Consideraciones y soluciones para el puesto de trabajo digital del sector público

Alcatel·Lucent Enterprise

Libro electrónico

Indice

Información general

En todas las organizaciones del sector público hay trabajadores que desempeñan las actividades fundamentales de la administración de las que todos dependemos. No se puede subestimar el papel que juegan. A menudo influyen directamente en la vida de miles de personas.

La digitalización está en marcha desde hace tiempo. Con la presión constante para mejorar los servicios públicos y reducir los costes, la pandemia ha acelerado aún más esta tendencia. Sin embargo, no había forma de prever, hace dos años, el gran porcentaje de trabajadores del sector público que pasaría a trabajar desde casa, y la mano de obra distribuida que surgiría.

Los retos de los trabajadores que esperan un mundo más digital, y los complejos requisitos de apoyo a una fuerza de trabajo distribuida, han creado la necesidad de que las organizaciones del sector público pasen de soluciones temporales a soluciones más permanentes para apoyar la nueva fuerza de trabajo híbrida.

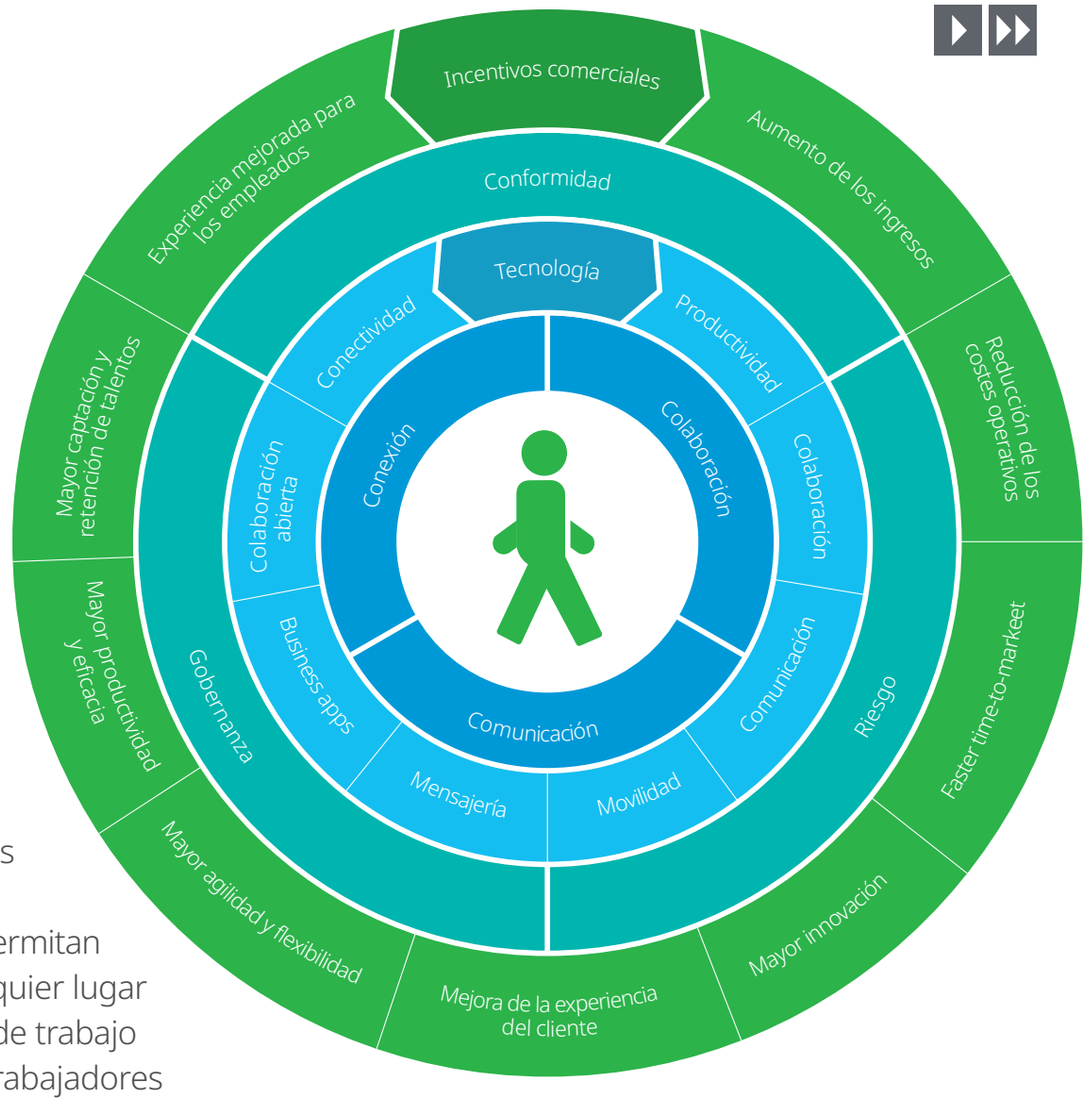
Deloitte[1] ofrece un excelente gráfico que explica cómo encaja el lugar de trabajo digital y las ventajas que ofrece.

