



Tornar a resiliência e a segurança uma prioridade

Soluções Alcatel-Lucent Enterprise para o setor de Educação

Índice

- | Visão geral
- | Colaboração de TI/TO em ambientes educacionais
- | Soluções de rede resilientes e seguras
- | Soluções de comunicação resilientes e seguras
- | Proteção do seu pessoal e dos seus ativos
- | Soberania e segurança dos dados



Visão geral

Com os crescentes desafios globais e o aumento dos riscos cibernéticos e físicos, os líderes universitários devem colocar a resiliência, a gestão de riscos e a sustentabilidade entre suas principais prioridades. As ameaças cibernéticas e físicas estão em constante crescimento, e as instituições de ensino enfrentam expectativas cada vez maiores de manter seus serviços operando sem interrupções, proteger dados confidenciais e garantir a segurança de alunos e colaboradores. Segundo a EdTech Magazine, os ataques cibernéticos contra universidades aumentaram 70% em 2023.¹ Nesse contexto, proteger a infraestrutura digital e física não é um luxo, é uma necessidade.

Por que as TIC são mais críticas do que nunca na educação

A educação passou por uma grande mudança digital, com universidades oferecendo aprendizado híbrido, acesso remoto a laboratórios e exames digitais. Os alunos

esperam experiências digitais sempre ativas, contínuas e seguras. Professores e funcionários trabalham e colaboram cada vez mais em vários locais. Enquanto isso, as universidades precisam proteger um grande volume de informações sensíveis, que vão desde dados de pesquisa até registros pessoais.

A Alcatel-Lucent Enterprise apoia instituições de ensino em todo o mundo, reconhecendo a importância de proteger pessoas, dados, ambientes de aprendizagem e operações. Nossas soluções são desenvolvidas com foco em resiliência e privacidade — abrangendo desde salas de aula e laboratórios de pesquisa até dormitórios e escritórios de segurança nos campi. Este e-Book fornece insights sobre resiliência e segurança para suas soluções de rede, nuvem e comunicações ALE.

¹ [Ciberataques contra os governos aumentaram 95% no último semestre de 2022, diz CloudSek](#). CSO Estados Unidos, Janeiro de 2023.

² <https://www2.deloitte.com/uk/en/insights/industry/public-sector/government-digital-transformation-strategy.html>.

