DEPARTAMENTO DE ENGENHARIA INFORMÁTICA

Sprint3

Grupo 46
José Mota (1161263)
Pedro Real (1170689)
João Flores (1171409)
Patrick Timas (1171352)

Dezembro, 2019

isep Instituto Superior de Engenharia do Porto

Índice

Introdução

Este relatório foi realizado com objetivo de implementar um plano de recuperação em caso de desastres.

Este plano suporta a parte fabril tal como o MDP e MDF, a parte de gestão de clientes e respetivas encomendas e a planeamento.

O plano tem em consideração fatores internos e externos, tais como erros por parte humana, problemas de internet, incêndios, entre outros.

Tendo em consideração estes fatores, é necessário um mecanismo de rotina que garanta a possibilidade de regredir para uma certa versão caso necessário. A nosso objetivo com o plano é garantir que o sistema está coerente, os dados são concisos e que o serviço e negócio estão operacionais.

Metodologia de trabalho

Este projeto foi realizado por todos os elementos do grupo, tendo todos ponderado realizado as tarefas pedidas e estipuladas.

Passamos à divisão de tarefas por todos os elementos, tal ajuda a rentabilizar o tempo, o grupo continuou unido e a ajudar sempre que possível. A nossa divisão permitiu que todos os elementos possam trabalhar sem atrapalhar os colegas.

Política

A empresa tem o encargo de descrever o plano compreensivo para qualquer trabalhador independente do cargo ocupado.

Todos os elementos das equipas devem ter conhecimento do plano e saber o que deve fazer para o seu cargo.

O plano deve cobrir todos dados, infraestruturas e sistemas de acordo com o que é necessário para a empresa poder continuar no ativo caso algo ponha em causa a sua sustentabilidade.

O plano deve ser testado frequentemente, garantindo que está disponível a qualquer altura, principalmente em casos de emergência.

Caso algo seja necessário alterar no plano deve ser prioridade do encarregado realizar as alterações para este estar operacional.

Objetivos

O principal objetivo do plano de recuperação é de desenvolver, testar e documentar um conjunto de ações e medidas no caso de algum problema que possa por em causa a infraestrutura, sistema ou propriedade da empresa.

A documentação deve ser de fácil compreensão, de rápido e acessível acesso, deve ter em consideração todo o pessoal que possa ser afetado por alguma falha, sendo estes os trabalhadores, clientes e possíveis colaboradores.

DRP

O Disaster Recovery Plan usa dos conceitos como o RPO (objetivo de ponto recuperação), RTO (objetivo de tempo de recuperação), deve ser implementado um “mirror” de modo a caso ocorram desastres que colocem em causa o negócio, a réplica possa ser utlizada, garantindo a continuidade da empresa.

Estrutura Informática

A rede de abastecimento de elétricidade deve ser redundante, com acesso a geradores em caso de falha externa haver um plano alternativo.

A planificação do uso de servidores acenta no uso de vários servidores tanto “on-site” como “off-site”, implementação da tecnologia SAN rede de área de armazenamento.

Plano de Continuidade Negócio (BCP)

Dada a estrutura da empresa e a área onde pretende chegar é necessário ter um plano de continuidade bem organizado e definido, para o caso de existir algum problema/falha ser possível resolver sem colocar em causa a credibilidade e futuro da empresa.

Consiste num conjunto de estratégias, planos e comportamentos de prevenção, para assegurar que os danos sejam minimizados. Os sistemas informáticos e elétricos são sistemas bastante sensíveis, por isso devem ser implementadas medidas que caso haja algum problema seja possível implementar outro modo de funcionamento. Devem ser implementadas soluções para desastres/falhas com maior probabilidade de acontecer. Existe um certificado do BCP, com normas específicas.

É necessário compreender os SPOF, single point failure, compreendendo-se por isto os pontos nos quais o sistema está mais vulnerável, onde pode levar a ruína do sistema. Devemos procurar minimizar os SPOF nas implementações que definimos no BCP.

O BCP consiste 4 fases, na qual a segunda pode ser subdividida, sendo elas análise, desenvolvimento solução, testes e implementação.

Análise – Avaliar/Analisar projeto, necessidades e recursos.

Desenvolvimento – Soluções mais rentáveis, custo tendo em consideração soluções mais viáveis.

