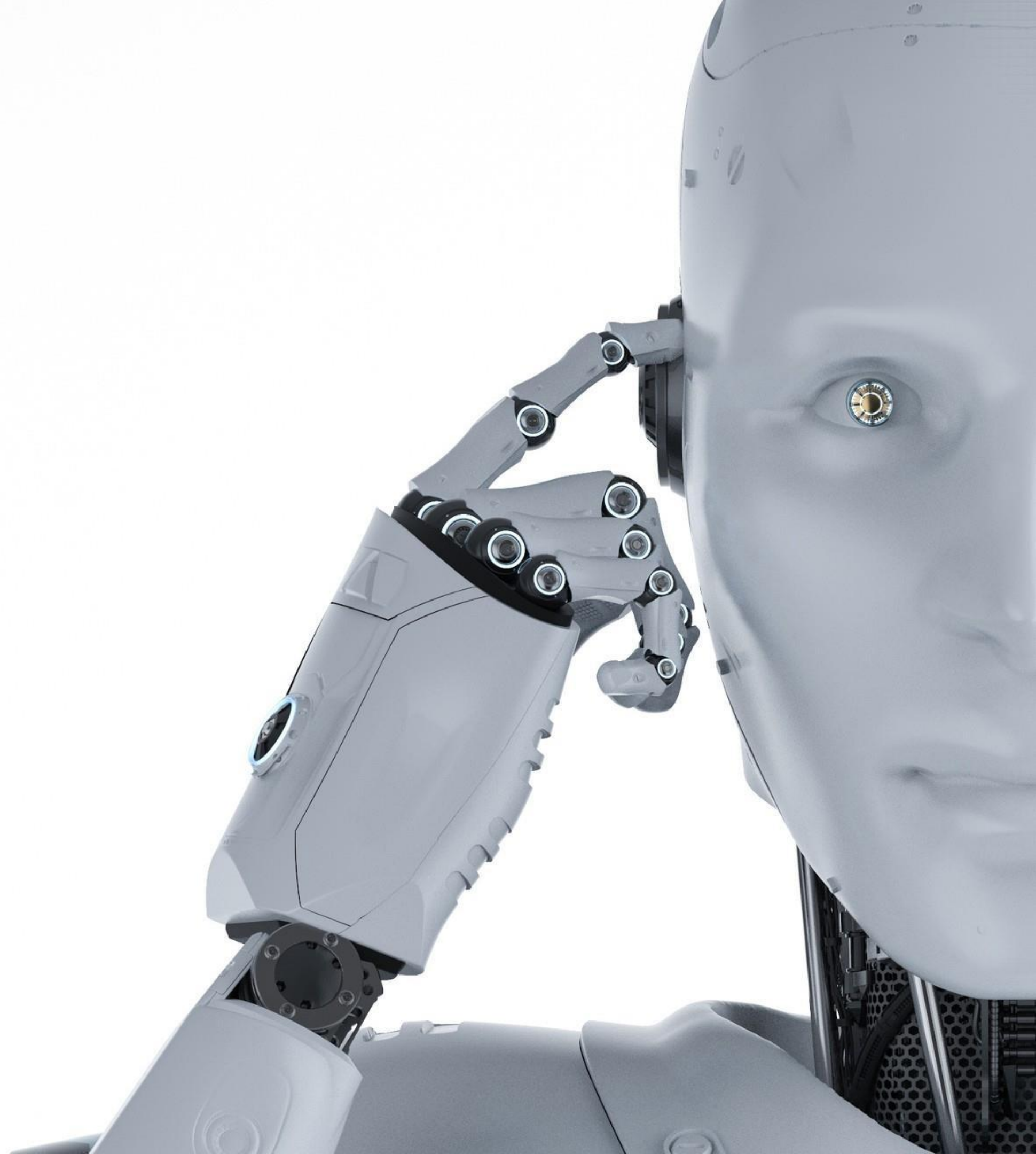




Ciberseguridad para empresas





Konektor



Sobre Konektor

9

Países

+900

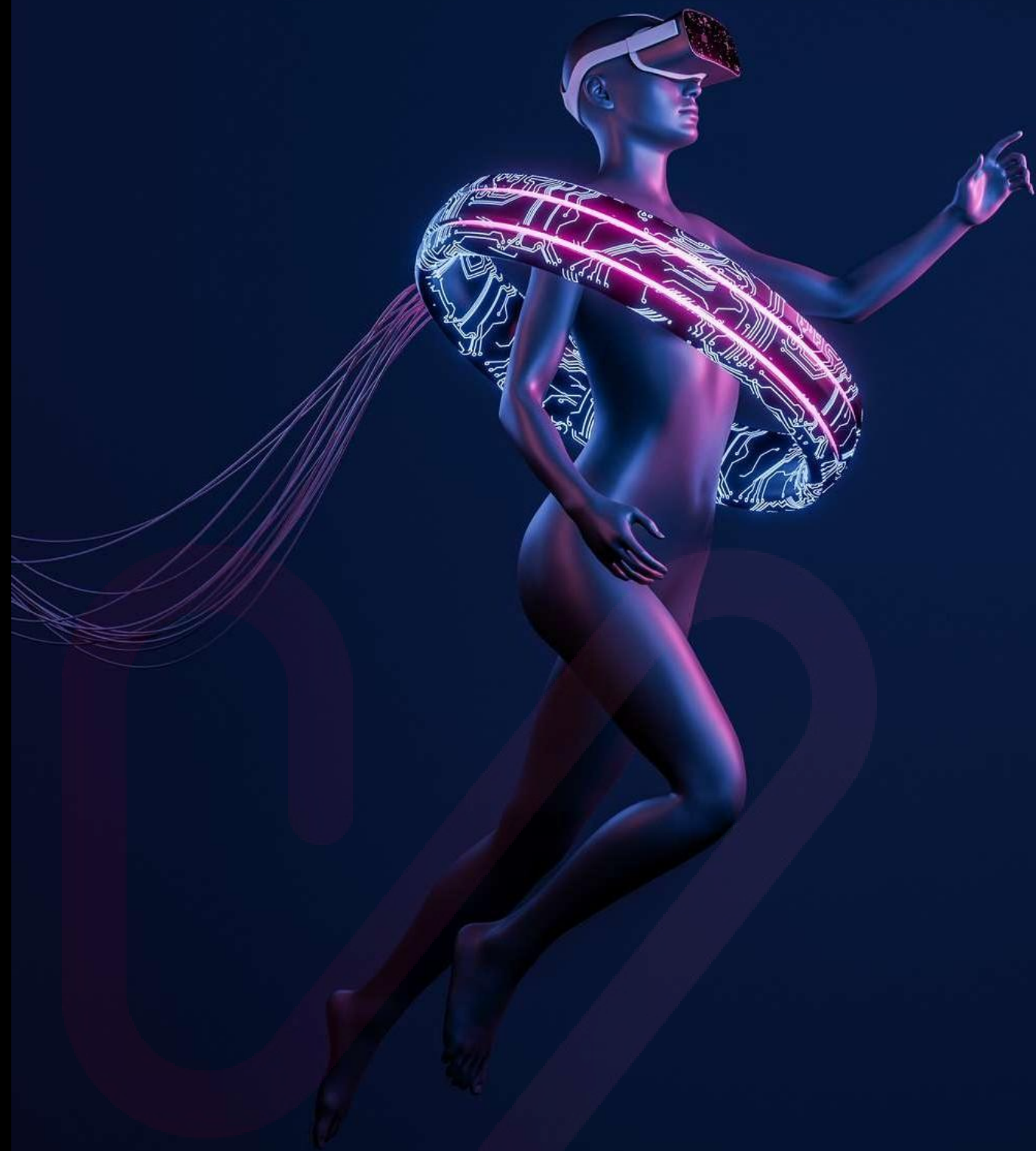
Proyectos

4

Años

+30

Sectores



Konektor Cyber

Ciberseguridad práctica para empresas

La digitalización, el trabajo en la nube y la incorporación de herramientas de IA están aumentando los puntos de exposición de las empresas. Sin embargo, muchas organizaciones no tienen una visión clara de dónde están realmente sus riesgos ni qué deberían corregir primero.

Konektor Cyber nace con un enfoque muy concreto: **detectar vulnerabilidades, reducir riesgos y preparar a las personas para evitar incidentes.**

Trabajamos sobre tres áreas:

- **Diagnóstico:** Analizamos sistemas, accesos, configuraciones y procesos para detectar los principales puntos de riesgo.
- **Personas:** Formamos a los equipos frente a phishing, fraude, robo de credenciales, fuga de información y uso inseguro de IA.
- **Validación:** Ponemos a prueba la seguridad mediante simulaciones y pruebas controladas para comprobar qué ocurriría ante un ataque real.

Un enfoque orientado a saber dónde estamos, qué riesgo tenemos y qué debemos hacer.

Nuestros Clientes

IIVAS

Ferrer&Ojeda
INSURANCE PARTNERS

 XUNTA
DE GALICIA

grupoGodo

ingenico

BYD

YOU
FIRST

stayforlong

 UNIVERSITAT DE
BARCELONA

 COSTAISA GROUP

+ Cruz Roja

Puro



RE/MAX

 CAFÉ
fortaleza
- DESDE 1885 -

PrimaPriX

 **vytrus**
biotech

LAIVE

HYATT

Análisis Personalizado

La seguridad de una empresa va mucho más allá de tener antivirus

Nuestro diagnóstico revisa los principales puntos desde los que actualmente puede producirse un incidente de seguridad.

