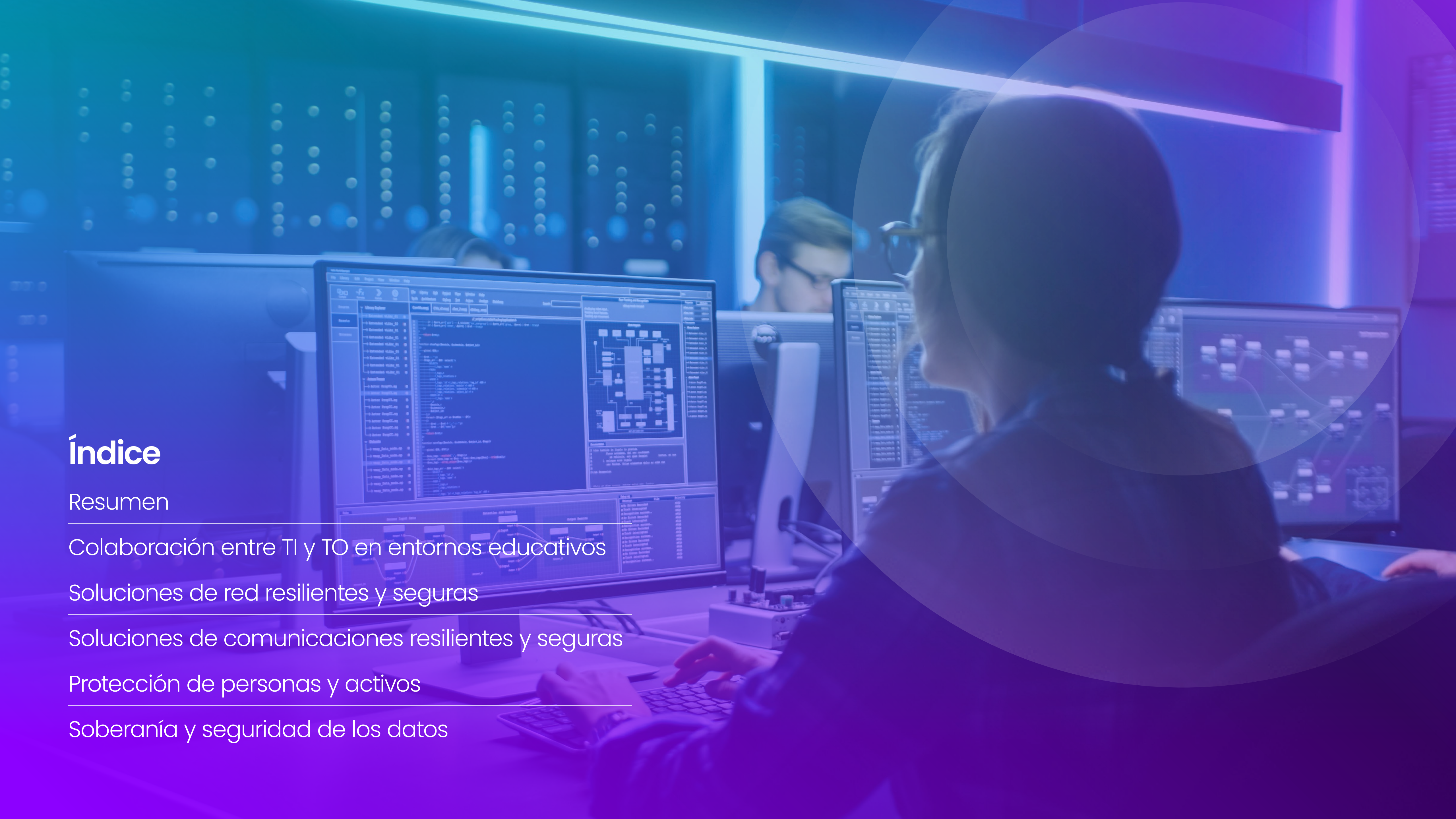


Dar prioridad a la resiliencia y la seguridad

Soluciones de Alcatel-Lucent
para el sector educativo

Alcatel-Lucent 



Índice

Resumen

Colaboración entre TI y TO en entornos educativos

Soluciones de red resilientes y seguras

Soluciones de comunicaciones resilientes y seguras

Protección de personas y activos

Soberanía y seguridad de los datos



Resumen

Ante los crecientes retos globales y el aumento de los riesgos cibernéticos y físicos, los responsables de los campus deben dar prioridad a la resiliencia, la gestión de riesgos y la sostenibilidad. Las amenazas cibernéticas y físicas van en aumento, y las instituciones educativas se enfrentan a unas expectativas cada vez mayores para mantener los servicios en funcionamiento, proteger los datos sensibles y garantizar la seguridad de los estudiantes y del personal.

