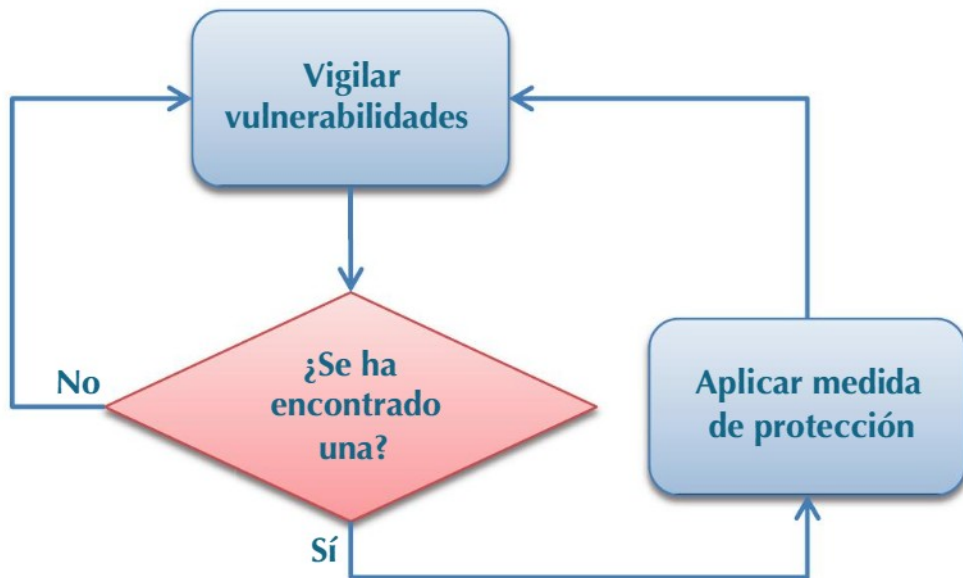




# Pautes i pràctiques de tractament segur de la informació Part III

# PROTECCIÓ

## Cicle de supervisió de vulnerabilitats



# PROTECCIÓ

**¿Qué deguem tenir en compte?**

- ➔ Analitzar les amenaces potencials
- ➔ Analitzar les pèrdues que podrien generar
- ➔ Probabilitat de que es produïska l'incident

[Video: Conceptes bàsics sobre SI](#)

# PROTECCIÓ

## Auditoria de seguretat de sistemes informàtics

Una auditoria de seguretat informàtica comprén **l'anàlisi i gestió dels sistemes per a identificar i posteriorment corregir** les diverses vulnerabilitats que puguen presentar-se en una revisió exhaustiva de les

Els resultats es detallen, s'arxiven i reporten als responsables els qui hauran d'establir mesures preventives i de reforç

Els objectius de l'auditoria: Els SI

- ➔ Revisar la seguretat dels entorns i sistemes
- ➔ Verificar el compliment de la normativa i legislació vigents
- ➔ Elaborar un informe independent

# PROTECCIÓ

## Tipus d'auditoria

- ➔ **Auditoria de seguretat interna:** es contrasta el nivell de seguretat de les xarxes locals i corporatives de caràcter intern.
- ➔ **Auditories de seguretat perimetral:** s'estudia el perímetre de la xarxa local o corporativa, connectat a xarxes públiques
- ➔ **Test d'intrusió:** s'intenta accedir als sistemes, per a comprovar el nivell de resistència a la intrusió no desitjada
- ➔ **Anàlisi forense:** anàlisi posterior d'incidents mitjançant el qual es tracta de reconstruir com s'ha penetrat en el sistema al mateix temps que es valoren els danys ocasionats
- ➔ **Auditoria de codi d'aplicacions:** comprovar vulnerabilitats com la injecció de codi SQL

