Dell Technologies recomienda la plataforma Intel vPro®: diseñada para la empresa

Los empleados están eligiendo su forma de trabajar

Y, con la estrategia digital segura adecuada, esto podría resultar muy beneficioso para su empresa: hoy y en el futuro

DELL Technologies

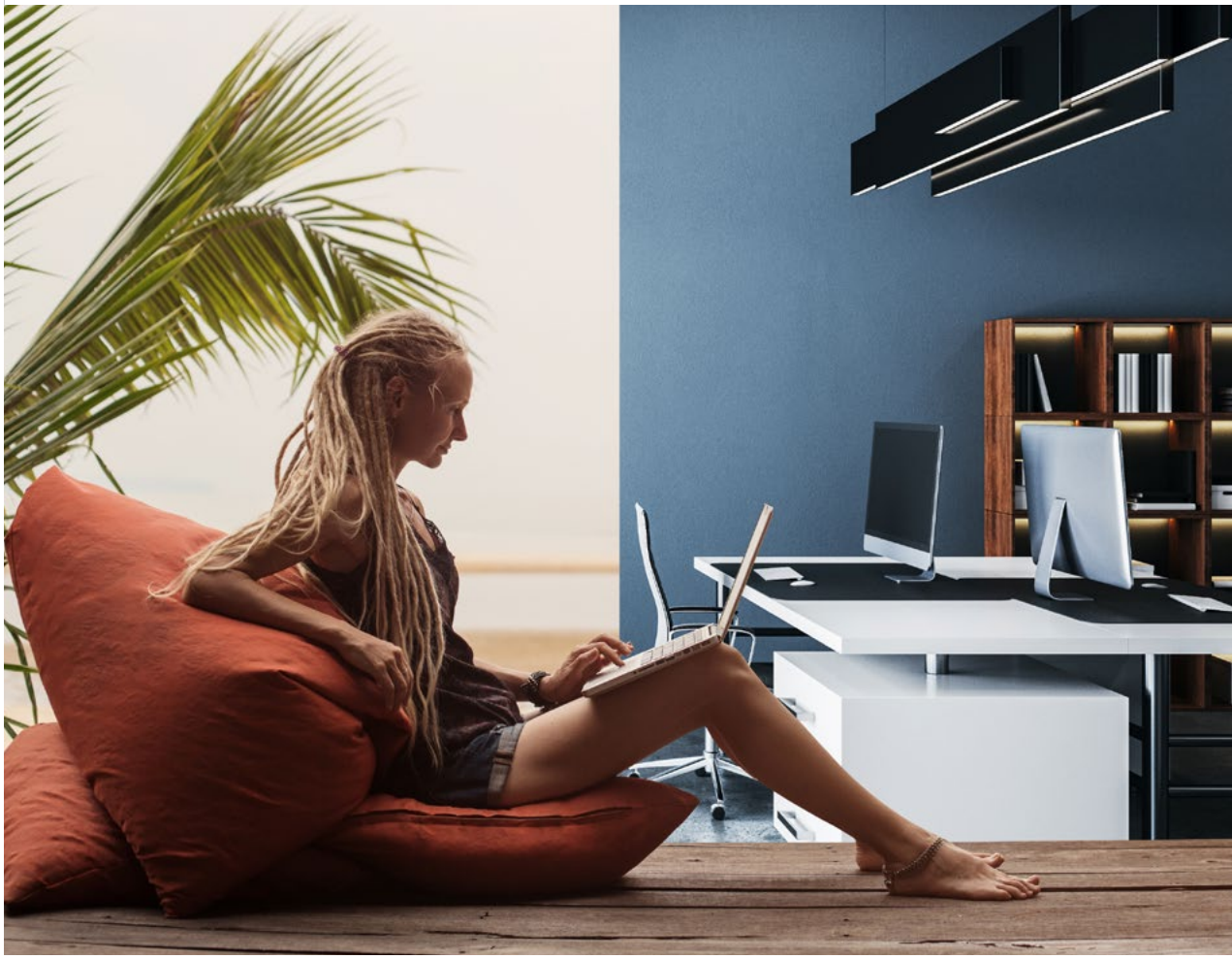
Innovation Built-In intel

Contenido

1

El trabajo ha cambiado y volverá a hacerlo

Los empleados están redefiniendo el lugar de trabajo como nunca y las empresas inteligentes están sacando provecho de ello



Contenido

"La medida de la inteligencia es la capacidad de cambiar".

Esta cita, atribuida a Albert Einstein, es especialmente aplicable al cambio sísmico que se está produciendo hoy en día en nuestros lugares de trabajo. Es difícilmente discutible que nuestra forma de trabajar actual es muy diferente a la de hace unos pocos años. Independientemente de que las posibilidades del cambio les perturben o les entusiasmen, las organizaciones han tenido que mejorar sus estrategias tecnológicas para permitir que las personas trabajen desde cualquier lugar e interactúen con los clientes de nuevas formas digitales.

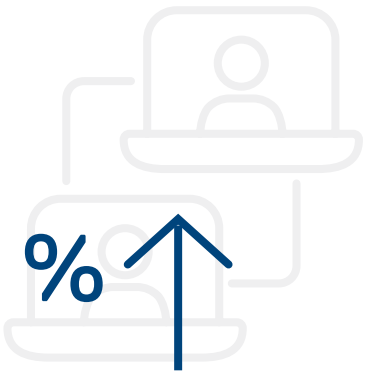
Para mantenerse conectados, productivos y seguros en un mundo en el que muchas formas de trabajo se pueden llevar a cabo de forma remota, los empleados necesitan confiar en que el entorno digital no obstaculizará su capacidad para hacer su trabajo lo mejor posible. Una investigación global de Statista demuestra que el 80 % de los empleados que trabajan al menos de forma parcialmente remota se lo recomendaría a un amigo. Sin embargo, como indica el estudio: "La actitud en el teletrabajo es positiva si a los empleados se les ofrecen las herramientas y la tecnología adecuadas para trabajar de forma remota. Entre ellas se incluyen las herramientas de gestión de la productividad y colaboración digital, así como el hardware necesario".[1]

Estas actitudes están cambiando profundamente el papel de la función de TI dentro de las organizaciones de todo el mundo. Ahora más que nunca, el papel de los líderes de TI a la hora de ofrecer una experiencia digital moderna a los empleados, brindándoles un acceso seguro a todas las herramientas y recursos necesarios para los diferentes roles, está proporcionando una clara ventaja de productividad a las empresas más vanguardistas. Por ejemplo, un estudio realizado en 2021 determinó que las personas con acceso al teletrabajo aumentaron la innovación en un 63 %, la participación laboral en un 75 % y el compromiso organizativo en un 68 %.[2]

Priorizar la experiencia de los empleados

Los equipos de TI son muy conscientes de esta creciente responsabilidad. El análisis de Gartner predice que "para 2025, más del 50 % de las organizaciones de TI utilizarán la experiencia digital de los empleados para priorizar y medir el éxito de las iniciativas digitales, lo que representa un aumento significativo respecto al menos del 5 % de 2021".[3] Existe un claro cambio hacia la colocación de las necesidades digitales específicas de los empleados en el núcleo de la estrategia digital, con la TI como motor para crear nuevas oportunidades de negocio a medida que el lugar de trabajo evoluciona hoy y lo sigue haciendo en el futuro.

