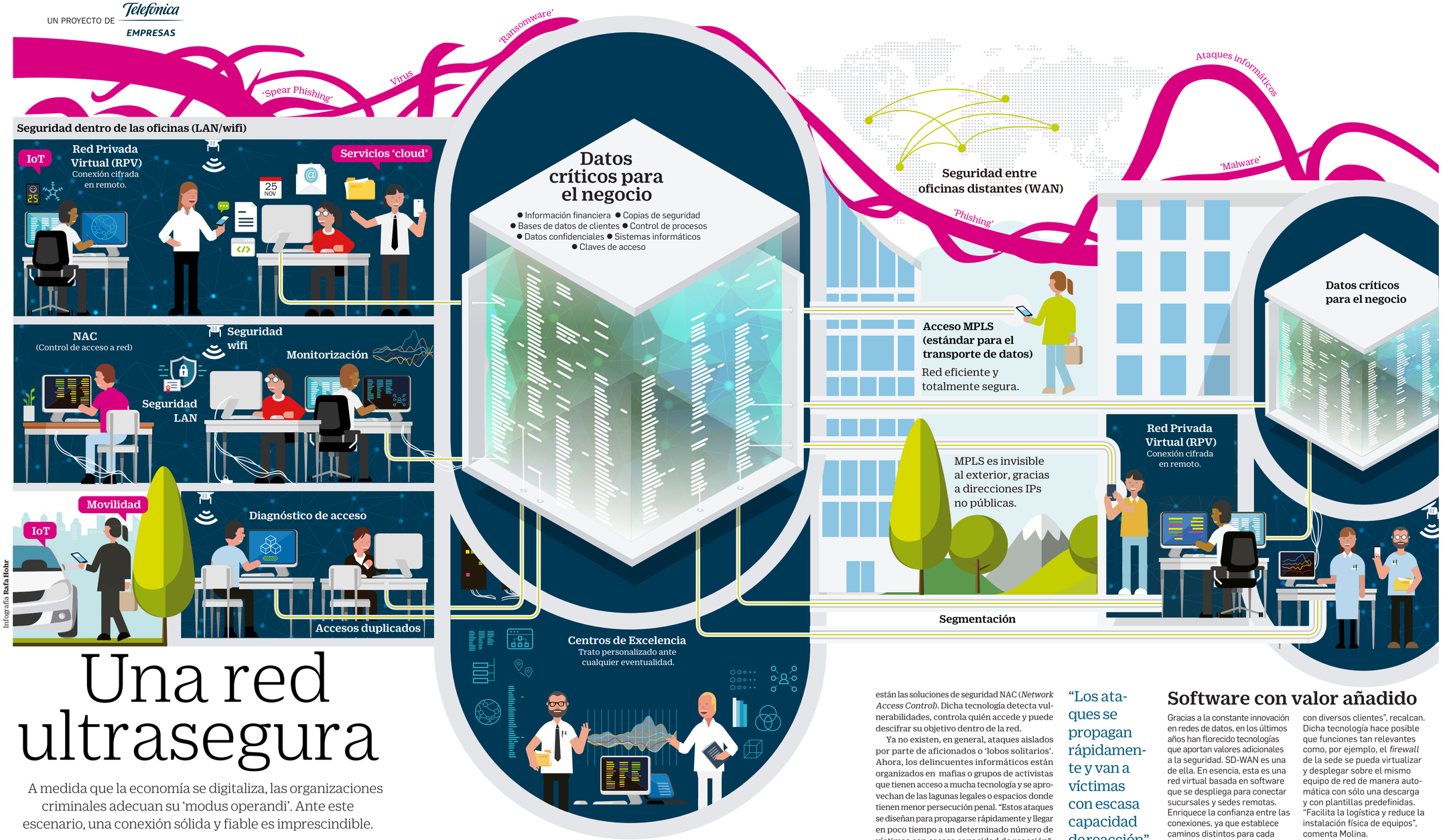


Infografía **Rafa Hohr**

# Una red ultrasegura

A medida que la economía se digitaliza, las organizaciones criminales adecuan su 'modus operandi'. Ante este escenario, una conexión sólida y fiable es imprescindible.

Nueva York, febrero de 2015. Un grupo de anarquistas informáticos logra entrar en los servidores de E Corp, un conglomerado estadounidense fabricante de dispositivos móviles y dueño de un firma financiera, el principal objetivo del ataque. Los *hackers*, bajo el nombre de Fsociety, bloquean las operaciones con tarjeta y los cajeros automáticos de todo Estados Unidos. En cuestión de minutos, el caos y el pánico se extienden por el mundo. El *status quo* de una de las grandes industrias del planeta se ha puesto en vilo.

