Observatorio TAI
Puesto de trabajo

PATROCINADORES

citrix™ | SAMSUNG | SOPHOS | VIRTUAL CABLE

TAI | ciberseguridadTIC | directorTIC

Introducción

El gran reto ya no es trabajar desde cualquier lugar, sino hacerlo sin perder visibilidad ni control

Hace apenas unos años el puesto de trabajo estaba asociado a un espacio físico, un ordenador corporativo y un conjunto de aplicaciones accesibles desde la red de la empresa. Hoy esa realidad ha cambiado por completo. Los empleados trabajan desde múltiples ubicaciones, acceden a aplicaciones en la nube, utilizan distintos dispositivos y colaboran en entornos cada vez más distribuidos. El puesto de trabajo ha dejado de ser un lugar para convertirse en un ecosistema digital.

Este cambio ha transformado también las prioridades de las organizaciones. El debate ya no gira únicamente en torno a la movilidad o al teletrabajo. La cuestión es cómo ofrecer a los usuarios una experiencia ágil y productiva sin perder el control sobre los accesos, los dispositivos y los datos. En otras palabras, el gran desafío ya no es permitir trabajar desde cualquier lugar, sino hacerlo de forma segura, eficiente y sostenible desde el punto de vista operativo.

La evolución de la nube ha desempeñado un papel decisivo en este proceso. Cada vez más aplicaciones y servicios se consumen bajo modelos SaaS, mientras que los usuarios esperan acceder a ellos con la misma facilidad independientemente de dónde se encuentren. Al mismo tiempo, muchas organizaciones siguen conviviendo con infraestructuras heredadas, aplicaciones críticas y modelos de acceso tradicionales que añaden complejidad a la gestión diaria.

La seguridad se ha convertido en uno de los principales factores que condicionan cualquier estrategia de puesto de trabajo. La expansión de los entornos híbridos, la proliferación de dispositivos y el aumento de las amenazas obligan a las organizaciones a replantear la forma en que gestionan identidades, accesos y equipos. No es casualidad que conceptos como Zero Trust, gestión unificada de dispositivos o acceso seguro a aplicaciones hayan ganado protagonismo en los últimos años.

A este escenario se suma la irrupción de la inteligencia artificial. Más allá de la expectación generada por la IA generativa, las organizaciones comienzan a explorar su aplicación práctica en ámbitos como la productividad, la automatización de tareas o la asistencia al usuario. Aunque todavía existen diferencias importantes en los niveles de adopción, la IA ya forma parte de las conversaciones sobre el futuro del puesto de trabajo y de las prioridades tecnológicas de muchas compañías.

El puesto de trabajo inteligente toma forma: seguridad, simplificación e IA marcan la agenda empresarial

Con el objetivo de conocer cómo están respondiendo las organizaciones a estos desafíos, Director TIC y Ciberseguridad TIC han elaborado el estudio "El puesto de trabajo inteligente: seguridad, experiencia y control en la nueva era digital", con la colaboración de Citrix, Samsung, Sophos y Virtual Cable. A través de una encuesta dirigida a responsables de tecnología, ciberseguridad y transformación digital, el informe analiza aspectos como los modelos de trabajo predominantes, el acceso a aplicaciones y datos, la gestión de dispositivos, la virtualización, la adopción de la inteligencia artificial y las prioridades de inversión para los próximos años.

La encuesta revela que las organizaciones están intentando resolver una ecuación compleja: ofrecer más flexibilidad sin perder control, simplificar la gestión sin aumentar el riesgo y aprovechar el potencial de la inteligencia artificial sin comprometer la seguridad. Los resultados permiten dibujar una fotografía precisa del momento que atraviesa el puesto de trabajo digital y de los retos que marcarán su evolución durante los próximos años.

Porque si algo muestran los datos de este estudio es que el puesto de trabajo ha pasado de ser una cuestión puramente tecnológica a convertirse en un elemento estratégico para la productividad, la experiencia del empleado y la resiliencia de las organizaciones.

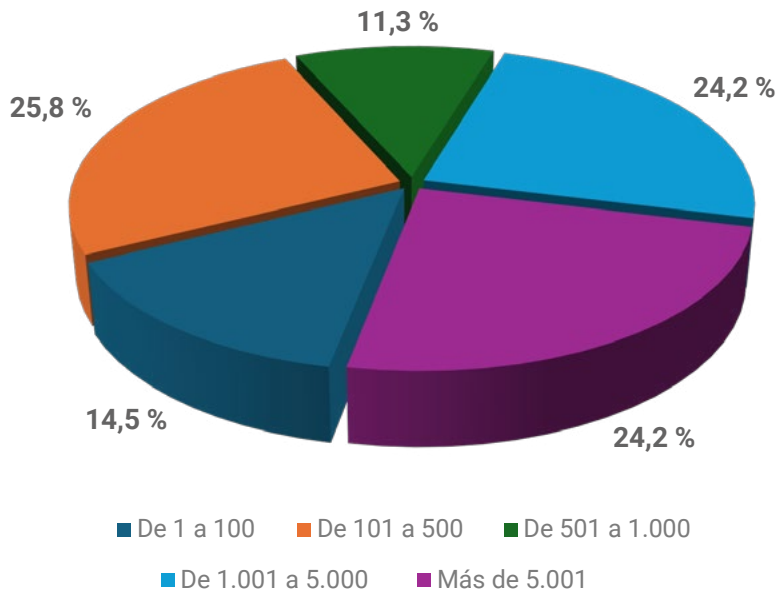
Tipología de la muestra

Los responsables de ciberseguridad y tecnología constituyen el núcleo principal de la muestra. Los CISO representan el grupo más numeroso, con un 30,7 % de las respuestas, seguidos por los CIO, que aportan un 21 % de los participantes. También destaca la presencia de directivos de distintas áreas de negocio y tecnología, que suponen un 19,4 % del total.

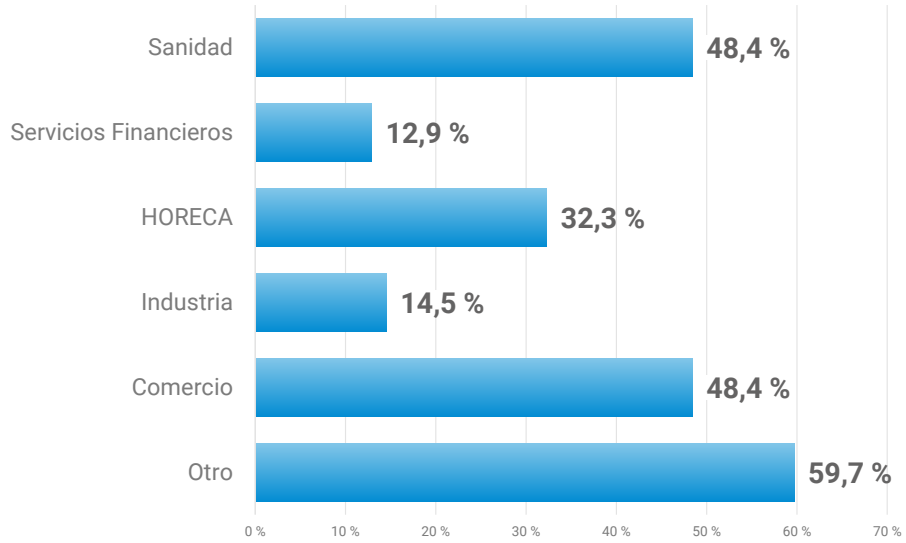
Junto a estos perfiles aparecen otros puestos de responsabilidad (17,7 %) y profesionales técnicos especializados (11,3 %), enriqueciendo la muestra con perspectivas complementarias sobre la gestión y operación del puesto de trabajo.

La elevada presencia de perfiles con capacidad de decisión aporta un valor añadido al estudio, ya que las respuestas proceden en gran medida de profesionales involucrados tanto en la definición de las estrategias tecnológicas como en su ejecución y supervisión.

Tamaño de empresa



Sector de actividad

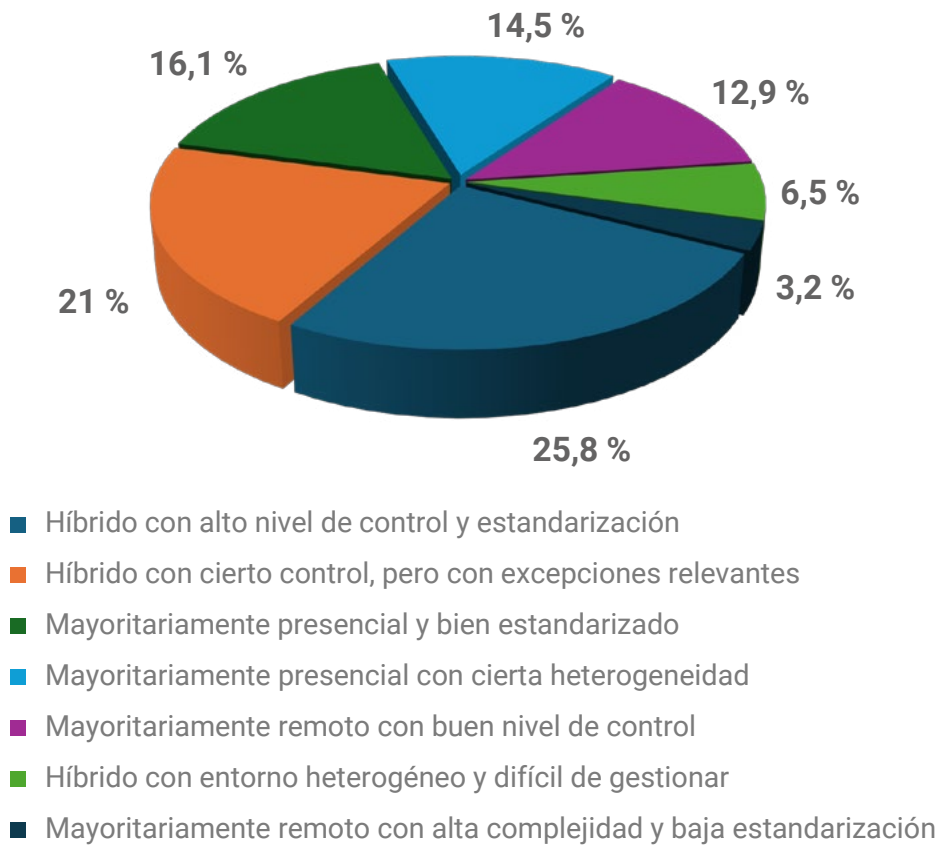


Las empresas de entre 501 y 1.000 empleados aportan un 11,3 % de las respuestas, mientras que las organizaciones con hasta 100 trabajadores representan el 14,5 % de la muestra. Esta composición permite recoger la visión tanto de medianas empresas como de grandes corporaciones, dos entornos con necesidades, niveles de complejidad y prioridades muy diferentes en la gestión del puesto de trabajo digital.

