INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN

Ciclo 2025 - 1
SI904V (ST215V) - Seguridad de Sistemas
Jesús Huapaya Ciriaco, MBA

Content

Title: "Historia de la Seguridad de la Información y Conceptos Clave"

Subtitle: "Ciberseguridad y el Rol de los Profesionales en el Desarrollo de Sistemas"

Sources:

History of Information Security - Wikipedia

Introduction to Information Security - NIST

What is Cybersecurity? - Cisco

YouTube Video: A Brief History of Cybersecurity and Hacking

Introduction to Information Security

Definition of Information Security (Confidentiality, Integrity, Availability - CIA Triad).

Importance of protecting data in the digital age.

Sources:

CIA Triad Explained - TechTarget

Information Systems Security Audit: An Ontological Framework

A Beginner's Guide to Cybersecurity: Start with the ABCs

YouTube Video: What Is Cyber Security | How It Works? | Cyber Security In 7 Minutes | Cyber Security | Simplilearn

History of Information Security

Early days: Physical security (locks, keys).

1970s: Birth of cybersecurity with ARPANET.

2000s: Rise of malware, hacking, and modern cybersecurity.

Sources

Listening to the echoes of cybersecurity history

Evolution of Cybersecurity - Kaspersky

A Brief History of Cybersecurity - Norton

YouTube Video: Evolution of cybersecurity (conventional to AI/ML based)

Key Concepts in Information Security

CIA Triad (Confidentiality, Integrity, Availability)

Non-repudiation, Authentication, Authorization.

Risk Management and Threat Modeling

Sources

CIA Triad - NIST

Essential Functions of a Cybersecurity Program

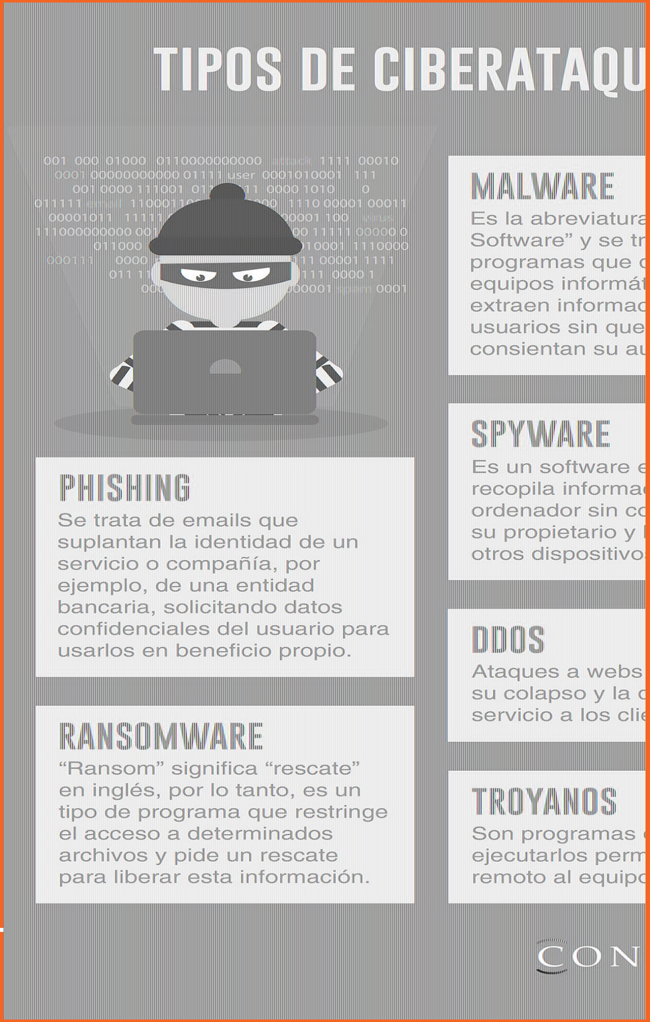
Threat Modeling - OWASP

YouTube Video: What is the CIA Triad

Threats to Information Security

Malware, Phishing, Ransomware.
Insider Threats, Social Engineering.
Advanced Persistent Threats (APTs).

