ANNEX III

I. IDENTIFICACIÓ DEL CERTIFICAT DE PROFESSIONALITAT

Denominació: Seguretat informàtica

Codi: IFCT0109

Família professional: Informàtica i comunicacions

Àrea professional: Sistemes i telemàtica

Nivell de qualificació professional: 3

Qualificació professional de referència:

IFC153_3 Seguretat informàtica (RD 1087/05, de 16 de setembre)

Relació d'unitats de competència que configuren el certificat de professionalitat:

UC0486_3: Assegurar els equips informàtics.
UC0487_3: Auditar xarxes de comunicació i sistemes informàtics.
UC0488_3: Detectar i respondre davant d'incidents de seguretat.
UC0489_3: Dissenyar i implementar sistemes segurs d'accés i transmissió de dades.
UC0490_3: Gestionar serveis al sistema informàtic.

Competència general:

Garantir la seguretat dels accessos i els usos de la informació registrada en equips informàtics, així com la del sistema, protegint-se alhora dels possibles atacs, identificant vulnerabilitats i aplicant sistemes de xifratge a les comunicacions que es realitzin cap a l'exterior i a dins de l'organització.

Entorn professional:

Àmbit professional:

Desenvolupa la seva activitat professional en l'àrea de sistemes del departament d'informàtica d'empreses públiques o privades que utilitzen equipament informàtic, exercint tasques d'auditoria i de configuració, així com temes relacionats amb la seguretat informàtica, tant per compte aliè com per compte propi.

Sectors productius:

Està present en múltiples sectors productius, especialment en el sector serveis, tot i que es percep una marcada característica de transsectorialitat. També està present en els següents tipus d'empreses:

- Empreses de qualsevol sector i mida que utilitzen equipament informàtic en els seus processos de gestió.
- Empreses que presten serveis d'assistència tècnica informàtica.
- Empreses d'externalització (*outsourcing*) de serveis.

Ocupacions o llocs de treball relacionats:

3820.1017 Programador/a d'aplicacions informàtiques.
3812.1014 Tècnic/a en informàtica de gestió.
Tècnic/a en seguretat informàtica.
Tècnic/a en auditoria informàtica.

Durada de la formació associada: 500 hores

Relació de mòduls formatius i unitats formatives:

MF0486_3: Seguretat en equips informàtics (90 hores).
MF0487_3: Auditoria de seguretat informàtica (90 hores).
MF0488_3: Gestió d'incidents de seguretat informàtica (90 hores).
MF0489_3: Sistemes segurs d'accés i transmissió de dades (60 hores).
MF0490_3: (Transversal) Gestió de serveis al sistema informàtic (90 hores).
MP0175: Mòdul de pràctiques professionals no laborals de seguretat informàtica (80 hores).

II. PERFIL PROFESSIONAL DEL CERTIFICAT DE PROFESSIONALITAT

El perfil professional del certificat de professionalitat es defineix per la qualificació professional i/o per les unitats de competència del Catàleg Nacional de Qualificacions Professionals que aquest tingui de referència. Inclou les realitzacions professionals (RP) i els criteris de realització (CR) de cadascuna de les unitats de competència que conformen el certificat de professionalitat.

Aquesta informació es pot consultar, en català, al Catàleg de Qualificacions Professionals de Catalunya publicat al web de l'Institut Català de Qualificacions Professionals, a http://aplitic.xtec.cat/e13_cfp_icqp/menuInici.do.

III. FORMACIÓ DEL CERTIFICAT DE PROFESSIONALITAT

MÒDUL FORMATIU 1

Denominació: SEGURETAT EN EQUIPS INFORMÀTICS

Codi: MF0486_3

Nivell de qualificació professional: 3

Associat a la unitat de competència:

UC0486_3: Assegurar equips informàtics.

Durada: 90 hores

Capacitats i criteris d'avaluació

C1: Analitzar els plans d'implantació de l'organització per identificar els elements del sistema implicats i els nivells de seguretat que s'han d'implementar.
CE1.1 Identificar l'estructura d'un pla d'implantació i explicar els continguts que

figuren a cada secció.
CE1.2 Distingir els sistemes que poden aparèixer en el pla d'implantació i descriure les funcionalitats de seguretat que implementen.
CE1.3 Descriure els nivells de seguretat que figuren en el pla d'implantació i associar-los als permisos d'accés per a la implantació.
CE1.4 En un supòsit pràctic en què es demana analitzar el pla d'implantació i les repercussions que té en el sistema:
- Determinar els sistemes implicats en el pla d'implantació.
- Analitzar els requisits de seguretat de cada sistema.
- Descriure les mesures de seguretat que cal aplicar a cada sistema.
- Emplenar els formularis per a la declaració de fitxers de dades de caràcter personal.

C2: Analitzar i implementar els mecanismes d'accés físics i lògics als servidors segons les especificacions de seguretat.
CE2.1 Descriure les característiques dels mecanismes de control d'accés físic i explicar-ne les funcions principals.
CE2.2 Exposar els mecanismes de traça i associar-los al sistema operatiu del servidor.
CE2.3 Identificar els mecanismes de control d'accés lògic i explicar-ne les característiques principals (contrasenyes, filtratge de ports IP, entre d'altres).
CE2.4 En un supòsit pràctic d'implantació d'un servidor segons unes especificacions donades:
- Determinar la ubicació física del servidor per assegurar-ne la funcionalitat.
- Descriure i justificar les mesures de seguretat física que cal implementar per garantir la integritat del sistema.
- Identificar els mòduls o les aplicacions addicionals per implementar el nivell de seguretat requerit pel servidor.
- Determinar les amenaces a què s'exposa el servidor i avaluar-ne el risc d'acord amb el context del servidor.
- Determinar els permisos assignats als usuaris i grups d'usuaris per utilitzar el sistema.

