
Kingston
TECHNOLOGY
La protección de los datos y la ciberseguridad después del RGPD
#KingstonIsWithYou

La protección de los datos y la ciberseguridad después del RGPD

Prólogo

Innumerables empresas y organizaciones se esforzaron mucho, e hicieron importantes inversiones en recursos humanos, para prepararse de cara al RGPD. Posiblemente la suya fuese una de ellas. No obstante, debido a la naturaleza continuamente cambiante de las ciberamenazas, no es posible pararse a recuperar el aliento. Cumplir el RGPD no es un formalismo, sino un marco mediante el cual se evaluarán sus medidas permanentes de protección de los datos y de ciberseguridad. No hay espacio para la complacencia.

En este breve libro electrónico hemos reunido los conocimientos de algunos de los comentaristas británicos más experimentados en ciberseguridad para hablar sobre cómo ha evolucionado la protección de datos desde la implementación del RGPD. También veremos cómo las empresas capacitan a sus empleados en la necesidad de cumplimiento, y cómo los departamentos de TI y proveedores técnicos pueden proteger mejor las infraestructuras informáticas y explicar a los usuarios finales los nuevos retos en materia de seguridad.

La protección de los datos y la ciberseguridad después del RGPD

Colaboradores

Este breve libro electrónico ha sido compilado por cinco expertos en protección de datos y ciberseguridad.

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.

Tara Taubman-Bassirian
@clarinette02

Tara ostenta muchos títulos: abogada, procuradora, mediadora, investigadora, consultora, disertante y escritora. Con un altísimo grado de especialización en áreas como la privacidad, la propiedad intelectual y la protección de datos, se ha ganado una merecida reputación en diversas regiones del mundo, sobre todo en el Reino Unido, Francia y EE.UU.

Rafael Bloom
@rafibloom73

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

Miriam Brown
@Kingston_MBrown

Gerente de Marketing Estratégico B2B en Kingston Technology, ha estado en nuestra empresa desde 1997. En su cargo, Miriam es responsable de la estrategia, contenidos y campañas de marketing de todos los productos B2B de Kingston.

Sally Eaves
@sallyeaves

La Prof. Sally Eaves ha sido calificada como la 'abanderada de la tecnología ética'. Aporta su amplia experiencia como Consejera Delegada y Directora Tecnológica, profesora de Tecnologías emergentes y asesora estratégica global Sally es una galardonada disertante, autora, investigadora e influencer internacional conocida por su original liderazgo intelectual.

La protección de los datos y la ciberseguridad después del RGPD

Índice

Sección 1 – ¿Cómo ha cambiado la protección de datos desde el RGPD?

Las organizaciones han recorrido un largo camino. En los dos últimos años, los equipos jurídicos se han reforzado, la contratación de Delegados de protección de datos se ha disparado[1] y han crecido las consultas a asesores externos especializados en privacidad de datos. Hoy en día, miles de organizaciones ya están familiarizadas con la preparación de evaluaciones de impacto de protección de datos (EIPD).

Pero todavía queda un largo camino por recorrer.

Uno de los mayores retos que plantea el RGPD es que no es posible dormirse en los laureles. En la mayoría de las organizaciones, en cualquier momento, seguramente casi cualquier integrante del personal podría contravenir la normativa. El problema se magnifica en sectores en los que la fuerza de trabajo está tan distribuida o cuenta con un alto grado de autonomía, como la atención sanitaria, la educación y el derecho. Por ejemplo, en este último sector, los abogados consideran inocuo intercambiar detalles de casos sensibles mediante datos adjuntos a un correo electrónico. Los profesionales sanitarios compartirán datos de pacientes y los resultados de una resonancia magnética desde direcciones de correo electrónico no seguras. En las organizaciones sometidas a altos niveles de estrés basta con un poco de presión adicional para que se incumplan los protocolos de cumplimiento. Al parecer, la productividad está por encima de los protocolos.

Esto debe cambiar.

