Curs d'especialització en Ciberseguretat en entorns de les tecnologies de la informació

1. Relació de mòduls professionals i unitats formatives

Mòdul Professional 1: Incidents de ciberseguretat
Durada: 99
Equivalència en crèdits ECTS: 9
Unitats formatives que el componen:
UF 1: Incidents de ciberseguretat. 99 hores

Mòdul Professional 2: Enfortiment de xarxes i sistemes
Durada: 132
Equivalència en crèdits ECTS: 10
Unitats formatives que el componen:
UF 1: Enfortiment de xarxes i sistemes. 132 hores

Mòdul Professional 3: Posada en producció segura
Durada: 99
Equivalència en crèdits ECTS: 7
Unitats formatives que el componen:
UF 1: Posada en producció segura. 99 hores

Mòdul Professional 4: Anàlisi forense informàtic
Durada: 99
Equivalència en crèdits ECTS: 7
Unitats formatives que el componen:
UF 1: Anàlisi forense informàtic. 99 hores

Mòdul Professional 5: Hacking ètic
Durada: 99
Equivalència en crèdits ECTS: 7
Unitats formatives que el componen:
UF 1: Hacking ètic. 99 hores

Mòdul Professional 6: Normativa de ciberseguretat
Durada: 66
Equivalència en crèdits ECTS: 3
Unitats formatives que el componen:
UF 1: Normativa de ciberseguretat. 66 hores

Mòdul Professional 7: Formació en centres de treball
Durada: 126

Unitats formatives que el componen:
UF 1: Formació en centres de treball. 126 hores

2. Descripció dels mòduls professionals i de les unitats formatives

Mòdul Professional 1: Incidents de ciberseguretat

Durada: 99
Equivalència en crèdits ECTS: 9
Unitats formatives que el componen:
UF 1: Incidents de ciberseguretat. 99 hores

UF1: Incidents de ciberseguretat
Durada: 99 hores
Resultats d'aprenentatge i criteris d'avaluació

1. Desenvolupa plans de prevenció i conscienciació en ciberseguretat, establint normes i mesures de protecció.

Criteris d'avaluació

- 1.1. Defineix els principis generals de l'organització en matèria de ciberseguretat, que han de ser coneguts i recolzats per la direcció de la mateixa.
- 1.2. Estableix una normativa de protecció de el lloc de treball.
- 1.3. Defineix un pla de conscienciació de ciberseguretat dirigit als empleats.
- 1.4. Desenvolupa el material necessari per dur a terme les accions de conscienciació dirigides als empleats.
- 1.5. Realitza una auditoria per verificar el compliment de el pla de prevenció i conscienciació de l'organització.

2. Analitza incidents de ciberseguretat utilitzant eines, mecanismes de detecció i alertes de seguretat.

Criteris d'avaluació

- 2.1. Classifica i definit la taxonomia d'incidents de ciberseguretat que poden afectar a l'organització.
- 2.2. Estableix controls, eines i mecanismes de monitoratge, identificació, detecció i alerta d'incidents.
- 2.3. Estableix controls i mecanismes de detecció i identificació d'incidents de seguretat física.
- 2.4. Estableix controls, eines i mecanismes de monitoratge, identificació, detecció i alerta d'incidents a través de la recerca en fonts obertes (OSINT: Open Source Intelligence).
- 2.5. Realitza una classificació, valoració, documentació i seguiment dels incidents detectats dins de l'organització.
- 2.6. Investiga incidents de ciberseguretat analitzant els riscos implicats i definint les possibles mesures a adoptar.

3. Recopila i emmagatzema de forma segura evidències d'incidents de ciberseguretat que afecten l'organització.

Criteris d'avaluació

3.1. Realitza una anàlisi d'evidències.
3.2. Realitza la investigació d'incidents de ciberseguretat.
3.3. Intercanvia informació d'incidents, amb proveïdors i / o organismes competents que podrien fer aportacions al respecte.
3.4. Inicia les primeres mesures de contenció dels incidents per limitar els possibles danys causats.
3.5. Implementa mesures de ciberseguretat en xarxes i sistemes responent als incidents detectats i aplicant les tècniques de protecció adequades.

4. Desenvolupa procediments d'actuació detallats per donar resposta, mitigar, eliminar o contenir els tipus d'incidents de ciberseguretat més habituals.

Criteris d'avaluació

4.1. Prepara respostes ciberresilients davant incidents que permetin seguir prestant els serveis de l'organització i enfortint les capacitats d'identificació, detecció, prevenció, contenció, recuperació i cooperació amb tercers.
4.2. Estableix un flux de presa de decisions i escalat d'incidents intern i / o extern adequats.
4.3. Duu a terme les tasques de restabliment dels serveis afectats per un incident fins a confirmar la volta a la normalitat.
4.4. Documenta les accions realitzades i les conclusions que permetin mantenir un registre de "lliçons apreses".
4.5. Realitza un seguiment adequat de l'incident per evitar que una situació similar es torni a repetir.
4.6. Detecta i documenta incidents de ciberseguretat seguint procediments d'actuació establerts.

5. Desenvolupa un procediment d'actuació detallat per a la notificació d'incidents de ciberseguretat en els temps adequats.

Criteris d'avaluació:

5.1. Notifica l'incident de manera adequada al personal intern de l'organització responsable de la presa de decisions.
5.2. Notifica l'incident de manera adequada a les autoritats competents en l'àmbit de la gestió d'incidents de ciberseguretat en cas de ser necessari.
5.3. Notifica formalment l'incident als afectats, personal intern, clients, proveïdors, etc., en cas de ser necessari.
5.4. Notifica l'incident als mitjans de comunicació en cas de ser necessari.

Continguts:

1. Desenvolupament de plans de prevenció i conscienciació en ciberseguretat:
   1.1. Principis generals en matèria de ciberseguretat.
   1.2. Normativa de protecció de el lloc de la feina.
   1.3. Pla de formació i conscienciació en matèria de ciberseguretat.
   1.4. Materials de formació i conscienciació.
   1.5. Auditories internes de compliment en matèria de prevenció.
2. Auditoria d'incidents de ciberseguretat:
   2.1. Taxonomia d'incidents de ciberseguretat.

2.2. Controls, eines i mecanismes de monitorització, identificació, detecció i alerta d'incidents: tipus i fonts.
2.3. Controls, eines i mecanismes de detecció i identificació d'incidents de seguretat física.
2.4. Controls, eines i mecanismes de monitorització, identificació, detecció i alerta d'incidents a través de la recerca en fonts obertes (OSINT).
2.5. Classificació, valoració, documentació, seguiment inicial d'incidents de ciberseguretat.