# AUDITORIA

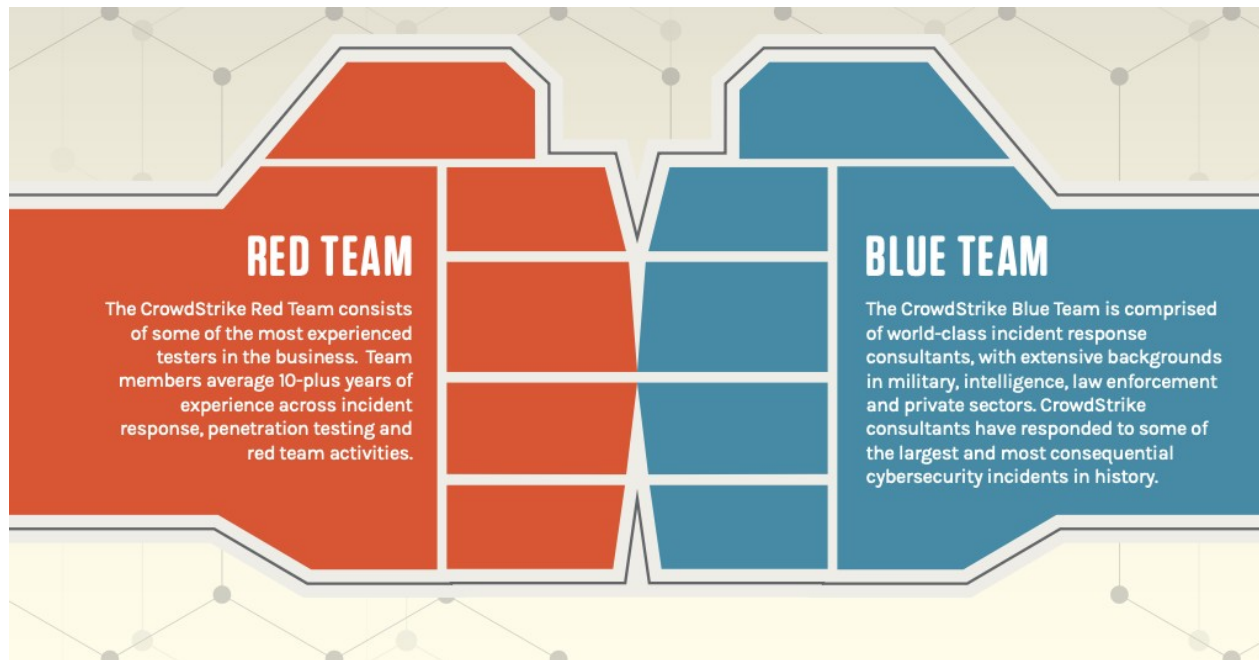
## Exemples pràctics

- Auditories wireless
- Auditoria d'accés a sistemes operatius
- Auditoria d'accés segur a dades i aplicacions segures.
- Auditoria de versions insegures d'aplicacions i sistema operatiu

# AUDITORIA

**RED TEAM**  
**BLUE TEAM**

**PURPLE TEAM**





# PLA INTEGRAL DE PROTECCIÓ PERIMETRAL



# QUÈ ÉS ?

La seguretat perimetral és el conjunt de mecanismes i sistemes relatius al control de l'accés físic de persones a les instal·lacions, així com la detecció i la prevenció d'intrusions

# OBJECTIUS

- Suportar els atacs externs.
- Detectar i identificar els atacs rebuts i alertar sobre ells.
- Segmentar i securitzar els sistemes i serveis en funció de la seua superfície d'atac.
- Filtrar i bloquejar el trànsit il·legítim.


# Plataformes de seguretat informàtica

- Tallafocs
- IDS / IPS
- Honeypots
- Sistemes anti Ddos
- Passarel·les antivirus i antispam
- VPN
- Control d'accés i identitat

# Elaboració d'un pla de seguretat

## Etales

- Revisió / auditoria de seguretat
- Revisió de la eficiència de la xarxa
- Redacció del pla
- Aprovació del pla ( gerència )
- Difusió del pla en la organització
- Posada en producció del pla
- Revisió periòdica / auditoria del pla



Mantindre's sempre informat  
i al dia és la primera i millor  
recomanació en matèria de  
seguretat informàtica

# Anàlisi Forense

Definicions: forense, informàtica forense

Funcions d'un informàtic forense

Fases d'una anàlisi forense

# Definició “forense”

## Origen

Préstec (s. XVII) del llatí forensis ‘de la plaça pública, del fòrum’, ‘forense, judicial’, derivat de fòrum ‘recinte sense edificar’, ‘plaça pública’, i d'ací ‘vida pública i judicial’, ‘tribunals de justícia’ per celebrar-se allí els judicis.

Ciències forenses, també conegudes com les branques de la criminalística...

Arte Forense  
 Antropología Forense  
 Balística Forense  
 Dactiloscopia  
 Documentoscopia  
 Entomología Forense  
 Fisionomía Forense  
 Fotografía Forense  
 Genética Forense

Hematología Forense  
 Incendios y explosivos  
**Informática Forense**  
 Medicina Forense  
 Meteorología Forense  
 Odontología Forense  
 Patología Forense  
 Peritaje caligráfico  
 Psicología Forense

Química Forense  
 Toxicología Forense

# DEFINICIONS

La informàtica forense és la ciència forense que s'encarrega d'assegurar, identificar, preservar, analitzar i presentar la prova digital, de manera que aquesta siga acceptada en un procés judicial.

