Release No. 02
Mexico City, January 11th, 2026

IPN Ready to Support Cybersecurity Efforts for the FIFA World Cup 2026

- **Strengthening cybersecurity protocols is essential for an event of this scale, says Eleazar Aguirre Anaya, specialist at the Centro de Investigación en Computación (CIC)**
- **IPN offers technology transfer, as well as containment, eradication, and response strategies and protocols, to government agencies and organizing bodies**

The Instituto Politécnico Nacional (IPN) has made its expertise available to authorities through the transfer of technology, along with cybersecurity strategies and protocols for containment, eradication, and response, in the context of the FIFA World Cup 2026, which will be hosted in Mexico. This initiative aims to strengthen the protection of national institutions and organizing bodies, stated Eleazar Aguirre Anaya, researcher at the Cybersecurity Laboratory of the Centro de Investigación en Computación (CIC).

He emphasized that large-scale events such as the FIFA World Cup—scheduled to begin on June 11 across Mexico, the United States, and Canada—require updates to cybersecurity protocols, as well as proactive action and comprehensive preparation before, during, and after the event. Fortunately, he noted, there is coordination among the three host countries to address potential cybersecurity challenges arising from this global event.

Aguirre Anaya explained that cybersecurity involves four key stages. The first is preparation, which focuses on developing strategies to address potential vulnerabilities. The second stage is containment, aimed at preventing incidents from spreading. The third involves eradication, and the fourth consists of leveraging the knowledge gained to anticipate future incidents—a process known as cyber resilience.

He acknowledged that cybersecurity follows a continuous cycle in which the implementation of protocols requires the participation of specialists in monitoring, vulnerability management, containment, immediate incident response, control implementation, and the definition of resilience strategies.

For this reason, said Aguirre Anaya—who holds a PhD in Communications and Electronics and whose research focuses on network security, operating systems, digital forensics, and offensive security—a broad range of experts is required. According to the European Union Agency for Cybersecurity, at least 12 different types of cybersecurity specialists are needed to effectively address this field.

He further noted that cybersecurity acts as an enabler of economic growth and national development. When a country strengthens its cybersecurity programs, the entire response chain involving institutions and companies is reinforced, generating impact at the local, national, and global levels.

At the international level, Aguirre Anaya stressed that human rights and the protection of personal data in cyberspace must be fully safeguarded.

Within this global context, he emphasized that Mexico is taking a proactive role in regional cybersecurity efforts. With the support of universities, research centers, and government agencies, the country is working to strengthen collaborative networks to address priority challenges in this field.

For more information, visit www.ipn.mx

===000===