La tecnología proporciona herramientas para mejorar las comunicaciones y la colaboración en cualquier lugar o dispositivo; sin embargo, asegurarse de que se dispone de la tecnología adecuada para el resultado deseado puede ser más complicado.

Alcatel-Lucent Enterprise ha estado trabajando con clientes de todo el mundo para entender los nuevos retos a los que se enfrentan y proporcionar soluciones de tecnología digital que permitan a los trabajadores trabajar desde cualquier lugar y con cualquier dispositivo. El puesto de trabajo digital ha creado eficiencias para los trabajadores del sector público, permitiendo una mayor productividad, con menos desplazamientos, lo que a su vez es una ventaja para el planeta.

Este libro electrónico se centrará en tres elementos clave del puesto de trabajo digital del sector público:

- Comunicación y colaboración
- Conectividad
- Seguridad



Además, analizaremos las soluciones de Alcatel-Lucent Enterprise que ayudan a las organizaciones del sector público a avanzar con éxito hacia el puesto de trabajo digital con flexibilidad, agilidad y seguridad.

1 - https://www2.deloitte.com/content/dam/Deloitte/be/Documents/technology/The_digital_workplace_Deloitte.pdf

Consideraciones clave para el puesto de trabajo digital del sector público

Comunicación y colaboración

Hoy en día los empleados dividen su puesto de trabajo entre el hogar, los lugares remotos y la oficina. La oficina ya no es el lugar donde se trabaja a diario. Se utiliza más a menudo para reuniones de grupo, formación y encuentros cara a cara con los ciudadanos. Los empleados ya no van a un único lugar para trabajar y reunirse con sus equipos. Esto ha tenido un impacto fundamental en el entorno de trabajo, haciendo que las comunicaciones y la colaboración sean más importantes que nunca.

Las comunicaciones son un componente crítico para el éxito del puesto de trabajo digital. Mantener a los empleados comprometidos, productivos y motivados es el reto. Los empleados necesitan herramientas de comunicación que faciliten sus actividades diarias y les permitan comunicarse y colaborar con sus colegas, equipos y ciudadanos, independientemente de la ubicación de su lugar de trabajo o de su dispositivo.

Para garantizar unas comunicaciones conectadas, recomendamos:

- Funcionalidad de comunicaciones avanzadas para los empleados, incluidos: voz de alta calidad, chat de grupo, mensajes de voz y la capacidad de pasar de una llamada a un vídeo sea cual sea el dispositivo
- Funcionalidades de colaboración, como compartir la pantalla, controlar el escritorio remoto y compartir archivos de gran tamaño
- Comunicaciones seguras y colaboración con contactos externos
- Continuidad de las llamadas en toda la organización con una conexión instantánea a y una guía de contactos coherente
- Un canal de difusión de noticias, que mantiene a todo el mundo al día de los últimos anuncios o normativas
- La comunicación y colaboración deben ser intuitivas

Para garantizar que todos los empleados tengan todo lo que necesitan, recomendamos:

