esadealumni

ADVANTIO

ADVENS

AUBAY

CHECK.WEBSITE

FACTUM

IEAISA

INCIDE

IPM, A RICOH COMPANY

LISOT

OPTIMUMTIC

SECDAT

SEVEN SECTOR TECHNOLOGIES

ZEROLYNX

Especial
Ciberseguridad para empresas 2023

La creciente relevancia de la ciberseguridad para empresas

Si bien las capacidades y la conciencia alrededor de la ciberseguridad parecen estar mejorando, desafortunadamente la amenaza y la sofisticación de los ataques cibernéticos también aumentan.

En nuestro entorno digital actual, cada empresa es ahora un objetivo alcanzable, y cada empresa, grande o pequeña, tiene operaciones, marca, reputación y canales de ingresos que están potencialmente en riesgo. Los sistemas de seguridad informática trabajan con el principal objetivo de brindar protección a las entidades ante el riesgo de sufrir ciberataques que hagan peligrar el negocio, siendo igual de importante la regulación para aplicar esas medidas.

La IA, aparte de jugar en nuestro beneficio, también supone infinitos peligros que en su mayoría desconocemos, puesto que sigue siendo una ciencia muy reciente y desconocida para su tratamiento regulado y para la adaptación humana, por lo que supone una gran amenaza a la seguridad tanto de personas jurídicas como físicas.

Gracias a la tecnología es posible acelerar, automatizar procesos y reducir riesgos, pero al fin y al cabo son las personas quienes ejecutan dichos procesos. Por lo tanto, la concienciación es esencial en cualquier empresa.

INVERTIR Y PREVENIR

Por ello, la inversión en prevención es clave. Hay que dar un paso más allá en la formación y concienciación de los empleados, buscando generar una cultura de ciberseguridad que sea capaz de transformar el comportamiento en sí, de manera que se interioricen los conceptos y se logre la adquisición de nuevas habilidades y hábitos seguros en el uso de la tecnología y de la información. La capacitación especializada para los integrantes de los equipos de seguridad para mantenerse actualizados y así poder proteger a la organización ante las nuevas amenazas y riesgos que evolucionan cada día también es esencial.

Las organizaciones deben abordar el desafiante campo de la ciberseguridad mediante sistemas que combinen adecuadamente múltiples capas o niveles de seguridad, proporcionando así diversos mecanismos de detección. Para conocer más a fondo todos estos aspectos, entrevistamos a expertos del sector sobre los riesgos y también las oportunidades con las que se enfrentan en el día a día.

Para el 2025 se estima que la falta de conocimiento y el error humano serán los principales causantes de más de la mitad de los incidentes cibernéticos más significativos. ¿Cómo pueden las empresas prepararse frente a esta situación?

Si bien las capacidades y la conciencia alrededor de la ciberseguridad parecen estar mejorando, desafortunadamente la amenaza y la sofisticación de los ataques cibernéticos también aumentan.

FRANCISCO JURADO (PDC '18)

Business Development Director de IEAISA

"Desde IEAISA recomendamos que se tomen medidas ahora y no esperar a ser parte del % de empresas que se han usado para la estadística. Para minimizar al máximo este factor de riesgo, dentro del plan estratégico de ciberseguridad de la empresa tendríamos que incluir, por una parte, una formación continua sobre ciberseguridad para los empleados; por otra, y muy recomendable, una solución de concienciación que regularmente realice ataques simulados para poder evaluar el nivel de mejora y la evolución con el paso de los meses. Finalmente, habría que diseñar un plan específico para los grupos o usuarios que se vea que tienen más dificultades".

ROSA ORTUÑO

CEO de OptimumTIC

"Consideramos vital contar con programas de concienciación con el objetivo de formar y preparar al personal y de esta manera mantenerlos actualizados y educándolos hacia mejores prácticas, con conocimiento del uso continuo que hace de las tecnologías como es su 'smartphone', IoT en las casas, etc., y asegurando la privacidad por defecto, pudiendo elegir entre funcionalidad y/o practicidad-seguridad, pero siempre con conocimiento. La seguridad absoluta no existe y el error humano es algo inevitable, pero con la educación, formación continua y la concienciación se reducirá el impacto de los ciberdelitos, mitigaremos el riesgo y habrá menor pérdida de información y económica, y, en última instancia, mejor reputación ante los clientes y/o sociedad, creando un perímetro estable y seguro".

JOSÉ LUIS DÍAZ

CEO Advens Iberia

"Las empresas deben seguir preparándose para hacer frente a un ciberataque. Es necesario tener un SOC para detectar y reaccionar. Pero dada la naturaleza de los ataques, el factor humano debe volver a situarse en el centro de la ciberseguridad. Es fundamental concienciar a todos y ayudar a los usuarios a tener los reflejos adecuados. La conciencia es esencial. No podemos olvidarnos de los usuarios y sus roles en la ciberdefensa. Todos deben contribuir a ser el eslabón más fuerte de la cadena".

HIRAM FERNÁNDEZ

CEO de Seven Sector Technologies

"Las ciberamenazas son cambiantes, y las soluciones que has adoptado hace tiempo deben ir adaptándose. Es por ello que se necesita contemplar en tu estrategia un sistema de Detección Temprana de Amenazas y la Respuesta Extendida (XDRNet). El punto de la seguridad ofensiva es algo que hasta ahora no se estaba usando y nos permite incluso automatizar acciones o estrategias frente a los distintos tipos de amenazas. Necesitamos un sistema de Detección Temprana de Amenazas y Respuesta Extendida basado en XDR pero a nivel de red, es decir, un XDRNet que permita bloqueos de amenazas en cualquier entorno sin necesidad de desplegar software. Cada vez son más los entornos donde no podemos instalar agentes (IoT/OT/Cloud). Necesitamos un sistema que incluya los sensores, actuadores, PLC, etc., y no los dejemos atrás".

Se espera que el fraude causado por la inteligencia artificial cambie el tipo de los ataques a las empresas. ¿Están las empresas suficientemente sensibilizadas y mentalizadas para este tipo de amenazas y sus graves consecuencias?

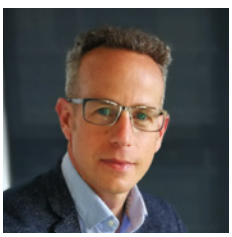
Implementar medidas de protección avanzadas y estar al tanto de las últimas amenazas y técnicas utilizadas por los atacantes son estrategias esenciales para mantenernos seguros en un entorno digital cada vez más complejo y sofisticado".

ABRAHAM PASAMAR

CEO de INCIDE

"Por naturaleza, los seres humanos tienden a ser bastante confiados. Cuando alguien de nuestro entorno nos pide un favor o nos brinda información que nos genera confianza, solemos ser colaborativos y no desconfiar demasiado. Los atacantes cibernéticos explotan constantemente esta dinámica para llevar a cabo sus ciberataques, y las estadísticas demuestran que estos ataques están en aumento y son altamente lucrativos (como los ataques BEC o los fraudes del CEO). La inteligencia artificial, especialmente la capacidad de crear contenido sintético (audio y vídeo), ha añadido un elemento determinante para el éxito de los ciberataques.

Imaginemos que nuestro jefe nos convoca a una videollamada donde interactuamos con él viéndolo y escuchándolo. Si se comporta y habla de manera habitual y nos pide que realicemos una transferencia bancaria a una cuenta específica, ¿cómo puede el usuario promedio dudar de esa solicitud si la tiene frente a sus ojos? Este es solo uno de los muchos peligros que la inteligencia artificial aporta al ámbito de los ciberataques. Es fundamental comprender estos riesgos y estar preparados para hacerles frente".



DAVID LÓPEZ

Cybersecurity Product Specialist de IPM, a Ricoh Company

"La AI como ChatGPT está dando sus primeros pasos y ya puede hacer cosas increíbles. Pero, como ya ha pasado antes, esa tecnología en malas manos puede ser usada con fines maliciosos. Se podrán automatizar y perfeccionar los ataques, con lo que las empresas que no tengan soluciones que les permitan tener plena visibilidad de lo que ocurra no podrán protegerse. Soluciones XDR y SOC son necesarios en cualquier empresa de tamaño medio".

