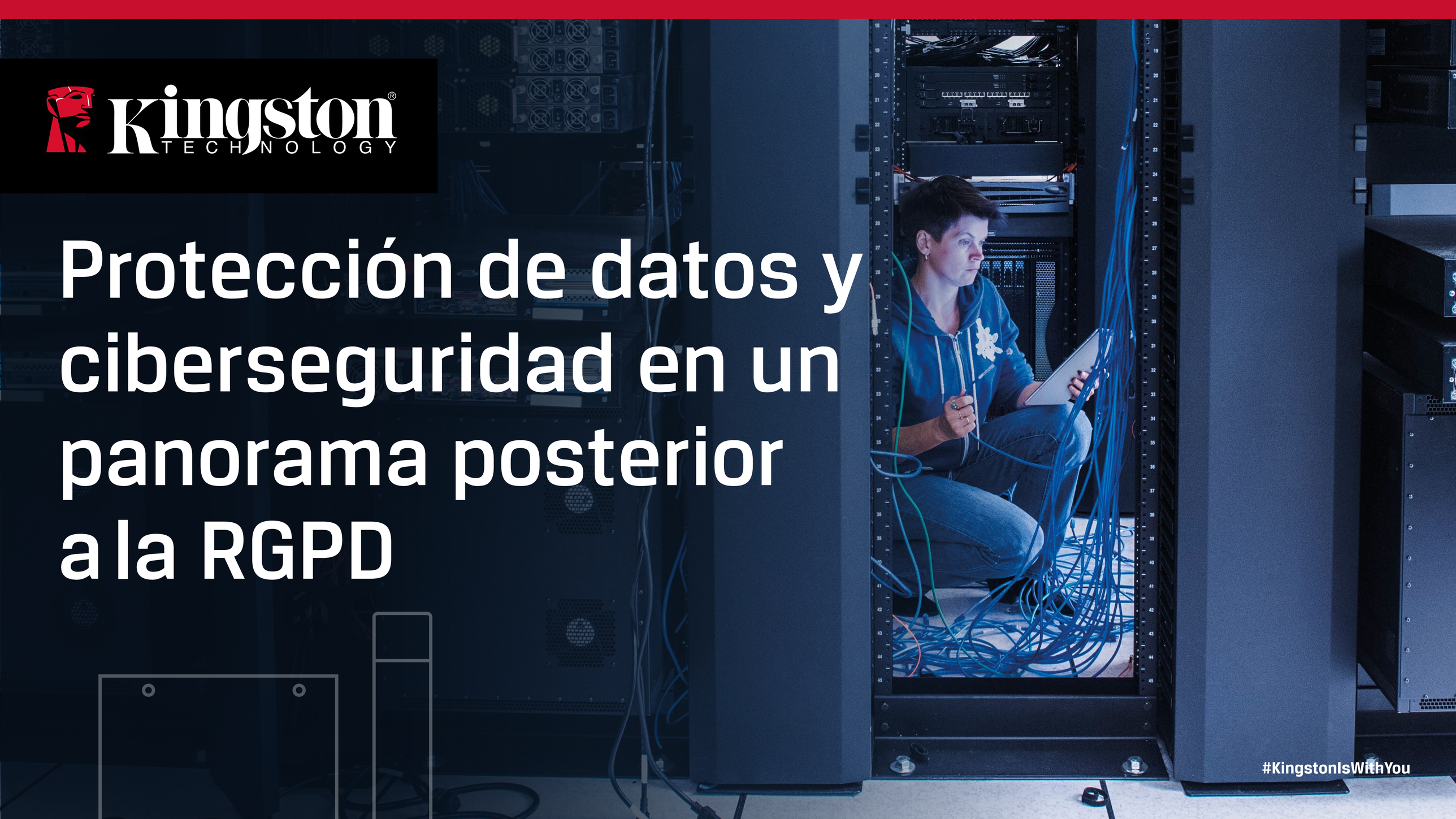
Protección de datos y ciberseguridad en un panorama posterior a la RGPD



#KingstonIsWithYou

Protección de datos y ciberseguridad en un panorama posterior a la RGPD

Prólogo

Innumerables empresas y organizaciones trabajaron duro, y contrataron a muchas personas, para prepararse para la GDPR. Quizás la suya fue una de ellas Sin embargo, la naturaleza de la constante evolución de las amenazas cibernéticas demuestra no se puede dar el lujo de detenerse y recuperar el aliento. El cumplimiento de la GDPR no es un ejercicio de verificación, sino un marco a través del cual se juzgan sus esfuerzos continuos de protección de datos y seguridad cibernética. No hay lugar para la complacencia.

