



Cuadro de "Las hilanderas" o la fábula de Aracne (Velázquez) Museo del Prado

Nace EVE, el algoritmo que anticipa cuándo somos más vulnerables frente a los ciberataques

- Los mitos que antaño hablaban de engaño, deseo y miedo, nos sirven para explicar los rasgos psicológicos que utilizan los ciberdelincuentes.
- Más información: **La inteligencia artificial será la aliada indiscutible de la ciberseguridad en 2025, pero también su talón de Aquiles**



Yolanda Rodríguez

Publicada

10 noviembre 2025 01:42h

Las claves

Se presenta EVE, un algoritmo predictivo que anticipa los momentos de mayor vulnerabilidad emocional ante ciberataques, analizando patrones psicológicos y respuestas emocionales.

La tecnología, pionera en neurociberseguridad, identifica cuándo un usuario es susceptible de ser engañado según su perfil emocional y contexto de decisión, sin analizar contraseñas ni configuraciones técnicas.

La presentación en el Museo del Prado relacionó obras de arte clásicas con situaciones de riesgo digital, ilustrando cómo la impulsividad, el miedo o la curiosidad pueden facilitar fraudes online.

EVE ha sido desarrollado por universidades y empresas tecnológicas españolas, con apoyo del INCIBE y fondos europeos, y pone el foco en la prevención y la educación como principales defensas frente a amenazas digitales.

En un inusual diálogo entre arte, psicología y tecnología, el Museo del Prado acogió esta semana la presentación de **EVE (*Emotions and Vulnerabilities Exposed and Protected*)**, un algoritmo predictivo diseñado para anticipar cuándo una persona es más vulnerable frente a los ciberataques.

La presentación prescindió de gráficos y paneles técnicos para apoyarse, en cambio, en seis obras maestras de la pinacoteca. El objetivo era recordar que la **ciberseguridad** no se juega solo en algoritmos, sino en la forma en que sentimos, decidimos y reaccionamos: se utilizó la historia del arte como un espejo para entender nuestros impulsos cuando navegamos por internet.

Para sobrevivir necesitamos defendernos de amenazas. Los mitos que antaño hablaban de engaño, deseo y miedo y ahora nos sirven para

explicar los rasgos psicológicos que los ciberdelincuentes explotan hoy en el mundo digital. Nuevos problemas, viejas soluciones... Los mitos clásicos hablaban de trampas y aprendizajes; hoy, **la ciberseguridad los traduce en sesgos, estímulos y decisiones digitales.**



Inteligencia artificial, ciberseguridad y talento marcan la agenda TI de 2025

Nuestro cerebro fue afinado para reaccionar ante las amenazas. Abrir un correo malicioso no nos va a matar, pero puede exponernos. EVE ayuda a conocer hasta qué punto estamos expuestos, incluso si creemos que “no, yo no, porque soy súper listo”.

EVE no analiza contraseñas ni configuraciones de red. Analiza **emociones y patrones psicológicos**. Según sus creadores, se trata de un software pionero en neurociberseguridad: capaz de identificar cuándo un usuario está más expuesto a ser engañado basándose en su **perfil emocional** y en el contexto en el que toma decisiones.

La vulnerabilidad digital empieza en la mente

Se trata de una herramienta que **analiza nuestras respuestas emocionales para anticipar riesgos en el entorno digital**. Sus creadores la describen como un “**algoritmo ético**”, diseñado para **predecir cuándo un usuario es más susceptible de caer en un engaño online** a partir de sus rasgos de personalidad y su estado psicológico.

El proyecto se adentra en un territorio poco explorado: **cómo el “ángulo ciego” de nuestra mente condiciona las decisiones que tomamos en internet**. Ese “**cuarto oscuro**”, explican, donde



Google advierte de una nueva era de ciberataques híbridos en Europa: objetivos críticos y desinformación coordinada

el cansancio, la prisa o el miedo **se imponen sobre el pensamiento racional** y abren la puerta al error.

Para ello, EVE analiza tres brújulas internas: **BIS (Behavioral Inhibition System): responde al miedo y a la evitación, nos paraliza o nos hace actuar precipitadamente por amenaza**; el **BAS (Behavioral Activation System): tendencia a actuar por impulso ante recompensas y reconocimiento, sin valorar contexto ni consecuencia**, y **NC**, la necesidad de cognición, la curiosidad por saber y comprender.

