

# Priorizando a resiliência e a segurança

## Soluções Alcatel-Lucent Enterprise para a Educação

Alcatel·Lucent



# Índice


Visão geral

Colaboração entre TI e TO em ambientes educacionais

Soluções de rede resilientes e seguras

Soluções de comunicação resilientes e seguras

Protegendo pessoas e ativos

Soberania e segurança dos dados



# Visão geral

Com o aumento dos desafios globais e dos riscos cibernéticos e físicos, os líderes das instituições de ensino devem priorizar a resiliência, a gestão de riscos e a sustentabilidade. As ameaças cibernéticas e físicas estão aumentando, e as instituições de ensino enfrentam expectativas cada vez maiores para manter os serviços em funcionamento, proteger dados confidenciais e garantir a segurança de alunos e funcionários.

De acordo com a Pesquisa sobre Violações de Segurança Cibernética 2025/26 do governo do Reino Unido, 98% das instituições de ensino superior relataram ter sofrido uma violação ou ataque cibernético nos últimos 12 meses, e 27% afirmaram que tais incidentes ocorreram quase semanalmente.[1] Nesse contexto, proteger a infraestrutura digital e física não é um luxo — é uma necessidade.

## Por que as TIC são mais essenciais do que nunca na educação

A educação passou por uma grande transformação digital, com as universidades oferecendo ensino híbrido, acesso remoto aos laboratórios e provas on-line. Os alunos esperam experiências digitais sempre disponíveis, sem interrupções e seguras. O corpo docente e os funcionários trabalham e colaboram cada vez mais a partir de vários locais. Enquanto isso, as universidades devem proteger volumes enormes de informações confidenciais, desde dados de pesquisa até registros pessoais.

A Alcatel-Lucent Enterprise apoia instituições de ensino em todo o mundo, compreendendo a importância de proteger pessoas, dados, ambientes de aprendizagem e operações. Nossas soluções são desenvolvidas com resiliência e privacidade em mente — desde salas de aula até laboratórios de pesquisa, de dormitórios até escritórios de segurança do campus. Este e-book oferece insights sobre resiliência e segurança para suas soluções de comunicações, nuvem e rede da Alcatel-Lucent Enterprise.

1 https://www.gov.uk/government/statistics/cyber-security-breaches-survey-20252026/cyber-security-breaches-survey-20252026-education-institutions-findings - Gov.uk, abril de 2026

# Colaboração entre TI e TO em ambientes educacionais

Antes de explorar como a Alcatel-Lucent Enterprise pode fortalecer sua resiliência e segurança, é importante reconhecer como a relação entre tecnologia da informação (TI) e tecnologia operacional (TO) está evoluindo nos ambientes universitários. Esses dois domínios não podem mais operar isoladamente. A colaboração é essencial para proteger e otimizar as ferramentas digitais que mantêm os campi em funcionamento — desde sistemas de climatização e iluminação até quadros interativos e equipamentos de laboratório habilitados para a Internet das Coisas (IoT).

Tomemos a Internet das Coisas (IoT) como exemplo: se as equipes de manutenção instalarem iluminação inteligente ou sensores de ocupação sem o envolvimento da TI, esses dispositivos podem rapidamente se tornar riscos à segurança. Muitos possuem proteções fracas ou inconsistentes, e a TI paralela em um campus inteligente pode abrir as portas para malware, vulnerabilidades de rede ou até mesmo violações de registros acadêmicos confidenciais.

Ao trabalharem juntas, as equipes de TI e TO ganham a visibilidade e o controle necessários para garantir a conformidade, aumentar a resiliência e criar uma base segura para a inovação em todo o campus.



# Soluções de rede resilientes e seguras

A rede do campus é a espinha dorsal de todos os serviços digitais, desde provas e aulas on-line até o acesso a bancos de dados de pesquisa e sistemas de alerta de emergência. Uma interrupção na rede poderia afetar milhares de alunos e professores, prejudicar a reputação da instituição ou comprometer a integridade da pesquisa.

