Itinerari en Ciberseguretat a la IT Academy

Un programa de:

Ajuntament de Barcelona

Barcelona Activa

Amb la col·laboració de:

Cisco Networking Academy

El sector de la ciberseguretat

La ciberseguretat és el **conjunt d'estratègies, tecnologies i pràctiques** que tenen com a objectiu **protegir sistemes digitals, xarxes, dispositius i dades** davant accessos no autoritzats, atacs o danys. La seva importància ha crescut amb la digitalització global, ja que cada vegada més àmbits —empreses, administracions, salut, educació o ciutadania— depenen de la seguretat dels sistemes digitals. La ciberseguretat implica:

- Protecció tècnica
- Gestió dels riscos
- Formació de les persones usuàries i la
- Coordinació entre institucions

A Catalunya, **l'Agència de Ciberseguretat de Catalunya** és l'organisme públic que lidera la protecció i la resposta davant incidents dins del territori. A nivell estatal, aquesta tasca recau principalment en l'**INCIBE** (Institut Nacional de Ciberseguretat), centrat en la protecció de la ciutadania i les empreses i el **CCN-CERT** (Centre Criptològic Nacional), que vetlla per la seguretat de les administracions públiques. En l'àmbit europeu, la Unió Europea treballa de manera coordinada a través de l'**ENISA** (Agència Europea per a la Ciberseguretat) i la **Xarxa Europea de SOCs i CERTs**, que permet compartir informació sobre amenaces i reforçar la resposta comuna davant ciberatacs.

El sector de la ciberseguretat

Els SOC (Security Operations Center)

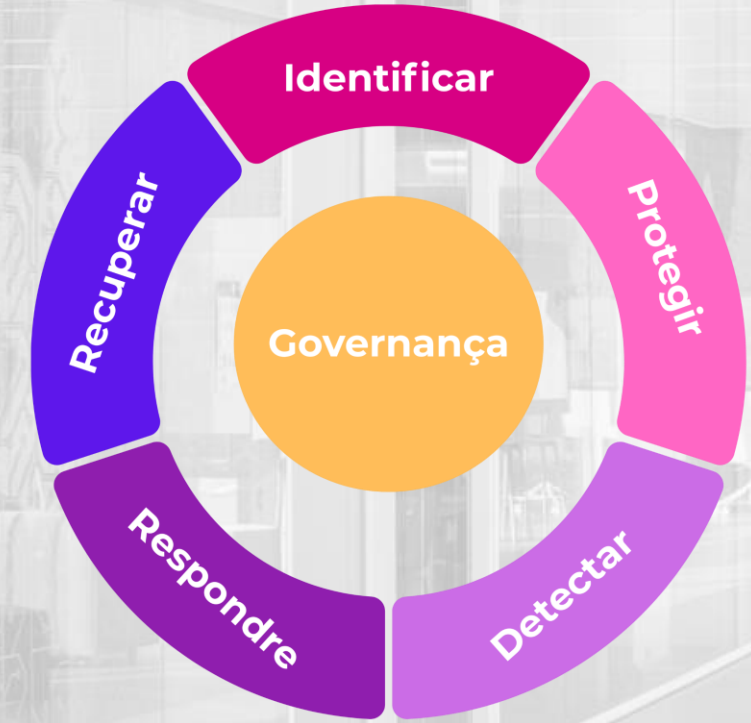
Un SOC és el Centre d'Operacions de Seguretat, l'espai des d'on un equip de professionals de la ciberseguretat **vigila**, **detecta** i **respon** a possibles ciberatacs o incidents que afecten una organització. La seva missió és **garantir que els sistemes, les xarxes i les dades es mantinguin segures les 24 hores del dia**.

Els SOC estan formats per equips que treballen en diferents nivells (*tiers*) segons la seva experiència i responsabilitats:

- **Nivell 1:** analistes júnior que fan la **monitorització** constant i identifiquen alertes sospitoses.
- **Nivell 2:** professionals més experimentats que **investiguen i responen** als incidents detectats.
- **Nivell 3:** experts que **realitzen anàlisis forenses**, determinen l'origen dels atacs i proposen millores estratègiques de seguretat.

A més dels SOC interns de cada empresa o organització, existeix la **xarxa nacional i europea de SOCs** que treballen coordinats per compartir informació sobre amenaces i prevenir atacs a gran escala. A l'Estat espanyol, aquesta tasca la lidera l'**INCIBE** (Institut Nacional de Ciberseguretat), en col·laboració amb el CCN-CERT.