En este documento, Dell Technologies y nuestros socios de Intel analizan los retos y las oportunidades principales que surgen del lugar de trabajo cambiante. Juntos definimos las mejores prácticas de liderazgo en TI que garantizarán que los empleados puedan trabajar, colaborar e innovar de forma segura y productiva desde cualquier lugar y, lo que es más importante, acelerar la empresa para que alcance sus objetivos.



63 %

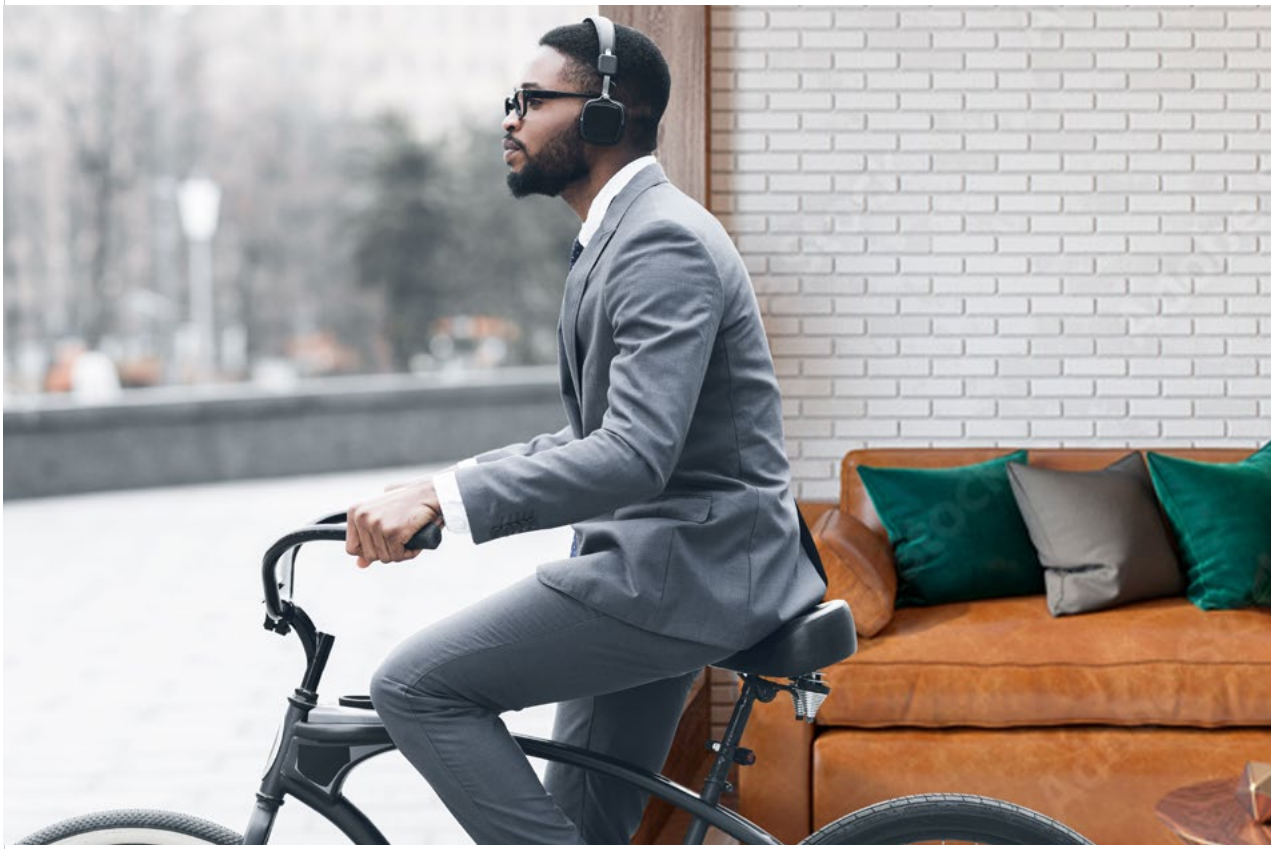
de aumento en la innovación mediante el acceso al teletrabajo

Contenido

2

Lecciones del pasado, nuevas oportunidades

Lo que los cambios tecnológicos históricos nos pueden decir sobre el futuro y cómo sacar el máximo provecho a la empresa



Contenido

Vamos a abordar un tema difícil y a veces controvertido. Para muchos líderes empresariales, puede parecer contraintuitivo que las necesidades tecnológicas de teletrabajo de los empleados puedan dictar la forma en que una organización debe operar e innovar. No obstante, el cambio en el lugar de trabajo se va a producir igualmente.

En la presentación del informe de tendencias de selección globales de 2022 de LinkedIn, Jennifer Shappley, directora global de adquisición de talentos, dijo lo siguiente: "El contrato entre empleados y empleadores se está reescribiendo. Lo que los empleados solían aceptar ya no les resulta aceptable. Cuando no sienten el cuidado y el cariño de sus empleadores, se van". [4]

Adaptarse a los cambios

En medio de este clima, los ejecutivos tienen que tomar una decisión fundamental: mantener la estrategia actual o adaptarse con las fuerzas del cambio en el lugar de trabajo. En la batalla por obtener talentos cualificados, las organizaciones en rápido cambio están optando por adaptarse. El portal de búsqueda de empleo Ladders predice que el 25 % de los puestos de trabajo bien remunerados estará disponible de manera remota para finales de 2022.[5]

Para aquellos que todavía dudan sobre si apoyar las capacidades del teletrabajo a largo plazo, en especial porque fusionan la línea entre la vida personal/de consumidor y la vida laboral/de empleado, puede resultar útil tener en cuenta otros momentos en el pasado reciente en los que las tecnologías personales y laborales han convergido y, en el proceso, han generado grandes oportunidades de negocio...

1. La consumerización de la TI: en 2005, Gartner describió la migración al lugar de trabajo del software y del hardware diseñados para uso personal como "la tendencia más significativa que afectará a la TI en los próximos 10 años". Hoy en día, es difícil imaginar un negocio que funcione sin tecnologías móviles, banda ancha accesible y la capacidad de utilizar dispositivos personales en un contexto laboral.

2. El Internet of Things (IoT): la creación de una red de objetos físicos, dotados de software y sensores, y con capacidad para intercambiar datos con otros dispositivos y sistemas, ha creado un nuevo mundo de posibilidades para los consumidores, como la gestión de la energía en el hogar. Al mismo tiempo, ha presentado grandes oportunidades para las empresas, como el mantenimiento predictivo para impulsar la eficiencia en las fábricas.

3. Aplicaciones móviles y servicios de cloud: la primera aplicación para muchos fue el juego "Snake" en el Nokia 6110. Sin embargo, las aplicaciones se generalizaron con el lanzamiento de la App Store de Apple en julio del 2008. En la actualidad, las aplicaciones móviles y los servicios de cloud que las respaldan son el alma de la productividad cotidiana de los trabajadores de las organizaciones de todo el mundo.

