



Abordagem de três pilares para enfrentar os desafios atuais de energia e serviços públicos

Índice

- | Identificação dos desafios de energia e serviços públicos
- | Três pilares para enfrentar os desafios
 1. Segurança em primeiro lugar
 2. Aumentar a eficiência das operações
 3. Melhorar o gerenciamento dos clientes
- | A ALE atende às necessidades do setor de energia e serviços públicos



Identificação dos desafios do setor de energia e serviços públicos

Hoje, as mudanças climáticas estão forçando as empresas de energia e serviços públicos a se transformarem, fornecendo mais energia renovável, reduzindo pegadas de carbono e limitando a poluição. Essa realidade global está levando as empresas de energia e serviços públicos a implementar em políticas de eficiência e melhorias tecnológicas para ajudar na redução do consumo, assim como aumentar sua resiliência para garantir a continuidade do serviço e um plano eficiente de recuperação.

As concessionárias de energia e serviços públicos estão enfrentando três tipos de desafios, incluindo os globais, tecnológicos e a retenção de clientes.

- **No plano global**, elas precisam aumentar a segurança e a proteção de suas operações, reduzir sua pegada de carbono, proteger-se contra ataques cibernéticos e lidar com novas regulamentações.
- **No campo tecnológico**, as organizações de energia e serviços públicos precisam lidar com planos de migração, obsolescência tecnológica, interconexão entre a tecnologia nova e antiga e o gerenciamento de redes de grande escala.
- **Do lado do cliente**, as organizações precisarão desenvolver novas estratégias de relacionamento com o cliente e serviços para atender a novos tipos de clientes, atender às suas expectativas, demanda de consumo e usos.

Três pilares para enfrentar os desafios

Uma abordagem de três pilares que foca em aprimorar a segurança e a proteção, aumentar a eficiência operacional e melhorar o engajamento do cliente pode ajudar os operadores de energia e serviços públicos a enfrentar esses desafios.

1. Segurança em primeiro lugar

Conforme as violações de cibersegurança, vandalismo e ataques terroristas se tornam generalizados, o setor de energia e serviços públicos deve estar preparado para lidar com as ameaças. O investimento é necessário em diversas áreas, incluindo: construir uma infraestrutura digital sólida e segura para redes e comunicações; proteger pessoas e bens; desenvolver mecanismos para enfrentar ameaças à segurança cibernética.

Para enfrentar essas ameaças, a rede de TI deve fornecer múltiplas camadas de resiliência, otimizar os fluxos de tráfego e minimizar a interrupção do serviço. É necessário um plano de resiliência que garanta a continuidade do serviço e um plano eficiente de recuperação de desastres. O plano de resiliência deve ser apoiado por uma infraestrutura confiável e uma rede de missão crítica. Deve ser seguro em termos cibernéticos, compatível com aplicações e com uma plataforma de gerenciamento unificada.

Um **backbone de rede forte** precisa ser confiável, resiliente e seguro para interconectar os diferentes domínios. Deve continuar sem interrupção da rede, mesmo quando esta tiver sido comprometida.

As comunicações abrangem uma variedade de atividades como: segurança operacional, segurança do pessoal, proteção do trabalhador de campo em ambientes perigosos. A ativação de um plano de resiliência requer **uma infraestrutura de comunicações confiável** para garantir a continuidade da operação.

Uma infraestrutura de rede e comunicações confiável

As soluções de rede e comunicações devem ser altamente confiáveis e preparadas para o futuro, capazes de enfrentar os desafios de hoje e de amanhã.

O backbone da rede deve ter as seguintes capacidades:

- Segmentação de serviço
- Convergência de rede de aplicativos multisserviço
- QoS determinístico para atender aos requisitos específicos do aplicativo
- Alta disponibilidade de rede
- Segurança granular
- Sincronização de rede precisa
- Gerenciamento de rede simples e centralizado

Uma infraestrutura de comunicação confiável inclui:

- Redundância hot standby para um sistema de comunicação robusto
- Redundância geográfica para backup de localização física
- Comunicações confiáveis para uma plataforma de comunicação sempre ativa
- Implantação em locais remotos, com serviços de continuidade por meio da capacidade de sobrevivência local
- Conformidade com vários dispositivos para fins específicos, como IP, SIP, TDM, analógico
- Virtualização completa para implantação de otimização do data center
- Arquitetura híbrida para proteger investimentos e evoluir para novos modelos
- Suporte para serviços de nuvem privada e pública



