Los retos de la seguridad de los trabajadores móviles, y cómo resolverlos

#KingstonIsWithYou

Los retos de la seguridad de los trabajadores móviles, y cómo resolverlos

Prólogo

Es hora que sus trabajadores pasen del dicho al hecho en materia de protección de los datos. Ya se sabe que el trabajo a distancia es un factor favorable para la empresa. No obstante, los retos que supone para la seguridad de sus redes y para el cumplimiento del RGPD son demasiado grandes como para ignorarlos. Muchas empresas consideran que mantener un control demostrativo sobre el ecosistema informático es un obstáculo invencible sin una inversión significativa. Pero no tiene que ser así. Los costes no pueden ser una excusa.

Los sistemas, servicios y productos ya están ahí, y cuestan menos de lo que podría pensarse. De hecho, la realidad es que el reto para la seguridad no es solamente financiero o técnico, sino cultural. Es posible crear un entorno informático adecuado para el trabajo remoto con relativa facilidad. Pero a menos que su personal adopte las actitudes y comportamientos correctos de cara a la seguridad y al cumplimiento normativo de la protección de datos, su empresa está en riesgo. Y los potenciales costes de las vulneraciones son increíblemente altos.

Los productos ya están en el mercado.
Pero la educación lo es todo.

Índice

Este breve libro electrónico ha sido compilado por tres expertos en protección de datos y trabajo a distancia.

Rob Allen
@Rob_A_kingston

Rob es Director de Marketing y Servicios Técnicos de Kingston Technology, empresa a la que llegó en 1996. En su calidad de tal, Rob es responsable de supervisar las RR.PP., las redes sociales, el marketing de canal con soportes y creativos de marketing digital para todas las marcas y productos de Kingston.

Rafael Bloom
@rafibloom73

Rafael es Director de Salvatore Ltd. Su cometido es ayudar a las empresas a gestionar los retos y oportunidades estratégicas, comerciales y procedurales creados por los cambios tecnológicos y reglamentarios.

Sarah Janes
@SarahkJanes

Sarah es Directora Ejecutiva de Layer 8 Ltd. desde 2014. Su misión es empoderar a los directores de seguridad para promover un cambio cultural efectivo y sostenible en materia de seguridad entre todo tipo de organizaciones, desde pymes a grandes corporaciones.

Los retos de la seguridad de los trabajadores móviles, y cómo resolverlos

Índice

Sección 1 – El problema

El acceso remoto es crítico

Los días en que se trabajaba exclusivamente en una oficina central pertenecen ya a un lejano pasado. El personal accede al correo electrónico del trabajo desde sus teléfonos inteligentes personales. El Director de Operaciones pasa días enteros trabajando desde casa o desde su cafetería favorita. El equipo de ventas accede a datos comerciales críticos desde sitios de los clientes. El trabajo remoto es la nueva norma.

Impulsa la productividad y la retención de empleados.[1] Reduce los gastos generales de la empresa.[2] Es bueno para el medio ambiente.[3] Los estudios apuntan a que **el 70% de los profesionales teletrabaja al menos una vez por semana.**[4]

Sin embargo, una sola persona puede comprometer la integridad de la seguridad de toda la organización si no se atiene a los protocolos de seguridad necesarios.

El cumplimiento del RGPD es obligatorio

Una seguridad adecuada no es negociable, tanto para la integridad de su organización como para prevenir incumplimientos del RGPD. Y el RGPD es algo serio. Recientemente, la ICO, Oficina del Comisionado de Información (el organismo regulador de la protección de datos del Reino Unido) impuso multas a British Airways y a la cadena hotelera Marriott por un total de casi 300 millones de libras esterlinas por vulneraciones de datos.[5]

El 70% de los profesionales teletrabaja al menos una vez por semana.[4]

¿Qué tipo de empresas están en riesgo?

Si entre su personal hay empleados que trabajan a distancia, o que utilizan sus propios dispositivos para acceder a los sistemas empresariales, su empresa está en riesgo. Así de sencillo.

