DISASTER RECOVERY PLAN TEMPLATE

Dell PowerProtect Cyber Recovery Vault – EcoTech

Data Criação: 25/04/2024

Version: 00

CONTEÚDO

CONTROLE DO DOCUMENTO

Histórico de Testes

DATA	VERSÃO	DESCRIÇÃO	AUTOR/REVISOR

Histórico de Revisão

DATA	VERSÃO	DESCRIÇÃO	AUTOR/REVISOR

Time Dell Tecnologies

Nome	Função	E-mail

Time cliente

Nome	Função	E-mail

PROPÓSITO

Este Disaster Recovery Plan (DRP) fornece os processos e procedimentos necessários para se recuperar de um ataque cibernético.

Este plano trata da recuperação do sistema de TI da EcoTech. Este sistema é composto por 3 *clusters* VMware, dos quais dois são críticos para o negócio: o *cluster* SAP e o *cluster* Oracle legado. Os hosts críticos que fazem parte do *cluster* SAP estão descritos abaixo, sendo no total 9 máquinas virtuais.

Recursos do sistema

Esta seção traz a relação entre os hosts do sistema e os dados críticos que estão salvos no Cyber Recovery Vault. Esta enumeração deve ter sido aprofundada em etapas anteriores da metodologia de identificação de recursos críticos:

- ecotech-prod-db – Dados do banco de dados presentes no host
- ecotech-prod-web – Banco de dados prod
- ecotech-backup-db – Dados do banco de dados presentes no host
- ecotech-monitor – Banco de dados prod
- ecotech-analytics – Banco de dados prod
- ecotech-iot – Banco de dados prod
- ecotech-dev-db – Dados do banco de dados presentes no host
- ecotech-dev-web – Banco de dados dev
- ecotech-dev-analytics – Banco de dados dev

Requisitos do sistema

Para cada recurso, a relação de requisitos de *downtime*:

MTPD: tempo que levaria para que os impactos de uma interrupção se tornassem inaceitáveis, para atividades priorizadas.

RTO: período máximo que o sistema levará para voltar a operar após uma parada ou pane

RPO: o ponto funcional para o qual uma atividade deve ser recuperada, para atividades priorizadas.

Recurso (Host)	Papel do recurso	MTPD	RTO	RPO
ecotech-prod-db	Banco de dados principal para operações de produção	24h	2h	12h
ecotech-prod-web	Aplicação web para gestão e monitoramento de operações	24h	3h	12h
ecotech-backup-db	Banco de dados de backup	24h	2h	12h
ecotech-monitor	Sistema de monitoramento de produção e desempenho	24h	4h	12h

ecotech-analytics	Sistema de análise de dados para insights operacionais	24h	4h	12h
ecotech-iot	Sistema IoT para coleta e análise de dados de sensores	24h	4h	12h
ecotech-dev-db	Banco de dados para desenvolvimento	24h	6h	12h
ecotech-dev-web	Aplicação web para ambiente de desenvolvimento	24h	6h	12h
ecotech-dev-analytics	Sistema de análise de dados para ambiente de desenvolvimento	24h	6h	12h
ecotech-prod-db	Banco de dados principal para operações de produção	24h	2h	12h

ESCOPO

Contatos

A tabela abaixo identifica os contatos principais que têm a responsabilidade de atualizar, manter e executar o plano:

Nome	Função	Email	Telefone
Fulano da Silva	Vault Manager	fulano.silva@ecotech.com.br	(99) 99999-9999
Ciclano da Silva	Storage Admin	ciclano.silva@ecotech.com.br	(99) 99999-9999

A tabela abaixo lista os *stakeholders* que serão comunicados durante a execução do plano:

Nome	Função	Email	Telefone
Fulano de Andrade	Gerente de TI	fulano.andrade @ecotech.com.br	(99) 99999-9999

Ativação do plano

O plano de recuperação deve ser ativado em caso de indisponibilidade dos recursos listados. Alguns incidentes que podem levar a ativação do plano são:

1. Acidentes/desastres naturais
2. *Malwares*
3. Vandalismo

Plano de comunicação

Esta seção diz respeito aos contatos que devem ser comunicados durante cada etapa do plano de recuperação. É ideal que seja produzido um plano de comunicação para que o processo de recuperação seja iniciado o quanto antes e aconteça de maneira mais eficiente possível.

