esadealumni

A2SECURE

INFRA AI

LISOT

NEXTRET

O. BROKERS

T-SYSTEMS

Especial
Ciberseguridad para Empresas y Protección de Datos 2024

La ciberseguridad: un pilar fundamental para las empresas

En la era digital, las empresas dependen cada vez más de la tecnología para operar y crecer. Sin embargo, esta creciente dependencia también las expone a una amplia gama de amenazas cibernéticas que pueden poner en peligro su reputación, sus operaciones e incluso su supervivencia. Hablamos con los profesionales del sector sobre los principales riesgos, así como tendencias actuales.

¿POR QUÉ ES TAN IMPORTANTE LA CIBERSEGURIDAD PARA LAS EMPRESAS?

Las empresas manejan una gran cantidad de información confidencial, como datos de clientes, información financiera y propiedad intelectual.

Un ciberataque puede resultar en la pérdida o el robo de estos datos, lo que puede tener graves consecuencias legales y financieras. Además, los clientes son cada vez más conscientes de los riesgos cibernéticos y esperan que las empresas tomen medidas para proteger sus datos, ya que una violación de los mismos puede erosionar la confianza de los clientes y dañar la reputación de la marca.

La ciberseguridad es un campo en constante evolución, por lo que las empresas deben mantenerse al día con las últimas tendencias para protegerse de las amenazas emergentes. Los ciberdelincuentes están desarrollando ataques cada vez más sofisticados que utilizan técnicas de inteligencia artificial y *machine learning*.

La migración a la nube también ha aumentado la superficie de ataque para las empresas, ya que los datos se almacenan en la nube y pueden ser vulnerables a ataques.

Para protegerse de las amenazas cibernéticas, las empresas deben implementar una estrategia de seguridad integral que incluya la concientización de los empleados, la seguridad de la red, el cifrado de datos y la gestión de incidentes.

MITOS EN CIBERSEGURIDAD

Uno de los problemas más comunes en materia de ciberseguridad es la existencia de mitos que hacen que nos confiemos y pensemos que no somos un objetivo para los ciberatacantes.

Toni Alés (EDIK 91), socio sénior de Mediterrània Space, director académico y profesor en Esade y vocal en la junta directiva del Club Business Innovation & Technologies de Esade Alumni, considera que los principales mitos se basan en la creencia de que solo las grandes empresas son blanco de ciberataques. “Muchas pequeñas y medianas empresas piensan que su tamaño las protege. Sin embargo, el 43% de los ataques cibernéticos están dirigidos a pymes, según datos de Google y la Agencia EFE, que muestran violaciones de datos en 2023. Los atacantes saben que las pymes suelen tener menos recursos para invertir en seguridad, convirtiéndolas en un objetivo atractivo”. Otro mito es que el *software* antivirus y las herramientas de seguridad son suficientes para protegernos. “El fuerte crecimiento de las amenazas se refleja en el número de muestras de *malware* registradas por el instituto AV-TEST. De 2019 a 2020, se reportaron 113 millones de muestras, y en 2021 esa cifra creció en más de 170 millones, un aumento de casi el 33%. Este incremento es uno de los más significativos en la última década”, añade Alés. Finalmente, está el mito de que la ciberseguridad es responsabilidad exclusiva del departamento de TI. La realidad es que cada empleado juega un papel crucial en la defensa cibernética. Según un informe del INCIBE (Instituto Nacional de Ciberseguridad), el 95% de las violaciones de datos son causadas por errores humanos.

Andrea Bodei, CEO de Infra AI, está de acuerdo en que un mito común es que solo las grandes empresas

Los protagonistas

TONI ALÉS
(EDIK 91)
Socio sénior de Mediterrània Space

ANDREA BODEI
CEO de Infra AI

Los protagonistas

MARTA OLLER
(Lic&MBA 07)
Directora de O. Brokers

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

JORDI TORRUELLA
Socio director de NexTReT Ciberseguridad

son objetivos de los ciberataques: "En realidad, cualquier empresa con información valiosa puede ser un blanco. También se cree que usar un antivirus es suficiente, cuando en realidad se necesita una estrategia de seguridad más robusta, incluyendo herramientas como Infra para identificar y mitigar vulnerabilidades de manera proactiva".

