FORO TAI
grupotai

Revista digital

FORO TAI

CIBERSEGURIDAD TIC

- ✓ Conoce a los patrocinadores
- ✓ Descubre todo el contenido
- ✓ Accede a los vídeos
- ✓ Todo a un *click*

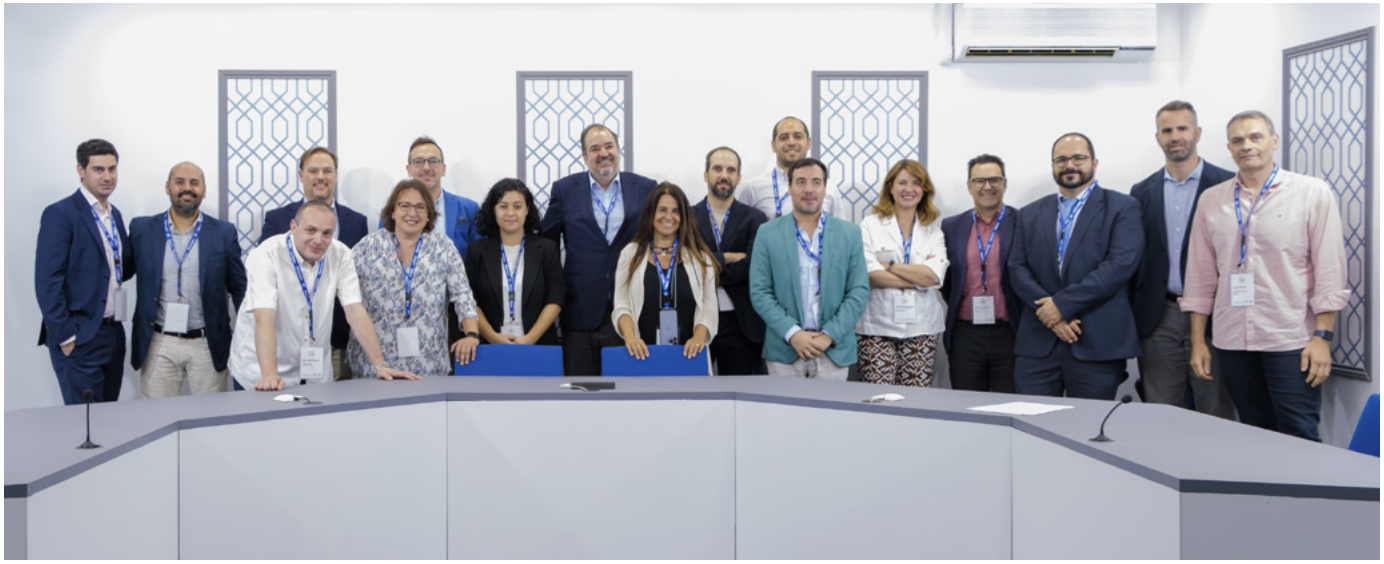
"Innovación disruptiva en ciberseguridad"

BeDisruptive · ENTHEC · SONICWALL · SOPHOS · WatchGuard

“Innovación disruptiva en TI y ciberseguridad”

Dirigido a responsables de TI y ciberseguridad, Foro TAI celebró dos jornadas para hablar de innovación, para saber qué preocupa a los responsables tecnológicos de las empresas y analizar qué necesitan.

