Seja bem-vindo à sua
transformação digital absoluta:

segura, escalável e com alta disponibilidade.

fc nuvem

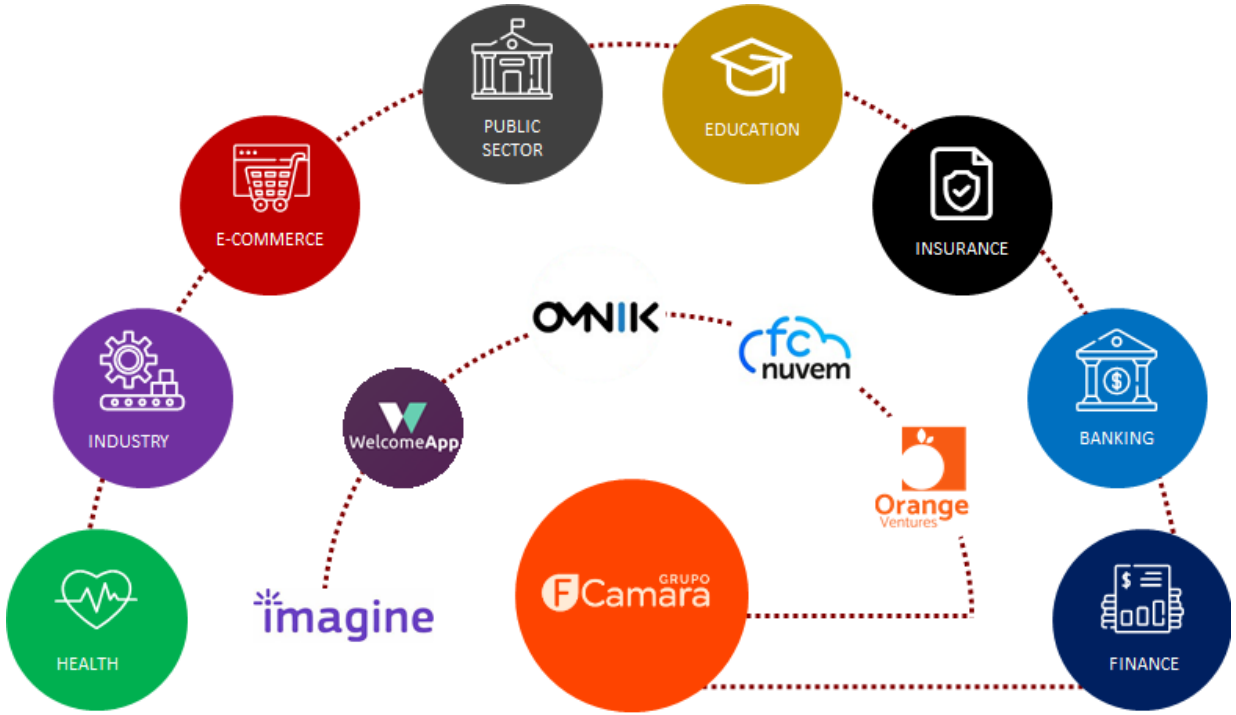
GRUPO Camara

SOBRE NÓS

FC Nuvem – Uma empresa do Grupo FCamara

Repensamos e suportamos sua empresa para uma transformação digital absoluta, dando capacidade de **crescimento exponencial** com **escalabilidade**, **performance**, **alta disponibilidade** e **segurança**.

Escutamos, entendemos e projetamos com cada cliente, analisando suas necessidades de forma minuciosa e propondo a melhor solução para o seu cenário e objetivos, sempre de forma clara e transparente.



O Grupo FCamara promove a transformação digital com foco em negócio, oferecendo múltiplas soluções digitais.