4. Ludificación: la "ludificación", acuñada por primera vez por el programador informático británico Nick Pelling en 2002, se refiere a la utilización de las mecánicas de los juegos para aumentar el compromiso, la felicidad y la fidelidad de un público. Hoy en día, es una parte esencial del compromiso empresarial con empleados y clientes, desde la formación hasta el marketing.

5. Inteligencia artificial y aprendizaje automático: la IA y el ML, que ahora están detrás de muchas de las interacciones que tenemos en línea y a través de aplicaciones móviles, tienen una capacidad casi ilimitada para entretener e involucrar, a la vez que transforman casi todos los sectores y funciones organizativas, lo que hace que la vida sea más fácil, más eficiente y potencialmente más significativa, tanto dentro como fuera del lugar de trabajo.

6. 5G: cuanto más integrados están los dispositivos móviles en nuestras vidas, más evolucionan las redes inalámbricas en cuanto a cobertura y velocidad, lo que ha generado nuevas oportunidades para las empresas. Con la implementación del 5G, la conexión a Internet rápida y permanente está proporcionando la infraestructura para las tecnologías en las que las empresas confían y las que aún están por crearse.

Por lo tanto, de la misma forma que la fusión entre la tecnología empresarial y la de uso personal generó en el pasado nuevas oportunidades para las empresas, las preferencias de trabajo y las necesidades digitales cambiantes de los empleados pueden crear nuevas posibilidades para las empresas de hoy en día, lo que les permitirá beneficiarse de un nuevo valor, seguir siendo competitivos y superar las interrupciones.

Superar los retos

Sin embargo, para aprovechar al máximo estas oportunidades, las organizaciones deben superar retos clave y, entre ellos, el principal es hacer frente a nuevos riesgos de ciberseguridad. Dado que las plantillas, las aplicaciones y los datos se distribuyen cada vez más entre ubicaciones centrales y remotas, y que los empleados utilizan tanto dispositivos de trabajo como sus propios dispositivos personales, las amenazas de seguridad de los datos están en aumento.

Como resultado, a los equipos de TI les cuesta cada vez más mantener un control seguro de sus entornos y el funcionamiento óptimo para satisfacer las necesidades empresariales. En una encuesta reciente entre los responsables de la toma de decisiones de TI de Vanson Bourne, el 50 % expresó su preocupación por mantener la seguridad de su organización frente a las crecientes amenazas de ciberseguridad, mientras que al 49 % le preocupa su capacidad para proporcionar asistencia de TI proactiva y remota a una plantilla cada vez más distribuida.[6]

Por lo tanto, está claro que las organizaciones que obtengan la mayor ventaja competitiva de esta nueva realidad laboral serán las que construyan una ciberresiliencia preparada para el futuro, proporcionen una experiencia de empleados optimizada, moderna y segura para respaldar la productividad y aborden las consideraciones culturales que garantizan que todo el mundo vea la seguridad como parte de su papel: hoy y en el futuro.

El 25 %

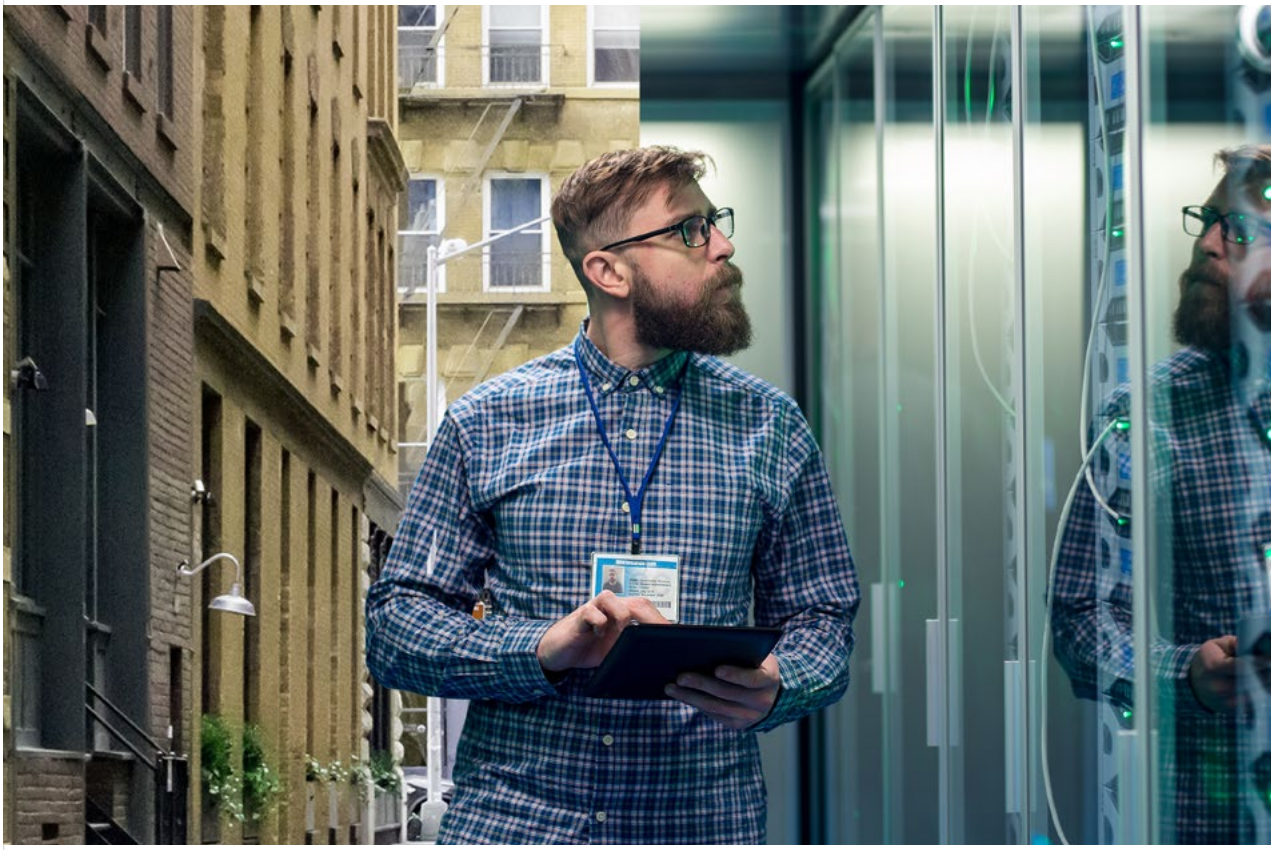
de los trabajos bien remunerados estarán disponibles de forma remota para finales de 2022

Contenido

3

Adéntrese en el futuro de forma segura

Las investigaciones demuestran que, para maximizar las oportunidades empresariales del trabajo híbrido, es necesario centrarse en la ciberresiliencia



Contenido

En el trabajo, todo el mundo necesita la ayuda de su equipo de TI de vez en cuando, pero ¿adónde recurre el equipo de TI para obtener ayuda? A medida que se esfuerzan por ofrecer experiencias digitales mejoradas dondequiera que estén trabajando los empleados, las funciones de TI son muy conscientes de que necesitan asistencia.

