DOCUMENTOS SiC
Nº 29
NOVIEMBRE 2019

## Servicios gestionados

# LA EXPERIENCIA E INNOVACIÓN EN CIBERSEGURIDAD DEL MAYOR OPERADOR GLOBAL EUROPEO

T · · Systems · Let's power higher performance

- SOCs: inteligencia y servicio en una red integrada de 14 centros especializados
- VUMES: gestión del ciclo completo de vulnerabilidades
- ESARIS, framework propio de protección cibernética
- Enfoque: Zero Outage + Zero Trust

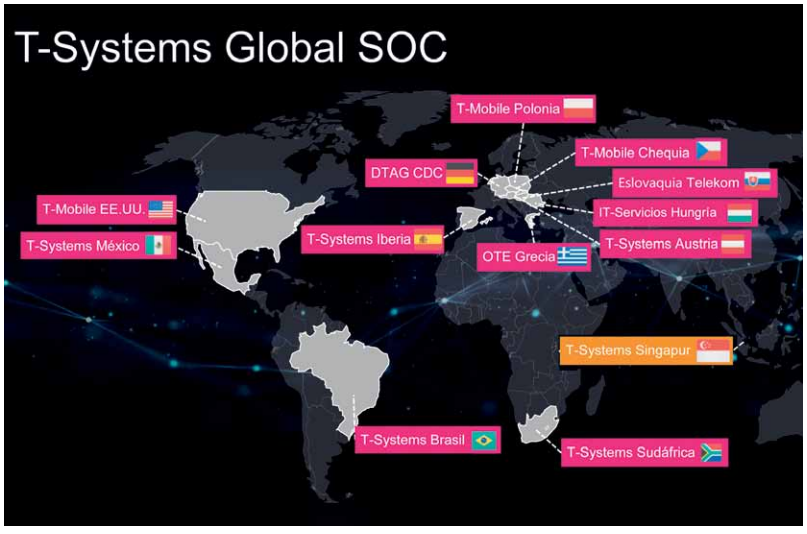
**Ángel Otermin**
Head of Cybersecurity Sales de T-Systems Iberia

# Servicios globales de ciberseguridad gestionada inteligente con visión alemana

**Con una red de 14 SOCs, incluido uno especializado en coches conectados, más de 37.500 expertos y presencia en 20 países, T-Systems es uno de los referentes mundiales en TI y ciberseguridad gestionada. Propiedad del mayor operador de telecomunicaciones europeo, Deutsche Telekom, su metodología 'Zero Outage' (cero fallos) propone anticiparse a cualquier tipo de incidente y gestionar de forma eficaz los riesgos.**

¿Qué sentido tiene correr si se va en la dirección equivocada?, dice un proverbio alemán. Para evitar ese riesgo en un mundo hiperconectado,**T-Systems**, la filial tecnológica de **Deutsche Telekom**, ha desarrollado una propuesta de valor que se resume en su lema *'Let's Power Higher Performance'* que establece cuatro entornos estratégicos: Conectividad, Nube, Digitalización y, por supuesto, Ciberseguridad, que además es transversal a los anteriores a través de una organización del Grupo Deutsche Telekom que toma cuerpo en la unidad global **Telekom Security**, en la que se integran todos los profesionales de ciberseguridad de las filiales del Grupo. Para acompañar a las empresas en su viaje digital, la organización alemana ha desarrollado un portafolio de servicios de ciberseguridad que abarca los cinco ámbitos de la protección a partir de su marco de trabajo **ESARIS,** basado en la metodología del **Instituto Nacional de Estándares y Tecnología (NIST)**. "La prevención y la detección son los pilares sobre los que se han asentado las arquitecturas de seguridad tradicionales, centradas en la respuesta al incidente. Sin embargo, en un mundo conectado esta postura ya no basta", recuerdan. Por eso, T-Systems ha desarrollado su concepto '***Cyber Security Protection Shield***', que permite trabajar con un enfoque integrado,

contando con método, herramientas y grandes expertos para "apoyar la transformación de la empresa con activos de alto rendimiento", objetivo para el que también trabaja con socios de referencia en ciberseguridad como **Cisco, Check Point, Symantec, Microsoft, McAfee, IBM, Zscaler y Zimperium,** entre otros. Consciente de que la tecnología no es todo, T-Systems valora el conocimiento y experiencia de su equipo de expertos, que disponen de las certificaciones necesarias en todas las disciplinas que componen las TIC.