C3: Avaluar la funció i la necessitat de cada servei en execució al servidor segons les especificacions de seguretat.
CE3.1 Identificar els serveis habituals al sistema informàtic d'una organització i descriure la seva missió dins de la infraestructura informàtica i de comunicacions.
CE3.2 Identificar i descriure els serveis necessaris per al funcionament d'un servidor, en funció de la seva missió dins del sistema informàtic de l'organització.
CE3.3 Descriure les amenaces dels serveis en execució, aplicant els permisos més restrictius per garantir-ne l'execució i minimitzar els riscos.
CE3.4 En un supòsit pràctic d'implantació d'un servidor amb un conjunt de serveis en execució amb correspondències a un pla d'explotació donat:
- Indicar les relacions existents entre aquest servidor i la resta del sistema informàtic de l'organització.
- Extreure del pla d'implantació els requisits de seguretat aplicables al servidor.
- Determinar els serveis mínims necessaris per al funcionament del sistema.

C4: Instal·lar, configurar i administrar un tallafoc de servidor amb les característiques necessàries segons les especificacions de seguretat.
CE4.1 Classificar els tipus de tallafocs, de xarxa i locals, maquinari i programari, de paquets i aplicació, i descriure'n les característiques i

funcionalitats principals.
CE4.2 Descriure les regles de filtratge d'un tallafoc de servidor i explicar-ne els paràmetres principals.
CE4.3 Explicar el format de traça d'un tallafoc de servidor i reflectir la informació de seguretat rellevant.
CE4.4 Partint d'un supòsit pràctic d'instal·lació d'un tallafoc de servidor en un escenari d'accessos locals i remots:
- Determinar els requisits de seguretat del servidor.
- Establir les relacions del servidor amb la resta d'equips del sistema informàtic.
- Elaborar el llistat de regles d'accés que cal implementar al servidor.
- Compondre un pla de proves del tallafoc implementat.
- Executar el pla de proves i redactar les correccions necessàries per corregir les deficiències detectades.

Sumari

matèria de protecció de dades de caràcter personal.

6. **Seguretat física i industrial dels sistemes. Seguretat lògica dels sistemes.**
   - Determinació dels perímetres de seguretat física.
   - Sistemes de control d'accés físic més freqüents a les instal·lacions de l'organització i a les àrees en què estan ubicats els sistemes informàtics.
   - Criteris de seguretat per a l'emplaçament físic dels sistemes informàtics.
   - Exposició d'elements més freqüents per garantir la qualitat i la continuïtat del subministrament elèctric als sistemes informàtics.
   - Requeriments de climatització i protecció contra incendis aplicables als sistemes informàtics.
   - Elaboració de la normativa de seguretat física i industrial per a l'organització.
   - Sistemes de fitxers més utilitzats.
   - Establiment del control d'accessos dels sistemes informàtics a la xarxa de comunicacions de l'organització.
   - Configuració de polítiques i directives del directori d'usuaris.
   - Establiment de les llistes de control d'accés (ACL) a fitxers.
   - Gestió d'altes, baixes i modificacions d'usuaris, i privilegis que tenen assignats.
   - Requeriments de seguretat relacionats amb el control d'accés dels usuaris al sistema operatiu.
   - Sistemes d'autenticació d'usuaris febles, forts i biomètrics.
   - Relació dels registres d'auditoria del sistema operatiu necessaris per monitorar i supervisar el control d'accessos.
   - Elaboració de la normativa de control d'accessos als sistemes informàtics.

7. **Identificació de serveis.**
   - Identificació dels protocols, serveis i ports utilitzats pels sistemes d'informació.
   - Ús d'eines d'anàlisi de ports i serveis oberts per determinar els que no són necessaris.
   - Ús d'eines d'anàlisi de trànsit de comunicacions per determinar l'ús real que fan els sistemes d'informació dels diferents protocols, serveis i ports.

8. **Enfortiment de sistemes.**
   - Modificació dels usuaris i les contrasenyes per defecte dels diferents sistemes d'informació.
   - Configuració de les directives de gestió de contrasenyes i privilegis en el directori d'usuaris.
   - Eliminació i tancament de les eines, les utilitats, els serveis i els ports prescindibles.
   - Configuració dels sistemes d'informació perquè utilitzin protocols segurs allà on sigui possible.
   - Actualització de pedaços de seguretat dels sistemes informàtics.
   - Protecció dels sistemes d'informació davant de codi maliciós.
   - Gestió segura de comunicacions, carpetes compartides, impressores i altres recursos compartits del sistema.
   - Monitoratge de la seguretat i l'ús adequat dels sistemes d'informació.

9. **Implantació i configuració de tallafocs.**
   - Relació dels diferents tipus de tallafocs per ubicació i funcionalitat.
   - Criteris de seguretat per a la segregació de xarxes al tallafoc mitjançant zones desmilitaritzades (DMZ).
   - Ús de xarxes privades virtuals (VPN) per establir canals segurs de comunicacions.

- Definició de regles de tall als tallafocs.
- Relació dels registres d'auditoria del tallafoc necessaris per monitorar i supervisar el funcionament correcte i els esdeveniments de seguretat.
- Establiment del monitoratge i proves del tallafoc.

Orientacions metodològiques

Formació a distància:

Mòdul formatiu	Nombre total d'hores del mòdul	Nombre màxim d'hores susceptibles de formació a distància
Mòdul formatiu - MF0486_3	90	40

Criteris d'accés per als alumnes

Són els que estableix l'article 4 del reial decret que regula el certificat de professionalitat de la família professional que acompanya aquest annex.

MÒDUL FORMATIU 2

Denominació: AUDITORIA DE SEGURETAT INFORMÀTICA

Codi: MF0487_3

Nivell de qualificació professional: 3

Associat a la unitat de competència:

UC0487_3: Auditar xarxes de comunicació i sistemes informàtics.

Durada: 90 hores

Capacitats i criteris d'avaluació

C1: Analitzar i seleccionar les eines d'auditoria i detecció de vulnerabilitats del sistema informàtic, i implantar les que s'adeqüin a les especificacions de seguretat informàtica.

CE1.1 Explicar les diferències entre vulnerabilitats i amenaces.

CE1.2 Enunciar les característiques dels principals tipus de vulnerabilitats i programes maliciosos existents, i descriure'n les particularitats.

CE1.3 Descriure el funcionament d'una eina d'anàlisi de vulnerabilitats, i indicar les principals tècniques emprades i la seva fiabilitat.

CE1.4 Seleccionar l'eina d'auditoria de seguretat més adequada en funció del servidor o la xarxa i els requisits de seguretat.

