# De la continuidad de negocio a la resiliencia segura

Diciembre 2020

# De la continuidad de negocio a la resiliencia segura

**2020 se ha convertido en el año que ha puesto a prueba la resiliencia empresarial. Conectar gente, asegurar los negocios y automatizar procesos, a veces de manera urgente y en ocasiones de manera diferente, son las claves de la resiliencia empresarial, tan necesaria para mantener el negocio a pleno rendimiento.**

Cisco es un testigo de excepción para hablar de lo que ha ocurrido durante la pandemia. Como proveedor de soluciones de colaboración, la compañía ha podido ver el crecimiento que se producido en relación con este tipo de herramientas y los problemas de seguridad que han generado algunas de ellas. Durante un encuentro con varios responsables de ciberseguridad, recordaba Eutimio Fernández, Director de Ciber-seguridad de Cisco España, que la compañía también es experta en el tema de comunicaciones y "también somos proveedores de una arquitectura muy amplia de ciberseguridad", lo que le permite estar muy involucrado en las necesidades de los clientes.

La experiencia durante la pandemia lleva a Eutimio Fernandez a decir que no estábamos preparados y que "nos está obligando a cambiar la forma de hacer IT"; sobre la situación de la ciberseguridad durante los primeros meses de este año dice el director de Ciber-seguridad de Cisco España que si bien no ha habido innovación en los ataques, sí que ha habido un gran incremento.

"Desde el punto de vista de tecnología y de ciberseguridad está siendo un momento muy entretenido", apuntaba el directivo. Los negocios se redefinen por los cambios de hoy y por las incertidumbres del futuro. Cambios e incertidumbres que establecen nuevas prioridades, como empoderar a los empleados para que trabajen desde cualquier sitio y con cualquier dispositivo, pero de una mane-


**DE LA CONTINUIDAD DE NEGOCIO A LA RESILIENCIA SEGURA. CONCLUSIONES**

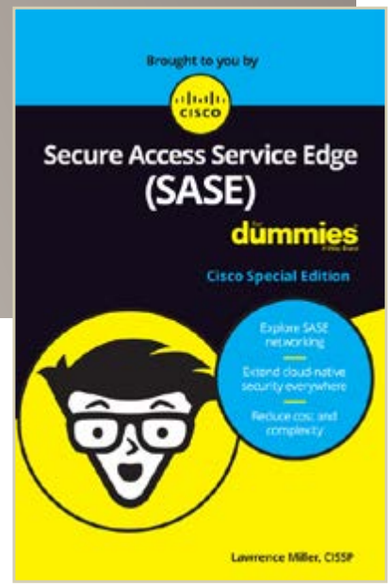
**CLICAR PARA VER EL VÍDEO**

ra segura, de forma que el rendimiento empresarial llegue al hogar.

¿Cuáles han sido los retos a los que se han enfrentado los responsables de ciberseguridad de las empresas?, ¿qué se ha aprendido de la pandemia?, ¿cómo se ha afrontado la aceleración de la transformación digital vista en los últimos meses? Estas son algunas de las preguntas que se han debatido en un Encuentro ITDS patrocinado por Cisco y en el que han participado Jesus Alonso Murillo, CISO de Ferrovial Servicios; Mónica de la Huerga, CISO de Sopra Steria; Josep Bardallo, CISO del Grupo Recoletas; Carlos Manchado CISM CISSP, CISO de Naturgy; Jorge Arrufat Tejera, Head of Security de BBVA Next Technologies; Ruben Fernandez Nieto, CISO de DIA Group y Eutimio Fernández García-Donas, Director de Ciber-seguridad en Cisco España.

## SASE PARA DUMMIES, BY CISCO

Los equipos de TI de hoy se enfrentan a un desafío común: cómo habilitar de forma segura el creciente universo de usuarios, dispositivos y aplicaciones SaaS sin agregar complejidad o reducir el rendimiento del usuario final, todo ello mientras aprovechan sus inversiones de seguridad existentes. Este libro examina el panorama cambiante de la red y la seguridad, y los pasos que puede tomar para mantener su organización segura y protegida a medida que evoluciona su red.