JUAN ANTONIO CALLES

CEO de Zerolynx

"La inteligencia artificial está siendo una revolución, y de sus capacidades se están ya beneficiando tanto los 'buenos', como los 'malos'. Los delincuentes están haciendo uso de ellas para aprender acerca de nuevas vías de ataque, vías de evasión o vías de exfiltración, mientras que los equipos de ciberdefensa están haciendo uso de ellas para mejorar la detección y contención. Sin embargo, la sensibilización es muy baja, y solo las empresas que más invierten están haciendo 'challenge' al problema. En esta batalla, los sectores financiero y asegurador son, sin duda, por necesidad de su negocio, los mejor preparados. Cualquier ciudadano, gracias a las herramientas proporcionadas por entidades como OpenAI o Microsoft, ya hace uso de IAs de forma cotidiana, por lo que las empresas y sus sistemas de seguridad no iban a ser menos. Si bien la IA ya había aterrizado hace algunos años en el sector cíber, en estos últimos meses el número de productos se ha disparado, por lo que los analistas empiezan a contar con herramientas de gran potencia que, sin duda, están y seguirán mejorando las capacidades de detección y respuesta".

Además de contar con la tecnología, ¿cómo de importante es la concienciación del equipo humano?

La formación y concienciación en ciberseguridad se define como un conjunto de medidas y prácticas con el objetivo de que los usuarios conozcan y apliquen una serie de iniciativas para ayudar a garantizar la seguridad de una organización. Un aspecto básico.

CÁSTOR TORRES (EMDB 20)

Founder and Managing Director de SECDAT

"Las soluciones tecnológicas son una de las capas de protección; sin embargo, son los empleados quienes interactúan diariamente con los sistemas y datos de la empresa y, por ende, el objetivo de ataque. La concienciación del equipo humano se traduce en la comprensión de las prácticas de seguridad, la identificación de posibles amenazas y la adopción de comportamientos seguros. Sigue siendo necesario capacitar y educar a los empleados sobre las mejores prácticas de ciberseguridad, como la gestión de contraseñas seguras, la identificación de correos electrónicos de 'phishing' y la protección de la información confidencial de la empresa. Para ello, hace falta un enfoque integral de seguridad donde cada individuo se convierte en un defensor activo en la organización".

IOSU ARRIZABALAGA

Fundador y CEO de Factum

"El rápido avance de las nuevas tecnologías accesibles para el público ha generalizado la idea de que, si una empresa cuenta con la tecnología adecuada, no es necesaria la intervención humana. Sin embargo, una herramienta avanzada no dispone de la capacidad de razonamiento que puede tener un equipo humano. Por ello, como CEO de una compañía de ciberseguridad, yo mismo me decanto por medidas de seguridad proactivas o automatizadas, siempre y cuando mi equipo cuente primero con la concienciación necesaria e indispensable para evitar errores humanos. No tendría sentido invertir en tecnologías avanzadas si mi equipo no está capacitado para manejarlas con seguridad. Es importante que la capacitación y la concienciación sobre seguridad informática sean una prioridad en todas las áreas de la empresa para garantizar la protección efectiva de nuestros sistemas y datos empresariales".

ANDREA-GIAIME BODEI

CEO de Check.Website

"En Check.Website, creemos que la tecnología y la concienciación del equipo humano deben ir de la mano para una ciberseguridad efectiva. Nuestro software ayuda a detectar vulnerabilidades y proporciona informes detallados, lo que puede ser una herramienta educativa valiosa para aumentar la concienciación del equipo humano. Al entender mejor las amenazas y vulnerabilidades, el equipo puede tomar medidas más informadas para proteger la seguridad de la empresa".

¿Cuáles son las novedades más importantes que nos deparan los sistemas de seguridad informática para las empresas a corto y medio plazo?

Más allá de disponer de las capacidades tradicionales de detección de reglas establecidas, podemos utilizar herramientas capaces de generar patrones de comportamiento de usuarios y activos de la organización.

MANEL GARCÍA (DIRECCIÓN Y GESTIÓN MARKETING 01)
Director Unidad de Negocio de Aubay Spain

"En el corto plazo, el primer reto, aunque pueda parecer obvio, es disponer de un listado completo de los activos de la empresa. Sin este paso previo, no es posible atajar las vulnerabilidades que se puedan presentar con el paso del tiempo. Ya existen productos en el mercado que generan y mantienen actualizado el inventario del parque de sistemas y dispositivos IT/OT/IoT, priorizando la criticidad de la política de actuaciones, dependiendo del valor al negocio. Ante la creciente complejidad de los sistemas TIC, especialmente aquellos basados en el 'cloud computing', existen soluciones basadas en inteligencia artificial. Tampoco debemos olvidarnos de las ventajas de utilizar fuentes de inteligencia colectiva, que nos permiten estar al día de nuevos riesgos que en poco tiempo puedan afectarnos. Por otro lado, a medio plazo, se empiezan a introducir los sistemas que permiten la automatización de la evaluación de los controles de seguridad, la respuesta autónoma ante diferentes tipos de ataques, avanzados algoritmos de cifrado y modelos de confianza cero".

MANUEL FERNÁNDEZ
Director para España, Portugal y Latam de Advantio

"Los servicios de respuesta a incidentes (MDR) incorporados en los SOC (Security Operation Centers) no son una gran novedad, pero sí lo son en términos de adopción por parte de las empresas. Es decir, muchas más empresas deberán optar por pasar de sistemas de defensa pasivos ('firewalls', 'endpoints', etc.) a sistemas de defensa operados activamente por expertos. Cuando una empresa se convierte en objetivo de un ataque, necesita un equipo de defensa que reaccione en tiempo real. Como indicaba anteriormente, a medio-largo plazo, la irrupción de la computación cuántica supondrá una revolución tecnológica sin precedentes, que indudablemente tendrá impacto a nivel de seguridad".

IGNACIO DE LA SOTILLA (CE&MBA 89)
CEO de Lisot

"Hay que implementar sistemas de autenticación multifactor para acceder a los sistemas informáticos. Si por error humano consiguen los datos de usuario y contraseña de acceso al sistema, si esta requiere una validación multifactor, no podrán acceder a los recursos informáticos. Los certificados y la firma digitales como herramienta de seguridad es otro complemento para securizar los sistemas informáticos. En la medida en que las empresas generalicen el uso de certificados digitales, aumentaremos la seguridad en las comunicaciones. Otro punto es el acceso a los datos a través de VPN (Virtual Private Network); estos sistemas nos aseguran el acceso desde el exterior a nuestros sistemas informáticos. Cabe implementar sistemas XDR (Extended Detection and Response), que se basan en la integración de datos de seguridad provenientes de diversos puntos de la infraestructura de una organización, como servidores, redes, sistemas en la nube y registros de aplicaciones".

Su socio de confianza en ciberseguridad

ADVANTIO

Dirección postal:
Alfonso XII, 62, planta 2, 28014, Madrid
Teléfono: +34 91 076 70 92
E-Mail: spain@advantio.com
Web: www.advantio.com

PERSONAS DE CONTACTO

Director para España, Portugal y Latam de Advantio: Manuel Fernández López

Fundada en 2009, Advantio es una compañía que combina servicios profesionales (QSA PCI, ISO27001, SWIFT), tecnología (Risk Score, PCI Portal) y servicios de seguridad gestionados (MDR, SOC), todo ello con soporte multilingüe para proporcionar una solución de seguridad completa a organizaciones globales. Advantio ha sido reconocido por VISA como el segundo principal proveedor QSA en Europa. Las certificaciones de su equipo de seguridad abarcan, entre otras, toda la familia PCI junto con certificaciones de seguridad ISO. Especializados en securizar las transacciones de datos de pago, Advantio se ha convertido en el socio de seguridad preferido de muchas grandes corporaciones y empresas a nivel mundial, cubriendo una amplia gama de industrias, (banca, seguros, *gambling*, viajes, comercio minorista, telecomunicaciones, petróleo, gas y el sector público, entre otras).

Los experimentados equipos para pruebas técnicas y de seguridad de Advantio abarcan proyectos como revisión de código seguro, análisis completo y seguro del ciclo de vida del desarrollo de software (SDLC) y la ejecución fase por fase de los servicios de pruebas de penetración.

Advantio se enorgullece de proporcionar un servicio de clase mundial con su compromiso de entrega "A tiempo y dentro del presupuesto". Nuestros equipos se esfuerzan por involucrar al cliente en todas las etapas del proyecto para facilitar el diálogo abierto y ayudar al cliente a lograr sus objetivos de seguridad y cumplimiento.