Etapas do plano

As etapas a seguir são uma sugestão de quais passos devem ser realizados dentro do DRP, devendo ser adaptadas para as necessidades da EcoTech.
Visão geral de quais são as etapas do plano de recuperação:

1. Resposta ao ataque cibernético

a) Desativar o acesso ao CR Vault
b) Isolar o ataque
c) Comunicação do ataque

2. Análise forense e avaliação de danos – é recomendado que a empresa tenha ao menos um contato responsável para este fim.

a) Definir os recursos afetados pelo ataque
b) Realizar análise forense
c) Consolidar resultados da análise

3. Recuperação

a) Determinar estratégias de recuperação
b) Definir cópia para ser restaurada
c) Recuperar de acordo com prioridade de recursos

4. Validar que recuperação foi bem-sucedida

a) Avaliar de acordo com a estratégia que a recuperação foi bem-sucedida

b) Definir ações caso de reparo em caso de falha

5. Próximo passos

a) Comunicar autoridades sobre resultados da análise forense

b) Realizar treinamentos na companhia para prevenir novos incidentes

1 - Resposta ao Ataque Cibernético

A primeira etapa do plano é responder ao ataque cibernético, garantindo a segurança do ambiente de Vault e a contenção do vetor de ataque. As tabelas a seguir são um modelo de as ações para esta etapa do plano, que devem ser adaptadas para as necessidades da EcoTech.

	AÇÃO	TEMPO
PROCEDIMENTO PARA DESATIVAR O ACESSO AO CR VAULT		
1.	Verificar agendamento da replicação para o Vault. Se o air-gap estiver habilitado, nenhuma ação é necessária.	5 minutos
2.	Caso a replicação para o Vault estiver em andamento, desabilitar o air-gap.	10 minutos

	AÇÃO	TEMPO
PROCEDIMENTO PARA ISOLAR O ATAQUE		
1.	Identificar sistemas afetados	10 minutos
2.	Identificar redes onde os sistemas estão inseridos	10 minutos
3.	Desconectar sistemas afetados da rede	30 minutos

	AÇÃO	TEMPO
PROCEDIMENTO PARA COMUNICAÇÃO DO ATAQUE		
1.	Notificar responsáveis pelos sistemas afetados	30 minutos
2.	Notificar stakeholders afetados pelos ataques	1 hora
3.		

2 - Análise forense e avaliação de danos

A segunda etapa do plano é compreender os danos causados pelo ataque, elencando quais foram os recursos afetados, além de realizar uma análise forense para definir qual foi o vetor de ataque. Caso necessário, esta etapa pode ser realizada através de um consultor parceiro. As ações a seguir devem ser adaptadas as necessidades da EcoTech.

	AÇÃO	TEMPO
DEFINIR OS RECURSOS AFETADOS PELO ATAQUE		
1.	Examinar todos os recursos do sistema, definindo se o recurso foi afetado pelo malware	3 horas
2.		

	AÇÃO	TEMPO
PROCEDIMENTO PARA ANÁLISE FORENSE		
1.	Analisar logs do sistema para identificar vetor de ataque	4 horas
2.	Definir falha de segurança que levou ao ataque	2 horas
3.	Verificar se existem remediações imediatas a falha	2 horas

Utilizar informações coletadas na análise forense para responder as seguintes questões:

Qual é o vetor de ataque?	
Quando ocorreu o dano?	
Quem provocou o dano?	
O dano se espalhou?	
Qual é a origem do vetor de ataque?	

3 – Recuperação

Com base no que foi identificado na etapa anterior, determinar qual será a melhor estratégia de recuperação para este incidente. As ações a seguir devem ser adaptadas as necessidades da EcoTech.

- ***Restore* -** Esta opção deve ser selecionada caso os *backups* dos sistemas estejam comprometidos.
- ***Repair* -** Dependendo da gravidade e da extensão do ataque, a recuperação pode envolver o reparo de binários do sistema do *backup* de produção ou dos dados protegidos do Vault.

- ***Rebuild* -** Esta opção pressupõe que o ambiente de produção não está disponível e a reformatação a partir de dados no Vault é a única opção.

	AÇÃO	TEMPO
ESTRATÉGIA DE RESTORE DO SISTEMA		
1.	Com base nos recursos afetados e sua ordem de prioridade, definir a ordem de recuperação do sistema	20 minutos
2.	Restaurar recursos de acordo com seus *runbooks*	10 horas
3.		