## Red global de SOCs

El corazón del sistema de protección del Grupo es su *Centro de Operaciones de Seguridad* (SOC) y Defensa Cibernética (CDC), en Bonn. Desde él se coordina el trabajo de los más de 1.600 expertos que trabajan en su red de 14 SOCs, incluido uno en Madrid, desde los que ofrece sus servicios de seguridad gestionada, además de proteger a todas las empresas del Grupo Deutsche Telekom, un ecosistema que se basa en la premisa de que cuanto mayor sea una red, mejor será la información que aporte y, por tanto, el servicio de ciberprotección que ofrezca.

## Inteligencia predictiva

La red de SOCs permite, en 24 horas, la detección de más de 2,5 billones de

**La pregunta clave es: ¿tiene una empresa por sí sola capacidad de respuesta y recuperación tras sufrir un ciberataque severo o padecer una fuga de información? La respuesta es que en un mundo hiperconectado y con amenazas complejas no es posible gestionar en solitario la seguridad digital. Por eso, contar con un MSSP de confianza es casi obligatorio.**

amenazas, procedentes de 3.300 fuentes, contando también con uno de los bancos de ciberinteligencia más grandes del mundo, en el que se dispone de más de 20 millones de muestras de software malicioso, *ransomware*, ataques APT y *exploits* de día cero, entre otros. De hecho, sólo en el último año ha identificado y registrado más de 75.000 nuevos tipos de ciberataques de distinta intensidad y alcance.

### Filosofía 'cero fallos'

Estas capacidades brindan una alta ciberprotección a los clientes en su operación diaria, además de "implementar proyectos desde cero, o realizar el *upgrade* y la transformación digital de cualquier organización partiendo de sus infraestructuras existentes".

**T-Systems ha desarrollado para sus clientes el 'Cyber Security Protection Shield' con el que ofrece el mismo estándar de ciberseguridad con el que Deutsche Telekom protege sus redes.**

Para ello emplea la metodología '***Zero Outage'*** (Cero fallos), que busca la continuidad de negocio en cualquier situación, un enfoque que ha llevado a la compañía a contar con clientes de referencia, entre los que destacan organismos públicos, como la **Oficina Federal de Seguridad de la Información de Alemania (BSI)** o la **Comisión Europea (CE)**, hasta entidades como la **Asociación GSM (GSMA),** la **Agencia Europea de Seguridad (ENISA)** y empresas como **Continental,** el **Grupo VW,** además de las compañías del **DAX30** (el Ibex35 alemán) y 19 del **Fortune 100.**

## VISIÓN 'ZERO OUTAGE': LA OBSESIÓN POR LO PERFECTO

T-Systems basa su estrategia de TI, desde 2011, en la metodología **'Zero Outage' (Cero fallos),** certificada por **TÜV Rheinland**, que tiene como objetivo la continuidad del negocio sin importar la amenaza a la que hace frente. Por eso, es la piedra angular sobre la que articula su política de '*Security by Design*' en servicios y soluciones.

**1. Análisis de riesgos.** 'Zero Outage' parte de identificar más de 300 riesgos asociados al despliegue y la operatividad de los Sistemas de Información de los verticales con los que trabaja T-Systems, agrupándolos en 40 grupos, con un plan de acción para cada uno.

**2. Buenas prácticas.** Esta información se plasma en guías, instrucciones y buenas prácticas para una amplia variedad de situaciones, bajo el marco de trabajo ESARIS (***E**nterprise **S**ecurity **A**rchitecture for **R**eliable **I**CT **S**ervices*) para reforzar la seguridad del cliente (como se muestra en el gráfico).

