incibe emprende

Programa de **Impulso a la Industria de la Ciberseguridad Nacional**

#**INCIBE**emprende

Financiado por la Unión Europea NextGenerationEU

Gobierno de España · Ministerio para la Transformación Digital y de la Función Pública · Secretaría de Estado de Digitalización e Inteligencia Artificial

Plan de Recuperación, Transformación y Resiliencia

España | digital 2026

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017

Club del Emprendimiento
www.club del emprendimiento.com

incibe emprende

INCIBE Emprende desarrolla iniciativas de **ideación, incubación y aceleración** tanto para la promoción del emprendimiento en ciberseguridad, como de la ciberseguridad en el emprendimiento de base tecnológica, con el fin de **Impulsar la Industria Nacional de Ciberseguridad**.

- **Acompañamos** a emprendedores y start-ups españolas de **ciberseguridad, así como de base tecnológica** para la integración de la ciberseguridad en su proyecto.
- **Impulsamos el desarrollo de proyectos** independientemente de su grado de madurez: fomento de ideas - incubación de proyectos - aceleración de start-ups e internacionalización.
- Impulsamos la **innovación** y promocionamos la atracción de **inversión** a la misma.

Plan de Recuperación, Transformación y Resiliencia (PRTR) a través del Componente 15. Inversión 7 Ciberseguridad: Fortalecimiento de las capacidades de ciudadanos, PYMES y profesionales e impulso del sector.

Start-ups vs emprendimiento tradicional

- Empresas digitales/base tecnológica
- Explotación de nuevos modelos de negocio
- Modelo de negocio escalable: crecimiento exponencial en ventas y crecimiento lineal en costes
- Ventaja competitiva basada en la innovación
- Alto riesgo debido a su alto contenido innovador
- Necesidad de elevado volumen de financiación y dificultad de acceso a la misma en fases iniciales
- Fuentes de financiación FFF (family, fools and Friends), capital riesgo, business angels. La garantía la supone el equipo.
- Dependencia en captación y retención de empleados altamente cualificados.

VS

- Explotación de modelos de negocio convencionales
- Crecimiento estable, modelo de negocio sostenible
- Fuente de financiación tradicional: préstamos y recursos propios. Garantía real y/o personal.
- Centrada en mantener el negocio y/o generar un crecimiento % estable.

Sector de la ciberseguridad

SECTOR EN AUGE

122.284	24.119	83.000
Trabajadores empleados (2021)	Brecha de talento (2021)	Brecha de talento (2024)

VALOR ECOSISTEMA*

1.500M
Año 2020

8,12%
Crecimiento anual

2.000M
Previsión 2024

*Fuente: Security Spending Guide IDC 2021

Participación mundial en la industria de ciberseguridad

31% 69%

Participación estudiantes grados STEM

24% 76%

Participación estudiantes cursos ciberseguridad

18% 82%

Sector de la ciberseguridad

Ciberseguridad

La importancia de la ciberseguridad es **transversal** a todos los sectores de la economía

Digitalización sectores

La digitalización de todos los sectores está favoreciendo un **crecimiento global del mercado de la Ciberseguridad**

El sector que más peso aporta a la ciberseguridad es el de **distribución y servicios**, seguido del **financiero**

*Fuente: Security Spending Guide IDC 2021

Programa de apoyo al Emprendimiento en ciberseguridad

incibe emprende 2023-2026

Captación / Ideación

Charlas
Talleres
Eventos

Incubación

Formación
Mentorización
Asesoramiento legal
Asesor fiscal
Visita al ecosistema regional
Demo Day

Aceleración

Formación
Mentorización
Asesoramiento legal
Asesor fiscal
Visita al ecosistema regional
Demo Day
Aceleración Express

Club del Emprendimiento
www.club del emprendimiento.com

Captación / Ideación

Desarrollo y Despliegue seguro de aplicaciones

- Antonio Reche – Solutions Architect Veracode
- Cómo evitar vulnerabilidades en hacer que el código de tus desarrollos no sea vulnerable. Los hagas tú o te los hagan.

Charla

Introduce aquí el contenido de la charla correspondiente

Club del Emprendimiento
www.club del emprendimiento.com

Desarrollo y Despliegue seguro de aplicaciones : El impacto de la IA en la Ciberseguridad