Rosalía Arroyo



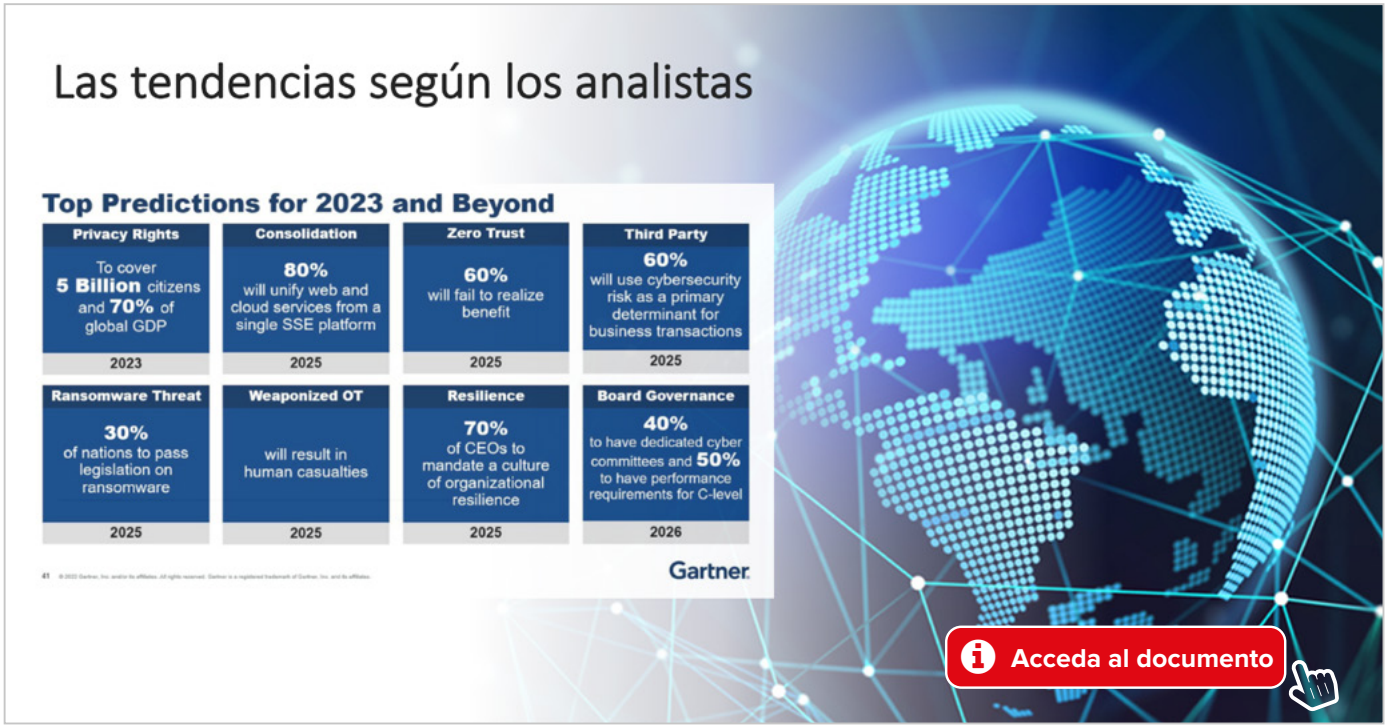
La primera jornada, dedicada a la ciberseguridad, contó con la participación de once responsables de TI y ciberseguridad, quienes debatieron sobre la evolución del SOC, ciberinteligencia, los servicios o una continuidad de negocio cada vez más compleja. Diego Durantes Toribio, CISO de Aenor; Francisco Sánchez Nauffal, IT Security Director de EcoVadis; Cristina García García, CIO de Edison Next Spain; Jesús Abascal Santamaría, CISO de Clarkemodet; Maica Aguilar Carneros, CISO de Ferrovial; Enrique Cervantes Mora, CISO de Fintonic; Jesús Valverde Romero, IT Director & CISO de Isemaren; Ángel Moreno Esteban, Jefe de Servicio TIC del Gobierno de la Rioja; Axier Amo Izarra, Director General de Transparencia y Buen Gobierno del Gobierno de la Rioja; David Cerrato de la Macorra, IT Director & CISO de KRUK España y José Luis Paramio, CISO de Userlytics, fueron los clientes participantes en el debate, acompañados de Pablo Teijeira, global business & marketing director de BeDisruptive; María Rojo, CEO de Enthec; Sergio Martínez, Iberia Regional Manager de SonicWall; Iván Mateos, Sales engineer de Sophos y Elena García-Mascaraque, responsable de MSSP de WatchGuard.

Innovando

Emilio Castellote, Business Transformation & CyberSecurity Strategy Senior Consultant, fue el encargado de la ponencia inaugural del primer Foro TAI, titulado “Innovación disruptiva en TI y Ciberseguridad”. Haciendo referencia al título, aseguraba Castellote que innovar es

un concepto que cuesta entender “porque la innovación no es hacer algo nuevo. La innovación es mejorar algo que existe y hacerlo más fácil”, y que en la actualidad “hay que ser disruptivo. Hay que hacer las cosas de otra forma, rompiendo estándares”.

Asegurando que para poder innovar y ser disruptivos hay que tener en cuenta lo que se prevé que va a pasar en el futuro, compartía Emilio Castellote ocho predicciones de Gartner en torno a la privacidad; consolidación a través de la SSE Platform; confianza cero, respecto a la cual asegura que para 2025 el 60 % de las implementaciones de Zero Trust fallarán; relación con terceros, por lo que para 2025, que el 60 % del negocio de las corporaciones grandes necesitarán establecer estándares de interoperabilidad seguros; *ransomware*; el impacto del mundo OT; resiliencia, una capacidad que el CEO tiene que trasladar a toda la organización; y consejos de administración que tendrán que incluir un subcomité de ciberseguridad alineado con el negocio.



Profundizaba Emilio Castellote en las predicciones comentando que la privacidad tiene mucho que ver con el dato, algo de lo que se han olvidado la mayoría de las estrategias de ciberseguridad, más pendientes de la seguridad de la red o los accesos. El dato, además, “no sólo hay

Emilio Castellote,
Business Transformation & CyberSecurity Strategy Senior Consultant

“La innovación no es hacer algo nuevo. La innovación es mejorar algo que existe y hacerlo más fácil”

que verlo dentro de la organización, sino también cuando la abandona"; un dato que estará en una plataforma *cloud* que deberá integrar todas las capacidades y funcionalidades "para servir ese dato de forma segura, para monitorizar ese dato de forma segura y para hacer que todo el conjunto funcione".

Diego Durantes Toribio,
CISO, **Aenor**

"Hay que elegir un proveedor que forme parte de tu organización, que trabaje contigo en el día a día, que entienda cuál es el *core* de tu negocio"

Avanzaba el experto hacia la tercera predicción asegurando que si el dato va a tener que ir hacia esas plataformas *cloud*, "hay que gestionar el acceso a ese dato". En esta gestión de acceso entra en juego el Zero Trust, un modelo que según Gartner no se está adoptando de la manera adecuada y fallará en el 60 % de los casos. Siguiendo con el dato y las previsiones, relacionaba Emilio Castellote el dato con lo que hacen con él terceras partes para asegurar que "el riesgo de seguridad no solo es nuestro, sino el de todas las terceras partes con las que me relaciono", a pesar de lo cual "son pocas las exigencias que estamos poniendo a la hora de interaccionar con terceros".