3. Investigació dels incidents de ciberseguretat:
   3.1. Recull d'evidències.
   3.2. Anàlisi d'evidències.
   3.3. Investigació de l'incident.
   3.4. Intercanvi d'informació de l'incident amb proveïdors o organismes competents.
   3.5. Mesures de contenció d'incidents.
4. Implementació de mesures de ciberseguretat:
   4.1. Desenvolupar procediments d'actuació detallats per donar resposta, mitigar, eliminar o contenir els tipus d'incidents.
   4.2. Implantar capacitats de ciberresiliencia.
   4.3. Establir fluxos de presa de decisions i escalat intern i / o extern adequats.
   4.4. Tasques per restablir els serveis afectats per incidents.
   4.5. Documentació.
   4.6. Seguiment d'incidents per evitar una situació similar.
5. Detecció i documentació d'incidents de ciberseguretat:
   5.1. Desenvolupar procediments d'actuació per a la notificació d'incidents.
   5.2. Notificació interna d'incidents.
   5.3. Notificació d'incidents a qui correspongui.

Mòdul Professional 2: Enfortiment de xarxes i sistemes
Durada: 132
Equivalència en crèdits ECTS: 10
Unitats formatives que el componen:
UF 1: Enfortiment de xarxes i sistemes. 132 hores

UF1: Enfortiment de xarxes i sistemes
Durada: 132 hores
Resultats d'aprenentatge i criteris d'avaluació

1. Dissenya plans de securització incorporant bones pràctiques per al enduriment de sistemes i xarxes.

Criteris d'avaluació

1.1. Identifica els actius, les amenaces i vulnerabilitats de l'organització.
1.2. Avalua les mesures de seguretat actuals.

1.3. Elabora una anàlisi de risc de la situació actual a ciberseguretat de l'organització.
1.4. Prioritza les mesures tècniques de seguretat a implantar en l'organització tenint també en compte els principis de l'Economia Circular.
1.5. Dissenya i elabora un pla de mesures tècniques de seguretat a implantar en l'organització, apropiades per a garantir un nivell de seguretat adequat en funció dels riscos de l'organització.
1.6. Identifica les millors pràctiques en base a estàndards, guies i polítiques de securització adequades per a l'enfortiment dels sistemes i xarxes de l'organització.

2. Configura sistemes de control d'accés i autenticació de persones preservant la confidencialitat i privacitat de les dades.

Criteris d'avaluació.

2.1. Defineix els mecanismes d'autenticació basant-se diferents / múltiples factors (físics, inherents i basats en el coneixement), existents.
2.2. Defineix protocols i polítiques d'autenticació basats en contrasenyes i frases de pas, en base a les principals vulnerabilitats i tipus d'atacs.
2.3. Defineix protocols i polítiques d'autenticació basats en certificats digitals i targetes intel·ligents, en base a les principals vulnerabilitats i tipus d'atacs.
2.4. Defineix protocols i polítiques d'autenticació basats en tokens, OTPs, etc., en base a les principals vulnerabilitats i tipus d'atacs.
2.5. Defineix protocols i polítiques d'autenticació basats en característiques biomètriques, segons les principals vulnerabilitats i tipus d'atacs.

3. Administra credencials d'accés a sistemes informàtics aplicant els requisits de funcionament i seguretat establerts.

Criteris d'avaluació.

3.1. Identifica els tipus de credencials més utilitzats.
3.2. Genera i utilitza diferents certificats digitals com a mitjà d'accés a un servidor remot.
3.3. Comprova la validesa i l'autenticitat d'un certificat digital d'un servei web.
3.4. Compara certificats digitals vàlids i invàlids per diferents motius.
3.5. Instal·la i configura un servidor segur per a l'administració de credencials (tipus RADIUS - Remote Access Dial In User Service).

4. Dissenya xarxes de computadors contemplant els requisits de seguretat.

Criteris d'avaluació.

4.1. Incrementa el nivell de seguretat d'una xarxa local plana segmentant-la físicament i utilitzant tècniques i dispositius d'encaminament.
4.2. Optimitza una xarxa local plana utilitzant tècniques de segmentació lògica (VLANs).

4.3. Adapta un segment d'una xarxa local ja operatiu utilitzant tècniques de subnetting per incrementar la seva segmentació respectant els encaminaments existents.
4.4. Configura les mesures de seguretat adequades en els dispositius que donen accés a una xarxa sense fils (encaminadors, punts d'accés, etc.).
4.5. Estableix un túnel segur de comunicacions entre dues seus geogràficament separades.

5. Configura dispositius i sistemes informàtics complint els requisits de seguretat.

Criteris d'avaluació.

5.1. Configura dispositius de seguretat perimetral d'acord a una sèrie de requisits de seguretat.
5.2. Detecta errors de configuració de dispositius de xarxa mitjançant l'anàlisi de tràfic.
5.3. Identifica comportaments no desitjats en una xarxa a través de l'anàlisi dels registres (Logs), d'un tallafoc.
5.4. Implementa contramesures enfront de comportaments no desitjats en una xarxa.
5.5. Caracteritza, instal·la i configura diferents eines de monitorització.

6. Configura dispositius per a la instal·lació de sistemes informàtics minimitzant les probabilitats d'exposició a atacs.

Criteris d'avaluació.

6.1. Configura la BIOS per incrementar la seguretat del dispositiu i la seva contingut minimitzant les probabilitats d'exposició a atacs.
6.2. Prepara un sistema informàtic per a la seva primera instal·lació tenint en compte les mesures de seguretat necessàries
6.3. Configura un sistema informàtic perquè un actor maliciós no pugui alterar la seqüència d'arrencada amb fins d'accés il·legítim.
6.4. Instal·la un sistema informàtic utilitzant les seves capacitats de xifrat del sistema de fitxers per evitar l'extracció física de dades.
6.5. Particiona el sistema de fitxers de sistema informàtic per minimitzar riscos de seguretat.

7. Configura sistemes informàtics minimitzant les probabilitats d'exposició a atacs.

Criteris d'avaluació.

7.1. Enumera i elimina els programes, serveis i protocols innecessaris que hagin estat instal·lats per defecte en el sistema.
7.2. Configura les característiques pròpies de sistema informàtic per impossibilitar l'accés il·legítim mitjançant tècniques d'explotació de processos.
7.3. Incrementa la seguretat de sistema d'administració remot SSH i altres.
7.4. Instal·la i configura un Sistema de detecció d'intrusos en un Host (HIDS) en el sistema informàtic.
7.5. Instal·la i configura sistemes de còpies de seguretat.

Continguts

1. Disseny de plans de securització:

1.1. Anàlisi de riscos.
1.2. Principis de l'Economia Circular en la Indústria 4.0.
1.3. Pla de mesures tècniques de seguretat.
1.4. Polítiques de securització més habituals.
1.5. Guies de bones pràctiques per a la securització de sistemes i xarxes.
1.6. Estàndards de securització de sistemes i xarxes.
1.7. Caracterització de procediments, instruccions i recomanacions.
1.8. Nivells, escalats i protocols d'atenció a incidències.

