são atualizados.
- Modificação de procedimentos e controlos para responder a eventos internos e externos que possam impactar o PCN incluindo:
    - Objetivo alcançado, sempre que justificado os procedimentos existentes são alterados para responder a evento que possam impactar o PCN.
- Eficácia dos controlos e medidas.
    - Objetivo alcançado, o comité de crise revê a eficácia das medidas.

Toda a documentação deve ser guardada como evidencia e os resultados da revisão devem ser comunicados as partes interessadas, e devem ser tomadas as ações apropriadas para implementar as ações necessárias.

- Objetivo não alcançado, não foram encontradas evidências do processo de revisão além das alterações efetuadas.

Após analise conclui-se que os processos e procedimentos são revistos de forma periódica embora a última atualização tenha sido feita há mais de um ano, no entanto não existem procedimentos de monitorização na organização e não são feitas auditorias internas de forma periódica como referenciado na ISO 22301.

***Compliance* = 54%**

5.4.7. Melhoria

A melhoria contínua pode ser definida como as ações que a organização toma para aumentar a eficácia e eficiência dos processos de forma a alcançar benefícios para a organização.

Sempre que existam não conformidades a organização deve:

- Identificar a não conformidade.
    - Objetivo alcançado parcialmente, as não conformidades são identificadas no entanto não existe um procedimento formal de identificação e tratamento de não conformidades do PCN.
- Reagir à não conformidade.
    - Tomar ações corretivas de modo a eliminar a não conformidade.
        - Objetivo alcançado parcialmente, são tomadas ações para corrigir não conformidades no entanto não existe um procedimento formal de identificação e tratamento de não conformidades do PCN.
    - Lidar com as consequências.
        - Objetivo alcançado, sempre que se registam não conformidades as consequências são tratadas.
- Avaliar a necessidade das ações para eliminar as causas da não conformidade.
    - Rever a não conformidade.

        - Objetivo alcançado parcialmente, não existe um procedimento formal de identificação e tratamento de não conformidades do PCN
    - Determinar as causas da não conformidade.
        - Objetivo alcançado parcialmente, não existe um procedimento formal de identificação e tratamento de não conformidades do PCN.
    - Verificar se existem não conformidades idênticas.
        - Objetivo não alcançado, uma vez que não existe um procedimento formal de identificação e tratamento de não conformidades do PCN não existe um histórico de não conformidades.
    - Avaliar a necessidade de ações corretivas de forma a assegurar que a não conformidade não volta a ocorrer no PCN.
        - Objetivo alcançado parcialmente, não existe um procedimento formal de identificação e tratamento de não conformidades do PCN, no entanto as ações tomadas tem como objetivo que a não conformidade não volte a ocorrer.
    - Determinar e implementar as ações corretivas.
        - Objetivo alcançado parcialmente, não existe um procedimento formal de identificação e tratamento de não conformidades do PCN
    - Rever a eficácia das ações implementadas.
        - Objetivo alcançado parcialmente, não existe um procedimento formal de identificação e tratamento de não conformidades do PCN
    - Alterar o PCN de necessário.
        - Objetivo alcançado, o PCN é alterado sempre que se justifique.
- Implementar as ações necessárias.
    - Objetivo alcançado, as ações necessárias a corrigir não conformidades são efetuadas.
- Rever a eficácia das ações corretivas implementadas.
    - Objetivo alcançado parcialmente, não existe um procedimento formal de identificação e tratamento de não conformidades do PCN

A organização deve guardar todos os documentos como evidencia de:

- Não conformidades e das ações corretivas implementadas.
    - Objetivo não alcançado, não foram encontradas evidências das ações corretivas.
- Resultados das ações corretivas implementadas.
    - Objetivo não alcançado, não foram encontradas evidências dos resultados das ações corretivas.

Após analisar este ponto conclui-se que a organização trata as não conformidades, mas não existe um procedimento de identificação e tratamento de não conformidades.

***Compliance* = 50%**

Após analisar todos os pontos da ISO 22301 verifica-se que apesar de a organização ter construído um PCN efetivo, ainda tem de desenvolver algumas ações para atingir um nível de *compliance* elevado, neste momento situa-se na casa dos 68.3%, sendo que alguns pontos necessitam de mais trabalho como é o caso do ponto de melhoria e do papel da gestão, que estão com nível de *compliance* aproximado de 50%.