Antonio Reche –Veracode

Las dos caras de la IA

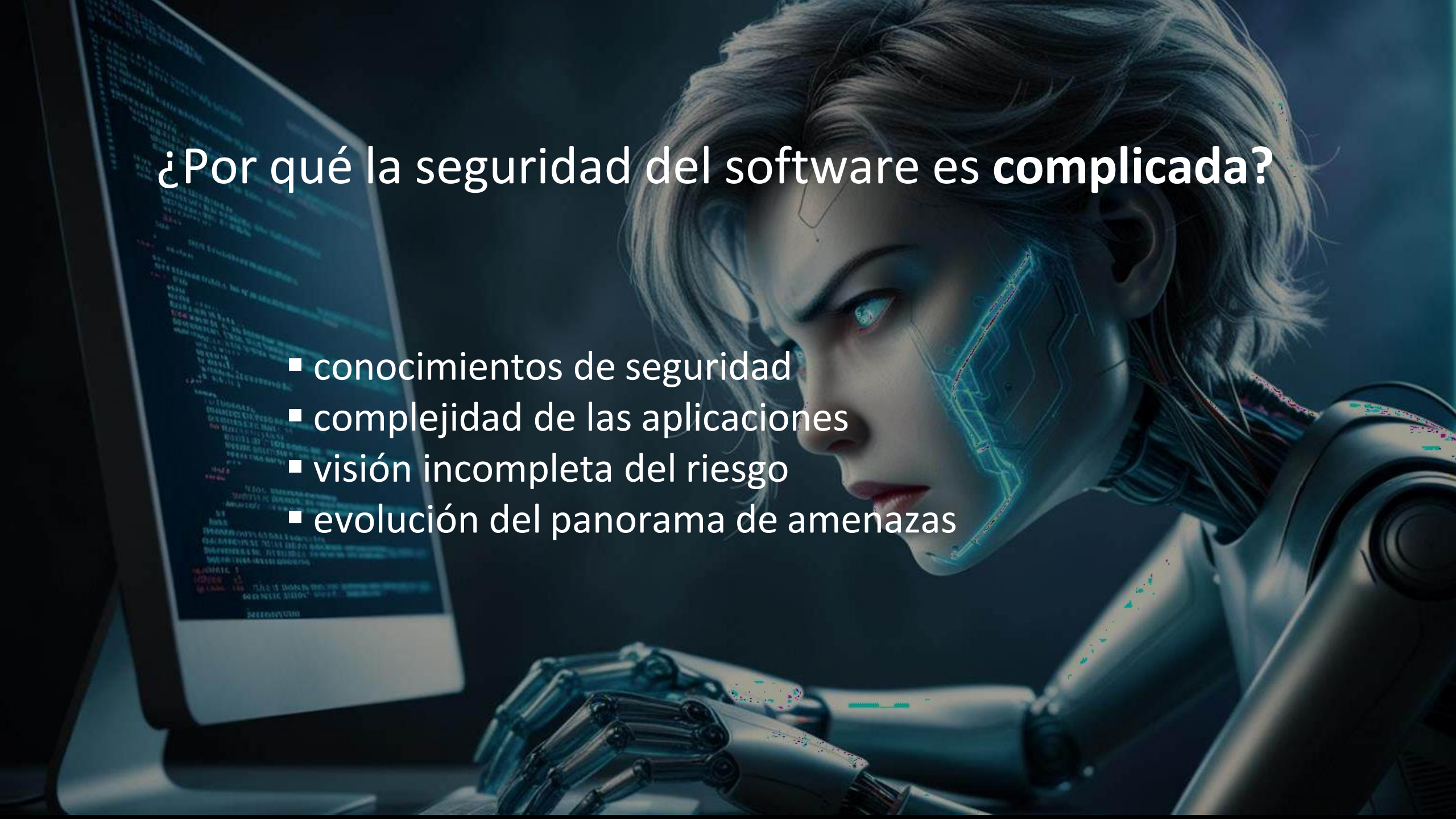

La forma de
crear software
ha cambiado
para siempre


La adopción de
devops


La adopción de
cloud infrastructure


La adopción de
secure by design

¿Por qué la seguridad del software es **complicada?**

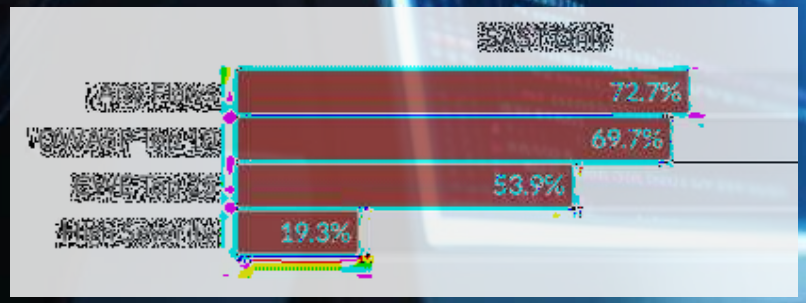


¿Por qué la seguridad del software es **complicada?**

- conocimientos de seguridad
- complejidad de las aplicaciones
- visión incompleta del riesgo
- evolución del panorama de amenazas

Mi código es seguro.
Mis aplicaciones son seguras.
No voy a sufrir una incidencia.