2. Configuració de sistemes de control d'accés i autenticació de persones:
   2.1. Mecanismes d'autenticació. Tipus de factors.
   2.2. Autenticació basada en diferents tècniques.
3. Administració de credencials d'accés a sistemes informàtics:
   3.1. Gestió de credencials.
   3.2. Infraestructures de Clau Pública (PKI).
   3.3. Accés per mitjà de Signatura electrònica.
   3.4. Gestió d'accessos. Sistemes NAC (Network Access Control, Sistemes de Gestió d'Accés a la Xarxa).
   3.5. Gestió de comptes privilegiades.
   3.6. Protocols RADIUS i TACACS, servei Kerberos, entre d'altres.
4. Disseny de xarxes de computadors segures:
   4.1. Segmentació de xarxes.
   4.2. Subnetting.
   4.3. Xarxes virtuals (VLANs).
   4.4. Zona desmilitaritzada (DMZ).
   4.5. Seguretat en xarxes sense fils (WPA2, WPA3, etc.).
   4.6. Protocols de xarxa segura (IPSec, etc.).
5. Configuració de dispositius i sistemes informàtics:
   5.1. Seguretat perimetral. Tallafocs de Propera Generació.
   5.2. Seguretat de portals i aplicatius web. Solucions WAF (Web Aplication Firewall).
   5.3. Seguretat de el lloc de treball i endpoint fix i mòbil. AntiAPT, antimalware.
   5.4. Seguretat d'entorns cloud. Solucions CASB.
   5.5. Seguretat del correu electrònic.
   5.6. Solucions DLP (Data Loss Prevention).
   5.7. Eines d'emmagatzematge de logs.
   5.8. Protecció davant atacs de denegació de servei distribuït (DDoS).
   5.9. Configuració segura de tallafocs, encaminadors i proxies.
   5.10. Xarxes privades virtuals (VPNs), i túnels (protocol IPSec).
   5.11. Monitorització de sistemes i dispositius.
   5.12. Eines de monitorització (IDS, IPS).
   5.13. SIEMs (Gestors d'Esdeveniments i Informació de Seguretat).

5.14. Solucions de Centres d'Operació de Xarxa, i Centres de Seguretat de Xarxa: NOCs i socs.

6. Configuració de dispositius per a la instal·lació de sistemes informàtics:
   6.1. Precaucions prèvies a la instal·lació d'un sistema informàtic: aïllament, configuració del control d'accés a la BIOS, bloqueig de l'ordre d'arrencada dels dispositius, entre d'altres.
   6.2. Seguretat en l'arrencada de sistema informàtic, configuració de l'arrencada segur.
   6.3. Seguretat dels sistemes de fitxers, xifrat, partició, entre d'altres.
7. Configuració dels sistemes informàtics:
   7.1. Reducció del nombre de serveis, Telnet, RSSH, TFTP, entre d'altres.
   7.2. Hardening de processos (eliminació d'informació de depuració en cas d'errors, aleatorització de la memòria virtual per evitar gestes, etc.).
   7.3. Eliminació de protocols de xarxa innecessaris (ICMP, entre d'altres).
   7.4. Securització dels sistemes d'administració remota.
   7.5. Sistemes de prevenció i protecció enfront de virus i intrusions (antivirus, HIDS, etc.).
   7.6. Configuració d'actualitzacions i pegats automàtics.
   7.7. Sistemes de còpies de seguretat.
   7.8. Shadow IT i polítiques de seguretat en entorns SaaS.

Mòdul Professional 3: Posada en producció segura
Durada: 99
Equivalència en crèdits ECTS: 7
Unitats formatives que el componen:
UF 1: Posada en producció segura. 99 hores

UF1: Posada en producció segura
Durada: 99 hores
Resultats d'aprenentatge i criteris d'avaluació

1. Prova aplicacions web i aplicacions per a dispositius mòbils analitzant l'estructura de el codi i el seu model d'execució.

Criteris d'avaluació

1.1. S'han comparat diferents llenguatges de programació d'acord a les seves característiques principals.
1.2. Descriu els diferents models d'execució de programari.
1.3. Reconeix els elements bàsics de la font, donant-los significat.
1.4. Executa diferents tipus de prova de programari.
1.5. Avalua els llenguatges de programació d'acord a la infraestructura de seguretat que proporcionen.

2. Determina el nivell de seguretat requerit per aplicacions identificant els vectors d'atac habituals i els seus riscos associats.

Criteris d'avaluació:

2.1. Caracteritza els nivells de verificació de seguretat en aplicacions establertes pels estàndards internacionals (ASVS, "Application Security Verification Standard ").
2.2. Identifica el nivell de verificació de seguretat requerit per les aplicacions en funció dels seus riscos d'acord a estàndards reconeguts.
2.3. Enumera els requisits de verificació necessaris associats al nivell de seguretat establert.
2.4. Reconeix els principals riscos de les aplicacions desenvolupades, en funció de les seves característiques.

3. Detecta i corregeix vulnerabilitats d'aplicacions web analitzant el seu codi font i configurant servidors web.

Criteris d'avaluació:

3.1. Valida les entrades dels usuaris.
3.2. Detecta riscos d'injecció tant al servidor com en el client.
3.3. Gestiona correctament la sessió de l'usuari durant l'ús de l'aplicació.
3.4. Fa ús de rols per al control d'accés.
3.5. Utilitza algoritmes criptogràfics segurs per emmagatzemar les contrasenyes d'usuari.
3.6. Configura servidors web per reduir el risc de patir atacs coneguts.
3.7. Incorpora mesures per evitar els atacs a contrasenyes, enviament massiu de missatges o registres d'usuaris a través de programes automàtics (bots).

4. Detecta problemes de seguretat en les aplicacions per a dispositius mòbils, monitoritzant la seva execució i analitzant fitxers i dades.

Criteris d'avaluació:

4.1. Compara els diferents models de permisos de les plataformes mòbils.
4.2. Descriu tècniques d'emmagatzematge segur de dades en els dispositius, per evitar la fuga d'informació.
4.3. Implanta un sistema de validació de compres integrades en l'aplicació fent ús de validació al servidor.
4.4. Utilitza eines de monitorització de trànsit de xarxa per detectar l'ús de protocols insegurs de comunicació de les aplicacions mòbils.
4.5. Inspecciona binaris d'aplicacions mòbils per buscar fuites d'informació sensible.

5. Implanta sistemes segurs de desplegat de programari, utilitzant eines per a l'automatització de la construcció dels seus elements.

Criteris d'avaluació:

5.1. Identifica les característiques, principis i objectius de la integració del desenvolupament i operació de programari.
5.2. Implanta sistemes de control de versions, administrant els rols i permisos sol·licitats.
5.3. Instal·la, configura i verifica sistemes d'integració contínua, connectant-los amb sistemes de control de versions.

5.4. Planifica, implementa i automatitza plans de desplegat de programari.
5.5. Avalua la capacitat de sistema desplegat per reaccionar de forma automàtica a fallades.
5.6. Documenta les tasques realitzades i els procediments a seguir per a la recuperació davant desastres.
5.7. Crea bucles de retroalimentació àgils entre els membres de l'equip.