En el estudio de Vanson Bourne, cuando se preguntó a los líderes de TI en qué área necesitaban asistencia para poder realizar la transición a un entorno de trabajo híbrido, la respuesta principal fue en "mantener la seguridad de los teletrabajadores" (48 %), por delante de factores como "mejorar la productividad" (45 %) y "mejorar la eficiencia" (40 %). Solo el 5 % de los líderes dijeron que no necesitaban ayuda en absoluto.[7]

No es de extrañar que las necesidades cambiantes de las plantillas cada vez más distribuidas sean un quebradero de cabeza para la seguridad de los líderes de TI de las organizaciones de todo el mundo. Debido al cambiante entorno de trabajo, la seguridad de los puntos finales se ha vuelto cada vez más compleja, con un perímetro de riesgo ampliado, aplicaciones y datos que se suministran desde una multitud de centros de datos tradicionales y en la cloud, y un rápido incremento en los dispositivos perimetrales que necesitan protección frente a la proliferación de ciberamenazas.

Ver la seguridad de forma diferente

Como ya hemos visto en los titulares de todo el mundo en los últimos años, las tácticas de ciberataques, como el ransomware, se abren paso una y otra vez en todos los sectores y tienen graves repercusiones tanto en las hojas de balance como en la reputación de las empresas.

De hecho, en el informe Global Security Insights 2021 de VMware, el 78 % de los profesionales de la seguridad encuestados confirmó que los ataques habían aumentado como resultado del teletrabajo. El 61 % reconoció la necesidad de ver la seguridad de manera diferente debido a la expansión de la superficie de amenazas.[8] Según el informe State of Ransomware 2022, estos ataques afectaron al 66 % de las organizaciones en 2021, frente al 37 % en 2020.[9]

Por lo tanto, hoy en día es fundamental mejorar la ciberresiliencia en todo el panorama del trabajo híbrido. El último estudio de ESG de 2022 muestra una correlación directa entre la inversión en ciberresiliencia, el desarrollo de una mayor rentabilidad y un entorno mejor y más positivo en relación con la productividad y la innovación.[10] En el estudio, se encuestó a los responsables de la toma de decisiones de TI y se les segmentó por la madurez de la ciberresiliencia de sus organizaciones. Se les hizo cuatro preguntas clave:

- **¿Cómo describiría el nivel de dotación de personal en su equipo de ciberseguridad?**
- **¿Cómo describiría el nivel de habilidades de su equipo de ciberseguridad?**
- **¿Cómo definiría la inversión de su organización en productos y servicios para proteger sus sistemas, aplicaciones y datos?**
- **¿Su organización audita o inspecciona la seguridad de sus socios/proveedores de TI?**

Solo el 5 %

de los líderes de TI afirman que no necesitan ayuda para realizar la transición a un entorno de trabajo híbrido

ESG clasificó solo al 10 % principal como organizaciones "preparadas" con el mayor nivel de madurez de ciberresiliencia. Estas empresas se definen por tener "un nivel óptimo de personal, de inversión en tecnología de seguridad e inspecciones exhaustivas de los riesgos de terceros". El siguiente 26 % se clasificó como "vulnerables" y el 64 % restante como "expuestas".

Se identificaron varias diferencias clave entre las organizaciones preparadas y aquellas con niveles más bajos de madurez de ciberresiliencia, específicas del valor comercial que surge de la utilización que hacen de la seguridad de los dispositivos de usuarios finales en toda la plantilla híbrida.

Por ejemplo, las organizaciones preparadas tienen 2,5 veces más probabilidades de ofrecer un tiempo de actividad del 99,99 % o superior para sus aplicaciones críticas para la empresa, lo que equivale a un ahorro estimado de 33,3 millones de dólares en tiempo de inactividad. También son mucho más ágiles en lo que respecta a detectar y responder a los incidentes, con una media de tiempo de detección un 20 % más rápida y una de recuperación un 35 % más rápida. Estas empresas han podido reducir de media la cantidad de dispositivos desprotegidos en un 33 %.[11]

Rendimiento de la inversión

A medida que las organizaciones buscan un nuevo futuro de trabajo híbrido, seguirle el ritmo al 10 % de las empresas más preparadas requerirá, sin duda, una inversión en habilidades, tecnologías de resiliencia y realizar inspecciones exhaustivas de los riesgos de terceros. Sin embargo, las investigaciones muestran claramente que este componente de coste conlleva un importante retorno de la inversión.

Ahora que pasamos a analizar los beneficios que la resiliencia puede aportar al compromiso y la productividad de los empleados, ese retorno podría llevar a una organización a áreas de oportunidad mucho más allá de a las que actualmente pueden acceder sus rivales menos maduras y más vulnerables.

33,3 millones de dólares de ahorro

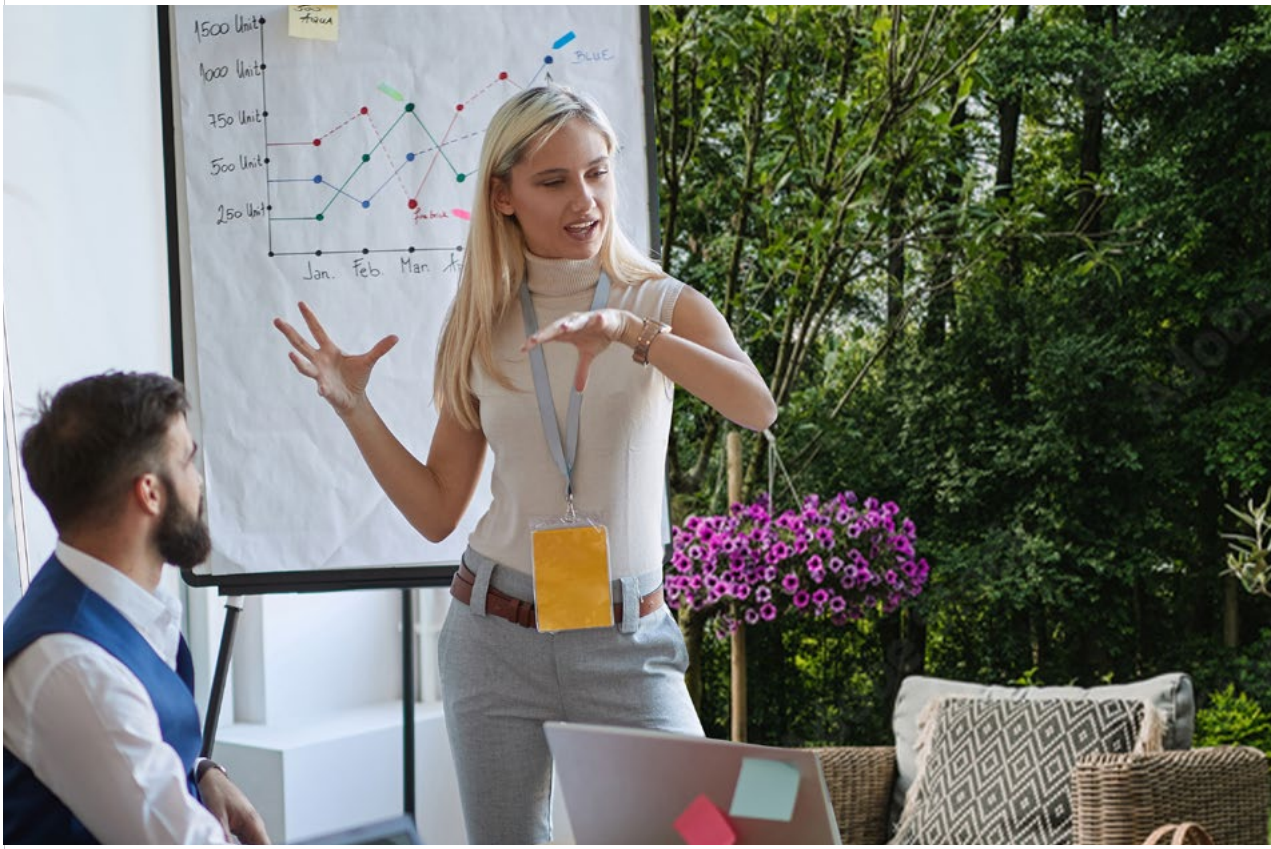
las organizaciones preparadas tienen 2,5 veces más probabilidades de ofrecer un tiempo de actividad del 99,99 % o superior, lo que equivale a un ahorro estimado de 33,3 millones de dólares en tiempo de inactividad.