Manter as pessoas seguras

A equipe de segurança e os responsáveis pela segurança pública devem agir de forma rápida e eficaz para enfrentar emergências. Eles não podem permitir que obstáculos operacionais interfiram na sua missão. Para responder rapidamente, eles exigem informações precisas sobre a pessoa que liga, incluindo localização e detalhes de emergência. Também é crucial transmitir mensagens para mobilizar a equipe e gravar chamadas para fins de treinamento e orientação ou para investigações posteriores. Os seguintes pontos podem ajudar os trabalhadores de campo, que realizam tarefas críticas e perigosas, a trabalhar com segurança:

- Uma **solução para os trabalhadores isolados** fornece um aparelho capaz de acionar alarmes em caso de incidente, além de fornecer a localização do trabalhador. Esses dispositivos fornecem informações como man-down, ausência de movimento, cordão de segurança e um botão de emergência. Um servidor de notificação pode aumentar a capacidade de resposta e a segurança da equipe operacional em todas as instalações, encaminhando as chamadas para as equipes de emergência corretas. Os serviços de notificação também permitem a transmissão de mensagens em qualquer dispositivo para mobilização da equipe durante incidentes.
- Uma solução de **assistência visual remota (RVA)** permite comunicações viva-voz, com ampla interação entre o técnico local e os especialistas. Os serviços compreendem sessões de voz, vídeo e compartilhamento de documentos (fotos e vídeos), que podem ser recolhidos e centralizados.

Manter os ativos protegidos

Controles de acesso são essenciais para proteger as instalações contra crimes e ataques. Mas, as instalações de energia e serviços públicos são grandes e remotas, o que muitas vezes dificulta o monitoramento. A implementação dos seguintes pontos pode ajudar a supervisionar as atividades:

- **Câmeras de vigilância (CCTV)** fornecem uma visão global das entradas e saídas. O vídeo inteligente, usando IA e análises, pode ajudar a identificar movimentos suspeitos e correlacionar comportamentos em todas as instalações.
- **Sensores de proteção contra invasões** conectados à rede de dados substituem protocolos proprietários e sistemas de comunicação dedicados por sistemas IP fáceis de integrar.
- **Processos de alarme e fluxos de trabalho seguros** permitem que as operações monitorem alarmes de uma ampla gama de sensores (como detecção de incêndio, vazamentos de gás, temperatura e alta pressão) e sensores da Internet Industrial das Coisas (IIoT) simplificam o fluxo de notificações de alarme para a equipe operacional.
- Um **servidor de notificação de emergência** segue um script para iniciar a ação correta, que pode incluir notificação por meio de uma ampla variedade de dispositivos de telefonia, aplicativos de colaboração e interações da Internet das Coisas (IoT).
- **Os switches industriais e os access points** oferecem recursos de nível industrial, com desempenho superior e altamente seguros para aplicações de missão crítica executados em ambientes adversos e temperaturas extremas. Isso permite a implantação de redes em áreas onde é necessário fornecer conectividade física para soluções de segurança. Está em conformidade com certificações, é seguro contra ameaças cibernéticas e pode ser gerenciado remotamente.



Segurança cibernética além da rede

Ao procurar ameaças, você precisa pensar além da segurança física, já que muitas ameaças agora são digitais. Maquinário avançado e TO com muitos sistemas de sensores, como IIoT, estão se tornando mais conectados e trazendo eficiências operacionais. Às vezes, estão até conectados a uma Internet pública e podem representar um grave risco de segurança. Os hackers podem facilmente usar dispositivos comprometidos para obter acesso ao restante da rede da empresa. A necessidade de conectividade móvel, com aplicações sem fio e em nuvem, aumenta ainda mais as ameaças.

A **arquitetura da rede baseada em confiança zero** é eficaz, fácil de gerenciar e extremamente escalável. Promove a segurança muito além do perímetro da rede e baseia-se numa abordagem multi-layer para levar segurança a toda a rede, incluindo dispositivos individuais. Parte do pressuposto de que os invasores já estão presentes e sempre prontos para agir. Não há confiança implícita. Os mesmos altos níveis de proteção e segurança são aplicados igualmente a todas as pessoas internas e externas, sistemas, subsistemas, aplicativos e dispositivos que tentam acessar a rede. O acesso é estritamente limitado aos recursos necessários quando a solicitação é feita, e todos os recursos de rede são continuamente escaneados em busca de atividades incomuns ou maliciosas.