- Evaluar los principales perfiles de usuario y los requisitos de comunicación, en función de la movilidad y la necesidad de acceso a las aplicaciones empresariales
- Ofrecer a los empleados en primera línea dispositivos optimizados que permitan un acceso rápido a la información y a las comunicaciones mientras están fuera

- Garantizar que el personal de atención al ciudadano disponga de acceso optimizado a la gestión de llamadas e interacciones, integrada con aplicaciones CRM o empresariales
- Permitir la colaboración con el personal administrativo para mejorar las tasas de resolución en la primera llamada
- Evaluar los requisitos legales locales/nacionales para proteger la privacidad de los datos

Para garantizar un alto rendimiento en el teletrabajo, recomendamos:

- Chat de grupo, capacidades de reuniones de audio y vídeo con pantalla compartida para colaborar desde cualquier dispositivo
- Continuidad de las llamadas utilizando una infraestructura subyacente para conectar todos los perfiles
- Una opción de teléfonos de escritorio para los empleados que pasan más de una hora al teléfono y gestionan llamadas importantes, como: servicios de atención al ciudadano, asistencia sanitaria y situaciones de emergencia
- Comunicaciones dentro de la aplicación empresarial preferida para facilitar la adopción por parte del usuario y mantener el escritorio ordenado
- Acceso remoto seguro para acceder de forma segura a la información sensible

Conectividad

El puesto de trabajo digital depende de una conectividad de alta calidad, resistente y segura. A medida que las nuevas formas de trabajo se normalizan y el puesto de trabajo digital toma forma, la infraestructura digital para conectar a los empleados debe estar en funcionamiento. Independientemente de la ubicación, hay que tener en cuenta algunos puntos clave.

- La seguridad debe ser una prioridad absoluta. Se requiere una solución de red con varios niveles de seguridad dentro de la red. Un marco de confianza cero asume que cada dispositivo o usuario es un riesgo para la seguridad. El control de acceso a la red debe estar habilitado.
- El acceso seguro a las aplicaciones en cualquier lugar crea la necesidad de conexiones de acceso basadas en el usuario. Los perfiles basados en el usuario proporcionan una conectividad segura y flexible sin pérdida de servicio, sea cual sea la ubicación.
- Los teletrabajadores con altos requisitos de seguridad y privacidad de los datos deben poder conectarse a la red corporativa desde sus casas o sucursales. Esto garantiza que se mantengan las políticas corporativas y la seguridad, y que el equipo de TI mantenga el control.
- Los trabajadores utilizan ahora ordenadores portátiles para aplicaciones en tiempo real (voz, vídeo) en la oficina y en casa. Esto supone un gran cambio para muchas organizaciones del sector público. La red inalámbrica debe ser capaz de soportar un mayor uso de aplicaciones en tiempo real en una zona más amplia. Esto debería tenerse en cuenta a la hora de delimitar la red.
- La resiliencia de la red inalámbrica ha subido en la lista de prioridades a medida que muchos más trabajadores se conectan de forma inalámbrica. Una red inalámbrica distribuida con inteligencia en los puntos de acceso significa que no hay un único punto de fallo, y en caso de que un punto de acceso se caiga, otros puntos de acceso en la red se harán cargo del servicio. Una red inteligente inalámbrica distribuida también elimina la necesidad de duplicar la red, lo que ahorra tiempo y dinero.
- El ritmo acelerado de la transformación digital crea presión para el equipo de TI, que ya está lidiando con las tareas del día a día. Hay que tener en cuenta las eficiencias que se pueden obtener. La reducción del número de interfaces de gestión y sistemas operativos en la red reducirá la carga de trabajo y el tiempo de formación. Además, la automatización reducirá el tiempo de implementación y gestión operativa de la red.
- El acceso de alta calidad es esencial. El puesto de trabajo digital crea eficiencias para permitir una mayor productividad y, si la conectividad falla, se pierde el aumento de la productividad.

Seguridad

Seguridad de comunicaciones

Las organizaciones gubernamentales y del sector público son objetivos importantes de los ciberataques. Es esencial implementar el equipo más seguro disponible. Las herramientas de gestión integradas deben permitir la supervisión de la seguridad en todos los elementos.

