

ANNEX XI

I. IDENTIFICACIÓ DEL CERTIFICAT DE PROFESSIONALITAT

Denominació: Gestió de sistemes informàtics

Codi: IFCT0510

Família professional: Informàtica i comunicacions

Àrea professional: Sistemes i telemàtica

Nivell de qualificació professional: 3

Qualificació professional de referència:

IFC152_3 Gestió de sistemes informàtics (RD 1087/2005, de 16 de setembre)

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

UC0484_3 Administrar els dispositius de maquinari del sistema.

UC0485_3 Instal·lar, configurar i administrar el programari de base i d'aplicació del sistema.

UC0486_3 Assegurar els equips informàtics.

Competència general:

Configurar, administrar i mantenir un sistema informàtic pel que fa al maquinari i al programari, garantint la disponibilitat, el rendiment òptim, la funcionalitat i la integritat dels serveis i recursos del sistema.

Entorn professional:

Àmbit professional:

Desenvolupa la seva activitat professional en empreses o entitats de naturalesa pública o privada de qualsevol mida en l'àrea de sistemes del departament d'informàtica.

Sectors productius:

Se situa en tots els sectors del teixit empresarial, atesa la seva característica de transsectorialitat com a conseqüència de la necessitat de les organitzacions de tractar i administrar la seva informació, independentment del sector al qual pertanyin. També està present en els següents tipus d'empreses:

Empreses o entitats de qualsevol mida que utilitzen sistemes informàtics per gestionar-se i que poden estar emmarcades en qualsevol sector productiu.

Empreses dedicades a la comercialització d'equips informàtics.

Empreses que presten serveis d'assistència tècnica informàtica.

Ocupacions o llocs de treball relacionats:

2721.1018 Administrador/a de sistemes de xarxes.
Administrador/a de sistemes.

Responsable d'informàtica.

Durada de la formació associada: 500 hores

Relació de mòduls formatius i unitats formatives:

MF0484_3: Administració del maquinari d'un sistema informàtic (120 hores).

- UF1891: Dimensionar, instal·lar i optimitzar el maquinari (70 hores).
- UF1892: Gestionar el creixement i les condicions ambientals (50 hores).

MF0485_3: Administració del programari d'un sistema informàtic (210 hores).

- UF1893: Instal·lació i parametrització del programari (90 hores).
- UF1894: Manteniment del programari (70 hores).
- UF1895: Auditories i continuïtat del negoci (50 hores).

MF0486_3: (Transversal) Seguretat en equips informàtics (90 hores).

MP0398: Mòdul de pràctiques professionals no laborals de gestió de sistemes informàtics (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: ADMINISTRACIÓ DEL MAQUINARI D'UN SISTEMA INFORMÀTIC

Codi: MF0484_3

Nivell de qualificació professional: 3

Associat a la unitat de competència:

UC0484_3: Administrar els dispositius de maquinari del sistema.

Durada: 120 hores

UNITAT FORMATIVA 1

Denominació: DIMENSIONAR, INSTAL·LAR I OPTIMITZAR EL MAQUINARI

Codi: UF1891

Durada: 70 hores

Referent de competència: Aquesta unitat formativa es correspon amb l'RP1, l'RP2 i l'RP3.

Capacitats i criteris d'avaluació

C1: Identificar els components de maquinari del sistema, distingir-ne les característiques i detallar els paràmetres i els procediments d'instal·lació.

CE1.1 Analitzar i explicar els fonaments de l'arquitectura física d'un sistema informàtic i descriure les diferents parts que el componen.

CE1.2 Enumerar i definir les funcions de cadascun dels components de maquinari d'un sistema informàtic i explicar-ne les característiques.

CE1.3 Classificar segons la tipologia els components de maquinari d'un sistema informàtic, tenint en compte les característiques, la utilitat i els propòsits de cada component.

CE1.4 Detallar les característiques tècniques i els procediments d'instal·lació i configuració dels components de maquinari d'un sistema informàtic segons les especificacions de funcionalitats donades.

CE1.5 Distingir i explicar els tipus de dispositius físics i les tècniques de comunicació possibles entre els diferents components de maquinari d'un sistema informàtic, i descriure'n la tipologia i les característiques principals.