Sources:
Types of Cyber Threats - CISA
McAfee Unveils 2025 Cybersecurity Predictions
What is Social Engineering? - Kaspersky
YouTube Video: Threats Vulnerabilities and Exploits - IBM



TIPOS DE CIBERATAQU

MALWARE
Es la abreviatura
Software" y se tr
programas que c
equipos informát
extraen informac
usuarios sin que
consientan su au

PHISHING
Se trata de emails que suplantan la identidad de un servicio o compañía, por ejemplo, de una entidad bancaria, solicitando datos confidenciales del usuario para usarlos en beneficio propio.

SPYWARE
Es un software e
recopila informac
ordenador sin co
su propietario y l
otros dispositivo

DDOS
Ataques a webs
su colapso y la c
servicio a los clie

RANSOMWARE
"Ransom" significa "rescate" en inglés, por lo tanto, es un tipo de programa que restringe el acceso a determinados archivos y pide un rescate para liberar esta información.

TROYANOS
Son programas c
ejecutarlos perm
remoto al equipo

Security in the System Development Lifecycle (SDLC)

Importance of integrating security into SDLC.

Secure coding practices.

Security testing (penetration testing, code reviews).

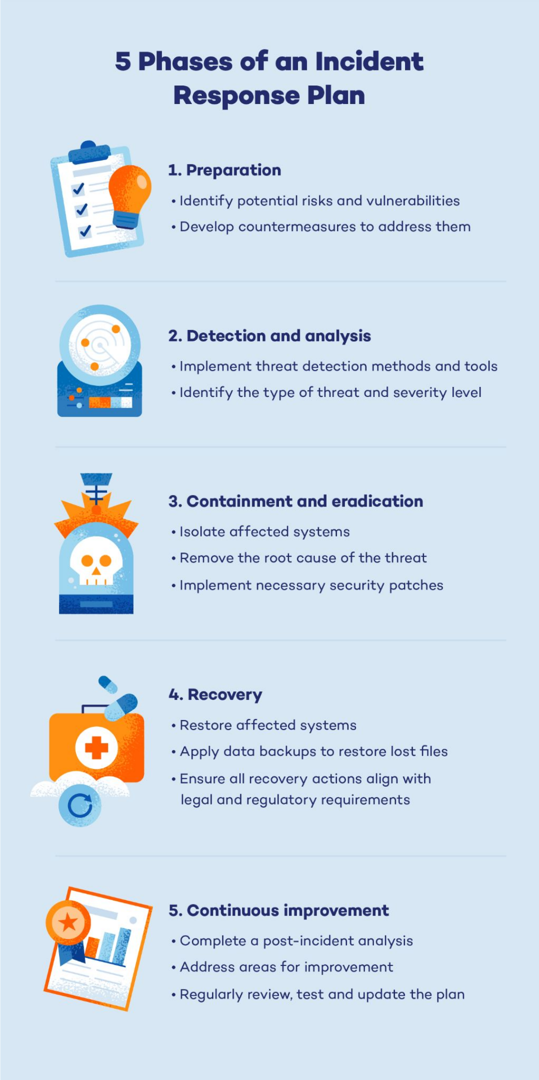
Sources:

OWASP Developer Guide

Engineering Trustworthy Secure Systems - NIST

Secure Coding Practices - CERT

YouTube Video: Secure Software Development Life Cycle | SSDLC



5 Phases of an Incident Response Plan

1. Preparation

- Identify potential risks and vulnerabilities
- Develop countermeasures to address them

2. Detection and analysis

- Implement threat detection methods and tools
- Identify the type of threat and severity level

3. Containment and eradication

- Isolate affected systems
- Remove the root cause of the threat
- Implement necessary security patches

4. Recovery

- Restore affected systems
- Apply data backups to restore lost files
- Ensure all recovery actions align with legal and regulatory requirements

5. Continuous improvement

- Complete a post-incident analysis
- Address areas for improvement
- Regularly review, test and update the plan

Role of Information Security Professionals

Responsibilities: Risk assessment, incident response, policy development.

Skills required: Technical knowledge, analytical thinking, communication.

Certifications: CISSP, CISM, CEH.