En este breve libro electrónico, agrupamos el conocimiento de algunos de los comentaristas más experimentados del Reino Unido en seguridad cibernética para analizar cómo ha cambiado la protección de datos desde la introducción de la GDPR. También abarcamos el cómo las empresas están educando a sus empleados sobre la necesidad del cumplimiento, y discutimos cómo los departamentos de TI y los proveedores de tecnología pueden proteger mejor la infraestructura de TI y educar a los usuarios finales sobre los desafíos de seguridad emergentes.

Protección de datos y ciberseguridad en un panorama posterior a la RGPD

Colaboradores

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

Rob Allen
@Rob_A_kingston

Rob es el Director de Marketing y Servicios Técnicos de Kingston Technology, y ha estado con la compañía desde 1996. En su labor, Rob es responsable de supervisar las RR.PP., las redes sociales, el marketing de canales con los medios de marketing digital y el equipo creativo de todas las marcas y productos de Kingston.

Tara Taubman-Bassirian
@clarinette02

Tara tiene muchos títulos: abogada, defensora, mediadora, investigadora, consultora, oradora y escritora. Con una experiencia increíble en áreas como la privacidad, la propiedad intelectual y la protección de datos, se ha hecho un nombre en varias lugares del mundo, especialmente en el Reino Unido, Francia y los Estados Unidos.

Rafael Bloom
@rafibloom73

Rafael es el Director de Salvatore ltd. En este cargo, ayuda a las empresas a gestionar los desafíos y oportunidades estratégicas, comerciales y de procedimiento creadas por el cambio tecnológico y normativo.

Miriam Brown
@Kingston_MBrown

Gerente de Marketing Estratégico B2B en Kingston Technology, y ha estado con la compañía desde 1997. En su rol, Miriam es responsable de la estrategia de marketing, el contenido y las campañas para todos los productos B2B de Kingston.

Sally Eaves
@sallyeaves

La profesora Sally Eaves ha sido descrita como la 'portadora de la antorcha para la tecnología ética". Aporta una gran experiencia a las funciones de Directora Ejecutiva y Directora de Tecnología, como profesora en Tecnologías emergentes y como Asesora estratégica global. Sally es una oradora internacional premiada, autora, investigadora e influenciadora que comparte un liderazgo de pensamiento original y auténtico.

Protección de datos y ciberseguridad en un panorama posterior a la RGPD

Tabla de contenidos

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

Las empresas han recorrido un largo camino. En los últimos dos años, los equipos legales se han expandido, la contratación de Oficiales de Protección de Datos se ha disparado[1] y las consultas con asesores externos de privacidad de datos se han incrementado. La finalización de las evaluaciones de impacto de protección de datos (DPIAs) ahora es familiar para miles de organizaciones.

Pero hay un largo camino por recorrer.

Uno de los mayores desafíos con la GDPR es que no le puedes quitar la vista a la pelota. En la mayoría de las organizaciones, casi cualquier miembro del personal, en cualquier momento, podría contravenir las reglas. El problema se magnifica en sectores donde la fuerza laboral es flexible o hay un alto grado de autonomía, como la salud, la educación y el derecho.

En el ámbito del derecho por ejemplo, a muchos abogados no les preocupará intercambiar detalles sensibles del caso a través de un simple archivo adjunto de correo electrónico. Los profesionales de la salud intercambiarán datos de pacientes o los resultados de una resonancia magnética desde direcciones de correo electrónico no seguras. En las organizaciones de alto estrés, todo lo que se necesita es un poco de presión adicional en la lista de tareas, para que el cumplimiento se olvide. La productividad, al parecer, triunfa sobre el protocolo.

Esto debe cambiar.

Luego está el tema de la conciencia en el sector de la caridad. Con frecuencia, las organizaciones benéficas parecen pensar que están exentas de la RGPD. Incluso entendiendo que la RGPD se aplica a todas las organizaciones privadas, públicas y del tercer sector, son, quizás entendible, reacios a desviar el dinero de su causa para invertir en protección de datos.
Eso es noble pero también ingenuo. Las posibles multas por contravenir la RGPD superan el eventual gasto en TI.