La muestra reúne organizaciones de sectores muy diversos, reflejando el carácter transversal que ha adquirido el puesto de trabajo digital en el tejido empresarial. Aunque la categoría “Otros” concentra el 59,7 % de las respuestas, también existe una representación significativa de actividades con elevados niveles de digitalización y exigencias regulatorias. La industria aporta el 14,5 % de los participantes, seguida por los servicios financieros, con un 12,9 %.

Resultados del estudio

1. ¿Cómo describiría el modelo de puesto de trabajo en su organización?

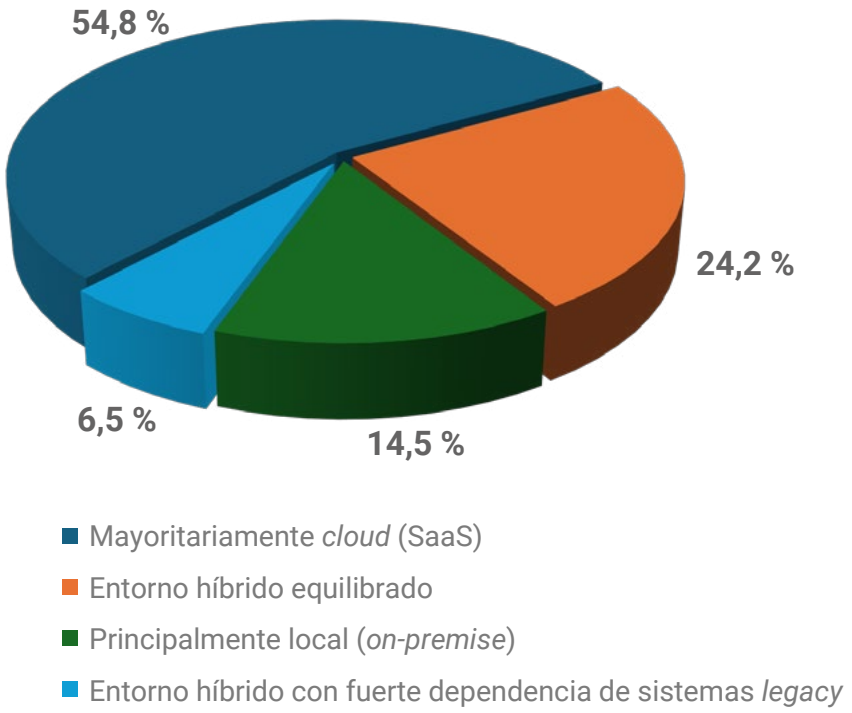


El trabajo híbrido se ha consolidado como el modelo predominante entre las organizaciones participantes. Un 25,8 % de los encuestados afirma operar en entornos híbridos con un alto nivel de control y estandarización, un 21 % lo hace bajo esquemas híbridos con cierto control, aunque con excepciones relevantes, y un 6,5 % reconoce entornos híbridos heterogéneos y difíciles de gestionar. En conjunto, el 53,3 % de la muestra trabaja ya bajo modelos híbridos.

El trabajo presencial mantiene una presencia significativa: un 30,6 % de las organizaciones se define como mayoritariamente presencial, ya sea con entornos estandarizados o con cierta heterogeneidad. Por su parte, los modelos mayoritariamente remotos representan el 16,1 % de la muestra.

La fotografía resultante muestra que las empresas han dejado atrás el debate entre presencialidad y teletrabajo. La prioridad parece centrarse ahora en garantizar una gestión eficiente del puesto de trabajo, independientemente de dónde se encuentren los usuarios.

2. ¿Qué modelo predomina en el acceso a aplicaciones y datos?

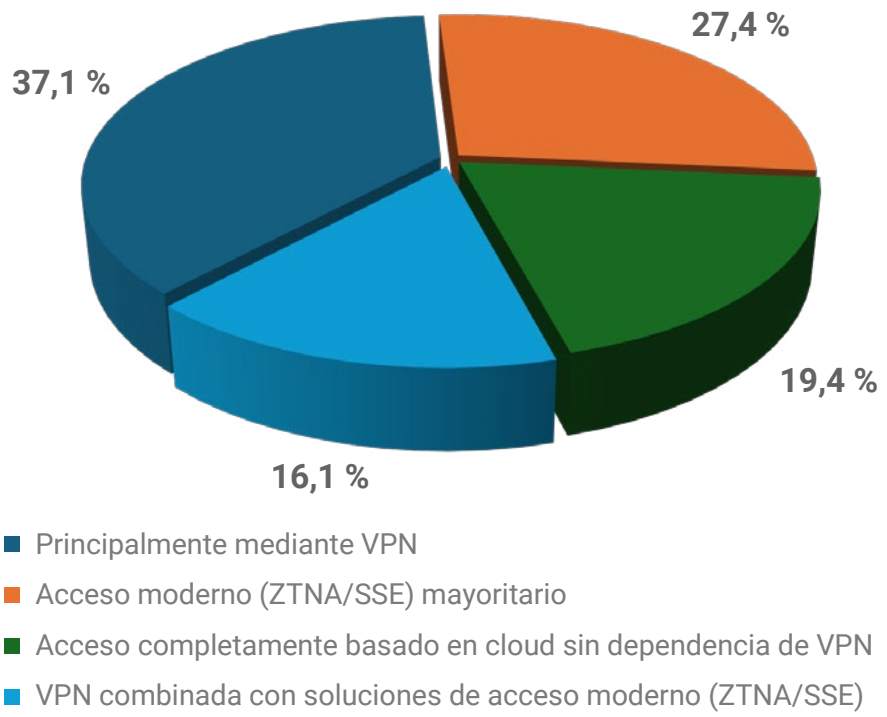


La nube se ha convertido en la principal vía de acceso a aplicaciones y datos para la mayoría de las organizaciones. Más de la mitad de los encuestados (54,8 %) afirma operar en entornos mayoritariamente *cloud* (SaaS), mientras que un 24,2 % combina recursos *cloud* y locales en un modelo híbrido equilibrado.

Los entornos principalmente *on-premise* representan ya una minoría, con un 14,5 % de las respuestas, mientras que solo un 6,5 % reconoce mantener una fuerte dependencia de sistemas heredados. En conjunto, cerca del 80 % de las organizaciones opera ya en modelos donde la nube tiene un peso relevante en el acceso a los recursos corporativos.

La fotografía que dibuja la encuesta confirma el protagonismo alcanzado por la nube en el puesto de trabajo moderno. Aun así, la migración no ha concluido y muchas organizaciones continúan operando en entornos mixtos donde conviven aplicaciones *cloud*, infraestructuras locales y sistemas heredados.

3. ¿Cómo se realiza el acceso remoto a aplicaciones y datos?

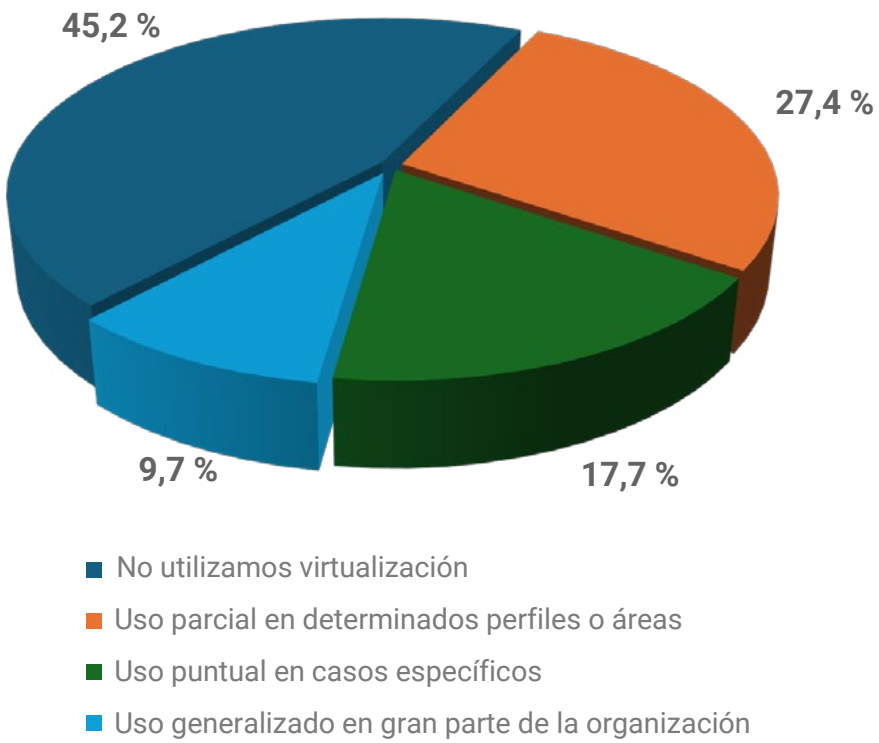


Aunque las tecnologías de acceso remoto han evolucionado notablemente en los últimos años, la VPN sigue siendo la opción más utilizada por las organizaciones. Un 37,1 % de los encuestados afirma que el acceso a aplicaciones y datos se realiza principalmente mediante VPN, mientras que un 16,1 % combina esta tecnología con soluciones más modernas de acceso seguro.

Al mismo tiempo, los modelos basados en Zero Trust continúan ganando presencia. Un 27,4 % de las organizaciones utiliza mayoritariamente soluciones ZTNA o SSE, y otro 19,4 % opera en entornos completamente basados en la nube sin dependencia de VPN. En conjunto, casi la mitad de los participantes ha adoptado ya modelos de acceso más modernos.

Más que una sustitución inmediata de tecnologías, la encuesta evidencia una etapa de transición en la que conviven modelos tradicionales y nuevos enfoques de acceso diseñados para responder a las necesidades de entornos distribuidos y cada vez más orientados a la nube.

4. ¿Qué nivel de adopción tiene la virtualización del puesto de trabajo?

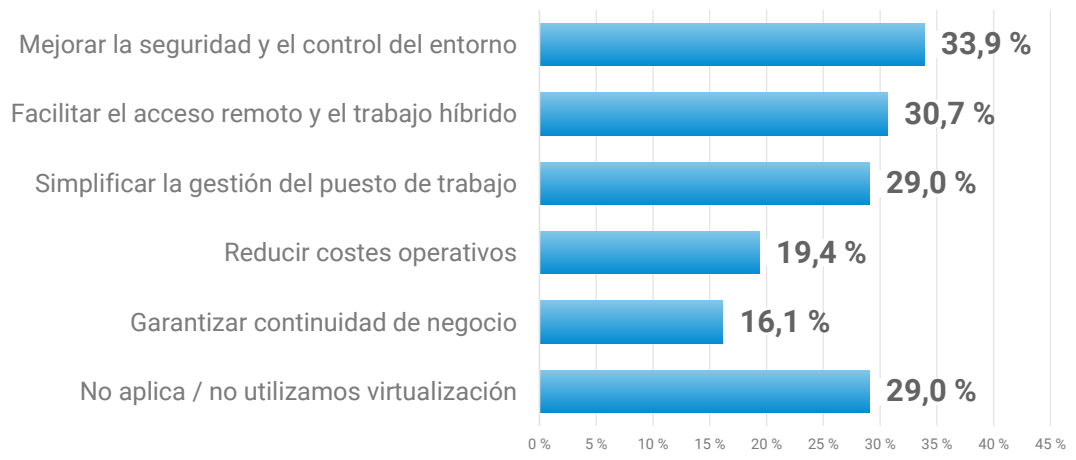


La virtualización del puesto de trabajo mantiene una presencia relevante en las organizaciones, aunque su adopción dista de ser generalizada. Un 45,2 % de los encuestados afirma no utilizar actualmente este tipo de tecnologías, mientras que un 27,4 % la emplea de forma parcial en determinados perfiles o áreas de negocio.