[1] **Inc.com: Un estudio realizado durante 2 años por Stanford refleja un asombroso incremento de la productividad por debido al trabajo desde casa -** www.inc.com/scott-mautz/a-2-year-stanford-study-shows-astonishing-productivity-boost-of-working-from-home.html

[2] **PGi: ¿Cuál es el ahorro de costes del teletrabajo? -** www.pgi.com/blog/2013/03/what-are-the-cost-savings-of-telecommuting/

[3] **FlexJobs: 5 estadísticas acerca del impacto ambiental del teletrabajo -** www.flexjobs.com/blog/post/telecommuting-sustainability-how-telecommuting-is-a-green-job/

[4] **CNBC: El 70% de la gente en todo el mundo trabaja a distancia al menos una vez a la semana, afirma un estudio -** www.cnbc.com/2018/05/30/70-percent-of-people-globally-work-remotely-at-least-once-a-week-iwg-study.html

[5] **The Guardian: Multas del RGPD: ¿dónde irán los 300 millones de libras esterlinas de BA y de Marriott? -** www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog

Sección 2 – Los retos del acceso remoto

El trabajo a distancia supone diversos retos para la seguridad.

Puede resultar difícil de conciliar, pero debe tomarse con la mayor seriedad en aras de la integridad de su organización.

Sarah Janes
@SarahkJanes

Director Ejecutivo
Layer 8 Ltd.

"Una de las principales preocupaciones por la nueva legislación del RGPD es que las empresas deben controlar los datos personales que obran en su poder. Esto no es posible si no se sabe dónde están guardados esos datos".

Las empresas se las ven y se las desean para mantener sus sistemas internos y sus dispositivos avanzando al ritmo general de desarrollo de la tecnología.

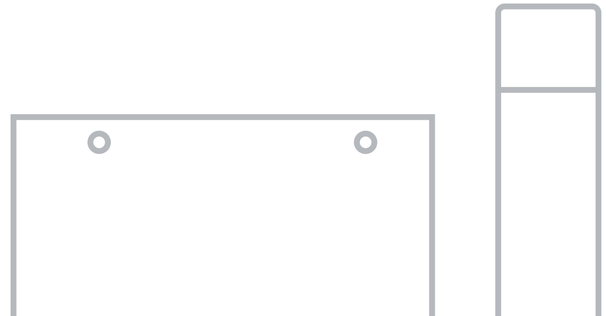
De hecho, el 38% de los teletrabajadores contratados por las pymes consideran que no cuentan con el apoyo o la especialización tecnológica que necesitan cuando trabajan desde casa o en un espacio público.

Esto puede llevarlos a buscar atajos que vulneren las iniciativas de protección de datos y dejen a su empresa expuesta a amenazas para la seguridad. A menos que los protocolos de seguridad estén diseñados para promover la eficiencia del personal, siempre encontrarán atajos, como guardar información sensible en sitios como Slack, Dropbox, sus buzones de correo personales o unidades USB privadas. O peor: promoverá una cultura de Ellos contra Nosotros entre departamento de protección informática y el resto de los trabajadores. Su empresa está en riesgo.

Rob Allen
@Rob_A_kingston

Director de Marketing y Servicios Técnicos, Kingston Technology

"Según mi experiencia, cuanto más grande una organización, más restrictivo y engorroso resulta para sus empleados trabajar a distancia: tiempos de inicio de sesión prolongados y demasiadas medidas de seguridad que atravesar".



Sección 2 – Los retos del acceso remoto

Traiga su propio dispositivo (BYOD)

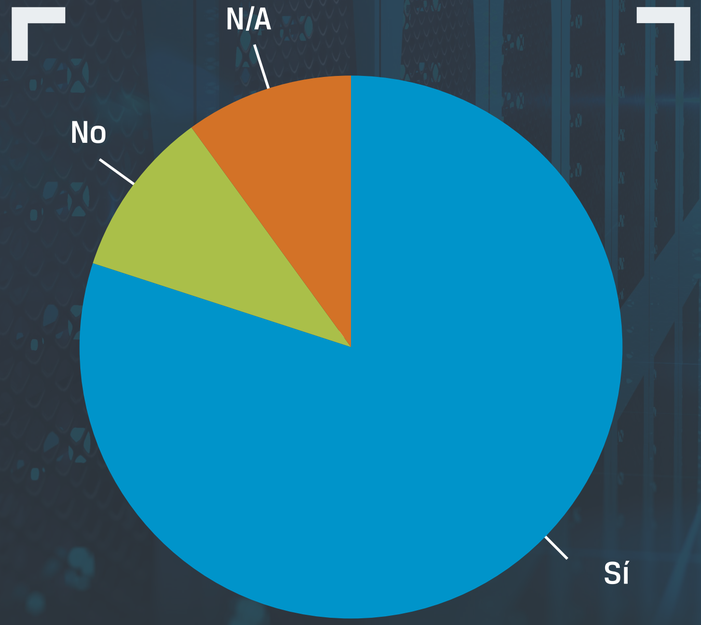
Para los profesionales modernos, es habitual utilizar sus teléfonos inteligentes para leer los mensajes de correo electrónico de trabajo; acceder a los datos de su organización desde sus portátiles y tabletas personales. Esto supone peligros. ¿Transfieren sus trabajadores datos fuera de la organización? ¿Está su hardware protegido contra ataques? ¿Es su software seguro? Estas son las preguntas que deben responderse.

