PLANO DE CONTINUIDADE DE NEGÓCIOS

SPN GESTÃO DE INVESTIMENTOS LTDA

Dez/2024

1. OBJETIVO

A SPN desenvolveu este plano de recuperação de desastres para ser usado no evento de uma interrupção significativa dos serviços de TI. O objetivo deste plano é delinear as principais etapas de recuperação a serem realizadas durante e após uma interrupção para que os serviços críticos de TI continuem em operação dentro de um período apropriado após a ocorrência do incidente.

2. ABRANGÊNCIA

Conectividade em home office, situações que caracterizem desastre ou danos permanentes no servidor local.

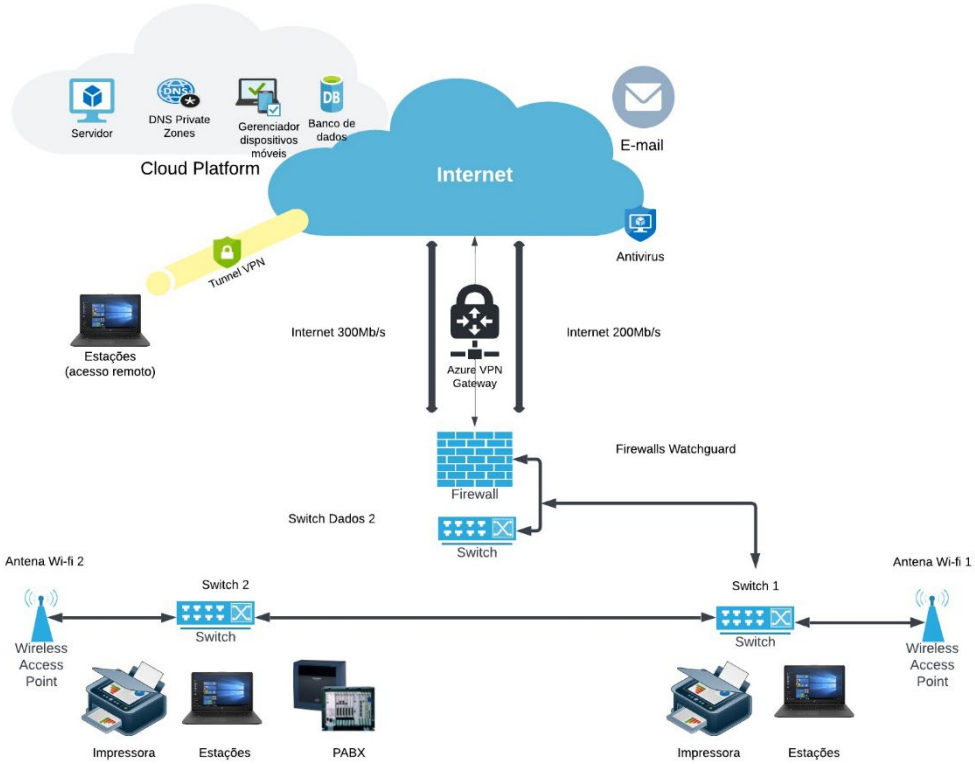
3. AMBIENTE DE SERVIDOR DE ARQUIVOS

O servidor de arquivos e Active Directory está hospedado na plataforma de nuvem do Microsoft Azure, e a conectividade com o serviço de nuvem é suportado por equipamentos de rede, switches, firewalls e serviços de internet redundantes. Os equipamentos de rede estão localizados no CPD e dentro dos padrões e recomendações de segurança, conforme abaixo:

I. Controle de acesso via cartão identificado
II. Sistemas de refrigeração redundante
III. Sistema de incêndio predial
IV. Eletricidade garantida por nobreak e gerador próprio

A plataforma Cloud utilizada garante 99,96% de disponibilidade/ano. Os equipamentos de redes contam com um sistema de redundância física onde, em caso de pane ou parada de um ativo, outro equipamento fica disponível para assumir toda a carga de trabalho. indisponibilidade máxima de 15 minutos.

a. Topologia



b.

c. Serviços cobertos

I. Autenticação das estações de trabalho;
II. Acesso à internet por meio da rede física e wireless;
III. Acesso ao servidor de arquivos;
IV. Resolução de nomes de domínios para navegação na internet;
V. Impressão na rede local.

4. PLANO DE COMUNICAÇÃO

Em caso de problemas ou indisponibilidades da infraestrutura de TI, o plano de comunicação seguirá a ordem conforme descrito na tabela.