Por su parte, un 17,7 % recurre a la virtualización en casos específicos, y solo un 9,7 % declara haber extendido su uso a una parte significativa de la organización. En conjunto, más de la mitad de los participantes (54,8 %) utiliza algún modelo de virtualización, aunque generalmente de forma selectiva.

Los datos sugieren que la virtualización sigue asociándose a necesidades concretas relacionadas con la seguridad, la movilidad o la gestión de determinados colectivos de usuarios, más que a una estrategia de despliegue universal dentro de la organización.

5. ¿Cuáles son los principales objetivos del uso de la virtualización en su organización?

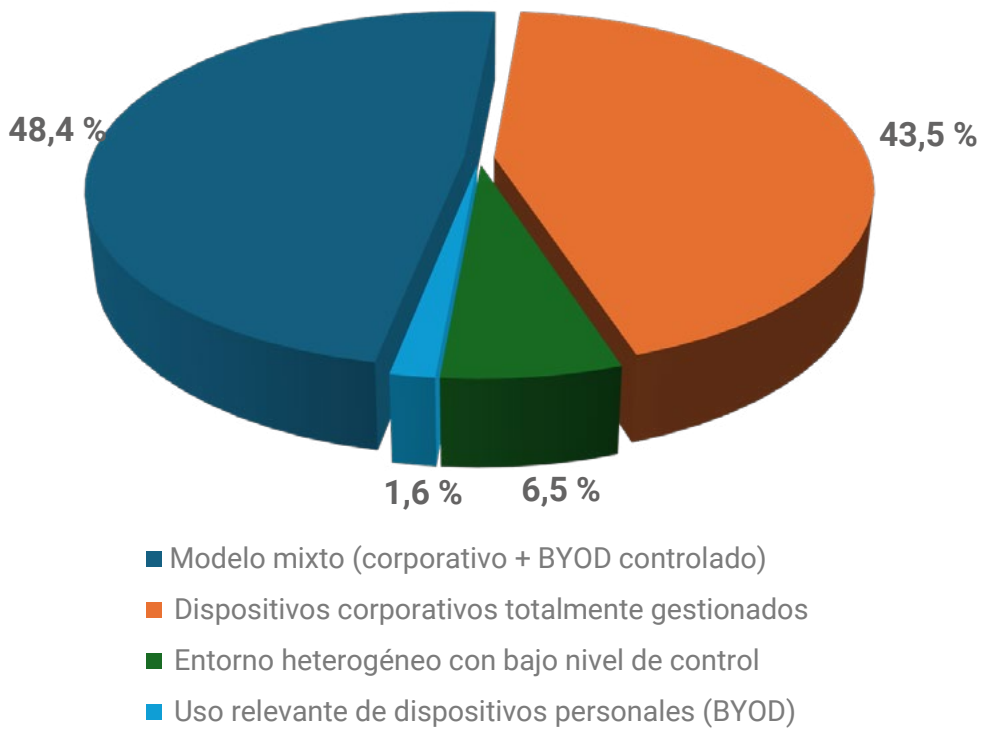


La seguridad y el control se sitúan como los principales impulsores de las iniciativas de virtualización. Un 33,9 % de los encuestados identifica la mejora de la seguridad y el control del entorno como uno de sus objetivos prioritarios, seguido muy de cerca por la necesidad de facilitar el acceso remoto y el trabajo híbrido (30,7 %).

La simplificación de la gestión del puesto de trabajo también ocupa un lugar destacado, con un 29 % de las respuestas. Por detrás aparecen factores tradicionalmente asociados a la virtualización, como la reducción de costes operativos (19,4 %) o la continuidad de negocio (16,1 %).

Resulta igualmente significativo que un 29 % de las organizaciones afirme no utilizar actualmente tecnologías de virtualización. Entre quienes sí las emplean, esta tecnología aparece cada vez más vinculada a objetivos estratégicos relacionados con la seguridad, la flexibilidad operativa y la gestión eficiente del puesto de trabajo.

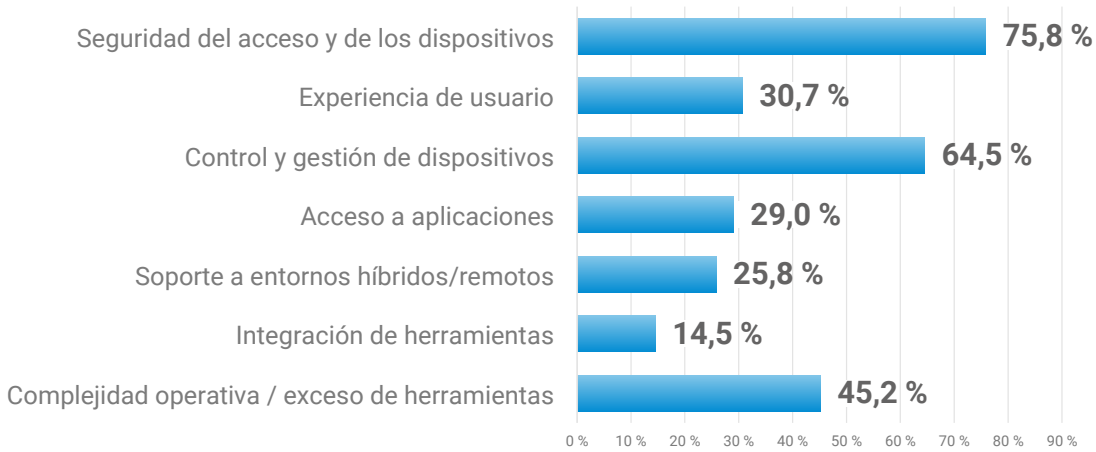
6. ¿Qué modelo de gestión de dispositivos predomina?



La gestión controlada de los dispositivos es ya la norma en la mayoría de las organizaciones. Casi la mitad de los encuestados (48,4 %) afirma operar bajo un modelo mixto que combina dispositivos corporativos con esquemas BYOD controlados, mientras que un 43,5 % utiliza exclusivamente dispositivos corporativos totalmente gestionados. Por el contrario, los entornos con bajos niveles de control representan únicamente el 6,5 % de la muestra, y el uso relevante de dispositivos personales sin una gestión estructurada apenas alcanza el 1,6 %. En conjunto, más del 90 % de las organizaciones mantiene algún tipo de gobierno formal sobre los equipos que acceden a aplicaciones y datos corporativos.

La encuesta sugiere que la adopción de modelos flexibles no implica una renuncia al control. Las organizaciones parecen haber encontrado fórmulas para compatibilizar movilidad, experiencia de usuario y requisitos cada vez más exigentes en materia de seguridad y cumplimiento.

7. ¿Cuáles son hoy los principales retos tecnológicos del puesto de trabajo?

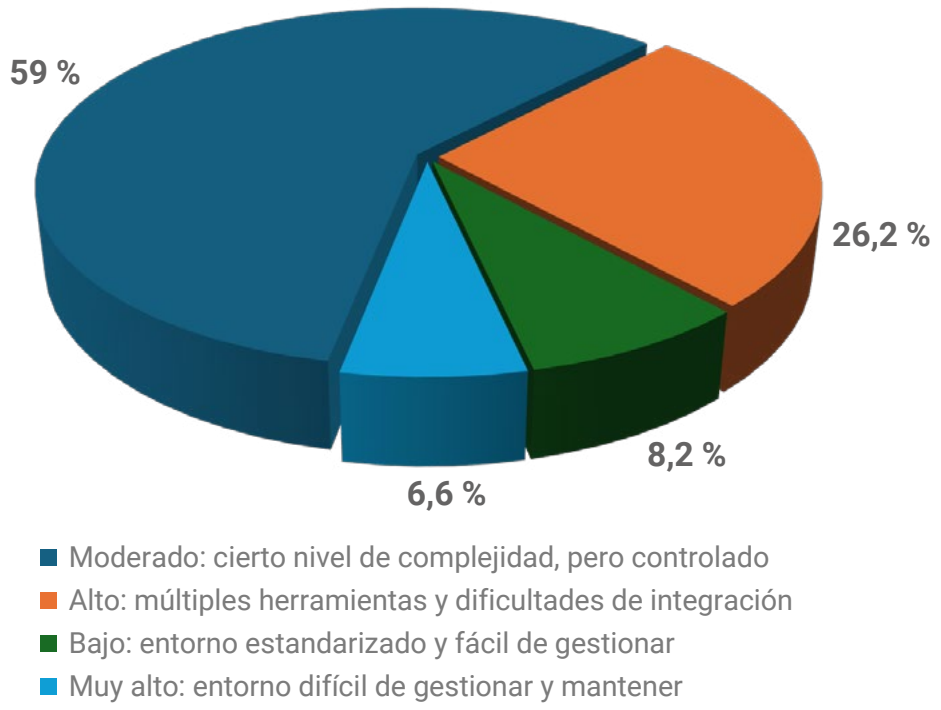


La seguridad continúa siendo la principal preocupación de las organizaciones en relación con el puesto de trabajo. Tres de cada cuatro encuestados (75,8 %) señalan la protección del acceso y de los dispositivos como uno de sus principales retos, situándola claramente por delante del resto de prioridades.

La gestión de dispositivos ocupa la segunda posición, con un 64,5 % de las respuestas, seguida por la complejidad operativa y el exceso de herramientas, mencionados por el 45,2 % de los participantes. Más atrás aparecen aspectos como la experiencia de usuario (30,6 %), el acceso a aplicaciones (29 %) o el soporte a entornos híbridos y remotos (25,8 %).

Más allá de la protección frente a amenazas, las respuestas ponen de relieve una preocupación creciente por la complejidad operativa y la capacidad de gestionar de forma eficiente entornos cada vez más distribuidos.

8. ¿Cómo describiría el nivel de complejidad en la gestión del puesto de trabajo?

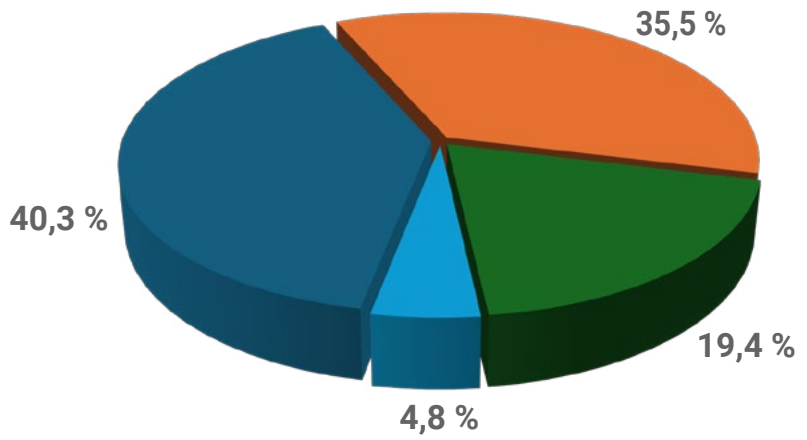


La mayoría de las organizaciones considera que la gestión de su puesto de trabajo presenta un nivel de complejidad asumible. Un 58,1 % de los encuestados describe su entorno como moderadamente complejo, con ciertos desafíos operativos, pero bajo control.

