2025-11-27

Ciberseguridad en la UAM: entre la ética digital y el autocuidado

Autor: Redacción

Género: Nota Informativa

https://amexi.com.mx/comunicados-de-prensa/ciberseguridad-en-la-uam-entre-la-etica-digital-y-el-autocuidado/

Número 749

27 de noviembre de 2025

La IA puede ser "envenenada" para ofrecer respuestas erróneas a usuarios sin conocimientos técnicos

En la etapa actual de hiperconectividad, donde cada acción en línea puede abrir un acceso o activar un riesgo, la ciberseguridad funciona como un acto reflejo de autocuidado, afirmó el maestro José Gabriel Aguilar Martínez, jefe del Departamento de Seguridad de la Información en la Dirección de Tecnologías de la Información (DTI) de la Universidad Autónoma Metropolitana (UAM). Desde su responsabilidad institucional, explicó que su labor consiste en proteger datos, servicios y a la comunidad, cuyos procesos dependen cada vez más de plataformas digitales.

Durante esta entrevista que marca el principio de una campaña permanente sobre ciberseguridad, Aguilar Martínez expuso que la ciberseguridad descansa en tres pilares: confidencialidad, integridad y disponibilidad. Para ilustrarlo, describió el caso de un usuario que consulta calificaciones en el portal de administración escolar: sólo la persona autorizada debe acceder a esa información mediante su nombre de usuario y contraseña. La Institución procura que así ocurra. Con ello se garantiza la confidencialidad.

La integridad se refiere a que nadie altere datos sin permiso. La disponibilidad implica que el sistema responda cuando la persona lo requiera. Ese momento no depende del diseño del servicio, sino de la necesidad concreta del usuario durante un trámite o consulta.

La pandemia aceleró el tránsito hacia trámites digitales y aumentó la presencia pública de la identidad digital. Aguilar Martínez recordó que, con el confinamiento, la población recurrió a más servicios en línea. La identidad digital se compone de una cuenta, un perfil de usuario y, con frecuencia, un mecanismo de pago. La protección debe evitar que terceros usen esa combinación.

La suplantación de identidad se volvió una práctica común a través de llamadas, correos o mensajes SMS, por lo que la verificación previa de cualquier solicitud de información es indispensable.

Inteligencia artificial: posibilidades y riesgos

La inteligencia artificial (IA) transformó la interacción con dispositivos y sistemas. Aguilar Martínez reconoció que la IA mejora servicios y facilita tareas desde navegadores y equipos de trabajo. Sin embargo, también existe un sector que busca vulnerar sistemas o aprovechar fallas.

Una persona sin formación técnica puede recibir guías mínimas para intentar un ataque a un servidor o para tomar la identidad de otra persona. Además, la IA puede ser "envenenada" de forma deliberada para entregar datos falsos a quienes no cuentan con contexto o experiencia, e incrementa la exposición a daños.

El especialista señaló que cualquier dispositivo conectado a Internet puede ser blanco de ataques, desde intentos de saturación de servidores hasta esquemas de extorsión. Los riesgos abarcan diversas modalidades: mensajes de

WhatsApp que buscan obtener datos, enlaces que capturan contraseñas o llamadas que solicitan códigos de acceso.

Frente a esta situación, la DTI impulsa un programa de concientización para la comunidad universitaria. El objetivo es ofrecer un lenguaje común que permita a las personas reconocer términos como "ingeniería social", "hacker" o "usurpación de identidad". Este proceso incluye talleres, cápsulas, podcasts y materiales escritos. Aunque aún no constituye un plan institucional, la intención es ampliar su alcance para que estudiantes, docentes y personal administrativo compartan esta información con su entorno cercano.

El desafío incluye la coexistencia de generaciones con grados distintos de familiaridad tecnológica. Aguilar Martínez apuntó que mientras parte de la comunidad nació con el acceso a dispositivos digitales, otra parte llegó a ellos en una etapa posterior, situación abre espacios que la delincuencia explota.

Infraestructura y estándares para fortalecer la seguridad institucional

El Día Mundial de la Ciberseguridad, conmemorado en el año el 30 de noviembre, e impulsado desde 1988 por la Association for Computing Machinery (ACM) tras el impacto del gusano Morris, busca promover conciencia sobre protección de información digital. Desde entonces, esta fecha funciona como recordatorio sobre la necesidad de fortalecer prácticas de seguridad y construir criterios de prevención ante riesgos que cambian a gran velocidad.

En la UAM, la seguridad se apoya en estándares internacionales como ISO y en marcos de trabajo como el del National Institute of Standards and Technology (NIST). El maestro Aguilar Martínez detalló que actuar de manera preventiva reduce costos, no sólo económicos. Un incidente afecta operaciones, procesos académicos y administrativos, así como la confianza de la comunidad.

Expuso que la fortaleza técnica enfrenta límites. La complejidad de contraseñas, por ejemplo, cambió con la evolución del poder de cómputo. Una contraseña de ocho caracteres puede romperse en segundos. Una de 25 o 30 caracteres, con letras, números y signos, resiste más, pero no de forma indefinida. Este escenario preocupa a quienes resguardan la integridad de los sistemas institucionales.

El avance del cómputo cuántico plantea riesgos mayores. Su capacidad de procesamiento podría transformar los tiempos necesarios para romper claves robustas. A esto se suma el crecimiento de la desinformación creada por IA, que puede afectar decisiones públicas y privadas. Ninguna medida de seguridad resulta efectiva y toda tecnología opera con riesgos inherentes.

Aguilar Martínez insistió en que la ciberseguridad debe asumirse como acto reflejo. Comparó la acción de proteger datos con el hábito de revisar ambos lados antes de cruzar una calle, incluso cuando el tránsito marca una dirección. Del mismo modo, el usuario debe dudar antes de abrir un enlace o de entregar datos confidenciales.

Para concluir, subrayó que el cuidado de la información es una responsabilidad compartida. La Institución desarrolla infraestructura y protocolos, pero la conducta del usuario cierra el círculo de protección. Validar fuentes, usar contraseñas robustas, activar factores adicionales de autenticación y evitar compartir información con desconocidos son prácticas que deben incorporarse de forma sistemática. Solo así se reduce la superficie de riesgo ante amenazas que evolucionan con rapidez.