cecib
centro de estudios en ciberseguridad

ADECUARSE
IT COUNSELING
http://www.adecuarse.com/

Cibersecurity Controls: Product/Process - Matrix

NIST RMF

FRAMEWORK

CIS Controls® Version 8

NIST Risk Management Framework

Categorize System | Select Controls | Implement Controls | Assess Controls | Authorize Systems | Monitor Controls

Cyberdefense Matrix /NIST Cybersecurity Framework (+Zero_Trust_Profile/ Ransomware_Profile) / VS Security Controls (CIS 18) - Maturity Model

Threat Modeling Framework

Define | Diagram | Identify | Mitigate | Validate

Identify PRE INCIDENT **Protect** | WOW | POST INCIDENT **Detect** **Respond** **Recover**

Identify - Devices

01 – Asset Management
02 - Host Configuration Manager
03 - Host Vulnerability scanning
04 - Certificate Manager (Devices)

Protect - Devices

05 - Endpoint Protection (EPP) - Antimalware
02 - Host Configuration Manager
06 - Mobile Device Management (MDM)
07 - Host Intrusion Prevention (HIPS)
09 - Soft delivery and Patch Manager
10 - Privileged Access Management (PAM)
11 - Public Key Infrastructure (PKI)

Detect - Devices

12 - Endpoint detection and response (EDR)
13 - User Endpoint behavior analytics (UEBA)
16 - File Integrity Monitoring (FIM)
07 - Host Intrusion Prevention (HIPS)

Respond - Devices

12 - Endpoint detection and response (EDR)
14 - Endpoint Forensics
15 - Security orchestration, automation and response (SOAR) Device Plug

Recover - Devices

Identify - Network

21 – Netflow Manager
22 - Network Vulnerability Scanning
42 - Network Configuration Manager

Protect - Network

23 - Edge Antimalware (Gateway)/ Sandboxing
25 - Micro/host-app Segmentation
26 - Web Filtering (URL Gateway)
27 - Remote Access (VPN)
42 - Network Configuration Manager
28 - Firewalls / Switch ACLs
29 - Email Filtering (Antimalware Gateway)
30 - Network Intrusion Prevention (IPS)
31 - Reverse proxy load balancer
32 - Zero Trust Network Access (ZTNA) - NAC

Detect - Network

33 - Extended detection and response (xDR) – Network Plug
34 - SSL Decryption
35 - DDoD Detection
36 - Netflow Analytics
37 - Threat Intelligence Feeds
38 - Network Risk Monitor
39 - Network SIEM & Analytics
30 - Network Intrusion Prevention (IPS)

Respond - Network

33 - Extended detection and response (xDR) – Network Plug
40 - Net DDoD Response
41 - Network Forensics
15 - Security orchestration, automation and response (SOAR) Device Plug

Recover - Network

Identify - Application

51 - App vulnerability scanning and code analysis (SAST/DAST)
53 - Library Management
55 - Identity Management (IDM)

Protect - Application

56 - Web Application Firewall (WAF)
57 - ZT Access Proxy / Web Single Sign-On (SSO)
58 - Key Management (vault)
59 - Authorization Server (AM)
60 - API Security Gateway
61 - Cloud Access Security Broker (CASB)
62 - Runtime application self protection (RASP)
63 - Software Change Manager

Detect - Application

64 - Deception / Honeypots
65 - App SIEM & Analytics
67 - Src Code Compromise

Respond - Application

15 - Security orchestration, automation and response (SOAR) Plug

Recover - Application

Identify - Data

71 - Data discovery and Labeling

Protect - Data

72 - Database Access Manager
73 - Database Encrytion / Masking / Tokenization
74 - IDAM Governace
75 - Record Manager (Auditor)
76 - DLP Gateway (EDGE)
77 - Endpoint DLP
78 - Network Encryption
79 - Endpoint Encryption (EE)
80 -Data Right Management

Detect - Data

81 - Deep Web Analysis
82 - Database Audit Monitoring
83 - Database Activity Monitoring

Respond - Data

15 - Security orchestration, automation and response (SOAR) DB Plug
84 - Database Forensics

Recover - Data

86 - Data BackUp and Recovery

Identify - Application

91 - User Directory
92 - Multi-Factor Authentication (MFA)
93 - Phishing simulations and tests

Protect - User

94 - Authentication Server (IDP)
95 - Cybersecurity awareness training platform (CBT)

Detect - User

96 - Fraud Detection
97 - User Behavior Analytics (UBA)
98 - Insider Threat Detection

Respond - User

15 - Security orchestration, automation and response (SOAR) IM Plug

Recover - User

Function ISO Office - Identify

F01 - Asset Management
F02 - Vulnerability Management
F03 - Configuration Management
F04 - Security Governance
F05 - Risk Assessment / BIA - Mapa de aplicativos
F06 - Security Architecture
F07 - Threat Modeling
F08 - Data Management
F09 - 3th Party Risk Management
F10 - Security Posture Management (SSPM)

Function ISO Office - Protect

F11 - Audit Log Management
F22 - Identity and Access Management
F23 - Patch Management
F24 - Awareness and Training
F25 - Change Management
F26 - Data Privacy Management
F27 - Red Team / Penetration Testing

Function ISO Office - Detect

F41 - Blue Teaming
F42 - Continuing audit and Compliance
F43 - Threat Hunting
F44 - Breach and attack simulation (BAS)
F45 - Security Alert Management

Function ISO Office - Respond

F61 - Incident Response Management
F62 - Forensics services

Function ISO Office - Recover

F81 - Incident Recovery Management
F82 - Data Breach Response (service)
F83 - Disaster Recovery Plan

CSF – ID RA - Risk Assessment

CSF – ID BE Business Environment

CSF ID SC Supply Chain Risk Management

CSF – ID AM - Asset Management

CSF – ID GV - Governance

CSF – ID RM - Risk Management Strategy

CSF PR AT - Awareness and Training

CSF PR AC - Identity Management, Authentication and Access Control

CSF PR DS - Data Security

CSF PR IP - Information Protection Processes and Procedures

CSF PR MA - Maintenance

CSF PR PT - Protective Technology

CSF DE CM - Security Continuous Monitoring

CSF DE AE - Anomalies and Events

CSF DE DP - Detection Processes

CSF RS RP - Response Planning

CSF RS CO - Communications

CSF RS AN - Analysis

CSF RS IM - Improvements

CSF RS MI - Mitigation

CSF RC IM - Improvements

CSF RC RP - Recovery Planning

CSF RC CO - Communications

CIS – 01 Inventory and Control of Enterprise Assets

CIS – 02 Inventory and Control of Software Assets

CIS – 03 Data Protection

CIS – 04 Secure Configuration of Enterprise Assets and Software

CIS – 05 Account Management

CIS – 06 Access Control Management

CIS – 07 Continuous Vulnerability Management

CIS – 08 Audit Log Management

CIS – 09 Email and Web Browser Protections

CIS – 10 Malware Defenses

CIS – 11 Data Recovery

CIS – 12 Network Infrastructure Management

CIS – 13 Network Monitoring and Defense

CIS – 14 Security Awareness and Skills Training

CIS – 15 Service Provider Management

CIS – 16 Application Software Security

CIS – 17 Incident Response Management

CIS – 18 Penetration Testing

cecib
centro de estudios en ciberseguridad

ADECUARSE
IT COUNSELING
http://www.adecuarse.com/