

COMUNICAÇÕES POR SATÉLITE EM SITUAÇÕES DE EMERGÊNCIA

Relatório técnico | Resiliência, independência de acesso e lições do incidente KA-SAT

As comunicações por satélite podem ser um meio alternativo valioso quando redes terrestres de fibra, cobre ou comunicações móveis deixam de funcionar. Contudo, também apresentam dependências e riscos que exigem planeamento.

1. Porque as redes terrestres falham

Tempestades, incêndios, cheias, obras, vandalismo, falhas energéticas e indisponibilidade de operadores podem interromper fibra ótica, estações móveis e equipamentos do cliente. Uma ligação de contingência pode reduzir a dependência de um único meio físico ou operador.

2. O que o satélite acrescenta

O terminal satélite comunica por uma infraestrutura espacial e segmento terrestre associado, permitindo cobertura em locais remotos ou em cenários em que não existe rede terrestre disponível. A independência é parcial: o sistema continua a depender de energia, terminais, gateways, centros de operação e fornecedores.

3. Tipos de rede e características

Satélites geoestacionários oferecem ampla cobertura com latência normalmente superior à de fibra; sistemas de órbita terrestre baixa podem reduzir latência mas dependem de constelações, terminais e condições próprias de operação. Tarifários, capacidade, disponibilidade e cobertura devem ser analisados por localização e caso de utilização.

4. Energia e autonomia

Uma ligação alternativa que partilha a mesma UPS descarregada ou o mesmo quadro afetado pode não assegurar continuidade. O planeamento deve incluir alimentação elétrica, baterias, UPS, proteção contra sobretensões, consumo do terminal, testes de autonomia e eventual gerador de emergência.

5. Integração com redes empresariais

O router ou firewall deve ser configurado para failover, com monitorização de conectividade efetiva e testes de recuperação. Dependendo do serviço, podem existir NAT, endereçamento diferente, restrições de portas ou variações de latência que afetam VPN, voz, aplicações de tempo real e acesso remoto.

6. Segurança e segmentação

A ligação de contingência não deve abrir acessos indiscriminados à rede interna. Use firewall, privilégios mínimos, autenticação forte e segmentação de equipamentos de administração. Contratos de serviço e fornecedores devem definir gestão de incidentes, contactos e responsabilidades.

7. Lições do ataque KA-SAT de fevereiro de 2022

O incidente KA-SAT demonstrou que infraestruturas satélite também têm superfícies de ataque no segmento terrestre e nos equipamentos dos utilizadores. O satélite em órbita não precisa de ser comprometido para que um grande número de clientes fique sem serviço. Diversificação tecnológica e segurança operacional complementam-se.

8. Teste de contingência

A ligação deve ser ativada em ensaios periódicos: desligar controladamente a ligação principal, confirmar autenticação, aplicações críticas, VPN e retorno à rota primária. Registe tempos reais, problemas de DNS, capacidade e autonomia. Um equipamento instalado mas nunca testado não demonstra continuidade.

9. Aplicações possíveis

Acesso de emergência em instalações isoladas, continuidade de operações de empresas, coordenação municipal, obras remotas, eventos temporários e comunicações de suporte em cenários de desastre. A adequação depende dos requisitos de latência, tráfego, disponibilidade e acordos de serviço.

10. Conclusão

As comunicações por satélite podem ser uma componente de resiliência, mas não substituem uma estratégia global de continuidade de negócio. A escolha deve basear-se em redundância real, energia independente, medidas de segurança, responsabilidade contratual e testes de funcionamento.