# LA VISIÓN DE LA INDUSTRIA IT

**Jesús Alonso, CISO, Ferrovial Servicios**

## "Nos hemos dado cuenta de que la tecnología existe"

Jesús Alonso, CISO, Ferrovial Servicios

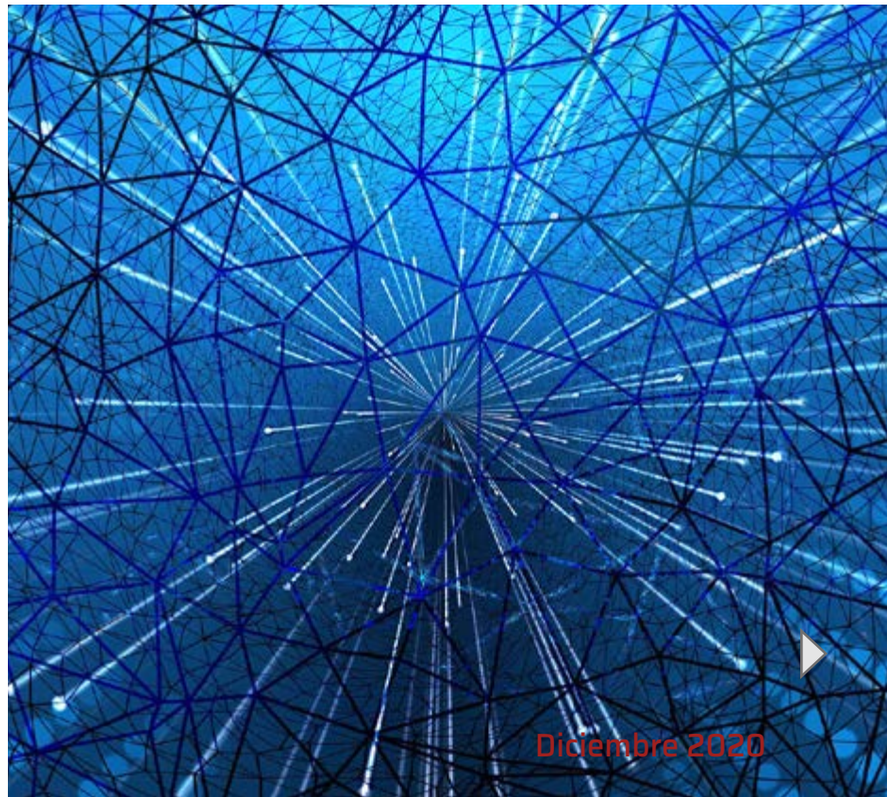
Explicando que en Ferrovial Servicios, donde ocupa el puesto de CISO, se ofrecen diferentes servicios, algunos públicos y de especial criticidad, como servicios de IT y todo lo que tiene que ver con seguridad en Hospitales, explicaba Jesús Alonso que uno de los retos a los que se ha tenido que enfrentar este año de pandemia ha sido el enviar a los empleados a casa a trabajar, que si bien es un reto per se, se complica cuando el que se ve afectado es un call center. "Nos hemos dado cuenta de que la tecnología existe, que permite establecer las conexiones de forma segura, el problema ha sido hacerlo de una manera excesivamente rápida", dice Jesús Alonso.

No hay mal que por bien no venga, porque lo que está ocurriendo es que las nuevas licitaciones o proyectos que se están viendo ahora ya incluyen el tema del acceso seguro de empleados remotos, lo que permite "desde el inicio, establecer los procesos para poder trabajar de una manera más segura".

"Hemos aprendido de la pandemia es que se pueden seguir operando y trabajando desde casa, o desde donde queramos, con tal de que tengamos una conexión medianamente razonable", dice el CISO de Ferrovial. Hace años que se habla de la pérdida de perímetro, y la pandemia ha terminado por eliminarlo definitivamente.

El objetivo ahora es "proteger el dato, la información, y cómo se accede a esa información". Ahora bien, este un binomio del dato y la autenticación, a lo que hay que añadir la trazabilidad y comportamiento del usuario, "no se puede aplicar absolutamente a todo porque podemos paralizar ciertos procesos, ciertos proyectos, ciertos servicios", dice Jesús Alonso. Asegura el directivo que hay que centrarse en el dato que de verdad sea importante, que de verdad sea crítico; "hay que intentar decidir qué es crítico y quitar el grano de la paja" y apostar por modelos SASE.

Durante su intervención Jesús Alonso decía también que en plena transformación digital, acelerada durante la pandemia sanitaria, "hay que alejarse un poco de hierro para externalizar cosas, e irnos al cloud, a un concepto de seguridad como servicio".