CE1.6 Definir i classificar els diferents tipus de dispositius perifèrics segons el seu propòsit, i descriure les diferents tècniques de comunicació utilitzades i les tecnologies disponibles en controladors d'entrada/sortida.

CE1.7 Identificar i classificar els diferents dispositius físics disponibles per connectar el sistema a través d'una xarxa de comunicacions.

CE1.8 A partir d'un supòsit pràctic d'identificació i registre de dispositius de maquinari:

- Classificar un conjunt de dispositius de maquinari segons diferents criteris: propòsit, idoneïtat per a un sistema i compatibilitat, entre d'altres.
- Utilitzar eines d'inventari i registrar de manera exhaustiva les característiques dels dispositius de maquinari en estudi.
- Documentar la instal·lació dels dispositius físics i detallar els procediments, les incidències més freqüents i els paràmetres utilitzats.

C2: Seleccionar i aplicar els procediments i les tècniques de monitoratge del rendiment dels dispositius per ajustar els paràmetres de configuració i assegurar l'absència de conflictes.

CE2.1 Enumerar i definir les mètriques de rendiment comunament utilitzades per mesurar el rendiment d'un sistema.

CE2.2 Caracteritzar i analitzar les tècniques i els procediments principals de monitoratge utilitzats per mesurar les prestacions d'un sistema.

CE2.3 Aplicar les tècniques i eines seleccionades per aconseguir un rendiment òptim, determinar l'estat del sistema analitzant els resultats dels mesuraments del rendiment i indicar si aquest està saturat, equilibrat o infrautilitzat.

CE2.4 Representar gràficament el rendiment del sistema segons les dades obtingudes del monitoratge.

CE2.5 Analitzar les alarmes obtingudes en el monitoratge, descriure els principals problemes de configuració relatius a dispositius de maquinari coneguts i explicar les solucions més comunes.

CE2.6 En una sèrie de supòsits pràctics de monitoratge i ajust de sistemes:

- Seleccionar les mètriques del rendiment que cal utilitzar segons les necessitats del sistema.
- Obtenir mesuraments del rendiment del sistema utilitzant amb destresa les eines necessàries.
- Analitzar els mesuraments obtinguts, documentar-los i presentar-los per facilitar la presa de decisions sobre el sistema.
- Configurar els paràmetres del sistema necessaris perquè es compleixin els requisits de rendiment.

- Reconfigurar el sistema en funció de les alarmes obtingudes en els mesuraments.
- Indicar i documentar les limitacions existents en intentar millorar les prestacions d'un sistema.

C3: Integrar i implantar en el sistema informàtic dispositius de maquinari que garanteixin la continuïtat en la prestació de serveis i la seguretat de les dades.

CE3.1 Identificar les diferents solucions de maquinari disponibles per assegurar la continuïtat del funcionament del sistema, i descriure'n les principals característiques i configuracions

CE3.2 Definir les diferents solucions de maquinari disponibles per assegurar la recuperació del sistema davant de situacions imprevistes, i descriure'n les principals característiques i configuracions.

CE3.3 Identificar les polítiques de seguretat i protecció de dades i la seva relació amb la recuperació i la continuïtat dels serveis i les aplicacions segons la normativa de seguretat informàtica.

CE3.4 En un supòsit pràctic, implementar i configurar solucions per assegurar la continuïtat del funcionament del sistema, atesos uns requisits previs:

- Analitzar el sistema per determinar les necessitats i la disposició de sistemes d'alimentació ininterrompuda.
- Instal·lar adequadament les unitats d'alimentació i els estabilitzadors de tensió respectant les característiques tècniques dels aparells i complint les normes relatives a la seguretat al lloc de treball.
- Parametritzar i monitorar els dispositius instal·lats i adequar-los al sistema per aconseguir una compatibilitat total i un funcionament, una gestió i un control òptims.
- Elaborar un pla d'intervenció i activació de possibles mecanismes alternatius.
- Documentar la instal·lació dels dispositius físics i detallar els procediments, les incidències més freqüents i els paràmetres utilitzats.