***Nível de Compliance com ISO 22301* = 68.3%**

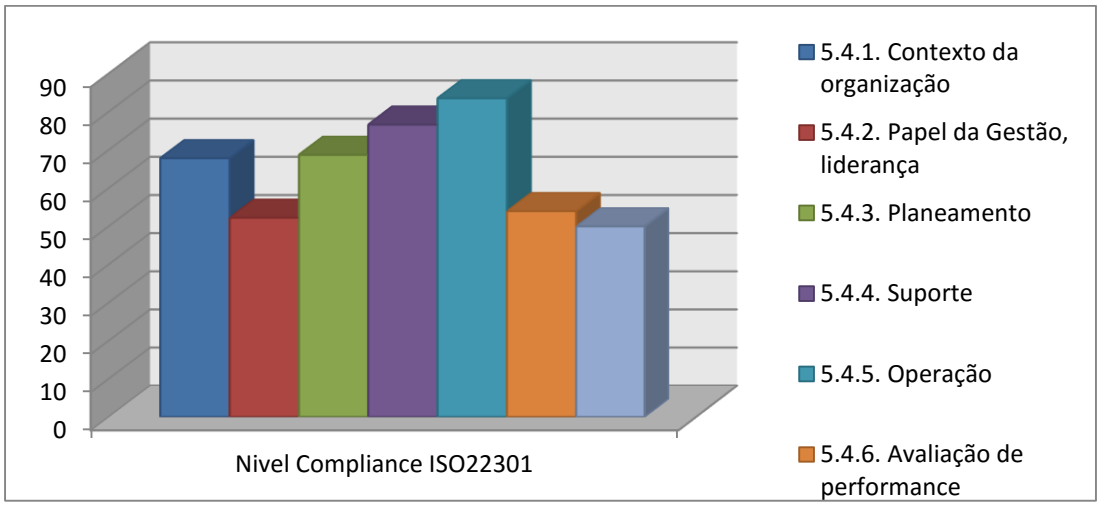


Fig. 32 - **Nível *compliance* ISO 22301**

5.5. Recomendações de melhoria

Neste ponto são sugeridas recomendações de melhoria com vista a alcançar um estado de *compliance* com as boas práticas apuradas, tendo em conta a análise feita no ponto anterior.

As recomendações serão apresentas em forma de tabela por cada ponto analisado, contendo a recomendação, o nível de prioridade (Alta, Media, Baixa) e estimativa de esforço para a realização da iniciativa (Baixo, Medio, Elevado).

5.5.1. Gestão da continuidade do negócio

Recomendação sobre as boas práticas gerais de gestão da continuidade do negócio encontradas na revisão da literatura face à análise efetuada ao PCN da organização.

Nível de *Compliance* atual = 86.6%

Recomendação	Prioridade	Esforço
Devem ser implementados controlos e métricas de forma a medir a capacidade global da organização de resposta a incidentes disruptivos.	Média	Elevado
Deve ser feita uma monitorização da performance e efetividade do PCN.	Média	Medio
Os processos de negócio devem sofrer uma reengenharia com vista à melhoria operacional.	Baixa	Elevado

Tabela 8 - Recomendações - Gestão de continuidade do negócio

5.5.2. Business Impact Analysis (BIA)

Recomendação sobre as boas práticas gerais de *Business Impact Analysis* encontradas na revisão da literatura face à análise efetuada ao PCN da organização.

Nível de *Compliance* atual = 33.3%

Recomendação	Prioridade	Esforço
Adicionar a criticidade de recuperação aos processos e sistemas críticos identificados.	Media	Baixo
Rever o BIA e adicionar a informação em falta respeitante aos equipamentos, aplicações e dados necessários após desastre.	Alta	Médio
Adicionar a prioridade de recuperação aos processos e sistemas críticos identificados.	Alta	Baixo

Tabela 9 - Recomendações – BIA

5.5.3. Análise face à ISO 22301

Recomendações sobre as boas práticas específicas relativas à ISO 22301 encontradas na revisão da literatura face à análise efetuada ao PCN da organização.

