#ITWebinars

# Brechas de seguridad, ¿hay opciones?

FORCEPOINT mobileiron okta sealpath

Diciembre 2020

itds

#ITWebinars

# Brechas de seguridad, ¿hay opciones?

**Las fugas de datos no discriminan. Adif, Mapfre, Tesla, Honda, EasyJet... son algunas de las empresas protagonistas este año de una brecha de seguridad que ha dejado expuestos los datos de miles de sus clientes. Sólo en España y hasta julio de 2020 se comunicaron a la Agencia Española de Protección de Datos (AEPD) más de 800 brechas de seguridad, 200 más que en el mismo periodo de hace un año.**

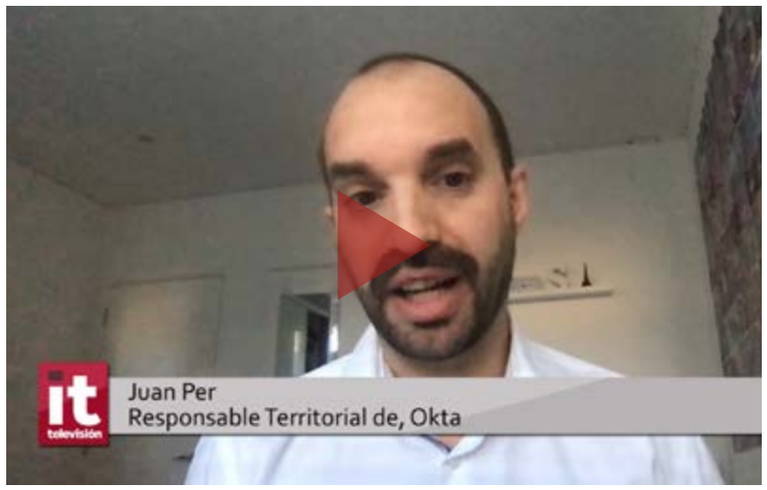


Hacer frente a una brecha de seguridad no es tarea fácil. En este ITWebinars podrás conocer varias propuestas para afrontar a una brecha de seguridad.

Una de las empresas participantes es Forcepoint, para quien el nuevo perímetro de seguridad está en el ser humano y que con su Human Centric Security protege datos y usuarios allí donde estén.

Experto en gestión unificada de endpoints, lo que MobileIron propone es que información corporativa fluye libremente y de manera segura por los dispositivos y servidores en la nube.

También veremos, a través de Okta, cómo las soluciones de gestión de identidades ayudan a proteger el acceso a la información conectando de forma segura a las personas adecuadas con las tecnologías adecuadas en el momento adecuado.





Por último contaremos con la visión de Sealpath, un experto en IRM cuya tecnología permite a profesionales y empresas proteger sus documentos críticos dondequiera que se encuentren, acompañándoles en todo momento.

A continuación, puedes leer un resumen de sus intervenciones, con los puntos más destacados. También puedes pinchar en cada una de las imágenes de sus portavoces para acceder a su intervención en el webinar o ver la sesión completa aquí.

**Luca Livrieri, Sales Engineer Manager Italy & Iberia, Forcepoint**

# “La seguridad debe cambiar de manera dinámica y ser un habilitado del negocio”

La protección de los datos es el principal reto al que se enfrentan las empresas, dice Luca Livrieri, Sales Engineer Manager Italy & Iberia de Forcepoint, en la sesión online Brechas de seguridad, ¿hay opciones?. Añade el directivo que los datos están en todas partes y que no sólo hay que proteger la oficina principal, sino las remotas; además, la pandemia sanitaria ha añadido el problema de proteger a los empleados en casa.