As soluções de Redes da Era Digital da Alcatel-Lucent Enterprise são construídas com a resiliência em seu cerne. Desde uma arquitetura segura por design até segmentação embutida e controle de acesso, nossas redes são reforçadas para resistir a interrupções. Oferecemos visibilidade em todo o campus, integração automatizada para dispositivos confiáveis e gerenciamento simplificado, tudo sem custos ocultos ou licenças adicionais.

## 7 práticas recomendadas para suas soluções de rede

De aulas on-line e projetos de pesquisa a sensores de IoT em salas de aula inteligentes, o tempo de inatividade ou violações de segurança afetam diretamente o ensino, a aprendizagem e a confiança dos alunos. Abaixo estão sete práticas recomendadas que universidades e escolas podem adotar para melhorar a resiliência e a segurança em seus ambientes de TI e TO.

1. Manter os sistemas atualizados por meio do gerenciamento do ciclo de vida, revisando regularmente as soluções com os fornecedores de tecnologia para garantir que as versões mais recentes de software, patches de segurança e aprimoramentos sejam implementadas. Utilizar ferramentas de gerenciamento do ciclo de vida, como o Alcatel-Lucent ProActive Lifecycle Management (PALM), para acompanhar a obsolescência e os marcos de "fim de vida útil", de modo que as substituições de hardware possam ser orçadas e planejadas antes que se tornem urgentes.
2. Reforçar a segurança dos switches no nível do código, protegendo sua infraestrutura ao garantir que o sistema operacional da rede esteja fortificado. O Secure Diversified Code da Alcatel-Lucent randomiza a alocação de memória para reduzir os riscos de exploração. A Verificação e Validação Independentes (IVV) realizadas por especialistas terceirizados adicionam outra camada de confiança ao identificar e eliminar possíveis vulnerabilidades antes que elas cheguem à produção.
3. Aplicar uma estratégia de segurança de confiança zero à rede do seu campus, implementando macro e microssegmentação para isolar sistemas confidenciais (como registros de alunos e laboratórios de pesquisa) do tráfego geral. Seguir uma abordagem em fases (monitorar, validar, planejar, simular e aplicar) para evitar interrupções e, ao mesmo tempo, melhorar a resiliência.
4. Incorporar redundância com o Shortest Path Bridging para proporcionar failover rápido e redirecionamento dinâmico do tráfego em caso de falhas de link ou de dispositivos. Isso cria uma rede eficiente e automaticamente conteinerizada, reduzindo a complexidade do gerenciamento de múltiplas redes locais virtuais (VLANs) — uma vantagem importante ao escalar em grandes campi.
5. Utilizar os recursos de chassi virtual para aumentar a confiabilidade em áreas de missão crítica. Isso permite atualizações de software em serviço (ISSU) sem tempo de inatividade, oferecer suporte a topologias em anel ou em malha e simplifica o gerenciamento ao apresentar vários dispositivos como uma única unidade lógica — tudo isso mantendo os custos previsíveis.
6. Automatizar o backup e a restauração com ferramentas de gerenciamento de rede, como o Sistema de Gerenciamento de Rede OmniVista® da Alcatel-Lucent. O OmniVista Resource Manager simplifica os backups de configuração, a aplicação de políticas e os processos de restauração. A automação das tarefas do ciclo de vida garante uma recuperação mais rápida em caso de interrupções ou erros de configuração, reduzindo a pressão sobre pequenas equipes de TI em escolas e universidades.
7. Garantir a redundância dos roteadores implementando o Protocolo de Redundância de Roteadores Virtuais (VRRP) para proporcionar failover contínuo entre os roteadores. Isso evita pontos únicos de falha e garante acesso contínuo a aplicativos críticos, como plataformas LMS, ferramentas de colaboração ou sistemas de alerta de emergência.