PRODUCTOS Y SERVICIOS

- Servicios profesionales de consultoría y certificación en toda la familia PCI para medios de pago por tarjeta (PCI DSS, PCI PIN, PCI 3DS, PCI P2PE, PCI SSF y Secure SLC , PCI TSP, PCI NESA, PCI Card Production).
- Servicios profesionales de consultoría y certificación para ISO 27001, 27701, 22301 SWIFT, ENS (Esquema Nacional de Seguridad), entre otros.
- Servicios profesionales técnicos de pruebas de seguridad:
  - Escaneos de vulnerabilidades internos y externos (incluyendo ASV Approved Scanning Vendor PCI).
  - Pruebas de penetración (Pen Tests).
  - Red team e Ingeniería social (*phishing*).
- Servicios de consultoría sobre nivel de madurez en ciberseguridad en las empresas.
- Servicios gestionados para aplicaciones seguras en la nube (MDR, SOC).
- Tecnología: Portal PCI ZeroRisk: Cumplimiento PCI de los comerciantes, Risk Score, Gestión centralizada de terminales de pago (inventario, seguridad y ciclo de vida).

VENTAJAS Y PUNTOS DIFERENCIALES

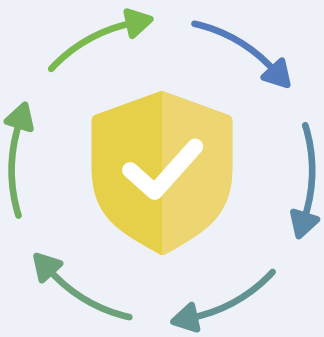
- Proyectos globales con reporte centralizado y entrega local en cada país e idioma. Perfecto para multinacionales.
- Experiencia enriquecida por equipos multinacionales.
- Compromiso de cumplimiento en plazos y costes comprometidos.
- Alta especialización en la ciberseguridad para entornos de banca, fintech y medios de pago.
- Asesores de clase mundial con muy alta reputación en la industria.
- Apoyo en el camino a la madurez en seguridad cibernética, más allá del cumplimiento normativo.
- Nuestra herramienta tecnológica ZeroRisk se ha ganado su relevante posición en el mercado por la capacidad de adaptarse a las necesidades específicas de cada adquirente o marca de distribución global.
- Nos avalan nuestros clientes, algunas de las empresa más importantes en industrias como banca, proveedores de servicios de pago, moda, alimentación...

ADVANTIO

Detección y respuesta ante Ciberataques

Nosotros defendemos tu negocio, tú lo haces crecer

Confía en nuestro servicio **MDR** (Managed Detection and Response), **especializado en compañías Fintech y Medios de Pago.** Detectamos, respondemos y detenemos ciber ataques en minutos gracias a nuestro Centro de Operaciones de Seguridad (SOC), disponible 24/7.



- Monitoreo y contención proactivos de amenazas 24x7
- SOC-as-a-service
- SIEM-as-a-service para gestión de logs y correlación
- Protección gestionada de endpoints
- Portal dedicado al cliente

ADVANTIO
MDR

Vigilancia de amenazas
24/7

Contacta ahora mismo con un experto en ciberseguridad

manuel.fernandez@advantio.com

+34 910 76 70 92

ADVANTIO.COM/ES/MDR

Ciberseguridad y compromiso: aDvens desembarca en España con una propuesta diferencial

Security for the greater good

ADVENS IBERIA

OFICINAS

Dirección postal: Paseo de la Habana, 9
28002 Madrid
Teléfono: +34 629 705 330
E-mail: jose-luis.diaz@advens.com
Web: www.advens.es

PERSONAS DE CONTACTO

Consejero Delegado: David Buhan
Director General: José Luis Díaz
Director Comercial: José Luis Díaz

Advens es una de las compañías líderes en ciberseguridad en Europa establecida en las bases de una alianza de conocimientos de vanguardia y un enfoque como servicio que busca conseguir brindar una experiencia global unificada. Proporcionamos servicios avanzados y resistentes que buscan proteger a nuestros clientes de las amenazas actuales y futuras. Nuestro principal objetivo es proteger a las organizaciones y a la sociedad de las ciberamenazas a través de servicios diferenciales y la excelencia en los mismos.

Aunque la propia ciberseguridad es la que consigue y permite que el mundo siga girando, nosotros buscamos actuar para convertirnos en una fuerza del cambio. Con nuestro crecimiento alcanzamos el intercambio de valor para fomentar este compromiso social.

Es por eso por lo que en Advens buscamos ir más allá y hemos creado un modelo de negocio innovador para cumplir con nuestro compromiso social a través de nuestra fundación Advens for People & Planet.

PRODUCTOS Y SERVICIOS

- MySOC: SOC-as-a-Service, Managed Detection & Response.
- Governance, Risk & Compliance consulting.
- Audit, Red & Team services.
- Technolgy integration and solutions management.
- CERT & Cyber threat intelligence.

VENTAJAS Y PUNTOS DIFERENCIALES

- Reunimos los conocimientos necesarios para definir y elaborar su hoja de ruta en materia de ciberseguridad y disponemos de los servicios de protección necesarios para mantener y mejorar su nivel de seguridad.
- Esta combinación de 360 grados y un enfoque de "seguridad como servicio" garantiza una protección óptima en todo momento.
- Un proyecto empresarial que va más allá de la Ciber gracias a una fundación que aprovecha nuestro desempeño económico para ayudar a las personas y al planeta.

SEE MORE.
STOP MORE.

24/7 Managed Detection & Response para todos sus entornos.

mySOC®
by Advens

END-POINTS NETWORK CLOUD APPLICATIONS OT/IOT

Nuestro servicio mySOC® protege todos sus entornos, proporcionándole una visibilidad completa de sus riesgos, vulnerabilidades y amenazas externas.

Nuestros analistas utilizan nuestra plataforma mySOC Open XDR para prevenir, detectar y responder a los incidentes de seguridad con usted en tiempo real.

Descubra nuestros servicios en www.advens.com

Tu socio en Ciberseguridad y Ciberinteligencia

AUBAY

OFICINAS

Dirección postal:
Doctor Zamenhof, 36 duplicado. 28027 Madrid
Ronda Sant Pere, 52, 3ª planta. 08010 Barcelona
Teléfonos: 91 326 92 70/ 93 445 68 00
E-mail: recepcion@aubay.es
Web: https://www.aubay.es/

PERSONAS DE CONTACTO

Presidente: Gérard Lucente
Director Alianzas: Alberto Sánchez
Director Business Unit: Manel Garcia

Aubay es un referente internacional en transformación digital, acompañando a nuestros clientes en los proyectos tecnológicos más ambiciosos.
Respaldados por un equipo de 7.800 apasionados consultores, contamos con una combinación única de profundos conocimientos empresariales y habilidades tecnológicas.

La explosión del uso de sistemas de información cada vez más complejos y distribuidos ha aumentado considerablemente los riesgos de ciberataques.
La generalización del teletrabajo en los últimos años no ha hecho sino amplificar estas nuevas amenazas.
Desde la definición de una arquitectura más segura, la inclusión de criterios de seguridad en los proyectos, auditoría, vigilancia de la seguridad, sensibilización de sus equipos humanos y ecosistema de *partners* de negocio, hasta la metodología para mejorar en su postura de ciberseguridad... Aubay le acompaña en la definición y aplicación de una política global que le permitirá alcanzar un alto nivel de resiliencia y proteger su empresa.

PRODUCTOS Y SERVICIOS

- Consultoría de Gobernanza, Riesgos y Cumplimiento.
- Servicios de Ciberinteligencia y Forenses.
- Implementación Plataformas SIEM.
- Seguridad de proyectos y desarrollo.
- Arquitectura segura.
- Auditorías / *pentesting*.