Tras analizar las cuatro primeras predicciones en base al dato, continuaba Emilio Castellote con las restantes tendencias estableciendo como hilo conductor una pregunta: ¿para qué? Es decir, ¿para qué pondremos foco en la privacidad, consolidaremos en plataformas *cloud*, adoptamos Zero Trust o tenemos en cuenta el riesgo de terceros? Entre otras cosas nos protegemos "para hacer frente al *ransomware*",

Pablo Teijeira,
global business & marketing director,
BeDisruptive

"Hay que dejar de lado el concepto tradicional de SOC y pensar en otros términos"

un aspecto sobre el que el legislarán el 30 % de las naciones; aseguraba también el experto que proteger el OT "es más importante de lo que pensamos" y que requiere de datos "que están vivos, que tienen que compartirse y que tiene que salir"; para aportar esa resiliencia

Jesús Abascal Santamaria, CISO, **Clarkemodet**

> "Hay que prestar atención al control de accesos de terceros, sobre todo para garantizar que el trato que se le da al dato es el correcto"

que nos dice que cuando se produzca un fallo, "tiene que haber algo detrás". El último "para qué" hace referencia a la última tendencia de Gartner, que dice "que en los consejos de administración tiene que estar presente la estrategia de ciberseguridad".

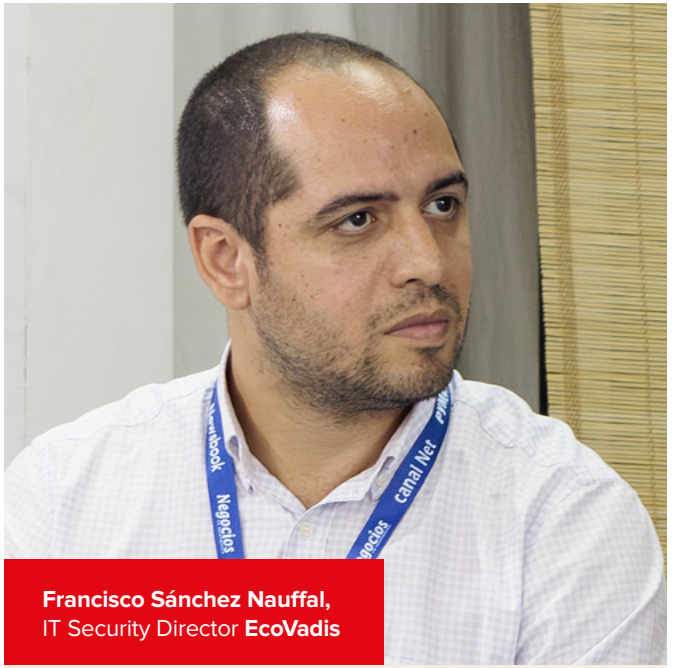
Antes de finalizar su ponencia, planteaba Emilio Castellote una serie de reflexiones. La primera hace referencia a la digitalización acelerada que se produjo durante la pandemia. De la noche a la mañana se pasó a un modelo de trabajo y conectividad diferente; "la suerte que tuvimos es que la tecnología existía, siempre estuvo ahí. La gran reflexión es: ¿qué nos impedía utilizarla?". Además, Castellote planteaba a los asistentes al Foro TAI otra serie de reflexiones:

- ¿Cómo nos ayudarán los frameworks de seguridad siendo de conocimiento público?
- ¿Qué impacto tendrán los servicios *cloud* en mi estrategia de ciberseguridad?
- ¿Qué papel jugará la IA en la ciberseguridad?
- ¿Hacia qué tipo de soluciones vamos?
- ¿Cómo nos gustaría que la industria nos apoyara en este recorrido?

Para finalizar, pedía que cada uno pensara en cómo le gustaría que la industria le acompañara, y planteaba a los asistentes que se preguntaran más a menudo "para qué estoy haciendo esto" y empezar a cuestionarse el porqué lo estoy haciendo".

El SOC a debate

Comenzaba el debate hablando de Centros de Seguridad de Operaciones, o SOCs. Concretamente se planteó a los asistentes cuál es el aspecto más relevante a la hora de interactuar con un SOC.



Francisco Sánchez Nauffal, IT Security Director **EcoVadis**

> "Para Ecovadis es relevante tener la capacidad de detectar y responder en momentos donde no está el equipo presente"

Contaba José Luis Paramio, CISO de Userlytics, que “para empresas que están 100 % en la nube, no es útil el SOC que se está vendiendo”. Explicaba que cuando te enfrentas a un SOC tradicional “hay un paquete base del que no puedes escapar y que está basado en tu red interna. Pero yo no tengo red interna, y además la mitad de lo que voy a pagar no lo necesito”, lo que le ha llevado a tener “algo parecido” a un SOC que cumple con sus necesidades.