Aunque parezca verdadero, el argumento anterior ha sido sacado de una serie de televisión: *Mr. Robot*. Lo que es una realidad es la fragilidad que tienen las redes de algunas empresas frente a la sofisticación de los ciberdelincuentes. "A medida que la economía se digitaliza y se realizan más transacciones en el ciberespacio, las organizaciones criminales adaptan su *modus operandi*", comenta Francisco José Molina, director de Ingeniería, Desarrollo de Negocio de Defensa y Seguridad en Telefónica Empresas. Hoy, la buena salud de una compañía también tiene que ver con la seguridad informática. Asegurar la continuidad de los sistemas se ha convertido en la impronta que marca el camino y el éxito del negocio, dice el experto de Telefónica Empresas. Bajo este escenario, las redes privadas virtuales (RPV) se abren paso como la mejor solución para resguardar el cúmulo de datos de una compañía. Sobre todo, la tendencia en el mercado es adoptar aquellas con tecnología MPLS (del inglés *Multiprotocol Label Switching*), un mecanismo que reduce las posibilidades de ataque y que pone énfasis en los enlaces entre las oficinas distantes (seguridad WAN).

> Energía y consumo son los sectores preferidos por los 'hackers'

"Una de sus características es que hace invisible la red hacia el exterior. Lo que no se puede ver es siempre más difícil de atacar. Esto se consigue a través de diversos mecanismos: el uso controlado de IPs privadas, la restricción de perfiles de usuario, autorizaciones de acceso y funciones de auditoría periódica", comenta Molina. Ya nadie está a salvo. Por ejemplo, el 76% de las compañías españolas ha tenido un incidente informático con consecuencias significativas en los últimos seis meses, de acuerdo con un análisis de la consultora Deloitte, publicado a mediados de este año.

Los puntos vulnerables están a flor de piel y han aumentando con el *boom* de los dispositivos móviles, el uso de la nube y la explosión del internet de las cosas (IoT, por sus siglas en inglés). Tradicionalmente, uno de los riesgos proviene de los accesos a través de una red local inalámbrica (LAN/wifi), desde fuera de la organización. La mejor forma de prevenirlo es controlando las posibles vías de infección: desde el control de los puertos físicos (por USBs, por ordenadores externos, etcétera), hasta las amenazas que provienen de la interconexión con internet. Para esto último existen herramientas de bloqueo o filtrado de navegación que nos permiten impedir la descarga y propagación de software malicioso o el acceso a campañas de *phishing*. También están las soluciones de seguridad NAC (*Network Access Control*). Dicha tecnología detecta vulnerabilidades, controla quién accede y puede descifrar su objetivo dentro de la red.

Ya no existen, en general, ataques aislados por parte de aficionados o 'lobos solitarios'. Ahora, los delincuentes informáticos están organizados en mafias o grupos de activistas que tienen acceso a mucha tecnología y se aprovechan de las lagunas legales o espacios donde tienen menor persecución penal. "Estos ataques se diseñan para propagarse rápidamente y llegar en poco tiempo a un determinado número de víctimas con escasa capacidad de reacción", destaca el experto de Telefónica Empresas.

El impacto económico puede ser importante. Al menos entre las empresas que facturan entre 2.000 y 5.000 millones de euros, que son las que experimentan un mayor número de incidentes al año, prácticamente cuatro al año, según Deloitte. Entre los sectores con más incidencias están el de energía y recursos, así como el de consumo y distribución, de acuerdo con el análisis. El coste del cibercrimen para el planeta asciende a unos 600.000 millones de dólares o, lo que es lo mismo, el 0,8% del PIB global, de acuerdo con un análisis de McAfee y el CSIS (*Centre for Strategic and International Studies*).

"Hay muchos tipos de impacto, no solo el económico, también el reputacional. Por eso, la seguridad de las redes debe ser un tema dentro de la agenda de cualquier empresario, gestor público o gerente", concluye el experto de Telefónica Empresas.

