Óscar Carrión pone la ciberseguridad al alcance de las pymes con iAPentest

El CEO de Tecnopersonal y creador de iAPentest defiende que la protección digital ha dejado de ser una cuestión reservada a las grandes empresas para convertirse en una responsabilidad clave para cualquier negocio. Tras más de 25 años en el sector IT, impulsa una solución que ayuda a pymes, autónomos y pequeñas organizaciones a conocer su exposición digital con un diagnóstico claro, comprensible y orientado a la acción.

Óscar, llevas más de 25 años vinculado al sector IT. Si miras hacia atrás, ¿qué momentos de tu trayectoria profesional te han llevado hasta la creación de iAPentest?

He tenido la suerte de vivir prácticamente todas las etapas de la tecnología: desde entornos muy tradicionales hasta la nube, la identidad digital o la ciberseguridad actual.

He trabajado con grandes organizaciones, he liderado equipos y he participado en proyectos complejos, pero hubo algo que se repetía constantemente: las pequeñas empresas siempre llegaban tarde a la ciberseguridad.

""Los ciberdelincuentes ya no eligen víctimas una a una. Automatizan ataques y buscan objetivos vulnerables"

No porque no les importara, sino porque no tenían tiempo, presupuesto o conocimiento para abordarla. Veía cómo muchas veces descubrían problemas importantes cuando ya habían sufrido un incidente o cuando un cliente les exigía ciertos niveles de seguridad. iAPentest nace precisamente de esa experiencia acumulada y de una pregunta muy sencilla: ¿por qué una pyme no puede tener acceso a un análisis serio y comprensible de su exposición digital?

La ciberseguridad suele percibirse como algo complejo, caro y reservado a grandes empresas. ¿En qué momento detectaste que las pymes, autónomos y pequeñas organizaciones necesitaban una solución más accesible para conocer su exposición digital?

Lo detecté escuchándolas.

Muchas veces la respuesta era la misma: "Eso es para empresas grandes" o "nosotros no podemos permitirnos una auditoría". Sin embargo, cuando revisabas sus webs o servicios expuestos, encontrabas problemas relativamente sencillos de identificar y corregir.

Ahí entendí que el verdadero problema no era únicamente técnico. Era de acceso. Había que democratizar la ciberseguridad, traducirla a un lenguaje cercano y ofrecer herramientas adaptadas a la realidad de quienes tienen que sacar adelante un negocio cada día.

Muchas pequeñas empresas creen que no son objetivo de los ciberdelincuentes porque "no tienen nada importante que robar". ¿Cuál es el mayor error de percepción que existe hoy sobre la ciberseguridad en las pymes?

Pensar que "a mí no me va a pasar".

Los ciberdelincuentes ya no eligen víctimas una a una. Automatizan ataques y buscan objetivos vulnerables. No importa si eres una multinacional o una empresa de cinco empleados.

Además, muchas pymes custodian información muy valiosa: datos de clientes, facturación, accesos a proveedores o la propia continuidad del negocio. A veces no buscan robar millones; basta con paralizar la actividad durante unos días para generar un daño enorme.

iAPentest nace con la idea de acercar el análisis de vulnerabilidades y errores de configuración a organizaciones sin grandes recursos técnicos. ¿Qué problema concreto querías resolver con este proyecto?

Quería resolver la incertidumbre. Muchísimas organizaciones no saben si están bien o mal. No tienen una fotografía objetiva de su situación. Y cuan-

do la obtienen, suele venir acompañada de informes técnicos imposibles de interpretar.

iAPentest pretende ofrecer precisamente eso: una primera visión clara, comprensible y accionable. Que una empresa pueda entender qué riesgos tiene, qué prioridad tienen y qué puede hacer para reducirlos.

El proyecto ha comenzado poniendo el foco en entornos WordPress, una tecnología muy utilizada por empresas, autónomos y medios digitales. ¿Por qué era importante empezar por ahí?

Porque WordPress es el escaparate digital de millones de organizaciones.

"La web ya no es solo una tarjeta de presentación; es una parte crítica del negocio"

La web ya no es solo una tarjeta de presentación; es un canal comercial, una herramienta de captación y, en muchos casos, una parte crítica del negocio. Además, precisamente por su enorme popularidad, también es uno de los entornos más atacados.

Empezar por WordPress nos permitía generar impacto desde el primer día allí donde existe una necesidad real y muy extendida.