Cristina Garcia Garcia,
CIO, **Edison Next Spain**

“TI y ciberseguridad utilizan terminologías diferentes. Necesitamos un mayor entendimiento”

Siendo también una empresa basada cien por cien en nube, Francisco Sánchez Nauffal, director de seguridad IT de Ecovadis, no comparte la opinión de José Luis Paramio. Explica que las empresas basadas 100 % en *cloud* tienden a ser más pequeñas, no tienen los mismos recursos y que lo tradicional va cambiando hacia una consolidación basada en necesidades, por lo que, en su caso, se ha optado por un SOC gestionado al que se añade la operación de red y la operación del SASE como servicio; “¿por qué no combinarlos en un único servicio?”, pregunta, teniendo en cuenta que para Ecovadis “es relevante tener la capacidad de detectar y responder en momentos donde no está el equipo presente”.

Fintonic es una empresa que nació hace diez años, es 100 % *cloud* y la regulación le obliga a tener un SOC, pero no le vale cualquier SOC sino “un SOC que entienda el negocio de

María Rojo,
CEO, **Enthec**

“Los servicios no automatizados que generan informes puntuales no valen para nada”

Fintonic y la infraestructura de Fintonic”, dice Enrique Cervantes Mora, CISO de esta compañía. Habla el directivo de un SOC “capaz, entre otras cosas, de detectar anomalías de comportamiento dentro del plano de gestión de mi infraestructura de empresa, porque necesito sa-

Maica Aguilar Carneros, CISO, **Ferrovial**

"Cuesta encontrar proveedores que tengan un enfoque orientado al cliente"

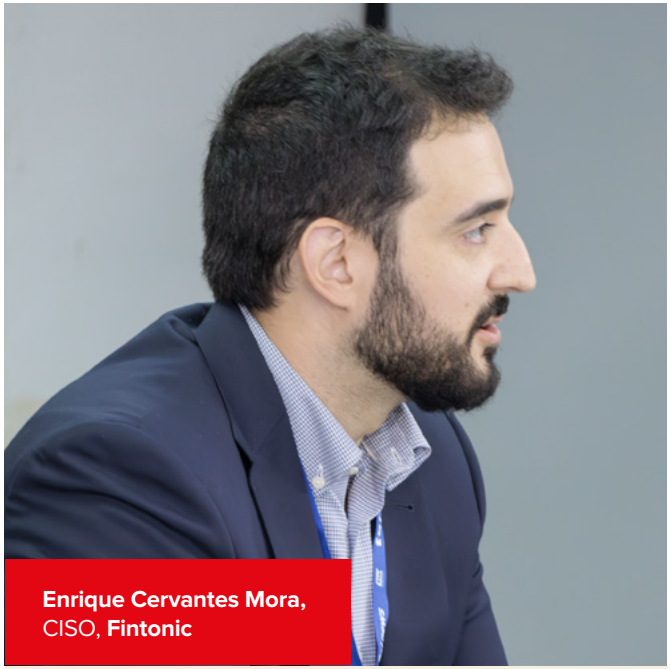
ber si un token de administrador se ha filtrado". Jesús Valverde Romero, IT Director & CISO de Isemaren, plantea que no es fácil pasar de cero a cien cuando se habla de SOC, porque se requiere una evolución y madurez interna, así como contar con un *partner* de confianza. Planteaba el directivo durante su intervención que, "si una empresa no tiene procedimientos, no tiene fuentes de información, no sabe cómo analizar la información, queda en manos del proveedor para que apliquen sus reglas de análisis, que no tienen por qué ser necesariamente las que necesita tu empresa".

"A mí lo que me hace falta es alguien que construya contigo un sistema de vigilancia 24 horas", decía Diego Durantes, CISO de Aenor, poniendo foco en el papel de los servicios.

Del SOC hacia el iSOC

Intervenía Pablo Teijeira, global business & marketing director de BeDisruptive, para comentar que habría que dejar de lado el concepto tradicional de SOC "y pensar en otros términos". Asegurando que hay que innovar en el servicio, y no tanto en la tecnología, comentaba el directivo que todo debe iniciarse como un viaje que tenga en cuenta desde el principio las problemáticas de los clientes.

"Puedo contratar el mejor SOC del mundo, pero no me sirve para nada si mi empresa no está preparada para usarlo", aseguraba David Cerrato de la Macorra, IT Director & CISO de KRUK España, trayendo a escena la importancia de la cultura empresarial y la necesidad de asegurar la información; "montar un plan director de seguridad basado en sistemas, y no en la información, es arcaico", aseguraba.



Enrique Cervantes Mora, CISO, **Fintonic**

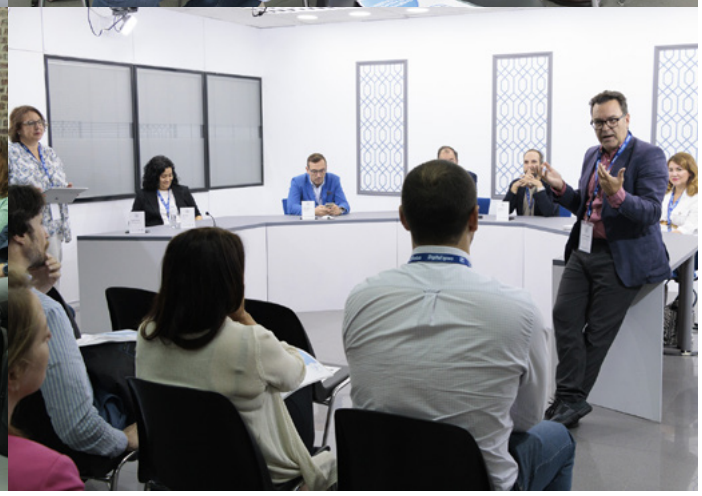
"Necesito un SOC capaz, entre otras cosas, de detectar anomalías de comportamiento dentro del plano de gestión de mi infraestructura"