Continguts

1. Prova d'aplicacions web i per a dispositius mòbils:
   1.1. Fonaments de la programació.
   1.2. Llenguatges de programació interpretats i compilats.
   1.3. Codi font i entorns de desenvolupament.
   1.4. Execució de programari.
   1.5. Elements principals dels programes.
   1.6. Proves. Tipus.
   1.7. Seguretat en els llenguatges de programació i els seus entorns d'execució ("Sandboxes").
2. Determinació del nivell de seguretat requerit per aplicacions:
   2.1. Fonts obertes per al desenvolupament segur.
   2.2. Llistes de riscos de seguretat habituals: OWASP Top Ten (web i mòbil).
   2.3. Requisits de verificació necessaris associats al nivell de seguretat establert.
   2.4. Comprovacions de seguretat a nivell d'aplicació: ASVS (Application Security Verification Standard).
3. Detecció i correcció de vulnerabilitats d'aplicacions web:
   3.1. Desenvolupament segur d'aplicacions web.
   3.2. Llistes públiques de vulnerabilitats d'aplicacions web. OWASP Top Ten.
   3.3. Entrada basada en formularis. Injecció. Validació de l'entrada.
   3.4. Estàndards d'autenticació i autorització.
   3.5. Robatori de sessió.
   3.6. Vulnerabilitats web.
   3.7. Emmagatzematge segur de contrasenyes.
   3.8. Contramesures. HSTS, CSP, CAPTCHAs, entre d'altres.
   3.9. Seguretat de portals i aplicatius web. Solucions WAF (Web Application Firewall).
4. Detecció de problemes de seguretat en aplicacions per a dispositius mòbils:
   4.1. Models de permisos en plataformes mòbils. Trucades al sistema protegides.
   4.2. Signatura i verificació d'aplicacions.
   4.3. Emmagatzematge segur de dades.
   4.4. Validació de compres integrades en l'aplicació.
   4.5. Fugida d'informació en els executables.

4.6. Solucions CASB.

5. Implantació de sistemes segurs de desplegat de programari:
    5.1. Posada segura en producció.
    5.2. Pràctiques unificades per al desenvolupament i operació de programari (devops).
    5.3. Sistemes de control de versions.
    5.4. Sistemes d'automatització de construcció (build).
    5.5. Integració contínua i automatització de proves.
    5.6. Escalat de servidors. Virtualització. Contenidors.
    5.7. Gestió automatitzada de configuració de sistemes.
    5.8. Eines de simulació de fallades.
    5.9. Orquestració de contenidors.

Mòdul Professional 4: Anàlisi forense informàtic
Durada: 99
Equivalència en crèdits ECTS: 7
Unitats formatives que el componen:
UF 1: Anàlisi forense informàtic. 99 hores

UF1: Anàlisi forense informàtic.
Durada: 99 hores
Resultats d'aprenentatge i criteris d'avaluació

1. Aplica metodologies d'anàlisi forense caracteritzant les fases de preservació, adquisició, anàlisi i documentació.

Criteris d'avaluació

1.1. Identifica els dispositius a analitzar per garantir la preservació d'evidències.
1.2. Utilitza els mecanismes i les eines adequades per a l'adquisició i extracció de les evidències.
1.3. Assegura l'escena i conserva la cadena de custòdia.
1.4. Documenta el procés realitzat de manera metòdica.
1.5. Considera la línia temporal de les evidències.
1.6. Elabora un informe de conclusions a nivell tècnic i executiu.
1.7. Presenta i exposa les conclusions de l'anàlisi forense realitzat.

2. Realitza anàlisis forenses en dispositius mòbils, aplicant metodologies establertes, actualitzades i reconegudes.

Criteris d'avaluació:

2.1. Realitza el procés de presa de evidències en un dispositiu mòbil.
2.2. Extreu, descodifica i analitza les proves conservant la cadena de custòdia.
2.3. Genera informes de dades mòbils, complint amb els requisits de la indústria forense de telefonia mòbil.

2.4. Presenta i exposa les conclusions de l'anàlisi forense realitzat a qui procedeixi.

3. Realitza anàlisis forenses en Cloud, aplicant metodologies establertes, actualitzades i reconegudes.

Criteris d'avaluació:

3.1. Desenvolupa una estratègia d'anàlisi forense en Cloud, assegurant la disponibilitat dels recursos i capacitats necessaris un cop passat l'incident.

3.2. Aconsegueix identificar les causes, l'abast i l'impacte real causat per l'incident.

3.3. Realitza les fases de l'anàlisi forense en Cloud.

3.4. Identifica les característiques intrínseques del núvol (elasticitat, ubiqüitat, abstracció, volatilitat i compartició de recursos).

3.5. Acompleix els requeriments legals en vigor, RGPD (Reglament general de protecció de dades) i directiva NIS (Directiva de la UE sobre seguretat de xarxes i sistemes d'informació) o les que eventualment puguin substituir-les.

3.6. Presenta i exposa les conclusions de l'anàlisi forense realitzat.

4. Realitza anàlisi forense en dispositius de l'IOT, aplicant metodologies establertes, actualitzades i reconegudes.

Criteris d'avaluació:

4.1. Identifica els dispositius a analitzar garantint la preservació de les evidències.

4.2. Utilitza mecanismes i eines adequades per a l'adquisició i extracció d'evidències.

4.3. Garanteix l'autenticitat, completesa, fiabilitat i legalitat de les evidències extretes.

4.4. Realitza anàlisis d'evidències de manera manual i mitjançant eines.

4.5. Documenta el procés de manera metòdica i detallada.

4.6. Considera la línia temporal de les evidències.

4.7. Manté la cadena de custòdia.

4.8. Elabora un informe de conclusions a nivell tècnic i executiu.

4.9. Presenta i exposa les conclusions de l'anàlisi forense realitzat.

5. Documenta anàlisis forenses elaborant informes que incloguin la normativa aplicable.

Criteris d'avaluació:

5.1. Defineix l'objectiu de l'informe pericial i la seva justificació.

5.2. Defineix l'àmbit d'aplicació de l'informe pericial.

5.3. Documenta els antecedents.

5.4. Recopila les normes legals i reglaments complerts en l'anàlisi forense realitzat.

5.5. Recull els requisits establerts pel client.

5.6. Inclou les conclusions i la seva justificació.

Continguts

1. Aplicació de metodologies d'anàlisi forenses:

1.1. Identificació dels dispositius a analitzar.

1.2. Recol·lecció d'evidències (treballar un escenari).
1.3. Anàlisi de la línia de temps (TimeStamp).
1.4. Anàlisi de volatilitat - Extracció d'informació (volatility).
1.5. Anàlisi de Logs, eines més usades.

