ASIST

2019/2020

Disaster Recovery Plan

Carlos Moreira (1161882)
José Santos (1161842)
Marco Pinheiro (1170483)
Pedro Barbosa (1150486)
Pedro Mendes (1161871)

Esta documento tem como objetivo especificar as medidas e estratégias a adoptar em caso de ocorrência de um desastre que resulte na perda total ou parcial das máquinas existentes na empresa My Own Cutlery.

Índice

Introdução

No âmbito da unidade curricular de ASIST foi proposto como Sprint 3 a elaboração de um plano de recuperação de desastres (DRP) para os sistemas considerados críticos da infraestrutura da empresa **My Own Cutlery.** Assim, este documento tem como objetivo identificar e quantificar os riscos bem como documentar os procedimentos para assegurar a continuidade de negócio da referida empresa.

Contexto

A **My Own Cutlery** é uma empresa do sector da indústria que se dedica à produção bem como à comercialização de utensílios de cozinha com principal enfoque em talheres. A produção dos referidos utensílios é efetuada com recurso a máquinas industriais cuja atividade é controlada essencialmente com recurso a sistemas de informação concebidos especificamente para o efeito.

Alguns desses sistemas assumem importância vital na atividade da empresa uma vez que a sua principal fonte de receita advém das vendas *on-line* dos produtos por esta fabricados. Sendo o *e-commerce* o único canal de vendas que a empresa possui, todo o seu sistema informático foi concebido para proporcionar um elevado grau de automatização de processos em função das encomendas recebidas, tais como:

- **Módulo SPA**: webpage da empresa na internet, sendo responsável por fornecer a *user-interface* necessária à realização de encomendas por parte dos clientes; este módulo disponibiliza também outras áreas específicas que são necessárias à configuração dos restantes sistemas da empresa.

- **Módulo de Gestão de Encomendas e Clientes**: sistema no qual é efetuada a gestão de encomendas efetuadas *on-line* bem como os respetivos dados dos clientes;

- **Módulo de Planeamento**: sistema responsável por efetuar a otimização do escalonamento da produção em função das encomendas recebidas e máquinas disponíveis;

- **Módulo de Gestão de Fábrica e Produção**: sistemas nos quais são efetuadas configurações de máquinas de produção bem como dos produtos a fabricar;

- **Módulo de Visualização**: sistema de apoio à configuração e de simulação de produção da fábrica;

Análise de Ameaças e Riscos

Ameaças	Descrição
Falha de hardware	Falhas relacionadas com o hardware dos servidores
Falha de rede / ISP	Problemas / avarias com a LAN e / ou WAN
Falha elétrica	Corte de fornecimento da rede, falhas técnicas
Ataques maliciosos	Ciberataques, sabotagem, vírus
Catástrofe	Incêndios, inundações, explosões, terrorismo
Falhas com Módulos de Software	Erros nos módulos aplicacionais ou em bases de dados

Riscos	Descrição
Perda de dados	Informação planeamento e produção, encomendas, dados de clientes
Roubo de informação	Exposição de dados sensíveis de clientes, informação confidencial de negócio
Perturbação de negócio	Impossibilidade de serem efetuadas encomendas ou de serem fabricados produtos

Análise de Cenários de Impacto

	Impacto				
Probabilidade	**1**	**2**	**3**	**4**	**5**
5	**5 (baixo)**	**10 (médio)**	**15 (alto)**	**20 (muito alto)**	**25 (muito alto)**
4	**4 (baixo)**	**8 (médio)**	**12 (alto)**	**16 (alto)**	**20 (muito alto)**
3	**3 (baixo)**	**6 (médio)**	**9 (médio)**	**12 (alto)**	**15 (alto)**
2	**2 (baixo)**	**4 (baixo)**	**6 (médio)**	**8 (médio)**	**10 (médio)**
1	**1 (baixo)**	**2 (baixo)**	**3 (baixo)**	**4 (baixo)**	**5 (baixo)**

Classificação do risco com base nos níveis de impacto e probabilidade da matriz de risco. O resultado é obtido em função do produto do impacto pela probabilidade:

Cenário	Impacto	Probabilidade	Resultado
Falha de hardware	5	2	*10*
Falha de rede / ISP	4	2	8
Falha elétrica	5	2	10
Ataques maliciosos	5	1	5
Catástrofe	5	1	5
Falha nas aplicações referentes aos módulos Gestão de Planeamento, Gestão de Produção, Gestão de Encomendas, Autenticação ou Website (SPA)	5	2	10
Falha na aplicação referente aos Módulo de Gestão de Fábrica	3	1	3
Falha na aplicação do Módulo de Visualização	2	1	2

Definição RPO e RTO

A tabela abaixo tem como objetivo a representar os tempos máximos de paragem admitidos, para os serviços onde é admissível a perda de dados em caso de desastre, bem como o tempo máximo admitido para a sua reposição dos mesmos, tendo estes valores sido ajustados em função do resultado da análise de risco.