BUNKER FC NUVEM
SEGURANÇA E RECUPERAÇÃO DE DADOS

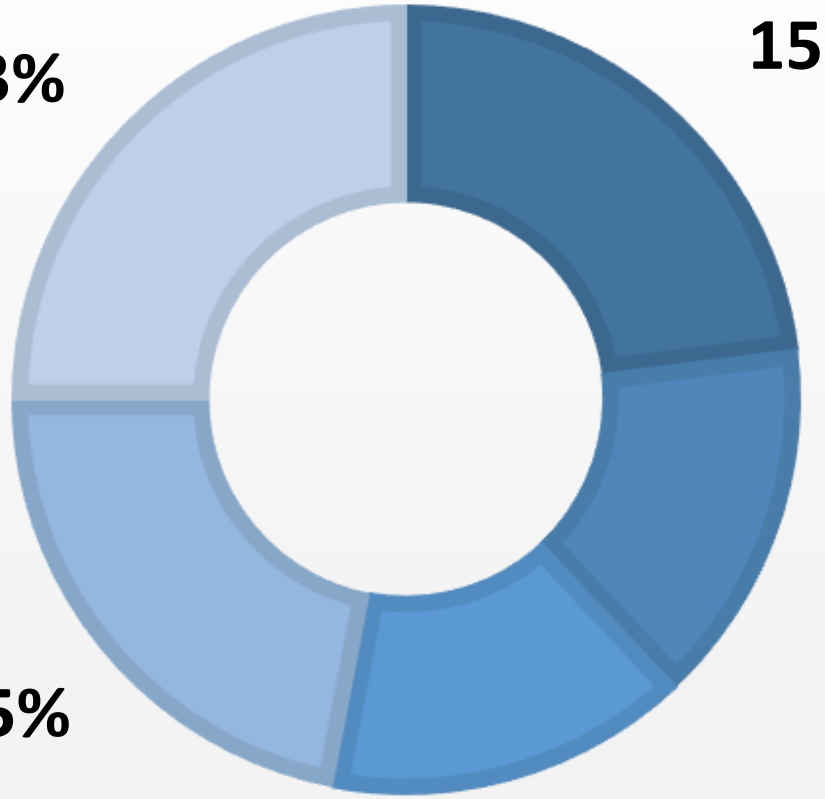
VOCÊ PRECISA ESTAR PREPARADO!

A quantidade de ataques **ransomware** cresceu **92%** no Brasil desde o início de 2021.

Somos o **5º** país com maior quantidades de ataques do tipo no 1º semestre do ano.

O custo médio de remediação à ataques **ransomware** no Brasil foi de **USD 820k** no ano passado

CONHEÇA AS PRINCIPAIS CAUSAS DAS FALHAS DE SEGURANÇA



Infraestruturas de segurança inadequadas — 23%

15% — Má fé ou negligência de pessoal interno

15% — Processos de segurança

Erros de configuração — 25%

22% — Ataques phishing

Fonte: BCG Executive Perspectives. The CEO's Guide to Cybersecurity. Setembro 2021.

CIBERSEGURANÇA COMO PARTE DA ESTRATÉGIA DO NEGÓCIO

PREVENÇÃO

Garanta que seus assets mais valiosos estão com os mais altos níveis de segurança e que haja revisão periódica de possíveis exposições.

DETECÇÃO

Invista em capacidade robusta de monitoramento para viabilizar a identificação rápida de brechas

RESPOSTA

Saiba como responder no caso de uma brecha ou ataque identificado: quanto mais rápido ações forem tomadas, maior a limitação do dano!

RECUPERAÇÃO

Garanta que existam meios de recuperação da sua infraestrutura e sistemas no caso de uma invasão. Prevenir é importante, mas garantir que existe remediação também!

A partir de agora, é imprescindível considerar segurança desde o estágio de desenvolvimento de processos e aplicações. Não espere para colocar a camada de segurança apenas ao final!

Fonte: BCG Executive Perspectives. The CEO's Guide to Cybersecurity. Setembro 2021.

SAIBA COMO SE PROTEGER

Você precisa de um bunker para o seu negócio, uma solução de **proteção máxima** para acionar em caso de ataques à sua infraestrutura!

- **Mitigação de riscos:** garantia de que existem meios para retomada do controle dos sistemas em caso de invasão, diminuindo o incentivo monetário do ataque;
- **Limitação de extensão do dano:** garantia de que seus dados estarão em local seguro e protegidos de vazamentos de informação;
- **Menor impacto nos negócios:** agilidade no reestabelecimento do controle, mantendo assim o seu negócio indisponível por menos tempo.

OBJETIVOS DO BUNKER FC NUVEM

1º Backup

Desenvolver uma solução que permita que os dados, sistemas e negócios estejam protegidos e possam ser restaurados o mais rápido possível.

2º Segurança

Com casos recentes de empresas que foram infectadas pelo vírus Ransonware, a solução deve garantir máxima segurança dos dados.