Según la Encuesta sobre Incidentes de Ciberseguridad 2025/26 del Gobierno del Reino Unido, el 98 % de las instituciones de educación superior declararon haber sufrido un incidente o ataque cibernético en los últimos 12 meses, y el 27 % afirmó

que dichos incidentes se producían casi semanalmente.¹ En este contexto, proteger la infraestructura digital y física no es un lujo, sino una necesidad.

Por qué las TIC son más importantes que nunca en la educación

La educación ha experimentado una importante transformación digital, y las universidades ofrecen ahora aprendizaje híbrido, acceso remoto a los laboratorios y exámenes digitales. Los estudiantes esperan experiencias digitales siempre disponibles, fluidas y seguras. El profesorado y el personal trabajan y colaboran cada vez más desde

múltiples ubicaciones. Mientras tanto, las universidades deben proteger enormes volúmenes de información confidencial, desde datos de investigación hasta expedientes personales.

Alcatel-Lucent presta apoyo a instituciones educativas de todo el mundo, consciente de la importancia de proteger a las personas, los datos, los entornos de aprendizaje y las operaciones. Nuestras soluciones se han diseñado teniendo en cuenta la resiliencia y la privacidad, desde las aulas hasta los laboratorios de investigación, pasando por las residencias de estudiantes y las oficinas de seguridad del campus. Este libro electrónico ofrece información sobre la resiliencia y la seguridad de sus soluciones de comunicaciones, nube y redes de Alcatel-Lucent.

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

Colaboración entre TI y TO en entornos educativos

Antes de analizar cómo Alcatel-Lucent puede reforzar su resiliencia y seguridad, es importante comprender cómo está evolucionando la relación entre la tecnología de la información (TI) y la tecnología operativa (TO) en los entornos universitarios. Estos dos ámbitos ya no pueden funcionar de forma aislada. La colaboración es esencial para proteger y optimizar las herramientas digitales que mantienen en funcionamiento los campus, desde los sistemas de climatización y la iluminación hasta las pizarras inteligentes y los equipos de laboratorio conectados al Internet de las cosas (IoT).

Tomemos como ejemplo el Internet de las cosas (IoT): si los equipos de mantenimiento instalan iluminación inteligente o sensores de ocupación sin la participación de TI, estos dispositivos pueden convertirse rápidamente en riesgos de seguridad. Muchos cuentan con medidas de seguridad débiles o inconsistentes, y la «TI en la sombra» en un campus inteligente puede abrir la puerta al malware, a vulnerabilidades de red o incluso a filtraciones de expedientes académicos confidenciales.

Al trabajar juntos, los equipos de TI y de tecnología operativa (OT) obtienen la visibilidad y el control que necesitan para garantizar el cumplimiento normativo, mejorar la resiliencia y crear una base segura para la innovación en todo el campus.



Soluciones de red resilientes y seguras

La red del campus es la columna vertebral de todos los servicios digitales, desde exámenes y clases en línea hasta el acceso a bases de datos de investigación y los sistemas de alertas de emergencia. Una interrupción de la red podría afectar a miles de estudiantes y profesores, dañar la reputación de la institución o comprometer la integridad de la investigación.

Las soluciones de redes para la era digital de Alcatel-Lucent se han diseñado teniendo la resiliencia como eje central. Desde una arquitectura segura por diseño hasta la segmentación integrada y el control de acceso, nuestras redes están reforzadas para resistir las interrupciones. Ofrecemos visibilidad en todo el campus, incorporación automatizada de dispositivos de confianza y una gestión simplificada, todo ello sin costes ocultos ni licencias adicionales.