Uma rede baseada em confiança zero pode proteger contra ameaças de cibersegurança para manter a integridade dos sistemas de energia e serviços públicos, ao mesmo tempo em que oferece capacidades operacionais completas. Essa abordagem protege os outros recursos da organização, não apenas a rede, com foco na proteção do acesso aos recursos.

Uma arquitetura baseada em confiança zero

Os atributos de uma arquitetura de confiança zero incluem políticas de segurança avançadas, autenticação, identificação, segmentação e microssegmentação de dispositivos. Além disso, deve-se considerar:

- Elementos de segurança incorporados à arquitetura
- Criptografia nativa para manter a integridade do sistema
- Melhores práticas para autenticação interna e externa
- Auditorias regulares do sistema e uma política de senhas
- Capacidades de suporte de software que atualizam o código em resposta à detecção de ataques e vulnerabilidades.
- Certificação ISO 27001 para gestão de segurança da informação
- Switches industriais que são reforçados em termos de segurança e incluem tecnologias avançadas de segurança verificadas e validadas por organizações terceirizadas
- Um sistema operacional único e seguro para reduzir a superfície de ataque da organização, simplificar a atenuação de riscos e permitir a correção direcionada.
- Soluções que incluem as principais tecnologias de segurança, como Wi-Fi Protected Access 3 (WPA3), Shortest Path Bridging (SPB), criptografia MACsec, Address Space Layout Randomisation (ASLR) e controle de acesso à rede baseado em função



2. Aumentar a eficiência das operações

As operações de energia e serviços públicos geralmente abrangem grandes áreas geográficas em ambientes complexos, com recursos humanos e técnicos limitados para gerenciá-las. Sem conectividade ou comunicações, a energia não pode ser gerada, extraída ou distribuída, o que significa que não há serviços públicos. Tecnologia e inovação nas mãos de pessoas inovadoras possibilitarão modelos operacionais ágeis para atender a esses requisitos.

CCO: o cérebro nos bastidores

O Centro de Controle de Operações (CCO) gerencia o monitoramento diário, a direção e a coordenação das atividades operacionais de energia e serviços públicos para garantir a qualidade dos serviços. Inclui suporte de manutenção remota para identificar e responder a situações inesperadas que exigem atenção, coordenações e ações específicas, imediatas e eficientes.

Essas ações são necessárias para evitar atrasos inaceitáveis e recuperar-se de interrupções operacionais, para minimizar impactos negativos no atendimento ao cliente, nos custos e na segurança. Um CCO inteligente depende de conectividade, digitalização, comunicação e colaboração em tempo real.

Enfrentar os principais desafios do CCO requer três áreas principais para consideração, incluindo:

- **Um local de trabalho digital eficiente** para agentes do Centro de Controle de Operações (CCO) gerenciarem tarefas de atendimento e despacho de chamadas, e para funcionários em campo ou no escritório facilitarem o trabalho diário, de qualquer lugar, com qualquer dispositivo ou aplicativo, utilizando qualquer mídia.
- **Proteção completa de pessoal e ativos** por meio de recursos de gravação e soluções de gerenciamento de emergência.
- **Serviços inovadores e eficientes** conectando tudo; pessoas, objetos e aplicações.

Eficiência na gestão e manutenção

As tecnologias modernas, como a IoT e a digitalização, têm um vasto número de aplicações que contribuem para a eficiência das operações. Todos os dispositivos, sensores e atuadores requerem manutenção tanto das equipes de gerenciamento de TI quanto de operações. Entretanto, manter os componentes funcionando requer conectividade da rede, bem como controle rápido e capacidade de resposta remota. Ferramentas centralizadas de gerenciamento e manutenção preventiva podem ajudar os operadores de energia e serviços públicos a economizar tempo e reduzir o período de inatividade da rede.

Gerenciamento centralizado: Essa ferramenta gerencia a WLAN e a LAN e simplifica as operações. A análise centralizada também ajuda nas decisões proativas e preventivas para manter a integridade da rede, melhorar o tempo operacional e reduzir os custos. A interoperabilidade e uma arquitetura aberta (APIs) com outros sistemas (SCADA, por exemplo) permitem a qualidade do serviço, a segurança e o dimensionamento, além de fornecer uma base para a convergência de TI/TO.

Manutenção preditiva: Um ajudante nas operações de rede baseado em IA pode fornecer monitoramento da rede em tempo real, alertas de possíveis riscos e resolução de problemas de rede, maximizando a qualidade da experiência (QoE). A manutenção preventiva da rede significa estar atento às soluções, detectar problemas antes que eles apareçam e cuidar proativamente da sua rede.