Sarah Janes
@SarahkJanes

Director Ejecutivo
Layer 8 Ltd.

"Las empresas tienen un importante reto retrospectivo solamente para entender dónde guardan sus datos".

¿Le inquieta que sus empleados busquen atajos indebidos para sortear las medidas de seguridad?



Fuente: Encuesta de Kingston, 2019

Redes wifi públicas

El problema no se limita a trabajar desde casa. ¿Qué pasa con quienes prefieren la cafetería, iniciando sesión con un café con leche en la mano? Las redes wifi públicas son el paraíso del hacker. Por eso, es necesario dotar a los trabajadores con las herramientas necesarias para mitigar el riesgo.

Ciberataques y suplantación de identidad (phishing) sofisticada

Los correos electrónicos que suplantan identidades, dirigidos a empleados individuales, son cada vez más sofisticados y convincentes. ¿Está su personal capacitado para identificarlos? ¿Y qué hay de la continua amenaza del malware y el ransomware? Sus dispositivos —todos ellos— deben estar protegidos.

Sección 3 – La infraestructura del acceso remoto (y una nota sobre una mentalidad orientada a la seguridad)

Ya existe la tecnología que simplifica los retos de seguridad del trabajo a distancia. Y no tiene por qué costar una fortuna.

Creación de la infraestructura correcta

Los empleadores deben asegurarse de que sus trabajadores móviles puedan acceder de manera fácil y eficiente a las herramientas y los datos necesarios para realizar sus tareas cotidianas y ser productivos. No necesariamente se trata de agregar nuevos productos, sino más bien de elegir los más adecuados. Por ejemplo, la mayoría de las empresas necesitarán ordenadores de sobremesa o portátiles. Así, pues, seleccione discos duros o unidades de estado sólido cifrados. De esta manera, si se extravían o roban los datos de la empresa, están protegidos para no caer en malas manos. Además, si se produce una violación de datos, la ICO adoptará una actitud más favorable si ha adoptado medidas demostrables para proteger los datos.

Trabaje con los proveedores adecuados

En el segmento de seguridad informática encontrará innumerables fabricantes y proveedores. Estudie el terreno. Se trata de conseguir un sistema que proceda de un proveedor de soluciones de confianza, preferiblemente especializado en habilitar a los trabajadores móviles.

VPN

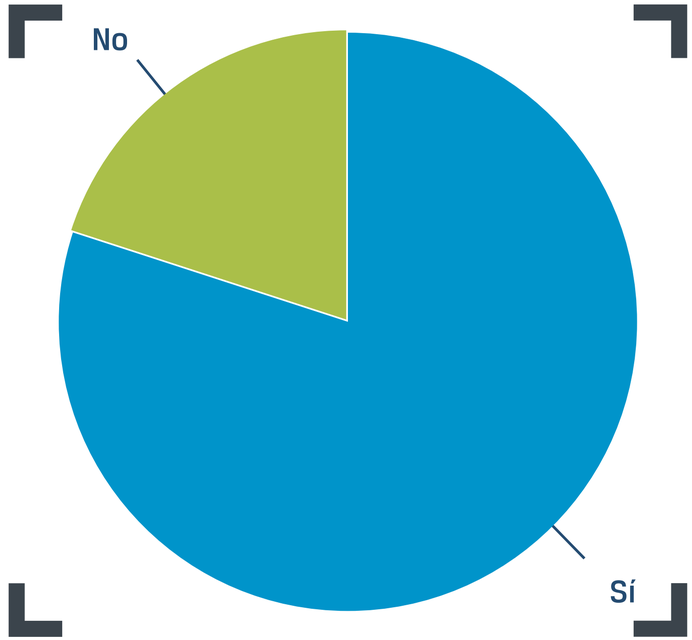
Si para proteger a su organización tiene que utilizar una red privada virtual (VPN), proporcionar a las personas adecuadas las herramientas correctas reducirá significativamente sus riesgos. Las VPN son especialmente idóneas para el personal que accede a los datos de la organización a través de redes wifi públicas.

