Preparem um documento breve de disaster recovery. Este documento deve conter 5 casos, as formas de como identificá-los e as estratégias para recuperar o ambiente.

Identificação de desastres:

Ataque cibernético: um ataque cibernético pode comprometer a segurança do ambiente do Spotify, resultando em roubo de dados, interrupção de serviços e danos à reputação da empresa.

Falha de hardware: uma falha de hardware pode afetar o desempenho do ambiente, resultando em tempo de inatividade e perda de dados.

Desastre natural: um desastre natural, como um terremoto ou uma enchente, pode danificar fisicamente os servidores do Spotify, resultando em interrupção de serviços.

Erro humano: um erro humano, como a exclusão acidental de dados críticos, pode levar à perda de dados e interrupção de serviços.

Falha de software: uma falha de software pode afetar o desempenho do ambiente, resultando em tempo de inatividade e perda de dados.

Estratégias de recuperação:

Ataque cibernético: Em caso de ataque cibernético, o Spotify irá isolar a parte afetada do ambiente, desativar o acesso externo, restaurar a partir de backups recentes e realizar uma auditoria completa de segurança.

Falha de hardware: Em caso de falha de hardware, o Spotify irá substituir o hardware defeituoso, restaurar a partir de backups recentes e realizar testes de integridade de dados.

Desastre natural: Em caso de desastre natural, o Spotify irá acionar um plano de contingência e transferir serviços para um site secundário, como um ambiente de nuvem ou um data center externo.

Erro humano: Em caso de erro humano, o Spotify irá restaurar a partir de backups recentes, realizar testes de integridade de dados e implementar medidas de segurança adicionais, como restrições de acesso e treinamentos para evitar futuros erros.

Falha de software: Em caso de falha de software, o Spotify irá isolar a parte afetada do ambiente, restaurar a partir de backups recentes e implementar correções de software.