Nível de *Compliance* atual = 68.3.6%

5.5.3.1. Contexto da organização

Nível de *Compliance* atual = 67.8%

Recomendação	Prioridade	Esforço
Criação de um documento global de risco contendo a estratégia global de risco assim como a apetência ao risco da organização, os fatores que potenciam o risco e definição do critério de risco tendo em conta apetência ao risco.	Alta	Elevado
Criação de um documento com os requisitos legais e regulatórios da sua atividade no que diz respeito à continuidade da atividade. Este documento que deve sofrer atualizações periódicas.	Alta	Elevado
Criação de um documento formal de definição de âmbito do PCN, incluindo natureza, tamanho e complexidade da organização.	Alta	Médio

Tabela 10 - Recomendações - Contexto da organização

5.5.3.2. Papel da Gestão, liderança

Nível de *Compliance* atual = 52.3%

Recomendação	Prioridade	Esforço
Deverão ser feitas comunicações institucionais periódicas a comunicar reforçar a importância do PCN.	Baixa	Baixo
Deverá ser criado um documento com a política da continuidade da atividade apropriada à atividade pela gestão de topo, contendo critérios de aceitação de risco, uma *framework* de definição de objetivos, enfatizar a melhoria continua, depois de aprovada a politica de continuidade da atividade deverá ser comunicada à organização e revista periodicamente.	Alta	Elevado
Criar um plano de auditoria interna ao PCN.	Alta	Elevado

Tabela 11 - Recomendações - Papel da gestão, liderança

5.5.3.3. Planeamento

Nível de *Compliance* atual = 68.7%

Recomendação	Prioridade	Esforço
Criação de um documento formal de objetivos do PCN.	Média	Baixo

Tabela 12 - Recomendações – Planeamento

5.5.3.4. Suporte

Nível de *Compliance* atual = 76.7%

Recomendação	Prioridade	Esforço
Deve ser efetuado uma gestão efetiva de competências do pessoal que executa as operações do PCN, deve existir um documento de gestão de competências do PCN com o registo das diversas competências e deve ser assegurado que o pessoal tem a competência, educação e formação necessárias, sempre que necessário devem ser tomadas ações de forma a fornecer competências ao pessoal, e deve ser mantido um registo de evidencias de competências.	Média	Elevado
Atualização do procedimento de comunicação de modo a incluir a recção, documentação, e resposta a comunicação externa, assim como incluir a comunicação com as autoridades.	Baixa	Baixo
A organização deve tentar adaptar ou integrar um sistema de alerta de ameaças regional ou nacional.	Média	Baixo

Tabela 13 - Recomendações – Suporte

5.5.3.5. Operação

Nível de *Compliance* atual = 83.6%

Recomendação	Prioridade	Esforço
Criar um registo de controlo de execução de processos.	Baixa	Baixo
Alterar o BIA de modo a incluir a definição do critério e contexto da avaliação do impacto disruptivo.	Média	Baixo
Alterar o BIA para incluir uma análise sistemática e priorização de tratamento do risco e custos.	Média	Baixo
Alterar o BIA de modo a especificar os requisitos para que a informação permaneça confidencial.	Média	Baixo
Deverá ser feita uma análise aos potenciais eventos disruptivos e sinalizar os que requerem intervenção.	Média	Médio
Como indicado noutros pontos deverá se atualizado o procedimento de comunicação de modo a garantir a comunicação documentada com as entidades nacionais ou regionais de avisos de risco, onde deverá estar definida a estrutura de comunicação.	Média	Baixo
Devem ser incluídas medidas de bem-estar dos indivíduos no PCN	Baixa	Baixo
Todos os planos devem referenciar as suas interdependências internas e externas, os requisitos de recursos e fluxo de informação.	Média	Baixo
Após a execução do plano de testes devem ser produzidos relatórios com resultados, recomendações e ações de melhoria.	Alta	Médio
Devem ser respeitados os prazos definidos para a realização dos testes e atualização do PCN (anualmente ou sempre que se justifique).	Alta	Elevado