Testes – Testar os procedimentos implementados, provocar falhas nos vários sistemas que foram preparados.

Implementação – Reformular o plano, testes e necessidades conforme resultados obtidos nos testes. Procurar proteger os sistemas nas falhas obtidas nos testes.

SPOF

Na análise devem ter em consideração os SPOF’s, devendo identificar e fazer previsões de modo a evitar a ruína do sistema por simples pontos.

Plano de Contingência

A nossa empresa depende de muitos fatores por isso temos em consideração várias alternativas para cada caso.

Falha na Amazon:

Mais um servidor em cluster;

Alternativa ao servidor em uso;

Existência de plano de backup para os dados.

Falha no Azure:

Mais um servidor em cluster;

Alternativa ao servidor em uso.

Internet:

Empresa fornecedora tem alternativas instantânea em caso de falha;

Outra empresa fornecedora.

Servidor da Empresa:

Outro servidor disponível;

Existência de plano de backup para os dados.

Eletricidade:

Geradores;

Outra empresa fornecedora;

Empresa fornecedora tem alternativas instantânea em caso de falha.

Plano de Backup dados

Devem existem vários backups, vários locais onde os guardar e de preferência em diferentes alturas.

Em relação aos vários backups devem ser realizados de modo integral e incremental. Sendo que os integrais devem ser realizados quando com mais espaçamento entre si e quando os servidores estiverem com menos carga, uma boa altura para os realizar seria de semana a semana ou com uma semana de intervalo, por exemplo ao domingo depois da hora de maior tráfico. Este tipo de backup também deve ser realizado quando vão ser implementados

atualizações ou haja conhecimento de atualizações nos serviços usados. Os incrementais devem ser feitos com mais frequência, intervalo de tempo de horas.

Os locais onde guardamos os backups devem ser distintos uns dos outros, garantindo assim se um dos locais ficar comprometendo os outros, em princípio continuam prontos a utilizar. Bons locais para guardar as cópias seriam servidores remotos, servidores locais e vários discos locais.

O backup integral só existe necessidade de preservar o que foi realizado em último e o que estamos a realizar, podendo apagar os outros que vão acabar por ocupar muito espaço.

Devemos também nos certificar que os dados que estamos a guardar são guardados em locais que estão operacionais e que podemos obter esses registos sempre que necessário e que os dados que guardamos não ficam corrompidos, devendo de tempo a tempo, por exemplo de mês a mês, obter os dados dos vários locais e verificar se não estão desatualizados ou corrompidos.

Plano Segurança

A segurança deve ser assegurada para todos os envolvidos em atividades, deve existir confiança de parte a parte. Deve assegurar os vários princípios de confidencialidade, integridade, disponibilidade, autenticidade e legalidade. Esta segurança está restrita somente a computadores, mas sim a todo os locais onde possa por em causa os dados.

Para garantir a segurança, vários fatores devem estar de acordo com os princípios acima descritos.

Acesso físico:

Cada trabalhador deve ter acesso aos serviços da empresa através das credências geradas, clientes e outros devem requisitar as credências;

Apenas pessoal autorizado ao aceder ao servidor o pode fazer;

Acesso lógico:

Novamente os trabalhadores devem usar as suas credências para ter acesso, outros devem requisitar as credências;

O utilizador só tem acesso aos seus dados sensíveis e encomendas realizadas;

Conforme as suas funções, o trabalhador tem diferentes acessos, trabalhadores da fábrica só têm acesso ao que é necessário ao seu trabalho, os da produção só tem ao que é necessário ao produto, trabalhadores na área do cliente já tem acesso a certos dados de clientes.

O administrador de sistema deve ter acesso a tudo, desde os backups à área pessoal.

Autenticação e autorização:

A autentificação nos servidores só pode ser realizada por pessoal autorizado.

Para aceder à fábrica é necessário usar as credências.

Proteção de acesso:

Restringir os Ip's de acesso, apenas adicionar Ip's conhecidos tais como os da empresa que os trabalhadores necessitem para realizar o seu trabalho, podendo por exemplo pedir para adicionar o de casa de modo a trabalharem a partir de casa.

Restringir sites que possam por em causa os sistemas, tentando evitar possíveis ataques com scripts e malwares.