3. Aumentar o engajamento do cliente

Hoje, os clientes desejam uma experiência personalizada, dados detalhados sobre o seu consumo, bem como informações sobre atualização e modificação de contratos. As organizações de energia e serviços públicos precisam digitalizar seus processos para aprimorar sua abordagem centrada no cliente, impulsionar seu serviço para garantir que as necessidades de seus clientes sejam uma prioridade máxima e reduzir o tempo de resposta. A solução a seguir pode ajudar a fornecer a experiência que os clientes atuais exigem:

- **Recepção automatizada:** um atendente automatizado visual proporciona uma imagem profissional, com recepcionista virtual disponível 24 horas por, 7 dias por semana, oferecendo uma resposta de qualidade aos seus clientes. Uma excelente experiência de serviço começa com um atendimento cortês e encaminha os chamadores diretamente para os funcionários, departamentos ou correio de voz. A interface de programação é intuitiva, com prompts que podem ser facilmente personalizados e regras de roteamento que se adaptam instantaneamente às novas necessidades de negócios.
- **Contact center multimídia:** hoje, os usuários desejam entrar em contato com suas operadoras por meio do canal de sua preferência; desde voz e e-mail até chat ao vivo no site da empresa ou nas redes sociais. Um contact center multimídia otimiza as interações omnicanal por meio de canais digitais e de voz, com qualidade, disponibilidade e eficiência. O contact center multimídia é baseado em uma solução de Contact Center como Serviço (CCaaS) que permite às organizações aproveitar o poder da nuvem ao mesmo tempo em que aproveitam seus investimentos em equipamentos de comunicação. O contact center multimídia também oferece assistência baseada em IA para respostas rápidas e precisas, resultando em resolução logo no primeiro contato e melhoria na experiência do cliente.
- **Conectores e aplicativos baseados na nuvem:** aprimore as interações com o cliente, integrando comunicações em aplicativos de negócios existentes, como Gerenciamento de Relacionamento com o Cliente (CRM) e ferramentas de gerenciamento de serviços de TI. A função "clique-para-ligar" permite que os usuários iniciem facilmente chamadas para serviços de suporte ao cliente. A integração do CPaaS no site do operador ou no aplicativo móvel permite que os usuários finais interajam com agentes por meio de chatbots, mensagens de texto, comunicações por voz e vídeo.

A ALE atende às necessidades do setor de energia e serviços públicos

Serviços para cada etapa da jornada

Serviços Alcatel-Lucent Enterprise para cada etapa do ciclo da implantação para acompanhar e complementar seu sistema ALE Business Partner ou o integrador de sistemas. Nossa variedade de serviços está disponível imediatamente ou adaptada a necessidades específicas, entregue no local ou remotamente sobre as soluções, e inclui:

- **Serviços profissionais** disponíveis no local e remotamente, desde o gerenciamento de projetos e definição de design até a implementação, em colaboração com seu Business Partner integrador de sistemas
- **Serviços de treinamento** para ajudar a desenvolver ou aprimorar suas habilidades, adotar novas tecnologias e tornar-se autônomo
- **Serviços gerenciados** que ampliam Business Partner ofertas de serviços com opções de serviços flexíveis para dar suporte às operações de rede dos clientes, 24 horas por dia, 7 dias por semana, com acordos de nível de serviço e monitoramento aprimorados
- **Serviços de suporte** para ajudar a manter a continuidade dos negócios com serviços de suporte 24 horas por dia, 7 dias por semana
- **Serviços de personalização** para facilitar sua transformação digital, com treinamento para ajudar sua equipe a desenvolver a aplicação específica de que você precisa, ou mesmo desenvolvê-la com base em nossos módulos de tecnologia
- Os **Serviços de gestão de sucesso** permitem acompanhar seus usuários finais durante sua transformação digital, com a adoção de soluções e benefícios, definindo critérios de sucesso, habilitando-os e iniciando qualquer um dos serviços acima sobre nossas soluções ALE, conforme necessário



Estudo de Caso

Ocala Fiber Network

A visão de fornecer serviços de banda larga gerou economia e forneceu conectividade vital para clientes dos setores de Educação e Saúde durante uma crise.