Tara Taubman-Bassirian
@clarinette02

GDPR, Protección de datos y Consultor IP

"Muchas organizaciones del tercer sector dicen: 'La RGPD no se aplica a nosotros, solo somos una organización benéfica. Incluso en lo que respecta al cumplimiento en el sitio web, trato de decirles que no se trata de los datos que desea recopilar, sino de los terceros a los que está permitiendo acceder a los datos de sus visitantes".

Desde el 2016 La demanda de Oficiales de protección de datos (OPDs) se ha disparado y ha aumentado más del 700%.

1. Varonis: Un año en la vida de la GDPR: Estadísticas imprescindibles y conclusiones www.varonis.com/blog/gdpr-effect-review/ [accedido el 26.11.19]

¿Cómo ha cambiado la protección de datos desde la GDPR?

La minimización de datos es una tendencia alentadora

Vivimos en una era alarmante de recopilación de datos. Las cuatro grandes "The Big Four" (Google, Apple, Facebook y Amazon) almacenan grandes cantidades de datos de los clientes. La deducción que podría sacar las otras organizaciones sería imitar a "The Big Four" y recopilar la mayor cantidad de datos posible. Sin embargo, cuantos más datos tenga, mayor es el riesgo al que se expone. Una de las tendencias más positivas observadas desde la introducción de la GDPR es una rebelión contra la recopilación excesiva de datos. Las compañías inteligentes emplean un espíritu de minimización de datos: si no los necesita, no los recopile.

Tara Taubman-Bassirian
@clarinette02

GDPR, Protección de datos y Consultor IP

"La minimización de datos es probablemente uno de los mejores principios de la GDPR. Cualquier creación de una base de datos significa crear riesgos".

Rob Allen
@Rob_A_kingston

Director de Marketing y Servicios Técnicos, Kingston Technology

"Tenemos reglas estrictas de eliminación de datos. Sí, los datos críticos para el negocio deben almacenarse correctamente. Pero, ¿para todo lo demás? Después de que ha pasado un año. ¿Cuál es el punto de almacenarlos?"

Los beneficios se extienden más allá de limitar el riesgo. Mire a marketing, por ejemplo. Si su base de datos de marketing no está depurada, es posible que este almacenando datos obsoletos. Cuando su base de datos se encuentra con decenas de miles de personas y usted realiza frecuentes campañas de marketing por correo electrónico, los costos empiezan a sumar. Esto también sesga las estadísticas de rendimiento de su campaña.

La minimización de datos también se aplica a los datos físicos. Tenga cuidado con lo que imprime (como escaneos de pasaportes de clientes); tenga cuidado con lo que escribe (como las contraseñas de las cuentas). Y cuando necesite guardar una copia física de algo, guárdela de manera segura. Esa montaña de papeleo en su escritorio puede parecer imponente. Pero no es segura.

Rafael Bloom
@rafibloom73

Director, Salvatore Ltd

"Somos testigos de una forma completamente diferente de pensar acerca de la interfaz entre la tecnología y lo que realmente hace una empresa. Ese nivel de madurez digital dentro del liderazgo empresarial se necesitaba desesperadamente".

Impacto de la exposición: del "C-suite" (alta dirección) al consumidor

La protección de datos como concepto regulatorio existe desde hace décadas. Pero las grandes multas otorgadas hasta el momento a compañías como Google[1], British Airways y la cadena hotelera Marriott[2] , y la cobertura que generaron de los medios, han despertado la atención por la GDPR del "C-suite". Esto ha causado un efecto de goteo.

1. Varonis: Un año en la vida de la GDPR: Estadísticas imprescindibles y conclusiones www.varonis.com/blog/gdpr-effect-review/ [accedido el 26.11.19]
2. The Guardian: ¿Multas de la GDPR: A dónde irán las £300m de BA y Marriott? www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog [accedido el 26.11.19]

¿Cómo ha cambiado la protección de datos desde la GDPR?

Continuación...