VERACODE SOSS REPORT 2024

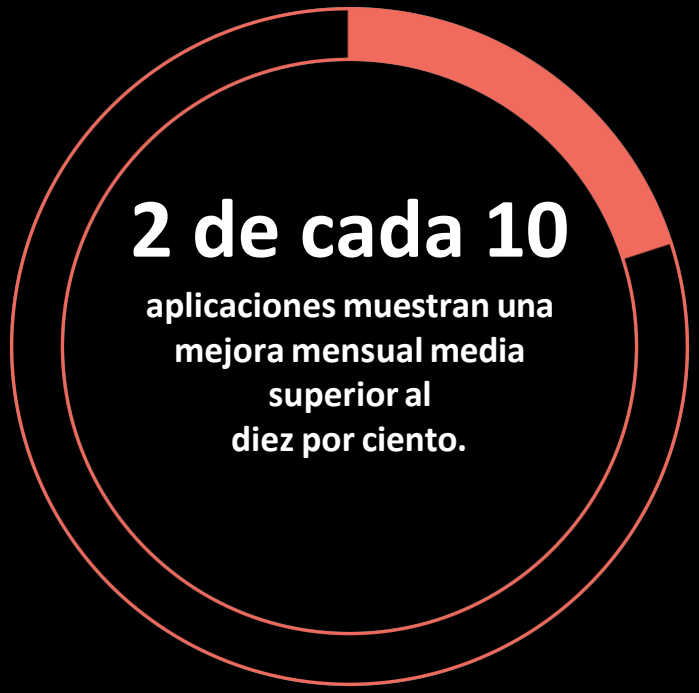


Code Injection (SQL Injection, NoSQL Injection, Command Injection, etc.) Cross-Site Scripting (XSS) Cross-Site Request Forgery (CSRF) Inyección de Código de Deserialización Insegura Exposición de Datos Sensibles Configuración de Seguridad Incorrecta Fallos de Autenticación y Gestión de Sesiones Control de Acceso Insuficiente Inseguridad en APIs Uso de Componentes con Vulnerabilidades Conocidas Logging y Monitoreo Insuficiente Seguridad en el Transporte Insuficiente Inyección de Dependencias Exposición de Servicios Internos … y un largo etc …

MOVEit Transfer Vuln (CVE-2023-34362) Spring4Shell (CVE-2022-22965) Follina (CVE-2022-30190) Log4Shell (CVE-2021-44228) SolarWinds Orion (CVE-2020-10148) BlueKeep (CVE-2019-0708) jQuery (CVE-2020-11022 y CVE-2020-11023) Jackson Databind (Múltiples CVEs) pache Struts (CVE-2017-5638) Heartbleed (CVE-2014-0160)… etc…

las organizaciones se ahogan en las deudas de seguridad

* We are defining all flaws that remain unremediated for over one year, regardless of severity, as security debt.
**Critical debt: High-severity flaws that remain unremediated for over one year.



pocos equipos
corrigen los fallos de seguridad lo suficientemente rápido como para reducir **el riesgo de seguridad a un ritmo significativo**