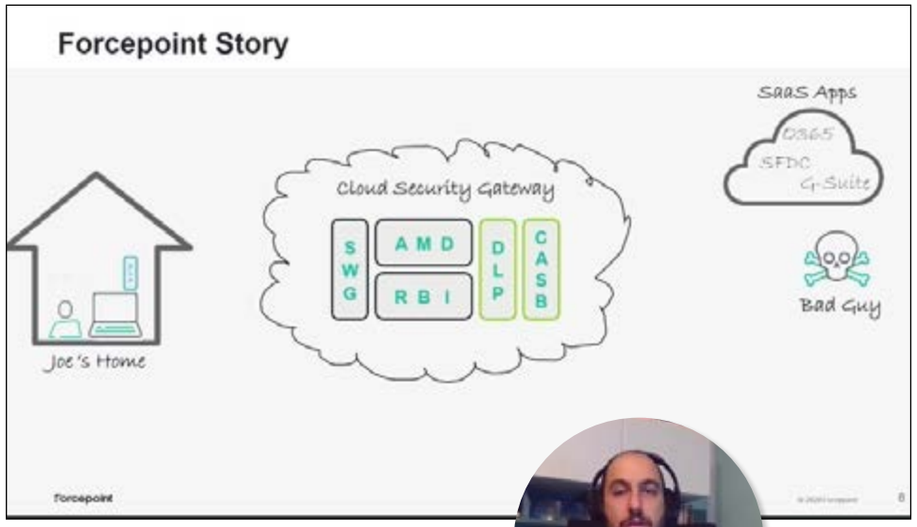
Para hacer frente a esta situación “se ha producido una convergencia de dos paradigmas: SASE y Zero Trust”, y si uno explica qué hay que proteger y el otro dice cómo hay que protegerlo en un mundo sin perímetro donde todo se mueve hacia la nube y los datos están disgregados. “Tenemos que cambiar el paradigma porque el nuevo perímetro es el usuario”, dice Luca Livrieri.

Explica el directivo de Forcepoint que el camino hacia la nube partió de una seguridad distribuida en silos, con una oferta muy fragmentada en diferentes soluciones, para pasar a una propuesta basada en la integración de productos que se hablan unos con otros y, finalmente, en la seguridad convergente, basada en servicios cloud y con un enfoque Zero Trust que valida los accesos y, muy importante para Forcepoint, verifica el comportamiento humano de manera constante.

Human Centric Cybersecurity es la propuesta de Forcepoint para los modelos Zero Trust y SASE y en la que convergen un cloud security gateway para