Tabela 14 - Recomendações – Operação

5.5.3.6. Avaliação de performance

Nível de *Compliance* atual = 54.6%

Recomendação	Prioridade	Esforço
Criação de um procedimento de monitorização para monitorizar em que medida o PCN e os seus objetivos são cumpridos, a conformidade dos seus objetivos com o ISO 22301 e que descreva o que deve ser monitorizado e medido, especificar métodos de monitorização, medida, analise e validação que assegurem resultados validos, quando deve ter lugar a monitorização, especificar um conjunto de métricas apropriadas, como resultado do processo devem ser fornecidos indicadores de performance dos processos e procedimentos.	Alta	Médio
Deve ser guardado um histórico com evidências de deficiências auditável**.**	Baixa	Médio
O resultado do processo de monitorização deve ser guardado de modo a facilitar as ações corretivas.	Médio	Médio
Deve ser estabelecido um plano destinado a estabelecer, implementar e manter um programa de auditorias, incluindo, a frequência, métodos, responsabilidades, requisitos de planeamento e relatório, critérios e âmbito. As auditorias devem ter em conta os resultados de auditorias passadas, o resultado das auditorias devem ser disponibilizados a todos os gestores relevantes para o processo.	Alta	Elevado
Devem ser guardadas evidências auditáveis como prova da implementação do plano de auditoria	Médio	Médio
Sempre que seja encontrada uma não conformidade, deverá ser endereçada.	Alta	Médio
Devem ser guardadas todos os documentos que sejam evidências do tratamento de não conformidades.	Baixa	Baixo
Toda a documentação deve ser guardada, e devem ser tomadas ações apropriadas para implementar as recomendações da auditoria e do plano de monitorização	Alta	Elevado

Tabela 15 - Recomendações - Avaliação de performance

5.5.3.7. Melhoria

Nível de *Compliance* atual = 50%

Recomendação	Prioridade	Esforço
Deve ser criado um procedimento de identificação e tratamento de não conformidades que deve tentar avaliar a necessidade das ações para eliminar as causas da não conformidade.	Alta	Elevado
As não conformidades devem ser identificadas e aplicadas ações corretivas de modo a eliminar as não conformidades	Alta	Médio
Devem ser guardadas evidências do tratamento de não conformidades.	Baixa	Médio

Tabela 16 - Recomendações - Melhoria

Conclusão

6.1. Conclusões

Este trabalho demostrou como uma organização inserida num contexto social e económico difícil como o que se tem vivido em Portugal nos últimos anos, implementou com sucesso um plano de continuidade da atividade.

Para isso foi demostrada a dependência das empresas das TI e o resultado dos períodos de *downtime* num estudo feito a nível global que conclui que os períodos de *downtime* levam em média a uma perda de receita de 36% e ao atraso no desenvolvimento de produtos em cerca de 34% outra das conclusões aponta para uma baixa taxa de empresas com *disaster recovery*, cerca de 51% e mais grave 71% do pessoal de TI não confia na sua capacidade de recuperar informação.

Para avaliar a implementação do PCN na organização foi feita uma revisão da literatura que apurou as melhores práticas de gestão da continuidade de negócio incluindo a norma ISO 22301.

Após o desenvolvimento de uma metodologia de investigação baseada no estudo de caso que foi desenhada no sentido de responder à questão "Como pode ser operacionalizado um plano de continuidade de negócio?" foi avaliado o processo de implementação do PCN.

Apesar de a organização ter implementado um plano de continuidade de negócio eficaz, não cumpre a 100% com as boas práticas apuradas na revisão da literatura.

Para medir a posição da organização face à ISO 22301 foi feita uma avaliação que concluiu que a organização cumpre com cerca de 68.3% das recomendações.

Após a análise dos resultados foi produzido um conjunto de recomendações com vista a elevar nível de *compliance* da organização para perto dos 100%.

Assim este estudo pretende ser uma mais-valia para as empresas em processo de implementação de um plano de continuidade de negócio fornecendo um conjunto de

boas-praticas e um exemplo de implementação num contexto real, assim com as bases de avaliação do processo face às boas práticas apuradas e à norma ISO 22301.

6.2. Limitações

Esta análise foi feita a uma organização específica num contexto social e económico particular. Os resultados e conclusões deste estudo não podem ser generalizados a outras organizações.

6.3. Investigações futuras

Como investigações futuras sugere-se a realização de estudos semelhantes a empresas do mesmo sector de atividade de modo a obter uma base de resultados que permita generalizar conclusões a organizações no mesmo setor de atividade.

Outra sugestão de investigação vai no sentido se encontrar um modelo concetual de avaliação de boas práticas em implementação de planos de continuidade de negócio, não só de *compliance* com a ISO 22301 mas avaliando um conjunto mais vasto de boas práticas.

Bibliografia

Barroso, L. A., Clidaras, J., & Hölzle, U. (2013). *The Datacenter as a Computer An Introduction to the Design of Warehouse-Scale Machines, Second Edition.* University of Wisconsin, Madison: Morgan & Claypool.

BCMInstitute. (2014). *BCMpedia. A Wiki Glossary for Business Continuity Management (BCM) and Disaster Recovery (DR).* Obtido de BCMPedia.org: http://www.bcmpedia.org/wiki/Main_Page

Bell, J. (2014). *Doing Your Research Project: A Guide For First-Time Researchers, 6 Revised edition.* Open University Press.