Gestores Anima	Contato
Caroline Sena (Compliance)	27 99939-2312
Vera Alves (Compliance)	11 99145-8074

Renan Oliveira (Controladoria de investimentos)	11 3019-2800

Sustentação Técnica	Contato
Fabiano Fortes (Gestor Técnico)	11 98499-0028
Luiz Carlos França (Analista de Suporte)	11 98330-3513

5. ANÁLISE DOS RISCOS

Ameaça	Severidade	Probabilidade	Risco	Medida de Controle
Blackout	Alta	Média	Perda de dados, problemas com disco rígido, falha de configurações, indisponibilidade do ambiente.	Testes periódicos no Nobreak.
Indiponibilidade do data center	Alta	Baixa	Indisponibilidade geral.	Aplicar Disaster Recovery na VM do Servidor.
Firewall	Média	Baixa	Falha no acesso à Internet, Windmill e e-mail.	Sistema dimensionado em alta disponibilidade. Na hipótese de problemas, o chaveamento é automático.
Link de Internet	Média	Baixa	Falha no acesso à Internet, Windmill e e-mail.	O Firewall realiza o balanceamento de ambos os links de dados. Na hipótese de problemas, o

				chaveamento é automático.
Equipamentos de Rede	Média	Baixa	Indisponibilidade Parcial	Em caso de falhas os equipamentos serão substituídos por equipamento backup em até 4 horas.

6. NÍVEL DE RECUPEÇÃO DE DESASTRES

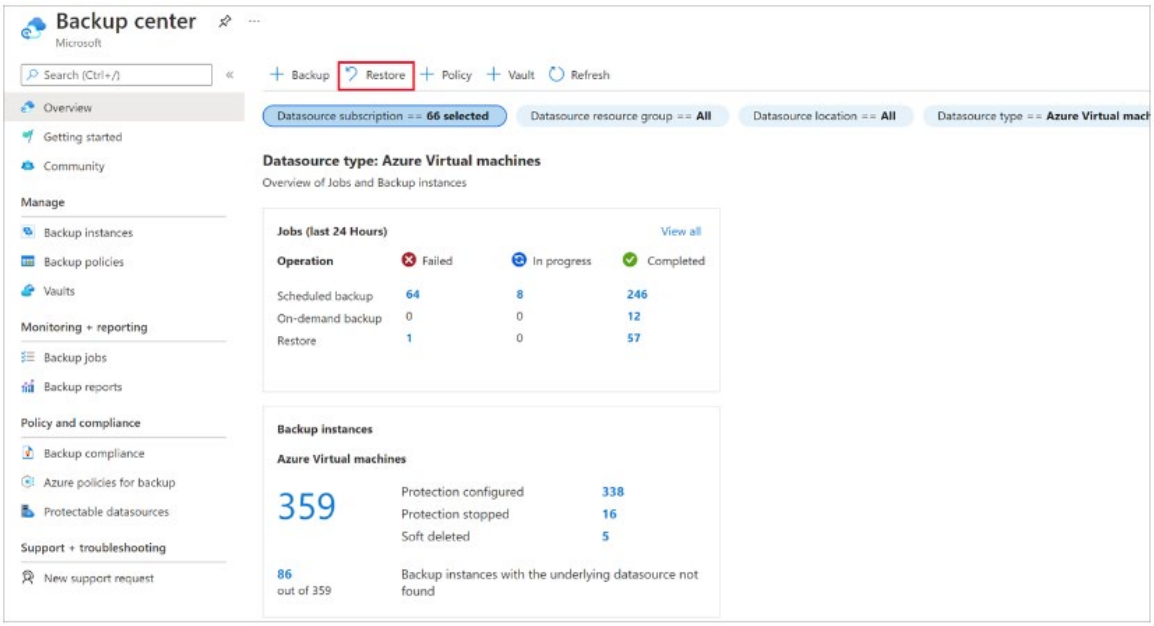
Solução	RPO	RTO	Fraqueza	Nível
Manual	24 horas	14 horas	Ações manuais e intervenção técnica	Atual

a. Métricas de recuperação de desastres

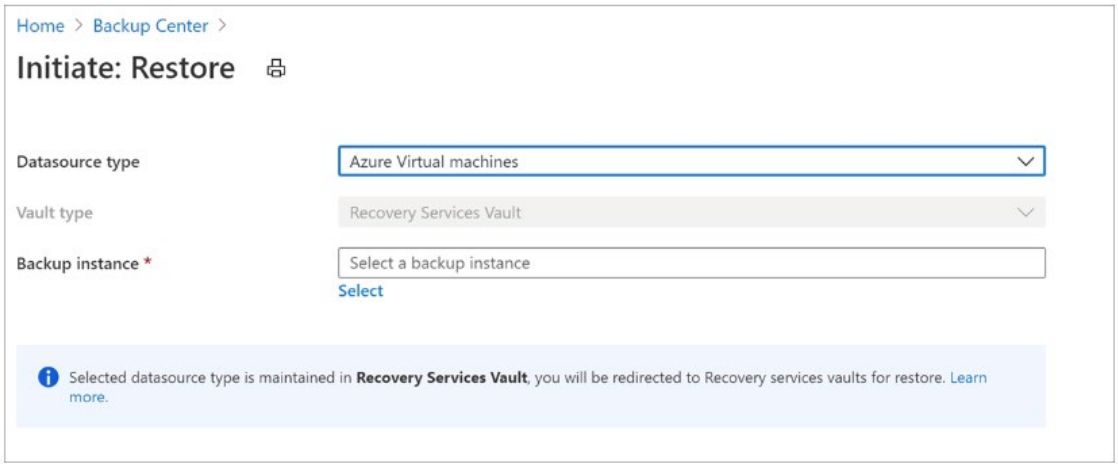
   I. RTO Recovery Time Objective: A meta de quanto tempo o serviço precisa ser recuperado após uma interrupção, com base na quantidade aceitável de tempo de inatividade e nível de desempenho.