CÓMO PREPARARSE

El riesgo cibernético fue destacado en el World Economic Forum de este año como el 5º riesgo a nivel global y en el *Informe Anual de Seguridad Nacional* del 2023 como uno de los riesgos con una tendencia más negativa a cinco años, detalla **Marta Oller (Lic&MBA 07), directora de O. Brokers.** "Las empresas están cada vez más protegidas y han aumentado su inversión en ciberseguridad en un 40% respecto al año anterior. Sin embargo, aún hay un 50% de empresas que no tienen contratado un ciberseguro. Disponer de una póliza de seguro de ciberriesgo es imprescindible para mitigar los efectos de un ciberataque. Un ciberseguro pone a disposición de las empresas un equipo de expertos que ayudan en el momento del incidente: contención tecnológica, informática forense, asesoramiento jurídico y asesoría en comunicación y gestión de crisis. Además, cubre los perjuicios financieros derivados del ciberataque, como la pérdida de beneficios por paralización, honorarios de consultores para recuperar datos y sistemas, y la extorsión cibernética. Por último, el seguro cibernético cubre las reclamaciones de terceros derivadas del ciberincidente y las sanciones administrativas vinculadas al RGPD. También se puede incluir una pequeña cobertura de fraude tecnológico (suplantación de identidad y robo electrónico de fondos) o contratarla por separado con límite y coberturas más completas", explica Oller.

> "Hay un 50% de empresas que no tienen contratado un ciberseguro. Disponer de una póliza de seguro de ciberriesgo es imprescindible para mitigar los efectos de un ciberataque"

Sobre cómo deben prepararse las empresas para responder a un ataque cibernético en caso de que ocurra, **Ignacio de la Sotilla (CE&MBA 89), CEO de Lisot**, explica que los principales fallos que cometen las empresas son "no actualizar los sistemas informáticos a nivel de *hardware* y *software*; no aplicar las normas básicas y de sentido común como la caducidad de contraseñas, no utilizar un usuario administrador del equipo para trabajar diariamente, limitar los permisos de los usuarios dentro de los sistemas informáticos, "bunkerizar" y externalizar las copias de seguridad, no implementar sistemas de autenticación multifactor o subestimar las amenazas internas". Para Ignacio es imprescindible disponer de un buen sistema de copias de seguridad y realizar auditorías de seguridad y *pentesting* (pruebas de penetración que simulan ataques).

TENDENCIAS ACTUALES

La inteligencia artificial (IA) y la computación cuántica, sin duda, abren un nuevo capítulo en el panorama de las amenazas cibernéticas. **Jordi Torruella, socio director de NexTReT Ciberseguridad,** explica que, gracias a herramientas basadas en IA, los atacantes pueden detectar vulnerabilidades con mayor

rapidez y llevar a cabo ataques a gran escala de manera más eficiente. Además, la personalización de estos ataques se ha vuelto más precisa, lo que aumenta su efectividad. "Utilizando datos personales o laborales, los cibercriminales pueden diseñar tácticas para manipular a las víctimas de manera más creíble. Como resultado, ataques como el *phishing* se vuelven más difíciles de identificar, ya que los mensajes pueden parecer extremadamente genuinos y específicos para la persona atacada. La IA también ha facilitado la creación de *deepfakes*, que son vídeos o audios falsos que resultan extremadamente realistas. Un ejemplo preocupante es el uso de *deepfakes* para imitar a directivos de empresas, con el fin de engañar a los empleados y obtener información confidencial o realizar transacciones fraudulentas, haciendo que el ataque sea casi indistinguible de una comunicación legítima", explica Torruella.

Por otro lado, uno de los avances más disruptivos que traerá la computación cuántica es su capacidad para comprometer los algoritmos criptográficos en uso hoy en día. Técnicas de cifrado comunes, como RSA y ECC, que protegen la mayor parte de las comunicaciones y datos, podrían volverse obsoletas frente a la potencia de los ordenadores cuánticos.