VERACODE

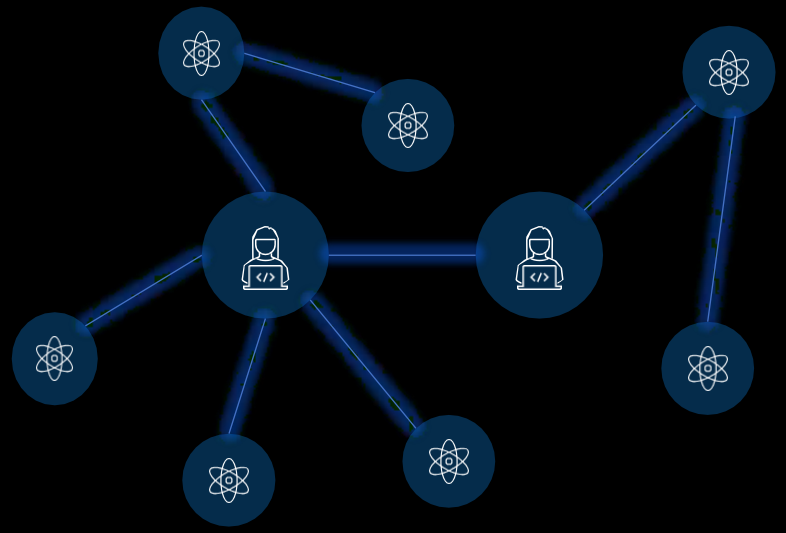

una buena seguridad
del software **protege**
lo importante

buena seguridad del software

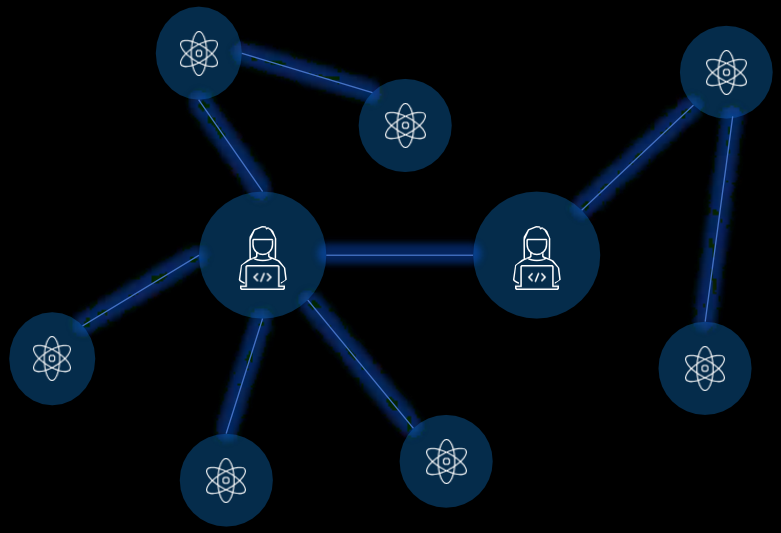
proteger lo importante


cómo creamos software
ha cambiado para siempre

las aplicaciones se ensamblan, **no sólo se escriben**



El 80% del código de las aplicaciones modernas **es código abierto**



cada paquete de OSS trae consigo otros 77 de forma transitoria

para ir más rápido los desarrolladores aprovechan

Open source

Repos de código

Large language models

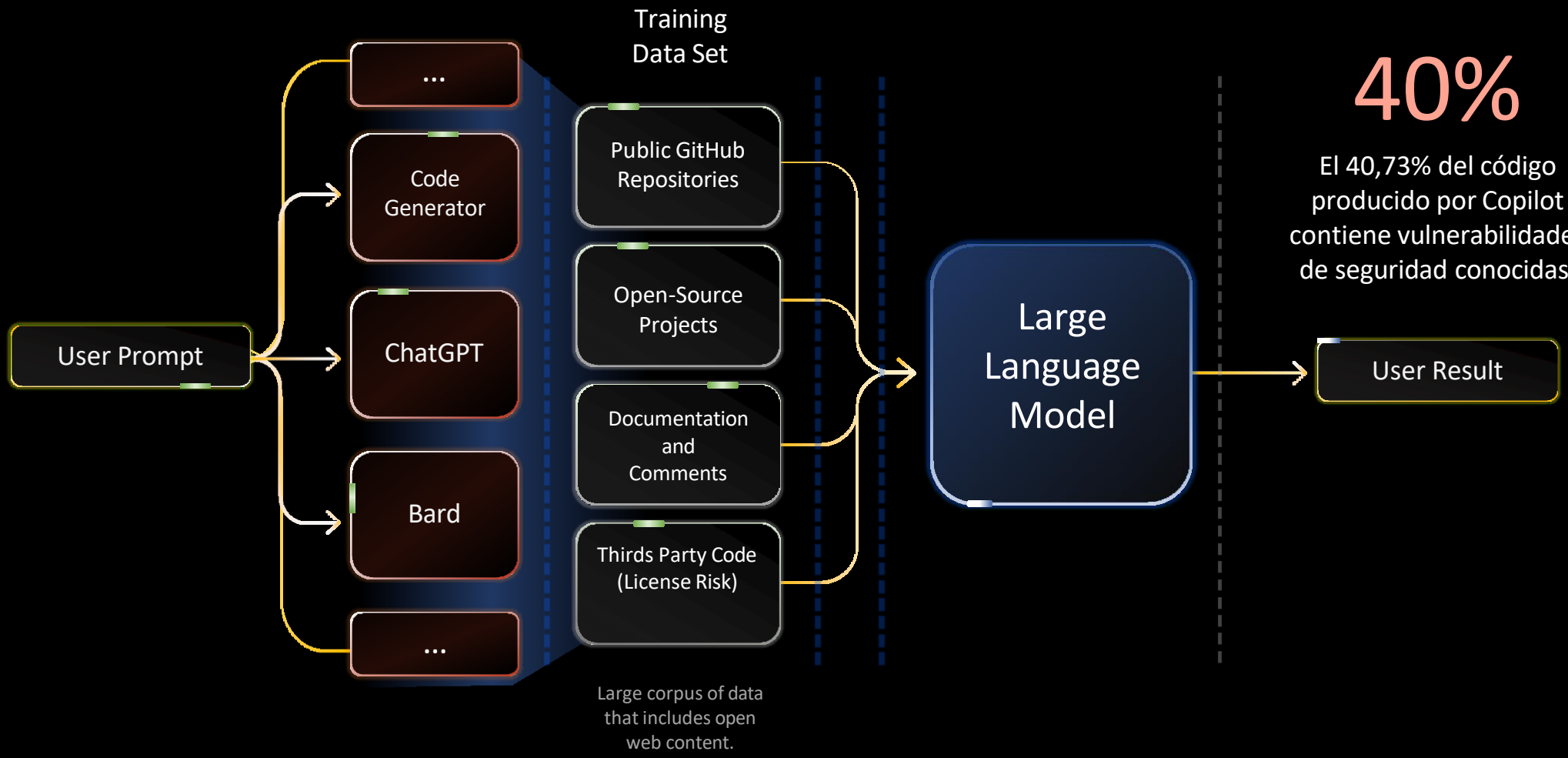
Generadores de código


Entrenar modelos con código abierto
vs
Eliminar cualquier vulnerabilidad antes de entrenar el modelo