**Carlos Manchado, CISO, Naturgy**

# "La movilidad del endpoint no es algo trivial"

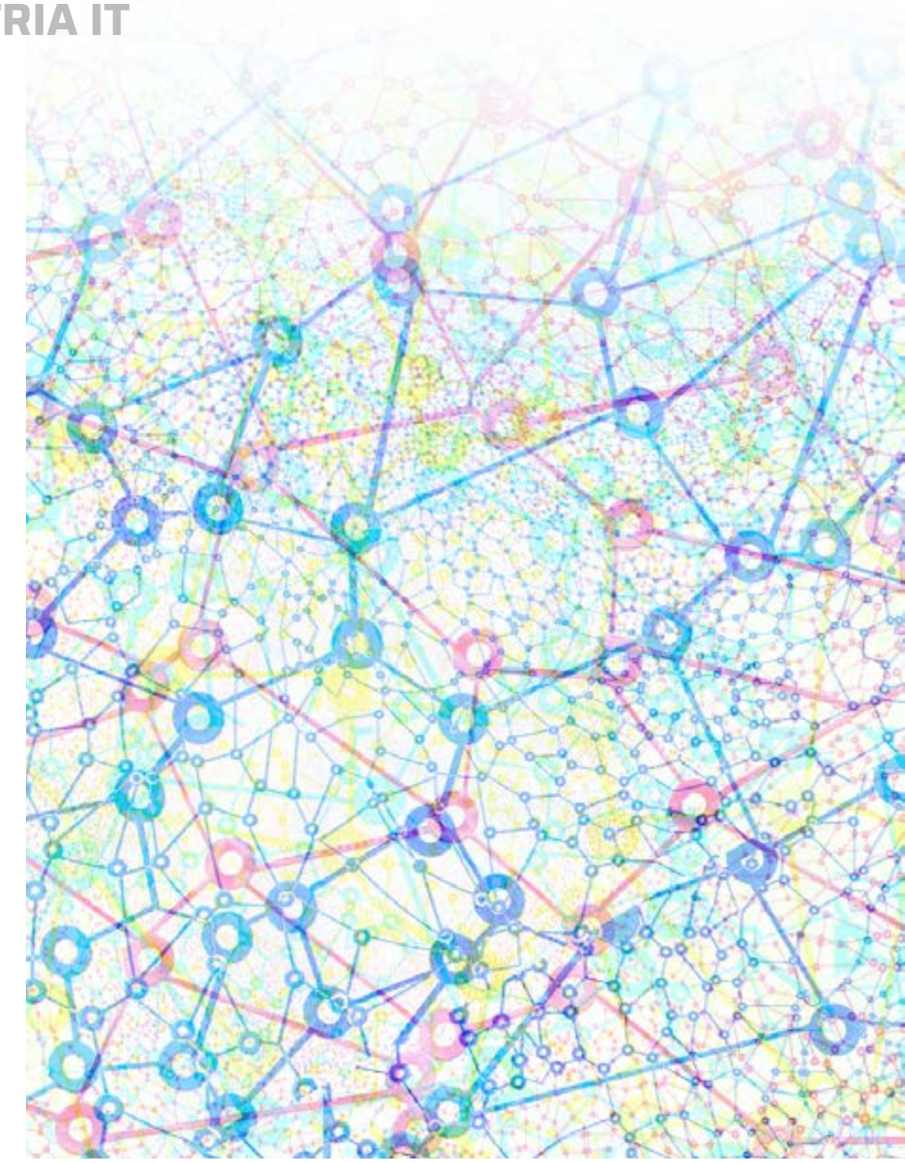
## Carlos Manchado, CISO, Naturgy

Ser una empresa de servicios esenciales y sometida a la Ley de Infraestructuras críticas llevó a Naturgy a trabajar con cuidado y contrarreloj para poder establecer una arquitectura que de manera segura permitiese conectar de forma remota con las instalaciones, explica Carlos Manchado, CISO de esta compañía, mencionando el primer reto al que tuvo que enfrentarse en los primeros momentos de pandemia.  Otro de los grandes desafíos ha sido "tener equipos que habitualmente estaban bajo el perímetro y bien custodiados y parcheados y pasar a gestionar equipos que no están en ese perímetro, que a veces son personales y que se conectan desde redes domésticas que no ofrecen ninguna garantía", explicaba el directivo.