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The Case Research Strategy in Studies of Information Systems. *MIS Quarter*, (pp. 369 - 386).

Cisco Systems, Inc. (2004). *DESIGNING AND MANAGING HIGH AVAILABILITY IP NETWORKS.* Cisco Systems, Inc.

Cisco Systems, Inc. (2004). *High Availability In Campos Network Deployments RST-2514.*

Creswell, J. W. (2003). *RESEARCH DESIGN Qualitative, Quantitative. and Mixed Methods Approaches.* Sage Publications.

EMC. (2014). *EMC.* Obtido de EMC GLOBAL DATA PROTECTION INDEX: https://www.emc.com/microsites/emc-global-data-protection-index/index.htm

INE. (06 de 11 de 2014). *Sociedade da Informação e do Conhecimento - Inquérito à Utilização de Tecnologias da Informação e da Comunicação nas Empresas.* Obtido de Instituto Nacional de Estatística: http://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=211421031&DESTAQUESmodo=2

International Organization for Standardization - Standards. (22 de 11 de 2014). Obtido de International Organization for Standardization: http://www.iso.org/iso/home/standards.htm

ISO 22301. (15 de 05 de 2012). *International Standard ISO 22301 Societal security - Business continuity management systems - Requirements*. Suiça: ISO.

Janssen, C. (2014). *High Availability (HA)*. Obtido de Techopedia: http://www.techopedia.com/definition/1021/high-availability-ha

Kusnetzky, D. (2011). *Virtualization: A Manager's Guide.* Califórnia, USA: O'Reilly Media, Inc.

Microsoft. (2008). *Microsoft High Availability Overview White Paper.* Microsoft.

Saunders, M. N., Lewis, P., & Thornhill, A. (2009). *Research Methods for Business Students, 5 edition.* Financial Times/ Prentice Hall.

Schmidt, K. (2006). *High Availability and Disaster Recovery Concepts, Design, Implementation.* Berlin: Springe.

Sekaran, U., & Bougie, R. (2013). *Research Methods for Business: A Skill-Building Approach, 6th Edition.* Wiley.

SHARE Inc. (2007). *Business Continuity: The 7-tiers of Disaster Recovery.* Obtido de Recovery Specialties: http://recoveryspecialties.com/7-tiers.html

St-GERMAIN, R. A. (s.d.). ISO 22301 Whitepaper. *Social security Business continuity management systems*. Proffesional Evalution and Certification Board. Obtido de Professional Evaluation and Certification Board: http://pecb.org/iso22301pt/

Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. (2010). *NIST 800-34, Contingency Planning Guide for Federal Information Systems* . National Institute of Standards and Technology. U.S. Department of Commerce.

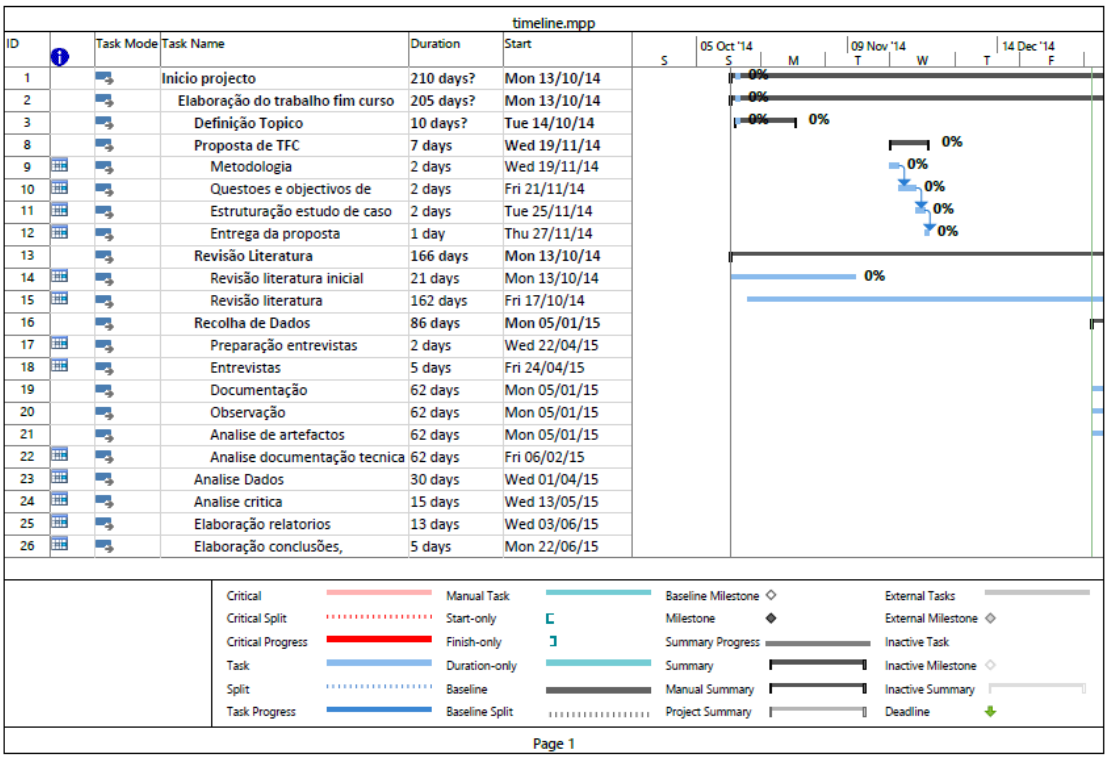
Weygant, P. S. (2001). *Clusters for High Availability.* New Jersey: Hewlett-Packard Company, Prentice Hall, inc.