CE3.5 En diversos supòsits pràctics d'implementació i configuració de solucions per a la recuperació del sistema davant de situacions imprevistes, amb uns requisits de seguretat que cal complir:

- Instal·lar i configurar un servidor local de seguretat que garanteixi la recuperació immediata del funcionament en casos de fallada del servidor principal.
- Instal·lar i configurar solucions d'agrupacions de discos per augmentar la tolerància a errors del sistema.
- Instal·lar i configurar un sistema de clústers segons la seva tipologia per augmentar la fiabilitat i productivitat del sistema.
- Elaborar un pla d'intervenció i activació de possibles mecanismes alternatius.
- Davant d'una possible avaria, localitzar els dispositius de maquinari responsables i establir els procediments necessaris per a la reparació o substitució.
- Configurar adequadament els dispositius substituïts seguint els passos establerts en el pla d'intervenció definit.
- Documentar la instal·lació dels dispositius físics i detallar els procediments, les incidències més freqüents i els paràmetres utilitzats.
- Documentar de manera exhaustiva els passos que cal seguir per a la recuperació del sistema un cop s'ha produït una situació imprevista.
- Planificar i dur a terme proves per verificar la idoneïtat de les solucions implementades, i efectuar les millores i els ajustos necessaris fins a aconseguir un funcionament òptim.

Sumari

1. Classificar i inventariar el maquinari.

- Identificar i classificar el maquinari.
 - Conèixer els diferents tipus de maquinari segons la finalitat.
 - Conèixer l'arquitectura de servidors i PC.
 - Diferenciar els components i identificar-ne les funcions.
 - Classificar els components segons característiques, utilitat i propòsit.
 - Instal·lar i substituir components en un sistema informàtic tenint en compte la documentació del fabricant i les normes de l'organització.
- Establir la connectivitat del maquinari.
 - Distingir els diferents busos de comunicació en un sistema informàtic.
 - Distingir els diferents tipus de connectivitat amb els dispositius perifèrics.
 - Identificar els diferents tipus de connectivitat i tecnologies de connectivitat entre els elements de maquinari que componen l'arquitectura d'una plataforma per a la prestació d'un servei.
 - Establir la connectivitat entre els PC o els servidors.
 - Connectar els servidors amb equips d'emmagatzematge extern.
 - Dissenyar la connexió amb equips de còpia de seguretat.
 - Establir la connexió amb Internet.
 - Seleccionar i instal·lar el controlador d'entrada/sortida més adequat segons la finalitat perseguida.
- Documentar i inventariar el maquinari.
 - Enumerar els equips i detallar-ne els components, l'estat i la ubicació.
 - Documentar les configuracions i parametritzacions.
 - Documentar les connectivitats.
 - Etiquetar el maquinari.
- Mantenir l'inventari.
 - Actualitzar-lo amb altes, baixes i modificacions.
 - Auditar l'inventari.

2. Monitorar el rendiment.

- Dissenyar el monitoratge.
 - Distingir els diferents tipus de monitoratge segons la seva finalitat.
Dissenyar el monitoratge extern per garantir la disponibilitat del sistema i dissenyar el monitoratge per a la gestió de la capacitat del sistema.
 - Seleccionar tècniques o eines en funció de les característiques del maquinari.
 - Definir els paràmetres que cal monitorar. Conèixer els paràmetres habituals que cal monitorar.
 - Monitorar la CPU, la RAM i els discos del sistema.
 - Monitorar la connectivitat.
 - Monitorar els serveis.
 - Seleccionar els elements que cal monitorar i els llindars d'avís segons els procediments definits per l'organització.
 - Configurar alertes davant de la indisponibilitat del servei i alertes per garantir una gestió correcta de la capacitat segons els procediments definits a l'organització.
- Monitorar el sistema.
 - Obtenir estadístiques de rendiment.
 - Interpretar correctament els informes gràfics d'ús.
- Diagnosticar l'estat del sistema.
 - Analitzar el rendiment: comparar els valors obtinguts amb l'historial d'ús del sistema i localitzar-hi colls d'ampolla.
 - Proposar millores.

- Avaluar la viabilitat de l'ampliació o la substitució dels elements de maquinari que causen els colls d'ampolla per altres de rendiment superior que compleixin la mateixa funció.
- Avaluar alternatives de disseny a l'arquitectura que s'adeqüin millor a les necessitats de rendiment del sistema.
- Optimitzar la parametrització per aconseguir un rendiment millor.
 - Revisar la configuració del BIOS del sistema.
 - Revisar la documentació del fabricant per cercar-hi noves versions de microprogramari que millorin el rendiment.