Para **David Mañas, VP Cloud & Cibersecurity Services de T-Systems,** todavía muchas empresas son reactivas en materia de ciberseguridad, y esto es un riesgo para nuestra economía y modelo productivo. Es necesario aumentar la inversión en soluciones de seguridad IT, pero también en la formación de los empleados. "No podemos dejar de mencionar la necesidad de talento en ámbitos de ciberseguridad, de profesionales formados y motivados para trabajar en un sector que necesita expertos constantemente, pero que requiere de una actualización permanente para estar al día de las nuevas amenazas y soluciones que van surgiendo. Es un sector apasionante, muy dinámico y a la cabeza de los avances tecnológicos, una de las profesiones con mayor proyección y demanda. Por desgracia, cada innovación tecnológica puede utilizarse para cometer delitos, lo que nos exige estar constantemente evaluando los riesgos y liderar en términos de innovación sostenible adelantándonos a posibles brechas de seguridad y problemas relacionados en las empresas", comenta.

Un alumni que quiera desarrollar su carrera en ciberseguridad se encuentra frente a una gran oportunidad, ya que puede combinar una visión estratégica de negocios con la necesidad crítica de proteger los activos digitales. "Nuestro consejo sería profundizar en conocimientos técnicos. No hablamos de ser un experto en *hacking*, pero sí de mejorar los conocimientos de seguridad de redes, gestión de riesgos, seguridad en la nube y cumplimiento normativo. Existen todo tipo de certificaciones que pueden ser muy valiosas para lograrlo. Con ello se le abren muchas oportunidades laborales en un sector en crecimiento", añade **Albert Morell, CEO y fundador de A2SECURE**.

> "Uno de los avances más disruptivos que traerá la computación cuántica es su capacidad para comprometer los algoritmos criptográficos en uso hoy en día"

Los protagonistas

DAVID MAÑAS
VP Cloud & Cibersecurity Services de T-Systems

ALBERT MORELL
CEO y fundador de A2SECURE

A2SECURE consolida la excelencia de sus servicios con el reconocimiento de Gartner

A2SECURE

OFICINAS

Barcelona - Av. de Francesc Cambó, 21, 10ª, Ciutat Vella, 08003 Barcelona
Madrid - Paseo de la Castellana, 210, planta 10, puerta 7, 28046 Madrid
Teléfono: 933 94 56 00
E-mail: info@a2secure.com
Web: www.a2secure.com

PERSONAS DE CONTACTO

Fundador y CEO:
Albert Morell (albert.morell@a2secure.com)
General Manager:
Joan Balcells (joan.balcells@a2secure.com)

En los últimos años A2SECURE se ha convertido en el socio de ciberseguridad de referencia para **más de 200 clientes internacionales**, mejorando rápidamente la seguridad digital de las empresas y organizaciones gracias a su equipo de expertos especializados.

La confianza de los clientes y la excelencia de los servicios han hecho que este 2024 **Gartner®** haya incluido a A2SECURE en la Market Guide de Servicios Co-gestionados de Supervisión de la Ciberseguridad. Una guía que, además de describir el estado y *modus operandi* de este mercado, enumera los **proveedores más representativos que ofrecen servicios en él.**

Servicios de ciberseguridad de vanguardia a través de un equipo experto y de alto rendimiento.

A2SECURE no solo ha sido nombrada como proveedor de servicios en esta guía, sino que es la **única empresa española en obtener este reconocimiento. Sin duda, un hecho que la consolida como la única compañía española en alcanzar este nivel de servicios y un proveedor líder en ciberseguridad.**

La compañía fue incluida en la Market Guide de Gartner debido a su cartera de soluciones avanzadas de detección, investigación y respuesta ante amenazas (TDIR) que cumplen con los criterios de excelencia de Gartner.