También tenemos este problema de concienciación en el segmento de las ONG. Con demasiada frecuencia, las ONG creen que están exentas de cumplir el RGPD. Incluso aquellas que entienden que el RGPD es de aplicación a toda entidad privada, pública y del tercer sector, son reacias —quizá comprensiblemente— a dedicar parte de los fondos dirigidos a promover sus causas e invertirlos en la protección de datos. Muy noble... pero también muy ingenuo. Las posibles multas por incumplir el RGPD empequeñecen el potencial gasto en TI.

Tara Taubman-Bassirian
@clarinette02

RGPD, protección de datos y consultores de TI

"Muchas organizaciones del tercer sector comentan: 'el RGPD no se aplica a nuestro caso: somos solo una ONG'. Incluso en lo que respecta al cumplimiento de sus sitios web trato de decirles que no solo se trata de los datos que desean recoger, sino de aquellos terceros a los que permiten acceder para conseguir los datos de sus visitantes".

Desde 2016 la demanda de Delegados de protección de datos (DPD) se ha disparado, incrementándose más de un 700%.

1. Varonis: A Year in the Life of the GDPR: Must-Know Stats and Takeaways (Un año en la vida del RGPD: Estadísticas de obligatorio conocimiento y aportaciones) www.varonis.com/blog/gdpr-effect-review/ [consultado el 26.11.19]

¿Cómo ha cambiado la protección de datos desde el RGPD?

La minimización de datos es una tendencia alentadora

Vivimos en una era de atroz recogida de datos. Las "Cuatro grandes" (Google, Apple, Facebook y Amazon) conservan enormes volúmenes de datos de clientes. La hipótesis sería que las demás organizaciones quieran imitar a las Cuatro Grandes y recopilar tantos datos como sea posible. Pero cuantos más datos se recogen, mayor es el riesgo de quedar expuesto. Una de las tendencias más positivas desde que se ha implementado el RGPD es una rebelión contra la excesiva recogida de datos. Las empresas pequeñas se atienen a la ética de la minimización de datos: si no los necesitas, no los recojas.

Tara Taubman-Bassirian
@clarinette02

RGPD, protección de datos y consultores de TI

"La minimización de datos es probablemente uno de los mejores principios del RGPD. La creación de cualquier base de datos supone una creación de riesgo".

Rob Allen
@Rob_A_kingston

Director de Marketing y Servicios Técnicos, Kingston Technology

"Tenemos reglas muy estrictas de supresión de datos. Obviamente, los datos críticos para la actividad deben estar almacenados correctamente. Pero, ¿y los demás? Transcurrido un año, ¿qué sentido tiene conservarlos?".

Las ventajas van más allá de la limitación de riesgos. Tomemos, por ejemplo, el marketing. Si su base de datos no está depurada, lo más probable es que contenga datos obsoletos. Si su base de datos cuenta con decenas de miles de personas y realiza frecuentes campañas de marketing por correo electrónico, los costes van sumando. Además, esto distorsiona las estadísticas de resultados de las campañas.

La minimización de datos también es aplicable a los datos físicos. Tenga cuidado con lo que imprime (como los escaneados de pasaportes de clientes); tenga cuidado con lo que anota (como las contraseñas de cuentas). Y en aquellos casos en que tenga que conservar una copia física de algo, guárdela de manera segura. Esa montaña de papeles sobre su escritorio puede parecer imponente. Pero segura, no lo es.

Rafael Bloom
@rafibloom73

Director de Salvatore Ltd.

"Estamos presenciando un modo de pensar totalmente diferente sobre la interfaz entre la tecnología y lo que la empresa está haciendo concretamente. Ese nivel de madurez digital dentro del liderazgo empresarial tuvo que surgir a la desesperada".

Repercusiones de la exposición: desde los más altos directivos hasta el consumidor

La protección de datos es un concepto regulador que circula desde hace décadas. No obstante, las grandes multas impuestas hasta el momento a importantes empresas, como Google[1], British Airways y la cadena hotelera Marriott[2] (así como la enorme cobertura en los medios que generaron) han conseguido centrar la atención de los altos directivos en el RGPD. Y esto ha causado un efecto de goteo.