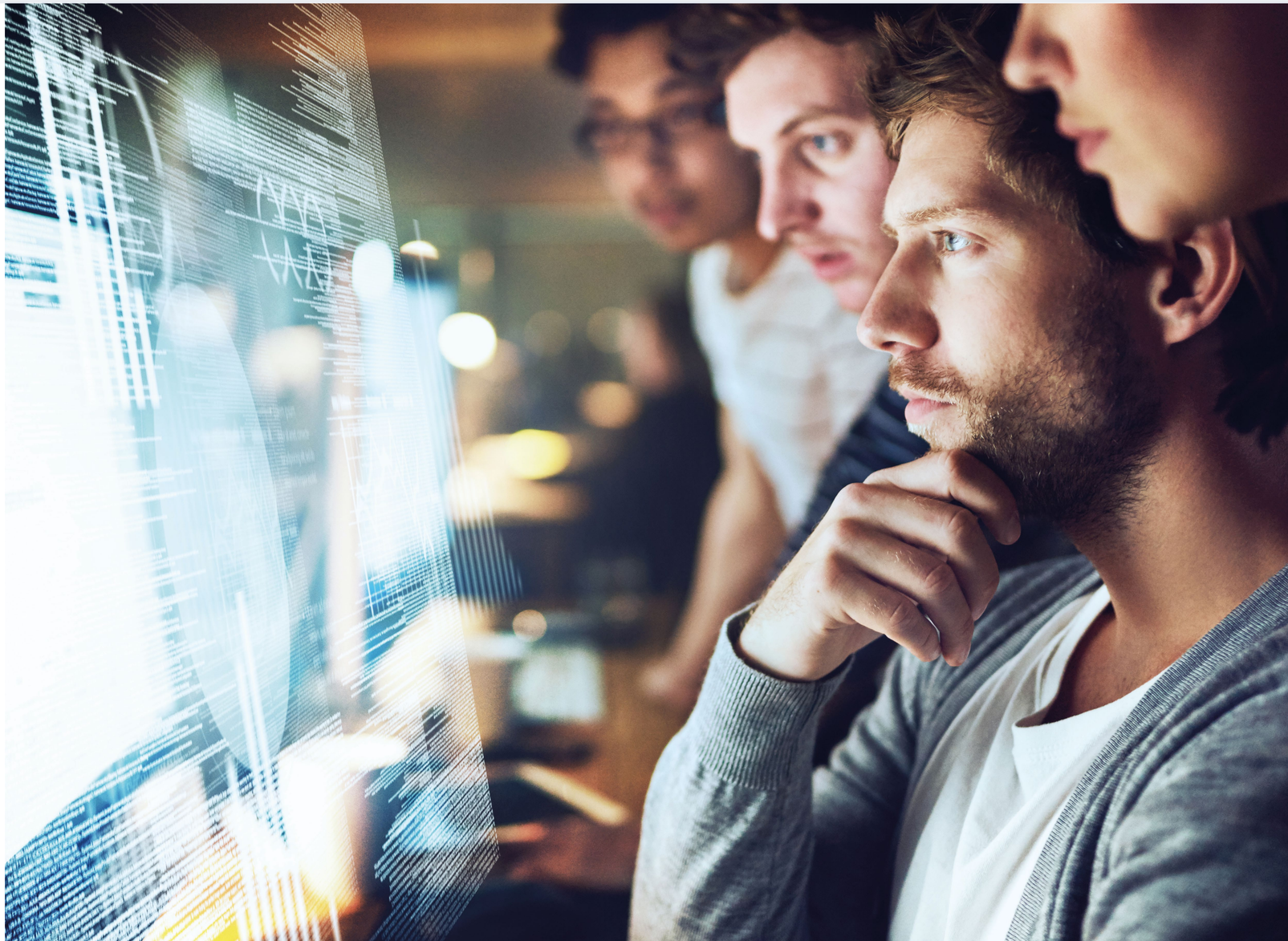
Otra fuerza impulsora detrás de la adopción de una sólida protección de datos es el negocio colaborativo. Las grandes empresas hoy realizan un proceso de debida diligencia en la integridad de la seguridad de los datos de un posible proveedor, porque no quieren ser responsables, por asociación, de las infracciones de datos.

También está la otra cara de la mayor conciencia comercial de la GDPR: los consumidores son más conscientes de sus derechos sobre los datos. Y saben que si una empresa pierde el control sobre sus datos, tenga en cuenta que no necesariamente tiene que haber una filtración, tienen derecho a una compensación. Las empresas deben mantenerse enfocadas

Sally Eaves
@sallyeaves

CEO y Directora,
Sally Eaves Consultancy

"La protección de datos se ha convertido en un factor fundamental, donde la confianza se puede ganar o perder".



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

Capacitación del personal: dos palabras capaces de hacer que su fuerza laborar ponga los ojos en blanco.