A Ocala Fiber Network, na Flórida, evoluiu a partir da concessionária de energia elétrica da cidade de Ocala, há duas décadas. Seu objetivo: fornecer uma variedade de serviços de Internet de banda larga com base na construção de uma rede 100% de fibra para agências da cidade e também para os cidadãos. A rede foi modernizada com switches Alcatel-Lucent Enterprise para oferecer velocidades mais altas, com melhor gerenciamento e desempenho de rede.

“Os switches OmniSwitch são a parte do cérebro que nos faz trabalhar. Todos os nossos switches ALE são vitais em todas as conexões e na entrega de serviços em nossa rede. A ALE oferece um grande equipamento. Meus engenheiros dizem que gostam da simplicidade e, o mais importante, do suporte que recebem.”

MEL POOLE, DIRETOR DA OCALA FIBER NETWORK

Os benefícios atuais incluem:

- Uma rede otimizada que oferece à OFN a capacidade de fornecer serviços mais amplos e maior largura de banda aos clientes
- O portfólio Alcatel-Lucent OmniSwitch® que permite à OFN aumentar o uso de forma integrada em tempos de crise
- Switches ALE preparados para o futuro que são 5 a 10 vezes mais rápidos que os switches de outros fornecedores

[Leia o estudo de caso completo](#)

e-Book

Abordagem de três pilares para enfrentar os desafios atuais de energia e serviços públicos



Soluções para hoje e amanhã

As soluções de energia e serviços públicos da Alcatel-Lucent

Enterprise abordam os desafios que as organizações enfrentam todos os dias, incluindo segurança e proteção, eficiência operacional e engajamento do cliente. Conectamos todos os subsistemas para permitir serviços mais inteligentes e ecológicos, com modelos “como serviço” (aaS) para passar de energia e serviços públicos conectados para serviços inteligentes. As soluções ALE proporcionam maior eficiência e minimizam o impacto ambiental antes, durante e depois da implementação, com:

- Produtos com consciência energética que requerem menos energia, gerenciam melhor a energia e reduzem a dissipação de calor
- Tamanho reduzido do hardware, componentes miniaturizados e portas densificadas
- Tecnologias de virtualização para eliminar completamente a necessidade de alguns hardwares
- Soluções em nuvem para reduzir os requisitos de espaço e energia
- Arquiteturas e ciclos de vida de produtos otimizados para máxima longevidade
- Materiais com embalagens ecologicamente corretas
- Conformidade com as diretrizes ambientais para o fim da vida útil e o descarte de produtos.
- Nosso programa Go Green combina nossos esforços com os de nossos fornecedores, parceiros e clientes para reduzir a poluição digital, melhorar o gerenciamento de resíduos e diminuir o consumo de energia em toda a cadeia de valor

Soluções da ALE para enfrentar os desafios do setor de Energia e Serviços Públicos

Soluções inovadoras da ALE, incluindo nossa família de switches industriais, recursos de comunicação e nuvem com middleware de aplicativos específicos para centros de controle, estão ajudando operadoras de energia e serviços públicos em todo o mundo a aumentar sua segurança, melhorar a eficiência e aprimorar suas interações com os clientes, com:

1. Conectividade por meio de nossas soluções de rede:

- Redes e infraestruturas de comunicação robustas e de missão crítica.
- Switches industriais de alta proteção para ambientes adversos
- Vigilância por vídeo e sensores de IoT para proteger pessoas e ativos
- Rede Zero Trust para reduzir as vulnerabilidades das ameaças cibernéticas
- Plataformas de manutenção preditiva usando integração baseada em IA
- Gerenciamento centralizado conectando todos os subsistemas de gerenciamento, assim como o SCADA
- Abertura para trabalhar em conjunto com outros aplicativos funcionais

- Validado pela ANSI e pelo DOD
- Zero emissões: Certificação e conformidade com a Responsabilidade Social Corporativa (CSR)
- Mais de 10 anos de serviços de suporte

2. Soluções de comunicação e colaboração:

- Centros de controle de operações inteligentes habilitados com comunicações avançadas
- Assistência visual remota entre o técnico no local e os especialistas remotos
- Atendente automático visual e centro de contato multimídia para aprimorar as interações.

3. Soluções de nuvem:

- Conectores API Rainbow e CPaaS para integrar as comunicações
- A solução de nuvem Rainbow™, da Alcatel-Lucent Enterprise implementada localmente com o Rainbow Edge
- API e SDK para implantações na nuvem



Saiba como as soluções da Alcatel-Lucent Enterprise estão ajudando o setor de energia e serviços públicos a enfrentar os desafios atuais.