Promover boas práticas que diminuam probabilidade de ataques do tipo "injection", problemas de encriptação, etc.

Equipamentos

Sem os equipamentos operacionais a empresa fica parada, por isso devemos apresentar soluções para esta não parar inesperadamente devido a uma falha. Devemos garantir boas condições e práticas para preservar os equipamentos, desde os servidores as máquinas.

Para os equipamentos:

Vistorias devem ser realizadas frequentemente;

Garantir que a rede está bem instalada.

Para os servidores:

Vistorias, verificando a performance, gastos energéticos e se não há perdas de dados.

Bom ambiente para servidores, temperatura por volta de 22ºC, dependendo dos servidores, humidade, poeiras e vibrações no mínimo, se possível zero.

Sistema elétrica bem instalada, não podem existir picos, estes podem comprometer os dados.

A rede, tanto elétrica como de internet deve ser redundante, caso haja um problema num lado, o outro garante que o sistema continua operacional.

Para a internet:

Este deve ser redundante para o caso de um problema num lado, o sistema pode continuar operacional.

Deve garantir que todos os trabalhadores têm acesso e de qualidade.

Geral:

Deve ser um local de trabalho agradável, com boas condições, logo têm de existir normas de segurança contra incêndios, deteção e extintores e segurança dos trabalhadores.

Análise Risco

Na análise de risco numa estrutura informática deve se abordar problemas em elementos que possam por em causa a continuidade do sistema. Com esta análise pretende-se compreender o impacto e probabilidade de acontecer um certo evento, o impacto e probabilidade vai ser considerados numa escala de 1(muito baixo) até 5(muito alto).

Foram consideradas vários riscos, cada um foi avaliado em termos de impacto, probabilidade, impacto geral na empresa, custos, dependências, recuperação e riscos.

Desastre	*RPO(H)*	*RTO(H)*	*Probabilidade*1*	*Impacto*2*	*Prioridade*3*
Incêndio	*20*	*6*	*3*	*4*	*12*
Extremo Calor	*8*	*2*	*3*	*2*	*6*
Cibercrime	*5*	*2*	*2*	*5*	*10*
Sabotagem Interna	*6*	*1*	*1*	*5*	*5*
Terrorismo	*1*	*1*	*1*	*5*	*5*
Perda conexões	*8*	*4*	*4*	*4*	*16*
Falha elétrica	*10*	*3*	*5*	*4*	*20*
Outro desastre	*12*	*5*	*3*	*4*	*12*

*1Probabilidade (1 muito baixo, 5 muito alto)

*2Impacto (1 muito baixo, 5 muito alto)

*3Prioridade (1 muito baixo, 25 muito alto)

Considerando os trabalhadores, localização e respetivo clima apuramos que os desastre que poderão ativar o plano de recuperação são os incêndios, extremo calor, perda de conexões, falhar elétrica e outro desastre que poderá não ter sido considerado.

Tendo em conta o desastre foi atribuído um RPO, RTO, probabilidade, impacto e prioridade.

RPO: Intervalo de tempo, desde a descoberta do problema/falha até ao momento onde o intervalo excede a tolerância sem que o negócio possa ser severamente afetado, chamado de “Bussiness Continuity Plan’s”

RTO: Previsão de tempo até o serviço estar restaurado tal como estava antes da falha.

Probabilidade: Métrica com escala de 1 a 5, muito baixo até muito alto, correspondente à chance de acontecer o desastre.

Impacto: Métrica com escala de 1 a 5, corresponde à consequência/efeito que teria para a continuidade da empresa continuar a prestar os seus serviços com qualidade expectada, tendo como comparação a qualidade antes do incidente.

Prioridade: Métrica com escala de 1 a 25, corresponde à multiplicação de probabilidade com o impacto, indica o leitor da escala que quanto mais alto o valor mais rápido tem de ser resolvido o problema/falha.

Incêndio

Analise impacto no negócio

- Empresa pode não continuar a trabalhar por tempo indeterminado;
- Originar grandes despesas;
- Originar perdas parciais/totais de bens matérias;
- Queimaduras;
- Perda de comunicações.

Classificação

- Crítico

Dependências

- Com as várias funções pode parar tudo, desde a produção até à gestão de clientes.