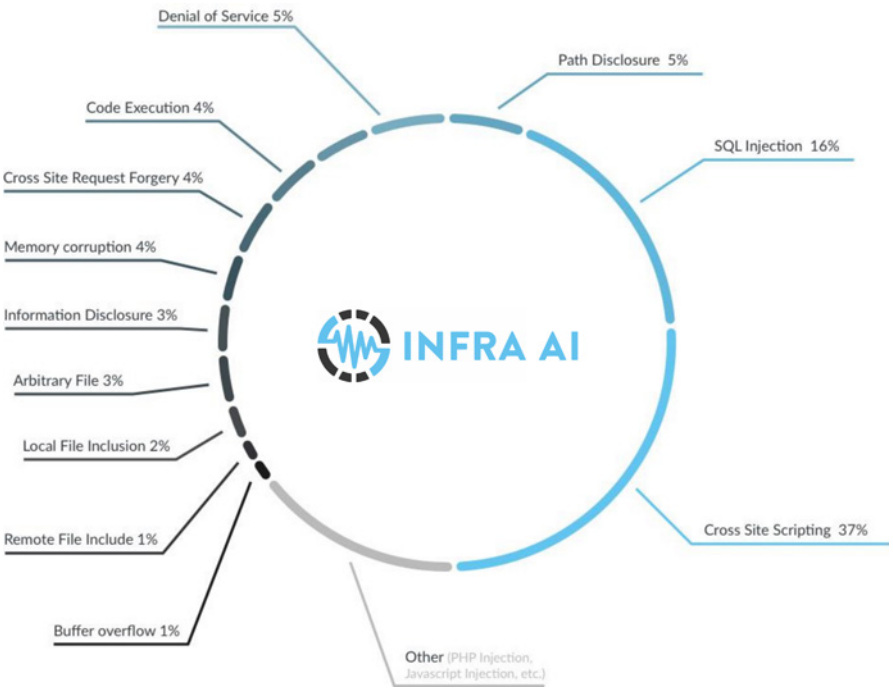
PRODUCTOS Y SERVICIOS

- **Governance & Compliance:** te ayudamos a cumplir con PCI DSS, DORA, NIS2, PCI PIN, SWIFT, ENS, etc.
- **SOC:** gestión de amenazas 24x7 basada en el modelo de detección avanzada, investigación y respuesta (TDIR).
- **Red Team:** servicio potenciado por inteligencia de amenazas y monitorización constante de la *dark web*: **creamos escenarios reales adaptados a tu sector.**
- **Digital Law e IA:** adapta, audita y protege jurídicamente tu negocio desde una perspectiva tecnológica.

NOVEDADES Y SOLUCIONES TECNOLÓGICAS

- Gestión de riesgos y amenazas más amplia, dinámica y continua.
- Ciclo de vida de detección de amenazas inteligente y basado en el riesgo.
- Operamos siempre teniendo en cuenta la continuidad del negocio.
- Equipo multidisciplinar y experto que aborda las vulnerabilidades con eficacia, **garantizando la tranquilidad de los clientes.**

AI Agents for Hacking



INFRA AI

OFICINAS
Teléfono: +34 620 36 81 72
E-mail: andrea@infrascan.net
Web: https://infrascan.net/

PERSONAS DE CONTACTO
CEO: Andrea Bodei

INFRA desarrolla soluciones automatizadas que incluyen tecnologías de escaneo y *hacking* ético, utilizando inteligencia avanzada para detectar vulnerabilidades conocidas y 0-day en redes, aplicaciones web y entornos de infraestructura críticos. Con un enfoque innovador, INFRA emplea múltiples agentes de IA que trabajan en equipo de manera autónoma para cubrir todas las etapas del *hacking* ético, desde la identificación de brechas hasta la explotación controlada. INFRA combina inteligencia OSINT, análisis de la *dark web* y la *blockchain* en la fase de recolección de información, lo que permite descubrir amenazas emergentes y ocultas con un nivel de precisión elevado. Además, un *chatbot* interactivo acompaña al usuario en cada paso, explicando los informes de seguridad y proporcionando asistencia personalizada para cumplir con los estándares de seguridad y obtener certificaciones de cumplimiento.

PRODUCTOS Y SERVICIOS

- INFRA Cloud: comprueba si su nube y sitios web han sido pirateados y ofrece inteligencia de la *dark web*.
- INFRA VM: incluye todas las ventajas de INFRA Cloud, aplicadas también a redes privadas.
- INFRA Cube: dispositivo de seguridad para analizar servidores, PCs, IoT, y *blockchain*.
- INFRA Mainframe: clúster de servidores para analizar grandes redes a nivel *enterprise*, con capacidades avanzadas de IA y OSINT.