	AÇÃO	TEMPO
ESTRATÉGIA DE REPAIR DO SISTEMA		
1.	Com base nos recursos afetados e sua ordem de prioridade, definir a ordem de reparação do sistema	20 minutos
2.	Identificar os binários necessários para cada recurso e fazer a reparação com base nos dados salvos no Vault	4 horas
3.		

	AÇÃO	TEMPO
ESTRATÉGIA DE REBUILD DO SISTEMA		
1.	Com base nos recursos afetados e sua ordem de prioridade identificada na BIA, definir a ordem de *rebuild* do sistema	*20 minutos*
2.	Realizar *rebuild* dos recursos de acordo com seus *runbooks*	*15 horas*
3.		

4 – Validar que recuperação foi bem sucedida

Dado que as ações de recuperação foram realizadas, o sistema deve estar funcional de acordo com os critérios de cada estratégia. Esta etapa tem o objetivo de validar a recuperação, definindo os critérios para confirmar que a etapa de recuperação foi realizada com sucesso. As ações a seguir devem ser adaptadas as necessidades da EcoTech.

	AÇÃO	TEMPO
VALIDAR ESTRATÉGIA DE RESTORE DO SISTEMA		
1.	Analisar os hosts contaminados com o *malware*, verificando que a presença do vetor foi eliminada	1 hora
2.	Fazer testes manuais nos componentes críticos do sistema, verificando que ele atende aos requisitos de negócio e de segurança	1 hora
3.		

	AÇÃO	TEMPO
VALIDAR ESTRATÉGIA DE REPAIR DO SISTEMA		
1.	Analisar os hosts contaminados com o *malware*, verificando que a presença do vetor foi eliminada	1 hora
2.	Fazer testes manuais nos componentes críticos do sistema, verificando que ele atende aos requisitos de negócio e de segurança	1 hora
3.		

	AÇÃO	TEMPO
VALIDAR ESTRATÉGIA DE REBUILD DO SISTEMA		
1.	Analisar os hosts contaminados com o *malware*, verificando que a presença do vetor foi eliminada	1 hora
2.	Fazer testes manuais nos componentes críticos do sistema, verificando que ele atende aos requisitos de negócio e de segurança	1 hora
3.		

5 – Próximos passos

Com a recuperação do sistema bem sucedida, estes são os próximos passos para garantir que as lições aprendidas com o incidente sejam utilizadas para fortalecer a resiliência cibernética da EcoTech. As ações a seguir devem ser adaptadas as necessidades da EcoTech.

	AÇÃO	TEMPO
CRIAÇÃO DE RELATÓRIO SOBRE O INCIDENTE		
1.	Criar documento especificando o passo a passo da execução do plano de recuperação	1 hora
2.	Definir fraquezas e pontos de melhoria que existem no plano	1 hora
3.		

DELL Technologies

RUNBOOK

SEÇÃO 1 – DOCUMENTOS DE REFERÊNCIA

Esta seção reúne onde é possível encontrar os principais documentos de referência relacionados ao recurso de produção.

DOCUMENTO	OBJETIVO	LOCALIZAÇÃO
Documentação SAP EcoTech	Entender o sistema SAP da empresa	Google Drive na pasta documentos

SEÇÃO 2 – RECURSOS E SOFTWARES

Nesta seção, estão listados os recursos (*softwares*, *hardwares*, ferramentas, entre outros) necessários para a recuperação do recurso de produção.

1 – Recursos para a recuperação

RECURSO	OBJETIVO	RECURSO A SER RECUPERADO
Código Terraform do banco de dados	Recuperação via código	ecotech-prod-db

2 – *Softwares* a serem recuperados

Nesta seção, estão listados os *softwares* que devem ser recuperados a fim de garantir o funcionamento dos recursos de produção.

SOFTWARE	RECURSO A SER RECUPERADO
Aplicação web	ecotech-prod-web

SEÇÃO 3 – PASSO-A-PASSO DE RECUPERAÇÃO DO RECURSO

Esta seção descreve quais os passos para que o recurso seja recuperado. Nela, há scripts nos passos em que é necessário.