1. Varonis: A Year in the Life of the GDPR: Must-Know Stats and Takeaways (Un año en la vida del RGPD: Estadísticas de obligatorio conocimiento y aportaciones) www.varonis.com/blog/gdpr-effect-review/ [consultado el 26.11.19]
2. The Guardian: GDPR fines: where will BA and Marriott's £300m go? (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 [consultado el 26.11.19]

¿Cómo ha cambiado la protección de datos desde el RGPD?

Continúa...

Otra fuerza motriz de la adopción de sólidas medidas de protección de datos es la economía colaborativa. Hoy, las grandes empresas efectúan exhaustivas comprobaciones de debida diligencia de la integridad de la protección de datos de potenciales proveedores porque no desean verse involucradas en vulneraciones de datos por asociación.

El refuerzo de la concienciación comercial del RGPD tiene también otra cara: los consumidores son más conscientes de sus derechos en materia de datos. Y saben que si una empresa pierde el control de sus datos —¡ojo!: no tiene que ser necesariamente una vulneración de datos— pueden exigir una compensación. Las empresas deben mantenerse atentas.

Sally Eaves
@sallyeaves

Consejera Delegada y Directora,
Sally Eaves Consultancy

"La protección de datos se ha convertido en un imperativo empresarial donde la confianza se puede ganar o perder".

Sección 2 – ¿Cómo están las organizaciones capacitando a sus empleados?

Capacitación del personal: un concepto capaz de disparar un vendaval de suspiros entre los empleados.

Otro motivo para asegurarse de que la capacitación resulte motivadora. Una fuerza de trabajo capacitada tiene menos probabilidades de contravenir las buenas prácticas en materia de protección de datos. Incluso en caso de producirse una vulneración de datos, la ICO (Oficina del Comisionado de Información (el organismo regulador de la protección de datos del Reino Unido) se mostrará menos rigurosa si, en su opinión, se puede demostrar que se han hecho esfuerzos por capacitar al personal en protección de datos.

Rafael Bloom
@rafibloom73

Director, Salvatore

"Prefiero considerar a los datos como un eslabón de la cadena de suministro, cuyo origen y la totalidad de su ciclo de vida deben estar sujetos a una gestión adecuada. Sí, está muy bien y es recomendable reunir al equipo en una sala durante media hora para explicarles qué hacer, por qué no triturar el material y los fundamentos de una contraseña adecuada. De este modo habrá conseguido disminuir el nivel de riesgo para la organización. Pero, de verdad, ¿existe alguna diferencia sustancial, fuera de ese pequeño impacto inicial que ha impuesto a la gente? Pues no".

Sin embargo, en abril de 2019, la Ministra de Industrias Digitales y Culturales, Margot James, sugirió que solo tres de cada diez organizaciones británicas contaba con personal debidamente capacitado para hacer frente a las ciberamenazas[1]. Ya es hora de tomarse en serio la capacitación.

Se trata de engendrar cultura, no de mero formalismo

La capacitación consiste en promover un genuino cambio de conducta y de cultura, no en mero formalismo. Resulta sencillo adquirir un paquete de capacitación en línea con algunas preguntas fáciles sobre protección de datos que cualquiera puede contestar correctamente. Sin embargo, ¿cree que así va a contribuir a proteger correctamente a su organización?

Las buenas prácticas de protección de datos tienen dos ingredientes fundamentales. En primer lugar, una capacitación inteligente, cautivante y dirigida a los retos específicos que debe afrontar su organización. En segunda instancia, concienciarse de que el RGPD es una cuestión de cultura laboral que involucra diariamente a todos los empleados. Se trata de hacer lo correcto con los datos en todos los niveles de la organización. Pensemos, por ejemplo, en RR.HH. Pensemos en los datos de todos los candidatos a un empleo que están guardados en los servidores de correo.
La protección de los datos es responsabilidad de todos y cada uno.