3. Dissenyar i implementar architectures amb tolerància a errors.

- Instal·lar els elements de maquinari del sistema d'acord amb les especificacions del fabricant i les normes de l'organització.
- Verificar el funcionament correcte del sistema un cop instal·lat.
- Dissenyar els punts de tolerància a errors del sistema.
 - Definir i implementar la tolerància a errors elèctrics.
 - Definir i implementar la tolerància a errors de disc i de connectivitat.
- Conèixer els procediments de suport i de recuperació d'errors definits a l'empresa.
 - Externalitzar i salvaguardar les còpies segons els procediments vigents a l'organització.
 - Facilitar als tècnics de còpies de seguretat els suports amb les còpies necessàries per a la restauració del servei.
 - Instal·lar i configurar l'arquitectura de maquinari necessària per a la instal·lació del sistema de còpies de seguretat.
- Conèixer architectures que permeten més tolerància a errors.
 - Conèixer el concepte de sistemes en clúster.
 - Dissenyar i implementar l'arquitectura de maquinari necessària per a la instal·lació d'un clúster. Implementar l'arquitectura de maquinari necessària per a la instal·lació d'un clúster de base de dades.
 - Conèixer el concepte de sistemes equilibrats per xarxa.

4. Diagnosticar i resoldre avaries.

- Consultar la documentació del fabricant i la documentació interna de l'organització, així com el servei d'assistència tècnica del fabricant o de tercers amb qui l'organització tingui un contracte de manteniment, per determinar l'origen i la resolució d'incidents.
- Utilitzar les eines de diagnòstic i documentació facilitades pel fabricant.
- Planificar i executar la reparació d'acord amb la documentació del fabricant i els procediments interns.
- Planificar i executar la reparació garantint la integritat de la informació i minimitzant l'impacte sobre la disponibilitat del servei.
 - Posar en marxa els mecanismes definits a l'organització per mantenir el servei mentre es procedeix a la substitució o reparació.
 - Substituir o reparar el component avariament atenent les especificacions del fabricant.
 - Verificar el funcionament correcte del sistema després de substituir els components avariats.
 - Restablir l'explotació normal del servei.
- Conèixer i interpretar adequadament els plans de recuperació del servei existents a l'empresa.

UNITAT FORMATIVA 2

Denominació: GESTIONAR EL CREIXEMENT I LES CONDICIONS AMBIENTALS

Codi: UF1892

Durada: 50 hores

Referent de competència: Aquesta unitat formativa es correspon amb l'RP4 i l'RP5.

Capacitats i criteris d'avaluació

C1: Analitzar i avaluar els dispositius disponibles al mercat per proposar implantacions de maquinari que millorin el rendiment i les prestacions del sistema informàtic.

CE1.1 Identificar, avaluar i classificar els dispositius de maquinari existents al mercat, segons evolució i tipologia, fent ús de catàlegs comercials, documentació tècnica, revistes especialitzades o qualsevol altre mètode o suport.

CE1.2 Identificar les parts d'un sistema informàtic típicament susceptibles de provocar colls d'ampolla i degradacions de la productivitat.

CE1.3 Explicar les tendències d'evolució tecnològica en els dispositius físics comuns d'un sistema informàtic per tal de proposar-hi millores.

CE1.4 En un supòsit pràctic de planificació de creixement d'un sistema correctament caracteritzat, segons unes estimacions de possibles augments de la càrrega de treball o d'usuaris:

- Analitzar les càrregues de treball esperades i futures i caracteritzar-les de manera adequada.
- Implementar les noves càrregues de treball i integrar-les en el sistema per observar possibles efectes en el rendiment.
- Analitzar els paràmetres de rendiment obtinguts després de sotmetre el sistema a les noves càrregues de treball.
- Planificar i executar la implantació de nous dispositius de maquinari necessaris per suportar les noves càrregues de treball i minimitzar-ne els efectes sobre el sistema.
- Documentar exhaustivament els resultats de l'avaluació del sistema sotmès a noves càrregues i proposar, de manera raonada, canvis en la configuració actual o noves implantacions de maquinari.