Una encuesta de Gartner revela que el **45% de los ejecutivos** afirma que **ChatGPT** ha provocado un **aumento de la inversión en IA**

El 70% de las organizaciones se encuentra actualmente en modo de exploración con IA generativa

Large Language Models



40%

El 40,73% del código producido por Copilot contiene vulnerabilidades de seguridad conocidas.

Implicaciones de seguridad de los LLMs

Estudio de la Universidad de Cornell sobre generadores de código de IA

35%

De los 435 fragmentos de código generados por Copilot, el 35% contienen fallos de seguridad, en 6 lenguajes de programación.

Estudio de la Universidad de Stanford sobre generadores de código de IA

52%

El 52% de las respuestas de ChatGPT contienen imprecisiones y el 77% son absurdas cuando responden a preguntas de ingeniería de software.

Estudio de la Universidad de Nueva York en GitHub Copilot

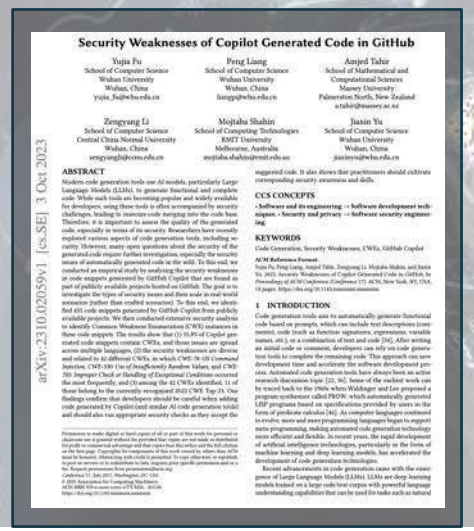
39%

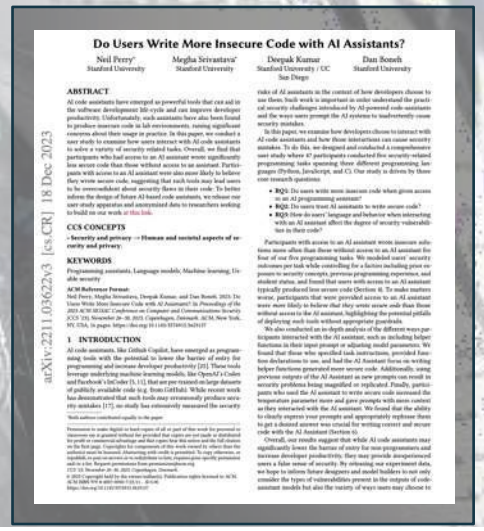
El 39,34% de los usuarios sigue prefiriendo las respuestas de ChatGPT por su exhaustividad y su estilo articulado.

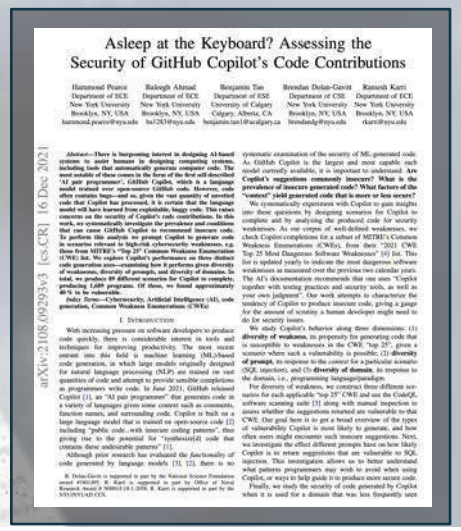
Universidad de Purdue sobre la precisión de ChatGPT

75%

El 75% de los desarrolladores han afirmado que GitHub CoPilot les hace codificar más rápido.


Security Weaknesses of Copilot Generated Code in GitHub


Do Users Write More Insecure Code with AI Assistants?