**LUCA LIVRIERI, SALES ENGINEER MANAGER ITALY & IBERIA, FORCEPOINT**

**CLICAR PARA VER EL VÍDEO**

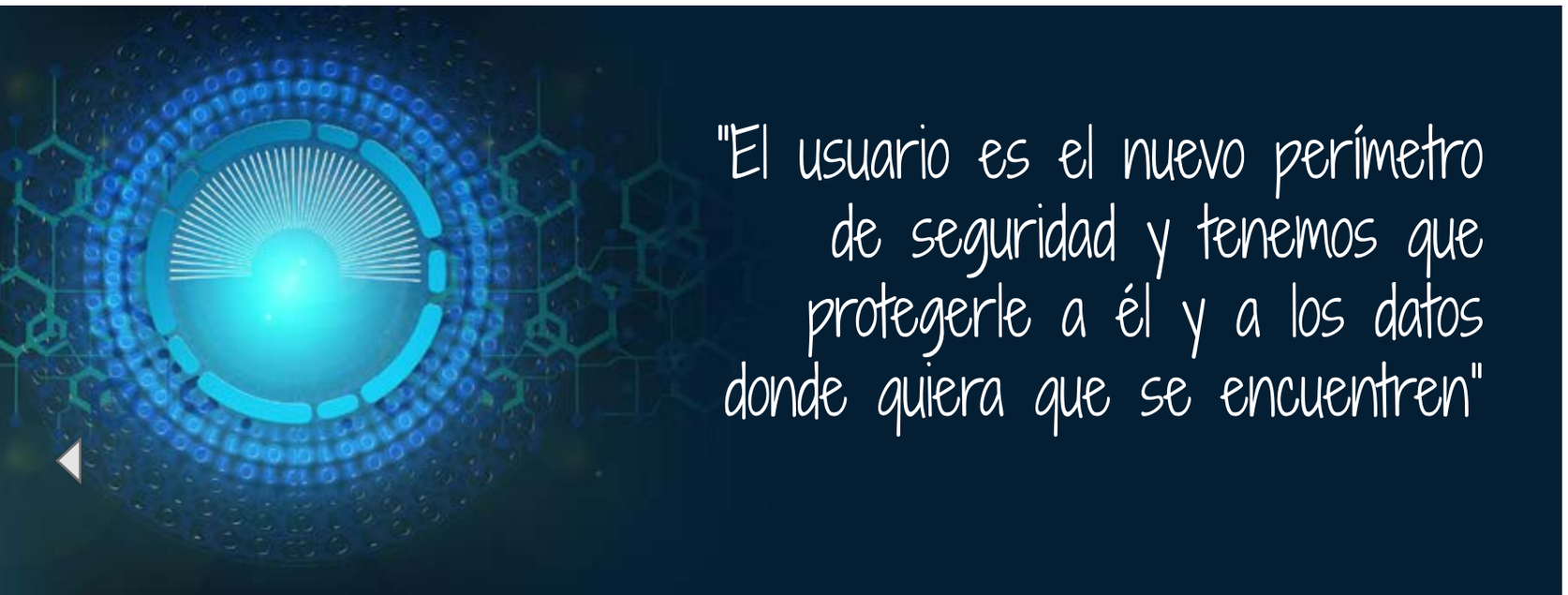



el tema de los accesos, una propuesta de DLP (Data Lost Prevention) y una oferta de protección de usuario basado en la verificación constante del comportamiento para aplicar una seguridad dinámica.

Con el objetivo de proteger los datos allá donde se encuentren, Luca Livrieri asegura que no se debe trabajar a nivel de perímetro y que una de las mejores prácticas para hacer frente a una brecha de seguridad es proteger el punto en el que los usuarios acceden a los datos, teniendo en todo momento un control sobre su comportamiento y pudiendo ofrecer una respuesta dinámica en función de este comportamiento para que la seguridad se convierta en un habilitador del negocio.

La propuesta Human Centric Cybersecurity de la compañía provee una visibilidad muy rica de la actividad del usuario para identificar y mitigar comportamientos; ofrece para las empresas de nube híbrida una protección de datos unificados y protege la red con un mejor costo-beneficio y mantiene seguro a los usuarios remotos de las ciberamenazas.

Vea aquí la intervención de Forcepoint en Brechas de Seguridad, ¿hay opciones?





La necesidad de teletrabajar ha potenciado el BYOD (Bring Your Own Device) y si bien esto permite que las personas sean más productivas, complica la seguridad cuando ésta se basa en un enfoque que asume que las personas y los dispositivos dentro de la red están implícitamente segura y a salvo. Este documento te ofrece una serie de pasos prácticos para adoptar el modelo Zero Trust, que desempeña un papel clave para permitir que las organizaciones respalden el trabajo remoto a largo plazo. implementar completamente todos los principios Zero Trust.

**Joaquín Malo de Molina, Responsable de canal, MobileIron**

# "Los códigos QR se han convertido en una creciente amenaza para los dispositivos móviles"


**JOAQUÍN MALO DE MOLINA, RESPONSABLE DE CANAL, MOBILEIRON**

**CLICAR PARA VER EL VÍDEO**

"Para los cibercriminales es el momento ideal, es la tormenta perfecta", asegura Joaquín Malo de Molina, responsable de canal e MobileIron, en la sesión online Brechas de seguridad, ¿hay opciones?, cuando le preguntamos qué es lo que está pasando en el mercado. Menciona el directivo que los hackers son cada vez mejores en lo que hacen y que las empresas suelen relegar a segundo plano la seguridad móvil "a pesar de que los empleados trabajan con estos dispositivos para acceder al correo electrónico, aplicaciones, etc.".

El phishing, circunscrito habitualmente al ordenador, también campa a sus anchas en los móviles. Existen muchos tipos de phishing, aunque todos buscan engañar al usuario para que pinche en un enlace externo que llevará a descargar malware, o ceder sus credenciales. Los móviles se han convertido en un objetivo muy atractivo para el phishing porque, según explica Joaquín Malo de Molina, el tamaño de su pantalla limita la informa-

## PROTEGIENDO LOS DATOS EN MOVIMIENTO EN DISPOSITIVOS MÓVILES

La VPN sigue siendo un componente integral para proteger todos los datos en movimiento cuando los usuarios de dispositivos móviles y PCs requieren acceso al correo electrónico, contenido y recursos de colaboración de la empresa que residen detrás de un firewall en las oficinas centrales locales o en la nube. MobileIron tiene una sólida solución de tecnología de túnel VPN para dispositivos móviles y plataformas de escritorio.


ción que puede ver el usuario; porque es difícil determinar si un SMS es auténtico o no, “y por la prácticamente imposibilidad de revisar cualquier web que el usuario vaya a visitar”. Soluciones como las de MobileIron protegen a los móviles de estas amenazas.