Contenido

4

Potencie la productividad de los empleados

Las empresas que proporcionan experiencias digitales seguras y sin impedimentos para los empleados de cualquier parte demuestran ser más productivas que aquellas que no lo hacen



Contenido

Vayamos al grano: si mantener y optimizar las prácticas de trabajo híbrido no creara un beneficio empresarial, la mayoría de las organizaciones probablemente no perseguirían esta transformación en un mundo sin interrupciones.

Sin embargo, en una encuesta global realizada por PwC a ejecutivos y líderes centrados en los recursos humanos y publicada a finales de 2021, el 57 % afirmó que el teletrabajo y el trabajo híbrido habían hecho que su organización obtuviera mejores resultados en relación con los objetivos de productividad y rendimiento de la plantilla durante los últimos 12 meses, frente al 4 % que afirmó que su empresa había obtenido resultados significativamente peores en ese tiempo.[12]

Ventajas comerciales

La productividad del negocio y, por lo tanto, los beneficios y el crecimiento son un factor clave para avanzar en el trabajo híbrido. Por lo tanto, es una evolución natural que permitir que las personas trabajen de forma segura y conforme a las normas, donde y como prefieran y en los dispositivos que elijan sea un gran objetivo de las organizaciones que están adoptando el futuro del trabajo híbrido.

Porque si los trabajadores tienen la libertad de trabajar con confianza donde y como quieran sin impedimentos, pueden seguir centrados en los objetivos principales de la organización y, al mismo tiempo, fortalecer su compromiso con la empresa.

Por ejemplo, la investigación de ESG de 2022 sobre la ciberresiliencia y el rendimiento de los usuarios finales muestra que los empleados de las organizaciones "preparadas" ofrecen a sus equipos de TI una puntuación de satisfacción cinco veces mayor que los de las organizaciones "expuestas".[13]

Lo más importante para los líderes empresariales es que esto se traduce en una ventaja comercial: esas mismas organizaciones tienen 7,7 veces más probabilidades que las organizaciones expuestas de comercializar nuevas ofertas antes que la competencia, y ahora prevén que sus ingresos crecerán el doble que sus homólogos.[14]

Esta información se basa en una investigación realizada por ESG a mediados de 2021, en la que se exploró si la adopción de la tecnología de dispositivos modernos está correlacionada con el éxito y la resiliencia de las empresas en general. El estudio determinó que, de media, las organizaciones que pueden clasificarse como "aceleradoras del lugar de trabajo digital" experimentan un 18 % menos de eventos graves relacionados con la puesta en peligro de los dispositivos.

Las mismas organizaciones proactivas también tienen 2,1 veces más probabilidades de superar los objetivos de satisfacción del cliente que sus homólogas más reactivas. De media, el 40 % de sus ingresos anuales proceden de ofertas innovadoras y recién desarrolladas.[15]

Contenido

Lugares públicos, datos privados

Pero, si bien la creación de entornos digitales seguros y sin impedimentos para los teletrabajadores y trabajadores híbridos tiene claras ventajas comerciales, ¿qué ocurre con las ocasiones en que esos trabajadores no pueden encontrar un espacio completamente privado en el que trabajar?

A muchos empleados les preocupa y, por lo tanto, en ocasiones les distrae, trabajar con información confidencial que otros puedan ver en espacios públicos. Esta es una preocupación muy válida, dado que, en un estudio de 2022, el 62 % de los trabajadores en el Reino Unido admitió haber mirado las pantallas de los teléfonos inteligentes de los pasajeros mientras se desplazaban.[16]

Cuando trabajar en un espacio completamente privado no es una opción, las organizaciones deben seguir garantizando que sus empleados puedan sentir confianza y ser productivos de forma segura y sin complicaciones a través de dispositivos diseñados para ofrecer privacidad inteligente.

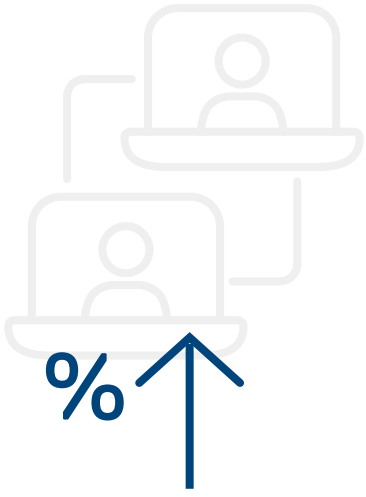
Por lo tanto, los líderes actuales de TI deben exigir dispositivos modernos a sus socios tecnológicos de confianza que ofrezcan una experiencia productiva intuitiva a los empleados, a la vez que ayudan a proteger los activos digitales y a mantener la privacidad de los datos confidenciales en todo momento.

Tecnologías avanzadas de privacidad

Por ejemplo, esto implica confiar en una suite completa de funciones de privacidad inteligentes, como la "detección de fisgones", que puede notificar a un usuario cuando hay un fisgón cerca y atenuar al instante la pantalla o activar un modo de pantalla segura.

Los PC más avanzados de hoy en día también pueden oscurecer la pantalla en el momento en que el usuario mira hacia otro lado, para dar al empleado la confianza continua de que sus datos seguirán protegidos si, de repente, necesita desviar su atención a otro lugar.

La productividad y los beneficios de permitir un trabajo híbrido y teletrabajo seguros y óptimos están hoy en día bien documentados y cada vez hay más pruebas. Con la estrategia y los dispositivos digitales adecuados, las organizaciones de todos los sectores pueden ofrecer experiencias de trabajo seguras y fluidas para los empleados que comenzarán a aumentar su ventaja en esta área a partir de hoy. Pero, como vamos a comentar a continuación, para que los beneficios sean duraderos, hay que tener en cuenta un elemento cultural clave...