Software DLP

Prácticamente todos los paquetes de software DLP ofrecen la posibilidad de restringir el acceso a la red y, al mismo tiempo, aprobar ciertos dispositivos, como unidades USB cifradas diseñadas para ser identificables. Se comercializan a un coste mínimo. (Eche un vistazo a la línea de unidades USB de Kingston, personalizables por su organización.)

¿Tiene o tuvo que realizar cambios significativos para asegurarse de que su empresa cumple los requisitos del RGPD?

Fuente: Encuesta de Kingston, 2019



Sección 3 – La infraestructura del acceso remoto (y una nota sobre una mentalidad orientada a la seguridad)

USB y SSD

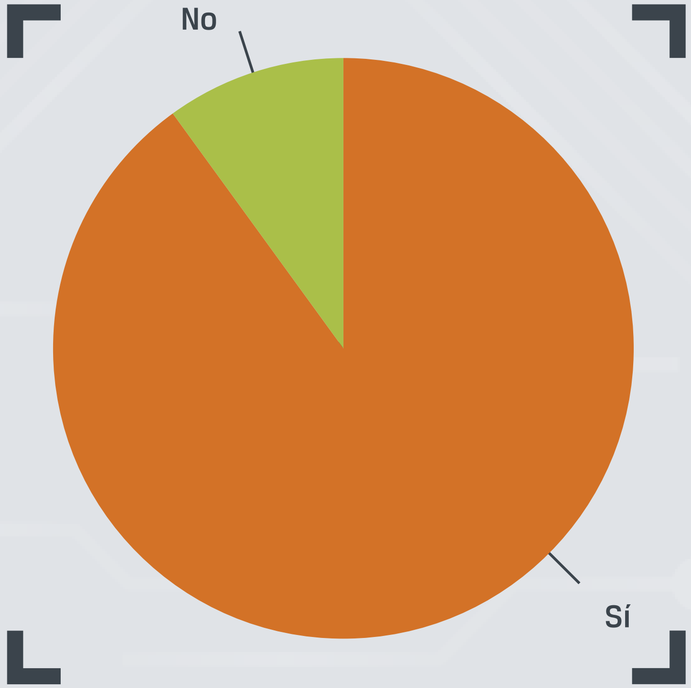
La implementación de unidades USB cifradas y equipar los portátiles con SSD de hardware cifrado constituyen grandes, enormes avances, en la resolución de los retos del trabajo remoto. Con una unidad USB cifrada y un disco SSD de hardware cifrado (wifi o no), sus datos estarán protegidos y disponibles en todo momento y en todo lugar. Y si un dispositivo se extravía, o lo roban, tendrá la tranquilidad de saber que nadie podrá acceder a los archivos cifrados. Incluso es posible destruir a la distancia las unidades USB extraviadas.

Piense siempre en lo peor

En ocasiones, una mentalidad optimista es el fino velo de una fe ciega. Como equipo de seguridad, lo mejor, y más necesario quizá, es pensar siempre en lo peor. Confíe en sus trabajadores, y más en sus medidas de seguridad. Pero siempre, siempre, póngase en el peor de los casos. Es mano de santo para la integridad de la seguridad de su red partir del supuesto de que puede, y será, vulnerada.

¿Complementa el software de protección de terminales con los dispositivos móviles de su lugar de trabajo? Por ejemplo, unidades USB, portátiles, etc.

Fuente: Encuesta de Kingston, 2019



Sección 4 – Educar al personal es el único camino

La tecnología adecuada es solamente la mitad de la batalla. El verdadero desafío es qué hace su personal cuando nadie mira. Ese es el motivo por el cual el reto de la seguridad es tanto una cuestión de cultura como un asunto de tecnología. Sin la educación adecuada, sus empleados siempre considerarán cosas como el RGPD, el RPCE y otros 'reglamentos' solo como una molestia.