CE1.5 Partint d'un supòsit pràctic, davant d'un sistema informàtic donat i en unes circumstàncies d'implantació concretes:

- Establir els requisits de seguretat que ha de complir cada sistema.
- Crear una prova nova per a l'eina d'auditoria partint de les especificacions de la vulnerabilitat.
- Elaborar el pla de proves tenint en compte el tipus de servidor analitzat.
- Utilitzar diverses eines per detectar possibles vulnerabilitats.
- Analitzar el resultat de l'eina d'auditoria i descartar els falsos positius.
- Redactar l'informe d'auditoria, reflectint les irregularitats detectades i els suggeriments de regularització.

C2: Aplicar procediments relatius al compliment de la normativa legal vigent.

CE2.1 Explicar la normativa legal vigent (autonòmica, nacional, europea i internacional) aplicable a dades de caràcter personal.

CE2.2 Exposar els tràmits legals que han de complir els fitxers amb dades de caràcter personal, tenint en compte la seva qualitat.

CE2.3 Descriure els nivells de seguretat establerts en la normativa legal vigent i associar-los als requisits exigits.

CE2.4 A partir d'un supòsit pràctic en què es disposa d'una estructura de registre d'informació d'una organització:

- Identificar els fitxers amb dades de caràcter personal, justificant el nivell de seguretat que li correspon.
- Elaborar el pla d'auditoria de compliment de legislació en matèria de protecció de dades de caràcter personal.
- Revisar la documentació associada als fitxers amb dades de caràcter personal i identificar-hi les mancances existents.
- Elaborar l'informe corresponent als fitxers de caràcter personal i indicar les deficiències trobades i les correccions pertinents.

C3: Planificar i aplicar mesures de seguretat per garantir la integritat del sistema informàtic i dels punts d'entrada i sortida de la xarxa departamental.

CE3.1 Identificar les fases de l'anàlisi de riscos i descriure l'objectiu de cada fase.

CE3.2 Descriure els termes associats a l'anàlisi de riscos (amenaça, vulnerabilitat, impacte i contramesures) i establir la relació entre ells.

CE3.3 Descriure les tècniques d'anàlisi de xarxes i explicar els criteris de selecció.

CE3.4 Descriure les tipologies de tallafocs de xarxa comunes i indicar-ne les funcionalitats principals.

Sumari

1. Criteris generals comunament acceptats sobre auditoria informàtica.

- Codi deontològic de la funció d'auditoria.
- Relació dels diferents tipus d'auditoria en el marc dels sistemes d'informació.
- Criteris que cal seguir per a la composició de l'equip auditor.
- Tipus de proves que cal realitzar en el marc de l'auditoria, proves substantives i proves de compliment.
- Tipus de mostreig que cal aplicar durant el procés d'auditoria.
- Ús d'eines de tipus CAAT (*Computer Assisted Audit Tools*).
- Explicació dels requeriments que han de complir les troballes d'auditoria.
- Aplicació de criteris comuns per categoritzar les troballes com a observacions o no conformitats.
- Relació de les normatives i metodologies relacionades amb l'auditoria de sistemes d'informació comunament acceptades.

2. Aplicació de la normativa de protecció de dades de caràcter personal.

- Principis generals de protecció de dades de caràcter personal.
- Normativa europea recollida a la Directiva 95/46/CE.
- Normativa nacional recollida al codi penal, la Llei orgànica de regulació del tractament automatitzat de dades (LORTAD), la Llei orgànica de protecció de dades (LOPD) i el Reglament de desenvolupament de la Llei orgànica de protecció de dades (RD 1720/2007).
- Identificació i registre dels fitxers amb dades de caràcter personal utilitzats

per l'organització.
- Explicació de les mesures de seguretat per a la protecció de les dades de caràcter personal recollides al Reial decret 1720/2007.
- Guia per a la realització de l'auditoria biennal obligatòria segons la Llei orgànica 15-1999 de protecció de dades de caràcter personal.

3. Anàlisi de riscos dels sistemes d'informació.
- Introducció a l'anàlisi de riscos.
- Principals tipus de vulnerabilitats, errors de programa, programes maliciosos i actualització permanent, així com criteris de programació segura.
- Particularitats dels diferents tipus de codi maliciós.
- Principals elements de l'anàlisi de riscos i models de relacions.
- Metodologies qualitatives i quantitatives d'anàlisis de riscos.
- Identificació dels actius involucrats en l'anàlisi de riscos i valoració.
- Identificació de les amenaces que poden afectar els actius identificats prèviament.
- Anàlisi i identificació de les vulnerabilitats existents en els sistemes d'informació que permetrien la materialització d'amenaces, inclosos l'anàlisi local i l'anàlisi remot de caixa blanca i de caixa negra.
- Optimització del procés d'auditoria i contrast de vulnerabilitats i informe d'auditoria.
- Identificació de les mesures de salvaguarda existents en el moment de realitzar l'anàlisi de riscos i efecte d'aquestes mesures sobre les vulnerabilitats i amenaces.
- Establiment dels escenaris de risc entesos com a parells actiu-amenaça susceptibles de materialitzar-se.
- Determinació de la probabilitat i l'impacte de materialització dels escenaris.
- Establiment del nivell de risc per als diferents parells actiu-amenaça.
- Determinació per part de l'organització dels criteris d'avaluació del risc, en funció dels quals es determina si un risc és acceptable o no.
- Relació de les diferents alternatives de gestió de riscos.
- Guia per a l'elaboració del pla de gestió de riscos.
- Exposició de la metodologia NIST SP 800-30.
- Exposició de la metodologia Magerit versió 2.

4. Ús d'eines per a l'auditoria de sistemes.
- Eines del sistema del tipus Ping, Traceroute, etc.
- Eines d'anàlisi de xarxa, ports i serveis de tipus Nmap, Netcat, NBTScan, etc.
- Eines d'anàlisi de vulnerabilitats de tipus Nessus.
- Analitzadors de protocols de tipus WireShark, DSniff, Cain & Abel, etc.
- Analitzadors de pàgines web de tipus Acunetix, Dirb, Parosproxy, etc.
- Atacs de diccionari i força bruta de tipus Brutus, John the Ripper, etc.