Òptiques des de les quals abordar la informàtica forense

- ✓ Judicial
- ✓ Empresarial



# Etaques que formen l'anàlisi forense

## Enfocament criminalístic

- Assegurar l'escena
- Identificar proves
- Adquirir dades
- Preservar (Cadena de custòdia)
- Analitzar dades
- Documentar resultats
- Presentar resultats (Informe pericial)

# Etapes que formen l'anàlisi forense

## Enfocament criminalístic



# Etapes que formen l'anàlisi forense

Enfocament criminalístic : **Informe pericial**

Les normes processals estableixen que els informes pericials els realitzaran els professionals que disposen del títol oficial corresponent a la matèria d'estudi.

En el nostre cas : Un **perit informàtic**.

Perquè el peritatge tinga validesa judicial, el professional ha d'actuar respectant les normes d'Enjudiciament Civil i Criminal i respectant una sèrie de principis:

- Està obligat a dir la veritat i sempre sobre la base de la seua formació tècnica.
- Ha d'actuar amb independència, és a dir, no esbiaixar el seu dictamen en funció de la part que el contracta.
- Ha de col·laborar amb el jutge o tribunal perquè és un auxiliar de la Justícia.

# Etapas que formen l'anàlisi forense

## Perit informàtic.

Requisits d'accés al curs

<https://www.unir.net/ingenieria/curso-perito-judicial-informatico/>

Per a exercir com a perit informàtic judicial, es pot consultar l'article 340 de la Lley 1/2000, de 7 de gener, de Enjudiciament Civil.

<https://www.boe.es/buscar/act.php?id=BOE-A-2000-323>

### Inicio

11 nov 2024

[VER CALENDARIO](#)

### Duración

4 meses

### Créditos

18 ECTS

### Metodología

A distancia, 100% online

### Bonificación

Curso bonificable para trabajadores en activo a través del programa de bonificación de su empresa

### Rama de Conocimiento

Escuela Superior de Ingeniería y Tecnología (ESIT)

# Etaques que formen l'anàlisi forense

## Enfocament empresarial

- Preparació i prevenció
- Detecció i anàlisi
- Contenció
- Recuperació
- Activitats post-incident



# Etaques que formen l'anàlisi forense

## Enfocament empresarial

L'informe pericial serveix, per tant, com a mitjà de prova en un procediment judicial, però també és de gran utilitat en **causes extrajudicials** que requerisquen un peritatge, és a dir, l'opinió experta sobre un tema i la seua comprovació mitjançant tècniques especialitzades.

# Detall de les etapes

## Preparació i prevenció

- Copia de seguretat
- Control (Monitorització)
- Plan de seguretat, SGSI
- CSIRT

## Detecció i anàlisis

- Identificació
- Classificació
- Priorització
- Notificació

## Contenció

- Minimització
- Protecció de proves
- Notificació

## Recuperació

- Recuperar sistemes
- Compilar i organitzar la informació
- Valorar danys i costos
- Revisar directives

# Ferramentes

Fase de prevenció:

- Cobian Backup
- Veeam (entornos virtualizados)
- Snort
- Suricata
- Nagios
- PRTG
- Zenoss

Fase de adquisició:

- CAINE
- Kali
- Deft\* Deft Zero
- FTK Imager
- EnCase Forensic Imager
- LiME

Fase de anàlisis.

- The Sleuth Kit y Autopsy
- Volatility
- OSForensics
- X-Ways
- Encase
- Forensics Took Kit
- Magnet AXIOM



# Auditories

Una auditoria, des d'un punt de vista molt general, és un procés executat per un auditor, que té la característica de ser sistemàtica, independent i documentada, i que busca obtenir a partir de la realització de proves d'auditoria registres, declaracions de fets o una altra informació coneguda com a proves d'auditoria.

Les proves d'auditoria han de ser verificables, pertinents i avaluables de manera objectiva amb la finalitat de determinar, d'acord amb aquestes, la mesura en què el fet auditat compleix uns criteris d'auditoria.

Finalment, el procés conclou amb l'anàlisi d'aquestes troballes per a poder emetre unes conclusions de l'auditoria.

# Auditories

Principis d'auditoria.

- Integritat / Conducta ètica
- Presentació justa i imparcial
- Atenció professional adequada
- Independent
- Enfocament basat en la prova
- Confidencialitat

Tipus d'auditories

- ✓ Auditories internes o de primera part
- ✓ Auditories de segona part
- ✓ Auditories de tercera part