2. Realització d'anàlisis forenses en dispositius mòbils:
   2.1. Mètodes per a l'extracció d'evidències.
   2.2. Eines de mercat més comuns.
3. Realització d'anàlisis forenses en Cloud:
   3.1. Núvol privat i núvol públic o híbrid.
   3.2. Reptes legals, organitzatius i tècnics particulars d'una anàlisi en Cloud.
   3.3. Estratègies d'anàlisi forense en Cloud.
   3.4. Realitzar les fases rellevants de l'anàlisi forense en Cloud.
   3.5. Utilitzar eines d'anàlisi en Cloud (Cellebrite UFED Cloud Analizer, Cloud Trail, Frost, OWADE, ...).
4. Realització d'anàlisis forenses a IOT:
   4.1. Identificar els dispositius a analitzar.
   4.2. Adquirir i extreure les evidències.
   4.3. Analitzar les evidències de manera manual i automàtica.
   4.4. Documentar el procés realitzat.
   4.5. Establir la línia temporal.
   4.6. Mantenir la cadena de custòdia.
   4.7. Elaborar les conclusions.
   4.8. Presentar i exposar les conclusions.
5. Documentació i elaboració d'informes d'anàlisis forenses. Apartats dels que es compon l'informe:
   5.1. Full d'identificació (títol, raó social, nom i cognoms, signatura).
   5.2. Índex de la memòria.
   5.3. Objecte (objectiu de l'informe pericial i la seva justificació).
   5.4. Abast (àmbit d'aplicació de l'informe pericial - resum executiu per a una supervisió ràpida de el contingut i resultats).
   5.5. Antecedents (aspectes necessaris per a la comprensió de les alternatives estudiades i les conclusions finals).
   5.6. Normes i referències (documents i normes legals i reglaments esmentats en els diferents apartats).
   5.7. Definicions i abreviatures (definicions, abreviatures i expressions tècniques que s'han utilitzat al llarg de l'informe).
   5.8. Requisits (bases i dades de partida establerts pel client, la legislació, reglamentació i normativa aplicables).
   5.9. Anàlisi de solucions - resum de conclusions de l'informe pericial (alternatives estudiades, quins camins s'han seguit per arribar-hi, avantatges i inconvenients de cadascuna i quina és la solució finalment triada i la seva justificació).
   5.10. Annexos.

Mòdul Professional 5: Hacking ètic
Durada: 99
Equivalència en crèdits ECTS: 7
Unitats formatives que el componen:
UF 1: Hacking ètic. 99 hores

UF1: Hacking ètic
Durada: 99 hores
Resultats d'aprenentatge i criteris d'avaluació

1. Determina eines de monitorització per detectar vulnerabilitats aplicant tècniques de hacking ètic.

Criteris d'avaluació:

- 1.1. Defineix la terminologia essencial del hacking ètic.
- 1.2. Identifica els conceptes ètics i legals davant el ciberdelicte.
- 1.3. Defineix l'abast i condicions d'un test d'intrusió.
- 1.4. Identifica els elements essencials de seguretat: confidencialitat, autenticitat, integritat i disponibilitat.
- 1.5. Identifica les fases d'un atac seguides per un atacant.
- 1.6. Analitza i defineix els tipus vulnerabilitats.
- 1.7. Analitza i defineix els tipus d'atac.
- 1.8. Determina i caracteritza les diferents vulnerabilitats existents.
- 1.9. Determina les eines de monitorització disponibles al mercat adequades en funció del tipus d'organització.

2. Ataca i defensa en entorns de prova, comunicacions sense fil aconseguint accés a xarxes per demostrar les seves vulnerabilitats.

Criteris d'avaluació:

- 2.1. Configura els diferents modes de funcionament de la targeta de xarxa sense fils.
- 2.2. Descriu les tècniques d'encriptació de les xarxes sense fils i els seus punts vulnerables.
- 2.3. Detecta xarxes sense fils i captura tràfic de xarxa com a pas previ al seu atac.
- 2.4. Accedeix a xarxes sense fils vulnerables.
- 2.5. Caracteritza altres sistemes de comunicació sense fils i les seves vulnerabilitats.
- 2.6. Utilitza tècniques de "Equip Vermell i Blau".
- 2.7. Realitza informes sobre les vulnerabilitats detectades.

3. Ataca i defensa en entorns de prova, xarxes i sistemes aconseguint accés a informació i sistemes de tercers.

Criteris d'avaluació:

- 3.1. Recopila informació sobre la xarxa i sistemes objectiu mitjançant tècniques passives.

3.2. Crea un inventari d'equips, comptes d'usuari i potencials vulnerabilitats de la xarxa i sistemes objectiu mitjançant tècniques actives.
3.3. Intercepta tràfic de xarxa de tercers per buscar informació sensible.
3.4. Realitza un atac d'intermediari, llegint, inserint i modificant, a voluntat, el tràfic intercanviat per dos extrems remots.
3.5. Compromet sistemes remots explotant les seves vulnerabilitats.

4. Consolida i utilitza sistemes compromesos garantint accessos futurs.

Criteris d'avaluació:

4.1. Administra sistemes remots a través d'eines de línia d'ordres.
4.2. Compromet contrasenyes a través d'atacs de diccionari, taules rainbow i força bruta contra els seus versions encriptades.
4.3. Accedeix a sistemes addicionals a través de sistemes compromesos.
4.4. Instal·la portes posteriors per garantir accessos futurs als sistemes compromesos.

5. Ataca i defensa en entorns de prova, aplicacions web aconseguint accés a dades o funcionalitats no autoritzades.

Criteris d'avaluació:

5.1. Identifica els diferents sistemes d'autenticació web, destacant les seves debilitats i fortaleses.
5.2. Realitza un inventari d'equips, protocols, serveis i sistemes operatius que proporcionen el servei d'una aplicació web.
5.3. Analitza el flux de les interaccions realitzades entre el navegador i l'aplicació web durant el seu ús normal.
5.4. Examina manualment aplicacions web a la recerca de les vulnerabilitats més habituals.
5.5. Fa servir eines de recerques i explotació de vulnerabilitats web.
5.6. Realitza la recerca i explotació de vulnerabilitats web mitjançant eines programari.

Continguts

1. Determinació de les eines de monitorització per detectar vulnerabilitats:
   1.1. Elements essencials del hacking ètic.
   1.2. Diferències entre hacking, hacking ètic, tests de penetració i hacktivisme.
   1.3. Recollida de permisos i autoritzacions previs a un test d'intrusió.
   1.4. Fases del hacking.
   1.5. Auditories de caixa negra i de caixa blanca.
   1.6. Documentació de vulnerabilitats.
   1.7. Classificació d'eines de seguretat i hacking.
   1.8. Clearnet, Deep Web, Dark web, Darknets. Coneixement, diferències i eines d'accés: Tor. ZeroNet, freenet.
2. Atac i defensa en entorn de proves, de les comunicacions sense fil:
   2.1. Comunicació sense fils.
   2.2. Mode infraestructura, ad hoc i monitor.