5. Descripció dels aspectes sobre tallafocs en auditories de sistemes informàtics.
- Principis generals dels tallafocs.
- Components d'un tallafoc de xarxa.
- Relació dels diferents tipus de tallafocs per ubicació i funcionalitat.
- Arquitectures de tallafocs de xarxa.
- Altres arquitectures de tallafocs de xarxa.

6. Guies per a l'execució de les diferents fases de l'auditoria de sistemes d'informació.
- Guia per a l'auditoria de la documentació i normativa de seguretat existent a

l'organització auditada.
- Guia per a l'elaboració del pla d'auditoria.
- Guia per a les proves d'auditoria.
- Guia per a l'elaboració de l'informe d'auditoria.

Orientacions metodològiques

Formació a distància:

Mòdul formatiu	Nombre total d'hores del mòdul	Nombre màxim d'hores susceptibles de formació a distància
Mòdul formatiu - MF0487_3	90	40

Criteris d'accés per als alumnes

Són els que estableix l'article 4 del reial decret que regula el certificat de professionalitat de la família professional que acompanya aquest annex.

MÒDUL FORMATIU 3

Denominació: GESTIÓ D'INCIDENTS DE SEGURETAT INFORMÀTICA

Codi: MF0488_3

Nivell de qualificació professional: 3

Associat a la unitat de competència:

UC0488_3: Detectar i respondre davant d'incidents de seguretat.

Durada: 90 hores

Capacitats i criteris d'avaluació

C1: Planificar i implantar els sistemes de detecció d'intrusos segons les normes de seguretat.

CE1.1 Descriure les tècniques de detecció i prevenció d'intrusos, o exposar els principals paràmetres que poden emprar-se com a criteris de detecció.

CE1.2 Determinar el nombre, el tipus i la ubicació dels sistemes de detecció d'intrusos, garantint el monitoratge del trànsit indicat al pla d'implantació.

CE1.3 Seleccionar les regles del sistema de detecció d'intrusos en funció del sistema informàtic subjecte al monitoratge.

CE1.4 Determinar els llindars d'alarma del sistema tenint en compte els paràmetres d'ús.

CE1.5 Elaborar regles de detecció partint de la caracterització de les tècniques d'intrusió.

CE1.6 Partint d'un supòsit pràctic convenientment caracteritzat en què s'ubiquen servidors amb possibilitat d'accessos locals i remots:
- Instal·lar i configurar programari de recollida d'alarmes.
- Configurar diferents nivells de recollida d'alarmes.

CE1.7 En una col·lecció de supòsits pràctics en un entorn controlat de servidors en diverses zones d'una xarxa departamental amb connexió a Internet:
- Decidir les àrees que cal protegir.
- Instal·lar un sistema de detecció d'intrusos.

- Definir i aplicar normes de detecció.
- Verificar el funcionament del sistema atacant àrees protegides.
- Elaborar un informe amb les conclusions.

C2: Aplicar els procediments d'anàlisi de la informació i contenció de l'atac davant d'una incidència detectada.

CE2.1 Analitzar la informació dels sistemes de detecció d'intrusos, extraient-ne els esdeveniments rellevants per a la seguretat.

CE2.2 Analitzar els indicis d'intrusió, indicant els condicionants necessaris perquè l'amenaça pugui materialitzar-se.

CE2.3 Classificar els elements de les alertes del sistema de detecció d'intrusions, establint les possibles correlacions existents entre ells i distingint les alertes per temps i nivells de seguretat.

CE2.4 A partir d'un supòsit pràctic en què es duen a terme intents d'intrusió al sistema informàtic:

- Recopilar les alertes dels sistemes de detecció d'intrusions.
- Relacionar els esdeveniments recollits pels sistemes de detecció d'intrusions.
- Determinar les alertes significatives.
- Elaborar l'informe corresponent indicant les possibles intrusions i el risc associat per a la seguretat del sistema informàtic de l'organització.

CE2.5 Establir processos d'actualització de les eines de detecció d'intrusos per garantir-ne la funcionalitat segons les especificacions dels fabricants.

C3: Analitzar l'abast dels danys i determinar els processos de recuperació davant d'una incidència detectada.

CE3.1 Descriure les fases del pla d'actuació davant d'incidents de seguretat i descriure els objectius de cada fase.

CE3.2 Indicar les fases de l'anàlisi forense d'equips informàtics i descriure els objectius de cada fase.

CE3.3 Classificar els tipus d'evidències de l'anàlisi forense de sistemes, i indicar-ne les característiques i els mètodes de recol·lecció i anàlisi.

CE3.4 Descriure les diferents tècniques per a l'anàlisi de programes maliciosos i indicar-ne casos d'ús.

CE3.5 En un supòsit pràctic en què s'ha produït una intrusió en un sistema informàtic:

- Dur a terme la recollida d'evidències volàtils.
- Dur a terme la recollida d'evidències no volàtils.
- Elaborar l'anàlisi preliminar de les evidències.
- Elaborar l'anàlisi temporal d'activitat del sistema de fitxers.
- Elaborar l'informe final, recollint les evidències trobades, les possibles vulnerabilitats utilitzades per a la intrusió i l'activitat realitzada per l'intrús que s'ha detectat al sistema.

CE3.6 Estandarditzar mètodes de recuperació de desastres d'equips informàtics davant de la detecció d'intrusions.

Sumari

2. **Implantació i posada en producció de sistemes IDS/IPS.**
   - Anàlisi prèvia dels serveis, protocols, zones i equips que l'organització utilitza per als seus processos de negoci.
   - Definició de polítiques de tall d'intents d'intrusió en els IDS/IPS.
   - Anàlisi dels esdeveniments registrats per l'IDS/IPS per determinar falsos positius i caracteritzar-los en les polítiques de tall de l'IDS/IPS.
   - Relació dels registres d'auditoria de l'IDS/IPS necessaris per monitorar i supervisar el funcionament correcte i els esdeveniments d'intents d'intrusió.
   - Establiment dels nivells requerits d'actualització, monitoratge i proves de l'IDS/IPS.