7 prácticas recomendadas para tus soluciones de red

Desde clases en línea y proyectos de investigación hasta sensores de IoT en aulas inteligentes, los tiempos de inactividad o las brechas de seguridad afectan directamente a la enseñanza, el aprendizaje y la confianza de los estudiantes. A continuación se presentan siete prácticas recomendadas que las universidades y centros educativos pueden adoptar para mejorar la resiliencia y la seguridad en sus entornos de TI y TO.

1. Mantenga los sistemas actualizados mediante la gestión del ciclo de vida, revisando periódicamente las soluciones con los proveedores de tecnología para garantizar que se apliquen las últimas versiones de software, parches de seguridad y mejoras. Utiliza herramientas de gestión del ciclo de vida como Alcatel-Lucent ProActive Lifecycle Management (PALM) para realizar un seguimiento de la obsolescencia y los hitos de fin de vida útil, de modo que la sustitución del hardware pueda presupuestarse y planificarse antes de que se convierta en algo urgente.
2. Refuerce la seguridad de los conmutadores a nivel de código, protegiendo su infraestructura al garantizar que el sistema operativo de red esté fortificado. La tecnología Secure Diversified Code de Alcatel-Lucent aleatoriza la asignación de memoria para reducir los riesgos de explotación. La verificación y validación independientes (IVV) realizadas por expertos externos añade otra capa de confianza al identificar y eliminar posibles vulnerabilidades antes de que lleguen a la fase de producción.
3. Aplique una estrategia de seguridad de «confianza cero» a la red de tu campus mediante la implementación de macro y microsegmentación para aislar los sistemas sensibles (como los expedientes de los estudiantes y los laboratorios de investigación) del tráfico general. Sigue un enfoque por fases (supervisar, validar, planificar, simular y aplicar) para evitar interrupciones y mejorar al mismo tiempo la resiliencia.
4. Incorpore redundancia mediante Shortest Path Bridging para proporcionar una conmutación por error rápida y un redireccionamiento dinámico del tráfico en caso de fallos en los enlaces o los dispositivos. Esto crea una red eficiente y automatizada en contenedores, lo que reduce la complejidad de gestionar múltiples redes de área local virtuales (VLAN), una ventaja importante a la hora de ampliar la red en campus de gran tamaño.
5. Utilice las capacidades de chasis virtual para mejorar la fiabilidad en áreas de misión crítica. Esto permite actualizaciones de software en servicio (ISSU) sin tiempo de inactividad, admite topologías en anillo o en malla y simplifica la gestión al presentar múltiples dispositivos como una única unidad lógica, todo ello manteniendo unos costes predecibles.
6. Automatice las copias de seguridad y la restauración con herramientas de gestión de red como el sistema de gestión de red OmniVista® de Alcatel-Lucent. OmniVista Resource Manager simplifica las copias de seguridad de la configuración, la aplicación de políticas y los procesos de restauración. La automatización de las tareas del ciclo de vida garantiza una recuperación más rápida en caso de interrupciones o errores de configuración, lo que reduce la presión sobre los pequeños equipos de TI de colegios y universidades.
7. Garantice la redundancia de los routers mediante la implementación del Protocolo de Redundancia de Routers Virtuales (VRRP) para proporcionar una conmutación por error fluida entre routers. Esto evita los puntos únicos de fallo y garantiza el acceso continuo a aplicaciones críticas, como plataformas LMS, herramientas de colaboración o



Invierte en soluciones de red resilientes y seguras

Invertir para garantizar que su red sea resiliente y segura siempre tiene sentido. Sin embargo, determinar dónde invertir mejor puede resultar complejo y llevar tiempo; la planificación es fundamental. Antes de empezar, aquí tiene algunos aspectos clave que debe tener en cuenta para asegurarse de obtener la seguridad y la resiliencia que su organización necesita:

- Junto con su socio comercial, revise y actualice el diseño de la red para garantizar que los requisitos de su organización queden reflejados en ella, incluido el nivel adecuado de resiliencia para las áreas sensibles y críticas que afectan a los servicios esenciales del campus. En el caso de las áreas críticas, considere la posibilidad de añadir servidores de respaldo y conexiones múltiples siempre que sea posible y aplicable.
- Mejore la respuesta ante incidentes utilizando las capacidades de inteligencia artificial (IA) y aprendizaje automático (ML) con [Alcatel-Lucent OmniVista Network Advisor](#). Esta herramienta garantiza que los problemas se resuelvan antes de que afecten a los usuarios finales, identificando y abordando de forma proactiva los problemas de red o de seguridad. Agiliza la resolución de problemas y mejora la seguridad de la red mediante auditorías de configuración y la gestión de alertas en tiempo real sobre cualquier cambio repentino en el comportamiento de la red.
- Considere la posibilidad de utilizar [conmutadores reforzados](#) para entornos hostiles. La gama de conmutadores Ethernet reforzados de Alcatel-Lucent está diseñada específicamente para rendir al máximo en entornos difíciles y a temperaturas extremas. Estos conmutadores están fabricados con

componentes reforzados y alojados en carcasas resistentes, lo que garantiza su durabilidad y fiabilidad, y cuentan con el mismo sistema operativo que el resto de conmutadores de Alcatel-Lucent. Para mejorar la seguridad y proteger la información confidencial, algunos modelos están equipados con alertas de intrusión y relés de alarma que permiten la conexión de sistemas de alarma externos. Algunos modelos incluso admiten MACsec (control de acceso a medios y seguridad) para garantizar la seguridad de las comunicaciones de datos. Gracias a la capacidad de chasis virtual de los conmutadores reforzados, se consigue una mayor redundancia, resiliencia y escalabilidad.

- Impartir [formación técnica de Alcatel-Lucent](#) al equipo operativo de la red para ayudarles a detectar y reaccionar rápidamente ante los problemas

Soluciones de comunicaciones resilientes y seguras

Las comunicaciones son fundamentales para que las instituciones educativas interactúen con los estudiantes, el personal y otras instituciones, así como para la difusión de información importante. Los sistemas de comunicaciones deben estar disponibles en momentos de crisis, cuando los estudiantes y el personal más necesitan la ayuda del campus. La resiliencia y la seguridad están en constante evolución, y las revisiones periódicas ayudarán a mantener segura y disponible su solución de comunicaciones de Alcatel-Lucent.

Las soluciones de comunicaciones de Alcatel-Lucent son seguras desde su diseño. Esto significa que tenemos en cuenta la seguridad en cada paso de la definición, el desarrollo y la entrega del producto. Todo el hardware y los sistemas operativos están reforzados, y la protección contra ataques de denegación de servicio (DoS) está integrada. Cumplimos con certificaciones y acreditaciones reconocidas en materia de normas globales de seguridad y privacidad (ISO 27001, ISO 27017 e ISO 27018). También cumplimos con normas de seguridad y privacidad específicas del sector, como la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA) en EE. UU. y la normativa «Hébergeurs de Données de Santé» (HDS) para el alojamiento de datos sanitarios en Francia, así como con normas regionales de seguridad y privacidad, como el Reglamento General de Protección de Datos (RGPD) en la UE.

7 prácticas recomendadas para sus soluciones de comunicaciones

A continuación se presentan siete buenas prácticas para garantizar que optimices al máximo la resiliencia y la seguridad de tus soluciones de comunicaciones de Alcatel-Lucent.

1. Revise periódicamente el estado del sistema con tu socio comercial para asegurarte de que se hayan instalado la última versión del software, los parches y las mejoras de seguridad, y de que tu contrato SPS esté al día
2. Revise periódicamente los componentes de seguridad y continuidad del servicio en su [sistema de gestión de redes Alcatel-Lucent OmniVista 8770](#), que incluye información y funciones valiosas sobre resiliencia y seguridad para su solución de comunicaciones
3. Considere la posibilidad de realizar copias de seguridad remotas y automatizadas del sistema para evitar la pérdida de datos de configuración
4. Configure la supervisión de alarmas y asegúrese de que se actualice periódicamente con los umbrales adecuados. Además, compruebe que las notificaciones de fallos del sistema de comunicaciones o las alertas de calidad se envíen a las personas adecuadas.
5. Revise y aplique una política de contraseñas sólida, preferiblemente utilizando autenticación externa (servidor RADIUS) y establecer recordatorios para los usuarios con el fin de ayudar a prevenir el fraude en las tarifas, que sigue siendo una amenaza en muchos países
6. Forme a los empleados y asegúrese de que conozcan los riesgos y las medidas de prevención
7. Revise el estado, la idoneidad y la operatividad de los servidores de aplicaciones críticas para el negocio
8. Considere la posibilidad de utilizar una VLAN específica para la voz. Separar el tráfico de voz del resto reduce la probabilidad de contaminación, lo que podría interrumpir las operaciones y, potencialmente, los servicios del campus.
9. Asegúrese de que sus controladores de borde de sesión (SBC) estén configurados correctamente. Es posible que los requisitos hayan cambiado con el tiempo.