**3. Estandarización.** Se crea un esquema común de clasificación y organización de los sistemas con el que se define el modelo al que cada actor debe contribuir en la forma y en el fondo marcado.

**4. Proceso de seguridad contínua.** Por último, se establecen unos controles de seguridad, clasificados y organizados para que puedan aplicarse de una manera estandarizada e industrializada. Este concepto de industrialización es la clave para asegurar la continuidad de los sistemas desde las tres dimensiones de la seguridad: confidencialidad, integridad y disponibilidad de la información.

## AUTOMOTIVE SOC: PROTEGIENDO YA EL COCHE CONECTADO

Alemania ha sido y es una de las grandes protagonistas del mundo del Motor con grupos industriales como Volkswagen y Daimler AG (Mercedes-Benz). No en vano, **Karl Benz** y **Nikolaus Otto**, fueron los que lo inventaron a finales del siglo XIX. Por eso, T-Systems ha considerado una prioridad la protección del coche conectado y autónomo. Para ello, desde 2019, cuenta en Bonn con el primer SOC especializado en vehículos (*Automotive SOC*) de Europa, en colaboración con **Argus Cyber Security**, propiedad de **Continental**, un centro que trabaja con el resto de la red de SOCs del Grupo analizando los datos de millones de coches conectados a través de su Sistema de Gestión de Información y Eventos (SIEM) para automóviles y sistemas de a bordo. De hecho, muchos fabricantes de automóviles (OEM) y operadores de flotas, ya usan su solución, que permite contar con "guardaespaldas digital y una defensa cibernética en tiempo real", según declaraciones de **Adel Al-Saleh**, CEO de T-Systems.

# Ángel Otermin

Head of Cybersecurity Sales de T-Systems Iberia

**Le apasiona ayudar a los clientes a proteger el negocio. Y destaca la importancia de contar para ello con un SOC en España, integrado en una red global en cuatro continentes. Para el responsable de ventas de T-Systems Iberia en ciberseguridad, Ángel Otermin, la "obsesión" alemana por la ciberseguridad supone un valor diferencial. ¿Un ejemplo? Los clientes de la compañía se benefician de la misma tecnología que protege a su empresa matriz, Deutsche Telekom, el primer operador de telecomunicaciones de Europa.**

## "Los clientes de T-Systems se benefician de las mismas tecnologías y servicios en los que descansa la seguridad digital de Deutsche Telekom"

**– Qué define a T-Systems Iberia en ciberseguridad…**

– Nos obsesiona la ciberseguridad y las cosas bien hechas. Por eso siempre trabajamos con procedimientos muy concretos y probados, ajustados a un marco normativo (*framework*) de elaboración propia. A veces, incluso, 'en exceso'… pero, en seguridad, nunca es suficiente. Por eso, nuestro enfoque de 'Seguridad por diseño' en servicios y productos sí marca una gran diferencia en calidad y en protección.

**– ¿Qué les diferencia de otros proveedores de servicios de ciberseguridad gestionada?**

– La proximidad. Es una de nuestras señas de identidad y lo que nos ha llevado a establecer SOCs en cuatro continentes. En nuestro caso, cuando una organización habla con nosotros lo hace con una persona en castellano y con cultura hispana. Y lo mejor es que nuestros clientes aquí se benefician de la inteligencia de cualquier SOC del mundo. En protección trabajar de forma conjunta con un gran equipo y tecnologías de valor es lo que realmente marca la diferencia.

**– ¿Cuál es su aspecto más desconocido en Iberia?**

– Se nos conoce mucho por la infraestructura pero menos por la ciberseguridad, que llevamos aplicando en ella durante lustros. Precisamente para protegerla se creó la actual red de SOCs. Así que cualquiera de nuestros clientes, sin importar su tamaño, se beneficia de la misma tecnología y herramientas que utilizamos para proteger Deutsche Telekom, el primer operador de telecomunicaciones europeo.