3. **Control de codi maliciós.**
   - Sistemes de detecció i contenció de codi maliciós.
   - Relació dels diferents tipus d'eines de control de codi maliciós en funció de la topologia de la instal·lació i les vies d'infecció que s'han de controlar.
   - Criteris de seguretat per a la configuració de les eines de protecció contra codi maliciós.
   - Determinació dels requeriments i les tècniques d'actualització de les eines de protecció contra codi maliciós.
   - Relació dels registres d'auditoria de les eines de protecció davant de codi maliciós necessaris per monitorar i supervisar el funcionament correcte i els esdeveniments de seguretat.
   - Establiment del monitoratge i proves de les eines de protecció contra codi maliciós.
   - Anàlisi dels programes maliciosos mitjançant desassembladors i entorns d'execució controlada.

4. **Resposta davant d'incidents de seguretat.**
   - Procediment de recollida d'informació relacionada amb incidents de seguretat.
   - Exposició de les diferents tècniques i eines utilitzades per a l'anàlisi i correlació d'informació i esdeveniments de seguretat.
   - Procés de verificació de la intrusió.
   - Naturalesa i funcions dels organismes de gestió d'incidents de tipus CERT nacionals i internacionals.

5. **Procés de notificació i gestió d'intents d'intrusió.**
   - Establiment de responsabilitats en el procés de notificació i gestió d'intents d'intrusió o infeccions.
   - Categorització dels incidents derivats d'intents d'intrusió o infeccions en funció del seu impacte potencial.
   - Criteris per a la determinació de les evidències objectives en què es fonamentarà la gestió de l'incident.
   - Establiment del procés de detecció i registre d'incidents derivats d'intents d'intrusió o infeccions.
   - Guia per a la classificació i l'anàlisi inicial de l'intent d'intrusió o infecció, amb càlcul de l'impacte previsible.
   - Establiment del nivell d'intervenció requerit en funció de l'impacte previsible.
   - Guia per a la investigació i el diagnòstic de l'incident d'intent d'intrusió o infeccions.
   - Establiment del procés de resolució i recuperació dels sistemes després d'un incident derivat d'un intent d'intrusió o infecció.
   - Procés per a la comunicació de l'incident a tercers, si escau.
   - Establiment del procés de tancament de l'incident i els registres necessaris per documentar l'històric de l'incident.

6. Anàlisi forense informàtic.

- Conceptes generals i objectius de l'anàlisi forense.
- Exposició del principi de Lockard.
- Guia per a la recollida d'evidències electròniques.
  - Evidències volàtils i no volàtils.
  - Etiquetatge d'evidències.
  - Cadena de custòdia.
  - Fitxers i directoris amagats.
  - Informació amagada del sistema.
  - Recuperació de fitxers esborrats.
- Guia per a l'anàlisi de les evidències electròniques recollides, inclosos l'estudi dels fitxers i els directoris amagats, la informació amagada del sistema i la recuperació dels fitxers esborrats.
- Guia per a la selecció de les eines d'anàlisi forense.

Orientacions metodològiques

Formació a distància:

Mòdul formatiu	Nombre total d'hores del mòdul	Nombre màxim d'hores susceptibles de formació a distància
Mòdul formatiu - MF0488_3	90	40

Criteris d'accés per als alumnes

Són els que estableix l'article 4 del reial decret que regula el certificat de professionalitat de la família professional que acompanya aquest annex.

MÒDUL FORMATIU 4

Denominació: SISTEMES SEGURS D'ACCÉS I TRANSMISSIÓ DE DADES

Codi: MF0489_3

Nivell de qualificació professional: 3

Associat a la unitat de competència:

UC0489_3: Dissenyar i implementar sistemes segurs d'accés i transmissió de dades.

Durada: 60 hores

Capacitats i criteris d'avaluació

C1: Avaluar les tècniques de xifratge existents per escollir la necessària en funció dels requisits de seguretat exigits.

CE1.1 Descriure les diferències entre els algoritmes de xifratge de clau privada i els de clau pública i indicar-ne els diferents usos.

CE1.2 Identificar els diferents modes de xifratge i descriure'n les característiques principals.

CE1.3 Classificar els diferents algoritmes de clau privada i descriure'n les fases d'execució.

CE1.4 Classificar els diferents algoritmes de clau pública i descriure'n les fases d'execució.

CE1.5 Identificar els diferents protocols d'intercanvi de claus i descriure'n el

funcionament.

C2: Implantar serveis i tècniques criptogràfiques als serveis que ho requereixin segons les especificacions de seguretat informàtica.

CE2.1 Justificar la necessitat d'utilitzar tècniques criptogràfiques a les comunicacions entre sistemes informàtics en funció dels canals utilitzats.

CE2.2 Definir les tècniques de xifratge per connectar de manera segura dues xarxes, i descriure les funcionalitats i els requisits necessaris.

CE2.3 Definir les tècniques emprades per connectar de manera segura dos equips (túnels SSL i SSH), i descriure les funcionalitats i els requisits necessaris.

CE2.4 En un cas pràctic en què es vol establir una comunicació segura entre dos sistemes informàtics:

- Analitzar els requisits de seguretat de l'arquitectura de comunicacions proposada.
- Indicar la solució més indicada, justificant la selecció.
- Instal·lar els serveis de VPN i IPSec per connectar xarxes.
- Instal·lar els serveis de túnels SSL o SSH per connectar equips distants.

C3: Utilitzar sistemes de certificats digitals a les comunicacions que requereixin integritat i confidencialitat segons les especificacions de seguretat.

CE3.1 Identificar els atributs utilitzats als certificats digitals per a servidors, i descriure'n els valors i la funció.

CE3.2 Descriure els modes d'ús dels certificats digitals i associar-los a les especificacions de seguretat: confidencialitat, integritat i accessibilitat.

CE3.3 Descriure l'estructura d'un sistema de segellat digital i indicar les funcions dels elements que la integren.

C4: Dissenyar i implantar serveis de certificació digital segons les necessitats d'explotació i de seguretat informàtica.

CE4.1 Descriure l'estructura de la infraestructura de clau pública i indicar les funcions dels elements que la integren.

CE4.2 Descriure els serveis i les obligacions de l'autoritat de certificació, i relacionar-los amb la política de certificat i la declaració de pràctiques de certificació.

CE4.3 Identificar els atributs obligatoris i els opcionals d'un certificat digital, i descriure'n l'ús habitual.

CE4.4 Descriure l'estructura d'una infraestructura de gestió de privilegis i indicar les funcions dels elements que la integren.