La tecnología no juzga, sino que identifica cuándo la persona está más expuesta y se anticipa desde el autoconocimiento. Como explicaron sus creadores, pasamos de la sabana natural, donde sobrevivíamos detectando el rugido de un león, a la *sabana digital*, donde sobrevivimos identificando el *phishing*: “No se trata de ser más desconfiados, sino de ser más conscientes”.

El arte como espejo psicológico

Bajo el título “**El arte de estar protegido**”, los impulsores de EVE guiaron al público por seis obras del Museo del Prado para explicar

cómo nuestras vulnerabilidades emocionales pueden abrir la puerta a un ciberataque. La propuesta hiló **mitología clásica, historia del arte y ciberseguridad** para lanzar una idea central: *“El caballo de Troya eres tú mismo”*.

En **“Mercurio y Argos”**, Velázquez narra cómo el gigante de los cien ojos cae víctima del engaño. La lección, trasladada al mundo digital, es clara: **cuando la atención se relaja, la astucia vence a la fuerza**. No importa lo preparado que uno se crea: un momento de distracción puede ser suficiente.

En **“Las Hilanderas”**, también de Velázquez, aparece otro patrón de riesgo: la **impulsividad**. Aracne, segura de su talento, desafía a la diosa Atenea sin medir las consecuencias. En clave digital, sería el **clic rápido**, la oferta que “parece demasiado buena”, el enlace que promete una recompensa inmediata: **el terreno favorito del fraude online**.



En “**El Rapto de Europa**” de Rubens aflora una vulnerabilidad distinta: la **curiosidad confiada**. Zeus, disfrazado de toro blanco, se acerca sin violencia a Europa. Igual que un correo convincente o un perfil aparentemente legítimo. “La lección es desconfiar de lo demasiado perfecto, aunque despierte nuestra curiosidad”.

La “**Cabeza de Medusa**” encarnó el miedo que paraliza. Muchos ataques se sostienen en mensajes urgentes —multas falsas, supuestos familiares en apuros— que buscan una reacción rápida. El consejo de los expertos fue sencillo: “**Hay que ser Perseo**”: detenerse, mirar de reojo, **verificar antes de actuar**. No decidir desde la urgencia.

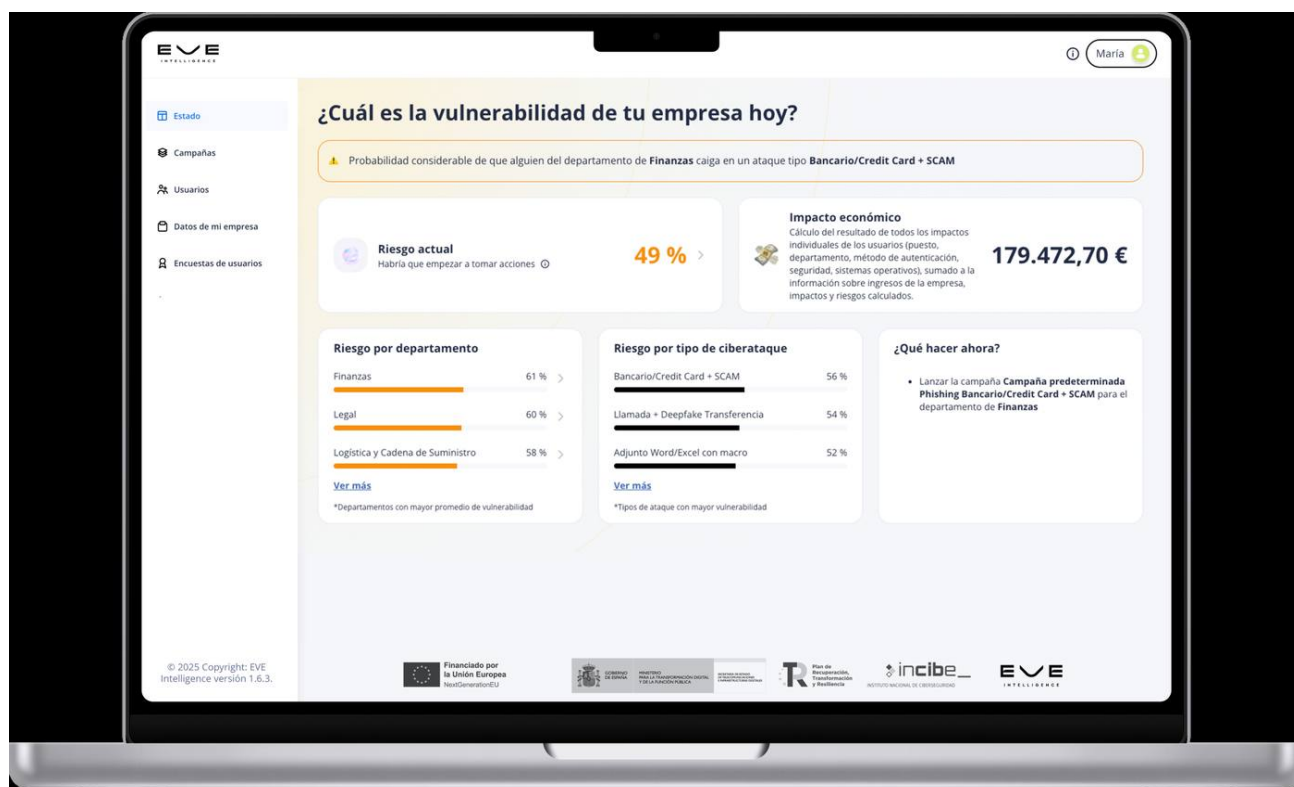
“**El Jardín de las Delicias**” del Bosco permitió explicar que **curiosidad, deseo y miedo** conviven también en nuestras decisiones digitales. El tríptico representa, de forma sorprendentemente actual, los tres sistemas psicológicos que analiza EVE: el miedo que frena, el impulso que empuja y la curiosidad que explora. Una obra del siglo XV convertida, por un momento, en **mapa mental de nuestro comportamiento en internet**. Todo el tríptico es una representación magistral de estas fuerzas que nos mueven.