VENTAJAS Y PUNTOS DIFERENCIALES

- Amplio equipo de profesionales especializados.
- Alianzas con los principales fabricantes del sector.
- Servicios de proximidad con alto nivel de especialización.
- Alto nivel de certificaciones profesionales.
- Compañía multinacional con centros distribuidos geográficamente.

aubay
ahead of innovation

UTILISE
our curiosity
17 offices in 7 countries

HARNESS
our expertises
10 excellence fields

ANTICIPATE
Tech Trends
7000 employees

#CIBERSECURITY

#BIGDATA

#BLOCKCHAIN

#AI / ML

#CONSULTING

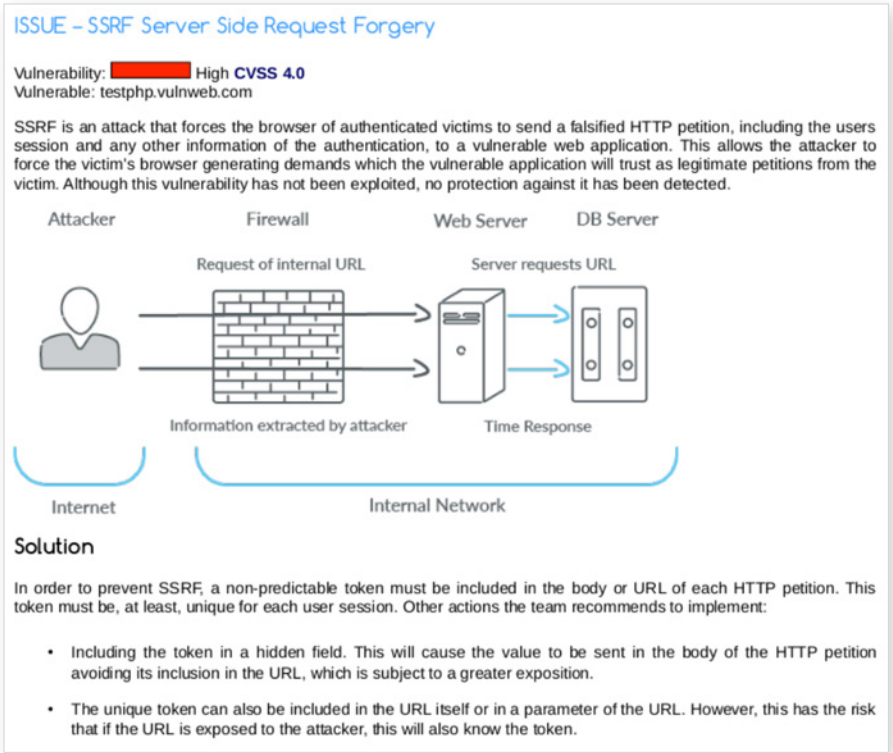
#INNOVATION

#INDUSTRY4.0

aubay
ahead of innovation

splunk> DARKTRACE ivanti LACEWORK

Verifica si tu web está segura con Check.Website



CHECK.WEBSITE

OFICINAS
E-mail: info@andreabodei.com
Web: https://check.website

PERSONAS DE CONTACTO
CEO: Andrea-Giaime Bodei

En la era digital, la seguridad de las páginas web es primordial debido a las amenazas cibernéticas. Check.website, plataforma de seguridad web, proporciona protección integral contra estas amenazas. Su software realiza análisis exhaustivos, identificando vulnerabilidades y generando informes detallados.

Check.website garantiza una defensa sólida para tu sitio web, brindando confianza y tranquilidad. Independientemente de si tienes un negocio en línea, un blog personal o un *e-commerce*, su servicio es esencial. En resumen, Check.website es tu solución para la seguridad web, permitiéndote identificar y solucionar vulnerabilidades. Confía en Check.website para mantener tu página segura constantemente.

PRODUCTOS Y SERVICIOS

- Plataforma especializada en seguridad web.
- Software avanzado para realizar análisis exhaustivos.
- Escaneo completo y evaluación de vulnerabilidades en páginas web.
- Generación de informes detallados sobre debilidades de seguridad.
- Protección contra ataques cibernéticos.
- Solución integral para proteger la seguridad de páginas web.

VENTAJAS Y PUNTOS DIFERENCIALES

- Identificación y evaluación exhaustiva de vulnerabilidades.
- Informes detallados que permiten conocer las debilidades de seguridad.
- Protección sólida contra posibles ataques cibernéticos.
- Enfoque automatizado que garantiza una detección precisa de vulnerabilidades.
- Solución confiable para proteger páginas web en diferentes contextos (negocios en línea, blogs personales, plataformas de comercio electrónico...).

¡Verifica si tu web está segura! check.website

¡Prueba nuestro software automático de seguridad web hoy mismo!

Si tienes un sitio web, sabes lo importante que es la seguridad. Pero, ¿cómo puedes estar seguro de que tu sitio está protegido? Los hackers pueden atacar tu sitio web de muchas maneras. Puede ser difícil detectar vulnerabilidades por tu cuenta, pero ahora hay una solución. Nuestro software automático de seguridad web puede realizar un escaneo completo de tu sitio web en solo unos minutos y detectar todas las vulnerabilidades. El software comprueba automáticamente la seguridad de tu sitio web y te proporciona un informe completo de cualquier vulnerabilidad encontrada. Con nuestro software, puedes estar seguro de que tu sitio web está protegido contra cualquier amenaza cibernética. No arriesgues la seguridad de tu sitio web.

https://check.website

Solo aquellos que no están preparados tienen miedo

FACTUM

OFICINAS

Dirección postal:
Doctor Zamenhof, 36 Bis, 1ª planta
28027 Madrid
Teléfono: 913 52 44 79
E-mail: info@factum.es
Web: www.factum.es

PERSONAS DE CONTACTO

Fundador y CEO: Iosu Arrizabalaga Cortabarría
iosu.arrizabalaga@factum.es

Factum es una compañía española participada por Banco Santander especializada en soluciones de ciberseguridad para empresas. Nació en 2009 y actualmente cuenta con más de 140 especialistas que proporcionan servicio a más de 200 clientes a nivel internacional.

La alianza estratégica con proveedores líderes globales en tecnología de ciberseguridad, así como la eficacia y profesionalidad de su equipo de especialistas, ha dado lugar a un rápido crecimiento que se ha materializado en la gestión de 600.000 dispositivos en más de 60 países.

En un mundo cada vez más tecnológico en el que la digitalización de las empresas y las administraciones se ha convertido en una necesidad, Factum trabaja fusionando innovación y talento para conseguir que la seguridad cibernética sea un derecho al que todos los usuarios tengan acceso de una forma fácil y sencilla.

PRODUCTOS Y SERVICIOS

Auditoría Técnica: comprueba la postura de seguridad técnica de una organización mediante pruebas de penetración y tests de intrusión.

Virtual CISO: lidera y supervisa la estrategia de seguridad de la información y ciberseguridad de la empresa.

Plan Director de Seguridad (PDS): establece una hoja de ruta clara y coherente para el desarrollo, implementación y mejora continua de las medidas de seguridad de la información en una organización.

Protección de la Información: se refiere a las medidas y acciones tomadas para salvaguardar la confidencialidad, integridad y disponibilidad de la información frente a ataques.

Protección de la Red: mantiene la higiene de la red, controlando el acceso de cualquier dispositivo, tanto interno como externo.

MDR (Managed Detection and Response): permite identificar amenazas en base a fuentes predefinidas en los principales vectores de compromiso. Su capacidad para combinar sistemas, plataformas, aplicaciones y entornos facilita el proceso de monitorización unificada 24/7 y reacción temprana.

EDR (Endpoint Detection and Response): detecta y responde rápidamente ante amenazas avanzadas, identificando el comportamiento anómalo de los dispositivos finales.

VENTAJAS Y PUNTOS DIFERENCIALES

- Compañía con 14 años de experiencia en el sector.
- Equipo formado por más de 140 especialistas.
- Empresa participada por Banco Santander.
- Presencia y prestación de servicios en el ámbito nacional e internacional.
- Personalización de los servicios adecuados a las necesidades específicas.
- Colaboración con el Instituto Nacional de Ciberseguridad (INCIBE) y el Centro Criptológico Nacional (CCN) para garantizar la consonancia de nuestros servicios con la actualidad cibernética.
- Cumplimiento de la normativa ISO 27001, ISO 14001 y ISO 9001.
- Posibilidad de contratar el servicio integral o servicios modulares.

FACTUM

Cybersecurity

Auditorias técnicas · Adecuación a marcos normativos

Análisis de vulnerabilidades · Pentesting · EDR

Protección de la red · Protección de la información

Plan Director de Seguridad · Ciso virtual · MDR

+200 clientes en el mundo +130 especialistas +14 años de experiencia

Soluciones tecnológicas 360º a la medida de nuestros clientes

IEAISA

OFICINAS

Dirección postal: Calle Dels Pous, 20
08740 Sant Andreu de la Barca
Barcelona
Teléfono: +34 93 682 57 88
E-mail: ieaisa@ieaisa.com
Web: www.ieaisa.es

PERSONAS DE CONTACTO

CEO: Julian Martos
CEO: Paco Escane
Business Development Director PDC 2018: Francisco Jurado

IEAISA fue fundada en el año 2000 con el claro objetivo de poder cubrir las necesidades en materia tecnológica de empresas de todos los tamaños y sectores. Nuestra misión se centra en ofrecer soluciones tecnológicas de alto valor añadido y en acompañar a nuestros clientes muy estrechamente durante todo el proceso de toma de decisión. Es para nosotros un orgullo poder decir que somos una de las pocas empresas de IT con capacidad para poder ofrecer una solución extremo a extremo con recursos totalmente propios.