A continuación unos consejos.

No existen normas sin motivos

"No vaya detrás de ese árbol"
"No vaya detrás de ese árbol porque hay un león"

¿Qué se recuerda mejor? Los humanos no responden bien a las normas si no se les explica un motivo. En primer lugar, ayuda a sus empleados a entender por qué existen las normas.

Conviértalo en algo personal

Del mismo modo, sus trabajadores entenderán mejor el desafío para la seguridad cuando les muestre que es relevante para sus vidas Tomemos, por ejemplo, el RGPD. Para ayudar a su equipo a entender que detrás de cada conjunto de datos hay una persona, plantéeles cómo se sentirían si una organización descuidase los datos personales suyos que tiene guardados. ¿Cómo se sentirían si sus datos cayesen en malas manos?

"Cuando le explicas a un empleado que la seguridad y el RGPD son importantes por sus propios intereses, fuera del trabajo, empiezan a entender por qué una organización está obligada a protegerlos".

Rafael Bloom
@rafibloom73
Director de Salvatore Ltd.

"En última instancia, el mejor método para concienciar en materia de seguridad es entablar conversaciones abiertas con los empleados para buscar estrategias que sean a la vez seguras y productivas".

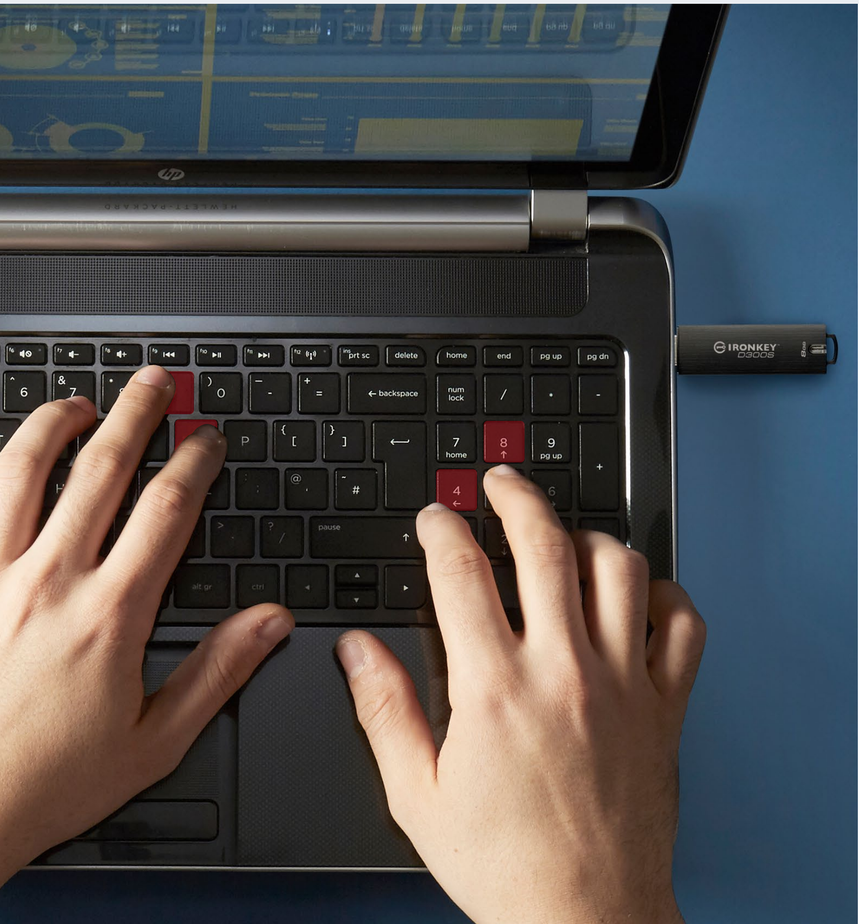
Sarah Janes
@SarahkJanes
Director Ejecutivo Layer 8 Ltd.

Fuente: Encuesta de Kingston, 2019

¿Audita periódicamente el uso de almacenamiento externo de sus empleados?

