RELATÓRIO DO SPRINT 3

DISASTER RECOVERY PLAN

Turma 2DH _ Grupo 43
1190929 _ Patrícia Barbosa
1190947 _ Pedro Fraga
1190956 _ Pedro Garcia
1190963 _ Pedro Preto

Professor:
André Moreira, ASC
Unidade Curricular:
Administração de Sistemas

Data: 22/01/2021

ÍNDICE

INTRODUÇÃO

O presente documento caracteriza o plano de recuperação de desastres (DRP), pedido na user story 1 do sprint 3 de ASIST.

O DRP é um artefacto que prevê possíveis riscos e/ou catástrofes, avalia o seu risco e impacto no sistema e define os processos de planeamento para superar o risco, e retomar o funcionamento normal do sistema em causa, o mais rapidamente possível, de modo a diminuir os impactos causados pela falha do sistema.

DESENVOLVIMENTO

DECLARAÇÃO DO PROPÓSITO

Este documento tem como propósito definir medidas de prevenção e estabelecer políticas de planeamento, para a recuperação e reposição do sistema, na ocorrência de um desastre. Um desastre pode ser qualquer ocorrência que impeça o normal funcionamento de um ou vários sistemas, como por exemplo uma falha de rede, ou catástrofes naturais, como terramotos e tornados.

Aquando de tal ocorrência, devem ser seguidos os passos sugeridos neste plano.

DECLARAÇÃO DE POLÍTICA

- Será desenvolvido um plano de recuperação de desastres.
- Será feita uma análise de risco para identificar requisitos.
- O plano será constantemente testado e atualizado, num ambiente simulado de emergência
- Todos os membros da equipa sabem da existência do plano e a respetiva posição no mesmo.

OBJETIVOS

- Reduzir ao máximo o tempo de paragem e perdas de dados em caso de desastre;
- Estabelecer planos de emergência
- Otimizar a reposição dos serviços afetados
- Definir cenários de desastre e os processos de recuperação.

CONTACTOS CHAVE

NOME	EMAIL	CONTACTO
Patrícia Barbosa	1190929@isep.ipp.pt	919276691
Pedro Fraga	1190947@isep.ipp.pt	967785200
Pedro Garcia	1190956@isep.ipp.pt	937377821
Pedro Preto	1190963@isep.ipp.pt	918624012

CONTACTOS EXTERNOS

FUNÇÃO	NOME	EMAIL	CONTACTO
Proprietário	**ISEP**	info-sa@isep.ipp.pt	22 834 0500
Companhia de Eletricidade	**EDP**	apoiocliente@edp.pt	21 353 5353
Fornecedor de Rede	**MEO**		16 200

ARMAZENAMENTO DA DOCUMENTAÇÂO DO PLANO

Cópias do plano, em papel e formato digital (CD's), serão armazenadas em múltiplas localizações seguras, definidas pela empresa. Todos os membros da equipa terão acesso a uma cópia digital do DRP. Os membros da equipa de recuperação após desastre têm acesso a uma cópia digital, assim como a uma cópia física.

ESTRATÉGIA DE RECUPERAÇÃO

O sistema como um todo, é a junção entre vários componentes, e a relação entre si. Desta forma, é crítico que existam *backups* para todos os componentes de sistema.

Para qualquer um dos componentes (Master Rede Social, Master Data Posts, etc…), foi definido que existirão 3 *backups*: um *backup* na *cloud*, salvaguardando de danos físicos, como furtos ou catástrofes, um *backup* num servidor remoto, e por fim uma cópia num disco externo, guardada num local seguro, salvaguardando de possíveis falhas de rede.

Esta estratégia segue o princípio "3,2,1", que diz devem existir 3 cópias, em 2 *media* diferentes, sendo que 1 cópia deve ficar armazenada num local diferente.

ANÁLISE DE RISCOS

De modo a compreender melhor quais as ameaças ao sistema informático, assim como as medidas a tomar no caso de estas se concretizarem, deve ser elaborada uma análise de riscos.

Uma análise de riscos é, como o nome indica, uma análise detalhada de todos os riscos ou ameaças, da probabilidade e impacto causado por essa ameaça, e as medidas a tomar. Desta maneira, os riscos são quantificados, e o sistema ficará mais salvaguardado.

Apresenta-se na tabela seguinte, a matriz de riscos desenhada, onde cada ameaça é cotada de 1 a 5 em termos de probabilidade e risco, onde 1 é muito baixo e 5 muito elevado, e de seguida é calculado o risco, através da fórmula:

$$risco = probabilidade * impacto$$

AMEAÇA	PROBABILIDADE	IMPACTO	RISCO	PREVENÇÃO
Ataque informático	5	5	25	Investimento em antivírus e equipa de segurança. Promoção de boas práticas de segurança.
Falha elétrica	4	4	16	Geradores de energia automaticamente iniciados quando ocorre uma falha elétrica
Ataque terrorista	2	5	10	Monitorização de atividade suspeita. Reforço de segurança
Incêndio	2	4	8	Detetores de fumo e fogo com aspersores.
Inundação	1	5		Hardware crítico localizado nos pisos superiores
Terramoto	1	4	4	Construções antissísmicas

PROTEÇÃO CONTRA AMEAÇAS

Nem todos os riscos são extremamente perigosos para o sistema, devido ao impacto e a probabilidade dos mesmos. Desta forma, nem sempre é necessário a criação e investimento em soluções para essas possíveis ameaças.