1. Intelligent CISO: One year on, what has been the impact of GDPR on data security? (Tras un año de su implementación, ¿cuál ha sido la repercusión del RGPD en la protección de los datos?) www.intelligentciso.com/2019/04/16/one-year-on-what-has-been-the-impact-of-gdpr-on-data-security/ [consultado el 26.11.19]

¿Cómo están las organizaciones capacitando a sus empleados?

Siempre hay una persona detrás de los datos

En la primera sección señalamos que los consumidores son cada vez más conscientes acerca de sus derechos en materia de datos. Un buen método para abordar la capacitación en protección de datos es contribuir a que el personal haga la conexión de que siempre hay una persona detrás de los datos. Pida a sus empleados que piensen en todas las organizaciones a las que hayan facilitado sus datos y tomarán conciencia de que la protección de los mismos es una cuestión de privacidad personal.

Tenga preparado un plan de contingencia

Sally Eaves
@sallyeaves

"La capacitación continua de los empleados en protección de los datos y privacidad es un imperativo empresarial. No hablamos de una única sesión anual de capacitación, sino de una experiencia proactiva, interactiva y motivadora que se convierta en parte de la experiencia laboral cotidiana. Los empleados deben estar involucrados en el diálogo sobre qué queremos mitigar, gestionar y defender".

Miriam Brown
@Kingston_MBrown

"Me parece interesante cuando, en una capacitación, le decimos a la gente: '¿qué pasaría si fuesen tus datos?' Si el gerente de mi banco estuviese trabajando con su portátil desde casa y tuviese datos sensibles en ese dispositivo, yo querría que dicho aparato estuviese cifrado".

Rob Allen
@Rob_A_kingston

"Trata los datos como si fuesen los tuyos".

Sección 3 – ¿Cómo están las organizaciones capacitando a sus empleados?

El trabajo remoto es la nueva norma

Lo más probable es que el personal acceda a su entorno de trabajo desde diversos dispositivos, incluyendo equipos personales que pueden dejarse olvidados en un tren o extraviarse en un taxi. El reto consiste en encontrar la manera de que trabajen de manera eficiente sin exponernos a los riesgos de seguridad y a las vulneraciones de datos. Basta con una sola persona para echar por la borda todas las iniciativas de protección de datos.

Sally Eaves
@sallyeaves

Consejera Delegada y Directora, Sally Eaves Consultancy

"Los datos deben estar protegidos en tránsito, en reposo y en uso: es fundamental contar con un plan exhaustivo de protección, recuperación y supresión de datos que abarque todos estos contextos. Es de especial importancia poner atención en las áreas de riesgo habitualmente subestimadas, como por ejemplo unidades USB no cifradas, uso del correo electrónico para enviar datos adjuntos no cifrados y funciones de navegadores web que exponen datos sensibles de los usuarios. Con tantos dispositivos conectados y un entorno de transformación de los patrones de trabajo, es fundamental garantizar que los datos guardados en un teléfono móvil estén tan seguros como los almacenados en un servidor de la empresa".

Autenticación de dos factores

En una organización promedio, sin duda lo mejor y más fácil que se puede hacer es proteger el perímetro de la red. Y eso puede ser tan sencillo como el empleo de administradores de contraseñas y autenticación de dos factores. Un buen ejemplo de autenticación de dos factores es cuando se pide al usuario que introduzca una contraseña en el portátil y, si lo hace correctamente, enviarle un código de entrada a su teléfono móvil.

VPN y discos SSD y unidades USB cifrados

Las redes privadas virtuales, VPN, son cada vez más populares entre las pymes. Las VPN son especialmente idóneas para el personal que accede a los datos de la organización a través de redes wifi públicas. No obstante, las empresas deben tener cuidado de no sobreestimar las capacidades de las VPN. Son una parte de la solución, no la solución integral. Con mucha frecuencia las empresas implementan VPN solamente para que los trabajadores remotos utilicen dispositivos sin hardware cifrado. Prácticamente todos guardan archivos en sus portátiles. ¿Y qué pasa si ese dispositivo es pirateado o robado, o se extravía? Los USB y SSD cifrados son apenas un poco más caros que las versiones estándar. 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. 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.