Identidades y accesos

- Usuarios activos e inactivos
- Permisos y privilegios
- Contraseñas
- MFA / doble factor
- Cuentas con permisos administrativos

Entorno tecnológico

- Microsoft 365 / Google Workspace
- Equipos y dispositivos
- Actualizaciones y parches
- Servidores e infraestructura
- Copias de seguridad

Exposición externa

- Servicios accesibles desde Internet
- Configuraciones vulnerables
- Dominios y servicios corporativos
- Vulnerabilidades conocidas

Personas y procesos

- Phishing e ingeniería social
- Gestión de incidentes
- Teletrabajo y Wi-Fi
- Uso de dispositivos corporativos
- Acceso y compartición de información

IA y datos

- Uso de ChatGPT, Copilot y otras herramientas
- Información sensible introducida en IA
- Gestión de permisos
- Riesgo de fuga de información corporativa

Konektor Cyber Audit

La puerta de entrada a la ciberseguridad

Una auditoría diseñada para empresas que quieren conocer su situación actual sin empezar por proyectos técnicos complejos.

Durante el proyecto realizamos sesiones con dirección y/o IT, analizamos la infraestructura y revisamos los principales puntos de riesgo de la organización e incluye:

- Revisión de Microsoft 365 / Google Workspace
- Usuarios, permisos, accesos y MFA
- Equipos, servidores y actualizaciones
- Backups y capacidad de recuperación
- Exposición externa
- Vulnerabilidades y configuraciones inseguras
- Riesgos asociados al uso de IA
- Procedimientos frente a phishing, fraude e incidentes
- Revisión de las principales prácticas internas de seguridad

El objetivo no es entregar un listado técnico de problemas, sino **determinar cuáles pueden tener impacto real sobre el negocio y establecer un orden claro para corregirlos.**

Precio orientativo: 1.450 € + IVA





Entregables **Post Auditoria**

Al finalizar el Cyber Audit transformamos los hallazgos técnicos en un documento comprensible para dirección y accionable para el equipo responsable.

Informe ejecutivo: Resumen de la situación actual, principales riesgos detectados y nivel general de exposición.

Mapa de riesgos: Cada incidencia se clasifica según su impacto:

Crítico - Puede provocar acceso no autorizado, pérdida de información, fraude o interrupción relevante del negocio.

Importante - Debe corregirse para reducir significativamente la exposición de la empresa.

Recomendable - Mejoras destinadas a elevar progresivamente el nivel de seguridad.

Roadmap de actuación - Para cada punto indicamos:

- Qué hemos detectado
- Qué riesgo supone
- Qué debería hacerse
- Qué prioridad tiene
- Qué complejidad aproximada implica

Finalizamos con una **sesión de presentación a dirección / IT** para revisar conjuntamente los resultados y siguientes pasos.

Cyber Audit 360

Auditoría + Formación + Pruebas reales de seguridad

Cyber 360 está pensado para empresas que no quieren limitarse a recibir un diagnóstico, sino **comprobar su exposición real y reducir el riesgo desde el primer proyecto.**

Incluye todo el alcance de **Konektor Cyber Audit**, más dos bloques adicionales:

1. Formación y concienciación

- Sesión práctica dirigida a empleados sobre:
- Ingeniería social y phishing
- Robo de credenciales
- Contraseñas y MFA
- Fraudes y suplantación de identidad
- Deepfakes y clonación de voz
- Teletrabajo y dispositivos
- Uso seguro de ChatGPT / Copilot
- Fuga de información corporativa
- Cómo actuar ante un incidente

02. Security Testing

- Realizamos pruebas controladas para identificar vulnerabilidades que podrían ser aprovechadas por un atacante.
- Simulación de phishing
- Escaneo de vulnerabilidades
- Revisión de exposición externa
- Pentesting controlado sobre el alcance acordado
- Revisión básica de web o aplicaciones cuando aplique
- Retest posterior para comprobar las correcciones

Precio orientativo: desde 2.900 € + IVA

Metodología de seguridad

Phishing simulado - Enviamos una campaña controlada a los empleados para medir:

- Quién abre el correo
- Quién accede al enlace
- Quién intenta introducir credenciales
- Qué departamentos presentan mayor exposición
- El resultado permite adaptar posteriormente la formación.

Escaneo de vulnerabilidades - Analizamos sistemas y servicios para localizar:

- Software vulnerable
- Configuraciones inseguras
- Servicios expuestos
- Puertos abiertos
- Vulnerabilidades conocidas

Pentesting

Sobre los sistemas previamente autorizados intentamos explotar de forma controlada las vulnerabilidades encontradas.

El objetivo es responder a una pregunta, **“Si alguien intentara entrar hoy, ¿hasta dónde podría llegar?”**

Todo el proceso se realiza con alcance previamente acordado y autorización expresa de la empresa.





Konektor