En el ADN de IEAISA, se encuentra una fuerte vocación por diseñar soluciones a la medida del cliente y acompañarle durante toda su trayectoria ayudándole con el diseño continuo de su estrategia digital.

Las diferentes áreas de negocio en las que centramos nuestras soluciones son: infraestructuras físicas, ciberseguridad y normativa, telecomunicaciones y *networking*, *cloud computing*, sistemas de alta disponibilidad para el Data Center, copias de seguridad y continuidad de negocio, además de servicios profesionales de consultoría y gestión de los sistemas.

ÁREAS DE PRÁCTICA

- **CIBERSEGURIDAD** – Auditorías, sistemas de protección perimetral, en la nube y del puesto de trabajo, sistemas de acceso remoto.
- **CLOUD COMPUTING** – Soluciones de *cloud* privado y público.
- **INFRAESTRUCTURAS** – Instalación de sistemas de comunicaciones y CPDs.
- **NETWORKING** – Soluciones de comunicación tanto para oficinas como entre sedes.
- **DATA CENTER** – Virtualización, alta disponibilidad de los datos, copias de seguridad y continuidad de negocio.
- **SERVICIOS PROFESIONALES** – Consultoría, instalación y mantenimiento de sistemas.

PRODUCTOS Y SERVICIOS

- *Firewalls*.
- Sistemas de acceso remoto
- Vpn *(virtual privat network)*
- Seguridad del *end point*
- Auditorías de ciberseguridad
- Servidores virtuales
- Escritorios virtuales
- Almacenamiento *cloud*
- Sistemas de correo electrónico
- Instalaciones de cableado estructurado y fibra óptica
- Instalación de centros de datos (cpds)
- Sistemas de comunicaciones LAN *(local area network)*
- Sistemas de comunicaciones WAN *(wide area network)*
- Sistemas de hiperconvergencia
- Servidores de misión crítica
- Soluciones de *storage*
- Virtualización
- *Backup* y *disater recovery*
- Servicios de mantenimiento 360
- Servicios de consultoría
- Servicios de instalación

IEAISA
INGENIERÍA

IEAISA Ingeniería
Soluciones y servicios TIC

CIBERSEGURIDAD

Auditorías, Sistemas de protección perimetral, en la nube y del puesto de trabajo, Sistemas de acceso remoto, Análisis forense, protección frente a estafas y suplantación de identidad

CLOUD COMPUTING

Soluciones de Cloud privado y público y escritorios Virtuales como servicio

INFRAESTRUCTURAS

Instalación de sistemas de comunicaciones y CPDs

NETWORKING

Soluciones de comunicación WIFI, LAN y WAN para empresas y entre sedes

DATA CENTER

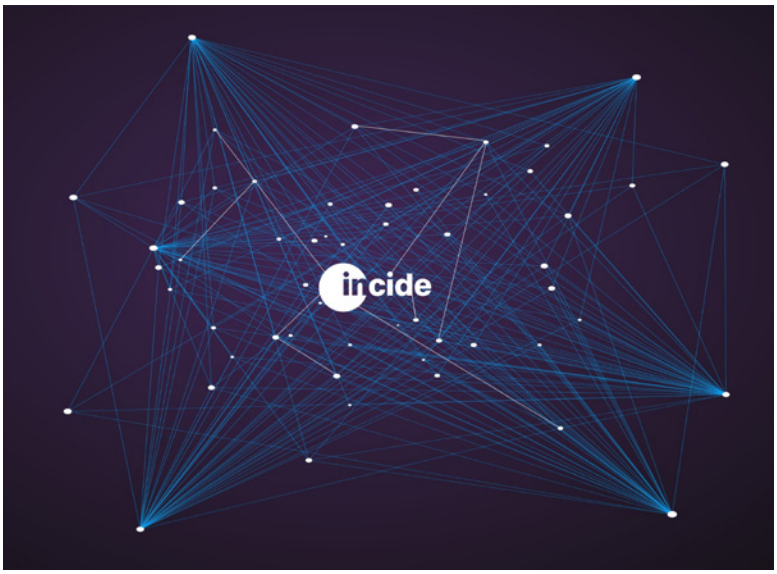
Virtualización, alta disponibilidad de los datos, copias de seguridad y continuidad de negocio

SERVICIOS PROFESIONALES

Consultoría, instalación y mantenimiento de sistemas informáticos

www.ieaisa.es

Expertos en servicios de alto valor añadido



INCIDE

OFICINAS

BARCELONA
Avenida Diagonal, 622, 7A - 08021 Barcelona

MADRID
C/ Miguel Yuste, 6, 2º C - 28037 Madrid

Teléfono: 93 254 62 77
E-mail: info@incide.es
Web: www.incide.es

PERSONAS DE CONTACTO

CEO de Incide: Abraham Pasamar
Security Assessment Department Manager: Carlos Fernández
Detect & Respond Department Manager: Cristina Roura

Desde 2005, en INCIDE nos enfocamos en la ciberseguridad y protección de la información. Nuestra experiencia en gestión de incidentes nos permite ofrecer una protección integral y eficaz de activos digitales.

Nuestro equipo realiza un exhaustivo análisis de los incidentes con el objetivo de identificar el vector de entrada y las acciones ejecutadas por los atacantes. Nos enorgullece ofrecer informes forenses detallados que proporcionan una visión clara de los eventos ocurridos, así como informes de recomendaciones para fortalecer la seguridad. Nuestro compromiso es brindar un análisis minucioso que permita comprender y abordar de manera efectiva las amenazas, proporcionando a nuestros clientes las herramientas necesarias para fortalecer su postura de seguridad.

Ofrecemos soluciones gestionadas y monitoreo constante para proteger los activos. Mediante nuestro equipo experto en *pentesting, red teaming* y *purple teaming* identificamos vulnerabilidades y fortalecemos la seguridad. Mantenemos alianzas estratégicas y seguimos las últimas tendencias en ciberseguridad. Con experiencia en informes forenses, gestión de incidentes, auditorías y servicios gestionados de seguridad, brindamos confianza en la protección de activos digitales en un mundo digital en constante evolución y cambio.