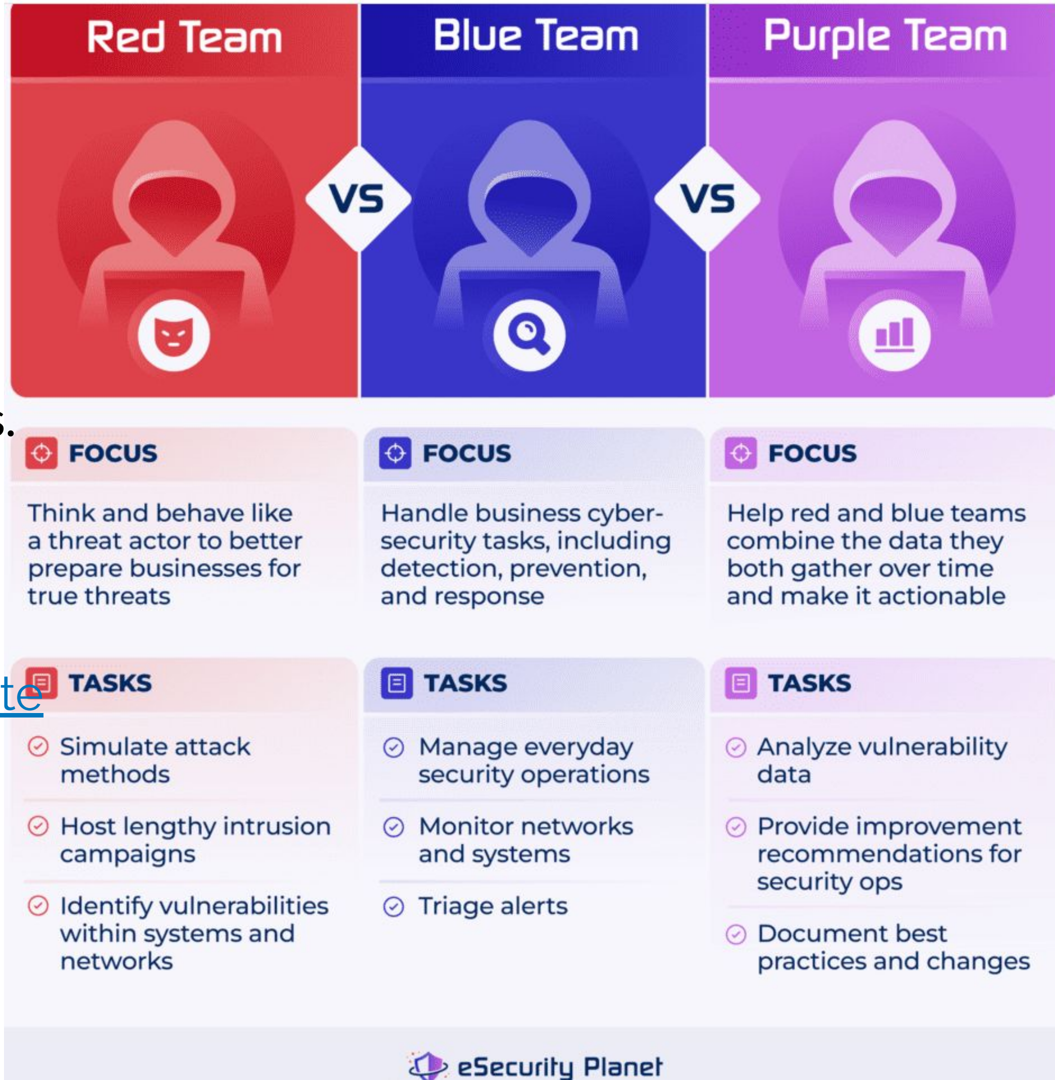
Sources:
The Real-World Impact of AI on Cybersecurity Professionals - ISC2
Cybersecurity Skills and Workforce Frameworks - NIST
Top Cybersecurity Certifications - CompTIA
YouTube Video: Day In The Life Of A Cyber Security Analyst

Introduction to Cybersecurity Teams

Overview of Red, Blue, and Purple Teams.

Roles and responsibilities of each team.

Sources:
[Red Team vs Blue Team - SANS Institute]
[What Is a Red Team in Cybersecurity?]
[Career Path, Skills, and Job Roles]
YouTube Video: [Red Teaming vs Blue Teaming in Cyber Security]



Red Team	Blue Team	Purple Team
FOCUS	**FOCUS**	**FOCUS**
Think and behave like a threat actor to better prepare businesses for true threats	Handle business cyber-security tasks, including detection, prevention, and response	Help red and blue teams combine the data they both gather over time and make it actionable
TASKS	**TASKS**	**TASKS**
✓ Simulate attack methods ✓ Host lengthy intrusion campaigns ✓ Identify vulnerabilities within systems and networks	✓ Manage everyday security operations ✓ Monitor networks and systems ✓ Triage alerts	✓ Analyze vulnerability data ✓ Provide improvement recommendations for security ops ✓ Document best practices and changes

Red Team

Role: Simulate attacks to test defenses.