"Una vez conocí un experto en ciberseguridad que intentaba persuadir al Consejero Delegado de una empresa para que adoptase la autenticación de dos factores a quien se le respondió: 'No; no vamos a hacerlo. Es demasiado esfuerzo, un paso adicional. No lo quiero'. Poco tiempo después fue víctima de un fraude de 40.000 libras esterlinas".

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".

Rob Allen
@Rob_A_kingston

Director de Marketing y Servicios Técnicos, Kingston Technology

¿Cómo están las organizaciones capacitando a sus empleados?

Servidores privados y Proveedores de Servicios Administrados

Un creciente número de grandes organizaciones han tomado la decisión de volver a tener sus servidores en sus instalaciones. Con ello pretenden tener el control absoluto de sus granjas de servidores, sin guardar nada en la red accesible públicamente. También existen soluciones de servidores híbridos, en virtud de las cuales los datos no sensibles se mantienen en la nube, y los datos personales en local. Para las pymes y organizaciones del tercer sector, tener servidores propios puede resultar demasiado caro. Ahí es donde entran en juego los proveedores de servicios administrados y los servidores privados virtuales. Estas soluciones se centran en la protección y no incrementan drásticamente los gastos de explotación.

Señalización automática de los datos que caducan

Una de las obligaciones del RGPD es la necesidad de borrar los datos antiguos. Por ejemplo, ciertos tipos de datos personales no pueden conservarse durante más de siete años. ¿Que pasaría si se le indicase automáticamente cuando los datos estén a punto de 'caducar'? Con la base de datos correcta, a su departamento de TI le resultaría fácil crear un comando que envíe un mensaje electrónico autogenerado al Delegado de Protección de datos cuando se aproxime la fecha límite de retención de 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 las organizaciones de su sector o segmento. Asegúrese de que los proveedores que elija no solamente tengan la tecnología, sino que también entiendan las dificultades de adopción de métodos de protección de datos.

Sección 4 – ¿Cómo pueden los proveedores de tecnología mejorar los procesos y la comprensión?

Centros de aprendizaje y enseñanza para los DPD

Desde 2016, la demanda de Delegados de protección de datos (DPD) se ha disparado, incrementándose en más de un 700%.[1] Hoy en día, en Europa hay empleados más de 500.000 DPD, seis veces más de lo que se preveía en 2017.[2] No obstante, su importancia suele subestimarse y trivializarse.

Un DPD tiene que ser plenamente visible en el entorno de la protección y privacidad de datos de su empresa. Se trata de un trabajo a tiempo completo. No obstante, en algunas organizaciones, 'DPD' no es más que una etiqueta asignada al miembro del personal que mejor entiende la tecnología. Son responsables de la privacidad de los datos en toda la empresa, además de tener que cumplir sus obligaciones habituales.

La realidad es que sería necesaria una serie de servicios y herramientas profesionales a disposición de esta nueva generación de DPD. Incluso si su entidad tiene un DPD a tiempo completo, la protección de los datos es una cuestión muy dinámica y siempre habrá retos que requieran una segunda opinión. Trabajar con una consultoría o un asesor externo especializados en protección de datos puede resultar muy útil, aunque lo más conveniente es tener las cosas lo más ordenadas posible a nivel interno.

Claridad, contingencia y cohesión

Su infraestructura de TI es tan sólida como su elemento más débil. Ese es el motivo por el cual, para cualquier nueva adición a su ecosistema informático, su proveedor de tecnología debe proporcionar una claridad total sobre las potenciales amenazas a la seguridad, y asesorar de manera transparente sobre cómo utilizar de manera segura el nuevo producto.