7. PROCEDIMENTOS DE RECUPERAÇÃO

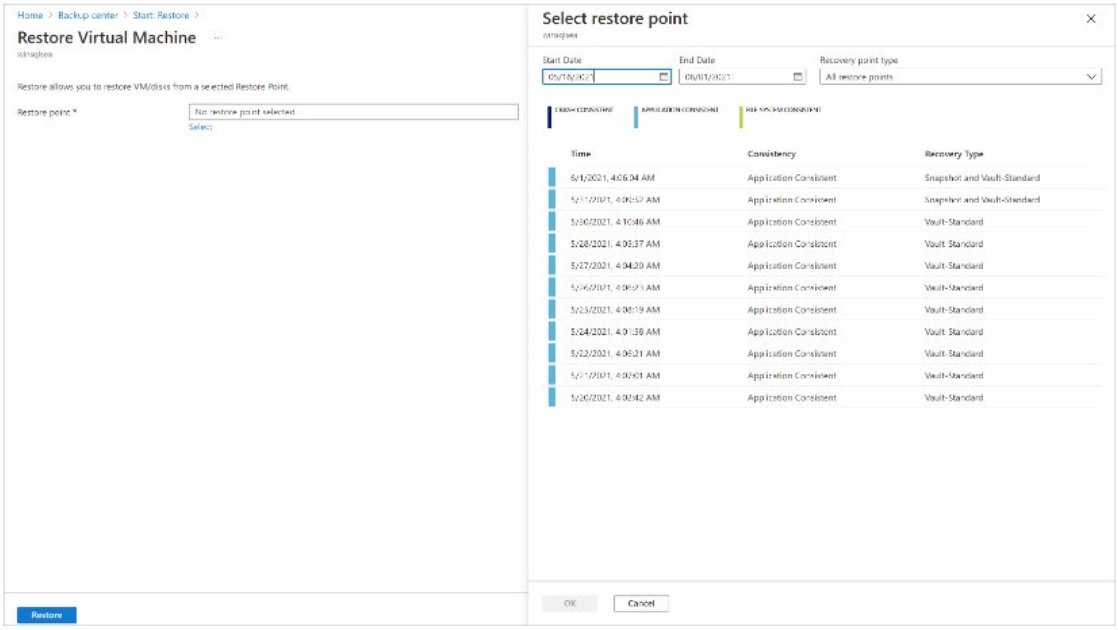
a. Selecionar um ponto de restauração a partir do Backup Center do Microsoft Azure.



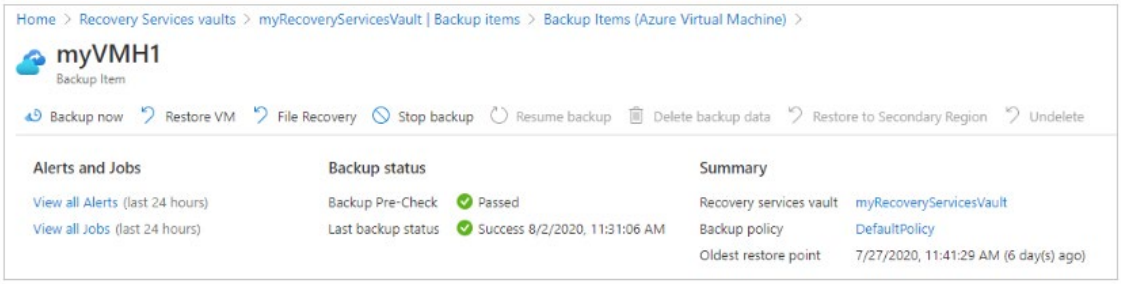
b. Selecionar as máquinas virtuais do Azure como o tipo Datasource e selecionar uma instância de Backup.



c. Selecionar uma VM.