Una buena razón para asegurarse de que su entrenamiento sea atractivo. Es menos probable que una fuerza laboral educada contravenga las buenas prácticas en materia de protección de datos. Y si hay una violación de datos, la Oficina del Comisionado de Información "Information Commissioner's Office" (ICO) lo mirará con más benevolencia, si puede probar que ha hecho esfuerzos para capacitar a su personal en seguridad de datos.

Rafael Bloom
@rafibloom73

Director,
Salvatore

"Me gusta pensar en los datos como un elemento de la cadena de suministro, donde su procedencia y todo su ciclo de vida deben tener una gestión adecuada. Está muy bien tener a su equipo en una habitación durante media hora y decirles qué hacer, por favor no triture cosas, por favor tenga una contraseña decente. Claro, ha reducido el riesgo para la organización. Pero luego, ¿hay realmente una diferencia material aparte de ese pequeño impacto inicial que impuso en las personas? No."

Sin embargo, en abril de 2019, la ministra digital Margot James sugirió que tres de cada diez organizaciones del Reino Unido tienen personal capacitado para hacer frente a las amenazas cibernéticas[1]. Es hora de tomarse en serio el entrenamiento.

Se trata de engendrar cultura, no de capacitar marcando casillas

La capacitación se trata de afectar el cambio genuino de comportamiento y cultural, no de marcar casillas. Es fácil comprar un paquete de capacitación en línea con algunas preguntas sencillas sobre protección de datos que cualquiera puede responder correctamente. ¿Pero eso va a ayudar realmente a proteger su organización?

Los buenos comportamientos en protección de datos tienen dos ingredientes fundamentales. En primer lugar, una capacitación inteligente, atractiva y orientada a los desafíos únicos de su organización. En segundo lugar, darse cuenta de que la GDPR es una asunto profundo de cultura laboral que impacta diariamente a todos los empleados. Se trata de hacer lo correcto con los datos, de forma adecuada a través de la organización. Mire a recursos humanos, por ejemplo. Piense en todos los detalles personales del candidato que se encuentran en los servidores de correo electrónico.
La protección de datos es responsabilidad de todos.

1. Intelligent CISO: Un año después, ¿cuál ha sido el impacto de la GDPR en la seguridad de los datos? www.intelligentciso.com/2019/04/16/one-year-on-what-has-been-the-impact-of-gdpr-on-data-security/ [accedido el 26.11.19]

¿Cómo están educando las organizaciones a sus empleados?

Hay una persona detrás de los datos

En la primera sección notamos que los consumidores están cada vez más conscientes de sus derechos sobre los datos. Una buena manera de posicionar la capacitación en protección de datos, es ayudar a su personal a establecer la conexión de que siempre hay una persona detrás de los datos. Pídales a sus empleados que piensen en todas las organizaciones a las que les han dado sus datos y se den cuenta de que la protección de datos se trata de privacidad personal.

Tenga un plan de contingencia

Sally Eaves
@sallyeaves

"La educación continua para los empleados sobre la seguridad y la privacidad de los datos es un factor fundamental. Esta no debe ser una sesión de capacitación única, una vez al año, sino una experiencia proactiva, interactiva y atractiva, para que sea parte de la experiencia laboral diaria. Los empleados deben participar en el diálogo sobre lo que queremos mitigar, gestionar y defender".

Miriam Brown
@Kingston_MBrown

"Creo que es interesante durante la capacitación cuando le dices a la gente: '¿Y si se tratara de sus datos? Si el gerente de mi banco trabajara desde su casa en su computadora portátil y tuviera información confidencial en esa computadora portátil, me gustaría que estuviera en una unidad encriptada".

Rob Allen
@Rob_A_kingston

"Trate los datos como si fueran suyos".

Sección 3 –
¿Pueden los departamentos de TI proteger mejor los dispositivos?

El trabajo remoto se volvió normal

Es probable que su personal acceda a su mundo laboral desde varios dispositivos diferentes, incluyendo dispositivos personales que pueden dejarse fácilmente en un tren o perderse en un taxi. Su desafío es encontrar una manera de ayudar a su personal a trabajar de manera eficiente sin estar expuesto a riesgos de seguridad e infracciones de datos. Todo lo que se necesita es a una persona que ponga fin a sus esfuerzos de protección de datos.