Mientras que algunas empresas tenían experiencia en la movilidad del endpoint, en otras empresas o sectores "esto no era trivial", dice Carlos Manchado cuando se le pregunta por las lecciones aprendidas durante la pandemia. "Hemos aprendido a que no es lo mismo tener un equipo de sobremesa detrás de un perímetro que no es que se haya difuminado, es que ha saltado por los aires, por mucho que se hubiera hablado del tema", explica el CISO de Naturgy añadiendo que "también te das cuenta de que las VPN están muy bien a nivel IT y para un primer momento, pero que tienen muchos riesgos".

Añade el directivo un tercer aprendizaje: "las grandes suites de colaboración y compartición nos han hecho un gran favor, pero tienen unos riesgos terribles porque ninguna está securizada desde el comienzo".

Una de las formas de afrontar el perímetro es con concienciación, algo que para Carlos Manchado es clave pero que "no es tan fácil como montar un appliance o hacer una integración de tecnologías. La formación de los empleados es un tema mucho más costoso". Si nos centramos en el tema tecnológico "tenemos que cambiar el paradigma totalmente," dice el CISO de Naturgy poniendo sobre la mesa los conceptos Zero Trust y SASE y asegurando que en su compañía se tiene claro que es hacia estos paradigmas hacia donde hay que ir; "creo que tiene que haber un elemento central por el que en todas las conexiones, ya sea en terceros y de personal interno o externo, se apliquen los mismos controles".



**Jorge Arrufat, Head of Security, BBVA Next Technologies**

El reto, o retos, a los que se han enfrentado los responsables de ciberseguridad durante este año de pandemia "va muy en línea con el punto en el que te encuentres de tu transformación digital", dice Jorge Arrufat, Head of Security de BBVA Next Technologies. Añade el directivo que la pérdida de perímetro ha hecho que la confianza se haya tenido que reevaluar y que el mayor beneficio de la pandemia ha sido su impulso en la transformación digital de las empresas, un impulso que en muchos casos no se ha visto acompañado de seguridad.

"De la pandemia hemos aprendido que esto no va de comprar una solución y darle a un botón, sino de plantear una estrategia de seguridad para que todo nazca seguro", dice Jorge Arrufat. De los empleados siempre se ha dicho que son el eslabón más débil porque están en el otro lado de ese túnel que les permite acceder a la información y al dato, y durante este año también se ha aprendido que estos usuarios "tienen que entender esos riesgos de seguridad, y no sólo sobre el papel"

"Esto no va de comprar una solución y darle a un botón"

Jorge Arrufat, Head of Security, BBVA Next Technologies

Para Jorge Arrufat, la identidad es clave. Dice el Head of Security de BBVA Next Tehnologies que una vez que el perímetro ha desaparecido, igual ocurre con la confianza, que ha de re-evaluarse siempre para cada identidad, tanto de humanos como de dispositivos, así como de los sistemas de información". Es lo que persigue Zero Trust, una filosofía que no es nueva y que requiere de unas tecnologías para poder hacerse realidad; "ahí la clave está en que todas las tecnologías se hablen y se complementen, que sepamos sacar provecho de ellas". Menciona de manera específica las técnicas de inteligencia artificial "que nos pueden ayudar a analizar el comportamiento de la identidad o el comportamiento del usuario en el acceso a estos datos".

**Josep Bardallo, CISO, Grupo Hospitalario Recoletas**

"Estar preparados para la contingencia de las personas" es uno de los retos a los que se ha enfrentado Josep Bardallo, CISO del Grupo Hospitalario Recoletas. Con 22 centros hospitalarios, los planes de contingencia de la compañía estaban preparados para los sistemas, "pero no para que un médico se ponga enfermo, esté en su casa y tenga que dar servicio". En apenas unos días se puso sobre la mesa cómo acelerar todos los proyectos de transformación digital, que en el caso de Grupo Recoletas eran proyectos de telemedicina.

Otro gran reto que no estaba contemplado fue el de las integraciones: "todos los hospitales privados

## "Se apuesta por todo tipo de tecnologías que ayuden a garantizar quien está accediendo al dato"

Josep Bardallo, CISO, Grupo Hospitalario Recoletas

se tuvieron que integrar con la sanidad pública, y desde el punto de vista de la seguridad es una pesadilla".

"Básicamente nosotros lo que hemos aprendido es que desde seguridad tenemos que trabajar asumiendo riesgos y en silencio", dice Josep Bardallo, explicando que durante los últimos meses se han tenido que dar soluciones e implementar tecnologías "pero sin molestar al usuario y sin dejar de dar servicio".