Ciberinteligencia

La ciberinteligencia es la recopilación y el análisis de datos de ciberseguridad de múltiples fuentes utilizando algoritmos analíticos avanzados. Al recopilar grandes cantidades de datos sobre las amenazas y tendencias de los ciberdelincuentes se puede obtener información útil que ayude a los clientes a detectar y prepararse mejor para las ciberamenazas. ¿Está la empresa española adoptando este tipo de servicios?

Asegurando que es muy interesante cómo se ve tu empresa desde fuera, decía David Cerrato, IT Director y CISO de KRUK España, que la ciberinteligencia "es el futuro. Para mí lo de ayer ya no vale. Creo en la monitorización".

También se habló durante el debate del control de la Huella Digital o Huella Electrónica, que hace referencia al rastro de datos que dejas cuando usas Internet. Este tipo de servicios genera un informe que, en opinión de María Rojo, CEO de Enthec, "no vale para nada" porque "son servicios que no están automatizados". Explicaba la directiva que su compañía se ha pasado años desarrollando tecnología

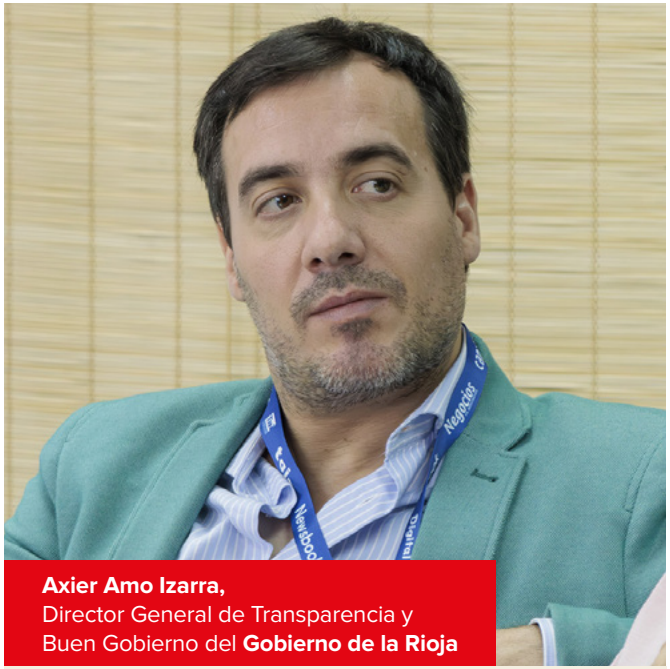


con inteligencia artificial incorporada que trabaja de forma continua.

Le parece muy interesante a Francisco Sánchez Nauffal, IT Security Director de EcoVadis, tener información de lo que ha podido pasarle a una empresa del mismo sector o que tiene una tecnología parecida "para tomar medidas, bien sea a nivel de procesos o de tecnologías para proponer un servicio que se adapte a lo que yo necesito".

¿Cuántos proveedores tenéis? ¿Cuántos son críticos? ¿Cuántos datos de vuestras empresas

estáis compartiendo con todos esos proveedores? Tres preguntas que planteaba María Rojo a los asistentes para explicarles que lo que hace Enthec es “aplicar toda la inteligencia artificial no solamente para que os aseguréis vosotros”, sino empezar a asegurar a los proveedores con lo que se trabaja, y además de manera tan fácil como hacer búsquedas de dominio.



Axier Amo Izarra,
Director General de Transparencia y Buen Gobierno del **Gobierno de la Rioja**

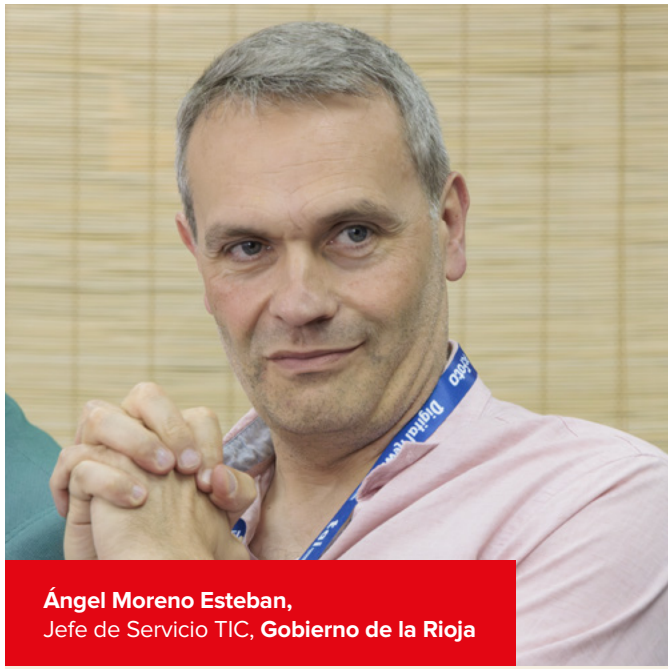
“Al ser administración pública, nosotros apostamos por la apertura del dato”

RETOS

“La descentralización de servicios” es lo que más preocupa a Francisco Sánchez Nauffal. Explica que se tienen muchas plataformas y que para obtener la información que necesita debe recabarla de muchas fuentes distintas para hacer la correlación. Menciona también como preocupante la tendencia de hay en el mercado de tener más servicios de los que se utilizan y el que “las empresas tienden a ser más especialistas en todo, cuando en muchos casos lo que necesito es gente específica en áreas determinadas y alguien que me ayude a orquestar a esos especialistas a nivel de servicio”.