Fases de la Ciberseguretat



- **Governança:** Gestió i comunicació (establiment de l'estratègia de gestió de riscos, expectatives i polítiques de gestió, comunicació i seguiment)
- **Identificar:** Entendre el context. Conèixer els actius i els riscos.
- **Protegir:** Aplicació de controls per mitigar riscos.
- **Detectar:** Control i monitorització.
- **Respondre:** Reduir l'impacte d'un incident potencial.
- **Recuperar:** Resiliència i recuperació davant d'incidents.

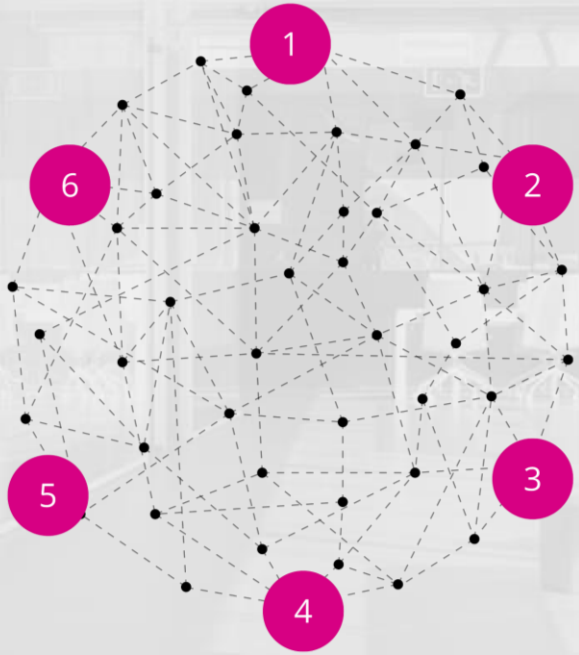
Font de la imatge: https://www.nist.gov

Rols laborals en Ciberseguretat

6. Gestió i estratègia
- CISO (Director/a de seguretat en la informació)
- DPO (Delegat de protecció de dades)

5. Auditoria i compliment
- Auditor/a de ciberseguretat
- **Hacker Ètic**
- Consultor de riscos
- Normativa

4. Resposta i recuperació
- Especialista en resposta d'incidents
- Pèrit forense digital



1. Anàlisi i monitorització
- **Analista de Ciberseguretat**
- **Analista SOC (Nivell 1-3)**
- Especialista en Intel·ligència d'amenaces

2. Enginyeria i Arquitectura
- Enginyer/a de Ciberseguretat
- Enginyer/a de Xarxes Segures
- Especialista en Seguretat al núvol

3. Desenvolupament segur
- Especialista DevSecOps
- Arquitecta d'aplicacions segures

Per a més informació sobre els perfils laborals, pots consultar l'última publicació d'ENISA en aquest enllaç.

Proposta d'itinerari Analista Junior en Ciberseguretat

FASE 1 – 176h

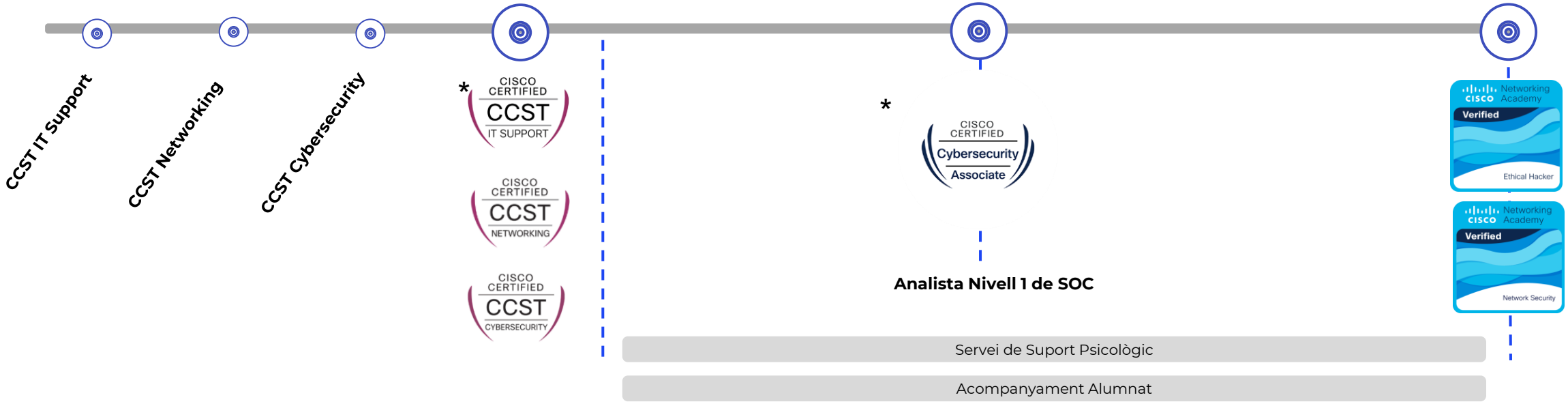
Fonaments Analista Júnior en Ciberseguretat