## Invista em soluções de rede resilientes e seguras

Investir para garantir que sua rede seja resiliente e segura sempre faz sentido. No entanto, entender onde é melhor investir pode ser complexo e demorado — o planejamento é fundamental. Antes de começar, aqui estão algumas áreas-chave a serem consideradas para garantir que você obtenha a segurança e a resiliência de que sua organização precisa:

- Juntamente com seu parceiro de negócios, analise e atualize o projeto da rede para garantir que os requisitos da sua organização sejam refletidos na rede, incluindo o nível adequado de resiliência para áreas sensíveis e críticas que afetam serviços essenciais do campus. Para áreas críticas, considere adicionar servidores de backup e múltiplas conexões sempre que possível e aplicável.
- Melhore a resposta a incidentes utilizando recursos de inteligência artificial (IA) e aprendizado de máquina (ML) com o Alcatel-Lucent OmniVista Network Advisor. Essa ferramenta garante que os problemas sejam resolvidos antes que afetem os usuários finais, identificando e resolvendo proativamente problemas de rede ou de segurança. Ela agiliza o diagnóstico de falhas e melhora a segurança da rede por meio de auditorias de configuração e alertas em tempo real sobre quaisquer mudanças repentinas no comportamento da rede.
- Considere o uso de switches robustos para ambientes adversos. A família de switches Ethernet reforçados da Alcatel-Lucent Enterprise foi projetada especificamente para ter excelente desempenho em ambientes desafiadores e temperaturas extremas. Esses switches são construídos com componentes reforçados e alojados em gabinetes resistentes, garantindo durabilidade e confiabilidade, e possuem o mesmo sistema operacional que outros switches da Alcatel-Lucent Enterprise. Para aumentar a segurança e proteger informações confidenciais, alguns modelos são equipados com alertas de intrusão e relés de alarme que permitem a conexão de sistemas de alarme externos. Alguns modelos oferecem até mesmo suporte a MACsec (controle de acesso à mídia e segurança) para comunicações seguras de dados. Com a capacidade de chassi virtual nos switches reforçados, você pode obter maior redundância, resiliência e escalabilidade.
- Ofereça treinamento técnico da Alcatel-Lucent para a equipe operacional de rede, a fim de ajudá-la a detectar e reagir rapidamente aos problemas.

# Soluções de comunicação resilientes e seguras

As comunicações são essenciais para que as instituições de ensino interajam com alunos, funcionários e outras instituições, bem como para a divulgação de informações importantes. Os sistemas de comunicação devem estar disponíveis em momentos de crise, quando alunos e funcionários mais precisam da assistência do campus. A resiliência e a segurança estão em constante evolução, e revisões regulares ajudarão a manter sua solução de comunicações da Alcatel-Lucent Enterprise segura e disponível.

As soluções de comunicação da Alcatel-Lucent Enterprise são seguras desde a concepção. Isso significa que levamos em conta a segurança em todas as etapas do design, desenvolvimento e entrega do produto. Todo o hardware e os sistemas operacionais são reforçados, e a proteção contra ataques de negação de serviço (DoS) é integrada. Cumprimos certificações e acreditações reconhecidas para padrões globais de segurança e privacidade (ISO 27001, ISO 27017 e ISO 27018). Também seguimos normas de segurança e privacidade específicas do setor, como a Lei de Portabilidade e Responsabilidade do Seguro Saúde (HIPAA) nos EUA e a Hébergeurs de Données de Santé (HDS) para hospedagem de dados de saúde na França, bem como normas regionais de segurança e privacidade, como o Regulamento Geral de Proteção de Dados (GDPR) na União Europeia.

## 7 práticas recomendadas para suas soluções de comunicação

A seguir, apresentamos sete práticas recomendadas para garantir que você otimize totalmente a resiliência e a segurança de suas soluções de comunicação da Alcatel-Lucent Enterprise..