Sin embargo, la complejidad sigue siendo un factor relevante para una parte importante de la muestra. Un 25,8 % afirma enfrentarse a múltiples herramientas y dificultades de integración, mientras que un 6,5 % califica su entorno como muy complejo y difícil de gestionar. En el extremo opuesto, solo un 8,1 % dispone de un entorno altamente estandarizado y fácil de administrar.

La percepción general es que la complejidad forma parte ya de la gestión cotidiana del puesto de trabajo. Aunque pocas organizaciones describen su entorno como inmanejable, la mayoría reconoce que la integración de herramientas y plataformas seguirá siendo uno de los grandes desafíos para los equipos de TI.

9. ¿Qué papel está teniendo la inteligencia artificial en el puesto de trabajo?



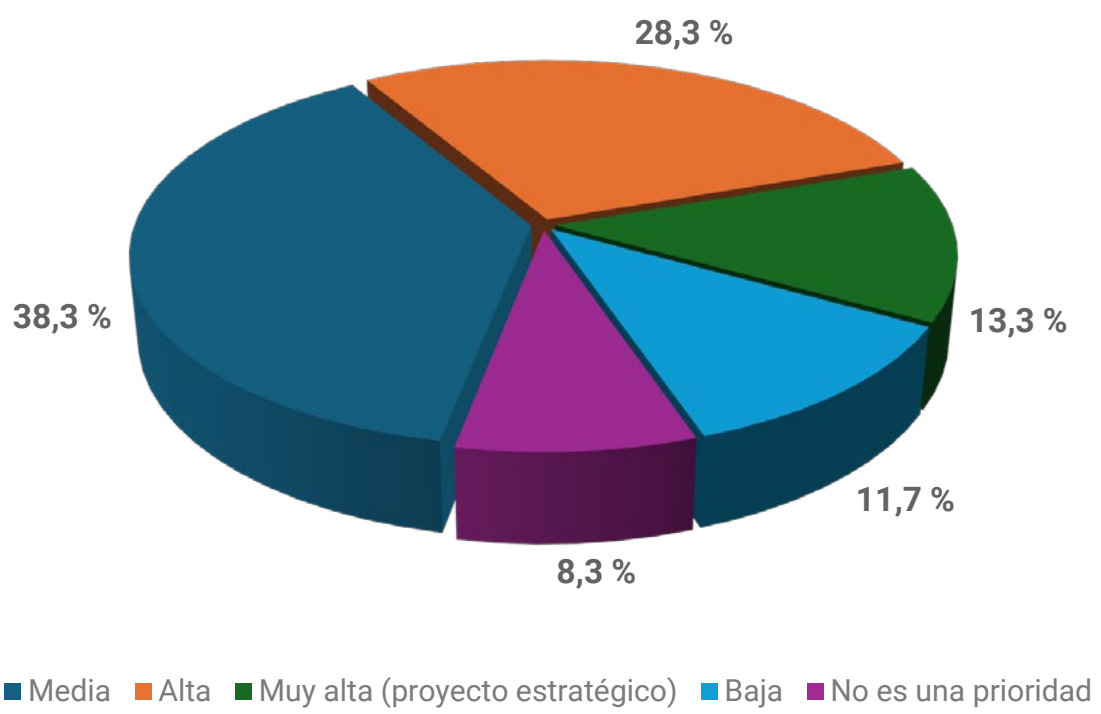
- Uso creciente en productividad y soporte (productividad individual, soporte IT, automatización de procesos)
- Uso puntual en herramientas concretas (principalmente en: productividad individual / análisis de datos / otras áreas)
- Uso extendido con impacto relevante en procesos (automatización, seguridad, análisis de datos, soporte IT)
- No se utiliza actualmente

La inteligencia artificial ha comenzado a integrarse de forma significativa en el puesto de trabajo, aunque su nivel de adopción sigue siendo desigual. El 40,3 % de los encuestados afirma que su uso está creciendo en ámbitos relacionados con la productividad y el soporte al usuario, mientras que un 35,5 % limita su utilización a herramientas concretas y casos de uso específicos.

Por otro lado, casi una de cada cinco organizaciones (19,4 %) asegura que la IA ya está teniendo un impacto relevante en sus procesos, impulsando iniciativas de automatización y mejora operativa. Solo un 4,8 % reconoce no utilizar actualmente este tipo de tecnologías.

Todo apunta a que la IA ha dejado de ser una tecnología emergente para convertirse en una herramienta cada vez más presente en la actividad diaria de los empleados. Aunque la mayoría de las iniciativas siguen centradas en productividad y automatización, los datos sugieren que las organizaciones han pasado de la fase de experimentación a una etapa de adopción progresiva y casos de uso concretos.

10. ¿Qué nivel de prioridad tiene actualmente la transformación del puesto de trabajo?

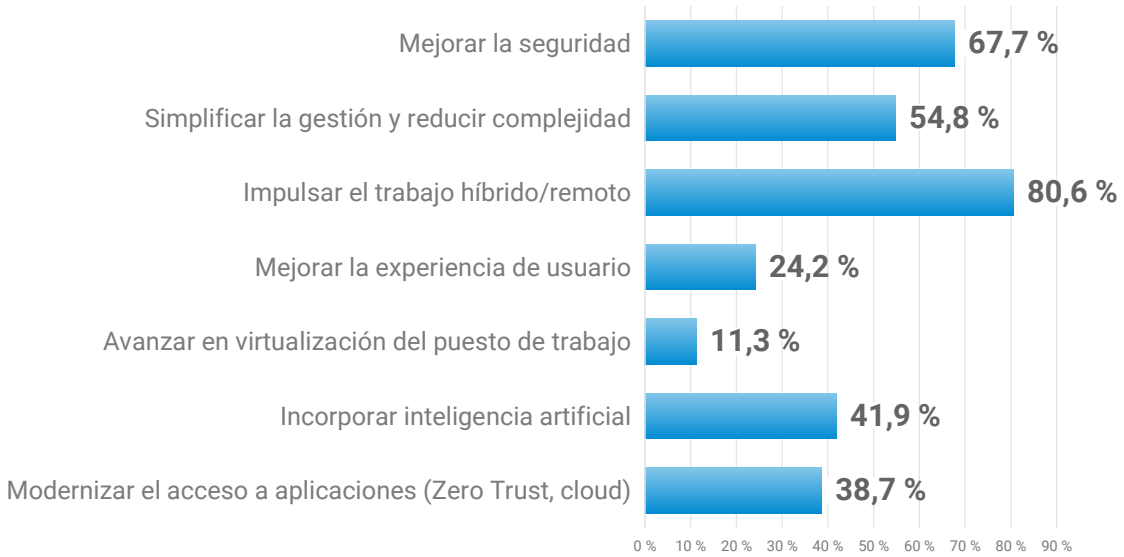


La transformación del puesto de trabajo se mantiene entre las prioridades de las organizaciones, aunque no siempre ocupa la primera posición en la agenda tecnológica. Un 37,1 % de los encuestados le otorga una prioridad media, mientras que un 27,4 % la considera alta. Además, un 12,9 % la sitúa entre sus proyectos estratégicos más relevantes.

En el lado opuesto, un 11,3 % afirma que tiene una prioridad baja y un 8,1 % asegura que actualmente no forma parte de sus prioridades. En conjunto, casi ocho de cada diez organizaciones reconocen que la evolución del puesto de trabajo sigue siendo un ámbito relevante de inversión y transformación.

La evolución del puesto de trabajo parece consolidarse como un proceso continuo de mejora y adaptación, más que como un proyecto aislado con un principio y un final definidos.

11. ¿Cuáles son sus principales prioridades en el puesto de trabajo en los próximos 12-24 meses?



La seguridad seguirá marcando la evolución del puesto de trabajo durante los próximos años. Un 67,7 % de los encuestados la identifica como una de sus principales prioridades, situándola claramente por delante del resto de iniciativas. A continuación, aparece la simplificación de la gestión y la reducción de la complejidad, señalada por el 54,8 % de los participantes.

La inteligencia artificial también gana protagonismo en las hojas de ruta tecnológicas. Un 41,9 % prevé incorporarla al puesto de trabajo, mientras que un 38,7 %
tiene previsto modernizar el acceso a aplicaciones mediante enfoques como Zero Trust o modelos *cloud*.

Por detrás se sitúan la mejora de la experiencia de usuario
(24,2 %), la virtualización (11,3 %) y el impulso del trabajo híbrido o remoto (8,1 %).

Las prioridades para los próximos años dibujan una hoja de ruta clara: reforzar la seguridad, reducir la complejidad operativa y aprovechar el potencial de tecnologías como la inteligencia artificial para impulsar nuevas formas de productividad.

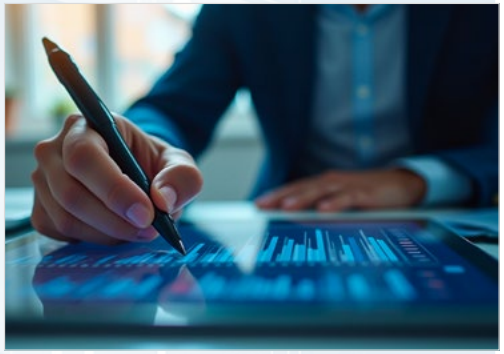
Sumario ejecutivo

Los resultados de este estudio muestran que el puesto de trabajo atraviesa una nueva etapa de madurez. Las organizaciones ya no están centradas en decidir si sus empleados deben trabajar desde la oficina, desde casa o en movilidad. El verdadero reto consiste en ofrecer acceso seguro a aplicaciones y datos desde cualquier lugar sin perder control, visibilidad ni capacidad de gestión.

El trabajo híbrido se ha consolidado como el modelo más extendido, presente en el 53,2 % de las organizaciones participantes. Al mismo tiempo, la nube continúa ganando protagonismo: cerca del 80 % de las empresas opera ya en entornos *cloud* o híbridos para el acceso a aplicaciones y datos. Sin embargo, la transición sigue conviviendo con infraestructuras heredadas y modelos de acceso tradicionales.

La seguridad destaca como la principal preocupación de los responsables de tecnología y ciberseguridad. La protección de accesos y dispositivos encabeza tanto los retos actuales como las prioridades de inversión para los próximos años. En paralelo, los modelos Zero Trust avanzan progresivamente, aunque más de la mitad de las organizaciones sigue apoyándose en tecnologías VPN para el acceso remoto.

