TICDEFENSE®
CYBERSECURITY.

Founded in 2017, TIC Defense® is a global cybersecurity company with a presence in **America, Europe and Asia**, we help Organizations protect themselves against cyber risks, defend themselves and limit the severity of attacks and ensure continued survival despite an attack.

WWW.**TICDEFENSE**.COM

CERTIFICATIONS

TICDEFENSE® CYBERSECURITY.

PCI DSS QSA ACCREDITATION

The Payment Card Industry Data Security Standard (PCI-DSS) is a set of requirements that ensure that companies that store, process, or transmit credit card information provide a secure environment for their customer data. www.pcisecuritystandards.org

WE ARE A COMPANY CERTIFIED BY THE INTERNATIONAL ORGANIZATION APPLUS MÉXICO S.A. OF C.V IN THE NORMS:

- **ISO 9001**: Quality Management System
- **ISO 20000-1**: Information Technology Service Management System
- **ISO 22301**: Business Continuity Management System
- **ISO 27001**: Information Security Management System
- **ISO 37001**: Anti-bribery Management System

GLOBAL CREST CERTIFICATION IN THE PENTEST SPECIALTY

CREST works to give organizations the confidence that they are hiring qualified individuals with up-to-date knowledge, skills, and competency on the latest vulnerabilities and techniques used by real attackers www.crest-approved.org

ACCREDITED CYBER INCIDENT RESPONSE TEAM

- Accreditation as National Computer Security Incident Response Teams (CSIRTs) by the Software Engineering Institute (SEI) of Carnegie Mellon University www.sei.cmu.edu
- Accreditation as Spanish Cybersecurity and Incident Management Teams by www.csirt.es
- Accreditation as Incident Response and Security Teams by the global Forum of Incident Response and Security Teams www.first.org

TIC DEFENSE is the only private agency in the world as a CSIRT.

ACKNOWLEDGMENTS

THE PROCESSES CERTIFIEDIN ISO STANDARDS ARE:

- Vulnerability scan
- Penetration tests
- Risk Analysis and Management
- Analysis and External Monitoring of information
- Network Operations Center "NOC"
- Security Operations Center "SOC"
- Detection, Analysis and Managed Response
- Computer Emergency Response
- Cybersecurity Services
- Digital Forensics
- Security government
- Normative compliance
- Digital Information Analysis
- Professionalization and Organizational Awareness
- Digital Protection of Corporate Identity
- Cybersecurity Consulting in Operational Technologies "OT", Industrial, Internet of Things "IoT" and Cloud Environments
- RED TEAM, BLUE TEAM and PURPLE TEAM Adversary Modeling
- Security Analysis of Application Source Code and Consulting in the Secure Development Life Cycle "SDLC"
- Help Desk Specialized in the Attention and Management of Information Security Incidents

MAIN SERVICES

- Specialized service in PCI DSS QSA (PCIQSA)
- Governance, Risks and Regulatory Compliance (GRC)
- Point-to-point Managed Cybersecurity Service
- Cybersecurity Operations Center
- Cybersecurity Awareness and Training Service (CATS)
- Assessment, Pentest and Vulnerability Analysis Service (APVAS)
- Red Team Services (RTS)
- Secure Development Life Cycle (SDLC)
- Supply Chain Security (SCS)
- Cloud Security (CS)
- Industrial Cybersecurity Services (ICS)
- Computer Emergency Response Services (CSIRT)
- Cyber Resilience Services (CRES)
- Cyber Intelligence and Threat Hunting Services (CITHS)
- Cyber Patrolling and Corporate Cyber Defense Services (CPCDS)

HUMAN CAPACITY

There is a minimum staff of **120 specialists**; our specialists are certified in the following frameworks:

- **CEH:** Certified Ethical Hacker de EC-Council.
- **OSCP:** Offensive Security Certified Professional of Offensive Security
- Certified Network Defender de EC-Council
- Computer Hacking Forensic Investigator
- **CISSP:** Certified Information Systems Security Profesional
- **CISM:** Certified Information Security Manager
- **CISA:** Certified Information System Auditor
- **PECB:** Certified Auditor Leader
- Certified Data Privacy Professional
- **GIAC:** GPEN, GAPT, GCFA
- And others

EXPERIENCE CAPACITY

We have the support of the experience of more than **300** organizational clients, the main sectors are listed below:

- Government
- Banking and financial sector
- Automotive section
- Transfer of securities
- Hospitality
- Travel agency
- Retail
- Communication
- Manufacturing
- Energy
- Insurance
- Department stores
- And others

TICDEFENSE®
CYBERSECURITY.

CORPORATE

Séneca 134 Int. 301, Col. Los Morales, C.P. 11540
Del. Miguel Hidalgo, CDMX.

International presence: Spain, United States of America, Dominican Republic, Puerto Rico, Panama, Colombia, Peru, Chile and Qatar.

CYBERSECURITY APPLICATION CAPACITY

We have our own authorship platforms, such as:

- Cyber Patrol Engines
- Phishing Detection Platform
- Cyber Threat Intelligence Platform
- Infrastructure and Application Vulnerability Scanners
- Application source code analyzers
- Virtual campuses
- Incident response platforms
- Helpdesk specialized in cybersecurity
- Deception Detection Systems, digital polygraphs

TICDEFENSE®
CYBERSECURITY.

CYBERSECURITY INFRASTRUCTURE CAPACITY

The following specialized infrastructure is available:

- Cybersecurity Operations Center and Attention to Cyber Incidents "**CYBERSOC**", with the following components:
  - Monitoring 7/24/365
  - Help desk
  - Prevention, detection and response
  - Vulnerability Management
  - Security correlation
  - Intrusion detection
  - Behavior monitoring
  - Asset Discovery
- Threat Intelligence Center
- Digital forensic laboratory
- Intelligence Center for Information Analysis on the internet and deep networks for brand protection

TICDEFENSE®
CYBERSECURITY.

INTERNATIONAL COLLABORATION AGREEMENTS

with INTERNATIONAL ASSOCIATION OF FINANCIAL CRIMES INVESTIGATORS

TIC DEFENSE has a collaboration protocol with the "INTERPOL Working Group of the Americas of Heads of Units to Combat Cybercrime" with the following scope:

- Share relevant information about incidents and any other type of information that is considered useful in cybersecurity matters.
- Collaborate with other similar forums and initiatives at a national and international level.
- Share information on recent attacks affecting critical infrastructure
- Generate protection and defense strategies for critical cyber infrastructure.
- Share scientific research for the prevention and investigation of cybercrimes.
- Share indicators and statistics of computer crimes for the design of prevention strategies.
- Promote actions to consolidate cyber security schemes that contribute to the development of digital economy.
- Strengthen the digital incident identification, prevention and management scheme.

INTERNATIONAL ASSOCIATION OF FINANCIAL CRIMES INVESTIGATORS