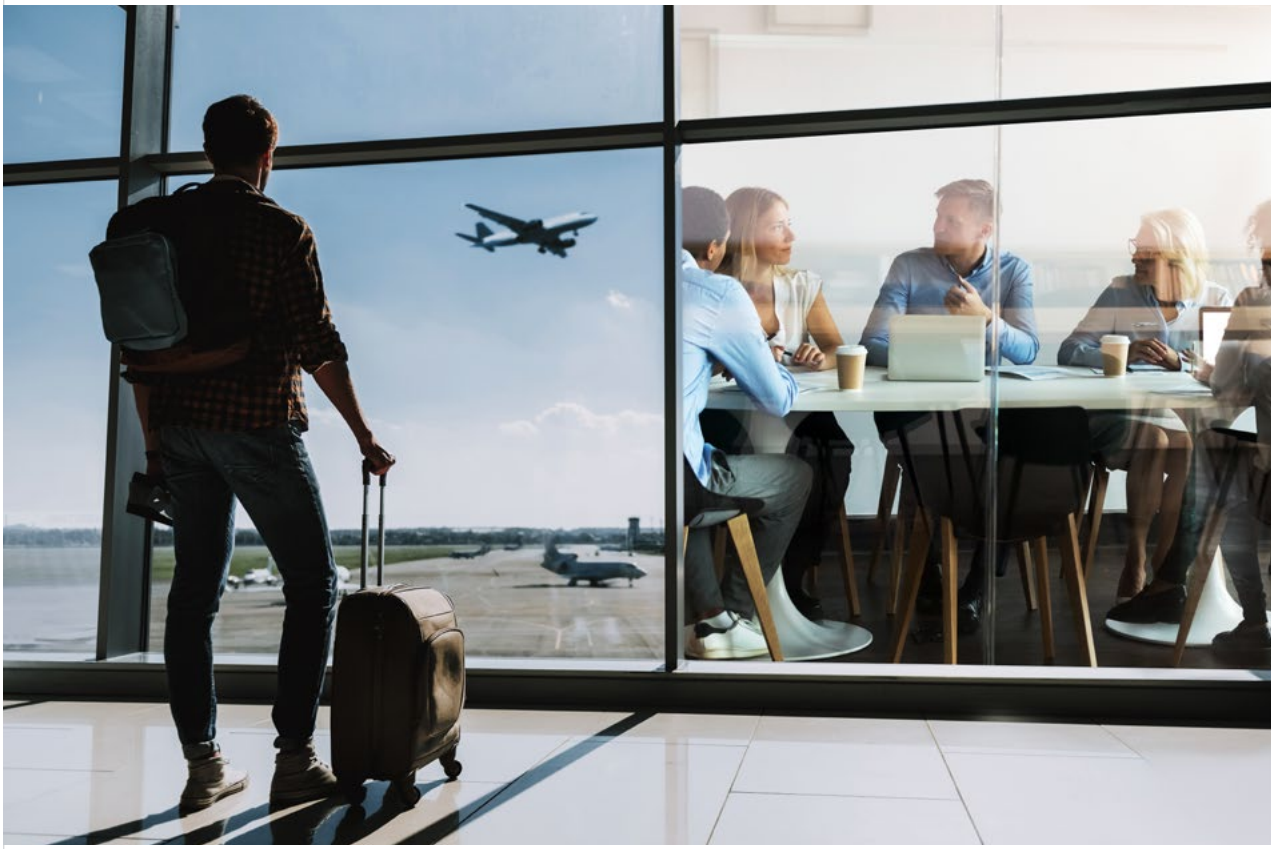
40 %↑

más de ingresos derivados de ofertas innovadoras y desarrolladas recientemente en organizaciones consideradas "aceleradoras del lugar de trabajo digital"

5

Por qué la seguridad es asunto de todos

Si las empresas quieren obtener beneficios duraderos del trabajo híbrido, la seguridad no puede dejarse en manos del equipo de TI



Contenido

Al igual que los tres cerditos de la clásica fábula para niños, los teletrabajadores y los trabajadores híbridos deben enfrentarse a tanto intentos coercitivos ("déjame entrar") como intentos a la fuerza ("soplaré y tu casa derribaré") de vulnerar su seguridad. Lamentablemente, los cibercriminales actuales tienen formas mucho más sutiles y sofisticadas de acceder que las que utiliza un lobo gruñón ficticio.

Como ejemplo, tenemos el reciente ataque de phishing "browser-in-the-browser" o "BitB", que falsifica de forma convincente las ventanas de inicio de sesión seguro (SSO) para robar las credenciales de inicio de sesión, como las de cuentas de Google y Microsoft. Es el último ejemplo del mundo de la "ingeniería social" maliciosa, en constante evolución, y que John Scimone, presidente y director del departamento de seguridad en Dell Technologies, resumió con precisión en un podcast reciente de MIT Technology Review:

"La ingeniería social, en particular, sigue siendo una preocupación principal", dijo. "Para aquellos que desconocen la ingeniería social, es esencialmente cuando los criminales tratan de engañar a los empleados para que entreguen información o abran la puerta para que los criminales entren en su sistema, como por ejemplo, a través de correos electrónicos de phishing, que seguimos viendo como uno de los métodos más populares utilizados por los piratas informáticos para acceder a las puertas de las redes corporativas".

El deber de todos

Por este motivo, para cosechar continuamente los beneficios del trabajo híbrido a largo plazo, las organizaciones deben hacer que la defensa de la seguridad sea un deber continuo de todos los trabajadores de la empresa, en lugar de ser simplemente el papel de la función de TI. Scimone explica cómo Dell Technologies ha establecido esta filosofía dentro de su propio negocio: "Llevamos muchos años construyendo una cultura de seguridad en la que dotamos a nuestros empleados de los conocimientos y la formación adecuados para que puedan tomar las decisiones correctas".

"Un programa de formación concreto que ha tenido mucho éxito ha sido nuestro programa de formación sobre phishing. En este programa, estamos probando y capacitando continuamente a nuestros empleados enviándoles correos electrónicos de phishing simulados, para que se familiaricen con lo que deben buscar. Incluso solo en el último trimestre, hemos visto a más empleados detectar y reportar pruebas de simulación de phishing que nunca. Estas actividades de formación están funcionando y están marcando la diferencia".[17]

Es obvio que era mucho más fácil recordar a los empleados sus responsabilidades en materia de seguridad cuando se encontraban predominantemente en el lugar del trabajo, por lo que, como añade Scimone, es fundamental aumentar la concienciación con consejos específicos relacionados con las situaciones de teletrabajo: "... estamos incrementando nuestros esfuerzos y promoviendo la concienciación sobre la seguridad y las responsabilidades que tienen los miembros del equipo, ya sea cómo usar la VPN de forma segura o proteger su red doméstica o incluso cómo viajar de manera segura", afirma.

Contenido

Respaldar la educación con tecnología

Por supuesto, a la vez que proporcionan una formación continua, las organizaciones deben garantizar que los empleados estén siempre respaldados con soluciones y dispositivos preparados para el futuro que les protejan contra las amenazas en constante evolución propias del trabajo híbrido. Al plantearse cómo proteger los datos y los dispositivos distribuidos a largo plazo, es importante adoptar una visión holística.