Serviços Críticos	RPO	RTO
Gestão de Fábrica (Aplicação + Base de dados)	90 min	180 min
Gestão de Produção (Aplicação + Base de dados)	30 min	60 min
Gestão de Encomendas (Aplicação)	30 min	60 min
Módulo de Gestão de Planeamento (Aplicação + Base de dados)	60 min	120 min
Website (SPA)	30 min	480 min

Serviços Não Críticos	RPO	RTO
Módulo de Visualização	360 min	120 min

Para que a continuidade do negócio da empresa fique totalmente assegurada, os tempos de RPO e RTO definidos para os sistemas críticos tendem a ser bastante reduzidos enquadrando-se numa classificação **Tier 7**. Ainda que tal solução assuma um custo acrescido para a empresa a nível de recursos necessário, é crucial assegurar que, em caso de desastre, a atividade da empresa é retomada dentro de prazos efetivamente curtos. Devido ao elevado número de encomendas registados a cada hora, o não cumprimento dos prazos estabelecidos poderá comprometer seriamente a continuidade de negócio da empesa.

Estratégia de Backup

O *backup* das máquinas onde se encontram os sistemas da empresa são efetuadas através de geração de imagens e ocorre segundo o seguinte agendamento:

- **Módulos de Produção, Planeamento, Gestão de Fábrica:** efetuado *backup* a cada 2 horas durante o período de atividade da fábrica e uma cópia completa durante o período de inatividade noturno;

- **Módulos de Gestão de Encomendas/Clientes e Módulo SPA:** efetuado de hora a hora, 24 horas por dia;

- **Restantes módulos:** efetuado um *backup* por dia durante o período o período de inatividade noturno;

Uma vez criada a imagem inicial, são criadas imagens incrementais que adicionam as alterações (diferencial de informação). Por forma a salvaguardar toda a informação considerada crucial à continuidade de negócio da empresa, optou-se pela estratégia de *backup* 3-2-1 que consiste em efetuar **três** cópias de cada imagem efetuada. Estas ficam guardas em **dois** dispositivos *NAS* distintos localizados nas instalações da empresa, numa sala fechada e climatizada, à prova de fogo e inundações. Por último é efetuada **uma** terceira cópia que é guardada num servidor *FTP off-site* de uma empresa externa com a qual a **My Own Cutlery** tem contrato.

Semanalmente é também efetuado um *backup* completo de todos os sistemas, tendo este início no Domingo pelas 23:00h.

As cópias mensais de informação serão mantidas durante um período de 10 anos.

Nesta estratégia encontra-se também contemplado um acesso à *internet* com redundância de *link backup*, caso ocorra queda de sinal com um deles.

Plano de recuperação

Cenário	Falha de hardware
Sistemas	Gestão de Planeamento, Gestão de Produção, Gestão de Encomendas, Autenticação ou Website (SPA)
Plano de ação	● Identificar ocorrência e coordenar plano de ação com o responsável interno/externo ● Substituir o hardware em causa, procedendo, caso necessário, ao aluguer de material ● Obter uma cópia da imagem de backup mais recente ● Proceder à recuperação do sistema ● Efetuar login da aplicação via SPA ● Garantir que os dados estão de acordo com o último backup realizado

Cenário	Falha de rede / ISP
Sistemas	Gestão de Encomendas, Autenticação ou Website (SPA)
Plano de ação	● Identificar ocorrência e coordenar plano de ação com o responsável interno/externo ● Promover contacto com o ISP contratado para efeitos de *backup* por forma a repor a ligação ● Efetuar testes de acesso à SPA através de uma rede externa à empresa

Cenário	Falha elétrica
Sistemas	Gestão de Planeamento, Gestão de Produção, Gestão de Encomendas, Autenticação ou Website (SPA)
Plano de ação	● Identificar ocorrência e coordenar plano de ação com o responsável interno/externo ● Contactar o responsável pelos serviços de infraestrutura da empresa no sentido ativar a monitorização dos sistemas de UPS e promover o contacto com as entidades necessárias com vista à reposição do abastecimento de energia.