Asleep at the Keyboard? Assessing the Security of GitHub Copilot's Code Contributions


Who Answers It Better? An In-Depth Analysis of ChatGPT and Stack Overflow Answers to Software Engineering Questions

introducimos inadvertidamente
estas vulnerabilidades en nuestra
vida cotidiana

VERACODE

Whitepaper

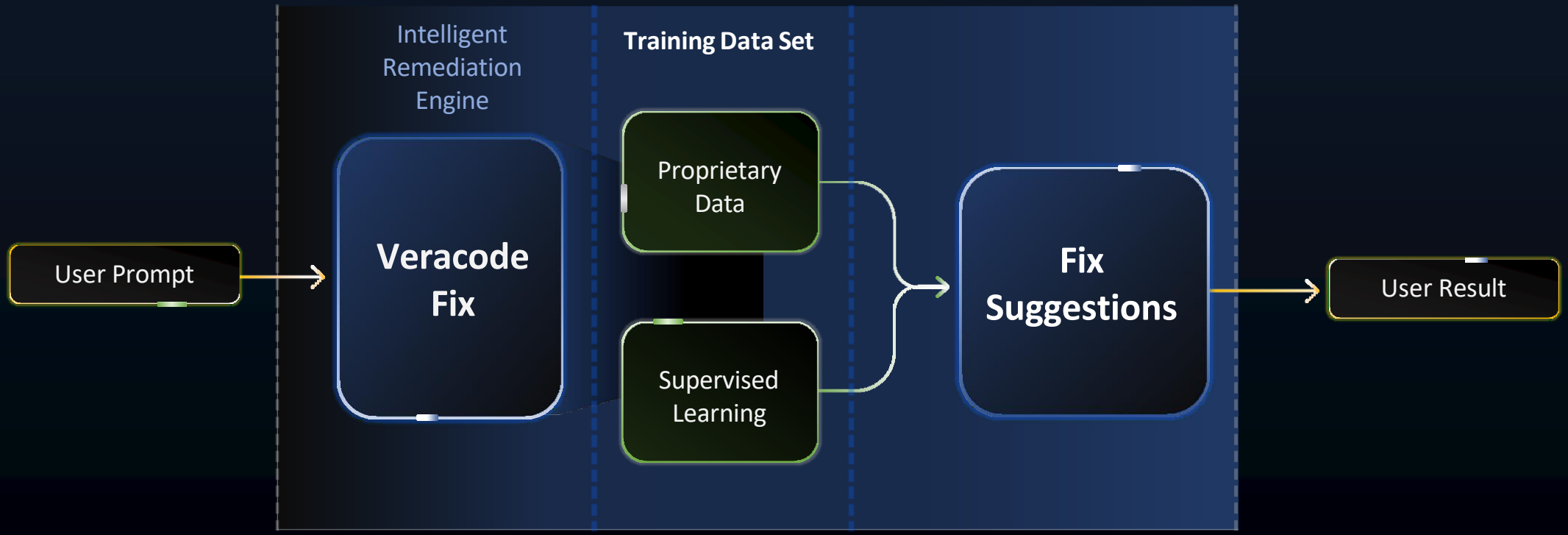
Veracode Fix: AI Code Remediation Done Right

"With Veracode Fix, developers receive precise guidance, reducing the time and effort needed to secure applications."

- Sebastian Wilke, Cybersecurity Manager, Banco Galicia

Veracode Fix Approach

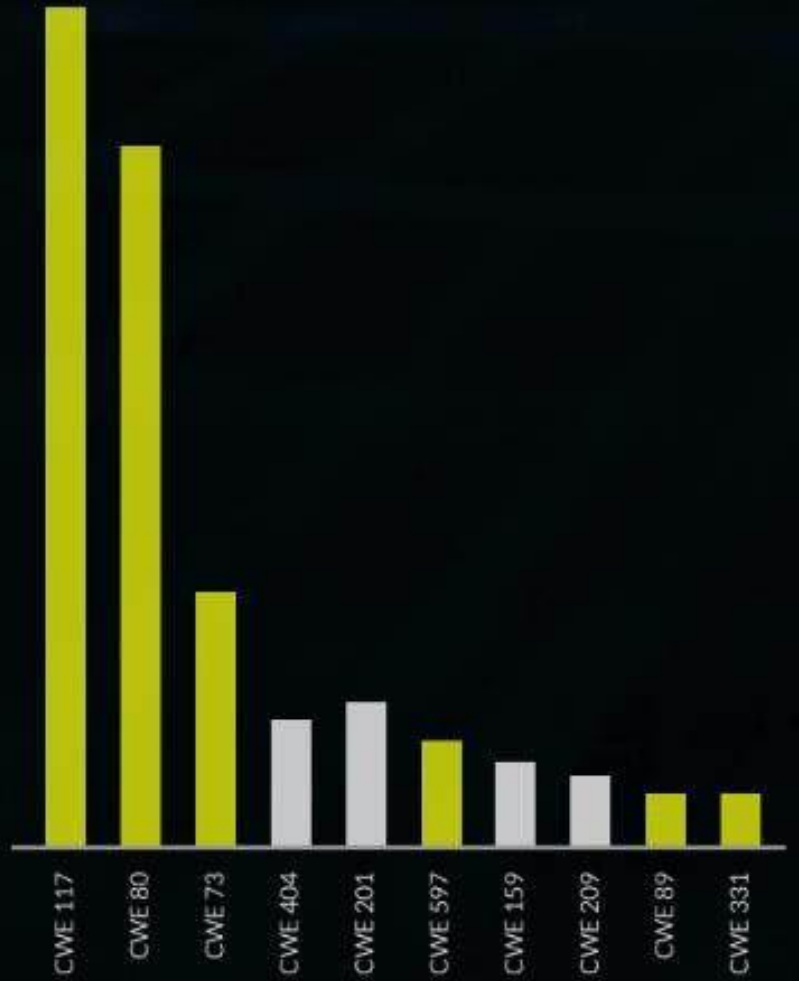
Conjunto de datos de Veracode	Garantía de procedencia del código	Respaldado por la plataforma de seguridad de software inteligente de Veracode	Cobertura todo lo que importa