Um indicador usado para verificar a viabilidade da cobertura de um risco, é o SLE (*single loss expenditure*), que é calculado através da multiplicação entre o fator de exposição ao risco de uma ameaça. AV, pelo valor do recurso, EF.

Outro indicador é o ALE (*annualized loss expectancy*), que é calculado pela multiplicação entre o SLE e a probabilidade de ocorrência anual de um risco.

O valor obtido por estes indicadores deve ser comparado ao custo necessário para mitigar a ocorrência da ameaça, para decidir se é viável ou não o investimento na prevenção de uma ou mais ameaças.

ATIVADORES DO PLANO

O DRP é automaticamente ativado aquando ocorrência de uma ou mais destas situações:

- Perda total das comunicações
- Perda total do edifício

- Falha de energia
- Inundação do edífício

PLANO DE RECUPERAÇÂO

Para a realização do plano de recuperação, é importante definir o RTO e o POR, que são indicadores do tempo médio de recuperação dos sistemas e o tempo máximo de perda de dados aceite, respetivamente. Tendo definidos estes valores, calcula-se o tempo necessário para a recuperação de dados e aplicações-

A equipa responsável pela recuperação dos sistemas é a equipa de recuperação de desastres (DR), enquanto a equipa responsável por ativar a emergência é a equipa de resposta de emergência (ERT).

NOME	EQUIPA
Patrícia Barbosa	ERT
Pedro Fraga	DR
Pedro Garcia	ERT
Pedro Preto	DR

A ERT define as medidas a ser invocadas pelo DRP, consoante a extensão do desastre, contacta as autoridades de emergência, contacta os funcionários para alocar responsabilidades e atividades necessárias e comunica com a equipa de recuperação de desastres para manter os serviços vitais e recuperar o controlo sistema.

A equipa DR é contactada pela ERT, e tem como responsabilidades resolver todas as falhas nas primeiras duas horas, restaurar todos os serviços base nas primeiras 4 horas, recuperar a atividade normal até ao final das primeiras 24 horas e, para finalizar, detalhar todas as falhar ocorrentes durante o desastre.

FORMULÁRIOS E AVALIAÇÃO DE DANOS

Após a ativação do DRP devem ser preenchidos formulários, onde se regista o evento que provocou a ativação do plano, os principais serviços afetados e a dimensão dos danos. Este tipo de registos permitirá estudar e aprofundar o conhecimento sobre um dado risco, e potencia a criação de uma solução melhorada.

Durante o desastre, todas as atividades executadas pela equipa de recuperação de desastres também são registadas, definindo bem as datas de início e fim, os recursos envolvidos, o responsável pela atividade, entre outros.

Se necessários, o plano também pode ser alterado durante esta fase, para melhor responder às adversidades.

Para além disto tudo, todos os eventos chave que ocorrem durante o desastre, têm de ser gravados, que posteriormente deverão ser condensados num *event log* pelo líder da equipa de recuperação de desastres.

FORMULÁRIO PÓS DESASTRE

Após o final do período de desastre, deve ser preparado um relatório acerca das atividades exercitadas durante a execução do DRP.

O relatório deve conter:

- Informação sobre a emergência, quem foi notificado e quando, e a ação tomada pelos responsáveis;
- As pessoas notificadas da emergência;
- As ações tomadas pelos membros da equipa de recuperação de um desastre.
- Resultados diretos dessas ações
- Aprendizagens com os eventos

ATUALIZAÇÃO DO DRP

Para atualizar o DRP, é necessário definir bem as mudanças propostas, com o intuito de corrigir eventuais lacunas no plano em vigor.

O DRP deve estar em constante atualização, servindo-se da obtenção de novas informações e da aprendizagem com desastres anteriores, assim como constantemente testado, de modo a apresentar-se o mais robusto possível e, desta forma, combater de forma mais eficaz as ameaças.

CONCLUSÃO

Para a realização deste sprint, estudámos e elaborámos o plano de recuperação de desastres, pelo que passámos a compreender melhor a sua função e aplicação, assim como a sua importância para a manutenção da continuidade do negócio. Uma resposta rápida e eficaz, que será um resultado direto de um DRP eficiente, permite uma melhor continuidade de negócio, diminuindo as perdas e contribuindo para a um melhor futuro do negócio em causa.

WEBGRAFIA

- https://www.ibm.com/docs/en/i/7.3?topic=system-example-disaster-recovery-plan
- https://www.dei.isep.ipp.pt/~asc/doc/ASIST/2014-2015/T04.pdf
- https://www.microfocus.com/media/unspecified/disaster_recovery_planning_template_revised.pdf