Además, los dispositivos móviles están transformando el panorama de las comunicaciones y aumentando la necesidad de seguridad a medida que los ciberatacantes explotan los crecientes volúmenes de código contenidos en cada punto de acceso. El cifrado de nivel de defensa, la privacidad de los datos y los entornos de comunicación seguros requieren una infraestructura segura y disponible que sea eficiente y fácil de administrar.

Nuestras recomendaciones:

Actualice y supervise su sistema de comunicaciones:

- Las actualizaciones del sistema son de vital importancia en términos de ciberseguridad. Esto mantiene sus sistemas de comunicación actualizados con protección contra la vulnerabilidad del software.
- Habilite la supervisión de su sistema de comunicaciones para rastrear actividades sospechosas mediante la configuración de umbrales de uso y alarmas en el sistema de gestión de la red

Autentique y cifre:

- Habilitar la autenticación mutua entre todos los dispositivos (teléfonos y pasarelas) y el sistema de comunicaciones
- La señalización debe estar encriptada para evitar los ataques de envenenamiento del protocolo y los ataques de intermediario
- Las comunicaciones IP deben estar encriptadas para evitar las escuchas

Haga que sus sistemas sean redundantes y añada un componente de seguridad:

- El riesgo nunca puede ser igual a cero. Si una puerta de enlace o el sistema de comunicaciones principal no funciona, un sistema de reserva puede tomar el relevo sin problemas cuando hay redundancia espacial.
- Añada los componentes necesarios para proteger su sistema de comunicaciones, como un Session Border Controller o un Reverse Proxy, mientras que los servidores de notificaciones se utilizan para alertar a las personas necesarias

Eduque:

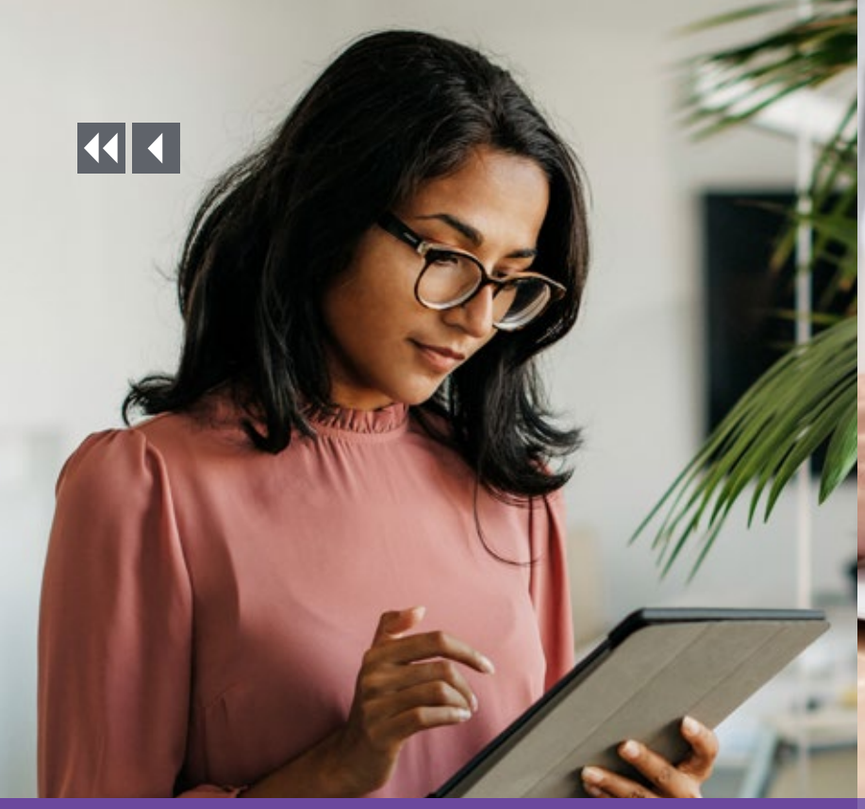
- Eduque a los usuarios y administradores; aplique las mejores prácticas en sus equipos, incluyendo recordatorios para actualizar las contraseñas, forme a los usuarios sobre cómo luchar contra la ciberdelincuencia y cómo reconocer una llamada encriptada con el icono del candado en el teléfono.