La simplificación de la gestión aparece como otro de los grandes desafíos. Aunque la mayoría considera que la complejidad se mantiene bajo control, una de cada tres organizaciones reconoce enfrentarse a importantes dificultades derivadas de la integración de herramientas, plataformas y dispositivos.



La inteligencia artificial emerge como uno de los fenómenos más relevantes del estudio. El 95 % de las organizaciones ya utiliza esta tecnología de alguna forma, principalmente para mejorar la productividad, apoyar a los usuarios o automatizar procesos. Aunque los niveles de madurez son todavía dispares, la IA se ha incorporado de lleno a la agenda de transformación del puesto de trabajo.

En conjunto, la encuesta dibuja un escenario marcado por cuatro grandes prioridades: reforzar la seguridad, reducir la complejidad operativa, modernizar el acceso a aplicaciones y aprovechar el potencial de la inteligencia artificial. El puesto de trabajo del futuro será más flexible y más inteligente, pero también exigirá mayores niveles de control y capacidad de gestión.

El puesto de trabajo entra en una nueva etapa: más inteligente, más distribuido y más complejo de gestionar

El puesto de trabajo digital ha dejado de estar definido por un dispositivo. Hoy es un ecosistema en el que conviven aplicaciones SaaS, servicios cloud, identidades digitales, herramientas de inteligencia artificial y usuarios que trabajan desde múltiples ubicaciones. Al mismo tiempo, las organizaciones deben responder a mayores exigencias de seguridad, cumplimiento normativo y protección del dato.

Rosalía Arroyo

Esta evolución está obligando a replantear muchas estrategias. El reto ya no es únicamente proporcionar acceso a aplicaciones y datos, sino hacerlo garantizando una experiencia homogénea, manteniendo el control sobre la información y evitando que la seguridad se convierta en un freno para la productividad.

Para analizar cómo están afrontando este escenario las organizaciones, TAI Editorial reunió a responsables de tecnología y ciberseguridad de empresas privadas y organismos públicos en una nueva edición del Observatorio del Puesto de Trabajo. Durante el encuentro se abordaron cuestiones como la gestión de dispositivos, la virtualización, la inteligencia artificial, la soberanía digital, la monitorización de entornos distribuidos y la protección de la información.

Pese a la diversidad de sectores representados, los participantes coincidieron en una idea común: el futuro del puesto de trabajo dependerá de la capacidad de equilibrar productividad, experiencia de usuario, seguridad y gobierno del dato en entornos cada vez más complejos.

Productividad, acceso y control: el equilibrio que persigue el puesto de trabajo moderno

La primera cuestión planteada a los asistentes puso sobre la mesa uno de los grandes desafíos que afrontan actualmente las organizaciones: cómo ofrecer una experiencia de usuario homogénea en entornos donde los empleados trabajan desde múltiples ubicaciones, utilizan distintos dispositivos y acceden a un número creciente de aplicaciones, sin perder visibilidad ni control.

Las respuestas reflejaron realidades muy diferentes, pero también una preocupación común. Javier Villanueva, Global IS CX Architecture & Effectiveness Manager de ABB, situó la productividad como el principal indicador de éxito. La compañía opera en más de 90 países y necesi-

La IA, la movilidad y la experiencia digital están redefiniendo un puesto de trabajo donde productividad, seguridad y control deben avanzar de la mano

ta garantizar que sus empleados puedan trabajar con la misma eficacia independientemente del lugar desde el que accedan a los recursos corporativos. “Tengo que ser tan productivo en oficina como estoy en mi casa, o en cualquier lugar remoto”, resumió, añadiendo que para lograrlo, señaló, es necesario coordinar adecuadamente aspectos como la conectividad, los permisos, los accesos y las políticas de seguridad para que la experiencia no se vea afectada por el contexto.

Precisamente esa necesidad de ofrecer una experiencia consistente fue uno de los aspectos sobre los que incidió Cassia Cristina Nicolescu, New Models Business Unit Manager de Citrix. A su juicio, todas las organizaciones comparten el mismo objetivo: que el usuario pueda acceder a su entorno de trabajo sin importar el dispositivo utilizado, la ubicación desde la que se conecta o el tipo de aplicación que necesite utilizar. Sin embargo, advirtió de que alcanzar ese objetivo resulta cada vez más complejo porque los entornos tecnológicos son también cada vez más heterogéneos.

Según explicó, las empresas deben ser capaces de integrar aplicaciones SaaS, web y heredadas dentro de una experiencia unificada, al tiempo que aplican controles de acceso adaptados al contexto de cada usuario. “Tenemos que ofrecer un workspace que funcione igual en entornos híbridos”, defendió, destacando la importancia de que la experiencia sea consistente independientemente de dónde se encuentre el empleado o de cómo acceda a los recursos corporativos.

La identidad aparece como una de las herramientas clave para simplificar ese acceso. Lucía Martínez, CIO de AR Hotels explicó que en los en-

tornos que gestiona, una cadena hotelera y una consultora tecnológica con modelos de trabajo radicalmente distintos, el single sign-on se ha convertido en un elemento fundamental. “Para mí el single sign-on es clave”, afirmó. El objetivo es que el usuario pueda autenticarse una única vez y acceder desde ese momento a todas las aplicaciones autorizadas, manteniendo al mismo tiempo los controles necesarios para proteger la información y los dispositivos corporativos.

"La experiencia de usuario depende tanto de la conectividad y los permisos como de la capacidad de trabajar sin fricciones desde cualquier dispositivo"

Javier Villanueva, Global IS CX Architecture & Effectiveness Manager, **ABB**

La simplificación también fue uno de los conceptos más repetidos por Guillermo García Verdugo, Director de Puesto de Trabajo Digital en Madrid Digital. Desde su punto de vista, la mejor forma de gestionar la complejidad es reducirla desde el origen mediante la homogeneización de herramientas, equipos y mecanismos de acceso. "Lo que tratamos es de homogeneizar lo máximo posible", explicó. Aunque reconoció que todavía mantienen infraestructuras apoyadas en VPN, la organización ya está avanzando hacia modelos basados en ZTNA y nuevos sistemas de acceso más adaptados a los entornos actuales.

Para Cassia Cristina Nicolescu, el principal reto aparece precisamente cuando las organizaciones intentan combinar todas estas necesidades. Cada nueva capa de control, cada nueva herramienta de seguridad o cada nueva política de acceso puede introducir fricción en la experiencia del usuario y afectar a su productividad. Por ello defendió la necesidad de incorporar mecanismos de acceso inteligentes capaces de adaptar las políticas de seguridad en función de factores como el estado del dispositivo, la red utilizada, la ubicación o el nivel de riesgo asociado a cada conexión.

La portavoz de Citrix destacó además la importancia de optimizar el rendimiento tecnológico para evitar que la experiencia de usuario se vea penalizada por la complejidad de los entor-

"La identidad se ha convertido en la llave de acceso al puesto de trabajo moderno y el single sign-on es una pieza fundamental para simplificar la experiencia del usuario"

Lucía Martínez, CIO, **AR Hotels**

"La simplificación y la homogeneización tecnológica siguen siendo dos de las mejores herramientas para gestionar entornos complejos"

Guillermo García Verdugo, Director de Puesto de Trabajo Digital, **Madrid Digital**

nos actuales. A su juicio, las organizaciones no deberían verse obligadas a elegir entre experiencia de usuario y control. "Necesitamos una experiencia homogénea y el control total del entorno sin tener que elegir entre una cosa u otra", concluyó en su intervención.

Del control del dispositivo a la gestión de la experiencia digital

La conversación sobre la gestión de dispositivos puso de manifiesto hasta qué punto el puesto de trabajo ha evolucionado en los últimos años. Si hace una década las prioridades giraban en torno al inventario, el despliegue o el soporte técnico, hoy el foco se desplaza hacia la experiencia del empleado, la automatización y la capacidad de gestionar entornos cada vez más distribuidos desde plataformas unificadas.

Claudio Escudero, IT Manager Workplace de FCC, explicó durante su intervención que la compañía inició su proceso de transformación antes de la pandemia, una circunstancia que les permitió afrontar con mayor facilidad la transición hacia nuevos modelos de trabajo. La organización, presente en varias decenas de países y con actividades muy diversas, sustituyó progresivamente herramientas heredadas por plataformas capaces de gestionar de forma centralizada tanto equipos de usuario como dispositivos móviles, independientemente del fabricante. Tras varios años de evolución, considera que el control de la plataforma está razona-

"No basta con preguntar al usuario si está satisfecho; es necesario disponer de métricas objetivas que permitan entender qué ocurre realmente"

Claudio Escudero,
IT Manager Workplace, **FCC**

"El mejor puesto de trabajo es aquel que el usuario recibe listo para usar desde el primer minuto, sin configuraciones ni dependencias innecesarias"

Andrés García, IT Operations and Demand – IT Workplace Responsible, **MasOrange**

blemente resuelto. Ahora la atención se dirige hacia otro ámbito: "Nuestro foco ahora ya no es tanto en el control o en la capacidad de gestión, que yo creo que eso ya lo tenemos, sino en la introducción de herramientas que nos permitan medir la experiencia digital del empleado".

Una visión similar comparte Luis Ángel Hernando, Mobile Digital Workplace Manager de Grupo Adeo/Leroy Merlin. En su caso, la prioridad ya no pasa por comprobar si una aplicación funciona correctamente, sino por garantizar la disponibilidad del dispositivo antes de que aparezca cualquier incidencia. Explica que la organización utiliza capacidades de telemetría para anticiparse a posibles fallos y mantener la continuidad operativa en entornos con miles de terminales distribuidos entre tiendas y plataformas logísticas. Esta aproximación permite, además, optimizar el ciclo de vida del hardware y evitar sustituciones innecesarias, un aspecto especialmente relevante en un contexto de creciente presión sobre los costes tecnológicos.

La misma idea apareció también en las intervenciones posteriores. Martín Jones, IT Operations Manager de Cantabria Labs, describió un escenario marcado por el crecimiento internacional y la incorporación de nuevas compañías, cada una con sus propios entornos tecnológicos. El

"La unificación de entornos y la estandarización son fundamentales para gestionar organizaciones que crecen mediante adquisiciones e integración de compañías"

Martín Jones,
IT Operations Manager, **Cantabria Labs**

reto pasa ahora por unificar esa diversidad bajo modelos de gestión modernos basados en automatización, aprovisionamiento remoto y po-

líticas homogéneas de seguridad. El objetivo es que el usuario pueda recibir un equipo, autenticarse con sus credenciales corporativas y disponer desde el primer momento de todas las configuraciones y herramientas necesarias para trabajar. Al mismo tiempo, la compañía está impulsando iniciativas para medir el rendimiento del puesto de trabajo y garantizar una experiencia consistente independientemente de la ubicación desde la que se conecte el empleado.

