

Focus on Growth, We'll Handle the Threats: **SEIDOR Cybersecurity**

SEIDOR North America



It's not a question of whether our business will be compromised, but when

At SEIDOR, we accept responsibility for our customers' digital security as if it were our own in order to ensure a secure environment and business continuity through commitment and engagement. To do this, we base our actions on two levels:



Managed cybersecurity: SEIDOR-CSIRT

Reducing risk and responding to security incidents.



Information Security Consulting Products

We manage cyber strategy, risk, and compliance.



Develop and offer training and awareness

Manage your organisation's digital identity and reputation.



Cybersecurity Office

Definition and deployment of a cyber security strategy.



Technical audits

Assess the current state of the organization in terms of protection, control and security measures.



Prevention

Proactive management of infrastructures must be fundamental to keep the organisation safe.

Implementation of Fast-Track Services to ensure maximum security with minimum implementation times



SOC

Cybersecurity Monitoring



ERI

Incident Response Teams



A&I

Alerts and Warnings

Cybersecurity as a Service

- 24x7 monitoring
- Attack detection and alerting
- Service reporting
- Security intelligence sources
- 24x7 infrastructure operation
- Use case implementation
- Multi-vendor solution integration
- Workstation analysis
- Action plan elaboration
- Remote intervention

Key services of the SEIDOR CSIRT



SOC (Security Operations Center) - Monitoring of security events and incident detection, as well as dashboards depicting service evolution and recommendations for security improvements.



Cyber Intelligence, through the collection and analysis of information from various available sources regarding new vulnerabilities and threats, as well as the communication of the generated cyber intelligence.



DFIR – Digital Forensics and Incident Response



Sharing technical information about incidents with other CSIRTs



Definition of security alerts based on customized requirements



Development of **security solutions**



Continuous vulnerability analysis and management

What makes us different

We offer a complete portfolio of solutions and services to promote the competitiveness and transformation of the organizations.



45 countries

more than 85 offices in the USA, Europe, LATAM, , Middle East, Africa and Asia



9,000+

worldwide



8,500 customers+

large enterprises, SMEs and Public Sector



\$1B USD

annual revenue



■ Direct presence

■ Presence including partners



Google Cloud Platform



Azure



Microsoft



M I G N O W