Efficacy of Veracode Fix Across Programming Languages

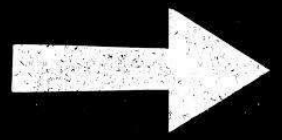
Percent of Veracode Static Analysis Java findings with Veracode Fix CWE coverage.

Top 10 Java CWE Static Analysis Findings



Veracode Fix revoluciona el proceso de remediación de vulnerabilidades, aprovechando el poder de la IA Generativa, para generar correcciones automáticas de fallos de seguridad.

Al entrenar el modelo GPT con datos cuidadosamente analizados y utilizando una amplia base de datos de parches de referencia escritos por nuestros investigadores de seguridad, Veracode Fix se convierte en una herramienta segura y eficiente.



Este enfoque mejorado con IA reduce reduce significativamente el tiempo de remediación de vulnerabilidades y por lo tanto la deuda técnica de seguridad

VERACODE

Application Risk Management Platform

Empowering the application security professionals and developers that create secure software for a safer world.

Use Cases

Secure Your SDLC

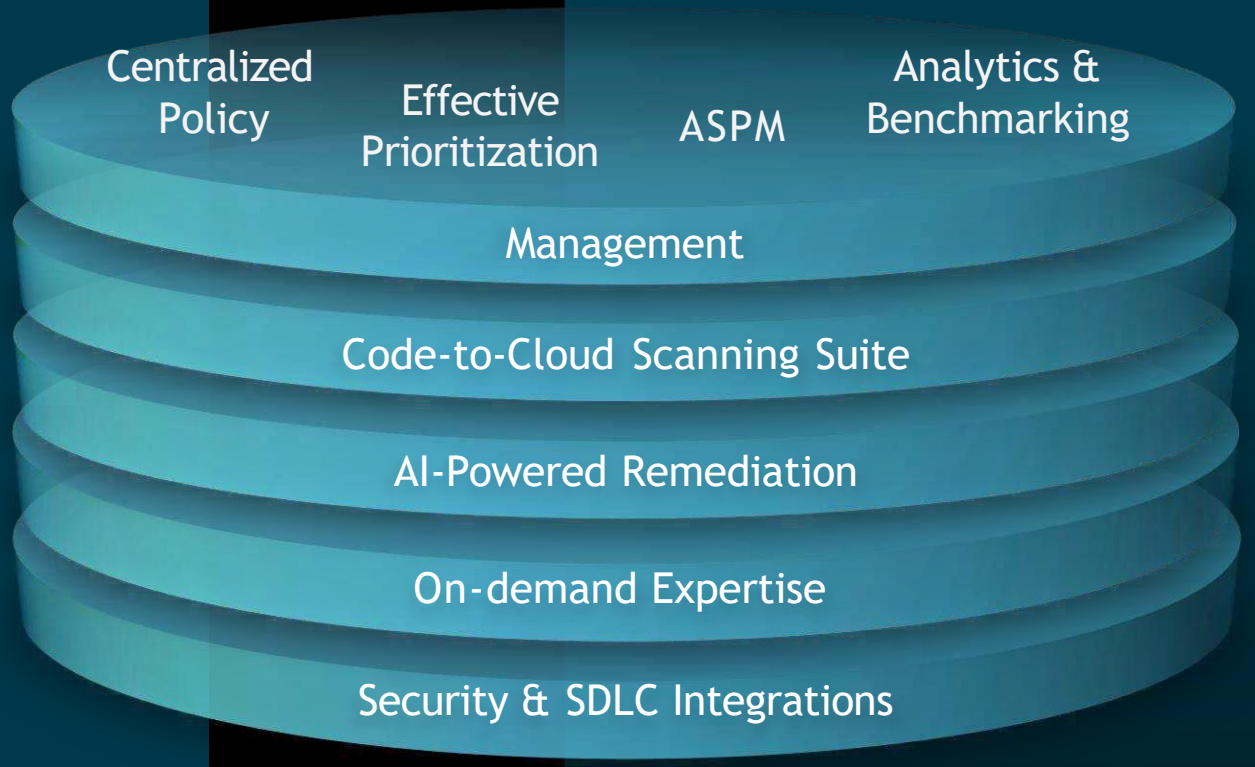
Protect Your Software Supply Chain

Remediate Risk

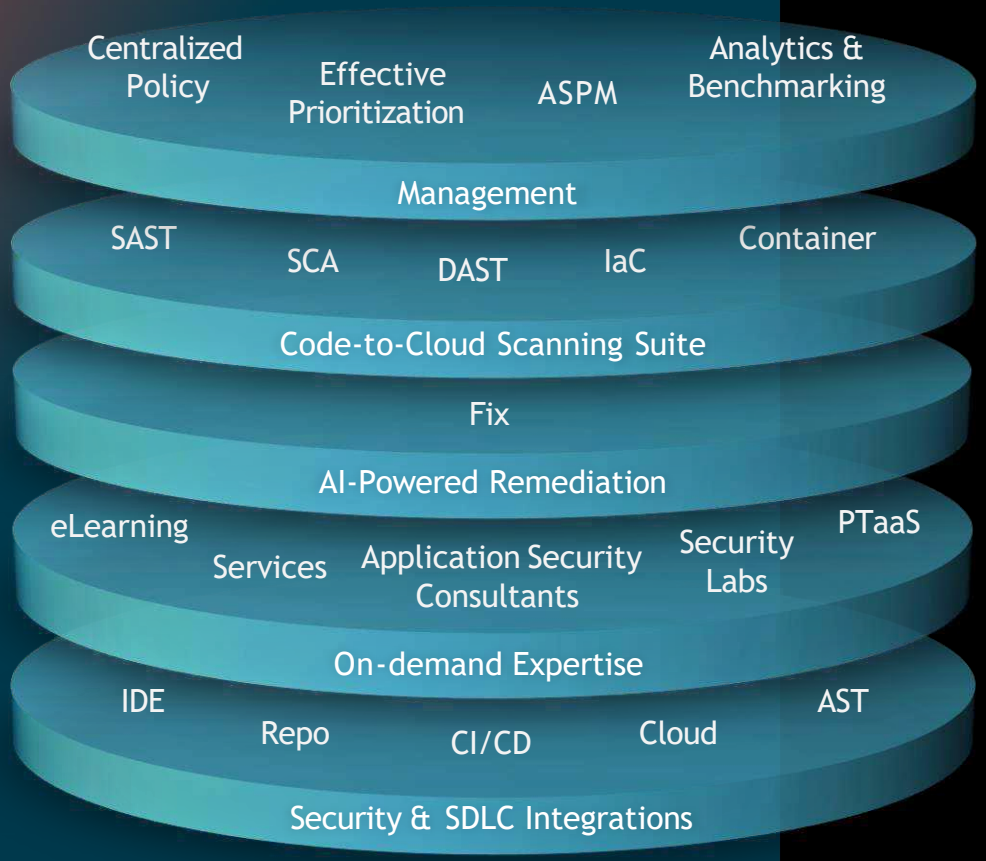
Stakeholders

Developer | Dev Ops | App Sec | Cloud Eng | CISO | Architect

Application Risk Management Platform



Application Risk Management Platform



Fast Start and Scale

- Automatically onboard developers
- Find and fix flaws in minutes

Actionable Visibility

- Code to Cloud Scanning Suite
- Highly accurate findings focus prioritization

Real-Time Flaw Remediation

- Rapid reduction of security debt