CE4.5 Determinar els camps dels certificats d'atributs i descriure'n l'ús habitual i la relació existent amb els certificats digitals.

CE4.6 En un cas pràctic en què es vol establir un sistema de certificació per a un sistema informàtic:

- Dissenyar una infraestructura de clau pública en funció de les especificacions.
- Justificar la jerarquia d'autoritats de certificació dissenyada.
- Emetre els certificats seguint els procediments indicats a la declaració de pràctiques de certificació.

Sumari

1. Criptografia.

- Perspectiva històrica i objectius de la criptografia.
- Teoria de la informació.
- Propietats de la seguretat que es poden controlar mitjançant l'aplicació de la criptografia: confidencialitat, integritat, autenticitat, no-repudi, imputabilitat i

segellat de temps.
- Elements fonamentals de la criptografia de clau privada i de clau pública.
- Característiques i atributs dels certificats digitals.
- Identificació i descripció del funcionament dels protocols d'intercanvi de claus més utilitzats.
- Algorismes criptogràfics més utilitzats.
- Elements dels certificats digitals, formats comunament acceptats i ús.
- Elements fonamentals de les funcions resum i criteris d'ús.
- Requeriments legals inclosos a la Llei 59/2003, de 19 de desembre, de signatura electrònica.
- Elements fonamentals de la signatura digital, els diferents tipus de signatura i criteris d'ús.
- Criteris per a l'ús de tècniques de xifratge de flux i de bloc.
- Protocols d'intercanvi de claus.
- Ús d'eines de xifratge de tipus PGP, GPG o CryptoLoop.

2. Aplicació d'una infraestructura de clau pública (PKI).
- Identificació dels components d'una PKI i model de relacions.
- Autoritat de certificació i elements.
- Política de certificat i declaració de pràctiques de certificació (CPS).
- Llista de certificats revocats (CRL).
- Funcionament de les sol·licituds de signatura de certificats (CSR).
- Infraestructura de gestió de privilegis (PMI).
- Camps de certificats d'atributs, incloses la descripció dels usos habituals i la relació amb els certificats digitals.
- Aplicacions que es fonamenten en l'existència d'una PKI.

3. Comunicacions segures.
- Definició, finalitat i funcionalitat de les xarxes privades virtuals.
- Protocol IPSec.
- Protocols SSL i SSH.
- Sistemes SSL VPN.
- Túnels xifrats.
- Avantatges i inconvenients de les diferents alternatives per a la implantació de la tecnologia de VPN.

Orientacions metodològiques

Formació a distància:

Mòdul formatiu	Nombre total d'hores del mòdul	Nombre màxim d'hores susceptibles de formació a distància
Mòdul formatiu - MF0489_3	60	40

Criteris d'accés per als alumnes

Són els que estableix l'article 4 del reial decret que regula el certificat de professionalitat de la família professional que acompanya aquest annex.

MÒDUL FORMATIU 5

Denominació: GESTIÓ DE SERVEIS AL SISTEMA INFORMÀTIC

Codi: MF0490_3

Nivell de qualificació professional: 3

Associat a la unitat de competència:

UC0490_3: Gestionar serveis al sistema informàtic.

Durada: 90 hores

Capacitats i criteris d'avaluació

C1: Analitzar els processos del sistema a fi d'assegurar un rendiment adequat segons els paràmetres especificats al pla d'explotació.

CE1.1 Identificar els processos del sistema i els paràmetres que els caracteritzen (processos pare, estat del procés, consum de recursos, prioritats i usuaris afectats, entre d'altres) per determinar-ne la influència en el rendiment del sistema.

CE1.2 Descriure les eines proporcionades pel sistema per a la gestió de processos a fi de permetre la intervenció en el rendiment general del sistema.

CE1.3 Explicar tècniques de monitoratge i eines destinades a avaluar el rendiment del sistema.

CE1.4 En un supòsit pràctic en què es disposa d'un sistema informàtic amb una càrrega de processos degudament caracteritzada:

- Utilitzar les eines del sistema per identificar quants processos actius existeixen i les característiques particulars d'algun d'ells.
- Dur a terme les operacions d'activació, desactivació i modificació de prioritat, entre d'altres, amb un procés en què s'utilitzin les eines del sistema.
- Monitorar el rendiment del sistema mitjançant eines específiques i definir alarmes que indiquin situacions de risc.

C2: Aplicar procediments d'administració a dispositius d'emmagatzematge per oferir a l'usuari un sistema de registre de la informació íntegre, segur i disponible.

CE2.1 Identificar els diferents sistemes de fitxers que es poden utilitzar en un dispositiu d'emmagatzematge determinat per optimitzar els processos de registre i l'accés a aquests sistemes.

CE2.2 Explicar les característiques dels sistemes de fitxers en funció dels dispositius d'emmagatzematge i els sistemes operatius utilitzats.

CE2.3 Descriure l'estructura general d'emmagatzematge al sistema informàtic i associar els dispositius amb els diferents sistemes de fitxers existents.

CE2.4 En un supòsit pràctic en què es disposa d'un sistema d'emmagatzematge de la informació amb diversos dispositius:

- Efectuar les particions, quan calgui, i generar la infraestructura dels sistemes de fitxers que cal instal·lar en cada dispositiu.
- Implementar l'estructura general d'emmagatzematge integrant tots els dispositius i els sistemes de fitxers corresponents.
- Documentar els requeriments i les restriccions de cada sistema de fitxers implantat.

C3: Administrar l'accés al sistema i als recursos per verificar-ne l'ús adequat i segur.

CE3.1 Identificar les possibilitats d'accés al sistema, distingint els accessos remots dels accessos locals.

CE3.2 Descriure les eines que s'utilitzen en la gestió de permisos a usuaris per a l'ús dels recursos del sistema.

CE3.3 En un supòsit pràctic en què es disposa del dret d'administració d'usuaris:

- Identificar els possibles accessos d'un usuari al sistema.
- Modificar els permisos d'ús d'un recurs del sistema a un usuari.
- Definir limitacions d'ús d'un recurs del sistema als usuaris.

C4: Avaluar l'ús i el rendiment dels serveis de comunicacions per mantenir-los dins dels paràmetres especificats.