Para Cristina García García, CIO de Edison Next Spain, las preocupaciones para este año son “todas”. Reconoce que los responsables de TI y de ciberseguridad utilizan terminologías diferentes y que se necesita un mayor entendimiento.

Descentralizar las aplicaciones y los sistemas, así como un mayor control de los terceros es



Ángel Moreno Esteban,
Jefe de Servicio TIC, **Gobierno de la Rioja**

“Tiene que haber un balance entre acceso a la información y seguridad”

la preocupación de Jesús Abascal Santamaria, CISO de Clarkemodet. Explica que la compañía trabaja en la adopción de una arquitectura SASE y que se están prestando mucha atención al control de accesos “sobre todo para saber qué dato está manejando para garantizar

Jesús Valverde Romero,
IT Director & CISO, **Isemaren**

> "Es indispensable tener claro dónde está el *core* del negocio, saber dónde no vas a poder llegar y encontrar un socio de confianza que te pueda ayudar"

que el trato que se le da al dato es el correcto". Frente a estos y otros muchos retos que se tienen en el mercado de ciberseguridad, plantea Sergio Martínez, responsable de SonicWall en el mercado de Iberia, que hay que adoptar una defensa por capas, desde el dato hasta la identidad, pasando por las aplicaciones... "hay muchas caras en este decaedro tan complicado que es la ciberseguridad", al que hay que añadir la inteligencia artificial que está tan de moda.

Añade el directivo que, según un estudio realizado por la compañía, "para el 91 % de los CISOs el mayor problema es el *ransomware*", un *ransomware* que, como recoge el informe "emplea una sutileza sin precedentes".

Inversiones en tecnología

Se habló también durante el Foro TAI de inversiones de ciberseguridad, de dónde puede no estarse llegando y dónde estaría el cambio que diera un empujón definitivo a la postura de ciberseguridad.

Durante su intervención destacaba Maica Aguilar, CISO de Ferrovial, lo enriquecedor del Foro TAI, donde quedaba patente que ni las empresas son iguales, ni se está en el mismo punto de madurez, ni todos necesitan los mismos servicios. "Está claro que la digitalización y el incremento de productos de seguridad hace que necesites ayuda" y que lo ideal es "que cada empresa busque aquello que necesite", decía la directiva, añadiendo que la ventaja es que hoy se puede elegir.

Reflexionaba la CISO de Ferrovial que, gestionando distintos tipos de servicios y muchos proveedores desde hace muchos años,

David Cerrato de la Macorra,
IT Director & CISO, **KRUK España**

> "Puedo contratar el mejor SOC del mundo, pero no me sirve para nada si mi empresa no está preparada para usarlo"

le cuesta encontrar “proveedores que tengan un enfoque orientado al cliente” y pedía a los proveedores asistentes que los servicios deberían “estar un poco más adaptados a las necesidades de cada cliente”, añadiendo que también hay que asegurarse de que el servicio es “bueno, adecuado” y “no conformarnos con pensar que porque tenemos contratado un servicio ya estamos viendo todo y no vamos a tener problemas”.

Sergio Martínez,
Iberia Regional Manager, **SonicWall**

“Hay muchas caras en este decaedro tan complicado que es la ciberseguridad”

Axier Amo Izarra, Director General de Transparencia y Buen Gobierno del Gobierno de la Rioja, apuntaba durante el debate que, al ser Administración Pública, se apuesta por la apertura del dato.

Estando en el lado del desarrollo y habiendo vivido algún incidente de seguridad, tiene claro Ángel Moreno Esteban, Jefe de Servicio TIC del Gobierno de la Rioja, que “tiene que haber un balance entre acceso a la información y seguridad”. Se dan algunos casos únicos, como que la Ley de Transparencia obliga a que sean públicos los nombres, cargos y correos electrónicos de los funcionarios, una información que desde el punto de vista de la ciberseguridad no estaría disponible. “Entendemos que hay datos públicos disponibles que se pueden utilizar para lanzar ataques, entendemos los riesgos, pero es que nos obliga la Ley”, asegura Ángel Moreno.

Tras comentar varios de los asistentes el mal uso que hacen los trabajadores al utilizar sus direcciones de correo profesionales para darse de alta en servicios personales interviene David Cerrato para comentar que “es mucho peor cuando se dan de alta en páginas de sanidad porque el dato sanitario es súper clasificado y

Iván Mateos,
Sales Engineer, **Sophos**

“El futuro no está tanto en la tecnología como en el servicio”

José Luis Paramio, CISO, **Userlytics**

> "Para empresas que están 100 % en la nube, no es útil el SOC que se está vendiendo"

eso cambia la clasificación de la información de tu sistema".