Invertir en soluciones de comunicaciones resilientes y seguras

Los campus modernos necesitan sistemas de comunicación que estén siempre disponibles, ya sea para la docencia, la investigación o las alertas de emergencia. A medida que las instituciones planifican soluciones de última generación, estas son las áreas clave a las que deben dar prioridad:

- Implemente servidores de llamadas y servicios de aplicaciones duplicados en ubicaciones críticas, como centros de salud, residencias de estudiantes y centros de investigación. La redundancia garantiza que la comunicación siga estando disponible incluso si falla un sistema, lo que protege el bienestar de los estudiantes y la continuidad operativa.
- Asegúrese de que la cobertura DECT (Digital Enhanced Cordless Telecommunications) o Wi-Fi abarque no solo las aulas, sino también zonas sensibles y de difícil acceso, como laboratorios, centros de datos y zonas al aire libre. Una cobertura integral facilita tanto el aprendizaje diario como las comunicaciones de emergencia.
- Utilice herramientas como [Alcatel-Lucent Visual Notification Assistant](#) o Rainbow™ para crear flujos de trabajo con activadores automáticos, ya sean personas, dispositivos IoT o sistemas. Esto garantiza que el personal clave sea notificado inmediatamente de cualquier incidencia, lo que permite una respuesta y una recuperación más rápidas.
- Implemente [Rainbow™ de Alcatel-Lucent](#), la herramienta colaborativa ideal para complementar las soluciones de comunicaciones de Alcatel-Lucent. Rainbow ofrece servicios seguros de voz, vídeo, mensajería e intercambio de archivos, lo que facilita la enseñanza híbrida, la movilidad del profesorado y la colaboración a distancia. Su arquitectura híbrida (en la nube y en las propias instalaciones) garantiza la resiliencia al funcionar desde diferentes ubicaciones, manteniendo las comunicaciones abiertas incluso durante interrupciones locales. Funciones como el intercambio de imágenes y vídeos, incluidas las transmisiones de vigilancia, mejoran el conocimiento de la situación tanto para fines académicos como de seguridad.
- Para las instituciones con requisitos estrictos de gobernanza de datos, Rainbow Edge puede implementarse en una nube privada o regional, lo que garantiza el cumplimiento de las políticas de datos académicas o nacionales sin dejar de ofrecer funciones modernas de colaboración
- Alcatel-Lucent ofrece soluciones flexibles para la enseñanza a distancia, el profesorado itinerante y las configuraciones híbridas del personal, con el fin de facilitar la comunicación segura por voz, vídeo y colaboración desde cualquier lugar, entre las que se incluyen:
 - Rainbow para la colaboración basada en la nube
 - [SoftPhone de escritorio IP/SoftPhone](#) para personal remoto o híbrido
 - [El teléfono de sobremesa con VPN integrada puede implementarse de forma masiva](#) para despliegues seguros a gran escala.



Protección de personas y activos

Un campus inteligente es mucho más que una conexión rápida a Internet: es un entorno conectado en el que la tecnología protege de forma activa a los estudiantes, al personal y a los recursos esenciales. Al integrar las comunicaciones, el Internet de las cosas (IoT) y el análisis de datos, las universidades y los centros educativos pueden ir más allá de un enfoque reactivo y crear una cultura de seguridad proactiva.