Whitcher, R. (06 de 2009). *BS 25999 – a framework for resilience and success.* Obtido de Efectus: http://www.efectus.cl/upload_files/documentos/27102009085025-141381139.pdf

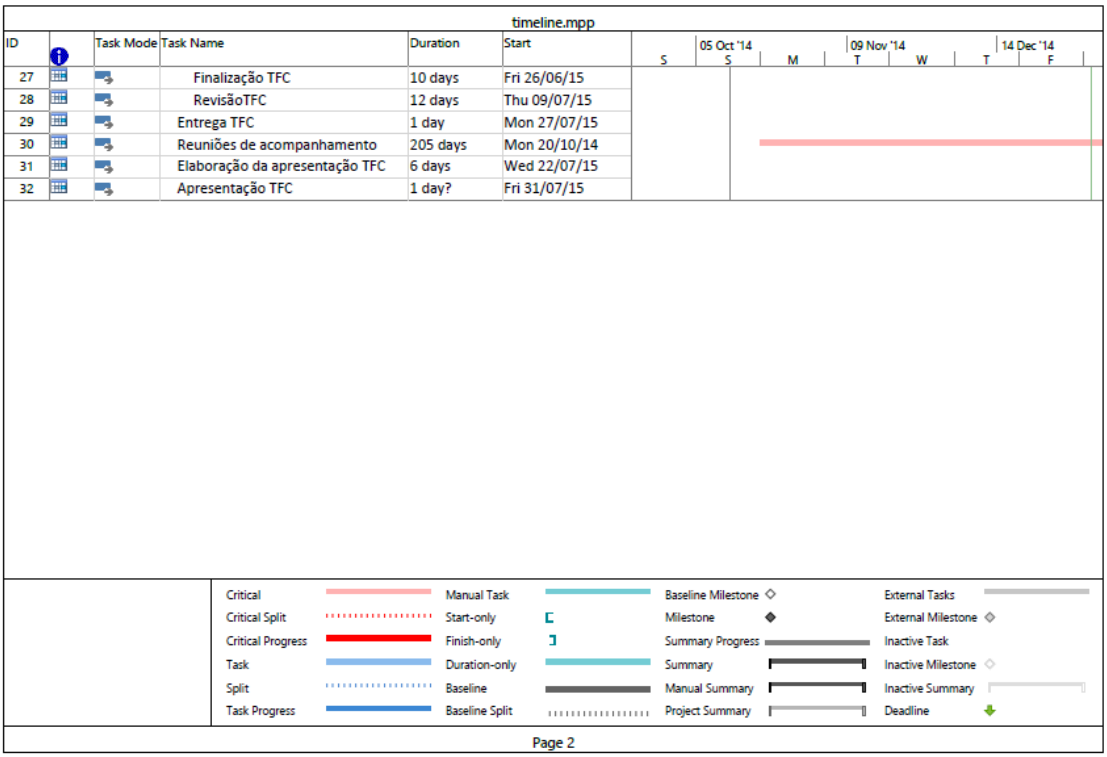
Yin, R. K. (2013). *Case Study Research: Design and Methods* . SAGE Publications, Inc.