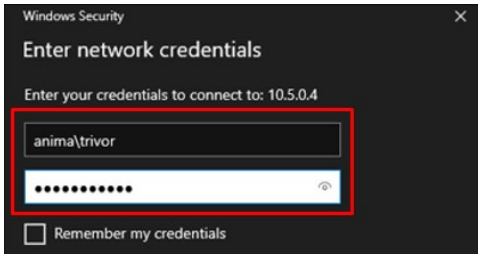


d. Na tela seguinte, selecionar um ponto de restauração a ser usado para a recuperação.

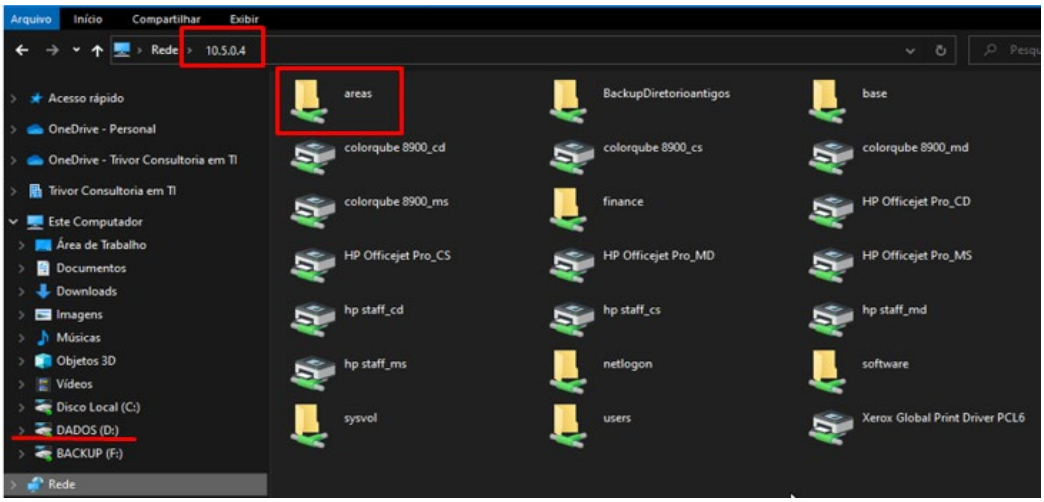


e. Configurar conexão client-to-site VPN (baixar, instalar e importar o certificado de conexão do Azure).

f. Mapear o acesso aos arquivos: utilizar o IP do servidor de contingência, login e senha do usuário para mapear os arquivos da rede.

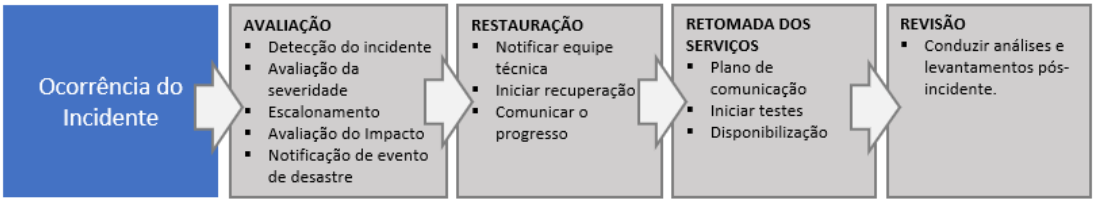


Servidor de Contingência (visão da base de arquivos e impressoras):



8. PROCEDIMENTO DE RESPOSTA A DESASTRES

A resposta a desastres ocorre em várias fases de acordo com o diagrama abaixo.



Quando ocorre um evento, a equipe avalia o evento e decide se a comunicação do desastre é necessária. No caso de ocorrer um desastre, a equipe inicia procedimentos para recuperação do(s) serviço(s) de TI, utilizando, se necessário, um local alternativo.

Assim que os serviços essenciais e necessários retomarem o funcionamento, a Gestora pode voltar às operações normais. A etapa final é realizar uma revisão e análise do evento até o momento em que os serviços normais foram retomados.

9. TESTES DE RECUPERAÇÃO DE DESASTRES

A criação de um plano de recuperação de desastres de TI eficaz e de alto padrão é o resultado de uma boa coesão da equipe. Portanto, testes e verificações são obrigatórios para atingir o objetivo final de recuperação de desastres confiável.

É imperativo que essas revisões ocorram periodicamente, especialmente porque as alterações que não estão conectadas à tecnologia podem provavelmente ter um impacto significativo no plano de DR.

I. Atualizar o plano para atender às novas mudanças organizacionais, prioridades e objetivos.
II. Certificar-se de atualizar as listas de equipes (plano de comunicação).
III. Verificar se as atualizações foram efetuadas para quaisquer alterações relevantes nas configurações no ambiente.

Um bom plano de recuperação de desastres é aquele que pode ser executado com eficácia e sem problemas sempre que necessário. Cada pessoa e cada sistema envolvido no plano deve ser parte integrante da prática. A cada seis meses, o plano de recuperação de desastres deve ser verificado e executado.