PRODUCTOS Y SERVICIOS

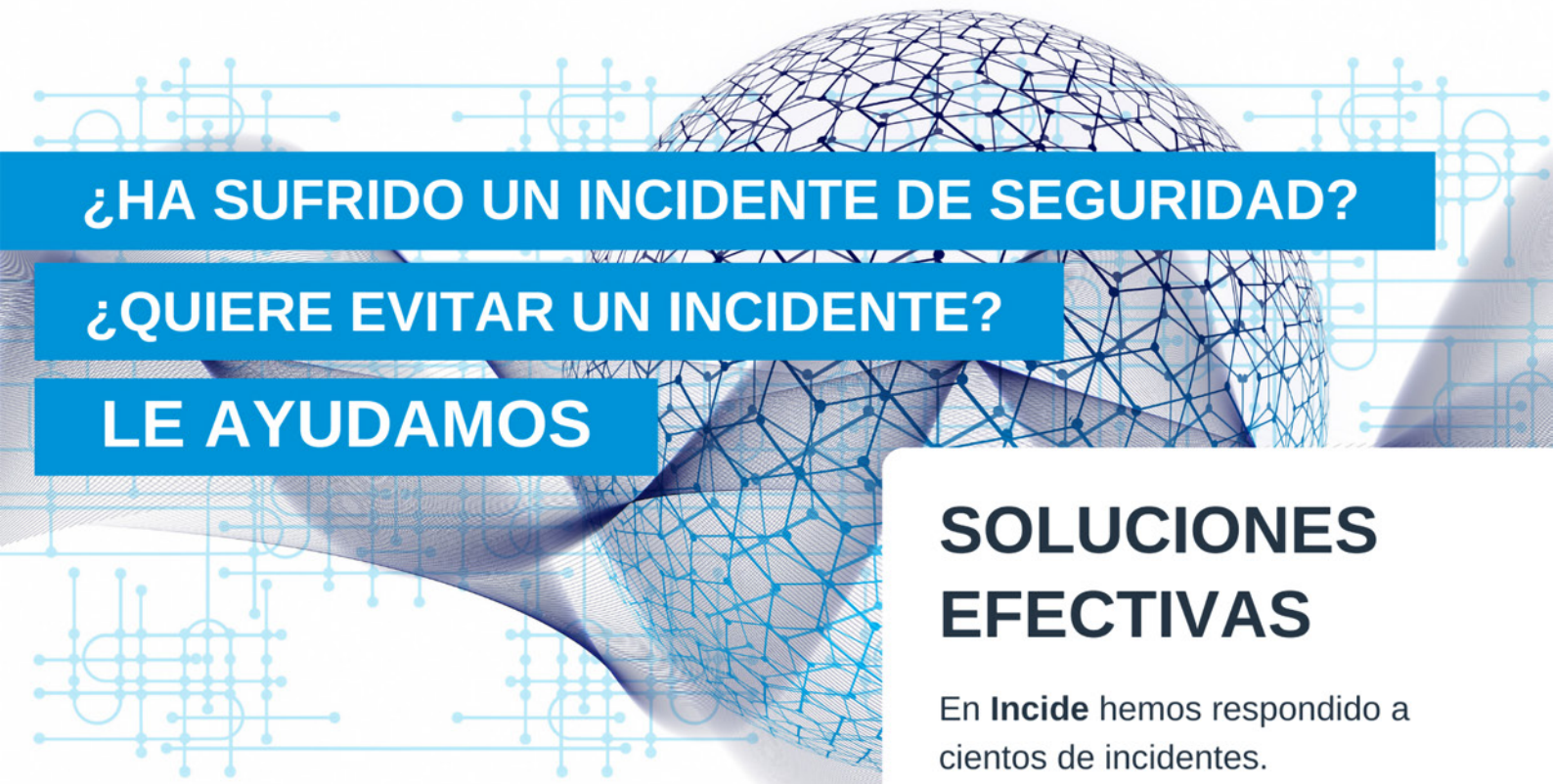
En INCIDE, el Blue Team (Detect and Respond) y el Red Team (Security Assessment) colaboran para ofrecer una protección completa y proactiva en seguridad digital. El Blue Team gestiona incidentes, realiza Threat Hunting, Detection Engineering, Compromise Assessment y Análisis Forense. El Red Team evalúa riesgos, realiza simulaciones adversariales y *pentests*. Ambos equipos colaboran en el Purple Team para brindar servicios gestionados de alta efectividad como MDR, MTD, ITE y MTI.

VALOR AÑADIDO INCIDE

- Más de 4000 horas anuales en incidentes.
- Intervenciones en más de 10 países.
- Servicios recurrentes con clientes IBEX35.
- Más de 6 años de experiencia en Penetration & Red Team.
- Reproducción de más de 30 amenazas inminentes en 12 meses.

incide

SOLUCIONES DE CIBERSEGURIDAD



¿HA SUFRIDO UN INCIDENTE DE SEGURIDAD?

¿QUIERE EVITAR UN INCIDENTE?

LE AYUDAMOS

SOLUCIONES EFECTIVAS

En **Incide** hemos respondido a cientos de incidentes.

Conocemos los procedimientos y técnicas que utilizan los atacantes y podemos evaluar y mejorar las capacidades de detección y respuesta.

SERVICIOS DFIR

Respuesta a Incidentes, Análisis Forense, Threat Hunting, Detection Engineering

SERVICIOS DE ASSESSMENT

Evaluación de riesgos, Penetration Test y **Simulación Adversarial**

SERVICIOS GESTIONADOS

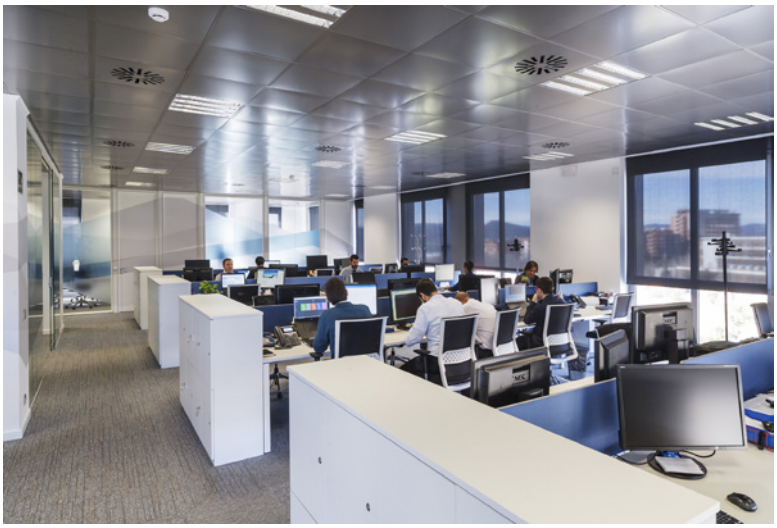
Managed Detection ad Response, Managed Threat Intelligence, Managed Threat Detection, Imminent Threat Exposure

¡PROTEGE A TU EMPRESA DE LOS CIBERATAQUES!

Contacta con nosotros

Avenida Diagonal 622, 7 A, C.P. 08021 Barcelona www.incide.es info@incide.es 932546277

IPM, a Ricoh Company, una compañía global



IPM, A RICOH COMPANY

OFICINAS

Dirección postal: Av. Barcelona, 115
08970 (Sant Joan Despí) Barcelona
Teléfono: +34 934 770 436

PERSONAS DE CONTACTO

Cloud Specialist - BDM for Cloud|Workplace| Security|ModernApps: Raúl Coria
Cybersecurity Product Specialist: David López
Modern Data Center and CIL Manager: Juan Manuel López
Digital Workplace Specialist: Manuel Gil
Managed Services Manager: Ramón Garrigosa

Con más de 40 años de experiencia en el sector tecnológico, IPM, a Ricoh Company es una empresa española que proporciona soluciones y servicios transversales de TI a medianas y grandes organizaciones.
Perteneciente al Grupo Ricoh desde 2019, junto al cual acompaña a sus clientes en todo el proceso de digitalización, logrando una óptima gestión de la estrategia TI con una cobertura *end to end*.
El alcance de los servicios abarca desde las labores de asesoramiento, consultoría y diseño, hasta proyectos de implantación y mantenimiento proactivo de servicios gestionados en estas cinco áreas: Hybrid Cloud, Cyberseguridad, Modern Data Center, Modern Apps y Digital Workplace.
La metodología de IPM se adapta a cada empresa para garantizar una transición efectiva y segura en todo el proceso de modernización, con proyectos de digitalización en cualquier país del mundo.

NUESTRAS SOLUCIONES

Hybrid Cloud
Combinamos todas las funcionalidades de tu Data Center con las ventajas de la nube pública para modernizar y gobernar de forma unificada todos tus servicios *cloud*.

Modern Apps
Incrementamos tu competitividad e innovación con Modern Applications, gestionando el ciclo de vida de forma ágil y adaptándolas a las necesidades de tu negocio.

Modern Data Center
Habilitamos y desarrollamos las infraestructuras modernas para obtener los beneficios de la tecnología actual y futura.

Cybersecurity
Minimizamos el riesgo para garantizar la seguridad de la información, los servicios y los datos corporativos.

Digital Workplace
Mejoramos la experiencia de los usuarios y aumentamos su productividad y seguridad con una gestión flexible y automatizada del entorno de trabajo.

Managed Services
Optimizamos tus servicios gestionados mediante la automatización, reduciendo costes, garantizando la calidad del servicio y aumentando la disponibilidad de los equipos contratados.

Soluciones y servicios **para acelerar tu negocio**

POR QUÉ IPM, A RICOH COMPANY

- Calidad en el servicio
- Asesoramiento experto
- Innovación
- Soluciones que generan ventajas competitivas en nuestros clientes
- 8 de cada 10 clientes nos recomiendan
- Socios de las organizaciones más exigentes y exitosas del mercado

www.ipm.es

El valor de la experiencia, la pasión por el futuro

A RICOH Company

DELL Technologies TITANIUM PARTNER · vmware Principal Partner · VEEAM Value-Added Reseller Gold · TREND MICRO Gold Partner

Microsoft Partner Network · Google Cloud · aws partner network Select Consulting Partner · Quantum · HashiCorp

Ayudamos a las empresas a defenderse de los ataques en la jungla digital

LISOT

OFICINAS

Dirección postal: Casp, 118 - 08013 Barcelona
Teléfono: +34 93 266 24 03
E-mail: lisot@lisot.com
Web: www.lisot.com

PERSONAS DE CONTACTO

CEO: Ignacio de la Sotilla, CEO de Lisot CE y MBA'89

El mundo digital se ha convertido en una auténtica jungla: *hackers, phishing, malware*... Está lleno de amenazas frente a las cuales todos estamos expuestos. En Lisot ayudamos a las empresas a construir un entorno digital seguro y a prevenir, defenderse y recuperarse rápidamente en caso de incidencias o ataques.