Sally Eaves
@sallyeaves

CEO y Directora,
Sally Eaves Consultancy

"Los datos deben protegerse en tránsito, en reposo y en uso; es fundamental contar con un plan de seguridad, recuperación y eliminación de datos que abarque todos estos contextos. Llamar la atención sobre las áreas de riesgo que a menudo están subestimadas es particularmente importante, por ejemplo, USBs sin encriptar, usar el correo electrónico para enviar archivos adjuntos no encriptados y características del navegador web que exponen datos confidenciales del usuario. Con tantos dispositivos conectados y modalidades de trabajo en constante cambio, es fundamental garantizar que los datos almacenados en un teléfono móvil estén tan seguros como los datos almacenados en el servidor de una empresa ".

Autenticación de dos factores

Para la organización promedio, lo mejor y más fácil que puede hacer es proteger el perímetro de su red, y eso puede ser tan simple como el uso de administradores de contraseñas y autenticación de dos factores. Un buen ejemplo de autenticación de dos factores es cuando se le pide al usuario que proporcione una contraseña en una computadora portátil, así como un código de acceso que se envía a su teléfono móvil una vez que se ha entregado la contraseña con éxito.

VPNs y SSDs/USBs encriptados

Las VPNs son cada vez más populares entre las pymes. Son particularmente importantes para el personal que accede a datos empresariales a través de redes WIFI públicas. Pero las empresas deben tener cuidado de no sobreestimar las capacidades de las VPN. Son parte de esta, más no son la solución completa. Muy a menudo, las empresas implementan VPN, solo para que los trabajadores remotos utilicen computadoras portátiles o notebooks sin ningún encriptado por hardware. Casi todo el mundo almacena archivos en su computadora portátil. ¿Qué sucedería si ese dispositivo es pirateado, perdido o robado? Los USBs y SSDs encriptados son solo un poco más caros que las versiones estándar. La implementación de USBs encriptados y el equipar sus computadoras portátiles con SSDs encriptados por hardware ayuda mucho a resolver los desafíos del trabajo remoto. Y si un dispositivo se pierde o es robado, puede estar seguro de que nadie tendrá acceso a los archivos encriptados. Incluso puede destruir remotamente los USBs perdidos.

"Una vez conocí a un experto en seguridad cibernética que intentó persuadir al CEO de una empresa para que adoptara la autenticación de dos factores, solo para que existiera un poco de resistencia: 'No, no lo vamos a hacer, es una molestia, es un paso adicional, no lo quiero". Poco después fueron víctimas de un fraude de £40,000".

Rafael Bloom
@rafibloom73

Director, Salvatore Ltd.

"Al final, el mejor método para mejorar la concientización sobre seguridad, es abrir conversaciones con los empleados para encontrar estrategias que sean seguras y productivas".

Rob Allen
@Rob_A_kingston

Director de Marketing y Servicios Técnicos, Kingston Technology

¿Pueden los departamentos de TI proteger mejor los dispositivos?

Servidores privados y MSP

Se ha incrementado el número de grandes organizaciones que están pasando a tener nuevamente sus propios servidores en el lugar. Eso significa que tienen control total sobre el estado de su servidor, sin tener nada almacenado en la nube de acceso público. Luego están las soluciones de servidor híbrido donde los datos no confidenciales permanecen en la nube, pero los datos personales permanecen en el sitio. Para las PYME y las organizaciones del tercer sector, puede ser demasiado costoso tener su propio servidor. Y ahí es donde entran los proveedores de servicios administrados y los servidores privados virtuales. Mejoran el enfoque en la seguridad, sin inflar dramáticamente sus costos operativos.