**– ¿Qué aporta tener una visión alemana y depender de Deutsche Telekom?**

– La ciberseguridad en Alemania siempre ha sido una prioridad como país. Y el Grupo Deutsche Telekom también trabaja con esa visión. Nuestra gran ventaja respecto a la competencia es que, como operador,

controlamos las comunicaciones en gran parte del continente con lo que somos capaces de detectar, antes que nuestros competidores, cualquier incidente o amenaza que vaya por la infraestructura. A tal fin, y entre otras capacidades, tenemos desplegada una red de más de 3.000 señuelos (*honeypots)* que nos permiten ser ágiles detectando y rápidos actuando.

**– ¿Hay ventaja en disponer de un *framework* de ciberseguridad propio, ESARIS?**

– ESARIS (*Enterprise Security Architecture for Reliable ICT Services*) se creó para dar seguridad a Deutsche Telekom y ahora también a sus clientes, con lo que supone estar siempre en continua actualización. Estamos incorporando en él el concepto de 'Zero Trust', que supone no confiar en nada ni nadie e implementar la autenticación segura de las personas para ofrecer siempre la mayor seguridad posible. Gracias a Zero Trust se pueden prevenir muchas de las amenazas que aún no se conocen. Y es un excelente complemento a nuestra filosofía Zero Outage (cero fallos), que se aplica a todo el entorno TI y que garantiza que todos nuestros productos y servicios cumplen los estándares más exigentes de calidad y seguridad.

**– ¿Cuál es la clave para disponer de un nivel *top* de madurez en ciberseguridad?**

– Contar con capacidades de recuperación y respuesta. La ciberseguridad 100% no existe, es más un concepto de marketing. Pero si tras un ataque estás preparado para seguir con tu negocio en el menor tiempo posible, entonces tienes un buen nivel: eres resiliente.

**– Este año han integrado el SOC de Madrid en la red mundial de T-Systems…**

**"La integración del SOC de Madrid, en la red mundial de SOCs de Deutsche Telekom, nos ha convertido en una unidad de negocio con entidad propia en T-Systems Iberia. Somos, por tanto, un MSSP gestionado en local pero con alcance global y preparado para dar servicio 'Follow the sun'".**

– Ha sido un gran paso. El SOC de Madrid existía hace tiempo, pero para dar seguridad a nuestros clientes en nube, aplicaciones… Ahora se ha convertido en una unidad de negocio con entidad propia, conectada al SOC central, en Bonn, compartiendo y recibiendo inteligencia y ofreciendo servicios de ciberinteligencia avanzada, de gestión de *malware*, de *sandboxing*, herramientas, etc. Así somos un proveedor de ciberseguridad gestionada local, pero con alcance global y preparados para dar un servicio '*Follow the sun'* a través de nuestros SOCs en EE.UU., Singapur, Polonia, México…

**– ¿Trabajan para convertirlo en Centro de Excelencia del Grupo en algún aspecto concreto?**

Estamos liderando la línea de SOC industrial, junto con Alemania. Es una apuesta importante pero que se justifica porque España, tanto en volumen de negocio TI como en ciberseguridad, es el segundo país que más factura en Europa. Por eso, uno de nuestros grandes retos es que en el año 2020 sea una realidad y comience a trabajar de forma intensiva con los clientes.

**– Sus servicios más demandados…**

– Los de ciberinteligencia. Por ejemplo, el que permite monitorizar dominios (DNS) para saber si a una empresa le han creado varios similares al original… y alertarla de que puede sufrir un ataque de suplantación (*phishing*) por correo-e a través de ellos. También destacamos por nuestros servicios de detección de software malicioso analizando ficheros con *sandboxing*. Una información que compartimos todos los SOCs con la ventaja que supone para nuestros clientes en todo el mundo. Esa es otra de nuestras grandes ventajas competitivas: generamos nuestra propia inteligencia.