C2: Aplicar procediments de seguretat i de condicionament ambiental per garantir la integritat del sistema i l'entorn adequat segons les especificacions i els requisits dels sistemes que s'instal·laran.

CE2.1 Enumerar i descriure els principals factors ambientals i de l'entorn que cal tenir en compte en la instal·lació adequada d'equips informàtics, a fi d'establir les precaucions que puguin evitar-los o esmorteir-ne l'efecte.

CE2.2 Enumerar i descriure els principals factors ambientals i de l'entorn que poden degradar el funcionament d'una xarxa de comunicacions, a fi d'establir les precaucions que puguin evitar-los o esmorteir-ne l'efecte.

CE2.3 Interpretar les especificacions tècniques dels dispositius i el pla de seguretat per adequar-ne la instal·lació i ubicació física i aconseguir-ne un rendiment òptim.

CE2.4 Avaluar la instal·lació de la xarxa elèctrica, assegurant-se que la seva capacitat sigui suficient i que els equips disponibles siguin els adequats per connectar tots els dispositius de maquinari i presentin un funcionament òptim.

CE2.5 En un supòsit pràctic d'instal·lació d'equipament informàtic:

- Ubicar els equips informàtics respectant les condicions ambientals de temperatura i humitat recomanades pels fabricants.
- Ubicar els equips informàtics respectant les condicions ergonòmiques i de seguretat laboral recomanades.
- Comprovar que l'entorn d'instal·lació dels equips informàtics estigui lliure de fum, pols o qualsevol altra pertorbació ambiental.

- Documentar les característiques d'ubicació dels equips informàtics i detallar els procediments, les incidències més freqüents i els paràmetres utilitzats.

CE2.6 En un supòsit pràctic de comprovació de la seguretat del sistema informàtic:

- Assegurar la manipulació dels equips per part dels usuaris perquè no variïn les condicions inicials de temperatura i humitat.
- Assegurar la manipulació dels equips per part dels usuaris comprovant que es respecta la normativa quant a seguretat.
- Comprovar la realització de còpies de seguretat, assegurant la idoneïtat de la freqüència, el suport i la informació salvaguardada.
- Documentar les incidències de seguretat trobades per poder corregir-les posteriorment.
- Interpretar el pla de seguretat del sistema i extreure'n els procediments de seguretat que cal aplicar.

Sumari

1. Gestionar el creixement.

- Planificar les ampliacions. Dimensionar els creixements futurs.
 - Extrapolar els mesuraments de la plataforma en producció.
 - Simular amb models matemàtics les noves càrregues previstes.
 - Avaluar si les noves càrregues previstes són assumibles en la plataforma actual.
- Analitzar el mercat per cercar-hi les solucions de maquinari existents.
 - Conèixer el catàleg de productes dels principals fabricants.
 - Seleccionar el producte més adequat.
 - Identificar correctament els diferents tipus de maquinari.
 - Conèixer les orientacions de preus.
 - Raonar la proposta equilibrant el component tècnic i l'econòmic.
- Localitzar els prescriptors de mercat.
 - Utilitzar els informes comparatius com a suport per a l'elecció de maquinari.
 - Utilitzar els informes de tendències com a suport per a l'elecció de maquinari.
- Executar les ampliacions garantint la màxima disponibilitat del servei.

2. Establir les condicions ambientals adequades.

- Conèixer els factors ambientals que poden afectar el funcionament de la instal·lació.
 - Identificar els factors que afecten els equips informàtics.
 - Identificar els factors que afecten les comunicacions.
- Interpretar adequadament les necessitats ambientals del maquinari.
 - Identificar els paràmetres crítics ambientals per al funcionament correcte del maquinari: establir mesuraments de temperatura, humitat i pressió i establir mesures de sorolls, vibracions i camps electromagnètics.
 - Revisar les especificacions dels fabricants del maquinari.
 - Establir rangs d'ús dels paràmetres per a l'equipament.
- Comprovar la qualitat del subministrament industrial.
 - Comprovar la instal·lació elèctrica: verificar que la capacitat de la instal·lació elèctrica compleixi els valors esperats de consum i comprovar la connexió de l'equipament a circuits filtrats per SAI.
 - Comprovar la instal·lació de refrigeració: revisar les especificacions del condicionament de fred i comprovar que compleixi els requeriments de refrigeració esperats d'acord amb les especificacions tècniques de

- l'equipament de maquinari.
- Dissenyar la ubicació dels equips a la sala.
 - Dissenyar la distribució.
 - Triar l'emplaçament dels diferents equips de maquinari.