En este tipo de casos entra en juego "el nivel de madurez de la empresa, la formación y concienciación, y conseguir que el empleado sea la primera línea de defensa y no el primer cortafuegos", apunta Jesús Valverde, IT Director & CISO de Isemaren.

Para Iván Mateos, ingenieros preventa de Sophos, el futuro no está tanto en la tecnología como en el servicio. Comentaba que ser disruptivo es tener un punto de vista distinto y que, para ello, a veces hace falta un habilitador "que conozca al enemigo, sepa cómo se mueve, qué hace, por qué hace cosas que a lo mejor no me estaba esperando". Se refería el ejecutivo de Sophos al MDR (Managed Detection and Response), capaz de adaptarse a las necesidades e infraestructura de los clientes.

Modelos de implementación del SOC

Explicaba Francisco Sánchez Nauffal que la aproximación de la compañía a la hora de montar el SOC fue muy específica: poder cambiar al proveedor manteniendo dentro la ciberinteligencia, "y ese es el modelo que estamos siguiendo". Habla el directivo de EcoVadis de un modelo híbrido "en el que yo manejo la información y lo que hace el SOC es gestionarla en base a los criterios que definimos entre los dos". El modelo seguido en Isemaren ha sido montar el SOC internamente, "rodarlo con el conocimiento interno de mi sistema, de mis procedimientos, y a partir de ahí analizo si esto lo sigo haciendo internamente o contrato ayuda externa", cuenta Jesús Valverde. Considera indispensable que previamente se tenga claro dónde está el *core*

Elena García-Mascaraque, responsable de MSSP, **WatchGuard**

> "Es un riesgo el que un fabricante provea los servicios"

del negocio, saber dónde no vas a poder llegar por mucho que quieras y encontrar un socio de confianza que te pueda ayudar".

Para Diego Durante, CISO de Aenor, "el hecho de implantar un SOC en una organización va más allá de la tecnología. Hay que elegir un proveedor que forme parte de tu organización, que realmente trabaje contigo en el día a día, que entienda cuál es el *core* tu negocio, cuál es el riesgo y lo entienda como si fuera algo suyo".

Elena García Mascaraque, responsable del negocio MSSP de WatchGuard, tomaba la palabra durante el Foro para hablar de disrupción en la manera en que se consume la ciberseguridad. Recordaba que hace tiempo que se previó que los servicios de ciberseguridad iban a estar cada vez más democratizados y que la industria debía trabajar para que "todo el mundo tuviese acceso a servicios de seguridad avanzados".

Decía la directiva que "es un riesgo el que un fabricante provea los servicios" y que la clave es una orquestación entre los procesos y necesidades de los clientes, la tecnología de los fabricantes y las empresas que prestan los servicios. Mencionaba García Mascaraque que nos encontramos en la tormenta perfecta: Tenemos un montón de tecnologías súper complicadas que hacen unas cosas chulísimas pero que no sabemos gestionar; tenemos una falta de talento evidente; y por otra parte tenemos el reto del coste y la necesidad de ser eficientes. Mantener esos tres elementos en su justa medida pasa por unos servicios gestionados "donde un proveedor de servicios y una tecnología se hablen muy bien para crear una plataforma que sea lo suficientemente hábil para que se conecte a vuestros procesos de negocio".

“La confianza se gana proyecto a proyecto y problema a problema”

La recurrencia es, en opinión de Pablo Teijeira, global business & marketing director de BeDisruptive, uno de los aspectos más relevantes a la hora de interactuar con el SOC. Habla el directivo de personalizar los servicios dependiendo de las necesidades de los clientes, algo que demandan los responsables de TI y ciberseguridad.

También le preguntamos por la manera de fomentar la cultura de colaboración y confianza entre los equipos del SOC y los clientes para promover la innovación, una confianza que se gana proyecto a proyecto y problema a problema y donde pone foco el directivo a la hora de innovar.

Habla Pablo Teijeira de la importancia del lenguaje cuando un CISO va a un consejo de administración; “muchas veces pensamos en innovar solo de una forma tecnológica, que también hay que hacerlo, pero innovar en cómo nos comunicamos también juega un papel muy importante”.

Pablo Teijeira, global business & marketing director, **BeDisruptive**

BeDisruptive™

“La ciberinteligencia aplicada a la ciberseguridad es crucial”

Dice María Rojo, CEO de Enthec, que la ciberinteligencia es un campo que crecerá mucho, y crecerá porque generamos una cantidad de datos ingentes y “si no tenemos ciberinteligencia y no hacemos después cosas útiles con esa información, vamos a estar totalmente colapsados”.

Aplicar inteligencia artificial a la ciberseguridad ayuda a gestionar y detectar aquello que suponga un riesgo, asegura la directiva, añadiendo que “la ciberinteligencia aplicada a la ciberseguridad es crucial porque los atacantes ya la están usando”.

Dice también la CEO de Enthec que conceptos como perímetro de seguridad o defensa en profundidad están maleados. “Nosotros proponemos una visión diferente”, explica María Rojo. Una visión que se basa en “mirar a la compañía de fuera hacia dentro”, saber qué información se está escapando de las empresas y saber qué conocen los ciberdelincuentes de nosotros.