Durante la pandemia sanitaria ha quedado claro que la nueva situación de telemedicina y el tener que abrir los sistemas a terceros ha obligado a poner herramientas de visibilidad y control "alrededor de nuestros datos sanitarios para ver por dónde llegan, como protegerlos, etc.".

Poniendo el perímetro en el dato, y siendo los datos que gestiona extremadamente sensibles, dice Josep Bardallo que se apuesta por "todo lo que sean tecnologías para identificar correctamente a la persona que acceda a los datos para protegerlos, temas de reconocimiento por patrones o temas de comportamientos inusuales (UEBA). En definitiva, se apuesta por todo tipo de tecnologías que ayuden a garantizar quien está accediendo al dato".

**Mónica de la Huerga, CISO, Sopra Steria**

"Dar soluciones de continuidad a nuestros clientes y sobre todo acelerar los procesos en los cuales estábamos trabajando con ellos", es el principal reto al que se tuvieron que enfrentar en Sopra Steria ante el contexto generado por la pandemia. Para Mónica de la Huerga, CISO de esta empresa, también supuso un reto la pérdida de perímetro y de control al tiempo que mantenían los servicios y los niveles de seguridad.

Sobre lo aprendido en la pandemia menciona Mónica de la Huerga varias cosas. Por un lado los CISO han ganado visibilidad a nivel de las empresas; "la seguridad tiene que estar ahí, sigue siendo una pieza clave y fundamental". Al mismo tiempo "hemos aprendido con la pandemia que no somos ni invencibles ni inmortales" y que puede haber flexibilidad en la tarea de un responsable de ciberseguridad, "que somos capaces de plantear alternativas, que gustan más o gustan menos, lógicamente, pero que sí, que tenemos esa capacidad de improvisación, de innovación, que al final es lo que necesita la compañía". Añade la CISO de Sopra Steria que nada está escrito y "hay que evolucionar, hay que adaptarse al ambiente, hay que tener en cuenta los nuevos riesgos, como por ejemplo el riesgo de pandemia".

En un mundo sin perímetro coincide Mónica de la Huerga en que es igual de importante proteger el dato, y, lógicamente, controlar quién puede acceder y cómo puede acceder al mismo. El problema,

## "Nada está escrito, hay que evolucionar y adaptarse al ambiente"

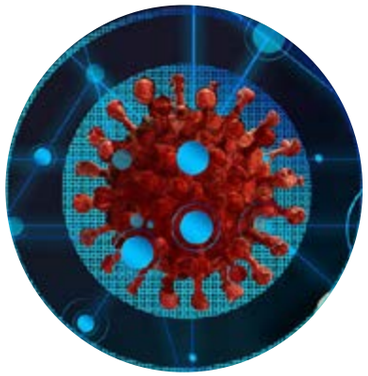
Mónica de la Huerga, CISO, Sopra Steria

añade la CISO de Sopra Steria, ya no es sólo que la seguridad perimetral haya desaparecido, sino que se ha fundido con el perímetro personal y del ámbito del domicilio de cada uno, “lo cual lo hace todavía más difícil de gestionar”. Cree que, al final, el foco sigue siendo “concienciar a los usuarios, ya no sólo a nuestros trabajadores, sino a la sociedad en general, de la importancia del dato, de la importancia de las conexiones, de la importancia de tener bien configurados nuestros equipos…”.

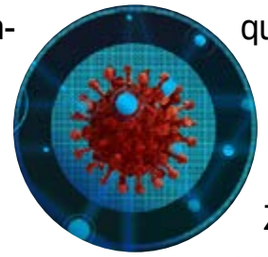
**Rubén Fernández, CISO, Grupo Dia**

Para Rubén Fernández, CISO de Grupo DIA, las empresas sí que estaban preparadas para las diferentes situaciones que se generaron durante la pandemia, “lo que no estábamos es dimensionados”. En caso del teletrabajo, estaba pensado para el 20% de la plantilla, pero en pocos días el 100% de las personas tiene que tener la capacidad de teletrabajar, “y obviamente hay que dimensionar de una manera correcta esta nueva situación”.

## "La pandemia ha provocado un cambio más cultural que de seguridad"



Rubén Fernández, CISO, Grupo Dia



Sí está de acuerdo es que se ha acelerado mucho la transformación digital y que el principal reto en ese sentido es acompañar correctamente esta aceleración que tenemos en el proceso de digitalización de las empresas con las opciones de seguridad que consideramos que son necesarias.