Por último, “**El Jarrón del Tesoro del Delfín**” evocó el mito de **Narciso**: el riesgo de quedar atrapados en nuestra propia imagen, reforzada por redes y algoritmos. EVE, explicaron, **aspira a devolver perspectiva**, no a juzgar: mostrar cuándo somos más vulnerables y ayudar a reconocernos antes de caer.

Una revolución aún en camino

Marco Antonio Lozano, responsable de Sectores Estratégicos para Servicios de Ciberseguridad para Turismo, Ocio e Industria de Contenidos Digitales del **Instituto Nacional de Ciberseguridad (INCIBE)**, destacó que “es una aplicación revolucionaria, que tiene un enorme componente de innovación”. Según explicó a EL ESPAÑOL, “la herramienta tiene en cuenta estos tres parámetros: el BIS, el BAS y el componente emocional, que pertenecen al ámbito psicológico, para determinar el nivel de vulnerabilidad que tiene una persona en relación con los distintos tipos de incidentes de ciberseguridad”.

Aun así, advirtió: “que nos queda mucho camino por recorrer” porque “somos vulnerables”



Una desde la visión del CISO (desde la organización) EVE

Y recordó que la primera defensa no es tecnológica, sino humana, para ello subrayó que lo más importante es: “prevención, educación, entrenamiento y capacitación”. O, traducido a la vida diaria: información, práctica y “los cinco sentidos —incluido el sentido común— hay que estar muy pendientes”.

Un proyecto colectivo

EVE ha sido desarrollado por **TechHeroX**, **Ticsmart**, **Softcom**, la **Universidad Pontificia Comillas** y la **Universidad Autónoma de Madrid**, con la cofinanciación del **Instituto Nacional de Ciberseguridad (INCIBE)** a través de fondos **NextGenerationEU** del **Plan de Recuperación, Transformación y Resiliencia**.

La predicción que realiza el algoritmo tiene una base científica, elaborada por **Lucía Halty**, directora de la Cátedra de Innovación y Salud Mental Digital de la Universidad Pontificia Comillas, experta en investigación en psicopatía y neurociencia, personalidad y perfiles criminales y aplicación neurociencia en contextos forenses, en colaboración con **Eugenia Hernández**, directora de la UNINT (Unidad de Análisis de Inteligencia de la Universidad Autónoma de Madrid).