Además del phishing, los códigos QR se han convertido también en una creciente amenaza para los dispositivos móviles. Utilizados por la inmensa mayoría de los usuarios, escanear uno de estos códigos puede desatar una auténtica debacle de la que la mayoría de los usuarios no son conscientes. Los código QR maliciosos pueden ser utilizadas por los hackers para espiar un teléfono, realizar un pago, hacer una suplantación de identidad, coger tus contactos, etcétera.

Para hacer frente a todas las amenazas propone Miguel Malo de Molina la solución MobileIron Threat Defense (MTD), que incorpora varias capas para “proteger y corregir amenazas conocidas y de día cero en dispositivos móviles sin interacción del usuario, lo que ayuda a impulsar la adopción al 100%”, y que está integrada en la solución UEM (Unified Endpoint Management) de la compañía. Desde una consola unificada la solución permite asegurar, controlar y gestionar todas las políticas de cumplimiento de PCs, portátiles, teléfonos inteligentes, tablets, etc.

En definitiva, MobileIron Threat Defense ofrece una seguridad móvil integral que permite a las empresas monitorizar, administrar y proteger los dispositivos móviles contra ciberataques de dispositivos,

"Nuestro MobileIron Threat Defense (MTD) permite implementar protección y correción de phishing multi vectorial para todo el tráfico basado en Internet independiente del navegador"

redes y aplicaciones, y sin ninguna interacción por parte del usuario y sin interrupciones en su productividad.

Vea aquí la intervención de MobileIron en Brechas de Seguridad, ¿hay opciones?

**Juan Per, Responsable Territorial Iberia, Okta**

# "Con un doble factor de autenticación se conseguiría reducir gran parte de las brechas de seguridad"

Nueve mil clientes, más de 2.000 empleados y una facturación anual de 560 millones de dólares convierten a Okta en una de las empresas líderes del mercado de gestión de accesos e identidades (IAM), dice Juan Per, responsable territorial de Okta, en la sesión online Brechas de seguridad, ¿hay opciones?. Añade el directivo que una de las grandes ventajas de su compañía es que "somos capaces de gestionar el área tradicional en la que se han focalizado las soluciones de IAM, que son los empleados, pero también el área de lo que definimos como colaboradores necesarios", que pueden ser los proveedores, los partners, colaboradores, etc., a los que también hay que darles cierto acceso a ciertas aplicaciones o infraestructuras.

Hace tiempo que hablamos de cloud, ¿cómo ha impactado en la empresa y en todo lo que tiene que ver con la gestión de identidades? Para Juan Per, "la nube lo ha cambiado todo. Ha sido la gran revolución en el mundo IT". Explica el directivo que Okta nació  en la nube y que se está viendo


**JUAN PER, RESPONSABLE TERRITORIAL IBERIA, OKTA**

**CLICAR PARA VER EL VÍDEO**


"Para que una empresa no sufra una brecha lo que tiene que securizar es la identidad de los usuarios"

cómo sectores que antes eran reacios a migrar a la nube, como la banca o los organismos gubernamentales, están yendo al cloud en todos sus proyectos de transformación digital, y añade que la gran mayoría de los proyectos que lleva a cabo su compañía compañía son híbridos porque los clientes están en una fase de transición y aún mantienen recursos on-premise.

La identidad ha evolucionado, explica el directivo de Okta. Si hace unos años era parte de un stack y hoy se apuesta por una plataforma independiente y neutral capaz de integrarse con el resto del ecosistema de IT, a lo que se va es "a gestionar la autenticación y la identidad, no de dispositivos o personas físicas, sino de cosas, a gestionar el IoT".