1. Analisar regularmente o status do sistema com seu parceiro de negócios para garantir que a versão mais recente do software, os patches e as melhorias de segurança estejam instalados e que seu contrato SPS esteja em dia.
2. Analisar regularmente os componentes de segurança e continuidade de serviço no seu Sistema de Gerenciamento de Rede Alcatel-Lucent OmniVista 8770, que inclui informações e recursos valiosos de resiliência e segurança para sua solução de comunicações.
   - Considerar o backup remoto automatizado do sistema para evitar a perda de dados de configuração.
   - Configurar o monitoramento de alarmes e certificar-se de que ele seja atualizado regularmente com os limites corretos. Além disso, verificar se as notificações sobre falhas no sistema de comunicação ou alertas de qualidade sejam enviadas às pessoas responsáveis.
3. Revisar e aplicar uma política robusta de senhas, de preferência utilizando autenticação externa (servidor RADIUS) e implementar alertas aos usuários para ajudar a prevenir fraudes nas tarifas, que ainda representam uma ameaça em muitos países.
4. Treinar os funcionários e certificar-se de que estejam cientes dos riscos e das medidas de prevenção.
5. Analisar os servidores de aplicativos essenciais aos negócios quanto à condição, adequação e capacidade de manutenção.
6. Considerar uma VLAN específica para voz. Separar os dados de voz do restante do tráfego reduz a chance de contaminação, o que poderia interromper as operações e, potencialmente, os serviços do campus.
7. Certificar-se de que seus Controladores de Borda de Sessão (SBCs) estejam configurados corretamente. Os requisitos podem ter sido alterados ao longo do tempo.



## Invista em soluções de comunicação resilientes e seguras

Os campi modernos precisam de sistemas de comunicação que estejam sempre disponíveis, seja para ensino, pesquisa ou alertas de emergência. À medida que as instituições planejam soluções de última geração, eis as principais áreas a serem priorizadas:

- Implemente servidores de chamadas e serviços de aplicativos duplicados em locais de missão crítica, como clínicas de saúde, dormitórios e centros de pesquisa. A redundância garante que a comunicação permaneça disponível mesmo que um sistema falhe, salvaguardando o bem-estar dos alunos e a continuidade operacional.
- Garanta que a cobertura de DECT (Digital Enhanced Cordless Telecommunications) ou Wi-Fi inclua não apenas salas de aula, mas também áreas sensíveis e de difícil acesso, como laboratórios, centros de dados e zonas externas. A cobertura abrangente dá suporte tanto ao aprendizado diário quanto às comunicações de emergência.
- Utilize ferramentas como o Alcatel-Lucent Visual Notification Assistant ou o Rainbow™ para criar fluxos de trabalho com acionamentos automáticos, sejam eles provenientes de pessoas, dispositivos IoT ou sistemas. Isso garante que as pessoas-chave sejam notificadas imediatamente sobre problemas, permitindo uma resposta e recuperação mais rápidas.
- Implemente o Rainbow™ da Alcatel-Lucent, a ferramenta colaborativa ideal para complementar as soluções de comunicação da Alcatel-Lucent Enterprise. O Rainbow oferece voz, vídeo, mensagens e compartilhamento de arquivos de forma segura, dando suporte ao ensino híbrido, ao corpo docente móvel e à colaboração remota. Sua arquitetura híbrida (na nuvem e no local) garante resiliência ao operar a partir de diferentes locais, mantendo as comunicações abertas mesmo durante interrupções locais. Recursos como compartilhamento de imagens e vídeos, incluindo imagens de vigilância, aprimoram a percepção situacional tanto para casos de uso acadêmicos quanto de segurança.
- Para instituições com requisitos rigorosos de governança de dados, o Rainbow Edge pode ser implantado em uma nuvem privada ou regional, garantindo a conformidade com políticas de dados acadêmicas ou nacionais e, ao mesmo tempo, oferecendo recursos modernos de colaboração.
- A Alcatel-Lucent oferece soluções flexíveis para o ensino à distância, professores móveis e equipes híbridas, a fim de oferecer comunicação de voz, vídeo e colaboração seguros, de qualquer lugar, incluindo:
  - Rainbow para colaboração baseada em nuvem.
  - SoftPhone IP para desktop/SoftPhone para equipes remotas ou híbridas.
  - O DeskPhone com VPN integrada pode ser implantado em massa para implantações seguras e em grande escala.



# Protegendo pessoas e ativos

Um campus inteligente é mais do que internet rápida – é um ambiente conectado onde a tecnologia protege ativamente os alunos, os funcionários e os recursos essenciais. Ao integrar comunicações, IoT e análises de dados, as universidades e escolas podem ir além de uma abordagem reativa e criar uma cultura de segurança proativa.