Orientacions metodològiques

Formació a distància:

Unitats formatives	Durada total de les unitats formatives en hores	Nombre màxim d'hores susceptibles de formació a distància
Unitat formativa 1 – UF1891	70	35
Unitat formativa 2 – UF1892	50	25

Seqüència:

Per accedir a la unitat formativa 2 cal haver superat la unitat formativa 1.

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: ADMINISTRACIÓ DEL PROGRAMARI D'UN SISTEMA INFORMÀTIC

Codi: MF0485_3

Nivell de qualificació professional: 3

Associat a la unitat de competència:

UC0485_3: Instal·lar, configurar i administrar el programari de base i d'aplicació del sistema.

Durada: 210 hores

UNITAT FORMATIVA 1

Denominació: INSTAL·LACIÓ I PARAMETRITZACIÓ DEL PROGRAMARI

Codi: UF1893

Durada: 90 hores

Referent de competència: Aquesta unitat formativa es correspon amb l'RP1 i l'RP3.

Capacitats i criteris d'avaluació

C1: Especificar i aplicar procediments d'instal·lació i configuració del programari de base i d'aplicació segons les necessitats d'explotació del sistema informàtic.

CE1.1 Explicar la idoneïtat dels diferents tipus de sistemes operatius per a diferents tipus de sistemes i propòsits.

CE1.2 Identificar i descriure les diferents fases que cal seguir en la instal·lació de programari en un sistema informàtic.

CE1.3 Identificar i explicar els principals paràmetres de configuració del sistema

operatiu per a l'administració de dispositius, la gestió de memòria, la gestió de processos i la gestió de sistemes de fitxers.

CE1.4 Reconèixer i descriure els principals paràmetres de configuració del programari d'aplicació per fer un ús correcte dels recursos del sistema.

CE1.5 Automatitzar i planificar tasques en el sistema mitjançant l'elaboració de scripts.

CE1.6 En diversos supòsits pràctics d'instal·lació i configuració d'un sistema operatiu en un sistema informàtic:

- Instal·lar el programari del sistema operatiu i documentar exhaustivament el procés, les incidències produïdes i els paràmetres utilitzats.
- Configurar adequadament els paràmetres del sistema operatiu relatius al sistema de memòria i indicar l'organització que cal seguir i l'ús de tècniques avançades de gestió.
- Configurar adequadament els paràmetres del sistema operatiu relatius a l'execució de tasques: planificació de treballs, mecanismes de sincronització i assignació de recursos.
- Parametritzar adequadament el sistema d'entrada/sortida i comprovar el funcionament òptim dels dispositius perifèrics.
- Organitzar els sistemes de fitxers i crear les estructures necessàries per al funcionament correcte del sistema.
- Configurar els paràmetres del sistema operatiu de manera que es compleixin les especificacions del pla de seguretat del sistema.
- Verificar el funcionament del sistema operatiu i els dispositius que intervenen en el sistema, i assegurar la configuració dels seus controladors i l'absència de conflictes mitjançant el programari de diagnòstic que sigui necessari.
- Establir i configurar els paràmetres de xarxa del sistema operatiu de manera que es garanteixin la integritat de les dades i la fiabilitat del sistema seguint en tot moment el pla de seguretat i qualitat de l'organització.
- Habilitar l'organització i la configuració d'usuaris segons les necessitats i el pla de seguretat de l'organització.
- Actualitzar el sistema operatiu del servidor assegurant la integritat del sistema i de les dades d'acord amb el pla de seguretat de l'organització.
- Documentar la configuració del sistema operatiu i detallar els paràmetres utilitzats.
- Interpretar adequadament el pla de seguretat de l'organització per implementar-ne les mesures especificades segons la normativa de seguretat informàtica.