- Proactive flaw prevention

Securing The Code Pipeline

Continuously Find and Fix Flaws at Every Stage of The Modern Software Development Lifecycle

Veracode Intelligent Software Security Platform

Policy Management	Reporting, Analytics & Peer Benchmarking	Data residency EU, FedRAMP	Developer & Security Tool integrations	Governance Risk & Compliance

Open API accessibility

DISCOVER	BUILD	DEPLOY	PRODUCTION
External Assets	Veracode Fix	Supply Chain (SBOM)	Drift Detection
Internal Repository Assets	SAST & SCA	DAST	Container vulnerabilities/base OS
	Developer Exp. Repository Scanning	API Scanning	IaC misconfigurations
	Cloud Native Support	Break the build	Kubernetes security
	Registry & Repository Support		Auto Remediation

VERACODE


Gracias
VERACODE

¡Ahora te toca!

¿Tienes una idea de negocio en ciberseguridad, tu proyecto necesita de ciberseguridad?

¡Te ayudamos a emprender!

¡Apúntate a los próximos **talleres de emprendimiento**!

¡O solicita plaza en el programa de **Incubación de INCIBE Emprende**!

Club del Emprendimiento
www.club del emprendimiento.com

Ediciones anteriores

INCIBE Emprende

¡Te estamos esperando!

proyectos@clubdelemprendimiento.com

www.clubdelemprendimiento.com

incibe emprende

Programa de **Impulso a la Industria de la Ciberseguridad Nacional**

#INCIBEemprende

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

España | digital 2026

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

017

Club del Emprendimiento
www.club del emprendimiento.com