CE4.1 Explicar els paràmetres de configuració i funcionament dels dispositius de comunicacions per garantir-ne la funcionalitat dins del sistema.

CE4.2 Relacionar els serveis de comunicacions actius al sistema amb els dispositius que utilitzen a fi d'analitzar-ne i avaluar-ne el rendiment.

CE4.3 En un supòsit pràctic amb un sistema informàtic connectat a l'exterior per mitjà de diverses línies de comunicacions:

- Identificar els dispositius de comunicacions i descriure'n les característiques.
- Verificar l'estat dels serveis de comunicacions.
- Avaluar el rendiment dels serveis de comunicacions.
- Detectar i documentar les incidències produïdes al sistema.

Sumari

1. Gestió de la seguretat i les normatives.

- Norma ISO 27002: Codi de bones pràctiques per a la gestió de la seguretat de la informació.
- Metodologia ITIL: Biblioteca d'infraestructures de les tecnologies de la informació.
- Llei orgànica de protecció de dades de caràcter personal.
- Normatives més utilitzades per a la gestió de la seguretat física.

2. Anàlisi dels processos de sistemes.

- Identificació de processos de negoci suportats per sistemes d'informació.
- Característiques fonamentals dels processos electrònics.
  - Estats d'un procés.
  - Maneig dels senyals, administració i canvis en les prioritats.
- Determinació dels sistemes d'informació que suporten els processos de negoci, i actius i serveis utilitzats.
- Anàlisi de les funcionalitats de sistema operatiu per al monitoratge dels processos i serveis.
- Tècniques utilitzades per gestionar el consum de recursos.

3. Demostració de sistemes d'emmagatzematge.

- Tipus de dispositius d'emmagatzematge més freqüents.
- Característiques dels sistemes de fitxers disponibles.
- Organització i estructura general d'emmagatzematge.
- Eines del sistema per a la gestió de dispositius d'emmagatzematge.

4. Ús de mètriques i indicadors de monitoratge de rendiment de sistemes.

- Criteris per establir el marc general d'ús de mètriques i indicadors per al monitoratge dels sistemes d'informació.
- Identificació dels objectes per als quals és necessari obtenir indicadors.
- Aspectes que cal definir per a la selecció i definició d'indicadors.
- Establiment dels llindars de rendiment dels sistemes d'informació.
- Recollida i anàlisi de les dades aportades pels indicadors.
- Consolidació d'indicadors amb un quadre de comandaments de rendiment de sistemes d'informació unificat.

5. Confecció del procés de monitoratge de sistemes i comunicacions.

- Identificació dels dispositius de comunicacions.
- Anàlisi dels protocols i serveis de comunicacions.
- Principals paràmetres de configuració i funcionament dels equips de comunicacions.
- Processos de monitoratge i resposta.
- Eines de monitoratge d'ús de ports i serveis de tipus Sniffer.
- Eines de monitoratge de sistemes i serveis de tipus Hobbit, Nagios o Cacti.
- Sistemes de gestió d'informació i esdeveniments de seguretat (SIM/SEM).
- Gestió de registres d'elements de xarxa i filtratge (encaminador, commutador, tallafoc, IDS/IPS, etc.).

6. Selecció del sistema de registre en funció dels requeriments de l'organització.

- Determinació del nivell de registres necessaris, els períodes de retenció i les necessitats d'emmagatzematge.
- Anàlisi dels requeriments legals amb referència al registre.
- Selecció de mesures de salvaguarda per cobrir els requeriments de seguretat del sistema de registres.
- Assignació de responsabilitats per a la gestió del registre.
- Alternatives d'emmagatzematge per als registres dels sistemes i característiques de rendiment, escalabilitat, confidencialitat, integritat i disponibilitat.
- Guia per a la selecció del sistema d'emmagatzematge i custòdia de registres.

7. Administració del control d'accessos adequats dels sistemes d'informació.

- Anàlisi dels requeriments d'accés dels diferents sistemes d'informació i recursos compartits.
- Principis comunament acceptats per al control d'accessos i dels diferents tipus d'accés locals i remots.
- Requeriments legals en referència al control d'accessos i assignació de privilegis.
- Perfils d'accés en relació amb els rols funcionals del personal de l'organització.
- Eines de directori actiu i servidors LDAP en general.
- Eines de sistemes de gestió d'identitats i autoritzacions (IAM).
- Eines de sistemes d'inici de sessió únic (SSO).

Orientacions metodològiques

Formació a distància:

Mòdul formatiu	Nombre total d'hores del mòdul	Nombre màxim d'hores susceptibles de formació a distància
Mòdul formatiu - MF0490_3	90	40

Criteris d'accés per als alumnes

Són els que estableix l'article 4 del reial decret que regula el certificat de professionalitat de la família professional que acompanya aquest annex.

MÒDUL DE PRÀCTIQUES PROFESSIONALS NO LABORALS DE SEGURETAT INFORMÀTICA

Codi: MP0175

Durada: 80 hores

Capacitats i criteris d'avaluació

C1: Proporcionar suport tècnic en matèria de seguretat.
CE1.1. Proporcionar assistència tècnica en el disseny i la configuració de solucions de seguretat.
CE1.2. Donar suport a altres àrees en les tasques de disseny i reenginyeria de processos per aportar la visió de seguretat.
CE1.3. Actuar com a enllaç entre les diferents àrees de la companyia per coordinar mesures de seguretat multidepartamentals.
CE1.4. Analitzar les regles específiques desenvolupades per les àrees tècniques específiques per a les eines de seguretat corporatives.
CE1.5. Coordinar l'ús de les eines de xifratge i la gestió de les claus.
CE1.6. Donar suport tècnic als comitès de direcció que calgui.
CE1.7. Avaluar i mantenir-se permanentment informat dels errors, informes, notícies, butlletins, etc. de seguretat rebuts i oferir el primer nivell de suport i distribució.
CE1.8. Desenvolupar les polítiques i els procediments operatius en matèria de seguretat de la informació i donar suport a les diferents àrees de l'organització per a la posada en producció.