Cenário	Falha de software
Sistemas	Gestão de Planeamento, Gestão de Produção, Gestão de Encomendas, Autenticação ou Website (SPA)
Plano de ação	● Identificar ocorrência e coordenar plano de ação com o responsável interno do respetivo módulo ● Em caso de deteção de bug crítico, comunicar incidente de imediato com classificação *blocker* ● Promover as medidas temporárias necessária e adequadas ao tipo de problema que garantam a continuidade do negócio/produção.

Cenário	Catástrofe – Incêndios, inundações, explosões, ataques terroristas
Sistemas	Gestão de Planeamento, Gestão de Produção, Gestão de Encomendas, Autenticação ou Website (SPA)
Plano de ação	● Coordenar plano de ação com o responsável interno do respetivo módulo ● Promover contacto com o provedor de serviços de *cloud* no sentido proceder ao aluguer temporário de servidores virtuais ● Proceder reinstalação dos módulos Gestão de Encomendas, Autenticação ou Website (SPA) a partir da imagem de *backup* mais recentes ● No caso de ocorrência de catástrofe que não impossibilite a continuidade da produção fabril, devem ser também garantidos servidores virtuais que possibilitem a instalação dos módulos de Gestão de Planeamento e Gestão de Produção ● Determinar e efetuar os procedimentos técnicos necessários ao redireccionamento das comunicações com o ambiente de fábrica (máquinas de produção).

Cenário	Ataques maliciosos
Sistemas	Gestão de Planeamento, Gestão de Produção, Gestão de Encomendas, Autenticação ou Website (SPA)
Plano de ação	● Coordenar plano de ação com o responsável interno do respetivo módulo ● Identificação do problema bem como a sua gravidade ● Promover medidas convenientes à contenção do ataque bem como a minimização de danos ● No caso de impossibilidade de autonomia na resolução do problema, promover contactos com entidades externas especializadas no sentido de mitigar o ataque

	• Obter uma cópia da imagem de backup mais recente • Proceder à recuperação do sistema • Efetuar login da aplicação via SPA • Garantir que os dados estão de acordo com o último backup realizado • Promover as ações necessárias por forma a rever as práticas atuais da empresa relativamente à segurança informática com vista a prevenir ataques futuros.

Plano de testes

Para que um plano descrito seja fiável é necessário que seja testado. A forma de o testar passa por simular uma situação semelhante à originada por um desastre que origine perda de informação.

Teste de simulação simples: A serem efetuados mensalmente e não devem impactar na normal atividade da empresa. Estes testes devem consistir na auditoria periódica da informação guardada em *backup*, como por exemplo, verificar se o *backup* do dia anterior reflete exatamente as transações efetuadas.

Teste de simulação integrais: Anualmente serão realizados testes que simulem o pior cenário possível, como por exemplo perda de comunicações, ativação dos meios de recuperação dos *backups*, etc. Este tipo de testes deverá ser programado por forma a que ocorra fora do horário de funcionamento da fábrica e deverá também contemplar testes de resistência/potência aos sistemas de UPS (*Uninterruptible Power Supply*) da empresa.

Papéis e Responsabilidades

Os seguintes funcionários da empresa assumem a responsabilidade de restaurar ou reparar os serviços IT, quando o plano de recuperação de desastre for ativado.

Contactos Internos

Nome	Contacto	Encarregue de
Marco Pinheiro	1170483@isep.ipp.pt	Gestão de Fábrica
Pedro Mendes	1161871@isep.ipp.pt	Gestão de Encomendas e Produção
Pedro Barbosa	1150486@isep.ipp.pt	Gestão de Planeamento
Carlos Moreira	1161882@isep.ipp.pt	Spa e Autenticação
José Santos	1161842@isep.ipp.pt	Visualização

Contactos Externos

Nome	Organização	Contacto	Recuperação de
Jorge P. Leite	ISEP	jpl@isep.ipp.pt	Dados *backup* guardados em *cloud*