Tools: Metasploit, Nmap, Cobalt Strike.

Real-world example: Penetration testing.

Sources

What is a Red Team? - Red Team Guide

Red Team Tools - Kali Linux

Penetration Testing - OWASP

YouTube Video: Introduction To Red Teaming - HackerSploit

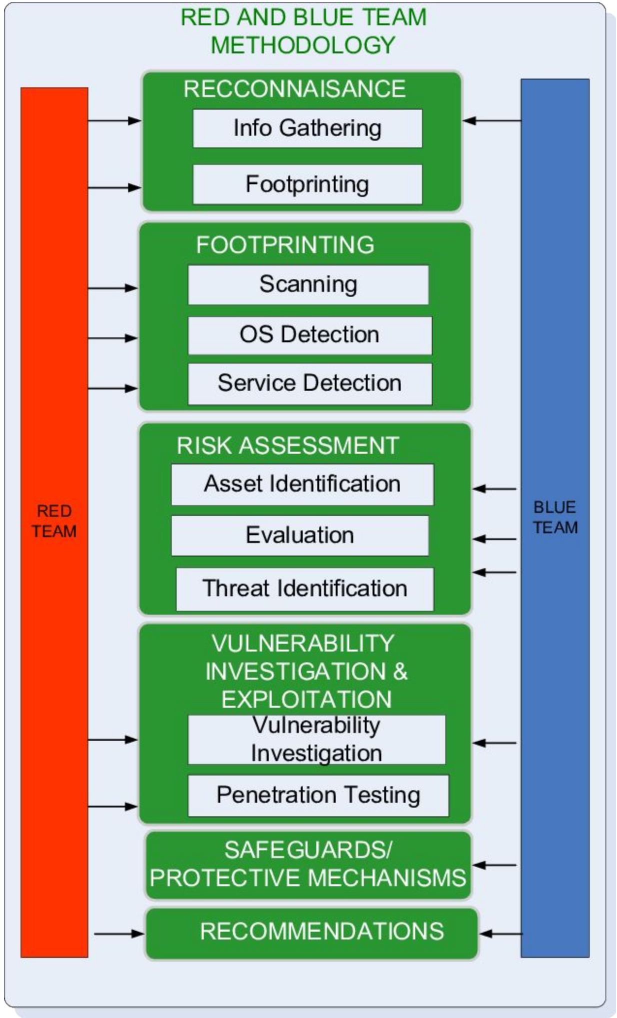
Blue Team

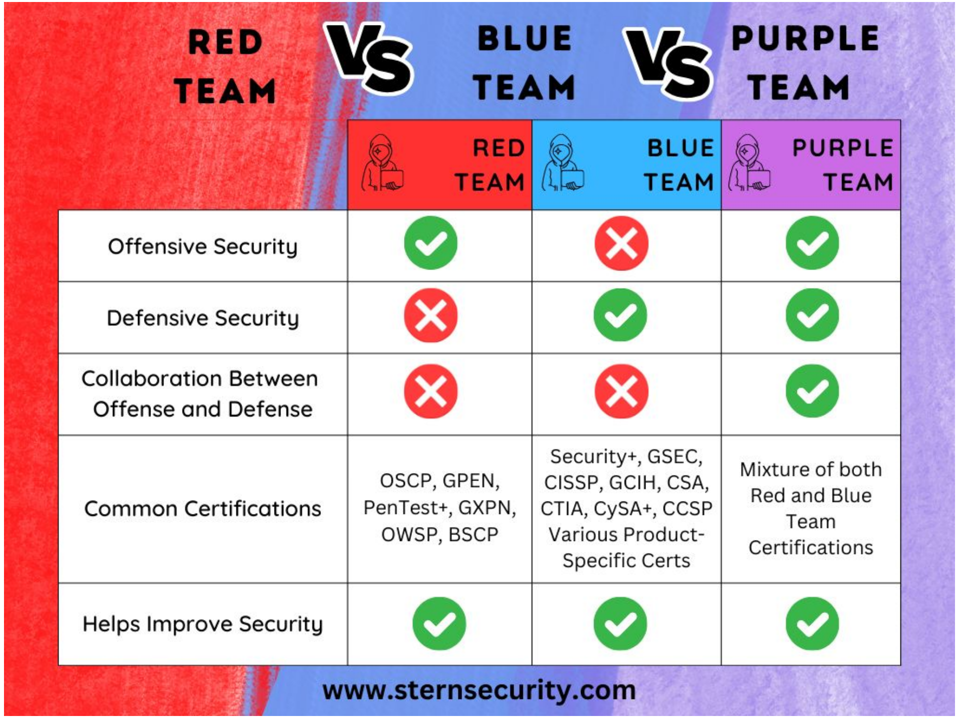
Role: Defend against attacks.