e-Book

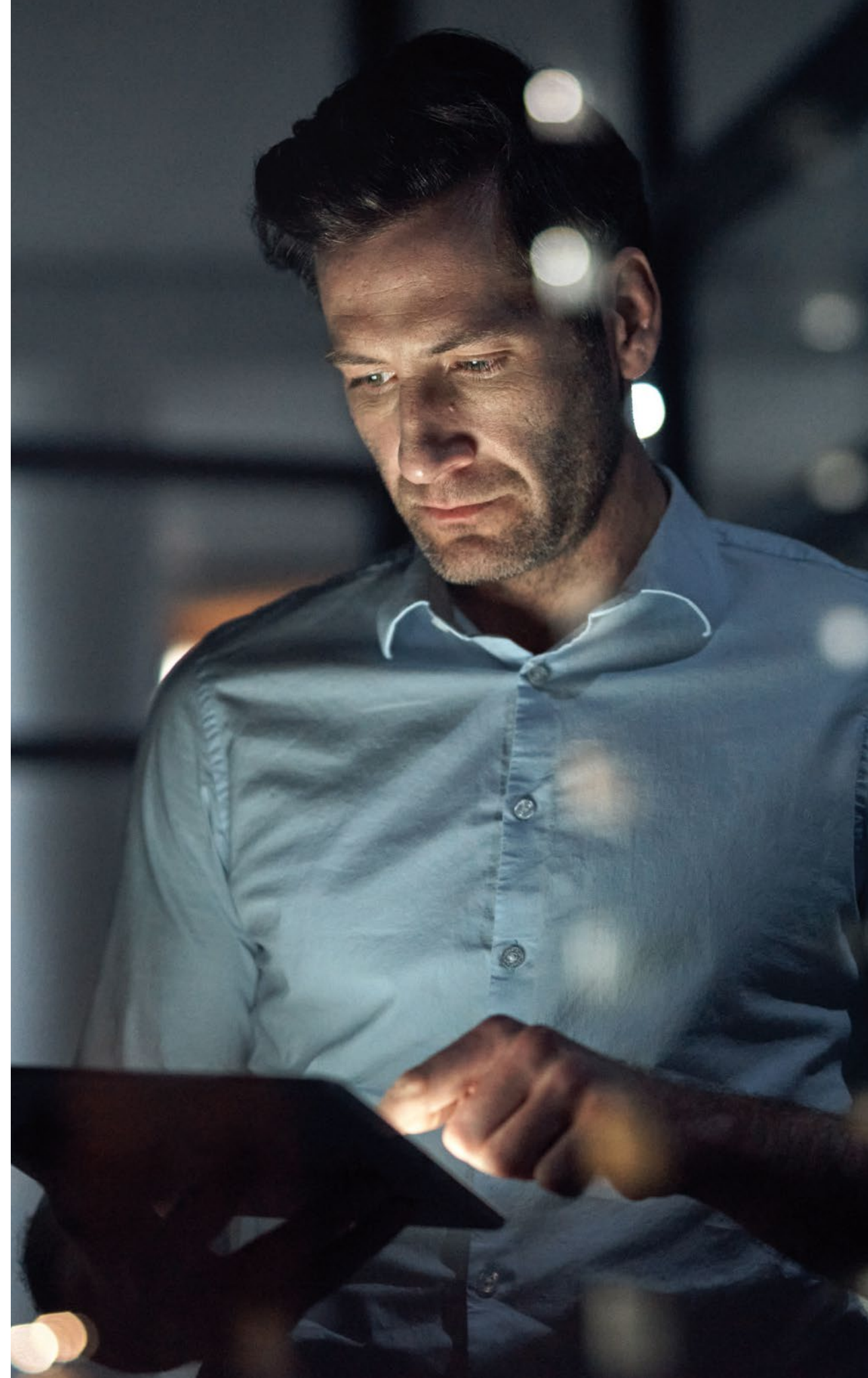
Tornar a resiliência e a segurança uma prioridade

Colaboração de TI/TO em ambientes educacionais

Antes de explorarmos como a Alcatel-Lucent Enterprise pode fortalecer a resiliência e a segurança da sua instituição, é importante entender como a relação entre a tecnologia da informação (TI) e a tecnologia operacional (TO) vem evoluindo nos ambientes universitários. Esses dois domínios não podem mais operar isoladamente. A colaboração é fundamental para proteger e otimizar as ferramentas digitais que mantêm os campi em funcionamento, abrangendo desde sistemas de HVAC e iluminação até quadros interativos e equipamentos de laboratório conectados via IoT.

Tomemos como exemplo a Internet das Coisas (IoT): se as equipes de infraestrutura implementarem sensores inteligentes de iluminação ou ocupação sem o envolvimento da equipe de TI, esses dispositivos podem rapidamente se transformar em potenciais riscos de segurança. Muitos desses dispositivos apresentam proteções fracas ou inconsistentes, e a TI paralela em um campus inteligente pode abrir portas para malware, vulnerabilidades de rede ou até mesmo para a exposição de registros acadêmicos confidenciais.

Ao trabalharem de forma integrada, as equipes de TI e TO obtêm a visibilidade e o controle necessários para garantir a conformidade, fortalecer a resiliência e estabelecer uma base segura para a inovação em todo o campus.



Soluções de rede resilientes e seguras

A rede do campus constitui a espinha dorsal de todos os serviços digitais, abrangendo desde exames e palestras online até o acesso a bancos de dados de pesquisa e sistemas de alerta de emergência. Uma queda na rede pode afetar milhares de alunos e professores, prejudicar a reputação da instituição ou comprometer a integridade das pesquisas.