Tara Taubman-Bassirian
@clarinette02

RGPD, protección de datos y consultores de TI

"Intento explicar a la gente que instala cámaras de CCTV por doquier que eso no es necesariamente seguridad, ya que suelen instalarlas sin contraseña. De ese modo, siempre será posible conectarse a sus sitios web, sentarse y observar. De hecho, le estamos diciendo al ladrón: '¡ven a vigilar y sabrás cuándo no estoy!"

1. Varonis: A Year in the Life of the GDPR: Must-Know Stats and Takeaways (Un año en la vida del RGPD: Estadísticas de obligatorio conocimiento y aportaciones) www.varonis.com/blog/gdpr-effect-review/ [consultado el 26.11.19]
2. The Guardian: GDPR fines: where will BA and Marriott's £300m go? (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 [consultado el 26.11.19]

¿Cómo pueden los proveedores de tecnología mejorar los procesos y la comprensión?

Tenemos la cuestión de la contingencia. ¿Qué ocurre cuando un producto llega al final de su vida útil, o necesita ser actualizado? Los proveedores de tecnología deben aportar asesoramiento de contingencia sobre sus productos si inadvertidamente dejan expuestos los datos que contienen o exponen la seguridad de su ecosistema informático en general. Consideramos, por ejemplo, un escáner de resonancia magnética. Puede incluir un disco SSD cifrado de 4 terabytes para almacenar las imágenes de los pacientes. Pero, ¿qué ocurre cuando el espacio se agota?

Además, tanto los proveedores de tecnología como las propias organizaciones deben facilitar un entorno de cohesión digital y de cohesión de los datos, no solo dentro de la organización, sino también al trabajar con proveedores y colaboradores externos. Eso es especialmente fundamental para las organizaciones polifacéticas, multidepartamentales y con múltiples sedes, como el NHS (Servicio Nacional de Salud británico).

Miriam Brown
@Kingston_MBrown

Gerente de Marketing Estratégico B2B en Kingston Technology

"Hemos vendido muchos productos al NHS, aunque existen diferencias de un grupo a otro, cuando preguntamos qué políticas y protocolos de protección tienen implementados".

Detección precoz

La tecnología avanza con gran rapidez, en ocasiones adelantándose a la seguridad. Con las tecnologías emergentes —como, por ejemplo, el pago mediante reconocimiento facial en China— a veces sucede que las organizaciones se lanzan a adoptar las tecnologías antes de considerar las potenciales implicaciones en materia de seguridad y protección de datos. La amplia disponibilidad de redes 5G es cuestión de uno o dos años, cuando la informática periférica y los silos de datos distribuidos se conviertan en realidad. Los proveedores de tecnología deberán estar capacitados para ayudar a las organizaciones a beneficiarse de las tecnologías emergentes sin poner en peligro la integridad de sus datos ni la seguridad de sus sistemas informáticos.

Sally Eaves
@sallyeaves

Consejera Delegada y Directora, Sally Eaves Consultancy

"Creo que comenzaremos a ver un cambio en el RGPD, una vez que concluyan las dificultades de la implementación, que se centrará en optimizar las ventajas, como la mejora de los procesos de TI, copia de seguridad y recuperación, así como perfeccionamiento de la seguridad, y utilizar esto como puntos de diferenciación en relación con sus homólogos".

Resumen

El RGPD ha cambiado a las empresas para mejor, poniendo la privacidad de los datos y la seguridad de las redes en el centro de atención de altos directivos y de consumidores por igual. No obstante, el cumplimiento normativo requiere una atención constante en la protección de los datos —día sí y día también— de parte de los empleados. La continua evolución de la tecnología y de las ciberamenazas supone que una buena infraestructura de seguridad y una buena capacitación —respaldadas por un buen respaldo y asesoramiento en tecnología y privacidad de datos— son factores críticos. Recordar al personal que detrás de los datos hay siempre una persona puede ser muy útil para promover una cultura de protección de datos entre los empleados. Un cambio cultural es muchísimo más efectivo que ejercicios de capacitación formalistas.

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