Okta Identity Cloud es la solución global de gestión de identidades de la compañía, una solución que está compuesta por siete módulos o productos, a los que los clientes pueden optar de manera independiente. El primero es Okta Single-Sing On, una herramienta de sesión de inicio único; le sigue Okta Adaptative MFA, o de múltiple factor de autenticación basada en contexto; con API Access Management se securizan todas las conexiones y la creación de APIs en las empresas; Okta Directory Universal permite consolidar diferentes directorios; Life Cicle Management es la herramienta de gestión de acceso de usuarios a aplicaciones; Okta Advanced Server Access y Okta Advanced Gateway se centran en la gestión de usuarios con privilegios y en las conexiones entre infraestructura on-premise y cloud.

Vea aquí la intervención de Okta en Brechas de Seguridad, ¿hay opciones?

it whitepapers

## LA IDENTIDAD EN EL CENTRO DEL PLAN DE SEGURIDAD

En la última década, empresas de todo el mundo han adoptado aplicaciones basadas en la nube, han reducido su infraestructura informática, han disminuido sus costes de adquisición y han permitido a sus empleados trabajar a distancia en cualquier lugar del mundo y en cualquier momento, pero eso ha complicado el tener una visión general única de todos los usuarios, terminales y aplicaciones. Por lo tanto, necesitan una plataforma de identidad unificada.

**Joaquín de la Torre, Director de Desarrollo de Negocio, Sealpath**

# "La información es uno de los activos más valiosos de cualquier organización"

Siendo la información uno de los principales activos de las empresas, solo en el 2,2% de las fugas de datos la información estaba protegida de algún modo, dice Joaquín de la Torre, Director de Desarrollo de Negocio de Sealpath en la sesión online Brechas de seguridad, ¿hay opciones?, lo que quiere decir que en el 98% de los casos los ciberdelincuentes que se llevan la información de las empresas "pueden hacer con ella lo que les dé la gana".


**JOAQUÍN DE LA TORRE, DIRECTOR DE DESARROLLO DE NEGOCIO, SEALPATH**

**CLICAR PARA VER EL VÍDEO**

Recuerda Joaquín de la Torre que las fugas de datos no sólo se producen por ataques externos, sino internos, y que los ataques no se producen sólo contra gente de la organización, sino contra colaboradores "con los que compartimos información". De lo que se deduce que la información debe estar protegida "frente a las amenazas externas, pero también frente a las internas. Y también cuando sale de nuestra organización, cuando la compartimos hacia afuera".

Lo que aporta Sealpath es "una protección persistente del documento", es "ir más allá del cifrado", es "poder controlar lo que la gente puede hacer con la información, aunque esta salga de nuestra organización", explica Joaquín de la Torre. Añade el directivo que la clave de la oferta de su compañía es que la información va a ser siempre del cliente, esté donde esté, porque la información va a seguir siempre las órdenes del dueño de la información, no del dueño del dispositivo en el que está la información, "con lo cual siempre se va a mantener un

## MANTENER EL CONTROL SOBRE NUESTROS DOCUMENTOS, ¿POR QUÉ ES TAN IMPORTANTE?

SealPath te permite asignar permisos sobre los documentos de forma que sólo quien tú decidas tendrá acceso a la documentación independientemente de dónde se encuentre. También te permite poner fechas de caducidad sobre los documentos para que pasada la misma determinadas personas dejen de tener acceso a la documentación. La documentación viaja siempre con la protección y está cifrada. Es una protección persistente que sólo quien la ha aplicado puede quitar.


**Compartir en RRSS**

"Podemos hacer una auditoría completa del acceso a la información en cualquier momento, y en cualquier momento vamos a poder revocar, modificar o cambiar completamente los permisos de acceso a la misma"

control completo sobre la información sensible de la organización".

Explica también el Director de Desarrollo de Negocio de Sealpath que lo que se propone es un nuevo modelo de protección basado en círculos de confianza "donde desaparece ese anonimato, tanto del receptor como del emisor, de la información y donde se puede controlar lo que la gente pueda o no puede hacer con la información, incluso modificar o revocar completamente los permisos de acceso a la misma si alguien abandona ese círculo de confianza".

Insiste Joaquín de la Torre que con Sealpath se puede controlar qué es lo que esa persona va a poder hacer con la información y también durante cuánto tiempo, independientemente del formato. Se puede decidir que no pueda modificarla, que no pueda imprimirla, que no pueda copiar su información de una documentación nuestra y llevársela a otro sitio, impidiendo la fuga de información.

Vea aquí la intervención de Sealpath en Brechas de Seguridad, ¿hay opciones?