71%	11%	9%	9%
Sí	No	No lo sé con seguridad	N/A

Sección 4 – Educar al personal es el único camino



La educación es el principio, no el final

Dado que la mayoría de las organizaciones ofrecen capacitación en la falta de seguridad a nivel interno, las empresas se han planteado llenar el vacío. Pero hay que tener cuidado con los falsos profetas. Normalmente, la capacitación ofrecida por los consultores externos está sesgada a los requisitos de cumplimiento normativo de las empresas (porque es de ahí de donde obtienen fondos), lo que implica que sus empleados no comprenderán y apreciarán plenamente la importancia de la ciberseguridad. Así, los comportamientos de inseguridad persistirán.

Sarah Janes
@SarahkJanes

Director Ejecutivo
Layer 8 Ltd.

"Si las organizaciones de verdad quieren cambiar los comportamientos, deben ser lo bastante valientes como para abstenerse de ofrecer cursos de capacitación que más bien parecen 'listas de la compra'. Tienen que pensar en ofrecer una capacitación que transmita los fundamentos de la comprensión de la seguridad y el mundo cibernético en general".

Del mismo modo, la capacitación no puede ser un recurso para salir del paso. Es demasiado fácil pensar que porque los empleados han recibido capacitación adoptarán automáticamente conductas seguras y se esforzarán por cumplir la normativa. Se trata de una ingenuidad peligrosa. Para tener éxito se requieren estímulos conductuales y culturales continuos.

Rafael Bloom
@rafibloom73

Director de Salvatore Ltd.

"He conocido empresas 'certificadas' que guardan hojas de cálculos o portátiles llenos de contraseñas, o que dejan copias no cifradas de sus discos duros en los coches de los empleados durante la noche. ¿Qué sentido tiene esa certificación si su gente no entiende los principios basicos?".

Asigne responsabilidades desde los niveles más básicos

Una estrategia para impulsar el necesario cambio cultural dentro de su empresa es adoptar Expertos en Seguridad, capaces de exponer los retos de seguridad y explicar los protocolos de seguridad a los empleados a partir de las bases.

Sarah Janes
@SarahkJanes

Director Ejecutivo
Layer 8 Ltd.

"Teniendo expertos que explican a los empleados la importancia de la seguridad en sus lugares de trabajo, combinados con materiales de capacitación en línea para facilitar los cambios, son el mejor método para conseguir que se adopten comportamientos seguros".

Resumen

La protección de los datos y la seguridad pueden percibirse como una responsabilidad onerosa. Sin embargo, con las herramientas correctas el trabajo remoto será más fácil y seguro. Y no es muy caro de implementar. Pero tenga en cuenta que debe haber un cambio cultural en su organización, además de la infraestructura de seguridad correcta, si se pretende que los empleados adopten comportamientos seguros.

A continuación presentamos un breve resumen.

- El trabajo remoto ha llegado para quedarse y supone numerosas ventajas: productividad, fidelidad del personal y reducción de gastos generales. Sin embargo, también plantea diversos retos para la seguridad.
- Las vulneraciones de datos son un serio problema: la ICO ha impuesto grandes multas por desobedecer el RGPD.
- El uso de dispositivos propios y de hardware inseguro, así como el uso indebido del software y las redes wifi públicas son amenazas comunes para la seguridad.
- Una infraestructura de seguridad adecuada debe promover —no inhibir— la eficiencia de los trabajadores. De lo contrario, el personal buscará atajos.
- Evalúe los fabricantes y proveedores de informática y elija los de mejor reputación.
- Herramientas como los discos SSD y las unidades USB cifradas, las redes privadas virtuales (VPN) y el software DLP, resultan fáciles de implementar y no tienen por qué ser caros.
- Para la protección y seguridad satisfactoria de los datos se requiere un cambio cultural y conductual dentro de la organización. El personal debe entender por qué existen las normas, en lugar de enseñarles que deben seguir ciegamente los protocolos.
- Los consultores externos pueden ayudar a capacitar al personal, aunque debe asegurarse de que los materiales sean adecuados y tener en cuenta que los empleados no adoptarán automáticamente los comportamientos adecuados solamente porque se les ha dicho en un curso.
- Adopte los expertos de seguridad para que expongan los retos de la cuestión y promuevan las conductas adecuadas a nivel básico.

Acerca de Kingston

Con más de 32 años de experiencia, Kingston cuenta con los conocimientos necesarios para identificar y resolver sus retos del trabajo remoto, facilitando a sus empleados trabajar con seguridad desde cualquier lugar sin comprometer a su organización.

#KingstonIsWithYou