Custos

- Custos muitos elevados, bens materiais que possam necessitar de reparação ou substituição.
- Trabalhadores podem não conseguir trabalhar originando mais custos.

Ameaças

- Acidente:
  - Impacto – 3
  - Probabilidade – 2
- Ataque:
  - Impacto – 4
  - Probabilidade – 3

Riscos

- Perda de comunicações:
  - Impacto – 3
  - Probabilidade – 3
- Perda de confiança:
  - Impacto – 4
  - Probabilidade – 4
- Perda de serviços:
  - Impacto – 5

    - Probabilidade – 5
- Destruição de propriedade:
    - Impacto – 4
    - Probabilidade – 4

Prevenção

- Verificações regulares;
- Detetores de fumo e meios de combate;

Recuperação

- Obter novamente a informação guardada.

Extremo Calor

Analise impacto no negócio

- Os servidores podem ser afetados na eficiência, devido a não estarem em condições ideais;
- Originar danificações parciais de bens matérias;
- Lentidão/atrasos por parte dos trabalhadores nos serviços prestados;
- Ambiente de trabalho não favorável para o sistema;

Classificação

- Normal

Dependências

- Com as várias funções podem parar ou ter uma marcha mais lenta do que o habitual, desde a produção até à gestão de clientes.

Custos

- Custos nos bens materiais que possam necessitar de reparação ou substituição devido ao sobreaquecimento do mesmo.
- Trabalhadores podem não conseguir trabalhar originando mais custos.
- Trabalhadores necessitam de suporte/condições para o trabalhar.

Riscos

- Perda/atraso dos serviços:

    - Impacto – 3
    - Probabilidade – 2

- Sobreaquecimento dos equipamentos:
    - Impacto – 3
    - Probabilidade – 2

Prevenção

- Verificações regulares dos equipamentos;
- Disponibilizar água potável aos trabalhadores - pelo menos 3 litros de água por dia e por trabalhador.
- Garantir ventilação e climatização nos edifícios;
- Garantir ventilação eficaz nos locais com maior risco de poluição;
- Utilizar termómetros para monitorização da temperatura ambiente.

Recuperação

- Estabilizar a temperatura do ambiente do trabalho e dos servidores.

Cibercrime

Analise impacto no negócio

- Empresa pode não continuar a trabalhar por tempo indeterminado;
- Originar grandes despesas;
- Perda de comunicações;
- Perda de confiança por parte dos clientes;
- Furto de informações;
- Exposição de informações confidenciais(protótipos).

Classificação

- Crítico

Dependências

- Com as várias funções pode parar tudo, desde a produção até à gestão de clientes.

Custos

- Custos muitos elevados, bens materiais que possam necessitar mais investimentos em segurança.
- Trabalhadores podem não conseguir trabalhar originando mais custos.
- Perda de clientes.

Ameaças

- Ataque:
  - Impacto – 5
  - Probabilidade – 2

Riscos

- Perda de informações:
  - Impacto – 3
  - Probabilidade – 4
- Perda de confiança:
  - Impacto – 4
  - Probabilidade – 5
- Perda de serviços:
  - Impacto – 5
  - Probabilidade – 5

Prevenção

- Verificações regulares nos sistemas de segurança(firewall);
- Redundância nos dados empresarias e pessoais.