FASE 2.1 – Cybersecurity Associate – 70h

Especialització d'Analista Júnior en Ciberseguretat

FASE 2.2 – Ethical Hacker – 140h

Especialització d'Analista Júnior en Ciberseguretat



* Les certificacions son voluntàries i el primer intent no té cost per l'alumnat que cursi la formació

Fonaments: Analista Júnior Ciberseguretat

CCST SUPORT

Conèixer les bases del suport tècnic a usuaris. S'inclou la instal·lació i manteniment de sistemes operatius, configuració de hardware i software, resolució d'incidències i atenció al client.

CCST NETWORKING

Introducció als fonaments de les xarxes informàtiques. Es veuen temes com model OSI, protocols TCP/IP, DNS, DHCP, ARP, ICMP, IPv4, IPv6, connectivitat i eines de diagnòstic.

CCST CYBERSECURITY

Introduir els principis essencials de la seguretat informàtica. S'aprèn sobre ciberatacs comuns, gestió de vulnerabilitats, polítiques de protecció de dades, defensa perimetral i pràctiques segures.

Especialització: Cibersecurity Associate, Networking Security i Hacker Ètic

CYBERSECURITY ASSOCIATE

Prepara't per a treballar en centres d'operacions en seguretat (SOC), enfrontant amenaces reals i gestionant incidents de ciberseguretat, on la monitorització té un paper important.

NETWORK SECURITY

Portar els coneixements sobre xarxes i la seguretat al següent nivell. Aprendre a assegurar xarxes, detectar intrusions i respondre a incidents. S'aprofundeix en tots els conceptes, acompanyant-ho de pràctiques que ajuden a consolidar els conceptes.

HACKER ÈTIC

Introducció a la seguretat ofensiva, aprenent a pensar con un hacker ètic per identificar i mitigar vulnerabilitats abans de que siguin explotades.

Sortides laborals amb l'itinerari de l'IT Academy

SORTIDES PROFESSIONALS AMB ELS FONAMENTS

- Help Desk junior
- Tècnic de suport IT
- Tècnic de suport/manteniment informàtic
- Resolució de problemes LAN/WAN
- Tècnic de comunicacions
- Administrador de xarxes junior
- Tècnic junior en ciberseguretat
- Analista júnior en ciberseguretat
- Assistent en gestió de riscos i resposta a incidents
- Operador d'alertes de seguretat

SORTIDES PROFESSIONALS AMB L'ESPECIALITZACIÓ

- Especialista en resposta a incidents
- Monitor de seguretat (SOC)
- Tècnic en anàlisis de tràfic de xarxes
- Assistent en gestió de vulnerabilitats
- Administrador de seguretat a les xarxes (Network Hardening)
- Blue Team Analyst junior
- Pentester junior
- SOC Analyst
- Gestor de vulnerabilitats júnior
- Ethical Hacker
- Red Team Analyst junior
- Consultor de seguretat ofensiva

FAQ's

Per on començo si soc junior?

- Aprèn fonaments de xarxes i sistemes operatius (Linux i Windows).
- Familiaritza't amb conceptes bàsics de seguretat: amenaces, vulnerabilitats, xifratge.
- Explora recursos gratuïts com **TryHackMe**, **Hack The Box** (HTB) i **OWASP** (Open Web Application Security Project).

He de saber programar?

No sempre. Tot i així, recomanem:

- **Python**, perquè permet automatitzar tasques, analitzar registres, fer escanejos de xarxa o desenvolupar eines de seguretat.
- **Bash** (Linux) i **PowerShell** (Windows) per entendre com funcionen els sistemes operatius i com automatitzar tasques d'administració i seguretat.

Necessito un títol universitari relacionat?

No és obligatori. Moltes empreses, com SIRT, valoren més les habilitats pràctiques i les certificacions.

IT ACADEMY

Gràcies!