Uno de los elementos diferenciales de iAPentest es la correlación y validación cruzada de evidencias para reducir falsos positivos. Explicado para una pyme sin conocimientos técnicos, ¿por qué es tan importante que una herramienta no solo detecte riesgos, sino que los interprete bien?

Porque no todas las alarmas significan peligro real. Si una herramienta te dice que tienes cincuenta problemas y la mitad no son relevantes, acabarás ignorando también los importantes. Y eso es muy peligroso.

Nuestro objetivo no es generar miedo ni listas interminables. Es aportar contexto. Ayudar a distinguir qué requiere atención inmediata, qué puede esperar y qué, simplemente, conviene revisar. La información solo genera valor cuando ayuda a tomar decisiones.

En ciberseguridad, recibir demasiadas alertas puede ser casi tan paralizante como no recibir ninguna. ¿Cómo debería una pequeña empresa priorizar los riesgos cuando no tiene un departamento especializado?

Con sentido práctico.

Primero, aquello que pueda afectar directamente a la continuidad del negocio: accesos comprometidos, copias de seguridad inexistentes o vulnerabilidades críticas expuestas a Internet. Después, los aspectos relacionados con la protección de datos y las obligaciones legales.

Y, por último, la mejora continua. No hace falta resolverlo todo en una semana. La ciberseguridad no es una meta; es un proceso de reducción progresiva del riesgo.

Tu proyecto incorpora también una visión vinculada a normativa, buenas prácticas y posibles implicaciones legales. ¿Estamos entrando en una etapa en la que la ciberseguridad ya no es solo una cuestión técnica, sino también de responsabilidad empresarial?

Sin ninguna duda. Hoy la ciberseguridad forma parte del gobierno de la empresa. Afecta a la reputación, a la confianza de clientes y proveedores y

al cumplimiento normativo.

Los consejos de dirección empiezan a entender que delegar completamente este asunto en "el informático" ya no es suficiente.
Igual que existe responsabilidad financiera o laboral, también existe responsabilidad sobre cómo protegemos la información y gestionamos el riesgo digital.

¡APentest ha sido reconocido dentro del programa europeo CYSSDE Open Call 3. Más allá del reconocimiento, ¿qué supone para un proyecto español recibir esta validación en un entorno europeo tan especializado?

Supone una enorme motivación.

Que expertos independientes europeos consideren que tu propuesta merece estar entre las mejor valoradas es una validación muy importante del trabajo realizado.

Pero, sobre todo, supone una responsabilidad. Significa que hay una oportunidad real de aportar valor más allá de nuestras fronteras y de demostrar que desde España también se puede innovar en ciberseguridad con propuestas cercanas, útiles y orientadas a necesidades reales.

"La autenticación multifactor es una de las medidas más eficaces y sencillas que existen"

Desarrollar una solución tecnológica en ciberseguridad exige conocimiento técnico, pero también visión de negocio. ¿Qué ha sido más difícil en este proceso: construir la tecnología, explicar el problema o demostrar que el mercado realmente la necesita?

Probablemente, explicar el problema.

La tecnología se puede desarrollar, mejorar y evolucionar. Pero convencer a alguien de que invierta en prevenir algo que todavía no le ha ocurrido es mucho más complejo.

Paradójicamente, muchas organizaciones entienden el valor de la ciberseguridad justo después de sufrir un incidente. El reto está en cambiar esa mentalidad y conseguir que la prevención deje de verse como un gasto para entenderse como una inversión en continuidad y confianza.

Desde tu experiencia, ¿qué tres aspectos debería revisar cualquier pyme mañana mismo para reducir su exposición digital sin necesidad de grandes inversiones?

Primero, activar la autenticación multifactor en el correo electrónico y en los accesos críticos. Es una de las medidas más eficaces y sencillas que existen.

Segundo, comprobar que las copias de seguridad funcionan realmente y que pueden recuperarse cuando haga falta.

Y tercero, revisar periódicamente qué está expuesto en Internet: la web, los accesos remotos o los servicios publicados. Muchas veces los mayores riesgos están a la vista de todos y pasan desapercibidos durante años.

Si me permites un último apunte…. La buena noticia es que mejorar la seguridad no siempre requiere grandes presupuestos.

A menudo empieza con pequeñas decisiones tomadas a tiempo.