**– ¿Cuál es su producto o servicio más innovador?**

– Hay muchos, pero destacaría tres: en primer lugar, VUMES, nuestro servicio de gestión de vulnerabilidades a lo largo del ciclo de vida. También una nueva herramienta que estamos desarrollando, con dos bancos muy grandes en España, para autenticar las operaciones que exige PSD2 a través de biometría basada en el tecleo. Y, por último, nuestra oferta para proteger y ser resilientes en redes industriales (OT) y ecosistemas IoT.

**– ¿Van a presentar en 2020 nuevos servicios?**

– Vamos a ser bastante innovadores. Por ejemplo, en ciberseguridad industrial, a través de alianzas con referentes como ABB, CyberX o Siemens, vamos a ofrecer mejores capacidades para la monitorización y respuesta de incidentes. Para la nube estamos desarrollando una solución completa y fácil de usar que incluirá la monitorización y la gestión de IaaS *(Infrastructure as a service),* con Check Point y su solución Dome9, de agente de seguridad de acceso a la nube (CASB), posiblemente con Symantec, un multifactor de autenticación reforzado, proxy de Internet y seguridad de aplicaciones. También continuaremos invirtiendo en tecnologías de automatización, aprendizaje automático, inteligencia artificial… El cibercrimen siempre va a contar con más medios e inversión y sólo siendo más eficientes y contando con los mejores aliados se le puede hacer frente.

# T-Systems Iberia Ciberseguridad: un MSSP de atención local con alcance global

**Desde que en 2001 T-Systems abrió su filial española, no ha dejado de crecer y ya representa el segundo mercado europeo de la firma. Su apuesta por una línea de negocio de ciberseguridad, con personalidad propia, le ha llevado a reforzar su SOC, en Madrid, integrándolo en la red global del Grupo. Desde él ofrece una oferta personalizada para ayudar a alcanzar a sus clientes un nivel mantenido de resiliencia en su evolución digital. Entre los servicios más demandados cabe destacar la gestión del ciclo de vida de vulnerabilidades y los basados en inteligencia predictiva de amenazas. En 2020, incrementará su propuesta en protección de servicios cloud, así como de entornos industriales e IoT.**

**T-Systems Iberia** es conocida en la Península Ibérica por ser uno de los referentes en materia de servicios y aplicación de TIC. De hecho, ha sido elegida por **Penteo,** por quinto año consecutivo, como líder en servicios de Cloud Híbrida. Su éxito en el ámbito TIC también es fruto del alto nivel de ciberseguridad que siempre ha mostrado en sus servicios y que han hecho que millones de clientes, corporativos y particulares, confíen en ella. Su fiabilidad viene de la mano de su marco de trabajo propio (ESARIS), así como de las reforzadas capacidades de su SOC, en Madrid, que se nutre de la inteligencia global de la red mundial de 14 centros.