Entre las consideraciones clave para la protección por encima del sistema operativo se incluyen: ¿Cómo ciframos la información confidencial y protegemos nuestros datos? ¿Cómo evitamos, detectamos y solucionamos los ataques? ¿Nuestros usuarios finales pueden acceder a las aplicaciones y los dispositivos de forma segura en cualquier lugar? Por otro lado, entre las consideraciones clave para la protección por debajo del sistema operativo se incluyen: ¿Estamos protegiendo las credenciales del usuario final? ¿Nuestro BIOS está protegido? ¿Protegemos también la privacidad digital?

En respuesta, las organizaciones deben asegurarse de equipar a su personal con dispositivos de confianza que creen una base segura: con capas de protección resilientes por encima y por debajo del sistema operativo que refuercen la superficie de ataque de puntos finales y protejan, detecten y respondan a las amenazas en evolución.

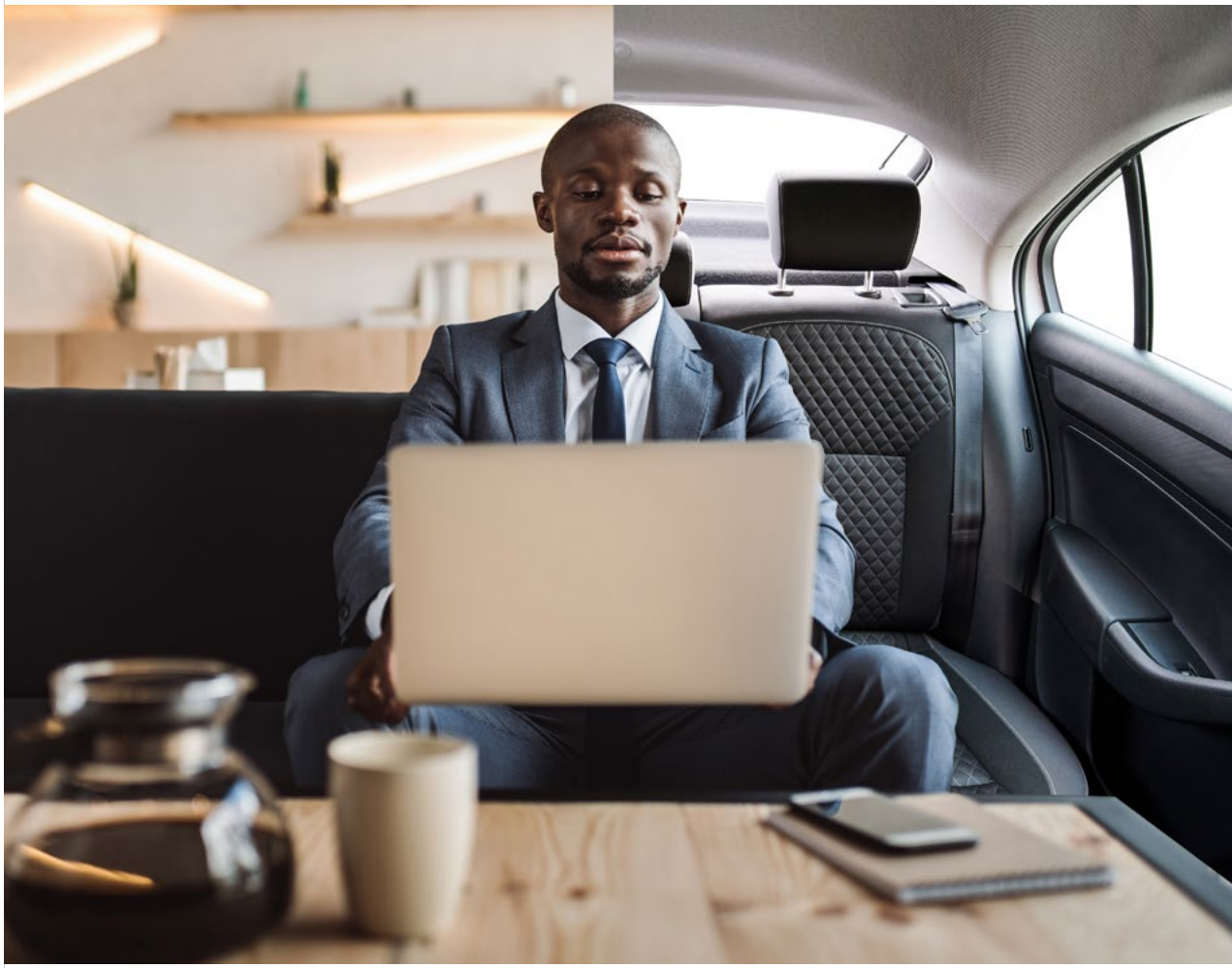
En un mundo en el que las normativas sobre cumplimiento de datos son cada vez mayores en todos los sectores y zonas geográficas, este enfoque holístico de la seguridad del trabajo híbrido es muy importante. Por ejemplo, en un estudio de ESG de 2022 se determinó que las organizaciones preparadas tienen un 44 % más de probabilidades de no informar de ninguna pérdida de datos debida a dispositivos en peligro en los últimos 12 meses, lo que supone claras ventajas financieras y de cumplimiento de las normativas.[18]

Solo mediante la educación, respaldada por la acción, las organizaciones pueden adentrarse en el futuro del trabajo híbrido con confianza y obtener una clara ventaja competitiva sobre los rivales que todavía tienen que hacer lo mismo.

> "Estamos probando y capacitando continuamente a nuestros empleados enviándoles correos electrónicos de phishing simulados, para que se familiaricen con lo que deben buscar".
>
> **John Scimone**, presidente y director del departamento de seguridad en Dell Technologies

Contenido

6 Asesoramiento y asistencia



Contenido

El trabajo ya no está vinculado a una ubicación. Las experiencias de trabajo híbrido seguras y sin complicaciones son un requisito previo para la productividad de los empleados y el crecimiento óptimo de la empresa. Con nuestras soluciones innovadoras, nuestra amplia experiencia y nuestra escala global, Dell Technologies e Intel son los socios digitales de confianza perfectos para ayudar a las organizaciones a sacar el máximo partido a este cambio fundamental en el lugar de trabajo.

Preparación para el futuro

Nuestra infraestructura digital segura preparada para el futuro, nuestros dispositivos modernos y nuestra experiencia de apoyo mantienen la privacidad de los datos confidenciales y, al mismo tiempo, ofrecen la experiencia del usuario moderna esencial para la innovación y la colaboración.

Por ejemplo, los dispositivos modernos de Dell Technologies, con tecnología Intel, ayudan a proteger los activos digitales y a mantener la privacidad de los datos confidenciales con la suite de funciones de privacidad inteligente más completa del mundo. Las capas resilientes de protección, por encima y por debajo del sistema operativo, refuerzan la superficie de ataque de puntos finales y le ayudan a garantizar que puede protegerse, detectar y responder a ciberamenazas en rápida evolución.