La pandemia ha provocado “un cambio más cultural que de seguridad”, dice Rubén Fernández. Hace referencia al teletrabajo, que muchas más empresas de las que estarían dispuestas a reconocerlo no veían con buenos ojos, un teletrabajo que se disfrutaba como un privilegio y que ahora es necesario para evitar contagios.

Además, la pandemia ha enseñado que “tenemos que reforzar mucho la parte de concienciación y la seguridad de los endpoints”, entre otras cosas porque al no estar en la oficina impactan en temas como la política de parcheo.

Afrontar un mundo sin perímetro de seguridad pasa por enfocarnos en modelos Zero Trust, en patrones de comportamiento, en herramientas tipo EDR que no se fijan tanto en firmas, o en herramientas de monitorización basadas en el comportamiento de un usuario, dice el CISO de Grupo DIA. Insiste Rubén Fernández en que “deberíamos utilizar más ese tipo de herramientas para intentar identificar patrones anómalos y posibles compromisos, tanto a nivel aplicación como a nivel de usuario porque ya no tenemos al empleado en la oficina”.

LA VISIÓN DE CISCO

# “Hay que cambiar la forma de hacer IT para dar soporte al teletrabajo y que éste sea seguro”

PROPUESTA TECNOLÓGICA CISCO SEGURIDAD

CLICAR PARA VER EL VÍDEO

No se sorprende Eutimio Fernández, Director de Ciber-seguridad de Cisco España, por ninguna de los retos que han planteado los seis CISO invitados al debate. Coincide con que la tecnología está, pero que no se estaba utilizando “pensando en que mis trabajadores son ahora tele-trabajadores”. El siguiente paso después de los primeros meses de pandemia ha sido empezar a pensar en cómo rehacer la IT antes de que llegue una tercera oleada, para lo que se ponen sobre la mesa conceptos como Zero Trust que faciliten que el teletrabajo esporádico sea algo habitual o que un PC se gestione de la misma manera estando fuera o dentro de la red.

De la pandemia “hemos aprendido de las experiencias de todos vosotros”, decía Eutimio Fernández a los CISOs participantes en un debate que, según el directivo, ponía sobre la mesa que la VPN no es el futuro porque “al menos para lo que son conexiones de usuarios hacia la compañía es inmanejable”; que se ha producido un cambio cultural que lleva a la adopción de la nube “porque es lo que me permite tener acceso desde cualquier sitio”; que la protección tiene que estar en el dato teniendo en cuenta que “en entornos cloud el dato es responsabilidad del cliente, no del proveedor de la aplicación”; o que realmente el perímetro de seguridad “está en la propia identidad”.

Teniendo en cuenta que la seguridad del dato y la identidad se han vuelto cruciales, y que la estrategia a la hora se securizar puede ser prácticamente la misma pensando que el trabajador puede estar en cualquier parte; “la idea es conseguir que plataformemos una vez, que nuestras medidas de se-

guridad sean lo más transparentes posibles y que la experiencia de usuario sea la misma esté donde esté".

Durante el debate surgen de manera recurrente conceptos como Zero Trust o SASE, modelos que en la empresa española han tenido una "aceleración muy fuerte", ya que prácticamente todas las compañías con las que se está hablando "están moviéndose a entornos SASE".

**Propuesta tecnológica**

Sobre la propuesta tecnológica de la compañía, explica Eutimio Fernandez en el vídeo, que está muy alineada con las necesidades que están demandando las empresas y que se ha "realizado una fuerte inversión en el modelo SASE", que ha evolucionado desde Cisco Umbrela.

La compañía ofrece, desde la nube, protección DNS, "que es la primera línea de defensa", así como firewall, proxy, DLP, CASB… y con un modelo bajo servicio. Se añade toda la estrategia SD-WAN de Cisco para ofrecer "una solución SASE que puede ir a todo tipo de cliente".

Desde el punto de vista de Zero Trust, explica Eutimio Fernández que gracias a una arquitectura que "es la más amplia del mercado" se garantizar una implementación de Zero Trust en todo tipo de entorno: Zero Trust para usuario remoto, Zero Trust para entorno de oficina y Zero Trust para entorno de Datacenter.

De esta forma, "desde el punto de vista de SASE y desde el punto de vista de Zero Trust tenemos arquitecturas completas para implementar en todo tipo de compañías"

"Se ha producido un cambio cultural que lleva a la adopción de la nube porque es lo que me permite tener acceso desde cualquier sitio"