NOVEDADES Y SOLUCIONES TECNOLÓGICAS

- Utiliza múltiples agentes de IA trabajando en paralelo para encontrar nuevos tipos de vulnerabilidades, incluyendo aquellas en la *dark web*.
- Herramientas integradas que respaldan el análisis automatizado, con un *chatbot* que ayuda a interpretar informes y a cumplir con estándares de seguridad.
- Identifica los tipos de pruebas a realizar y optimiza los resultados gracias a la colaboración de agentes de IA.
- Valida continuamente los resultados y permite repetir las pruebas, con alertas personalizadas y soporte de IA en tiempo real.

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

Somos la extensión IT de nuestros clientes

NEXTRET

OFICINAS

Dirección postal: Rambla Catalunya, 33
08007 Barcelona
Teléfono: 932 541 530
E-mail: cybersecurity@nextret.net
Web: www.nextret.net

PERSONAS DE CONTACTO

Socio Director de NexTReT Ciberseguridad:
Jordi Torruella

Somos una empresa dedicada a la optimización del área TIC de nuestros clientes, ofrecemos soluciones y servicios de infraestructuras, desarrollo, calidad de servicio y ciberseguridad. Nos responsabilizamos de que la informática esté disponible 24×7.
Nuestra estrategia de trabajo se basa en la reducción y flexibilización de costes, la mejora de la calidad del servicio y la agilización y adaptación del área TIC con compromiso y vocación de servicio.
Estamos certificados en el **Esquema Nacional de Seguridad Categoría Alta,** que acredita que apostamos por la seguridad y hemos adoptado e implementado los procedimientos y medidas de seguridad necesarias para poder ofrecer así unos servicios que protejan tanto la confidencialidad de los datos, como su autenticidad, integridad, disponibilidad y trazabilidad.
Más de 300 ingenieros implicados, certificaciones de los fabricantes más relevantes del mercado y metodologías de calidad garantizadas aseguran el éxito de nuestros proyectos y servicios.

SERVICIOS / PRODUCTOS

- Servicios de gestión del cumplimiento (ISO 27001, ENS, PCI-DSS...).
- Informática legal/forense (peritajes informáticos forenses).
- Auditorías y análisis de seguridad y evaluación de riesgos.
- Seguridad del dato y fugas de información.
- Productos y soluciones de seguridad.
- Oficina Técnica de Seguridad Integral.
- Ciberseguridad industrial / oT industrial /oT salud / IoT.
- VSOC (Centro Virtual de Operaciones de Seguridad).

VENTAJAS Y PUNTOS DIFERENCIALES:

- Empresa con un alto nivel de especialización.
- Técnicos certificados tanto en *hacking* ético como en todos los productos estratégicos en seguridad.
- Todos los servicios se realizan aplicando las máximas medidas de seguridad y han obtenido la certificación en la Categoría Alta del Esquema Nacional de Seguridad (ENS).
- Somos fabricantes de productos de seguridad.
- Platinum Partner del fabricante líder en ciberseguridad SentinelOne.

Una plataforma que protege los endpoints, la nube y los datos impulsada por la IA

NexTReT, platinum partner de SentinelOne

Protección de los Endpoints

Gestiona los recursos con seguridad en la superficie de ataque completa, con EPP, EDR y XDR basadas en IA.

Seguridad de la nube

Descubre todos tus activos e implementa protección impulsada por IA para proteger tu nube desde el momento de la compilación hasta el tiempo de ejecución

Defensa de las entidades

Reduce el riesgo para Active Directory, detecta y evita el uso ilícito de credenciales y prevé el desplazamiento lateral.

Más información:

93 254 15 30

cybersecurity@nextret.net

www.nextret.net

Seguridad por Diseño e IA, T-Systems impulsa la nueva era de la ciberseguridad

T-SYSTEMS

OFICINAS

Dirección postal: Calle Pere IV, 313, Edificio Smart 08020 Barcelona, España
Teléfono: +34 93 501 50 00
E-mail: FMB_TS_IB_MARCOM@t-systems.com
Web: https://www.t-systems.com/es/es/

PERSONAS DE CONTACTO

David Mañas

Actualmente, las infraestructuras tecnológicas de empresas y administraciones públicas se ven amenazadas cada vez con más frecuencia por ataques más sofisticados. Para proteger los datos, las aplicaciones y los usuarios, las organizaciones deben incorporar la seguridad "por diseño" a su estrategia y a la planificación de su ecosistema IT.