As soluções de Redes da Era Digital da ALE são construídas com base na resiliência. Da arquitetura segura por design à segmentação incorporada e controle de acesso, nossas redes são reforçadas para resistir a interrupções. Oferecemos visibilidade completa 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. Mantenha os sistemas atualizados com o gerenciamento do ciclo de vida, revisando regularmente as soluções com provedores de tecnologia para garantir que as versões mais recentes do software, patches de segurança e aprimoramentos sejam aplicados. Use ferramentas de gerenciamento de ciclo de vida como o ALE ProActive Lifecycle Management (PALM) para rastrear marcos de obsolescência e fim de vida útil, para que as substituições de hardware possam ser orçadas e planejadas antes que se tornem urgentes.
2. Fortaleça a segurança do switch no nível do código, protegendo sua infraestrutura ao garantir que o sistema operacional da rede esteja reforçado. O Secure Diversified Code da ALE randomiza a alocação de memória para reduzir riscos de exploração. A Verificação e Validação Independentes (IVV) por especialistas terceirizados acrescenta outra camada de confiança ao identificar e eliminar potenciais vulnerabilidades antes que elas cheguem à produção.
3. Implemente uma estratégia de segurança de confiança zero na rede do seu campus, utilizando macro e microsegmentação para isolar sistemas sensíveis — como registros de alunos e laboratórios de pesquisa — do tráfego geral. Adote uma abordagem em fases — monitorar, validar, planejar, simular e implementar — para evitar interrupções e, simultaneamente, aumentar a resiliência.
4. Crie redundância com Shortest Path Bridging para oferecer failover rápido e redirecionamento dinâmico de tráfego em caso de falhas do link ou dispositivo. Isso gera uma rede eficiente e automaticamente containerizada, reduzindo a complexidade do gerenciamento de múltiplas redes locais virtuais (VLANs) — uma vantagem significativa ao expandir operações em grandes campi.
5. Use 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, oferece suporte a topologias em anel ou malha e simplifica o gerenciamento ao apresentar vários dispositivos como uma unidade lógica, tudo isso mantendo os custos previsíveis.
6. Automatize o backup e a restauração com ferramentas de gerenciamento de rede como o Alcatel-Lucent OmniVista® Network Management System. O OmniVista Resource Manager simplifica os backups de configuração, a aplicação de políticas e os processos de restauração. A automatização de tarefas do ciclo de vida garante uma recuperação mais rápida caso ocorram interrupções ou configurações incorretas, reduzindo a pressão sobre pequenas equipes de TI em escolas e universidades.
7. Garanta a redundância do roteador implementando o Protocolo de Redundância de Roteador Virtual (VRRP) para fornecer failover contínuo entre 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.



Investir em soluções de rede resilientes e seguras

Investir para garantir que sua rede seja resiliente e segura sempre faz sentido. Entretanto, entender onde investir melhor pode ser complexo e levar tempo. Planejamento é fundamental. Antes de começar, aqui estão algumas áreas importantes a serem consideradas para garantir que você obtenha a segurança e a resiliência que sua organização precisa:

- Juntamente com seu parceiro de negócios, revise e atualize o design da rede para garantir que os requisitos da sua organização sejam refletidos na rede, incluindo o nível apropriado de resiliência para áreas sensíveis e críticas que afetam os 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 abordando proativamente problemas de rede ou segurança. Ela agiliza a solução de problemas e melhora a segurança da rede

por meio de auditorias de configuração e administração de alertas em tempo real sobre quaisquer mudanças repentinas no comportamento da rede.

- Considere usar [switches reforçados](#) para ambientes adversos. A família Alcatel-Lucent Enterprise de switches Ethernet robustos foi projetada especificamente para se destacar em ambientes desafiadores e temperaturas extremas. Esses switches são construídos com componentes robustos e alojados em gabinetes resistentes, garantindo durabilidade e confiabilidade, além de terem o mesmo sistema operacional dos outros switches ALE. Para aumentar a segurança e proteger informações sigilosas, alguns modelos são equipados com alertas de intrusão e relés de alarme que permitem a conexão de sistemas de alarme externos. Alguns modelos até suportam MACsec (controle de acesso à mídia e segurança) para comunicações de dados seguras. Com o recurso de chassi virtual em switches robustos, você pode obter redundância, resiliência e escalabilidade aprimoradas.
- Forneça [treinamento técnico ALE](#) para a equipe operacional da rede para ajudá-los a detectar e reagir rapidamente aos problemas

Soluções de comunicação resilientes e seguras

As comunicações são cruciais para que as instituições educacionais possam interagir com estudantes, funcionários e outras instituições, além de serem essenciais para o envio de informações importantes. Sistemas de comunicação devem estar disponíveis em tempos de crise, quando estudantes e funcionários mais precisam de assistência no campus. A resiliência e a segurança estão evoluindo, e revisões regulares ajudarão a manter sua solução de comunicação Alcatel-Lucent Enterprise sempre segura e disponível.

