



Aitor  
Jerez

Director de Ventas de  
la zona Norte de Sarenet

# “Queremos que los administradores de TI puedan centrarse en lo que aporte valor a su negocio”

## ¿Qué productos de tecnología les demandan en mayor medida las organizaciones para lograr ser más competitivos?

**Las soluciones de voz** por la búsqueda de nuevas fórmulas que permitan a la organización sacar mayor partido a sus recursos y el ahorro. **Las comunicaciones de datos** de alta capacidad y cuando haya varios centros, VPN con conexiones que les permitan utilizarlas simultáneamente para voz y datos buscando el ahorro y la simplificación en la gestión de cortafuegos y *routers*. Y los **servicios de data center**. En este último punto, aunque cada vez se ven más planteamientos de pago por uso, aún estamos lejos de estas aspiraciones y nos encontramos con escenarios mixtos.

Las empresas quieren desentenderse de lo que no les aporta valor, y al traer a nuestro *data center* sus equipos disfrutan de servicios de suministro eléctrico y refrigeración difícilmente replicables en sus centros. Las comunicaciones adquieren un carácter crítico, siendo necesario tener acceso constante a sus servidores. En este aspecto desde Sarenet aportamos nuestra experiencia ofreciendo enlaces redundados.

La siguiente servidumbre de la que se quiere liberar una empresa tiene que ver con la propiedad del hardware y su corto ciclo de vida. Empiezan externalizando sus servidores a la nube contratando infraestructura como servicio. En este estadio, al margen de adaptar las aplicaciones a su negocio, aún se ven en la obligación

de mantener la plataforma (parches del sistema operativo y de las aplicaciones que utiliza), los complementos necesarios para securizarla (cortafuegos de aplicaciones o tradicionales) y los relacionados con la pérdida de información (*back-ups*). Con el tiempo, estos complementos nos los terminan subcontratando.

Sin embargo, existen dos formas de prestar servicios a las organizaciones que les permiten centrarse aún más en su propio negocio. Son aquellas en las que la empresa se limita a gestionar la aplicación, en modelos de pago por uso.

Uno de nuestros puntos fuertes es que ofrecemos un ecosistema en el que una empresa puede abordar sin prisas y por fases la externalización de sus servidores, en todos los estadios antes mencionados.

## ¿Qué papel juegan las comunicaciones en la nueva era *Cloud*? ¿Qué soluciones forman parte de su portfolio?

Diferenciamos entre proyectos *cloud* orientados al acceso a los mismos desde Internet (portales o tiendas *online*), y los que consisten en la externalización de los servidores internos de una empresa. En el primer caso lo más importante es el ancho de banda asignado al servidor virtual y la calidad del mismo. La conexión, la garantizamos estando presente en los principales puntos neutros de intercambio (EspaNIX, AMSIX, CatNIX) en los que nos conectamos directamente con todos los allí presentes.

La externalización de los servidores internos de una empresa transforma en críticas las comunicaciones. Hay dos factores que se deben tener en cuenta. El primero es obvio, ya que de nada nos sirve garantizar que los servidores tienen alimentación y se encuentran refrigerados, si no podemos llegar a ellos desde nuestras instalaciones. Ofrecemos enlaces con respaldo automático con tecnologías de acceso diferentes y configurados en modo activo-pasivo o activo-activo. El otro factor, tiene que ver con la calidad con la que llegamos a estos servidores. Nuestro portfolio actual cubre las comunicaciones y los servicios *cloud* permitiéndonos con-



**Juan José Rey**  
DIRECTOR DE VENTAS PARA LA ZONA CENTRO DE SARENET

trolar todo el recorrido de ese flujo de datos. Dentro de nuestras VPN, podemos priorizar el tráfico de negocio y siguiendo nuestra máxima de transparencia, damos al cliente acceso a la visualización en tiempo real de este flujo.

### ¿Qué valor pueden aportar a los administradores de TI de las compañías?

Queremos que los administradores de TI puedan centrarse en lo que aporte valor a su negocio. Les ayudamos en el diseño de la solución que más les conviene desde una visión global. Las dimensiones de nuestra empresa también les permiten abordar proyectos de cierta envergadura contando con un

compañero de viaje muy ágil y accesible, dos de las cualidades más valoradas por nuestros clientes. Y por último, y lo que siempre nos ha diferenciado, les ofrecemos un soporte técnico impecable al que acudir cuando los problemas aparecen sin prácticamente rotaciones de personal.

### Por último, ¿qué tipo de seguridad están ofreciendo a sus clientes?

Ofrecemos seguridad transversal. Actualmente, sólo las organizaciones de cierto tamaño se pueden permitir disponer de personal especializado en seguridad, por este motivo, no solo ofrecemos los mecanismos para garantizar la seguridad, también

debemos configurarlos adaptados al cliente y actuar en caso de que se produzca un problema, hablamos de "seguridad gestionada".

Somos uno de los principales *partners* en España de Fortinet. Esto nos obliga a tener a nuestro personal certificado por el fabricante, actualizando constantemente sus conocimientos del producto.

Para cubrir la necesidad de proteger aplicaciones alojadas en servidores de nuestra nube, hemos desarrollado un cortafuegos propio que también incluye funcionalidades de balanceo y caché. Con este servicio minimizamos el riesgo que suponen los agujeros de seguridad de los CMS más populares.

Los ataques de denegación de servicio son muy difíciles de paliar, cuando se detecta uno podemos cortar el servicio para protegerlo pero supone facilitar al atacante su objetivo final. La detección y el corte, generalmente se realiza en dispositivos que tienen que colocarse interceptando el tráfico a la red o el servidor que se protege. Esto generalmente es un cuello de botella por el caudal que es canalizado a través de este punto. Entendíamos que la solución venía por controlar el tráfico en la frontera del proveedor por eso hemos desarrollado una herramienta innovadora que permite al cliente instalar filtros temporales en nuestros *routers* de frontera para proteger su servicio durante el ataque. **CW**