	AÇÃO	SCRIPT
PLANO DE RECUPERAÇÃO		
1.	Identificar *Datastores* / LUNs que devem ser recriados	**print do script**
2.	Caso *patches* estejam disponíveis, aplicá-los nas imagens de SO	
3.	Criar uma nova distribuição de *softwares* necessários para sistemas recuperados	
4.	Criar sequência de recuperação (*High-level*)	

5.	Verificar que o novo *server* (ou *server* limpo) na Produção está pronto para receber o *restore*	
6.	Validar qual será a cópia utilizada via Cyber Recovery para recuperação	
7.	Criar a estrutura no Data Domain do Vault antes de enviar os dados para produção	
8.	Criar o contexto de replicação reverso que será usado para transportas os dados entre Vault e produção	
9.	Iniciar o processo de recuperação reversa dos dados dentro do Vault para a produção.	
10.	Acompanhamento da recuperação reversa dos dados. (Ao realizar testes com o volume final dos dados após a definição das aplicações "Crown Jewel" atualizar o este campo e controlar o tempo de recuperação.)	
11.	Preparar os dados no Data Domain da produção recém recuperados do Vault.	
12.	Preparar o PowerProtect Data Manager para realizar o DR com os dados vindos do Vault.	
13.	Realizar o Disaster Recovery do PowerProtect Data Manager na produção	
14.	Validar as configurações da PowerProtect Data Mananger recém recuperado.	

SEÇÃO 4 – VALIDAÇÃO DA RECUPERAÇÃO

Esta seção descreve como será validado o sucesso da recuperação do recurso, além de quais testes devem ser realizados após a recuperação para garantir a funcionalidade adequada.

	AÇÃO	SCRIPT
PLANO DE RECUPERAÇÃO		
1.	Identificar *Datastores* / LUNs que devem ser recriados	**print do script**
2.	Caso *patches* estejam disponíveis, aplicá-los nas imagens de SO	
3.	Criar uma nova distribuição de *softwares* necessários para sistemas recuperados	
4.	Criar sequência de recuperação (*High-level*)	
5.	Verificar que o novo *server* (ou *server* limpo) na Produção está pronto para receber o *restore*	
6.	Validar qual será a cópia utilizada via Cyber Recovery para recuperação	
7.	Criar a estrutura no Data Domain do Vault antes de enviar os dados para produção	
8.	Criar o contexto de replicação reverso que será usado para transportas os dados entre Vault e produção	
9.	Iniciar o processo de recuperação reversa dos dados dentro do Vault para a produção.	
10.	Acompanhamento da recuperação reversa dos dados. (Ao realizar testes com o volume final dos dados após a definição das aplicações "Crown Jewel" atualizar o este campo e controlar o tempo de recuperação.)	

11.	Preparar os dados no Data Domain da produção recém recuperados do Vault.	
12.	Preparar o PowerProtect Data Manager para realizar o DR com os dados vindos do Vault.	
13.	Realizar o Disaster Recovery do PowerProtect Data Manager na produção	
14.	Validar as configurações da PowerProtect Data Mananger recém recuperado.	

SEÇÃO 5 – PROCEDIMENTOS ADICIONAIS DE CONTINGÊNCIA / PLANOS ALTERNATIVOS DE RECUPERAÇÃO

Esta seção descreve procedimentos de contingência e planos alternativos caso a recuperação não funcione. Para este caso, também há scripts nos passos em que é necessário.

	AÇÃO	SCRIPT
PLANO DE RECUPERAÇÃO		
1.	Identificar *Datastores* / LUNs que devem ser recriados	**print do script**
2.	Caso *patches* estejam disponíveis, aplicá-los nas imagens de SO	
3.	Criar uma nova distribuição de *softwares* necessários para sistemas recuperados	
4.	Criar sequência de recuperação (*High-level*)	
5.	Verificar que o novo *server* (ou *server* limpo) na Produção está pronto para receber o *restore*	
6.	Validar qual será a cópia utilizada via Cyber Recovery para recuperação	
7.	Criar a estrutura no Data Domain do Vault antes de enviar os dados para produção	
8.	Criar o contexto de replicação reverso que será usado para transportas os dados entre Vault e produção	
9.	Iniciar o processo de recuperação reversa dos dados dentro do Vault para a produção.	
10.	Acompanhamento da recuperação reversa dos dados. (Ao realizar testes com o volume final dos dados após a definição das aplicações “Crown Jewel” atualizar o este campo e controlar o tempo de recuperação.)	
11.	Preparar os dados no Data Domain da produção recém recuperados do Vault.	
12.	Preparar o PowerProtect Data Manager para realizar o DR com os dados vindos do Vault.	
13.	Realizar o Disaster Recovery do PowerProtect Data Manager na produção	
14.	Validar as configurações da PowerProtect Data Mananger recém recuperado.	

APÊNDICES

Adicionar documentos auxiliares a execução do plano (ex: *runbooks* de recursos) nesta seção.