El crecimiento de las amenazas a la seguridad obliga a mejorar la agilidad de las operaciones para responder de forma eficiente a los ataques y aumentar la capacidad de recuperación de la empresa. T-Systems promueve un enfoque Zero Trust entre sus clientes, limitando los riesgos a través de la verificación de identidades.

La división de Deutsche Telekom impulsa además la innovación para adelantarse a las amenazas que puedan surgir y cuenta con soluciones de seguridad combinadas con el uso de IA y una infraestructura robusta para garantizar la seguridad de sus servicios.

PRODUCTOS, SERVICIOS, NOVEDADES Y SOLUCIONES TECNOLÓGICAS

- Consultoría sobre seguridad: definición de los requisitos de seguridad para proteger la infraestructura adaptada al sector industrial y madurez digital de la empresa.
- Managed Detection and Response: protección de extremo a extremo combinada con una estrategia de respuesta mejorada ante ataques.
- Pruebas de penetración automatizadas: establecimiento de pruebas periódicas para la detección de las vulnerabilidades y definición de medidas de corrección para mejorar la seguridad.
- Microsegmentación: segmentación definida por *software* para crear zonas de seguridad eficaces y contener los ciberataques.
- Secure Access Service Edge: seguridad avanzada para proteger y utilizar las aplicaciones y datos de forma más eficaz.
- Seguridad OT: protege la infraestructura IT/OT de los nuevos tipos de amenazas.

T Systems

IA: la solución del *ahora* para las amenazas del *mañana*

visit t-systems.es

RETHINK
THE SYSTEM

Protege tu empresa del ciberriesgo: coberturas y soluciones de ciberseguro

O. BROKERS

OFICINAS

Dirección postal: Diagonal 571, 2ª planta, Barcelona
E-mail: info@o2bbrokers.com
Web: www.obrokers.es
LinkedIn:
https://www.linkedin.com/company/o-brokers

PERSONAS DE CONTACTO

Presidente: Melcior Oller
CEO: Marta Oller
Client Director: Anna Penas
Client Director: Helena Corominas

El ciberriesgo es la principal amenaza que tienen las empresas hoy en día. La probabilidad de una vulneración y encriptación de sistemas es más alta que la ocurrencia de un incendio, un impago de un cliente o una reclamación de un tercero.
Los incidentes cibernéticos han aumentado exponencialmente. Con la digitalización de la industria y el desarrollo de la IA, el impacto financiero y reputacional puede ser devastador. Las nuevas variaciones de *malware* y los ataques de ingeniería social cada vez más sofisticados amenazan diariamente los sistemas empresariales.
Invertir en medidas de protección es esencial para minimizar las probabilidades de un incidente, y **transferir el riesgo al mercado asegurador mediante la contratación de una póliza es clave para garantizar la continuidad de la empresa.**

En O. Brokers, acompañamos a nuestros clientes en la implementación de medidas de seguridad y procesos necesarios para cumplir con los requisitos de las compañías aseguradoras.
Asesoramos sobre coberturas y límites a contratar según la tipología de empresa.
Analizamos la oferta del mercado asegurador y negociamos las coberturas para ofrecer el mejor seguro Cyber a nuestros clientes.

PRODUCTOS, SERVICIOS, NOVEDADES Y SOLUCIONES TECNOLÓGICAS

COBERTURAS SEGURO CYBER

- **Servicios de gestión del incidente**
  - Servicio de primera respuesta.
  - Servicio de contención tecnológica e informática forense.
  - Asesoramiento jurídico.
  - Asesoramiento en comunicación y gestión de crisis.
  - Servicio para notificar a los afectados.
  - Servicio de control y monitorización de la información comprometida.
  - Asesoramiento en notificación al regulador.
- **Gastos propios**
  - Gastos de recuperación de datos y sistemas.
  - Pérdida de beneficios.
  - Extorsión cibernética.
- **Responsabilidad civil frente a reclamaciones de terceros**
  - Responsabilidad civil por contenido digital.
  - Responsabilidad civil por seguridad y privacidad.
  - Sanciones administrativas y PCI.
- **Fraude tecnológico**
  - Uso fraudulento de la identidad electrónica.
  - Robo electrónico de fondos.
  - Modificación de precios online.
  - Fraude en servicios contratados.
  - Suplantación de identidad.

esadealumni