2.3. Anàlisi i recollida de dades en xarxes sense fils.
2.4. Tècniques d'atacs i exploració de xarxes sense fils.
2.5. Atacs a altres sistemes sense fil.
2.6. Realització d'informes d'auditoria i presentació de resultats.

3. Atac i defensa en entorn de proves, de xarxes i sistemes per accedir a sistemes de tercers:
   3.1. Fase de reconeixement (footprinting).
   3.2. Fase d'escaneig (fingerprinting).
   3.3. Monitorizacion de trànsit.
   3.4. Intercepció de comunicacions utilitzant diferents tècniques.
   3.5. Manipulació i injecció de trànsit.
   3.6. Eines de cerca i explotació de vulnerabilitats.
   3.7. Enginyeria social. Phising.
   3.8. Escalada de privilegis.
4. Consolidació i utilització de sistemes compromesos:
   4.1. Administració de sistemes de manera remota.
   4.2. Atacs i auditories de contrasenyes.
   4.3. Pivotatge a la xarxa.
   4.4. Instal·lació de portes del darrere amb troians (RAT, Remote Access Trojan).
5. Atac i defensa en entorn de proves, a aplicacions web:
   5.1. Negació de credencials en aplicacions web.
   5.2. Recollida de dades.
   5.3. Automatització de connexions a servidors web (exemple: Selenium).
   5.4. Anàlisi de trànsit a través de proxies d'intercepció.
   5.5. Recerca de vulnerabilitats habituals en aplicacions web.
   5.6. Eines per a l'explotació de vulnerabilitats web.

Mòdul Professional 6: Normativa de ciberseguretat
Durada: 66
Equivalència en crèdits ECTS: 3
Unitats formatives que el componen:
UF 1: Normativa de ciberseguretat. 66 hores

UF1: Normativa de ciberseguretat.
Durada: 66 hores
Resultats d'aprenentatge i criteris d'avaluació

1. Identifica els punts principals d'aplicació per assegurar el compliment normatiu reconeixent funcions i responsabilitats.

Criteris d'avaluació:

1.1. Identifica les bases de compliment normatiu a tenir en compte en les organitzacions.

1.2. Descriu i aplica els principis d'un bon govern i la seva relació amb l'ètica professional.
1.3. Defineix les polítiques i procediments, així com l'estructura organitzativa que estableixi la cultura de l'acompliment normatiu dins de les organitzacions.
1.4. Descriu les funcions o competències del responsable de l'acompliment normatiu dins de les organitzacions.
1.5. Estableix les relacions amb tercers per a un correcte compliment normatiu.

2. Dissenya sistemes de compliment normatiu seleccionant la legislació i jurisprudència d'aplicació.

Criteris d'avaluació:

2.1. Recull les principals normatives que afecten els diferents tipus d'organitzacions.
2.2. Estableix les recomanacions vàlides per a diferents tipus d'organitzacions d'acord amb la normativa vigent (ISO 19.600 entre d'altres).
2.3. Realitza anàlisis i avaluacions dels riscos de diferents tipus d'organitzacions d'acord amb la normativa vigent (ISO 31.000 entre d'altres).
2.4. Documenta el sistema de compliment normatiu dissenyat.

3. Relaciona la normativa rellevant per al compliment de la responsabilitat penal de les organitzacions i persones jurídiques amb els procediments establerts, recopilant i aplicant les normes vigents.

Criteris d'avaluació:

3.1. Identifica els riscos penals aplicables a diferents organitzacions.
3.2. Implanta les mesures necessàries per eliminar o minimitzar els riscos identificats.
3.3. Estableix un sistema de gestió de compliment normatiu penal d'acord amb la legislació i normativa vigent (Codi Penal i UNE 19.601, entre altres).
3.4. Determina els principis bàsics dins de les organitzacions per combatre el suborn i promoure una cultura empresarial ètica d'acord amb la legislació i normativa vigent (ISO 37.001 entre d'altres).

4. Aplica la legislació nacional de protecció de dades de caràcter personal, relacionant els procediments establerts amb les lleis vigents i amb la jurisprudència existent sobre la matèria.

Criteris d'avaluació:

4.1. Reconeix les fonts de el Dret d'acord amb l'ordenament jurídic en matèria de protecció de dades de caràcter personal.
4.2. Aplica els principis relacionats amb la protecció de dades de caràcter personal tant a nivell nacional com internacional.
4.3. Estableix els requisits necessaris per afrontar la privacitat des de les bases del disseny.
4.4. Configura les eines corporatives contemplant el compliment normatiu per defecte.

4.5. Realitza una anàlisi de riscos per al tractament dels drets a la protecció de dades.
4.6. Implanta les mesures necessàries per eliminar o minimitzar els riscos identificats en la protecció de dades.
4.7. Descriu les funcions o competències del delegat de protecció de dades dins de les organitzacions.

5. Recull i aplica la normativa vigent de ciberseguretat d'àmbit nacional i internacional, actualitzant els procediments establerts d'acord amb les lleis i amb la jurisprudència existent sobre la matèria.

Criteris d'avaluació:

5.1. Estableix el pla de revisions de la normativa, jurisprudència, notificacions, etc. jurídiques que puguin afectar l'organització.
5.2. Detecta nova normativa consultant les bases de dades jurídiques seguint el pla de revisions establert.
5.3. Analitza la nova normativa per determinar si s'aplica a l'activitat de l'organització.
5.4. Inclou en el pla de revisions les modificacions necessàries, sobre la nova normativa aplicable a l'organització, per a un correcte compliment normatiu.
5.5. Determina i implementa els controls necessaris per garantir el correcte compliment normatiu de les noves normatives. incloses en el pla de revisions.

Continguts

1. Punts principals d'aplicació per a un correcte compliment normatiu:
   1.1. Introducció a l'acompliment normatiu (Compliance: objectiu, definició i conceptes principals).
   1.2. Principis de el bon govern i ètica empresarial.
   1.3. Compliance Officer: funcions i responsabilitats.
   1.4. Relacions amb terceres parts dins del Compliance.
2. Disseny de sistemes de compliment normatiu:
   2.1. Sistemes de Gestió de Compliance.
   2.2. Entorn regulador d'aplicació.
   2.3. Anàlisi i gestió de riscos, mapes de riscos.
   2.4. Documentació del sistema de compliment normatiu dissenyat.
3. Legislació per al compliment de la responsabilitat penal:
   3.1. Riscos penals que afecten a l'organització.
   3.2. Sistemes de gestió de Compliance penal.
   3.3. Sistemes de gestió anticorrupció.
4. Legislació i jurisprudència en matèria de protecció de dades:
   4.1. Principis de protecció de dades.
   4.2. Novetats de l'RGPD de la Unió Europea.
   4.3. Privacitat per Disseny i per defecte.
   4.4. Anàlisi d'Impacte en Privadesa (PIA), i mesures de seguretat.
   4.5. Delegat de Protecció de Dades (DPO).