As soluções de comunicação da ALE são seguras desde a concepção. Isso significa que consideramos a segurança em cada etapa da definição, do desenvolvimento e da entrega do produto. Todo o hardware e os sistemas operacionais são reforçados, e a proteção contra ataques de negação de serviço (DoS) está integrada. Estamos em conformidade com certificações e creditações reconhecidas para padrões globais de segurança e privacidade (ISO 27001, ISO 27017 e ISO 27018). Também seguimos padrões específicos de segurança e privacidade do setor, como a Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA) nos Estados Unidos e o Hôbergeurs de Données de Santé (HDS) para hospedagem de dados de saúde na França, além de padrões regionais de segurança e privacidade, como o Regulamento Geral sobre a Proteção de Dados (GDPR) na União Europeia.

7 Práticas recomendadas para suas soluções de comunicação

A seguir estão sete práticas recomendadas para garantir que você otimize totalmente a resiliência e a segurança das suas soluções de comunicação ALE.

1. Analise regularmente o status do sistema com seu parceiro de negócios para garantir que a versão mais recente do software, os patches e as atualizações de segurança estejam instalados e que seu contrato de SPS esteja atualizado.
2. Revise regularmente os componentes de segurança e continuidade de serviço em seu [Alcatel-Lucent OmniVista 8770 Network Management System](#), que inclui informações e recursos valiosos de resiliência e segurança para sua solução de comunicações.
 - Considere o backup automatizado do sistema remoto para evitar a perda de dados de configuração
 - Configure o monitoramento de alarmes e garanta que ele seja atualizado regularmente com os limites corretos. Além disso, verifique se as notificações de falhas no sistema de comunicação ou alertas de qualidade estão sendo enviados para os indivíduos certos
3. Revise e aplique uma política de senha forte, de preferência usando autenticação externa (servidor RADIUS) e defina lembretes para os usuários para ajudar a evitar toll fraud (fraude de chamadas), que ainda são uma ameaça em muitos países.
4. Treine os funcionários e garantir que estejam cientes dos riscos e das medidas de prevenção.
5. Analise os servidores de aplicativos essenciais aos negócios quanto à condição, adequação e capacidade de serviço.
6. Considere uma VLAN específica para voz. Separar os dados de voz de outros tipos de tráfego reduz a chance de contaminação, o que poderia interromper operações e, potencialmente, os serviços do campus.
7. Certifique-se de que seus Session Border Controllers (SBCs) estejam configurados corretamente. Os requisitos podem ter mudado ao longo do tempo.



Investir 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, aqui estão as principais áreas a serem priorizadas:

- Implante servidores de chamadas duplicados e serviços de aplicativos em locais de missão crítica, como clínicas de saúde, dormitórios e centros de pesquisa. A redundância garante que a comunicação permaneça disponível mesmo se um sistema falhar, protegendo o bem-estar dos alunos e a continuidade operacional.
- Garanta que a cobertura de DECT ou Wi-Fi inclua não apenas salas de aula, mas também áreas sensíveis e de difícil acesso, como laboratórios, data centers e áreas externas. A cobertura abrangente oferece suporte tanto ao aprendizado diário quanto às comunicações de emergência.
- Use ferramentas como o Alcatel-Lucent Visual Notification Assistant ou o Rainbow™ para criar fluxos de trabalho com gatilhos automáticos, sejam de pessoas, dispositivos IoT ou sistemas. Isso garante que o pessoal-chave seja notificado imediatamente sobre os problemas, permitindo resposta e recuperação mais rápidas.
- Implemente o [Rainbow™ da Alcatel-Lucent Enterprise](#), a ferramenta colaborativa ideal para complementar as soluções de comunicação da ALE. O Rainbow oferece comunicação segura por voz, vídeo, mensagens e compartilhamento de arquivos, dando suporte ao ensino híbrido, professores em mobilidade e à colaboração remota. Sua arquitetura híbrida (nuvem e on-premises) garante resiliência ao operar em múltiplas localidades, mantendo as comunicações ativas mesmo durante interrupções locais. Recursos como compartilhamento de imagens e vídeos, incluindo feeds de vigilância, aumentam a conscientização situacional tanto para finalidades acadêmicas quanto de segurança.
- Para instituições com requisitos rigorosos de governança de dados, o Rainbow Edge pode ser implementado em uma nuvem privada ou regional, garantindo conformidade com as políticas de dados acadêmicas ou nacionais, enquanto fornece recursos modernos de colaboração.
- A ALE oferece soluções flexíveis para ensino remoto, corpo docente móvel e configurações de equipe híbrida para oferecer suporte seguro de voz, vídeo e colaboração de qualquer lugar, incluindo:
 - Rainbow para colaboração baseada em nuvem
 - [IP Desktop SoftPhone/SoftPhone para funcionários remotos ou híbridos](#)
 - [O DeskPhone com VPN incorporada pode ser implantado em massa](#) para instalações seguras em larga escala.

e-Book

Tornar a resiliência e a segurança uma prioridade



Proteger seu pessoal e seus ativos

Um campus inteligente vai além de uma internet rápida: é um ambiente conectado onde a tecnologia protege de forma ativa alunos, colaboradores e recursos essenciais. Ao integrar comunicações, IoT e análises, universidades e escolas podem superar uma abordagem reativa e fomentar uma cultura de segurança proativa.

Informações em tempo real desempenham um papel central. Alarmes de incêndio, detectores de movimento, sistemas de controle de acesso e análises de vídeo baseadas em IA podem disparar alertas automaticamente para equipes de segurança ou gestores de instalações, reduzindo os tempos de resposta e evitando que pequenos incidentes se transformem em problemas maiores. Em vez de aguardar que os problemas sejam reportados, as instituições podem antecipar riscos e agir imediatamente, seja fechando um prédio, direcionando a manutenção para um sistema HVAC com falha ou respondendo a atividades suspeitas.

O verdadeiro valor surge quando dados, fluxos de trabalho e comunicações se unem. Ferramentas como Rainbow e Visual Notification Assistant podem conectar pessoas, sistemas e dispositivos IoT em fluxos de trabalho automatizados,

garantindo que as informações corretas cheguem às pessoas certas no momento certo. Essa abordagem baseada em contexto melhora a tomada de decisões, aumenta a consciência situacional e, por fim, fortalece a segurança e a resiliência operacional.

Proteger ativos é quase tão importante quanto proteger pessoas. Com recursos como rastreamento de ativos, os campi podem localizar equipamentos de pesquisa valiosos em mapas interativos, otimizando sua utilização e reduzindo o risco de perda ou roubo. As comunicações registradas e os históricos de ações também facilitam a análise pós-evento, ajudando as instituições a aprimorar seus processos de segurança e a cumprir os requisitos de conformidade.

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



Soberania e segurança dos dados

Proteger informações confidenciais, como registros de alunos, dados de pesquisa e informações de saúde, exige conformidade rigorosa e fortes práticas de segurança cibernética. Na ALE, nós:

- Seguimos as práticas recomendadas do Instituto Nacional de Ciência e Tecnologia (NIST) para avaliações de risco em nossas soluções, seja para novas funções ou ao implementar recursos de segurança cibernética, como criptografia nativa.
- Temos a certificação Common Criteria EAL2+ (Avaliação de Garantia de Nível 2 ou superior).
- Aplicamos as normas ISO 27001 a todas as nossas soluções baseadas em nuvem.
- Apoiamos a ZTNA, segmentação de rede granular e políticas de segurança altamente específicas para reduzir o risco de atividades não autorizadas.

- Executamos em nossos produtos testes de segurança altamente especializados e específicos, como testes de penetração.
- Garantimos que nossos produtos obtenham as principais certificações do setor, como HDS, HIPAA e Lei de Privacidade e Direitos Educacionais da Família (FERPA).

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

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