La experiencia de MasOrange ejemplifica bien la velocidad a la que está evolucionando este ámbito. Andrés García, IT Operations and Demand – IT Workplace Responsible de la compañía, recordó que la integración entre Orange y MásMóvil obligó a reconciliar dos modelos de gestión completamente distintos: uno basado en infraestructuras tradicionales y procesos altamente estandarizados, y otro mucho más orientado a servicios cloud y automatización. La apuesta final fue avanzar hacia un modelo de gestión moderna completamente apoyado en la nube. “En seis meses hicimos la migración completa de los 8.000 PCs de on-prem al modelo cloud”, explicó. El resultado es un entorno donde el empleado recibe un dispositivo listo para usar, se identifica con sus credenciales corporativas y queda automáticamente integrado en las políticas de gestión y seguridad de la organización.

En la réplica, Enrique Martín, director de Gran Cuenta de Samsung Electronics, defendió que toda estrategia de gestión moderna debe construirse sobre una base de confianza y visibilidad porque “si hay algo que no sabes qué tienes, es difícil que controles nada”. Desde su punto de vista, el primer paso sigue siendo disponer de un inventario preciso de los dispositivos y conocer en todo momento su estado. A partir de ahí,

"La concienciación sigue siendo una de las herramientas de seguridad más eficaces frente a amenazas cada vez más sofisticadas"

Miguel Ángel Campos,
Responsable de Ciberseguridad, **Monbake**

considera fundamental garantizar la confianza en el hardware, la cadena de suministro y los mecanismos de protección incorporados desde el origen.

Sin embargo, el portavoz de Samsung coincidió con los responsables de TI en que el verdadero diferencial ya no está únicamente en la gestión del dispositivo, sino en la capacidad de comprender cómo lo está utilizando el empleado y si realmente le permite desarrollar su trabajo de forma eficiente. "Primero mediría que está siendo productivo y luego, por supuesto, si eres productivo normalmente sueles estar contento", afirmó.

La monitorización continua del estado de los equipos, las aplicaciones y la experiencia del usuario se perfila así como una de las próximas fronteras del puesto de trabajo digital. No sólo permite detectar incidencias antes de que afecten a la productividad, sino también actuar de forma proactiva sobre aspectos tan diversos como el rendimiento de una aplicación, el estado de una batería o el cumplimiento de las políticas de seguridad. En definitiva, el dispositivo deja de ser un elemento aislado para convertirse en una fuente constante de información que ayuda a mejorar tanto la experiencia del empleado como la eficiencia operativa de la organización.

"El reto ya no es decidir si se adopta la inteligencia artificial, sino cómo gobernarla y controlar el uso que se hace de los datos"

Daniel Gonzalo Gago,
Iberia and LATAM CISO, **Nalanda Global**

El eslabón más débil ya no es el dispositivo: ahora es la confianza

Cuando se abordó la evolución de la seguridad en el puesto de trabajo, el debate dejó cla-

"La seguridad debe ser el punto de partida sobre el que se construyen la experiencia de usuario y la productividad"

Ricardo Ranz Pérez,
End User Support Service Manager, **Allfunds**

ro que las prioridades han cambiado. Aunque la protección de los dispositivos sigue siendo importante, la preocupación ya no se centra únicamente en evitar infecciones por malware o bloquear accesos no autorizados. El foco se está desplazando hacia riesgos mucho más difíciles de controlar: la ingeniería social, la manipulación mediante inteligencia artificial y la exposición involuntaria de información sensible por parte de los propios usuarios.

Miguel Ángel Campos, responsable de Ciberseguridad de Monbake, resumió bien esta evolución. Tras haber trabajado en entornos altamente controlados y en otros mucho más abiertos, reconoció que durante años la principal preocupación era impedir que un malware alcanzara el puesto de trabajo. Sin embargo, la realidad actual es diferente: "El foco que estamos viendo va más no por la parte de vamos a proteger el puesto de trabajo contra programas, sino contra la ingeniería social, los atacantes, las voces que te genera la IA o los mensajes que te genera la IA". La compañía ha reforzado por ello sus programas de concienciación y formación, incorporando ejercicios prácticos dirigidos tanto a empleados como a directivos

Si la ingeniería social preocupa cada vez más, la inteligencia artificial añade una nueva capa de complejidad. Para Daniel Gonzalo Gago, CISO para Iberia y Latinoamérica de Nalanda Global,

"La gestión de identidades y privilegios se ha convertido en una pieza esencial para controlar entornos cada vez más heterogéneos"

José Andrés Jiménez, jefe del Departamento de Asesoría TIC, **Congreso de los Diputados**

muchas organizaciones están pasando del problema del Shadow IT al del Shadow AI. A su juicio, el debate ya no consiste en decidir si la IA debe adoptarse o no, sino en cómo gobernarla

"La seguridad no puede convertirse en un freno para el negocio, pero tampoco puede sacrificarse en nombre de la comodidad"

Javier Arnaiz,
Socio de Ciberseguridad y Privacidad, **Écija Abogados**

adecuadamente. El principal desafío, explicó, aparece cuando las capacidades de inteligencia artificial se integran de forma transparente dentro de aplicaciones de uso cotidiano; "nos encontramos situaciones en las que los empleados dicen: he subido esta nómina a esta inteligencia artificial para que me haga un resumen", señaló, añadiendo que en muchos casos resulta difícil conocer dónde se almacenan esos datos, qué modelos los procesan o qué uso posterior se hará de ellos.

La preocupación por la pérdida de control sobre la información enlazó directamente con la visión aportada por Iván Mateos, Sales Engineer de Sophos Iberia. El directivo defendió que la ciberseguridad ha dejado de ser un complemento para convertirse en la base sobre la que se construyen todos los proyectos de transformación digital. "La ciberseguridad ya es el pilar que hace que todo eso no se caiga", afirmó, en referencia a iniciativas relacionadas con productividad, movilidad, automatización o experiencia de usuario.

Desde su punto de vista, proteger el puesto de trabajo exige abordar simultáneamente múltiples frentes. La formación de los usuarios sigue siendo tan importante como las herramientas tecnológicas, especialmente en un contexto en el que los atacantes combinan técnicas tradicionales con nuevas capacidades impulsadas

"La soberanía digital se perfila como una de las grandes prioridades tecnológicas de los próximos años"

Óscar Rodrigo Villar, subdirector General de Calidad de los Servicios Digitales y Ciberseguridad, **Ministerio de la Presidencia, Justicia y Relaciones con las Cortes**

por IA. Al mismo tiempo, las organizaciones deben reforzar la protección de identidades, la gestión de vulnerabilidades y la capacidad de respuesta ante incidentes, ya que los atacantes continúan encontrando nuevas formas de apro-

vechar fallos en infraestructuras y sistemas de acceso remoto.

Por otra parte, destacó Mateos una tendencia cada vez más visible en el mercado: las empresas están dejando de demandar únicamente productos para empezar a buscar servicios gestionados capaces de complementar unos equipos internos que, en muchos casos, no disponen de los recursos suficientes para cubrir todas las necesidades de vigilancia y respuesta. "Las compañías están dejando de pedir producto y directamente están pidiendo MDR", explicó.

La virtualización busca un nuevo papel en la era del SaaS, la IA y la resiliencia

La conversación sobre virtualización puso de manifiesto que esta tecnología atraviesa una etapa de redefinición. Lejos de los años en los que se asociaba principalmente a la reducción de costes o a la centralización de infraestructuras, hoy se enfrenta a nuevos retos vinculados a los entornos SaaS, la inteligencia artificial, la flexibilidad operativa y la continuidad de negocio.

Ángel Bascones, CIO de Vannilo Holding, expuso algunas de las dificultades que encuentran determinadas organizaciones a la hora de incorporar modelos de virtualización en determinados entornos de trabajo. En el caso de su actividad financiera, explicó que gran parte de las herramientas utilizadas por los analistas son aplicaciones SaaS o desarrollos muy específicos apoyados en Excel como plataforma principal de trabajo. "Aquí no somos capaces de utilizar escritorios virtuales", reconoció, apuntando a la complejidad que supone trasladar determinados procesos financieros altamente personalizados a modelos virtualizados.

La reflexión conectó con otra preocupación recurrente a lo largo del debate: el impacto de la inteligencia artificial en el puesto de trabajo. Methane Rahman, CIO / Head of Financial Cri-

"La productividad que aporta la IA solo será sostenible si se gestiona adecuadamente el riesgo asociado a la información"

Alejandro Velilla, CTO Embou-MasOrange, Alejandro Velilla, CTO **Embou-MasOrange**

me Risk and Compliance, Independent Advisor (Former Santander CIB & PagoNxt), con una amplia trayectoria en el sector financiero internacional, destacó que las organizaciones se encuentran todavía en una fase de aprendizaje respecto a cómo incorporar estas capacidades sin comprometer la seguridad, el cumplimiento normativo o la confidencialidad de la información. Según explicó, muchas compañías operan con datos especialmente sensibles y deben encontrar mecanismos que permitan aprovechar el potencial de la IA sin perder el control sobre la información. "Estamos en una etapa de nuevo mundo, de aprendizaje", resumió.

La formación volvió a emerger como uno de los factores clave para afrontar este escenario. Darío Ferraté, Gerente TIC de Ineco, defendió que la velocidad a la que evolucionan tanto las amenazas como las capacidades de la IA obliga a reforzar constantemente el conocimiento de los usuarios. A su juicio, tan importante como disponer de tecnología adecuada es que las personas entiendan qué pueden hacer, qué no deben hacer y cuáles son los riesgos asociados al uso de determinadas herramientas. "Siempre ante la duda hay que ser bastante cautos", señaló, recordando que muchas organizaciones siguen trabajando para evitar que los empleados compartan información sensible con plataformas que no ofrecen las garantías adecuadas.

"La incorporación de inteligencia artificial en sanidad debe avanzar al mismo ritmo que las garantías de protección de los datos clínicos"

Pedro Galbarro,
director del Área de Aplicaciones, **Vithas**

Durante su intervención Guillermo García Verdugo, Director de Puesto de Trabajo Digital de Madrid Digital, se mostró sorprendido por uno de los resultados del Observatorio: el reduci-

"La virtualización debe adaptarse a las necesidades reales del negocio y no al revés"

Ángel Bascones, CIO, **Vannilo Holding**

do porcentaje de organizaciones que identificaban la continuidad de negocio como uno de los principales motivos para apostar por la virtualización. "Me ha chocado mucho el tema de garantizar continuidad de negocio", comentó, planteando si la virtualización no debería desempeñar un papel mucho más relevante dentro de las estrategias de resiliencia empresarial.

La cuestión sirvió de punto de partida para la intervención de Fernando Feliu, executive managing director de Virtual Cable, quien defendió precisamente que la continuidad de negocio constituye hoy uno de los grandes argumentos a favor de la virtualización. Desde su punto de vista, la posibilidad de disponer de entornos redundantes, distribuidos y accesibles desde cualquier ubicación permite responder mejor tanto a incidentes tecnológicos como a requisitos regulatorios cada vez más exigentes. "La virtualización sí es una buena solución para la continuidad de negocio", afirmó, recordando además que normativas como DORA sitúan la resiliencia operativa en el centro de las estrategias tecnológicas.