Por ejemplo, Intel Hardware Shield se incluye en todos los dispositivos comerciales de Dell que se ejecutan en la plataforma Intel vPro® y ofrece funciones de seguridad mejoradas por hardware que ayudan a proteger todas las capas de la pila de computación desde el primer momento.

Los empleados de todo el mundo están transformando el futuro del trabajo y, junto con Dell Technologies e Intel, usted puede asegurarse de que esta nueva era del trabajo híbrido sea también una de las nuevas y emocionantes oportunidades de crecimiento para su empresa.

Referencias

1 https://www.statista.com/statistics/1111394/attitudes-on-remote-work-for-employees/#:~:text=In%20general%2C%20employees%20consider%20remote,company%20for%20a%20remote%20role.

2 https://blogs.lse.ac.uk/businessreview/2021/09/29/remote-work-can-boost-productivity-and-curb-burnout/#:~:text=Overall%2C%20compared%20to%20those%20without,likely%20to%20report%20feeling%20included.

3 https://www.1e.com/resources/report/gartner-innovation-insight-for-the-digital-employee-experience-dex/thank-you/?submissionGuid=ZwbrOlKg21dUNdg2ONjZ

4 https://www.cnbc.com/2022/02/04/companies-are-reinventing-rules-as-employees-seek-remote-work-and-flexible-hours.html

5 https://www.cnbc.com/2022/02/04/companies-are-reinventing-rules-as-employees-seek-remote-work-and-flexible-hours.html

6 https://www.delltechnologies.com/asset/en-us/solutions/business-solutions/briefs-summaries/vb-hybrid-work-productivity-and-collaboration-research.pdf

7 https://www.delltechnologies.com/asset/en-us/solutions/business-solutions/briefs-summaries/dell-empowering-the-future-of-work.pdf

8 https://www.vmware.com/resources/security/global-security-insights-report-2021-index.html

9 https://news.sophos.com/en-us/2022/04/27/the-state-of-ransomware-2022/

10 eBook de ESG por encargo de Dell Technologies, "Cómo crear un negocio ciberresiliente preparado para innovar y prosperar", marzo de 2022

11 Resumen de estudio de ESG por encargo de Dell Technologies, "Ciberresiliencia y rendimiento para el usuario final", marzo de 2022

12 https://www.pwc.com/gx/en/news-room/press-releases/2021/pwc-future-of-work-survey-2021.html

13 Resumen de estudio de ESG por encargo de Dell Technologies, "Ciberresiliencia y rendimiento para el usuario final", marzo de 2022

14 eBook de ESG por encargo de Dell Technologies, "Cómo crear un negocio ciberresiliente preparado para innovar y prosperar", marzo de 2022

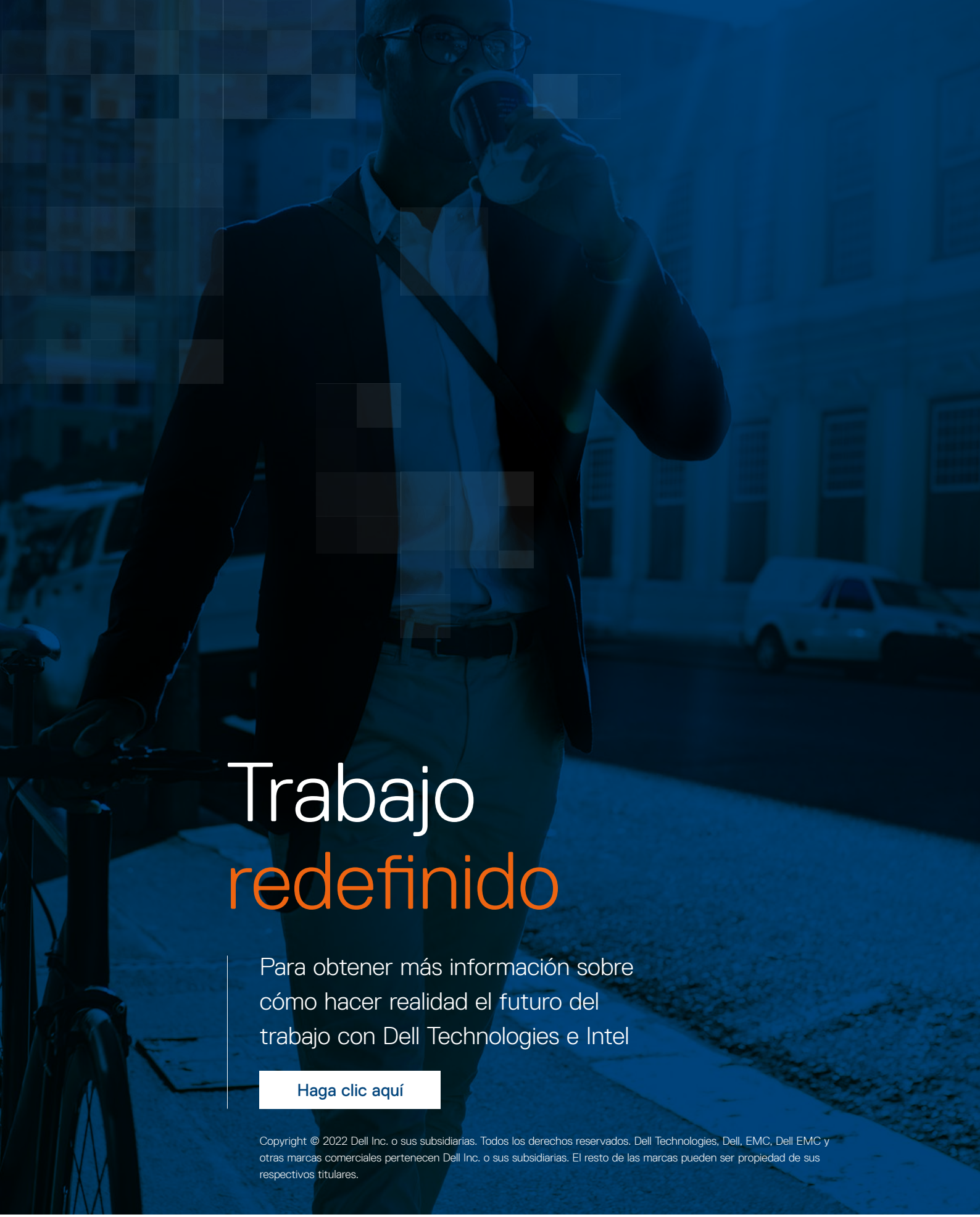
15 eBook de ESG por encargo de Dell Technologies, "Las organizaciones que aceleran su lugar de trabajo digital logran mejoras", abril de 2021

16 https://www.walesonline.co.uk/news/uk-news/brits-admit-spying-what-fellow-23734428

17 https://www.technologyreview.com/2021/11/22/1040358/security-is-everyones-job-in-the-workplace/

18 Resumen de estudio de ESG por encargo de Dell Technologies, "Ciberresiliencia y rendimiento para el usuario final", marzo de 2022

Contenido



Trabajo redefinido

Para obtener más información sobre cómo hacer realidad el futuro del trabajo con Dell Technologies e Intel

Haga clic aquí

DELL Technologies

Innovation Built-In intel