La información en tiempo real desempeña un papel fundamental. Las alarmas contra incendios, los detectores de movimiento, los sistemas de control de acceso o el análisis de vídeo basado en inteligencia artificial pueden activar automáticamente alertas dirigidas a los equipos de seguridad o a los responsables de las instalaciones, lo que reduce los tiempos de respuesta y evita que los pequeños incidentes se agraven. En lugar de esperar a que se notifiquen los problemas, las instituciones pueden anticiparse a los riesgos

y actuar de inmediato, ya sea cerrando un edificio, enviando al personal de mantenimiento a reparar o a responder una actividad sospechosa.

El verdadero valor surge cuando los datos, los flujos de trabajo y las comunicaciones se integran. Herramientas como Rainbow y Visual Notification Assistant pueden conectar a personas, sistemas y dispositivos del Internet de las cosas (IoT) en flujos de trabajo automatizados, garantizando que la información adecuada llegue a las personas adecuadas en el momento oportuno. Este enfoque sensible al contexto mejora la toma de decisiones, potencia la conciencia situacional y, en última instancia, refuerza tanto la seguridad como la resiliencia operativa.

Proteger los activos es casi tan importante como proteger a las personas. Gracias a funciones como el seguimiento de activos, los campus pueden localizar equipos de

investigación valiosos en mapas interactivos, lo que mejora su aprovechamiento y reduce el riesgo de pérdida o robo. Las comunicaciones grabadas y los registros de acciones también simplifican el análisis posterior a los incidentes, lo que ayuda a las instituciones a reforzar sus procesos de seguridad y a cumplir los requisitos normativos.

Para hacer posibles estas capacidades, es esencial contar con una base sólida. Una cobertura Wi-Fi ubicua, una integración segura del IoT y unos sistemas de comunicación resilientes proporcionan la columna vertebral que da soporte a todo, desde las aulas y las residencias hasta los laboratorios de investigación y las instalaciones al aire libre. De este modo, la resiliencia y la seguridad se convierten en una parte natural del funcionamiento diario del campus, transformando la tecnología en un aliado de confianza para la seguridad, la eficiencia y la innovación.



Soberanía y seguridad de los datos

La protección de información sensible, como los expedientes de los estudiantes, los datos de investigación y la información sanitaria, requiere un cumplimiento estricto y sólidas prácticas de ciberseguridad. En Alcatel-Lucent:

- Seguimos las mejores prácticas del Instituto Nacional de Ciencia y Tecnología (NIST) para la evaluación de riesgos en nuevas funcionalidades y a la hora de implementar características de ciberseguridad, como el cifrado nativo, en nuestras soluciones
- Contamos con la certificación Common Criteria EAL2+

- Aplicamos las normas ISO 27001 a todas nuestras soluciones basadas en la nube
- Admitimos ZTNA, la segmentación granular de la red y políticas de seguridad altamente específicas para reducir el riesgo de actividades no autorizadas
- Realizamos pruebas altamente especializadas y específicas de seguridad, como pruebas de penetración, en nuestros productos
- Garantizamos que nuestros productos cuenten con las certificaciones clave del sector, como HDS, HIPAA y la Ley de Derechos Educativos y Privacidad de la Familia (FERPA).

Como expertos reconocidos en ciberseguridad, contribuimos a las propuestas de la UE para las directivas de ciberseguridad. También aprovechamos nuestra experiencia en ciberseguridad para ayudar a los clientes a elegir e implementar la combinación adecuada de soluciones seguras de comunicaciones unificadas y colaboración que satisfagan sus necesidades, además de formar a sus empleados en las mejores prácticas de ciberseguridad.

Al combinar soluciones certificadas, una gestión proactiva de los riesgos y la sensibilización del personal, las universidades y los centros educativos pueden garantizar la soberanía de los datos al tiempo que mantienen el cumplimiento normativo y la confianza.

www.al-enterprise.com

© 2026 ALE International, ALE USA Inc. Todos los derechos reservados en todos los países. El nombre y el logotipo Alcatel-Lucent son marcas registradas de Nokia que se usan bajo licencia por ALE. Para saber de otras marcas con titularidad exclusiva de ALE, visite www.al-enterprise.com/es-es/legal/marcas-comerciales-copyright. Algunas imágenes de este documento pueden haber sido generadas mediante inteligencia artificial y tienen únicamente fines ilustrativos. DID2506050IES (septiembre 2026)