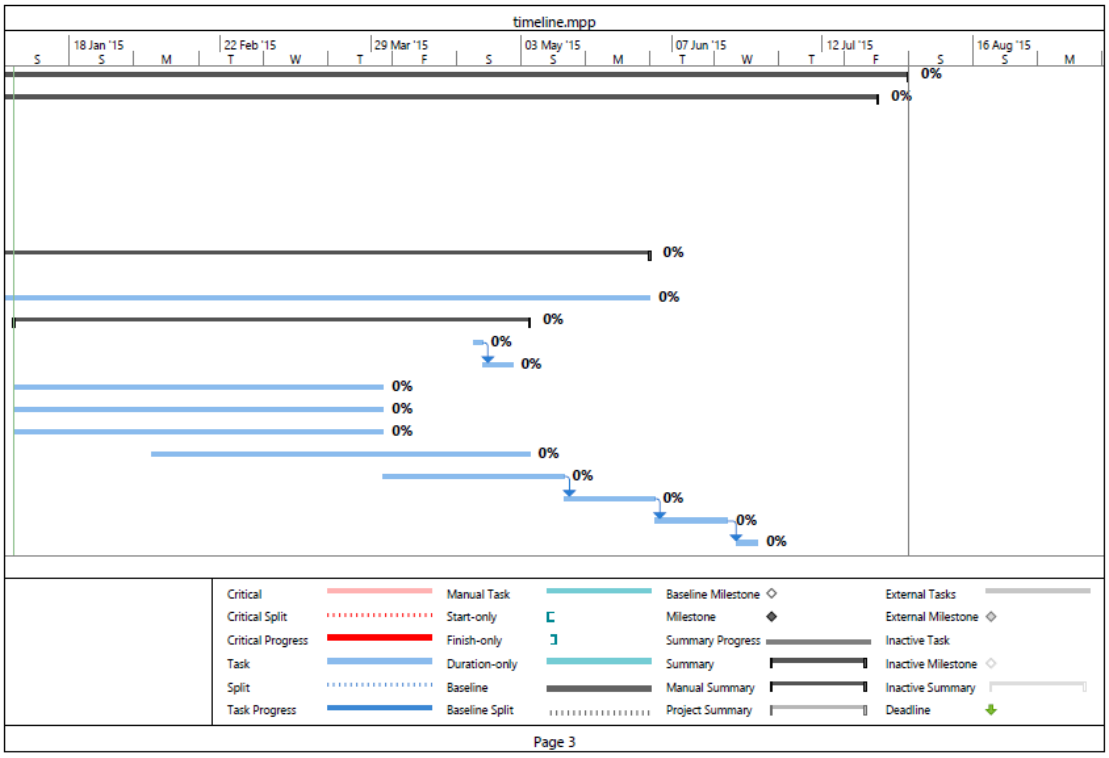
Anexos

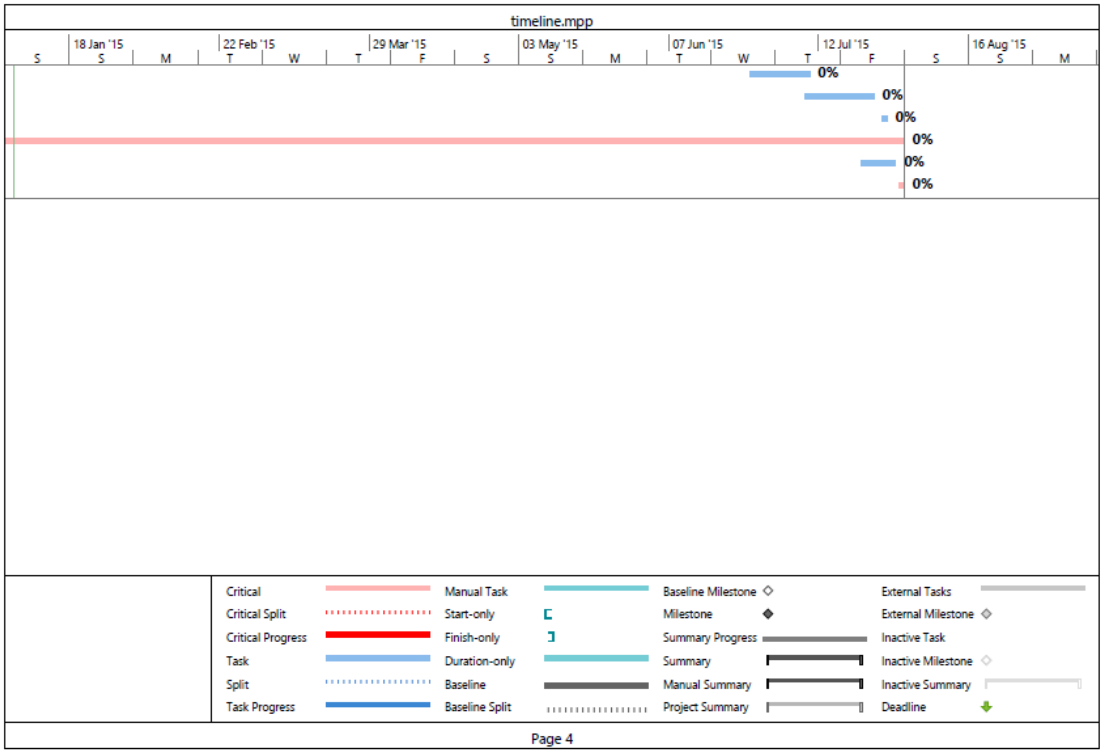
Cronograma



ID	Task Mode	Task Name	Duration	Start
1		Inicio projecto	210 days?	Mon 13/10/14
2		Elaboração do trabalho fim curso	205 days?	Mon 13/10/14
3		Definição Topico	10 days?	Tue 14/10/14
8		Proposta de TFC	7 days	Wed 19/11/14
9		Metodologia	2 days	Wed 19/11/14
10		Questoes e objectivos de	2 days	Fri 21/11/14
11		Estruturação estudo de caso	2 days	Tue 25/11/14
12		Entrega da proposta	1 day	Thu 27/11/14
13		Revisão Literatura	166 days	Mon 13/10/14
14		Revisão literatura inicial	21 days	Mon 13/10/14
15		Revisão literatura	162 days	Fri 17/10/14
16		Recolha de Dados	86 days	Mon 05/01/15
17		Preparação entrevistas	2 days	Wed 22/04/15
18		Entrevistas	5 days	Fri 24/04/15
19		Documentação	62 days	Mon 05/01/15
20		Observação	62 days	Mon 05/01/15
21		Analise de artefactos	62 days	Mon 05/01/15
22		Analise documentação tecnica	62 days	Fri 06/02/15
23		Analise Dados	30 days	Wed 01/04/15
24		Analise critica	15 days	Wed 13/05/15
25		Elaboração relatorios	13 days	Wed 03/06/15
26		Elaboração conclusões,	5 days	Mon 22/06/15


timeline.mpp
ID
Task Mode
Task Name
Duration
Start
05 Oct '14
09 Nov '14
14 Dec '14
27 Finalização TFC 10 days Fri 26/06/15
28 RevisãoTFC 12 days Thu 09/07/15
29 Entrega TFC 1 day Mon 27/07/15
