Mexicali, B.C., February 25th, 2026.

Through this document, we inform you that CETYS University has had an Information Security Program since 2018.

This is the Vision on Cybersecurity:

CETYS UNIVERSITY/IENAC is committed to ensuring the confidentiality, integrity, and availability of institutional information in the execution of its processes, seeking the continuity of services and accountability assurance, for the benefit of the CETYS Community, supported by cutting-edge technology and the continuous training of its staff.

The 2026 Cybersecurity Strategy integrates the following points:

a) Plan, Policy, and Procedures

a. Policies and procedures are being updated according to the guidelines provided by the various organizations that audit CETYS University.
b. The IENAC has a risk map that is updated and reviewed every 6 months.
c. There are two types of Security Committees; a Technical Security Committee made up of IT staff and an Operational Security Committee made up of various administrative areas from the 3 campuses.

b) Education for users and responsible personnel.

a. We currently have ongoing training campaigns for staff.
b. This year, the strategy includes providing us with online training tools with Kymatio the last year and Know be 4 for 2026.

c) Information protection and compliance with regulations.

a. Security controls are kept up to date because they go hand in hand with the Incident Plan.
b. Processes that allow PCI reaccreditation and Security audits are reinforced.
c. All employees sign a confidentiality agreement when they start working at CETYS UNIVERSITY.
d. In contracts with suppliers, clauses are established regarding information handling, supplier responsibilities, and controls to be followed.
e. Psychology students receive semi-annual training on the use, handling, and generation of personal data when preparing a clinical record.

d) Network security and technologies.

a. There is a plan for automating monitoring and detection processes.
b. There is a training plan for IT staff on how to implement and use network security tools.

e) Secure application development.

a. There is a plan to minimize the risk of vulnerabilities in in-house developed applications.
b. Developers have an annual training plan on secure development.
c. There is a list of security guidelines for acquiring new software.

f) Effective incident response.

a. CETYS UNIVERSIDAD has an Incident Response plan that stipulates the activities to be carried out and who is the responsible personnel to execute the activity, notify it, and close it.

b. Based on the incidents, an analysis is conducted from which corrective actions are derived that involve reviewing controls and updating the risk map.

g) Monitoring, metrics, and improvements.

a. CETYS UNIVERSIDAD has metrics that are used to support improvements as part of the Continuous Improvement Process.

MSI. Nadxiieli Esparza Avendaño.

Information Security and Compliance Coordinator