5. Normativa vigent de ciberseguretat d'àmbit nacional i internacional:
    5.1. Normes nacionals i internacionals.
    5.2. Sistema de Gestió de Seguretat de la Informació (estàndards internacionals) (ISO 27.001).
    5.3. Accés electrònic dels ciutadans als Serveis Públics. Esquema Nacional de Seguretat (ENS).
    5.4. Plans de Continuïtat de Negoci (estàndards internacionals) (ISO 22.301).
    5.5. Directiva NIS.
    5.6. Legislació sobre la protecció d'infraestructures crítiques. Llei PIC (Protecció d'infraestructures crítiques).

Mòdul Professional 7: Formació en centres de treball
Durada: 126
Unitats formatives que el componen:
UF 1: Formació en centres de treball. 126 hores

UF1: Formació en centres de treball.
Durada: 126 hores

1. Identifica l'estructura, l'organització i les condicions de treball de l'empresa, centre o servei, relacionant-les amb les activitats que realitza.

Criteris d'avaluació

1.1 Identifica les característiques generals de l'empresa, centre o servei i l'organigrama i les funcions de cada àrea.

1.2 Identifica els procediments de treball en el desenvolupament de l'activitat.

1.3 Identifica les competències dels llocs de treball en el desenvolupament de l'activitat.

1.4 Identifica les característiques del mercat o entorn, tipus d'usuaris i proveïdors.

1.5 Identifica les activitats de responsabilitat social de l'empresa, centre o servei envers l'entorn.

1.6 Identifica el flux de serveis o els canals de comercialització més freqüents en aquesta activitat.

1.7 Relaciona avantatges i inconvenients de l'estructura de l'empresa, centre o servei, davant d'altres tipus d'organitzacions relacionades.

1.8 Identifica el conveni col·lectiu o el sistema de relacions laborals al qual s'acull l'empresa, centre o servei.

1.9 Identifica els incentius laborals, les activitats d'integració o de formació i les mesures de conciliació en relació amb l'activitat.

1.10 Valora les condicions de treball en el clima laboral de l'empresa, centre o servei.

1.11 Valora la importància de treballar en grup per aconseguir amb eficàcia els objectius establerts en l'activitat i resoldre els problemes que es plantegen.

2. Desenvolupa actituds ètiques i laborals pròpies de l'activitat professional d'acord amb les característiques del lloc de treball i els procediments establerts pel centre de treball.

Criteris d'avaluació

2.1 Compleix l'horari establert.

2.2 Mostra una presentació personal adequada.

2.3 És responsable en l'execució de les tasques assignades.

2.4 S'adapta als canvis de les tasques assignades.

2.5 Manifesta iniciativa en la resolució de problemes.

2.6 Valora la importància de la seva activitat professional.

2.7 Manté organitzada la seva àrea de treball.

2.8 Té cura dels materials, equips o eines que utilitza en la seva activitat.

2.9 Manté una actitud clara de respecte vers el medi ambient.

2.10 Estableix una comunicació i relació eficaç amb el personal de l'empresa.

2.11 Es coordina amb els membres del seu equip de treball.

3. Realitza les activitats formatives de referència seguint protocols establerts pel centre de treball.

Criteris d'avaluació

3.1 Executa les tasques segons els procediments establerts.

3.2 Identifica les característiques particulars dels mitjans de producció, equips i eines.

3.3 Aplica les normes de prevenció de riscos laborals en l'activitat professional.

3.4 Fa servir els equips de protecció individual segons els riscos de l'activitat professional i les normes establertes pel centre de treball.

3.5 Aplica les normes internes i externes vinculades a l'activitat.

3.6 Obté la informació i els mitjans necessaris per realitzar l'activitat assignada.

3.7 Interpreta i expressa la informació amb la terminologia o simbologia i els mitjans propis de l'activitat.

3.8 Detecta anomalies o desviacions en l'àmbit de l'activitat assignada, n'identifica les causes i hi proposa possibles solucions.

Activitats formatives de referència

1. Activitats formatives de referència relacionades amb desenvolupar plans de prevenció i conscienciació en ciberseguretat, establint normes i mesures de protecció.

    1.1. Identificació dels principis generals en matèria de ciberseguretat.

    1.2. Aplicació de la normativa de protecció de el lloc de la feina.

    1.3. Desenvolupament d'un pla de formació i conscienciació en matèria de ciberseguretat.

    1.4. Desenvolupament de materials de formació i conscienciació.

    1.5. Realització d'auditories internes de compliment en matèria de prevenció.

2. Activitats formatives de referència relacionades amb analitzar incidents de ciberseguretat utilitzant eines, mecanismes de detecció i alertes de seguretat, recopilar i emmagatzemar de forma segura evidències d'incidents de ciberseguretat que afecten l'organització.

    2.1. Aplicació de la taxonomia d'incidents de ciberseguretat. Utilització de controls, eines i mecanismes de monitorització, identificació, detecció i alerta d'incidents.

    2.2. Aplicació de la classificació, valoració, documentació, seguiment inicial d'incidents de ciberseguretat. Recollida d'evidències, analitzar-les, investigar incidents i aplicar mesures de contenció.

3. Activitats formatives de referència relacionades amb desenvolupar procediments d'actuació detallats per donar resposta, mitigar, eliminar o contenir els tipus d'incidents de ciberseguretat més habituals i notificar l'incident.

    3.1. Desenvolupament de procediments d'actuació detallats per donar resposta, mitigar, eliminar o contenir els tipus d'incidents.

    3.2. Realització de tasques per restablir els serveis afectats per incidents.

    3.3. Realització del seguiment d'incidents per evitar una situació similar.

    3.4. Notificació d'incidents.

    3.5. Realització de l'anàlisi de riscos.

    3.6. Aplicació de principis de l'Economia Circular en la Indústria 4.0.

    3.7. Disseny del pla de mesures tècniques de seguretat i aplicar polítiques de securització més habituals.

    3.8. Realització guies de bones pràctiques per a la securització de sistemes i xarxes, aplicant estàndards de securització de sistemes i xarxes.

4. Activitats formatives de referència relacionades amb configurar sistemes de control d'accés i autenticació de persones preservant la confidencialitat i privacitat de les dades administrant credencials d'accés.

    4.1. Aplicació de mecanismes d'autenticació i la gestió de credencials basats en diferents tècniques.

    4.2. Desenvolupament d'infraestructures de Clau Pública (PKI).

    4.3. Aplicació d'accés per mitjà de Signatura electrònica.

    4.4. Administració de la gestió d'accessos. Sistemes NAC (Network Access Control, Sistemes de Gestió d'Accés a la Xarxa).

    4.5. Administració de la gestió de comptes privilegiades.

    4.6. Aplicació de protocols RADIUS i TACACS, servei Kerberos, entre d'altres.

5. Activitats formatives de referència relacionades amb dissenyar xarxes de computadors contemplant els requisits de seguretat.