Seguridad de red

Desde hace tiempo, la ciberseguridad ha sido una de las principales prioridades de las instituciones gubernamentales. Sin embargo, las necesidades de ciberseguridad están cambiando debido a la transformación digital que se está produciendo. A medida que el cambio se acelera, los antiguos métodos de seguridad de la red están quedando obsoletos. Como componente fundamental de la arquitectura de la red, la seguridad debe estar incorporada desde el principio y aplicarse de forma universal en todos los accesos a la red, tanto por cable como inalámbricos. A continuación se indican algunas áreas que debe tener en cuenta para asegurar su red a todos los niveles.

- **Nivel de usuario:** verificar que los usuarios estén siempre autentificados y autorizados con los derechos de acceso correctos (utilizando políticas y perfiles).
- **Nivel de los dispositivos**: comprobar que los dispositivos se han autenticado y que cumplen con las normas de seguridad establecidas. Esto puede lograrse con agentes instalados en los dispositivos que realizan un rápido análisis de seguridad antes de que los dispositivos se conecten a la red. Por ejemplo, el escaneo puede garantizar que los dispositivos que se unen a la red tienen un software antivirus actualizado y la última versión del sistema operativo.
- **Nivel de aplicación:** establezca reglas asociadas a aplicaciones específicas (incluyendo el bloqueo, la limitación del ancho de banda o la identificación de quién puede utilizarlas).
- **Analítica inteligente:** las capacidades de análisis en los conmutadores y puntos de acceso ayudan a proporcionar visibilidad e información detallada sobre la red, los usuarios, los dispositivos, y las aplicaciones que se utilizan en la red. También proporcionan capacidades de inspección pormenorizada de paquetes y otras tecnologías para detectar el tipo de datos y las aplicaciones que se mueven a través de la red, lo que permite identificar patrones inusuales de tráfico en la red y actividad no autorizada.
- **Técnicas de segmentación de la red**: la colocación de dispositivos de IoT en contenedores virtuales seguros permite que múltiples dispositivos y redes utilicen la misma infraestructura física y permanezcan aislados del resto de la red. Si se produce una brecha en una parte de la red virtual, no afecta a otras áreas de la red o aplicaciones.

Estas técnicas de seguridad ayudan a construir un marco de arquitectura de confianza cero, el siguiente nivel en la arquitectura de red que opera a partir de la premisa "nunca confíe, siempre verifique", donde todos los usuarios deben ser autenticados, autorizados y continuamente validados antes de que se les conceda acceso a las aplicaciones y los datos.



Puesto de trabajo digital

Modelos en la nube flexibles

Conectarlo todo

Soluciones de ALE para el lugar de trabajo digital del sector público

Comunicación y colaboración

Digital Age Communications (DAC) de Alcatel-Lucent Enterprise ofrece soluciones integrales de comunicaciones y colaboración en las instalaciones o basadas en la nube para abordar la transformación digital. El lugar de trabajo digital está evolucionando hacia un entorno de trabajo distribuido en el que el trabajo a distancia se ha convertido en algo normal, lo que hace que las comunicaciones en tiempo real sean esenciales para conectar a compañeros, ciudadanos y socios. Las soluciones de comunicaciones de Alcatel-Lucent Enterprise permiten la continuidad de las llamadas desde cualquier lugar, en cualquier situación y desde cualquier dispositivo.

Funciones clave de comunicación de ALE:

- **Conexión sin fisuras** dentro y fuera de la organización. La infraestructura de comunicaciones subyacente conecta a los trabajadores híbridos con los empleados de administración y de primera línea, sin importar cuáles sean sus dispositivos, a través de una variedad de tecnologías estándar como PSTN, TDM, IP, SIP, VoWIFI, DECT, y también proporciona las métricas para que la TI supervise la calidad de servicio (QoS).
- **El enrutamiento de un número** a través del teléfono de empresa y el softphone resulta perfecto para el trabajo híbrido. Tanto si los empleados trabajan desde casa como desde la oficina, no se pierde ninguna llamada y no es necesario desviarlas.