C2: Verificar l'aplicació correcta de les mesures de seguretat.
CE2.1. Dur a terme les verificacions necessàries per determinar el grau de vulnerabilitat de les diferents plataformes tecnològiques, així com la resta de revisions periòdiques de seguretat dels sistemes d'informació.
CE2.2. Mantenir actualitzat l'anàlisi de riscos de l'organització.
CE2.3. Coordinar les auditories tècniques de seguretat.

C3: Participar en els processos de treball de l'empresa d'acord amb les normes i instruccions establertes al centre de treball.
CE3.1 Comportar-se de manera responsable tant en les relacions humanes com en les laborals.
CE3.2 Respectar els procediments i les normes del centre de treball.
CE3.3 Emprendre amb diligència les tasques segons les instruccions rebudes i intentar que s'adeqüin al ritme de treball de l'empresa.
CE3.4 Integrar-se en els processos de producció del centre de treball.
CE3.5 Fer ús dels canals de comunicació establerts.
CE3.6 Respectar en tot moment les mesures de prevenció de riscos, salut laboral i protecció del medi ambient.

Sumari

1. Revisió de la situació de la seguretat de la informació.
- Revisió de les normes internes de seguretat.
- Revisió de la gestió d'usuaris, privilegis i política de contrasenyes.
- Revisió de les còpies de seguretat.
- Revisió de les incidències produïdes.
- Revisió de la situació respecte a la protecció contra codi maliciós.
- Revisió de la seguretat de les xarxes de dades.
- Revisió de la seguretat de servidors i llocs de treball.
- Revisió de la seguretat física, el subministrament elèctric, la climatització i la protecció d'incendis, segons calgui.

2. **Configuració de regles relacionades amb la seguretat.**
   - Configuració de la seguretat dels encaminadors.
   - Configuració de la seguretat dels commutadors.
   - Configuració de la seguretat dels tallafocs.
   - Configuració de la seguretat dels sistemes de detecció d'intrusos.
   - Configuració de la seguretat dels antivirus.

3. **Comunicació dels aspectes relacionats amb la seguretat.**
   - Establiment de canals per mantenir l'organització actualitzada en matèria de seguretat.
   - Establiment dels canals interns per coordinar la seguretat entre els departaments de l'organització.

4. **Monitoratge de la seguretat.**
   - Monitoratge de les comunicacions.
   - Monitoratge del rendiment dels sistemes.

5. **Aplicació de la normativa i metodologia de seguretat.**
   - Aplicació de codis de bones pràctiques de seguretat a la gestió diària dels sistemes d'informació.
   - Integració dels requeriments de seguretat en els processos de negoci de l'organització.

6. **Integració i comunicació al centre de treball.**
   - Comportament responsable al centre de treball.
   - Respecte dels procediments i les normes del centre de treball.
   - Interpretació i execució amb diligència de les instruccions rebudes.
   - Reconeixement del procés productiu de l'organització.
   - Ús dels canals de comunicació establerts al centre de treball.
   - Adequació al ritme de treball de l'empresa.
   - Seguiment de les normatives de prevenció de riscos, salut laboral i protecció del medi ambient.

IV. PRESCRIPCIONS DELS FORMADORS

Mòduls formatius	Acreditació requerida	*Experiència professional en l'àmbit de la unitat de	
		Si es disposa d'acreditació	Si no es disposa d'acreditació
MF0486_3: Assegurar equips informàtics.	• Llicenciat/ada, enginyer/a, arquitecte/a o títol de grau corresponent o altres títols equivalents. • Diplomat/ada, enginyer/a tècnic/a, arquitecte/a tècnic/a o títol de grau corresponent o altres títols equivalents.	1 any	3 anys
MF0487_3: Auditoria de seguretat informàtica.	• Llicenciat/ada, enginyer/a, arquitecte/a o títol de grau corresponent o altres títols equivalents. • Diplomat/ada, enginyer/a tècnic/a, arquitecte/a tècnic/a o títol de grau corresponent o altres títols equivalents.	2 anys	4 anys
MF0488_3: Gestió d'incidents de seguretat informàtica.	• Llicenciat/ada, enginyer/a, arquitecte/a o títol de grau corresponent o altres títols equivalents. • Diplomat/ada, enginyer/a tècnic/a, arquitecte/a tècnic/a o títol de grau corresponent o altres títols equivalents.	1 any	3 anys
MF0489_3: Sistemes segurs d'accés i transmissió de dades.	• Llicenciat/ada, enginyer/a, arquitecte/a o títol de grau corresponent o altres títols equivalents. • Diplomat/ada, enginyer/a tècnic/a, arquitecte/a tècnic/a o títol de grau corresponent o altres títols equivalents.	1 any	3 anys
MF0490_3: Gestió de serveis al sistema informàtic.	• Llicenciat/ada, enginyer/a, arquitecte/a o títol de grau corresponent o altres títols equivalents. • Diplomat/ada, enginyer/a tècnic/a, arquitecte/a tècnic/a o títol de grau corresponent o altres títols equivalents.	2 anys	4 anys

***** En els últims tres anys.

V. REQUISITS MÍNIMS D'ESPAIS, INSTAL·LACIONS I EQUIPAMENT

Espai formatiu	Superfície m^2 15 alumnes	Superfície m^2 25 alumnes
Aula de gestió	45	60

Espai formatiu	M1	M2	M3	M4	M5
Aula de gestió	X	X	X	X	X

Espai formatiu	Equipament
Aula de gestió	- Equips audiovisuals - Ordinadors instal·lats en xarxa, canó amb projecció i Internet. - Programari específic de l'especialitat. - Pissarres per escriure amb retolador. - Paperògraf. - Material d'aula. - Taula i cadira per al formador. - Taules i cadires per als alumnes.

No s'ha d'interpretar que els diversos espais formatius identificats s'hagin de diferenciar necessàriament mitjançant tancaments.

Les instal·lacions i els equipaments han de complir la normativa industrial i higienicosanitària corresponent, i han de respondre a mesures d'accessibilitat universal i seguretat dels participants.

El nombre d'utensilis, màquines i eines que s'especifiquen a l'equipament dels espais formatius ha de ser suficient per a 15 alumnes com a mínim, i s'ha d'augmentar en cas d'ampliar-se el nombre d'alumnes.

Quan la formació s'adreci a persones amb discapacitat, caldrà fer les adaptacions i els ajustos necessaris per assegurar que hi participin en condicions d'igualtat.