Y es que la continuidad de un negocio depende de la seguridad y acceso a sus datos y a la tecnología.
¿Qué pasaría si por cualquier motivo fuera robada o no estuviera disponible la información o la aplicación con la que trabajas diariamente?
Las consecuencias supondrían un coste incalculablemente elevado para tu empresa.

Desde **Lisot** podemos implantar un **sistema de seguridad informática adaptado a las necesidades de tu empresa**. Disponemos de un equipo de técnicos especializados que pueden solucionar cualquier necesidad para que puedas realizar tu trabajo sin necesidad de preocuparte por ningún tema relacionado con la tecnología y que puedas estar tranquilo en la jungla digital.

SERVICIOS

- Configuración de sistemas de seguridad informática.
- Tareas y operaciones de mantenimiento de seguridad informática.
- Detección de amenazas de seguridad informática.
- Mantenimiento de ordenadores, redes y servidores.
- Asistencia técnica remota y presencial.
- Instalación, suministro y configuración de redes informáticas.
- Certificados digitales.

VENTAJAS Y PUNTOS DIFERENCIALES

- Especializados en mantenimiento técnico y ciberseguridad.
- Respuesta garantizada ante un incidente informático.
- Más de 30 años de experiencia en el sector.
- Disponible cuando lo necesitas.
- Adaptamos la tecnología a las necesidades de tu empresa.
- Rentabilizamos al máximo los recursos informáticos.
- Equipo de técnicos informáticos con amplia experiencia y formación continua.
- Un único interlocutor capaz de ofrecer soluciones en todas las áreas de la informática.

lisot

Ayudamos a las empresas a construir un **entorno digital seguro** y a **prevenir y defenderse de los ataques**

Los hackers siempre están al acecho

93 266 24 03 lisot@lisot.com https://bit.ly/lisot

Haciendo de tu Seguridad de la Información un activo estratégico

SECDAT

OFICINAS
Dirección postal:
María de las Mercedes de Borbón, 128, 4º
Teléfono: (+34) 647 426 472
E-mail: hola@secdat.es
Web: www.secdat.es

PERSONAS DE CONTACTO
Fundador: Cástor Torres
Business Developer: Carmen Ríos

Somos una consultora boutique líder en Gestión de la Seguridad de la Información y la Privacidad, brindando las gestión integral de las certificaciones y soluciones tecnológicas para que las empresas tomen el control total de la seguridad de sus activos más valiosos.
A medida que la tecnología se convierte en un elemento clave en las estrategias empresariales y los marcos regulatorios y las demandas de los gobiernos en cuanto a altos estándares de seguridad de la información se han vuelto cada vez más exigentes, la protección de la información empresarial se ha vuelto cada vez más compleja, lo que hace imprescindible gestionar de manera eficiente la ciberseguridad y la privacidad.
Aquellas organizaciones que puedan ofrecer garantías sólidas en estas áreas obtendrán una ventaja competitiva significativa. Sin una estrategia adecuada para la gestión de la ciberseguridad y la privacidad, incluso los mayores esfuerzos podrían llevar al fracaso.
Para ello es necesario generar una estructura sólida y una gestión adecuada, para poder garantizar la protección de sus activos más valiosos y diferenciarse en el mercado, adoptando un enfoque integral que abarque todas las áreas relevantes de la organización, incluyendo la tecnología para controlarlo.
Confíe en expertos en seguridad de la información para asegurar el éxito de su organización.

PRODUCTOS Y SERVICIOS

- **Certificaciones ISO:** consultoría, asesoría y auditorías legal y normativo. Abarcamos las más importantes normas de Seguridad de la Información y de Privacidad. Adicionalmente, brindamos acompañamiento en procesos de certificación.
- **RegTech:** integración y automatización de procesos de cumplimientos con *partners* y herramientas lideres en el mercado.
- **Outsourcing:** ofrecemos la posibilidad de contratar personal especializado que gestione en nombre de nuestros clientes proyectos, servicios de cumplimiento de mantenimiento de certificados.
- **Auditoría:** servicios de auditoría interna, auditoría de proveedores o auditoría de GDPR.

Expertos en Seguridad de la Información y Privacidad

Somos una consultora boutique altamente especializada en Gestión de la Seguridad de la Información y la Privacidad, dedicada a brindar soluciones personalizadas a empresas que desean fortalecer y tomar control de la seguridad de sus activos más valiosos.

SECDAT

Ofertas especiales

esadealumni

Actualizaciones
ISO27001
Esquema Nacional de Seguridad (ENS)
TISAX

Consigue la tuya

GARANTIA

Ofrecemos Garantía de obtención de Certificación

RegTech
Servicios tecnológicos
Automatización de proceso de GRC

| CONSULTORÍA | AUDITORÍA | OUTOSOURCING | FORMACIÓN | PENTESTING | | INTERIM MANAGEMENT | RECRUITING |

SECDAT

CATÁLOGO DE EMPRESAS Y SOLUCIONES DE CIBERSEGURIDAD
EMPRESA REGISTRADA
incibe_

www.secdat.es

Seven Sector abre ronda de inversión

SEVEN SECTOR TECHNOLOGIES

OFICINAS
Dirección postal:
Avenida Diagonal, 131
Ed. Regus High Tech
08018 Barcelona
Teléfono: 93 694 08 39
E-mail: info@sevensector.com
Web: www.sevensector.com

PERSONAS DE CONTACTO
CEO: Hiram Fernández Ortiz
hfernandez@sevensector.com

Seven Sector crea una herramienta capaz de detectar y aislar ciberamenazas en cuestión de segundos. La *startup* catalana Seven Sector Technologies, experta en ciberseguridad para empresas, ha desarrollado una nueva tecnología bajo el modelo de seguridad reactiva y resiliencia, basado en la Detección Avanzada y Respuesta Extendida (**XDRNET**).

Esto permite detectar amenazas en tiempo real y aislar el equipo infectado sin necesidad de interactuar con él. El hecho de que no sea necesario instalar ningún agente hace posible un despliegue rápido, económico y efectivo.

La empresa catalana **Puig** ya ha mostrado interés en la solución y ha **puesto en marcha una prueba piloto** para la monitorización de parte de sus sistemas en *cloud*. Seven Sector se convierte así en la primera *startup* de ciberseguridad en posicionarse en el nuevo modelo ágil, de detección y prevención de amenazas para segmentos IoT, OT e IT.

PRODUCTOS Y SERVICIOS

Nuestra cartera de servicios está basada en tres pilares:

SERVICIOS DE CIBERSEGURIDAD TÉCNICOS

- Auditorías de seguridad
- Pruebas de penetración en los sistemas
- Simulaciones de ataques de ciberseguridad

SERVICIOS DE CIBERSEGURIDAD DE CONSULTORÍA

- Planes directores de ciberseguridad
- Sistemas de Gestión de Seguridad (SGSI)
- Adecuaciones a normativa

PRODUCTO SAAS – DETECCIÓN AVANZADA DE AMENAZAS

- Protección en cualquier entorno (IT/OT/IoT)
- Monitorización continua en la red
- Sin instalación de ningún agente
- Análisis de filtración de datos en la *dark web*
- Rápido despliegue
- Reducción Reduce

SEVEN SECTOR
TECHNOLOGIES

¿HAS PENSADO EN INVERTIR EN UNA EMPRESA DE CIBERSEGURIDAD?