As informações em tempo real desempenham um papel central. Alarmes de incêndio, detectores de movimento, sistemas de controle de acesso ou análises de vídeo baseadas em IA podem acionar automaticamente alertas para equipes de segurança ou gerentes de instalações, reduzindo os tempos de resposta e evitando que pequenos incidentes se agravem. Em vez de esperar que os problemas sejam relatados, as instituições podem antecipar riscos e agir imediatamente, seja isolando um prédio, direcionando a equipe de manutenção para um sistema de HVAC com defeito, ou respondendo a uma atividade suspeita.

O verdadeiro valor surge quando dados, fluxos de trabalho e comunicações se unem. Ferramentas como o Rainbow e o Visual Notification Assistant podem conectar pessoas, sistemas e dispositivos de IoT em fluxos de trabalho automatizados, garantindo que a informação certa chegue às pessoas certas no momento certo. Essa abordagem sensível ao contexto melhora a tomada de decisões, aprimora a percepção da situação e, em última instância, fortalece tanto a segurança quanto a resiliência operacional.

Proteger os ativos é quase tão importante quanto proteger as pessoas. Com recursos como o rastreamento de ativos, os campi podem localizar equipamentos valiosos de pesquisa em mapas interativos, melhorando a utilização e, ao mesmo tempo, reduzindo o risco de perda ou roubo. As comunicações gravadas e os registros de ações também simplificam a análise pós-evento, ajudando as instituições a fortalecerem seus processos de segurança e a atenderem aos requisitos de conformidade.

Para viabilizar esses recursos, é essencial uma base sólida. Cobertura Wi-Fi onipresente, integração segura da IoT e sistemas de comunicação resilientes fornecem a espinha dorsal que sustenta tudo, desde salas de aula e dormitórios até laboratórios de pesquisa e instalações ao ar livre. Dessa forma, a resiliência e a segurança tornam-se parte natural das operações diárias do campus, transformando a tecnologia em uma aliada confiável para a segurança, a eficiência e a inovação.



# Soberania e segurança dos dados

Proteger informações confidenciais, como registros de alunos, dados de pesquisa e informações de saúde, exige conformidade rigorosa e práticas robustas de segurança cibernética. Na Alcatel-Lucent Enterprise, nós:

- Seguimos as melhores práticas do Instituto Nacional de Ciência e Tecnologia (NIST) para avaliações de risco em novos recursos e ao implementar recursos de segurança cibernética, como criptografia nativa, em nossas soluções
- Possuímos a certificação Common Criteria EAL2+
- Aplicamos as normas ISO 27001 a todas as nossas soluções baseadas em nuvem
- Oferecemos suporte a ZTNA, segmentação granular da rede e políticas de segurança altamente específicas para reduzir o risco de atividades não autorizadas
- Realizamos testes altamente especializados e específicos de segurança, como testes de penetração, em nossos produtos
- Garantimos que nossos produtos obtenham as principais certificações do setor, como HDS, HIPAA e a Lei de Direitos Educacionais e Privacidade da Família (FERPA)

Como especialistas reconhecidos em segurança cibernética, contribuímos para as propostas da União Europeia relativas a diretivas de segurança cibernética. Também aproveitamos nossa expertise em segurança cibernética para ajudar os clientes a escolher e implementar a combinação certa de soluções seguras de comunicações unificadas e colaboração para atender às suas necessidades, além de treinar seus funcionários nas melhores práticas de segurança cibernética.

Ao combinar soluções certificadas, gestão proativa de riscos e conscientização da equipe, universidades e escolas podem garantir a soberania dos dados, mantendo a conformidade e a confiança.

**www.al-enterprise.com**

© 2026 ALE International, ALE USA Inc. Todos os direitos reservados em todos os países. O nome e o logotipo da Alcatel-Lucent são marcas comerciais da Nokia usadas sob licença pela ALE. Para ver uma lista de marcas registradas proprietárias da ALE, acesse: www.al-enterprise.com/pt-br/legal/trademarks-copyright. Algumas imagens neste documento podem ter sido geradas com IA e têm apenas fins ilustrativos. DID25060501PTBR (setembro 2026)

Alcatel·Lucent