Feliu sostuvo que la virtualización ha evolucionado mucho más allá del escritorio tradicional. Hoy permite controlar el acceso a aplicaciones, datos e incluso agentes de inteligencia artificial, definiendo qué recursos puede utilizar cada usuario y en qué condiciones. Todo ello sin necesidad de preparar equipos específicos ni de vincular la experiencia de trabajo a un dispositivo concreto. "Simplemente con cualquier navegador ya entran directamente a todo su entorno, con todas sus aplicaciones y con todos sus permisos", explicó.

"La trazabilidad y la capacidad de auditoría serán elementos fundamentales en los futuros entornos de trabajo impulsados por IA"

Methane Rahman, CIO / Head of Financial Crime Risk and Compliance, **Independent Advisor (Former Santander CIB & PagoNxt)**

"La formación continua es la mejor herramienta para afrontar un entorno tecnológico que cambia más rápido que nunca"

Darío Ferraté,
Gerente TIC, **Ineco**

El directivo defendió además que este enfoque facilita la implantación de modelos Zero Trust, simplifica la gestión de identidades y reduce el impacto de amenazas como el ransomware al mantener los datos y aplicaciones bajo control centralizado. También destacó la flexibilidad que aporta a organizaciones con infraestructuras heterogéneas, permitiendo combinar entornos cloud, on-premise e híbridos bajo una gestión unificada.

El debate evidenció así que la virtualización sigue teniendo un papel relevante dentro de las estrategias de puesto de trabajo, aunque sus objetivos están cambiando. Más que una herramienta para consolidar infraestructuras o reducir costes, empieza a posicionarse como una tecnología orientada a mejorar la resiliencia, simplificar la gestión, reforzar el control sobre los accesos y proporcionar una experiencia de trabajo consistente en entornos cada vez más distribuidos y complejos.

Seguridad sí, pero sin impedir que el negocio funcione

Cuando se planteó qué preocupa más actualmente en el acceso a aplicaciones y datos —la seguridad, la experiencia de usuario, la complejidad de gestión o la integración de todos estos elementos—, las respuestas dejaron claro que las organizaciones ya no pueden permitirse abordar estas cuestiones de forma aislada. El

"La IA tendrá éxito cuando desaparezca como tecnología visible y se integre de forma natural en los procesos cotidianos"

Enrique Martín,
director de Gran Cuenta, **Samsung Electronics**

reto consiste precisamente en hacerlas convivir. Ricardo Ranz, Service manager end user de Allfunds, fue directo al señalar cuál es la prioridad sobre la que se construye todo lo demás. "Lo

"El futuro del puesto de trabajo pasa por combinar gestión centralizada, soberanía del dato y capacidad de adaptación a nuevos modelos de uso"

Fernando Feliu,
executive managing director, **Virtual Cable**

más importante ahora mismo es la seguridad", afirmó. A su juicio, la protección de los accesos y de la información debe ser la base sobre la que posteriormente se construyen experiencias más ágiles, accesibles y eficientes para los usuarios. Pero esa protección no depende únicamente de la tecnología. La formación continua, la cultura de seguridad y la concienciación de los empleados siguen siendo elementos fundamentales para reducir el riesgo.

Sin embargo, la realidad de las organizaciones demuestra que encontrar el equilibrio no siempre resulta sencillo. José Andrés Jiménez, Jefe del Departamento de Asesoría TIC del Congreso de los Diputados, describió un entorno especialmente complejo, donde conviven perfiles muy diversos, distintas formas de trabajar y una elevada rotación de usuarios. En ese contexto, explicó, la ciberseguridad es un requisito irrenunciable, pero la experiencia de usuario también se convierte en una necesidad operativa. "Tenemos que amoldarnos a esas formas de trabajar que ya traen importadas", señaló.

Para gestionar esa complejidad, el Congreso ha puesto el foco en la gestión de identidades, accesos y privilegios, construyendo una base común que permita identificar correctamente a cada usuario y definir con precisión qué recursos puede utilizar. Un aspecto especialmente

"Las organizaciones no deberían verse obligadas a elegir entre productividad, control y seguridad; el reto consiste en equilibrar las tres dimensiones"

Cassia Cristina Nicolescu,
New Models Business Unit Manager, **Citrix**

relevante en un momento en el que la proliferación de herramientas de inteligencia artificial está multiplicando los escenarios de Shadow IT y Shadow AI dentro de las organizaciones.

"La ciberseguridad ha dejado de ser un complemento para convertirse en el pilar que sostiene toda la estrategia de puesto de trabajo digital"

Iván Mateos,
Sales Engineer de **Sopho** Iberia

Para Javier Arnaiz, Socio de Ciberseguridad y Privacidad de Écija Abogados, uno de los grandes desafíos sigue siendo encontrar el equilibrio entre seguridad y operativa. "La seguridad está muy bien, pero tenemos que seguir trabajando", resumió, añadiendo que, desde su experiencia, muchas medidas de protección encuentran resistencia cuando afectan al día a día de los usuarios, aunque reconoció que la percepción del riesgo ha cambiado y que las organizaciones son hoy mucho más conscientes de la necesidad de prevenir incidentes.

El experto advirtió además de los nuevos riesgos asociados a la inteligencia artificial. Cada vez es más frecuente que empleados utilicen herramientas de IA no autorizadas para procesar información corporativa o datos de clientes, lo que puede derivar en incumplimientos de las políticas internas o en exposiciones involuntarias de información sensible. A su juicio, el reto ya no es solo qué herramienta se utiliza, sino qué datos se comparten con ella y bajo qué condiciones.

Tras escuchar las distintas experiencias, Cassia Cristina Nicolescu, de Citrix, defendió que el verdadero problema ya no es funcional ni tecnológico, sino arquitectónico. Según explicó, las organizaciones han acumulado durante años herramientas diseñadas para resolver necesidades concretas, pero ahora necesitan integrarlas de forma coherente para evitar complejidad adicional. Asegurando que "el problema no es la falta de herramientas, sino que se conecten, se integren y sean coherentes entre

"La monitorización ya no consiste en detectar fallos, sino en anticiparse a ellos antes de que afecten a la actividad del usuario"

Luis Ángel Hernando, Mobile Digital Workplace Manager, **Grupo Adeo / Leroy Merlin**

ellas", considera que el mercado está evolucionando hacia plataformas cada vez más integradas, capaces de combinar seguridad, gestión, experiencia de usuario y control desde una misma capa tecnológica. A su juicio, el objetivo no debe ser obligar a las organizaciones a elegir entre protección, flexibilidad o productividad, sino construir entornos en los que todos esos elementos puedan coexistir.

La IA llegará al puesto de trabajo, pero su éxito dependerá del control y del caso de uso

La incorporación de inteligencia artificial a ordenadores, móviles y otros dispositivos de usuario fue otro de los temas que centró el debate. Aunque la tecnología avanza rápidamente y los fabricantes ya están integrando capacidades de IA directamente en los equipos, los asistentes coincidieron en que el verdadero desafío no está en disponer de la tecnología, sino en gobernarla adecuadamente y encontrar casos de uso que aporten valor real.

Alejandro Velilla, CTO de Embou-MasOrange, explicó que la inteligencia artificial ya forma parte de la actividad cotidiana de la compañía y que su adopción está creciendo de forma significativa entre los empleados. La organización trabaja con distintos modelos y asistentes y ha impulsado activamente su utilización como una herramienta para mejorar la productividad, optimizar procesos y ayudar en tareas repetitivas. Sin embargo, advirtió de que esta evolución también obliga a gestionar nuevos riesgos. "Tiene sus pros y sus contras", señaló al referirse a las diferencias existentes entre las distintas plataformas de IA. No todas ofrecen las mismas garantías en aspectos como la privacidad, la ubicación de los datos o la integración con los sistemas corporativos. A su juicio, el desafío consiste en aprovechar las ventajas que aporta la inteligencia artificial sin perder de vista la protección de la información, un aspecto que debe acompañar cualquier estrategia de adopción tecnológica.

Pedro Galbarro, director del área de aplicaciones de Vithas, recordó que la gestión del puesto de trabajo en el ámbito sanitario presenta una complejidad especial debido a la diversidad de perfiles profesionales y necesidades existentes dentro de una organización de este tipo. “Si algo falla ahí, no es tan importante como que se te escape un dato de un paciente”, advirtió al explicar cómo condiciona la seguridad cualquier decisión relacionada con la adopción tecnológica.

En este contexto, la incorporación de capacidades de inteligencia artificial avanza de forma progresiva y controlada. A su juicio, el principal desafío no es tecnológico, sino garantizar que cualquier nueva herramienta aporte valor sin comprometer la seguridad ni la confidencialidad de los datos sanitarios.

La intervención de Enrique Martín, de Samsung, aportó una visión más amplia sobre cómo evolucionará la relación entre los usuarios y la inteligencia artificial durante los próximos años. A su juicio, la mayoría de los empleados no demandan específicamente IA, igual que en su día tampoco pidieron 4G o 5G. Lo que realmente buscan es resolver problemas de forma más rápida y eficiente: “Al usuario le da igual la inteligencia artificial; lo que quiere es que el problema se le solucione”, afirmó.

> El puesto de trabajo digital exige combinar productividad, seguridad y experiencia de usuario en entornos cada vez más distribuidos

Aseguró el directivo que “la inteligencia artificial va a desaparecer dentro del dispositivo”, que acabará integrándose de forma natural en los dispositivos y aplicaciones hasta resultar prácticamente invisible. En lugar de interactuar conscientemente con una herramienta específica, los usuarios utilizarán procesos automatizados que les permitirán completar tareas cotidianas con menos esfuerzo y en menos tiempo.

También defendió Enrique Martin que los proyectos más exitosos no son necesariamente los más ambiciosos, sino aquellos que eliminan pequeñas fricciones en actividades muy concretas. Citó como ejemplo los sistemas de transcripción asistida para profesionales sanitarios, capaces de registrar automáticamente una consulta médica para que posteriormente el facultativo valide la información antes de incorporarla a la historia clínica. También mencionó escenarios industriales donde la IA ayuda a los operarios a acceder al conocimiento necesario en cada momento sin tener que consultar manuales o documentación compleja.

En todos los casos, insistió, la clave sigue siendo la misma: combinar productividad, control y seguridad. Para ello, considera fundamental disponer de mecanismos que permitan decidir qué información puede utilizar cada agente de IA, qué datos permanecen en local y cuáles pueden compartirse con modelos externos. La capacidad de orquestar esos flujos de información será, a su juicio, uno de los elementos diferenciales de los dispositivos inteligentes de nueva generación.

La visibilidad total sigue siendo una aspiración, no una realidad

La pregunta sobre si las organizaciones disponen realmente de visibilidad completa sobre lo que ocurre en el puesto de trabajo generó una de las respuestas más sinceras de toda la jornada. A medida que proliferan los dispositivos, las aplicaciones SaaS, las herramientas de inteligencia artificial y los entornos híbridos, los responsables de tecnología y ciberseguridad reconocen que mantener un control absoluto resulta cada vez más complejo.