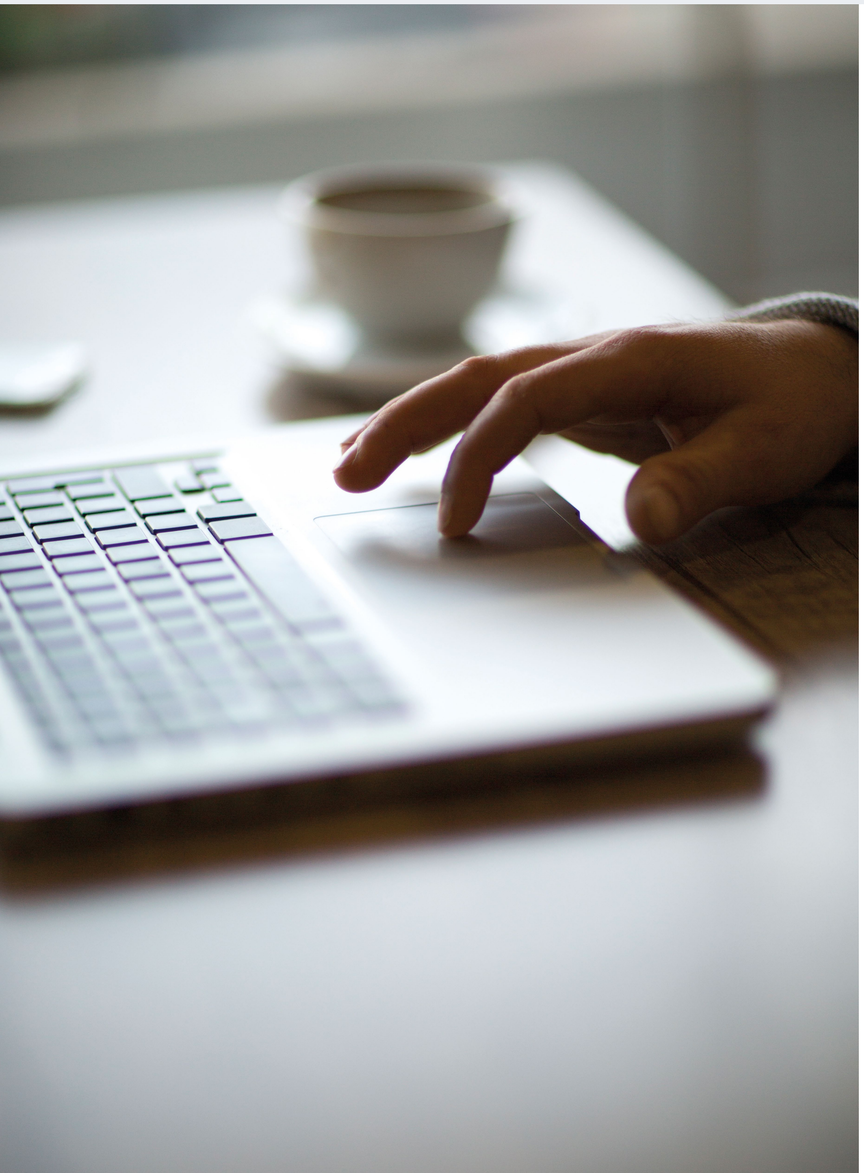
Disminución automática de datos en expiración

Uno de los principios de la GDPR es la necesidad de eliminar datos antiguos. Ciertos tipos de datos personales, por ejemplo, no deben almacenarse durante más de siete años ¿Y si se le indicara automáticamente cuando los datos estén a punto de 'expirar"? Con la base de datos correcta, sería fácil para su equipo de TI crear una acción que enviara automáticamente un correo electrónico al OPD cuando se acerque a una fecha corte de almacenamiento de datos.

Trabaje con los proveedores adecuados

Cuando se trata de seguridad de TI, hay innumerables fabricantes y proveedores. Haga su investigación. La idea es tener un sistema establecido que provenga de un proveedor confiable con experiencia específica en habilitar organizaciones dentro de su industria o sector. Asegúrese de que los proveedores que elija no solo tengan la tecnología, sino que también comprendan los desafíos de adopción en lo que respecta a la seguridad de los datos.

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



TLC para el OPD

Desde el 2016, la demanda de Oficiales de protección de datos se ha disparado, aumentando más del 700%.[1] Ahora hay más de 500,000 OPDs empleados en Europa, eso es seis veces más de lo que se pronosticaba en el 2017.[2] Y, sin embargo, la importancia del papel del OPD a menudo se pasa por alto y es trivializado.

Un OPD requiere una visibilidad total del panorama de seguridad y privacidad de los datos de su empresa. Es un trabajo de tiempo completo. Sin embargo, en algunas organizaciones el 'OPD es simplemente una etiqueta asignada al miembro del personal que mejor comprende la tecnología. Son responsables de la privacidad de los datos de toda la empresa, mientras realizan las tareas habituales de su trabajo diario.

La realidad es que debe haber una gama de servicios y herramientas profesionales disponibles para respaldar esta nueva generación de OPD. Incluso si tiene un OPD de tiempo completo, la seguridad de los datos cambia rápidamente y siempre habrán desafíos que requerirán una segunda opinión. Trabajar con una consultoría externa o un asesor en seguridad de datos puede ser muy útil, pero primero debe tener las cosas internamente lo más ordenado posible.

