



Comunicado No. 02
Ciudad de México, 11 de enero de 2026

Dispuesto IPN a apoyar en ciberseguridad para la Copa Mundial de la FIFA 2026

- Necesario, el fortalecimiento de los protocolos ante este evento de gran magnitud, señala el especialista del Centro de Investigación en Computación (CIC), Eleazar Aguirre Anaya
- Transferencia de tecnología, estrategias y protocolos de contención, erradicación y respuesta, pone el IPN a disposición de dependencias e instancias organizadoras

El Instituto Politécnico Nacional (IPN) pone a disposición de las autoridades la transferencia de tecnología, así como estrategias y protocolos de contención, erradicación y respuesta en materia de ciberseguridad, en el contexto de la Copa Mundial de la FIFA 2026 que se llevará a cabo en México, a fin de fortalecer la protección de las instituciones e instancias organizadoras nacionales, afirmó el científico del Laboratorio de Ciberseguridad del Centro de Investigación en Computación (CIC), Eleazar Aguirre Anaya.

Subrayó que eventos de gran magnitud como el Mundial de Fútbol —que en esta edición se realizará a partir del 11 de junio en México, Estados Unidos y Canadá— exigen cambios en los protocolos de ciberseguridad, así como una actuación proactiva y una preparación integral para estar listos antes, durante y después del evento. Afortunadamente —acentuó— existe coordinación entre los tres países para atender los desafíos en el ciberespacio que pudieran presentarse a raíz de este acontecimiento global.

Aguirre Anaya explicó que la ciberseguridad comprende cuatro momentos: el primero es la preparación de estrategias ante posibles vulneraciones para su atención; el segundo es la contención de los eventos, con el fin de evitar que sus efectos se extiendan; el tercero corresponde a la erradicación y, por último, el cuarto consiste en aprovechar el conocimiento adquirido para anticiparse a futuros incidentes, lo que se conoce como ciberresiliencia.

Reconoció que la ciberseguridad sigue un ciclo en el que, durante la implementación de los protocolos, se requiere la participación de especialistas en monitoreo, gestión de vulnerabilidades, contención y respuesta inmediata a incidentes, implementación de controles y definición de estrategias de resiliencia.

Por este motivo —indicó el especialista, doctor en Comunicaciones y Electrónica, cuyos temas de investigación abarcan la seguridad en redes, sistemas operativos, forense digital y seguridad ofensiva— se requiere un amplio abanico de expertos, al menos 12 tipos de especialistas en ciberseguridad, de acuerdo con la European Union Agency for Cybersecurity, para atender este fenómeno.



Sostuvo que la ciberseguridad es un habilitador de la economía y del desarrollo de los países, ya que cuando una nación avanza en el fortalecimiento de sus programas en la materia, se consolida toda la cadena de respuesta de organismos y empresas, con impacto a nivel local, nacional y global.

El doctor Eleazar Aguirre refirió que, a nivel internacional, los derechos humanos y los datos personales en el ciberespacio deben estar plenamente protegidos.

En el contexto internacional —enfatizó— México está dando un paso al frente en materia de ciberseguridad a nivel regional y, con el apoyo de universidades, centros de investigación y dependencias gubernamentales, se trabaja en el fortalecimiento de redes de colaboración para la atención de problemas prioritarios.

Para más información visita www.ipn.mx

====000====