    5.1. Disseny de la segmentació de xarxes.

5.2. Disseny de subnetting.

5.3. Disseny de xarxes virtuals (VLANs).

5.4. Disseny de la zona desmilitaritzada (DMZ).

5.5. Aplicació de seguretat en xarxes sense fils (WPA2, WPA3, etc.).

5.6. Aplicació de protocols de xarxa segura (IPSec, etc.).

6. Activitats formatives de referència relacionades amb configurar dispositius i sistemes informàtics complint els requisits de seguretat.

6.1. Configuració de seguretat perimetral. Configuració de tallafocs de Propera Generació.

6.2. Configuració de seguretat de portals i aplicatius web. Configuració de solucions WAF (Web Aplication Firewall).

6.3. Configuració de seguretat de el lloc de treball i endpoint fix i mòbil. Configuració d'antiAPT, antimalware.

6.4. Configuració de seguretat d'entorns cloud. Configuració de solucions CASB.

6.5. Configuració de la seguretat del correu electrònic.

6.6. Configuració de solucions DLP (Data Loss Prevention).

6.7. Configuració d'eines d'emmagatzematge de logs.

6.8. Configuració de protecció davant atacs de denegació de servei distribuït (DDoS).

6.9. Configuració de forma segura de tallafocs, encaminadors i proxies.

6.10. Configuració de xarxes privades virtuals (VPNs), i túnels (protocol IPSec).

6.11. Configuració de sistemes i dispositius.

6.12. Configuració d'eines de monitorització (IDS, IPS).

6.13. Configuració de SIEMs (Gestors d'Esdeveniments i Informació de Seguretat).

6.14. Configuració de solucions de Centres d'Operació de Xarxa, i Centres de Seguretat de Xarxa: NOCs i socs.

7. Activitats formatives de referència relacionades amb configurar dispositius per a la instal·lació de sistemes informàtics minimitzant les probabilitats d'exposició a atacs.

    7.1. Aplicació de precaucions prèvies a la instal·lació d'un sistema informàtic: aïllament, configuració del control d'accés a la BIOS, bloqueig de l'ordre d'arrencada dels dispositius, entre d'altres.

    7.2. Configuració de seguretat en l'arrencada de sistema informàtic, configuració de l'arrencada segur.

    7.3. Configuració de seguretat dels sistemes de fitxers, xifrat, partició, entre d'altres.

8. Activitats formatives de referència relacionades amb configurar sistemes informàtics, aplicacions web i aplicacions per a dispositius mòbils minimitzant les probabilitats d'exposició a atacs.

    8.1. Reducció del nombre de serveis, realització de hardening de processos, eliminació de protocols de xarxa innecessaris, securització dels sistemes d'administració remota, configuració de sistemes de prevenció i protecció enfront de virus i intrusions (antivirus, HIDS, etc.), configuració d'actualitzacions i pegats automàtics, configuració de sistemes de còpies de seguretat i configurar Shadow IT i polítiques de seguretat en entorns SaaS.

    8.2. Prova de la seguretat en els llenguatges de programació i els seus entorns d'execució ("Sandboxes").

    8.3. Anàlisi de les fonts obertes per al desenvolupament segur.

    8.4. Realització de llistes de riscos de seguretat habituals: OWASP Top Ten (web i mòbil).

    8.5. Establiment dels requisits de verificació necessaris associats al nivell de seguretat establert.

    8.6. Realització de les comprovacions de seguretat a nivell d'aplicació: ASVS (Application Security Verification Standard).

    8.7. Aplicar el desenvolupament segur d'aplicacions web.

    8.8. Realització de llistes públiques de vulnerabilitats d'aplicacions web. OWASP Top Ten.

    8.9. Anàlisi de l'entrada basada en formularis, injecció i validació de l'entrada.

8.10. Aplicació d'estàndards d'autenticació i autorització.

8.11. Detecció i correcció del robatori de sessió.

8.12. Detecció i correcció de vulnerabilitats web.

8.13. Anàlisi de l'emmagatzematge segur de contrasenyes.

8.14. Aplicació de contramesures. HSTS, CSP, CAPTCHAs, entre d'altres.

8.15. Detecció i correcció de seguretat de portals i aplicatius web. Solucions WAF (Web Application Firewall).

8.16. Anàlisi de la signatura i la verificació d'aplicacions.

8.17. Aplicació de l'emmagatzematge segur de dades.

8.18. Validació de compres integrades en l'aplicació.

8.19. Anàlisi de la fugida d'informació en els executables.

8.20. Aplicació de solucions CASB.

9. Activitats formatives de referència relacionades amb aplicar metodologies d'anàlisi forense caracteritzant les fases de preservació, adquisició, anàlisi i documentació en dispositius mòbils, en Cloud i en IoT.

9.1. Identificació dels dispositius a analitzar.

9.2. Recollida d'evidències.

9.3. Anàlisi de la línia de temps.

9.4. Anàlisi de la volatilitat d'informació.

9.5. Anàlisi de Logs utilitzant les eines més usades.

9.6. Documentació del procés realitzat.

9.7. Establiment de la línia temporal.

9.8. Manteniment de la cadena de custòdia.

9.9. Elaboració de les conclusions.

9.10. Presentació i exposició de les conclusions.

10. Activitats formatives de referència relacionades amb atacar i defensar en entorns de prova, aconseguint accés a xarxes per demostrar les seves vulnerabilitats.

    10.1. Atac i defensa, identificació de vulnerabilitats, anàlisi i recollida de dades.

11. Activitats formatives de referència relacionades amb identificar els punts principals d'aplicació per assegurar el compliment normatiu reconeixent funcions i responsabilitats.

    11.1. Compliment de la normativa.

    11.2. Identificació dels principis de el bon govern i de l'ètica empresarial.

    11.3. Compliance Officer: funcions i responsabilitats.

    11.4. Establiment de les relacions amb terceres parts dins del Compliance.

12. Activitats formatives de referència relacionades amb dissenyar sistemes de compliment normatiu seleccionant la legislació i jurisprudència d'aplicació i relacionar la normativa i legislació rellevant.

    12.1. Disseny d'un sistema de Gestió de Compliance.

    12.2. Estudi de l'entorn regulador d'aplicació.

    12.3. Realització de l'anàlisi i gestió de riscos, mapes de riscos.

    12.4. Documentació del sistema de compliment normatiu dissenyat.

    12.5. Identificació dels riscos penals que afecten a l'organització.

    12.6. Estudi dels sistemes de gestió de Compliance penal.

    12.7. Coneixement dels sistemes de gestió anticorrupció.

    12.8. Aplicació dels principis de protecció de dades.

    12.9. Coneixement de les novetats de l'RGPD de la Unió Europea.

    12.10. Aplicació de privacitat per disseny i per defecte.

    12.11. Realització de l'anàlisi d'Impacte en Privadesa (PIA), i mesures de seguretat.

    12.12. Estudi de les característiques del delegat de Protecció de Dades (DPO).