DESCÁRGATE NUESTRO DECK

www.sevensector.com – investors@sevensector.com

Avinguda Diagonal 131. Ed. Regus High Tech. Barcelona T: +34 93 694 08 39

Zerolynx: seguridad e inteligencia

ZEROLYNX

OFICINAS

Dirección Sede Central: Pol. Ventorro del Cano.
Avenida de Arroyomolinos, 15
28925 Alcorcón (Madrid)
Dirección Sede Norte: Parque Tecnológico de Álava.
Calle Hermanos Lumiere, 11.
01510 Miñano (Araba/Álava).
Teléfono: (+34) 91 164 93 01
E-mail: info@zerolynx.com
Web: www.zerolynx.com

PERSONAS DE CONTACTO

CEO: Juan Antonio Calles
COO: Daniel González

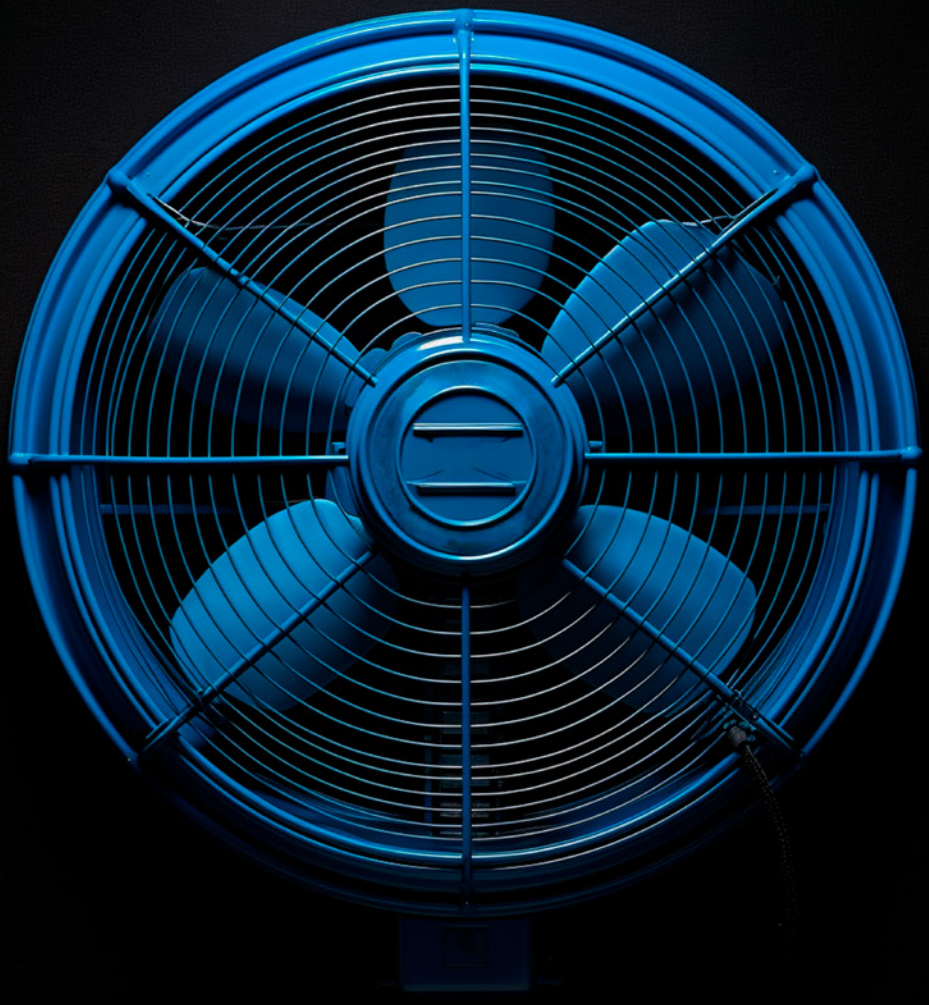
Zerolynx® es un grupo empresarial europeo especialista en ciberseguridad que cuenta con una extensa experiencia en la protección de grandes clientes, como primera línea de defensa frente a los ataques físicos y lógicos.
Actualmente, grupo Zerolynx cuenta con sedes en Madrid y País Vasco, desde donde se centralizan los servicios a nivel internacional.

Zerolynx integra profesionales con experiencia en el sector público, contando con exmiembros de las fuerzas y cuerpos de seguridad del Estado, y en el sector privado, que han trabajado en la protección de compañías del Fortune-500, Ibex 35 y otros grandes clientes a nivel internacional. Esta doble visión permite a Zerolynx disponer de una completa óptica de los escenarios de ataque actuales, teniendo una posición privilegiada para la protección efectiva de sus clientes y la reducción de su nivel de riesgo. Nuestros expertos cuentan con más de 50 de las certificaciones más destacadas del sector, lo que avala su trayectoria profesional y el esfuerzo de Zerolynx por aportar siempre los mejores servicios.

CONCENTRA SUS RECURSOS EN TRES ÁREAS DE NEGOCIO:

- **Análisis forense:** disponemos de un grupo de expertos en análisis forense digital y respuesta ante incidentes que pueden hacer frente, frenar y detener cualquier amenaza, intimidación, chantaje o incursiones maliciosas hacia tu empresa.
- **Inteligencia:** contamos con un amplio equipo de expertos que te ayudarán a conocer la huella en Internet de tu compañía, obtener información de tus proveedores, así como de tu competencia. Analizaremos y protegeremos los activos más críticos de tu organización para evitar amenazas internas y externas.
- **Seguridad ofensiva:** desde Zerolynx apostamos por frenar los ataques de los ciberdelincuentes antes de que sucedan. Por ello, analizamos los puntos débiles de tu empresa simulando los ataques de los ciberdelincuentes para ayudarte a detectar posibles puntos de acceso y fallos de seguridad antes de que la información se vea comprometida.

QUE ESTE VERANO
NADIE SE VENTILE TUS DATOS



SEGURIDAD E INTELIGENCIA

www.zerolynx.com

ZEROLYNX

OptimumTIC: Gestión de la Ciberseguridad Transversal

Equipo Directivo de OptimumTIC

OPTIMUMTIC

OFICINAS

Dirección postal: Plaça Francesc Macià, 7
08029 Barcelona
Teléfono: 932 527 467
E-mail: info@optimumtic.com
Web: OptimumTIC - Auditoría y Ciberseguridad

PERSONAS DE CONTACTO

CEO: Rosa Ortuño

Fundada en 2009, OptimumTIC es una consultoría de ciberseguridad formada por un equipo multidisciplinar tanto de técnicos, abogados y criminólogos como de Compliance. En OptimumTIC trabajamos bajo la visión de ser una empresa líder en servicios de ciberseguridad integrales y transversales y bajo la misión de acompañar a nuestros clientes hacia una estrategia de ciberseguridad que permita la continuidad de sus negocios.

Desde nuestros inicios, tenemos muy claros los valores que rigen nuestra organización y nuestra forma de trabajar y estos son: la experiencia, la excelencia, el conocimiento, la optimización y, sobre todo, la transversalidad, la cual nos permite implementar soluciones integrales que incluyen los aspectos técnicos, organizativos y legales de cumplimiento.

Aparte, somos *partners* certificados de varias plataformas distintas, las cuales ofrecen las mejores soluciones y herramientas del mercado actual de la ciberseguridad.

SERVICIOS

- Gestión e implementación de las soluciones de seguridad de red líderes del mercado como los de Palo Alto, Fortinet, Proofpoint etc.
- Servicios de ciberseguridad, tanto preventiva como gestionada y reactiva.
  - Servicios de control de *endpoint*, control de acceso, análisis de vulnerabilidades, etc.
  - Gestión de la seguridad de las infraestructuras de trabajo 360 grados de manera proactiva y en base a la mejora continua.
  - Security Operaciones Center (SOC) con el fin de mejorar constantemente los sistemas y reducir la superficie y los vectores de ataque.
- Servicio de Oficina de ciberseguridad, soporte en el diseño y desarrollo del Plan Director de Seguridad y estrategia cíber global.
- Consultoría en derecho tecnológico, adecuación a la normativa en protección de datos e implementación y acompañamiento en certificaciones como la ISO 27001.
- Auditorías de sistemas completos: *pentest*, auditoría de *hacking* ético, auditorías de código.

PUNTOS DIFERENCIALES

- Análisis real: disponemos de laboratorio propio.
- *Compliance* global: enfoque de cumplimiento.
- Resiliencia y proximidad: adaptados a cada cliente.
- Profesionalidad y transparencia: asesoramiento real y efectivo.
- Experiencia profunda, con más de 13 años de experiencia dentro del sector de la ciberseguridad.
- Equipo multidisciplinar formado por ingenieros, técnicos, abogados, auditores y criminólogos.
- *Partners* de los fabricantes líderes en el mercado de la ciberseguridad.

esadealumni