María Rojo, CEO, **Enthec**

ENTHEC

“Estamos viendo una evolución muy preocupante de los ataques IoT”

¿Qué estamos haciendo mal? Habla Sergio Martínez, responsable de SonicWall para el mercado de Iberia, que existe un *gap* entre lo que lo que necesitan las empresas y lo que se pueden permitir con sus presupuestos, que es lo que la compañía ha bautizado como el Cyber Security Business Gap, que genera una paradoja: nunca hemos invertido tanto en ciberseguridad y, sin embargo, aparentemente todo parece que va peor, según un estudio realizado por la compañía.

Menciona el directivo las amenazadas cifradas como uno de los graves problemas de ciberseguridad, al que se suma el *ransomware*, que ha conseguido desarrollar “una sutileza sin precedentes”. Alerta sobre que “este año estamos viendo una evolución muy preocupante de los ataques IoT, así como el cryptojacking”.

No se olvida de mencionar el tráfico cifrado como “uno de los problemas más importantes a los que nos enfrentamos”.

Sergio Martínez, Iberia Regional Manager, **SonicWall**

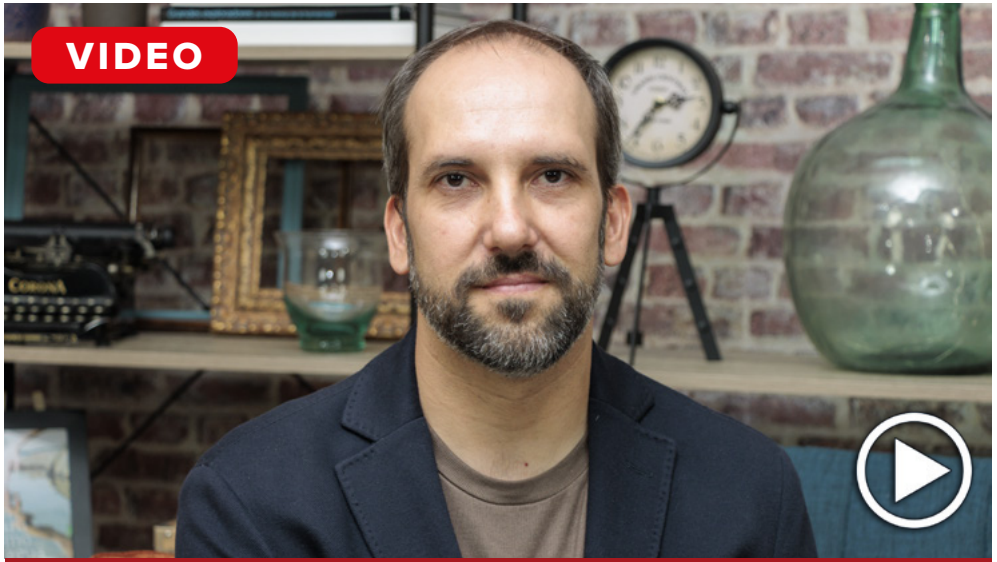
SONICWALL™

“La innovación llega en forma de servicios”

“Estamos aplicando innovación no sólo en las soluciones y los productos, sino en los servicios de ciberseguridad, servicios de respuesta ante incidentes, servicios de vigilancia, que es lo que nos estaban pidiendo las compañías”, nos cuenta Iván Mateos, ingeniero preventa de Sophos.

La manera de abordar la postura de seguridad también llega a través de los servicios, porque “hemos visto cómo muchas empresas tienen proyectos de Zero Trust o SASE, y sin embargo se estaban teniendo que enfrentar a todo eso con pocos recursos y unas dificultades enormes para retener el talento”.

Dice también Iván Mateos que, a pesar de que todo el mundo hable ahora de ChatGPT, “la inteligencia artificial se viene aplicando desde hace mucho tiempo”, y no solo de parte de los buenos. Añade que no se puede abordar ese volumen ingente de datos y ese volumen de eventos “si la inteligencia artificial no te ayuda”.



Iván Mateos, Sales Engineer, **Sophos**

SOPHOS

“Hay que buscar una seguridad proactiva”

Hablamos con el responsable de cuentas estratégicas de WatchGuard sobre la evolución de la protección *endpoint*, una evolución que ha pasado de buscar lo malo a permitir lo bueno; un cambio de paradigma debido a la capacidad que existe a la hora de “analizar las cosas con la soltura y con la solvencia” que permiten a la nube y tecnologías como la inteligencia artificial o el *deep learning*.

El talento es difícil de encontrar, y de retener, destaca Elena García Mascaraque, responsable de MSSP de WatchGuard, señalando el valor que tienen los proveedores de servicios a la hora de aglutinar ese talento, así como el de los fabricantes a la hora de facilitar que ese talento pueda trabajar de la mejor forma posible, con las mejores herramientas y la mejor inteligencia a su disposición.

En opinión de Carlos Castro “hay que buscar una seguridad proactiva”, adoptando tecnologías como el Threat Hunting no sólo para entender qué está pasando en tus sistemas, sino cómo te han atacado.

Elena García-Mascaraque, responsable de MSSP, **WatchGuard**
Carlos Castro, estrategic account manager de **WatchGuard**