> "Los ataques se propagan rápidamente y van a víctimas con escasa capacidad de reacción"

**600.000**
millones de dólares es el coste del cibercrimen en el mundo, que equivale al 0,8% de PIB global.

**76%**
de las firmas españolas ha tenido un incidente con consecuencias significativas en los últimos seis meses.

## Software con valor añadido

Gracias a la constante innovación en redes de datos, en los últimos años han florecido tecnologías que aportan valores adicionales a la seguridad. SD-WAN es una de ella. En esencia, esta es una red virtual basada en software que se despliega para conectar sucursales y sedes remotas. Enriquece la confianza entre las conexiones, ya que establece caminos distintos para cada tipo de tráfico. Con esta herramienta es posible reconfigurar la seguridad en tiempo real, adecuándose a las diferentes situaciones que pueden producirse: picos de carga de trabajo, ataques dirigidos, etcétera.

"SD-WAN abre un mundo de nuevas posibilidades", dice Francisco José Molina, director de Ingeniería, Desarrollo de Negocio de Defensa y Seguridad en Telefónica Empresas. Su futuro es prometedor. El SD-WAN es un mercado que va a crecer en torno al 50% en los próximos años, de acuerdo con los expertos de Telefónica Empresas, que llevan tres años trabajando con esta tecnología. "En Europa ya tenemos por delante más de 10.000 sedes comprometidas con diversos clientes", recalcan. Dicha tecnología hace posible que funciones tan relevantes como, por ejemplo, el *firewall* de la sede se pueda virtualizar y desplegar sobre el mismo equipo de red de manera automática con sólo una descarga y con plantillas predefinidas. "Facilita la logística y reduce la instalación física de equipos", comenta Molina.

La flexibilidad que ofrecen las 'funciones de red virtualizada' (NFV, por sus siglas en inglés) evita la dependencia de un único proveedor de software. "El cliente tiene alternativas en la misma categoría de producto, cuenta con la posibilidad de migrar de uno a otro, testear y calibrar diferentes tecnologías", añade el especialista.

Desde el punto de vista financiero, agrega el experto, la contratación de las NFV, como un servicio de valor añadido y no como un activo, cambia la naturaleza de los gastos de capital (*capex*) a gastos operativos (*opex*). "De esta manera se liberan fondos para invertir en la actividad principal del negocio", finaliza.

UN PROYECTO DE Telefónica EMPRESAS

**OPINIÓN**

## La seguridad del negocio empieza con la conectividad

**Andrés López Hedoire**
*Director de Marketing de Producto de Telefónica Empresas*

En las empresas los datos lo son todo y el primer paso es garantizar la seguridad de la información desde la red. Para lograrlo es fundamental asegurar su intercambio, su integridad y su uso autorizado. Esto implica supervisar las comunicaciones dentro y fuera de las oficinas y, por supuesto, con la cada vez más extendida *cloud*. Igualmente relevante es la gestión a nivel global de toda esta conectividad.

Si hablamos de las comunicaciones entre las oficinas, ese intercambio de datos seguro se realiza utilizando redes privadas virtuales para cada cliente. Estas cuentan con diversas medidas para garantizar su seguridad. Técnicamente destaca que las redes privadas no son visibles desde el exterior y, por tanto, no son atacables. Además, a nivel de servicio ofrecen mejores prestaciones: garantizan el caudal, aseguran la calidad (mejor experiencia del usuario) y tienen retardos menores, entre otras.

**Pero la seguridad va más allá del acceso.** Vivimos en un mundo donde los datos que pasan por la red crecen un 40% cada dos años. Los negocios viven momentos clave como el comienzo de las rebajas online o la retransmisión de un partido de final de Champions donde el éxito depende de que no falle la conectividad. Todo esto hace necesario cambiar radicalmente las redes, la forma de diseñarlas y las tecnologías que necesitamos emplear, como ya hemos hecho con el proyecto de Red Fusión en Telefónica. Gracias a esta red, completamente renovada y en alta disponibilidad, es posible asumir crecimientos exponenciales de tráfico y garantizar la continuidad de los negocios ante cualquier evento.

Finalmente es importante destacar que, además de tener la mejor tecnología en la conectividad, es fundamental contar con una gestión que tenga visión global del negocio, tanto de la red como de la seguridad. En Telefónica Empresas disponemos de un modelo de gestión personalizado a través de nuestros Centros de Excelencia donde ponemos a disposición de los clientes un único punto de contacto con atención personalizada y un equipo de seguridad con más de 400 expertos en las tecnologías líderes del mercado.

Por todo lo anterior, desde Telefónica Empresas tenemos claro que la seguridad empieza en la conectividad y por tanto llevamos las soluciones más robustas y seguras a todos nuestros clientes.