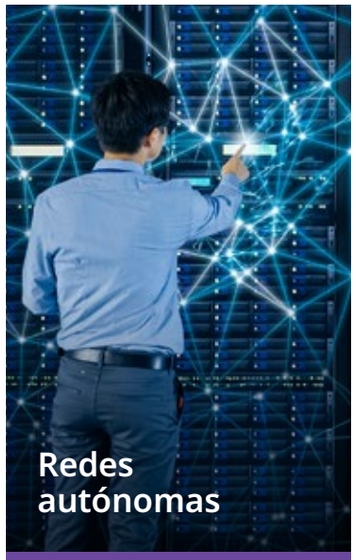
- Los teléfonos de escritorio de ALE **proporcionan calidad 3D Symphonic HD**, terminales robustos y aplicaciones para teléfonos inteligentes del personal móvil de primera línea, así como notificaciones y alarmas durante la itinerancia in situ.
- **El fácil acceso**a los mensajes de bienvenida para los clientes y a las funciones del agente, como los grupos de llamadas y las colas, permiten al personal de atención al cliente responder a todas las llamadas de los clientes.
- **La llamada de emergencia en conferencia de crisis** permite que los contactos predefinidos se incorporen automáticamente a una conferencia para la gestión de catástrofes o crisis con tan solo pulsar un botón.
- **La encriptación de extremo a extremo** proporciona la seguridad y la garantía de privacidad necesarias para las organizaciones del sector público.
- La comunicación y la colaboración para el espacio de trabajo digital es fácil mediante un **simple clic para llamar** a un contacto o iniciar una conferencia, o mediante características más avanzadas como el chat de grupo, la pantalla y el intercambio de archivos, reuniones de audio y vídeo en una sola aplicación, disponible como un cliente web. No requiere instalación. Hay aplicaciones disponibles para dispositivos y PC Android e IoS. Los clientes con soluciones de ALE pueden utilizar los terminales existentes con tecnología WebRTC.
- Los conectores para Microsoft® Teams y Google permiten a los empleados **comunicarse con facilidad** con toda la organización desde su espacio de trabajo digital Con los conectores para SaaS CRM e ITSM, los empleados pueden comunicarse y colaborar desde sus aplicaciones empresariales

Conectividad

Digital Age Networking de Alcatel-Lucent Enterprise suministra una red autónoma que proporciona una experiencia de conexión resistente y sin fisuras con Alcatel-Lucent OmniSwitch® (LAN) y Alcatel-Lucent OmniAccess® Stellar (WLAN), con un tiempo de convergencia ultrarrápido, un control de acceso seguro a la red y QoS garantizada. El Wi-Fi corporativo de nueva generación con control WLAN integrado en los puntos de acceso elimina la necesidad de disponer de controladores físicos centralizados. Las soluciones de ALE pueden gestionarse en las instalaciones y desde la nube.

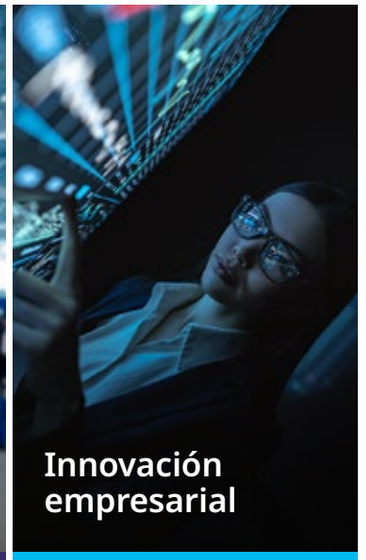
Características clave de conectividad de ALE:

- **Un único sistema de gestión de red (NMS)** proporciona un nivel adicional de integración entre las redes alámbricas e inalámbricas, lo que reduce la carga de trabajo del administrador de TI, ya que no es necesario manejar dos sistemas de gestión con dos conjuntos de políticas y reglas de configuración. El sistema de gestión de red Alcatel-Lucent OmniVista® Network Management System ofrece gestión unificada y visibilidad total de la red, lo cual puede mejorar el rendimiento de TI y la agilidad.
- **Aprovisionamiento automatizado** de una infraestructura de red segura simplifica las adiciones, los traslados y los cambios, a la vez que reduce el tiempo necesario para el mantenimiento y el funcionamiento de la red, creando eficiencia operativa y disminuyendo los costes y los riesgos.
- **Conexión de ruta más corta (SPB)** diseñada para apoyar la creación y el funcionamiento de una red menos compleja, y que construye y mantiene dinámicamente la tipología de la red entre los nodos. SPB comparte la carga y utiliza todas las conexiones físicas disponibles para proporcionar más ancho de banda.
- **Trabajadores híbridos (opción 1). El acceso remoto seguro** se habilita con el punto de acceso remoto (RAP). La red de la empresa puede extenderse fácilmente fuera de la sede principal, proporcionando conectividad a los trabajadores remotos como si estuvieran en la LAN de la empresa. Dependiendo del modelo, el RAP también puede proporcionar conectividad por cable para teléfonos IP o para otros dispositivos IoT. El acceso está respaldado por políticas de seguridad centralizadas y unificadas en las redes alámbricas e inalámbricas, lo que garantiza una gestión sencilla y una seguridad muy sólida y coherente.
- **Trabajadores híbridos (opción 2) SD-WAN y SASE**. El Secure Access Service Edge (SASE) conecta de forma segura ubicaciones remotas, sucursales y trabajadores remotos. La solución SASE para trabajadores remotos consiste en un software en el ordenador portátil del usuario que proporciona acceso seguro a las aplicaciones en el centro de datos de la empresa, en centros de datos privados o nubes de Internet o públicas, con gestión centralizada y sin que requiera hardware adicional en la ubicación del trabajador. SASE proporciona seguridad avanzada con el cortafuegos de nueva generación (NGFW), que incluye el filtrado de URL y el cortafuegos de aplicaciones, así como la gestión unificada de amenazas (UTM), que incluye el sistema de pevención de intrusiones de nueva generación (NGIPS), el antivirus y la funcionalidad antimalware.



Automatizar las operaciones de la red de misión crítica y mejorar la experiencia del usuario

Aumentar la digitalización a través de la incorporación y gestión segura de la IoT



Acelerar la transformación con flujos de trabajo automatizados

Seguridad

Seguridad de comunicaciones

Tanto si es responsable de un pequeño organismo gubernamental local como de uno de los grandes, su red de comunicaciones corre el riesgo de ser objetivo de los hackers.

Características clave de seguridad de ALE:

- **Conectividad segura** entre el sistema de comunicaciones en las instalaciones (PBX y teléfonos) y la infraestructura de la nube, totalmente desarrollada y operada por Alcatel-Lucent Enterprise, con autenticación mutua, cifrado y elementos de límite de seguridad (SBC).
- **Alta disponibilidad** con arquitecturas espacialmente redundantes, en las instalaciones, en nubes privadas o públicas, protección contra ataques de denegación de servicio (DoS), seguridad integrada con hardware reforzado y sistemas operativos.
- **Confidencialidad de las comunicaciones** con una robusta función de cifrado basada en estándares del sector implementados nativamente en la solución, sin que afecten la calidad y el rendimiento de la voz, y proporcionando la experiencia que esperan los clientes y los empleados.
- **Privacidad y protección de datos** con control de acceso basado en funciones y encriptación de los datos almacenados. Esto asegura que todos los datos cruciales que se recogen en el entorno laboral, que está en constante evolución, están totalmente protegidos de extremo a extremo y bajo su control.
- **Cumplimiento de reglamentos y normas** como (pero no limitado a) el Reglamento General de Protección de Datos (RGPD), ISO27001, Common Criteria EAL2+, HDS (certificación "Hébergeur Données Santé" de los servicios en la nube de ALE para el cumplimiento de la protección de datos del paciente en Francia).
- **La seguridad como proceso** con el equipo de respuesta a incidentes de seguridad de productos (PSIRT) para la gestión activa de la vulnerabilidad, la actualización periódica del software y la plataforma de políticas.