3º Alta Disponibilidade

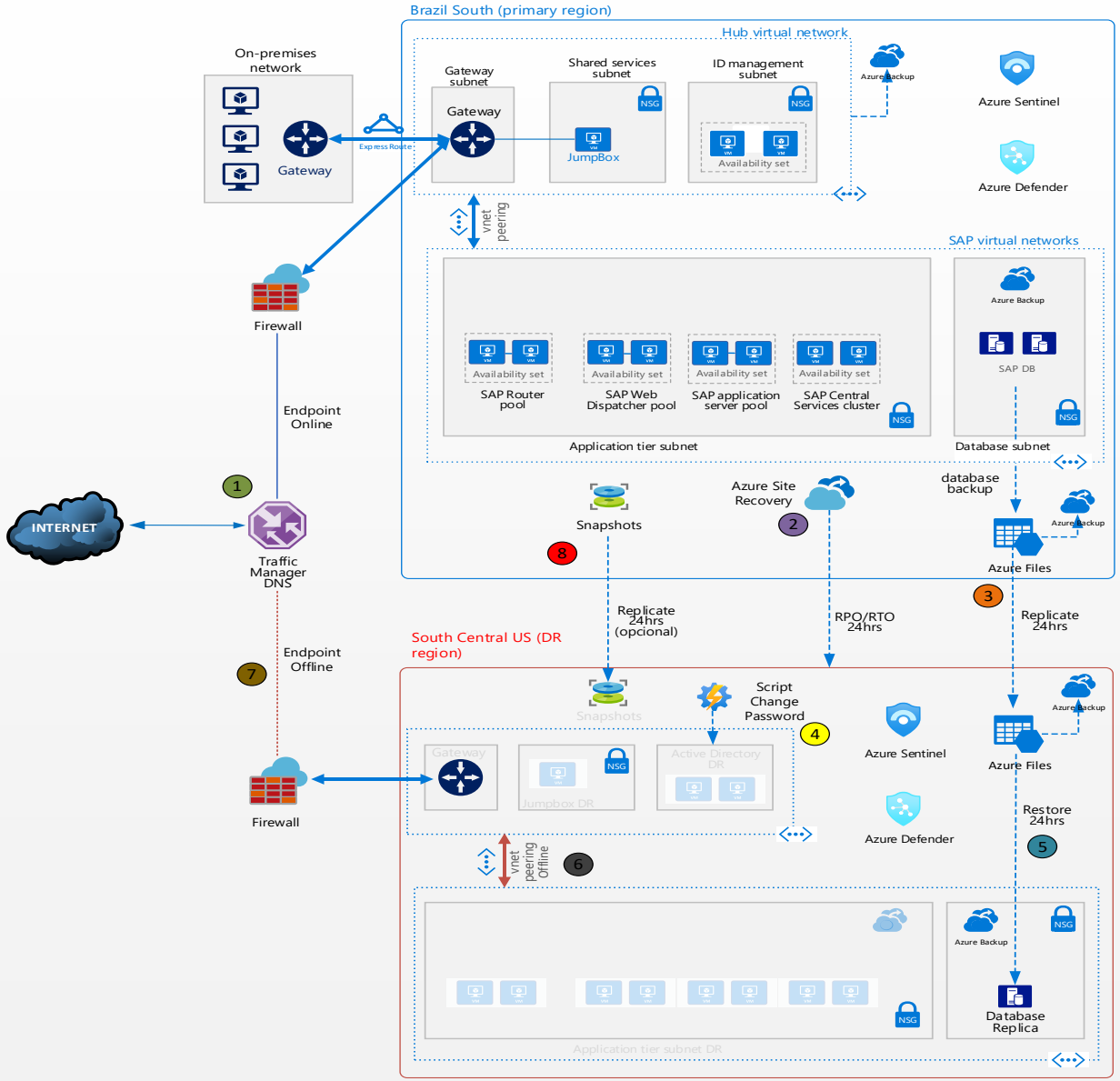
Em caso de desastre ter uma janela rápida de até 24 horas para restauração dos sistemas/dados em outra localidade totalmente separada e blindada.

4º Custo

Garantir o custo ideal para cenário proposto.