30 Reuniões de acompanhamento 205 days Mon 20/10/14
31 Elaboração da apresentação TFC 6 days Wed 22/07/15
32 Apresentação TFC 1 day? Fri 31/07/15
Critical
Critical Split
Critical Progress
Task
Split
Task Progress
Manual Task
Start-only
Finish-only
Duration-only
Baseline
Baseline Split
Baseline Milestone
Milestone
Summary Progress
Summary
Manual Summary
Project Summary
External Tasks
External Milestone
Inactive Task
Inactive Milestone
Inactive Summary
Deadline
Page 2


timeline.mpp
18 Jan '15
22 Feb '15
29 Mar '15
03 May '15
07 Jun '15
12 Jul '15
16 Aug '15
0%
Critical
Critical Split
Critical Progress
Task
Split
Task Progress
Manual Task
Start-only
Finish-only
Duration-only
Baseline
Baseline Split
Baseline Milestone
Milestone
Summary Progress
Summary
Manual Summary
Project Summary
External Tasks
External Milestone
Inactive Task
Inactive Milestone
Inactive Summary
Deadline
Page 3


timeline.mpp
18 Jan '15
22 Feb '15
29 Mar '15
03 May '15
07 Jun '15
12 Jul '15
16 Aug '15
0%
0%
0%
0%
0%
0%
Critical
Critical Split
Critical Progress
Task
Split
Task Progress
Manual Task
Start-only
Finish-only
Duration-only
Baseline
Baseline Split
Baseline Milestone
Milestone
Summary Progress
Summary
Manual Summary
Project Summary
External Tasks
External Milestone
Inactive Task
Inactive Milestone
Inactive Summary
Deadline
Page 4