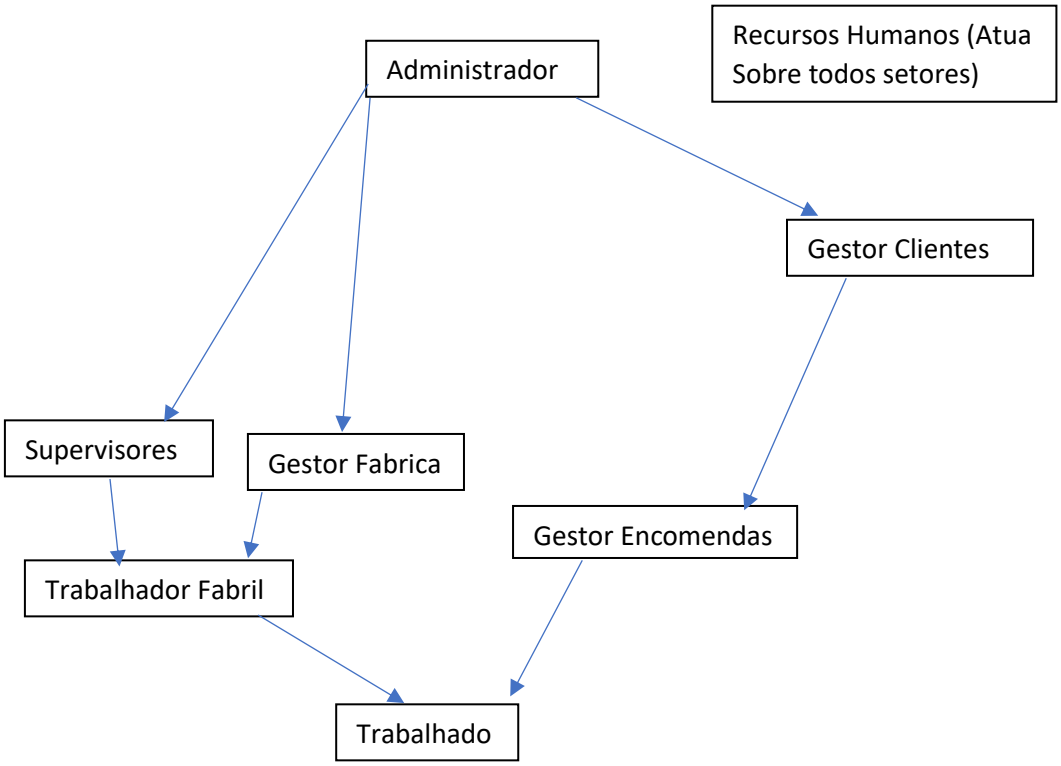
Recuperação

- Obter novamente a informação furtadas.

Equipa

Todos os trabalhadores devem são contratados para certas funções, tendo em conta os seus cargos cada um deve estar preparado e ter em conta as suas responsabilidades. Um trabalhador que esteja sem vontade, formação e desatento tende a provocar mais problemas e mais provável cometer erros.

Deve haver uma hierarquia entre funcionários, facilitando assim comunicações, resolução de problemas, etc.



Inventario

Todas as empresas necessitam de ter idenficado os equipamentos, seus valores e data de compras. Num estado ideial também se guardava o estado do material.

Productos	Preço
Router TL-WR841N N300	18,99 €
Router TL-WR940N N450	29,99 €
Router RT-AC5300	259,90 €
Router Xiaomi 4A	27,36 €
Router Archer C5400X	375,90 €
Secretária Bergamo	24,99 €
Secretaria Expand	49,99 €
Cadeira Opus	29,99 €
Cabo de Rede Ethernet RJ45 30M	9,21 €
Cabo MITSAI (1m - HDMI)	7,99 €
Armário rack mural 19" 6U	104,61 €
Servidor P06455-B21	9 486,99 €
Servidor 877621-421	2 181,47 €
Rato Logitech 603	40,65 €
Beelink T4 Desktop Mini PC	109,20 €
Impressora Laser Xerox B215	166,05 €
Portátil HP 15-DA0036NP	399,97 €
Custo Total	13 323,25 €

Conclusão

Em suma, as empresas devem ter sempre o plano atualizado, deve ser eficas e percetivel.

Uma empresa que esteja com um plano pouco eficaz, fica mais fragilizada e não consegue recuperar com tanta facilidade com uma empresa preparada.

Na generalidade, o grupo trabalhou bem, e os principais objetivos foram cumpridos e resolvidas tendo por base os conhecimentos adquiridos durante as aulas e através de diversos tutoriais presentes na internet.

Referências

https://pt.wikipedia.org/wiki/Recuperação_de_desastres

http://www.computerbusinessresearch.com/Home/enterprise-architecture/disaster-recovery

https://emergencymanagement.georgetown.edu/

https://www-356.ibm.com/partnerworld/gsd/search.do

https://getti.net.br/plano-de-recuperacao-de-desastres-dicas-para-um-plano-efetivo/

https://www.disasterrecoveryplantemplate.org/difference-between-drp-and-bcp/

https://pt.wikipedia.org/wiki/Planejamento_de_continuidade_de_negócios

https://en.wikipedia.org/wiki/Single_point_of_failure