Plano de Recuperação de Desastre

ASIST –Sprint C

Turma 3G _ Grupo 38
1190718 – João Beires
1190782 – José Soares
1190811 – Lourenço Melo
1191419 – José Maia

Data: 08/01/2023

Índice

Contactos de emergência

Nome	Função	Email	Telemóvel
José Maia	**Administrador**	1191419@isep.ipp.pt	**933 556 264**
José Soares	**Técnico do sistema de monitorização**	1190782@isep.ipp.pt	**911 108 710**
João Beires	**Chefe do comitê executivo de DRP**	1190718@isep.ipp.pt	**912 339 693**
Lourenço Melo	**Chefe da equipa de Resposta a Incidentes**	1190811@isep.ipp.pt	**918 523 150**

Propósito

As organizações não podem evitar desastres, porém podem desenvolver ações para minimizar seus efeitos. O objetivo de um DRP (Plano de Recuperação de Desastre) é reduzir o downtime e a perda de dados da organização no caso de desastres criados por fatores fora do controlo da empresa (incêndio, inundação, falha de energia).

Pré-planeamento e comitê executivo de DRP

Primeiramente, foi criado um comitê executivo que tem como objetivo planear e atualizar o DRP e orientar e fornecer apoio às equipas de projetos em assuntos referentes ao DRP. Os gerentes de projeto devem trabalhar com o comitê para finalizar o planeamento detalhado e desenvolver entrevistas para avaliar a segurança e elaborar a análise de impacto no negócio.

Existe um programa para a educação da gerência e das pessoas chave do projeto em relação ao DRP e aos procedimentos nele referidos.

Análise dos sistemas informáticos e avaliação da vulnerabilidade

São feitos backups noutra plataforma para a salvaguarda dos dados gerais. Estes backups serão feitos de 4 em 4 horas para um "*site backup*" que se localiza a mais de 10 km de distância e com acesso controlado.

O único acesso ao exterior é através da internet e, para isso, existem firewalls para evitar acessos não autorizados.

Existe um gerador de energia que consegue alimentar os servidores e a base de dados durante um certo espaço de tempo se houver uma falha de energia.

Sistemas e equipamentos informáticos usados:

- Luzes;
- Computadores fixos, monitores, teclados e ratos usados diariamente pelos trabalhadores;
- Computadores portáteis tanto pessoais como da empresa utilizados pelos colaboradores;
- Servidores da empresa;
- Sistema de videovigilância, que se encontra ligado durante a totalidade do dia. Em horas trabalho conectado ao centro de vigia do segurança do edifício;
- Sensores e alarmes de incêndio;
- Termómetros e sensores de humidade nas salas dos servidores e base de dados, para manter estas nas condições ideais ao funcionamento dos aparelhos;
- Alarmes anti roubo;
- Sistema de picagem do ponto e de autorização para entrar nas instalações, que usa o cartão de trabalhador para proceder a estas autenticações;
- Base de dados onde se armazena as informações necessárias ao negócio;

Avaliação da vulnerabilidade:

A Matriz de Riscos ou Matriz de Probabilidade permite de forma visual identificar quais são os riscos que devem receber mais atenção.

Figura 1 - Matriz de Risco

Ameaça	Probabilidade	Consequência	Risco
Falha energética	3	1	Baixo - 3
Sismo	1	3	Baixo - 3
Avaria num dos componentes informáticos	2	2	Médio - 4
Incêndio no data center	1	4	Médio - 4
Perda de informações essenciais	3	2	Médio - 6
Incêndio	3	3	Séria - 9
Ataques DDoS e DoS	3	3	Séria - 9
Falha da VM do DEI	4	2	Séria - 8
Falha nos servidores	3	3	Séria - 9
Sobrecarga do sistema	4	3	Alta - 12

Monitorização de falhas

Foi concebido um sistema automatizado de monitorização de falhas que se encontra sempre ligado, e executa testes e verifica as condições dos componentes necessários ao negócio. Para isso, também foi necessário formar um técnico com capacidade de verificar o bom funcionamento deste sistema e atualizá-lo se necessário (técnico do sistema de monitorização).

Alguns destes testes são:

- Verificação da temperatura e da humidade ideal nas salas dos servidores e base de dados;
- Bom funcionamento dos servidores, testando a velocidade de resposta dos mesmos.
- Testa o bom funcionamento e rapidez da internet nas instalações;
- Sistema de deteção de intrusão na rede;
- Teste do bom funcionamento do gerador de energia;

Prevenção de falhas

Para além de avaliar o tipo de falhas e monitorizá-las também é necessário precavê-las. Assim, a organização utiliza métodos de prevenção, tais como:

- Segurança para controlo do acesso físico às instalações;
- Temperatura e humidade controlada;
- Utilização de um gerador de energia para o caso de uma falha de energia;
- Sistemas de combate a incêndios, inundações e sismos;
- Uso de equipamentos de qualidade;
- Equipamentos extra caso haja a necessidade de troca;
- Sistema automatizado de monitorização de falhas;
- Educação e formação dos colaboradores e utilizadores do sistema;
- Atualizações e melhoramentos de software, componentes e instalações;
- Utilização de firewalls, e equipa de cyber segurança;
- Backups para outra plataforma para a salvaguarda dos dados necessários ao negócio;

Desastre

Acontecendo um desastre, uma equipa de Resposta a Incidentes será chamada e terá como principais funções a recuperação e avaliação dos danos. A equipa tentará chegar ao local afetado o mais rapidamente possível e começa imediatamente a tratar do problema.

Primeiramente, a equipa irá avaliar os danos, percebendo que consequências este desastre teve para o bom funcionamento do negócio. A equipa terá testes pré-preparados e especialistas para a dada ocasião e assim consegue avaliar rapidamente os danos.

Após a avaliação ser feita, os planos de recuperação serão postos em prática. A equipa começará por notificar a equipa de suporte técnico para fornecer ajuda e explicação do sucedido a qualquer utilizador que esteja a ter problemas devido a este acontecimento.

A equipa irá coordenar esforços e recursos necessários á resolução do problema, por exemplo:

- Necessidade do uso dos dados de backup;
- Necessidade de chamar certos especialistas, técnicos e/ou equipas para a resolução de problemas específicos;
- Pedido de novos equipamentos ou componentes que foram danificados;
- Alerta das autoridades, se necessário.
- Alertar a organização do estado de emergência, de modo que todos os esforços necessários sejam focados no restauro do sistema;

Caso a resolução do problema se torne demorada, as equipa irá trabalhar em turnos de 4 horas para não haver sobrecarga de trabalho e fazer com que este seja o mais eficiente possível. A manutenção normal da aplicação, enquanto a situação não se encontrar regularizada, não irá ser feita.

Após a adversidade ter sido resolvida a empresa será notificada, e a equipa de Resposta a incidentes (ERI) irá fazer um relatório detalhado sobre o sucedido. Depois da situação ser regularizada a organização voltará ao seu funcionamento normal e o relatório do desastre será depois analisado e discutido pela ERI, o comitê executivo de DRP e os administradores para reflexão do acontecimento e a tomada de medidas, se necessário.