Tools: SIEM (Splunk, QRadar), IDS/IPS.

Real-world example: Incident response.

Sources:
Blue team's role in security
SIEM Tools - Gartner
Incident Response - NIST
YouTube Video: Introduction To Blue Team Operations - HackerSploit





RED TEAM Vs BLUE TEAM Vs PURPLE TEAM

	RED TEAM	BLUE TEAM	PURPLE TEAM
Offensive Security	✓	✗	✓
Defensive Security	✗	✓	✓
Collaboration Between Offense and Defense	✗	✗	✓
Common Certifications	OSCP, GPEN, PenTest+, GXPN, OWSP, BSCP	Security+, GSEC, CISSP, GCIH, CSA, CTIA, CySA+, CCSP Various Product-Specific Certs	Mixture of both Red and Blue Team Certifications
Helps Improve Security	✓	✓	✓

www.sternsecurity.com

Purple Team

Role: Collaboration between Red and Blue Teams.

Benefits: Improved security posture.

Real-world example: Continuous security improvement.

Sources:
What is a Purple Team? - CrowdStrike
What is Purple Teaming in Cybersecurity?
YouTube Video: Operationalized Purple Teaming - SANS Offensive Operations

Case 1: Equifax Data Breach (2017)

Overview: Hackers exploited a vulnerability in Apache Struts, exposing 147 million records.

Impact: Financial losses, reputational damage, and regulatory fines.

Lessons: Importance of patch management and vulnerability scanning.

Sources:

Equifax Breach Analysis - Krebs on Security

YouTube Video: FTC investigating Equifax breach - CBS News

Case 2: WannaCry Ransomware Attack (2017)

Overview: Ransomware exploited a Windows SMB vulnerability, affecting 200,000+ systems globally.

Impact: Disrupted healthcare systems (e.g., NHS) and caused billions in damages.

Lessons: Importance of regular updates and backups.

Sources:

WannaCry Analysis - Symantec

YouTube Video: Cyber Attack: Ransomware causing chaos globally - BBC News

Case 3: SolarWinds Supply Chain Attac
(2020)

Overview: Hackers compromised SolarWinds' Orion software, affecting 18,000+ organizations.

Impact: Espionage on US government agencies and private companies.

Lessons: Importance of securing the software supply chain.

Sources:

SolarWinds Attack - FireEye

YouTube Video: The SolarWinds Hack And The Future Of Cyber Espionage - CNBC

Case 4: Target Data Breach (2013)

Overview: Hackers stole 40 million credit card records via a third-party HVAC vendor.

Impact: $18.5 million settlement and reputational damage.

Lessons: Importance of third-party risk management.

Sources:

Target Breach Report - Krebs on Security

YouTube Video: The Today Show talks about the new report regarding the Target breach

Case 5: NotPetya Cyberattack (2017)

Overview: Malware disguised as ransomware caused widespread destruction, targeting Ukraine initially.

Impact: Global losses exceeding $10 billion, affecting companies like Maersk and Merck.

Lessons: Importance of network segmentation and incident response planning.

Sources:

NotPetya Analysis - Wired

YouTube Video: What lessons can we learn from devastating NotPetya cyberattack?

Case 6: Colonial Pipeline Ransomware Attack (2021)

Overview: DarkSide ransomware group attacked the largest fuel pipeline in the US.

Impact: Fuel shortages, $4.4 million ransom paid, and national security concerns.

Lessons: Importance of critical infrastructure protection and ransomware preparedness.

Sources:

Colonial Pipeline ransomware attack

YouTube Video: Why this security expert calls the Colonial Pipeline attack 'our worst nightmare'