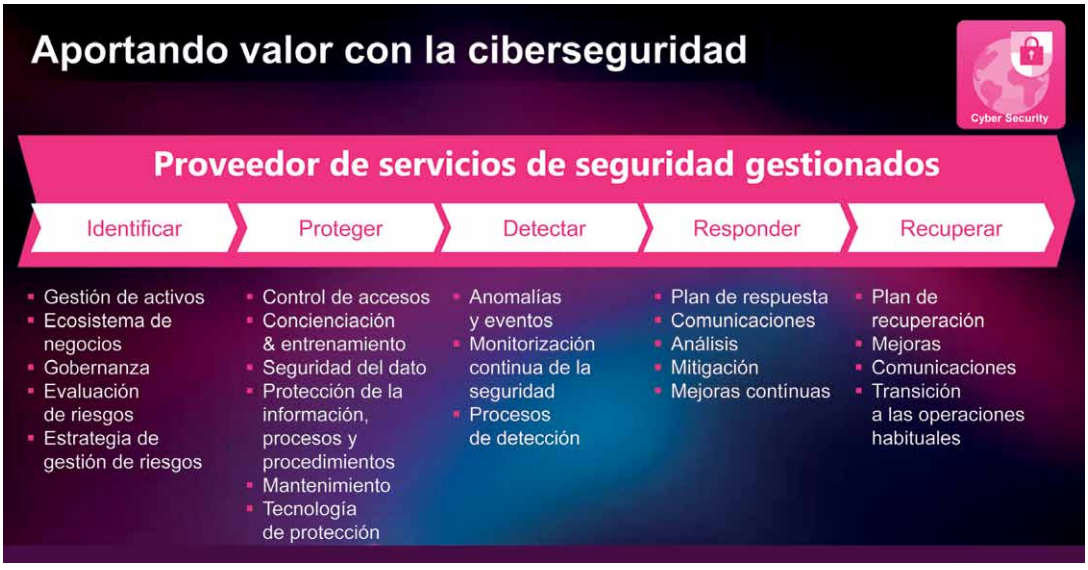
La historia de la compañía en España comenzó en 2001 cuando el grupo **Deutsche Telekom** se convirtió en el principal accionista de **Debis IT Services,** formada por la filial tecnológica de DaimlerChrysler. En 2006, adquirió **Gedas** y **TAO,** las filiales tecnológicas del **Grupo Volkswagen AG,** lo que supuso un fuerte impulso en el proceso de crecimiento de este proveedor en España.

### Unidad independiente de ciberseguridad

Fruto de su apuesta por la ciberseguridad, T-Systems Iberia tiene su propia línea de negocio para el mercado nacional. Para ello, cuenta en Madrid con un SOC que, desde 2018, se ha integrado en su red global de SOCs, compartiendo metodología, herramientas e inteligencia.

Desde él, ofrece ciberseguridad en la nube, puntos finales y gestión de incidentes, unas capacidades que la convierten en una referencia en el sector, aportando servicios y soluciones horizontales y verticales en todos los sectores industriales, con incidencia muy significativa en *manufacturing*, sector público, *utilities*, banca-seguros y logística-*retail*. Para el próximo año, además, la filial quiere que el SOC español sea la referencia del Grupo para el sector industrial.

**La postura de seguridad de una organización precisa de una composición equilibrada de controles y de una aproximación holística, adaptativa y automatizada. Y es ahí donde T-Systems presenta una propuesta diferenciadora.**



### Nube y autenticación biométrica

En su portafolio también ha puesto el foco en la protección de la nube permitiendo que el cifrado de la información de cualquier cliente "se produzca dentro de un entorno controlado por él, de manera que en ningún momento ni la clave de cifrado ni el dato en claro sean expuestos". Además, en 2020 ofrecerá una nueva herramienta para mejorar la seguridad del dato en este entorno.

La filial española también tiene una gran presencia en el sector bancario y financiero donde se ha incrementado la demanda de servicios de autenticación tras la entrada en vigor, en septiembre, de la directiva europea PSD2. Para dar respuesta a esta demanda ha desarrollado una solución puntera de autenticación con biometría del comportamiento a través del teclado.

Por último, también ofrece reforzar la seguridad del llamado 'eslabón más débil': las personas. Para ello dispone de un programa completo de concienciación y formación, basado en técnicas de 'gamificación' con una probada eficacia de asimilación por parte de los empleados.

Actualmente, T-Systems cuenta en España con clientes en el sector privado y público entre los que destacan desde **Seat** hasta la **Generalitat de Cataluña** y el **Defensor del Pueblo** (la información crítica de esta última entidad se protege desde el SOC con un enfoque extremo a extremo). Por supuesto, desde Iberia también se dan servicios a clientes globales de todo el mundo participando en proyectos innovadores de ciberseguridad en los que toma parte el Grupo y a los que también aporta, desde 2019, la tecnología que se desarrolla en el nuevo **BCN Innovation Lab**, en Barcelona.