Óscar Rodrigo Villar, subdirector general de Calidad de los Servicios Digitales y Ciberseguridad del Ministerio de la Presidencia, Justicia y Relaciones con las Cortes, aportó la perspectiva de una organización sometida a fuertes exigencias regulatorias y operativas. Explicó que la gestión de estos entornos está condicionada por numerosos factores que van más allá de la tecnología, al tiempo que señalaba que la implantación de nuevas medidas de seguridad no depende únicamente de criterios técnicos, sino también de aspectos legales, organizativos y operativos. En un entorno donde los usuarios desempeñan

funciones altamente especializadas y trabajan bajo marcos normativos muy exigentes, cualquier cambio puede requerir un delicado equilibrio entre protección, usabilidad y servicio. En tono distendido, llegó a afirmar que “nuestro cliente es nuestro principal enemigo”, una forma de ilustrar las dificultades que supone reforzar la seguridad sin afectar a la actividad diaria de los usuarios.

Frente a esa visión, Carlos Maza, subdirector TIC del Tribunal de Cuentas, defendió que la clave no consiste en aspirar a una visibilidad absoluta, sino en construir tantas capas de control como sea posible. La institución gestiona información extremadamente sensible procedente de todos los niveles de la administración pública y, por ello, la seguridad ocupa un lugar central en toda la estrategia tecnológica. “La ci-

La virtualización, la gestión centralizada y la soberanía del dato ganan protagonismo como pilares para construir un puesto de trabajo más flexible

berseguridad no es una prioridad, es una obsesión", aseguró.

Para reforzar ese control, el organismo combina herramientas de monitorización, servicios del Centro Criptológico Nacional, tecnologías EDR y XDR, plataformas de gestión de dispositivos móviles y nuevas capacidades de análisis sobre los flujos de información que entran y salen de la organización. Gracias a ello, dispone de una visión muy detallada de cómo interactúan los usuarios con aplicaciones, servicios cloud y herramientas de inteligencia artificial.

Ricardo Ranz, End User Support Service Manager de Allfunds, aseguró que los controles tecnológicos existen y están desplegados sobre los distintos entornos de usuario, pero que el verdadero reto continúa siendo el comportamiento de las personas. "El problema es el control de ese usuario, esa concienciación que hay que tener sobre qué hacer, cómo acceder y que no caigan en las trampas", explicó.

La inteligencia artificial añade además una nueva dimensión al problema. Consideraba Iván Mateos, durante su intervención que la cuestión ya no es si una organización tiene visibilidad completa sobre todo lo que ocurre, porque la respuesta inevitablemente será negativa. Lo importante es maximizar esa visibilidad y ser capaces de reaccionar con mayor rapidez. A su juicio, la IA está actuando como una prueba de estrés para todo el ecosistema tecnológico. Por un lado, obliga a las organizaciones a controlar qué herramientas utilizan los empleados, qué información comparten con ellas y dónde terminan almacenados esos datos. Por otro, está acelerando el ritmo de descubrimiento y explotación de vulnerabilidades hasta niveles desconocidos hasta ahora.

Mateos advirtió de que los modelos más avanzados ya son capaces de identificar vulnerabilidades y generar exploits en cuestión de minutos, reduciendo drásticamente el tiempo de reacción disponible para fabricantes y organizaciones. Este nuevo escenario obliga a replantear algunos de los enfoques tradicionales de protección. "La carrera de las vulnerabilidades es una carrera que hay que abandonar", afirmó, defendiendo una estrategia basada en el análisis de comportamientos y técnicas de ataque, más que en la simple aplicación de parches o la identificación de amenazas conocidas.

Flexibilidad, soberanía y control: las prioridades del puesto de trabajo que viene

La última pregunta del debate invitó a los participantes a mirar hacia atrás para identificar qué harían de forma diferente si tuvieran que rediseñar hoy su estrategia de puesto de trabajo. Las respuestas reflejaron hasta qué punto han cambiado las prioridades durante los últimos años y cómo conceptos como soberanía digital, gobierno del dato o flexibilidad operativa están ganando protagonismo frente a otros debates

que hace apenas cinco años ocupaban el centro de la conversación.

Desde el ámbito financiero, Methane Rahman planteó una reflexión centrada en la trazabilidad y el control. A su juicio, las organizaciones necesitan avanzar hacia entornos capaces de ofrecer una visibilidad mucho más detallada sobre qué ocurre con los datos, cómo se utilizan y quién accede a ellos. En sectores altamente regulados, donde las obligaciones de auditoría y cumplimiento son cada vez mayores, considera imprescindible disponer de mecanismos que permitan seguir el recorrido de la información y demostrar que cada proceso se ha realizado conforme a las exigencias regulatorias. “Me gustaría ver algún día mucha más trazabilidad y seguridad”, resumió.

Una preocupación que conecta directamente con otro de los conceptos que apareció durante el cierre del encuentro: la soberanía digital. Óscar Rodrigo Villar, del Ministerio de la Presidencia, Justicia y Relaciones con las Cortes, se mostró especialmente contundente sobre este aspecto. “La soberanía digital va a ser nuestro único motor”, afirmó. Aunque reconoció que su organización mantiene una presencia limitada en entornos cloud, advirtió de que incluso esa pequeña dependencia puede convertirse en una fuente de complejidad operativa en los próximos años, especialmente a medida que aumenten las exigencias regulatorias y las preocupaciones sobre el control de los datos.

No todos los participantes compartieron esa visión. Andrés García defendió precisamente el camino contrario a partir de la experiencia vivida durante la integración entre Orange y MásMóvil. Frente a quienes apostaban por mantener modelos más tradicionales, la organización decidió adoptar el enfoque cloud que utilizaba

MásMóvil y trasladarlo a una estructura mucho mayor. “Volvería a hacer exactamente lo mismo”, aseguró. La migración de miles de usuarios hacia un modelo completamente basado en la nube demostró, a su juicio, que la simplicidad operativa, la automatización y la facilidad de gestión pueden convertirse en ventajas decisivas cuando se ejecutan correctamente.

Las distintas posiciones reflejan una realidad que estuvo presente durante toda la jornada: no existe un modelo único de puesto de trabajo válido para todas las organizaciones. Las necesidades de una entidad financiera, un organismo público, una compañía de telecomunicaciones o un hospital son radicalmente distintas, tanto desde el punto de vista operativo como regulatorio.

Sobre esa idea construyó Fernando Feliu, de Virtual Cable, buena parte de su intervención de cierre. El directivo destacó que la diversidad de experiencias compartidas durante el debate demuestra precisamente que el puesto de trabajo debe ser capaz de adaptarse a contextos muy diferentes, manteniendo siempre un equilibrio entre control, seguridad y experiencia de usuario.

> La inteligencia artificial abre nuevas oportunidades para mejorar la eficiencia, pero también obliga a reforzar la gobernanza, la protección del dato y la formación de los usuarios para reducir nuevos riesgos

A su juicio, tres conceptos marcarán la evolución de los próximos años: flexibilidad, seguridad y robustez. Sin embargo, advirtió de que estos objetivos solo pueden alcanzarse si las organizaciones son capaces de gestionar de forma centralizada identidades, accesos, datos y recursos tecnológicos. El crecimiento de la inteligencia artificial añade además nuevos desafíos. Según recordó, cada vez es más habitual que los propios empleados incorporen agentes y herramientas inteligentes a su actividad diaria, generando nuevos riesgos relacionados con el cumplimiento normativo, la protección de la información y la gobernanza del dato.

Feliu insistió también en la importancia de la soberanía tecnológica y de mantener el control sobre la información crítica de las organizaciones. “El dato es el bien más preciado que tiene cualquier compañía”, afirmó. Por ello, considera que la seguridad del futuro no dependerá únicamente de proteger infraestructuras o dispositivos, sino de controlar quién accede a la información, cómo se utiliza y bajo qué condiciones puede ser procesada por nuevas herramientas y servicios.

La conversación concluyó así con una idea que resume buena parte de los mensajes escuchados durante la jornada. El puesto de trabajo del futuro será más inteligente, más distribuido y más flexible que el actual, pero también estará condicionado por nuevas exigencias de control, soberanía y cumplimiento. Y, aunque la tecnología seguirá evolucionando a gran velocidad, el verdadero reto seguirá siendo el mismo: encontrar el equilibrio adecuado entre productividad, experiencia de usuario, seguridad y gobierno del dato.

Experiencia de usuario, el gran motor del *digital workplace*, según Citrix

La experiencia de usuario se ha convertido en el gran eje de transformación del puesto de trabajo digital. En este vídeo, Cassia Nicolescu, *new model* Citrix *Business Unit manager*, analiza cómo las organizaciones están afrontando los retos de integrar aplicaciones, datos y dispositivos en entornos cada vez más distribuidos. Un análisis en el que aborda cuestiones como la virtualización, la inteligencia artificial, el dispositivo como servicio, la seguridad *zero trust* y el papel del *edge* en el futuro del trabajo y en el que se refleja la evolución del puesto de trabajo digital hacia modelos más flexibles, seguros y centrados en el usuario.

Cassia Nicolescu, *new model* **Citrix** *Business Unit manager*

"El futuro del puesto de trabajo pasa por la continuidad entre móvil, PC y *tablet*"

La inteligencia artificial está transformando la manera en que trabajamos, modificando el papel de las personas dentro de las organizaciones y redefiniendo el concepto de puesto de trabajo digital. En esta entrevista, Enrique Martín, director de gran cuenta de Samsung, analiza cómo está impulsando la productividad, especialmente entre los profesionales que trabajan fuera de la oficina. Un nuevo escenario en el que el puesto de trabajo evoluciona hacia un modelo más inteligente, conectado y centrado en la experiencia de usuario.

Enrique Martín, director de gran cuenta de **Samsung**

Navegadores seguros y MDR: las nuevas prioridades de las empresas

Los ciberataques son cada vez más numerosos, rápidos y sofisticados. En este vídeo Iván Mateo, ingeniero preventa de Sophos, analiza cómo están cambiando las amenazas y cuáles son los errores que siguen cometiendo muchas organizaciones al proteger a sus empleados remotos. El experto destaca los desafíos actuales de la ciberseguridad, con un trabajo híbrido que ha transformado la manera en la que las organizaciones operan. Una evolución que ha traído un aumento de los riesgos de ciberseguridad con la combinación de movilidad, entornos *cloud*, acceso remoto y herramientas de inteligencia artificial, modificando el panorama de amenazas al que se enfrentan las empresas.

Iván Mateo, ingeniero preventa de **Sophos**

Zero trust y virtualización, combinación clave para el trabajo híbrido

La virtualización se está consolidando como uno de los pilares fundamentales del puesto de trabajo digital. En esta entrevista Fernando Feliu, *executive managing director* de Virtual Cable, analiza cómo las organizaciones están utilizando esta tecnología para simplificar la gestión de infraestructuras, reforzar la seguridad y controlar el uso de la inteligencia artificial en entornos corporativos. Además, aborda el auge de las soluciones basadas en tecnologías abiertas, los beneficios del modelo *zero trust* y el papel que desempeña la virtualización en la protección de los datos empresariales.

Fernando Feliu, *executive managing director* de **Virtual Cable**