APOTECH
We make IT happen

Protecting your business through our Security Services to safeguard your assets from common and advanced cyber threats.

Cybersecurity Technologies

83% of companies say they have experienced at least one cyber-attack in the last 12 months[1]

Addressing Industry Challenges

- The cyber threat landscape is constantly evolving, and companies are facing increasingly more sophisticated andpersistent attacks.

- With the adoption of cloud technologies and the growth of data, enterprises face challenges in managing and protectingan increasingly complex IT and network infrastructure.

- Enterprises are facing increasingly sophisticated threats. These threats can evade traditional security solutions and compromise endpoints.

- Organizations are increasingly vulnerable and exposed to fallvictim to application security threats.

Scope of our services:

- ◎ Identify sensitive information and ensure that it's protected, available, and integrated, while complying with data protection regulations.

- ◎ Detect, protect and respond to cyber threats in critical infrastructure.

- ◎ Analyze and Detect Threats and Vulnerabilities in applications and during software development.

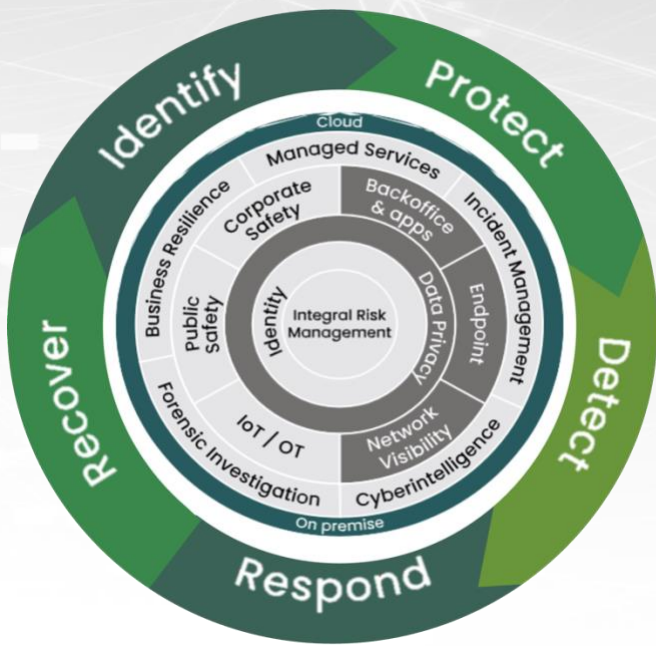| Network Protection	Endpoint Protection	Data Privacy	Application Security

[1] KPMG
https://assets.kpmg.com/content/dam/kpmg/ar/pdf/2022/triple-amenaza-en-%20las-americas-2022-kpmg-fraud-outlook-esp-ar.pdf

Discover all of Apotech's benefits. Get a quote at: **ruben.castaneda@apotechgroup.com**

We offer technical support, including implementation and managed services. In addition to options forthe different needs of organizations.

Network Protection	Endpoint Protection	Data Privacy	Application Security
- Web browsing and DNS protection -Advanced traffic inspection -Internal application security	- Endpoint management and monitoring -Endpoint Security -Investigation and Response	-Backups -Disaster recovery -File Integrity and data loss prevention	-Optimization and protection against attacks -Advanced attack protection -Reporting and analytics
-Control of allowed traffic and prioritization of bandwidth -Interconnection of branch offices or remote sites -Visualization of network flows interacting with your equipment -Simplify operation -Minimize the risks of IT security incidents	-Visibility into hardware inventory at each endpoint -Monitoring of basic security and risks identified at the endpoint -Control of devices that can be connected to the server and copy/paste or screen capture operations on your server -Minimize risks of IT security incidents -Simplifies operation by connecting to all servers centrally	- Visibility of critical information flow and backups - Compliance with PCI, SOX, NIST, HIPAA, etc. regulations and standards -Simplified the operation of automated backup creation, agile disaster recovery and automated monitoring of the integrity of critical files - Minimize the risks of IT security incidents - Business continuity by reducing the time to loss by anticipating disaster recovery methods	-Authorized traffic control -Visibility of traffic directed to your applications and data retention in the console for 90 days -Simplification of operation, through specific protection for web applications, optimizes response times and improves user experience -Minimize the risks of IT security incidents