## UN SOC NACIONAL CON CAPACIDADES GLOBALES

El SOC en Madrid de T-Systems, reforzado en capacidades y servicios desde 2018 tras su conexión con la red global de la compañía, se basa en la premisa de que cuanto mayor es la red, mejor será la información que aporte y, por tanto, se podrá ofrecer un mejor servicio. Desde él se ofrecen servicios de gestión automatizada de *malware*, '*red team*' y respuesta a incidentes, con el respaldo de la mayor empresa de telecomunicaciones en Europa.

## VUMES: UN ENFOQUE DE SERVICIO DE SEGURIDAD AUTOMATIZADA Y RETROALIMENTADA

Entre los servicios más novedosos de T-Systems cabe destacar, en España, su herramienta **VUMES** (**V**ulnerability **M**anagement **E**xpert **S**ystem). Se trata de una solución que gestiona el ciclo de vida completo de las vulnerabilidades. Para ello emplea un enfoque de servicio automatizado, retroalimentado y adaptativo y utiliza tecnologías avanzadas de IA, *Machine Learning* y respuesta automática a incidentes. Además, permite medir la ejecución de cada una de las fases del proceso:

**1. Categorización y agrupación de activos.** Se realiza un inventario automático y manual de los activos y la valoración de los mismos en las distintas dimensiones de la seguridad: integridad, confidencialidad y disponibilidad. Así, se priorizan los activos más críticos afectados.

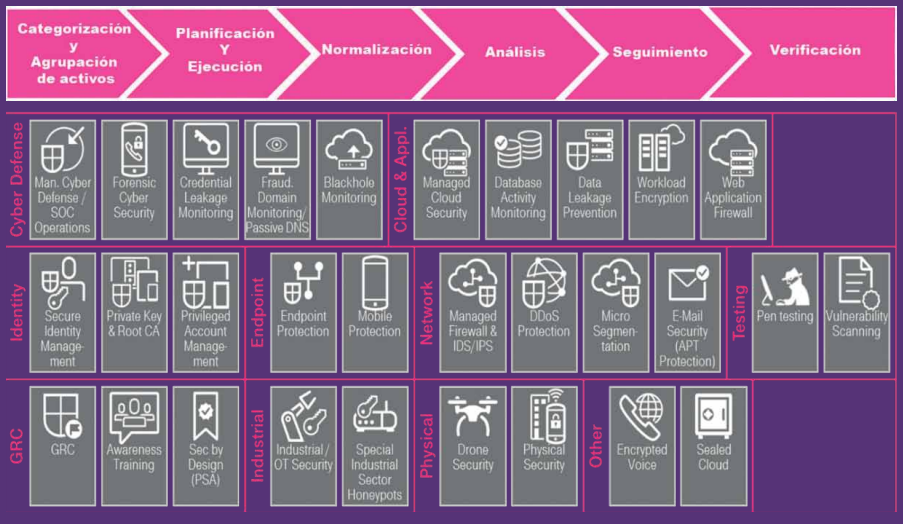
**2. Planificación y Ejecución.** Se trabaja de forma coordinada entre los responsables de servicio del SOC y del cliente. ¿El objetivo? Que ambas partes acepten, de manera explícita, un documento de planificación.

**3. Normalización de resultados.** Se normalizan los resultados obtenidos, se cargan y se procesan con la herramienta de Análisis VUMES, que se alimenta de los escaneos de vulnerabilidades de la compañía y de su inteligencia de amenazas.

**4. Análisis de impacto de las vulnerabilidades.** Para ello se emplea el sistema estándar CVSS v2, de cálculo de riesgos.

**5. Realización del seguimiento, la planificación y la trazabilidad de la aplicación** de las medidas correctoras propuestas. Así, las acciones correctoras también se integran en el proceso de Gestión del Cambio del cliente.

**6. Verificación.** Dado que el proceso de gestión de la vulnerabilidad es continuo, finalmente se comprueba que el cambio aplicado ha corregido la vulnerabilidad detectada. De no ser así, pasará por un nuevo ciclo.



# SECURITY

T · · makes it work.

T · · Systems · Let's power higher performance