ANSSI (CSPN)

ENS (Esquema Nacional de Seguridad)

Certificación establecida por el Sistema de Seguridad Nacional de Españapara disponer de un sistema que garantice la correcta protección de los sistemas de información frente a amenazas e incidentes externos.

ISO27001 - 017/018

La Agencia para una Italia Digital es responsabilidad de la Presidencia del Consejo de Ministros. Regula el uso, el almacenamiento y el acceso a los datos clave, garantizando la seguridad.

CERTIFICACIONES EN CURSO

Certificación BSI

La Oficina Federal de Seguridad de la Información (Bundesamt für Sicherheit in der Informationstechnik). Equivalente al CSPN de ANSSI (tercer trimestre de 2021)

Seguridad de red

La transformación digital ha cambiando profundamente las necesidades en ciberseguridad a medida que el número de dispositivos conectados aumenta, el perímetro de la red desaparece y los cambios se siguen produciendo de manera acelerada. Digital Age Networking de Alcatel-Lucent Enterprise mantiene la seguridad de los datos y activos de TI en la actual era de la transformación digital. Con esta solución, puede controlar estrictamente el acceso de los usuarios, reducir las vulnerabilidades creadas por los dispositivos móviles, de IoT y de red, impedir que la inevitable infracción genere puntos de ataque y proporcionar un ecosistema empresarial de confianza.

Las soluciones ALE están diseñadas con la seguridad en mente:

- **Código seguro diversificado** que promueve la seguridad y la garantía en el nivel de los dispositivos de red utilizando la verificación y validación de terceros independientes, incluyendo:
  - Análisis de código fuente, pruebas de caja blanca y caja negra por parte de una empresa especializada en ciberseguridad para eliminar vulnerabilidades, entre otras:
    - ¬ Amenazas de puerta trasera
    - ¬ Malware incrustado
    - ¬ Vulnerabilidades explotables
    - ¬ Exposición de información reservada y/o clasificada
- **Diversificación del software:** el software ALE implementa la aleatoriedad en la disposición del espacio de direcciones (ASLR). Cada arranque del conmutador genera dinámicamente una disposición de memoria única para impedir o prevenir la explotación del software.
- **Seguridad de confianza cero (micro y macrosegmentación):** el marco de confianza cero asume que hay hackers presentes. La empresa ya no se considera una zona de confianza implícita. Esto implica acciones como la autenticación de todas las conexiones. Ningún activo ni usuario es inherentemente fiable.
- **Seguridad por defecto:** el acceso remoto en el OmniSwitch debe estar habilitado, lo cual resulta ser lo contrario que la mayoría del resto de conmutadores en los que todos los accesos a los conmutadores/routers están activados por defecto y se deja a los administradores que averigüen cómo asegurar el dispositivo.
- **Protección integrada contra la denegación de servicio (DoS):** protección del sistema operativo y de los módulos de gestión frente a una serie de ataques DDOS que suelen utilizarse para provocar la utilización del 100 % de la CPU.
- **No hay paquetes de software** que comprar y seguir: todas las funciones y capacidades, incluso el código seguro ALE, están incluidas en el precio del conmutador: no se necesita añadir módulos ni comprar actualizaciones. Todo el software está incluido.
- **Incorporación automatizada y segura de la IoT:** mediante la toma de huellas dactilares de los dispositivos, la clasificación y la contenerización.

RGPD DE LA UE

US Federal

US Joint Interoperability

US MIL-STD

US Trade Agreements Act (TAA)

Más información

Obtenga más información sobre las soluciones de Alcatel-Lucent Enterprise para empresas y organismos públicos para el puesto de trabajo digital o póngase en contacto con nosotros para hablar de sus necesidades.

www.al-enterprise.com/es-es/industries/government

Alcatel·Lucent Enterprise