Claridad, contingencia y cohesión

Su infraestructura de TI es tan fuerte como su elemento más débil. Es por eso que para cualquier nueva incorporación a su ecosistema de TI, su proveedor de tecnología debe brindarle una claridad total sobre las posibles amenazas de seguridad y consejos claros sobre cómo usar su nuevo producto de forma segura.

Tara Taubman-Bassirian
@clarinette02

GDPR, Protección de datos y Consultor IP

"Trato de explicar a las personas que instalan cámaras de CCTV en todas partes que no es necesariamente seguridad, porque a menudo se instalan sin contraseña. Por lo tanto, cualquiera puede iniciar sesión en un sitio web, sentarse y mirar. En realidad usted le está diciendo a su ladrón: '¡venga y entre que no estoy allí!

1. Varonis: Un año en la vida de la GDPR: Estadísticas imprescindibles y conclusiones www.varonis.com/blog/gdpr-effect-review/ [accedido el 26.11.19]
2. The Guardian: ¿Multas de la GDPR: A dónde irán las £300m de BA y Marriott? www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog [accedido el 26.11.19]

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

Existe el problema de la contingencia. ¿Qué sucede cuando un producto alcanza el final de su vida útil o necesita una actualización? Los proveedores de tecnología deben proporcionar asesoramiento de contingencia sobre sus productos que comprometen inadvertidamente los datos que almacenan o que exponen la seguridad de su ecosistema de TI más amplio. Tome un escáner de resonancia magnética, por ejemplo. Puede venir con un SSD encriptado de cuatro terabytes para almacenar las imágenes de pacientes. Pero, ¿qué sucede cuando se agota el almacenamiento?

Los proveedores de tecnología y las propias organizaciones, también deben facilitar un entorno de cohesión digital y de cohesión de datos, tanto dentro de la organización como cuando se trabaja con proveedores y socios externos. Eso es especialmente crucial para organizaciones con múltiples facetas, múltiples departamentos y múltiples ubicaciones, como el NHS.

Miriam Brown
@Kingston_MBrown

Gerente de Marketing Estratégico B2B en Kingston Technology

"Hemos vendido muchos productos en el NHS, pero hay diferencias indiscutibles de una administración a otra cuando preguntamos qué políticas y protocolos de protección de datos tienen vigentes".

Escaneando de horizonte

La tecnología cambia rápidamente, a veces superando la seguridad. Con las tecnologías emergentes, como el pago a través del reconocimiento facial en China, a veces se da el caso de que las organizaciones compiten para lanzar la tecnología antes de considerar las posibles implicaciones de seguridad y protección de datos. La disponibilidad generalizada de redes 5G está a solo uno o dos años de distancia, donde la tecnología de punta y la distribución de silos de datos se convertirán en una realidad. Los proveedores de tecnología deben poder ayudar a las organizaciones a beneficiarse de manera segura de las tecnologías emergentes sin comprometer su propia integridad de datos o seguridad de TI.

Sally Eaves
@sallyeaves

CEO y Directora, Sally Eaves Consultancy

"Creo que comenzaremos a ver un cambio con la GDPR lejos de reducir las molestias de la implementación, para enfocarnos en optimizar las ganancias, tales como procesos de TI mejorados, respaldo y recuperación, y seguridad mejorada, y usarlos como un punto de diferenciación en relación con los pares de la industria".

Resumen

La GDPR ha cambiado los negocios para mejor, llevando la privacidad de los datos y la seguridad de la red a la atención del "C-suite" y de los consumidores. El cumplimiento sin embargo, requiere de atención constante a la seguridad de los datos, día tras día, en toda su fuerza laboral. La naturaleza en constante evolución de la tecnología y las amenazas cibernéticas significa que una buena infraestructura de seguridad y una buena capacitación, respaldada por un buen asesoramiento sobre tecnología y privacidad de datos, es fundamental para los negocios. Recordar al personal que siempre hay una persona detrás de los datos puede contribuir en gran medida a incorporar una cultura de protección de datos dentro de su fuerza laboral. Y el cambio cultural es mucho más efectivo que los ejercicios de capacitación en marcar casillas.

Acerca de Kingston

Con 32 años de experiencia, Kingston tiene el conocimiento para identificar y resolver sus desafíos de trabajo remoto, lo que facilita que su fuerza de trabajo se desempeñe de forma segura desde cualquier lugar, sin comprometer su organización.

#KingstonIsWithYou