EXEMPLO DE ARQUITETURA DA SOLUÇÃO

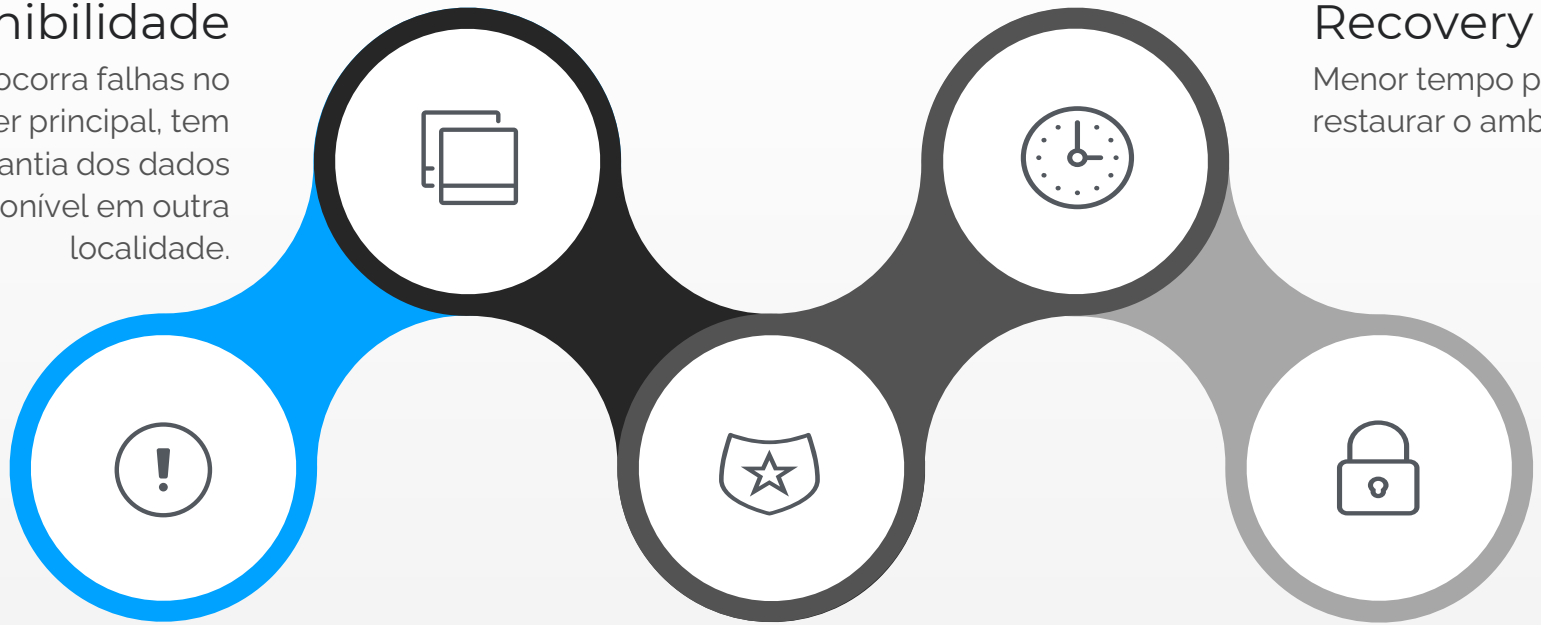
1. **Traffic Manager** – Funciona para redirecionamentos de DNS Externos. Necessário mudar o registro uma única vez apontando pros Endpoints do Traffic Manager;
2. **Azure Site Recovery** – Replicará todos os servidores, exceto o do banco de dados SAP. Mantém um histórico de RPO de 1h totalizando 24hrs;
3. **Azure Files** – Realiza uma cópia dos dados para outro Azure Files em outra região e mantém um backup;
4. Automation Script – Força a troca de senha no primeiro login de todos os usuários, após o failover do AD é executado o Script;
5. **Restore** – Realizar uma automação de restore no banco de dados do DR. Pode definir uma rotina diária para diminuir o tempo de restore;
6. **VNET Peering** – Fica desativado por padrão, será ativado após a garantia que o AD forçou o reset de senhas. O restore dos servidores SAP ocorre após a ativação, para evitar falha de relação de confiança;
7. **Traffic Manager Endpoint Offline** – Será ativado após toda a conclusão de todas as etapas de Restauração do ambiente;
8. **Snapshots** – Opcionalmente pode ser copiado os Snapshot de discos para outra localidade, uma forma de redundância de backups.



PORQUE RECOMENDAMOS ESTA ARQUITETURA DE SEGURANÇA

Alta Disponibilidade

Caso ocorra falhas no datacenter principal, tem uma garantia dos dados estarem disponível em outra localidade.



Recovery Time Objective

Menor tempo para equipe restaurar o ambiente.

Mitigação

Diminuir os impactos casos por invasões e infecções por Ransonware.

Isolamento

Restringir o máximo de acesso à este ambiente.

Proteção dos Dados

As camadas de backup e segurança protegem os dados e elimina o pagamento de resgate dos dados.

FLUXO DE SEGURANÇA DO BUNKER FC NUVEM

Azure Defender

Monitoramento de Integridade de arquivos (FIM) identifica o ataque nos arquivos da VM.

Azure Sentinel

O alerta de segurança é Gerado no Azure Sentinel com alta prioridade.

Monitoramento

O Azure Sentinel abre um chamado com alta prioridade para equipe de monitoramento 24x7.

Restabelecimento

O Sistema está disponível para uso externo/interno.

Disaster Recovery

Inicio do processo de DR e configurações de Sistemas.

Investigação

Inicia um processo de análise para determiner rapidamente se o recurso esta sobre ataque.

CONTE CONOSCO!