

Appendix 5. To the "Digital security" section

List of cybersecurity standards against which the KICS for Nodes and KICS for Network solutions, which are part of the KICS platform, are certified, as well as other international laws and industry standards whose requirements they address or help implement:

- ISO/IEC 27001 IEC 27002 (DIN 2008 in Germany) is a standard that establishes requirements for the creation, deployment, maintenance and continuous improvement of an information security management system within an organization;
- ISO/IEC 27019 (DIN 2011 in Germany) is a standard used to ensure information security in the energy sector;
- ISO/IEC 27032 is a standard that addresses internet security issues and provides recommendations for addressing the most common threats in this area (social engineering, zero-day attacks, spyware, etc.);
- ISO/IEC 15408, historically known as the "Common Criteria," represents the accumulated experience of various countries in the development and practical use of criteria for assessing the security of information technology;
- IEC 62443 (ANSI/ISA99) is a series of standards that contains requirements for the design of cybersecurity management systems for industrial control systems and SCADA;
- The NIST CSF is recommendations for ensuring the security of industrial control systems developed by the US National Institute of Standards and Technology (NIST), supported by, among others, ONG-C2M2, API-1164, TSA PSF, and CISA;
- NIST SP 800-82 is the US guide for securing industrial control systems (ICS), covering risk management, access control, incident response, security monitoring, and more;
- NERC CIP is a set of cybersecurity standards for critical infrastructure and power grid protection in the United States, which are also being adopted by some Latin American countries;
- NIS 2 Directive (EU) 2022/2555 is a new EU directive on cybersecurity;
- NIS/NIS2 is the first pan-European directive on cybersecurity, establishing a higher and more uniform level of security for network and information systems in the EU;
- IEC 62351 is standards for the security of power control systems and associated utility systems. It specifies requirements for security, protection measures, and communications networks in the power industry;
- IMO MSC.428(98) is a Maritime Safety Committee resolution that provides guidance on cyber risk management in the maritime industry as part of safety management systems;
- ICAO is a cybersecurity strategy for aviation¹;
- IAEA Nuclear Security Series No. 17-T (Rev. 1) is methods of ensuring computer security for nuclear facilities.

¹ FAA Advisory Circular 119-1 - Airworthiness and Operational Approval of Aircraft Network Security Program (ANSP).