CE1.7 En diversos supòsits pràctics d'instal·lació i configuració de programari d'aplicació en un sistema informàtic:

- Instal·lar el programari d'aplicació i documentar exhaustivament el procés, les incidències produïdes i els paràmetres utilitzats.
- Configurar els paràmetres del programari d'aplicació relatius a l'ús de recursos del sistema de manera que es minimitzi l'impacte sobre el rendiment.
- Configurar els paràmetres del programari d'aplicació de manera que es compleixin les especificacions del pla de seguretat del sistema.
- Verificar el funcionament del programari d'aplicació i els dispositius que componen el sistema, i assegurar la configuració dels seus controladors i l'absència de conflictes mitjançant el programari de diagnòstic que sigui necessari.
- Actualitzar el programari d'aplicació assegurant la integritat del sistema i de les dades d'acord amb el pla de seguretat de l'organització.
- Documentar la configuració del programari d'aplicació i detallar els

paràmetres utilitzats.

- Interpretar adequadament el pla de seguretat de l'organització per implementar-ne les mesures especificades segons la normativa de seguretat informàtica.

C2: Identificar els components de programari del sistema, distingir-ne les característiques i detallar els paràmetres.

CE2.1 Analitzar i enumerar els diferents tipus de sistemes operatius i precisar-ne les característiques més importants.

CE2.2 Classificar i descriure els diferents tipus d'aplicacions i components de programari i explicar-ne el propòsit, les característiques i les funcions principals.

CE2.3 Identificar les funcions que duu a terme un sistema operatiu instal·lat en un sistema informàtic.

CE2.4 Explicar els requisits legals relatius a la propietat intel·lectual que cal tenir en compte en la instal·lació de programari en el sistema.

CE2.5 A partir d'un supòsit pràctic d'identificació i registre de programari d'un sistema informàtic:

- Classificar un conjunt de programari instal·lat segons diferents criteris: propòsit, idoneïtat per a un sistema i compatibilitat, entre d'altres.
- Utilitzar eines d'inventari i registrar de manera exhaustiva les característiques del programari instal·lat.
- Comprovar el nombre i la ubicació de les llicències instal·lades d'aplicacions protegides per les lleis de propietat intel·lectual per assegurar-se que es compleixin.
- Comprovar les aplicacions instal·lades per assegurar-se que no hi hagi programari no permès.
- Registrar i controlar els privilegis d'accés a les aplicacions dels usuaris segons el pla de seguretat i les lleis de protecció de dades vigents.
- Documentar la instal·lació del programari i detallar els procediments, les incidències més freqüents i els paràmetres utilitzats.

Sumari

1. Programari.

- Conèixer i comprendre què és el programari i per a què serveix.
- Saber distingir el programari del microprogramari i del maquinari.
- Identificar els diferents tipus de programari.

2. Sistemes operatius.

- Comprendre la definició i utilitat dels sistemes operatius.
 - Enumerar les funcions d'un sistema operatiu.
 - Conèixer l'evolució històrica dels sistemes operatius.
 - Distingir els diferents components d'un sistema operatiu.
 - Comprendre la gestió de processos.
 - Distingir els diferents tipus de sistemes de fitxers.
 - Conèixer els sistemes d'entrada/sortida.
 - Conèixer l'ús de controladors per a la gestió del maquinari.
 - Distingir els paràmetres habituals que cal configurar i els seus valors típics.
 - Conèixer els serveis habituals i la seva finalitat.
 - Conèixer la utilitat dels usuaris i els grups d'usuaris, així com els d'ús habitual.
- Identificar els diferents tipus de sistemes operatius i descriure'n les funcions i l'estructura.
- Classificar els sistemes operatius.
 - Classificar els sistemes operatius segons el propòsit.

- Classificar els sistemes operatius segons el grau d'implantació.
- Sistemes operatius monousuari i multiusuari.
- Sistemes operatius monotasca i multitasca.
- Sistemes operatius distribuïts.
- Sistemes operatius en temps real.
- Conèixer les polítiques definides a l'organització per a la instal·lació del sistema operatiu.
- Instal·lar i parametritzar els sistemes operatius.
 - Dur a terme els preparatius previs a la instal·lació.
 - Recopilar els controladors necessaris.
 - Definir el tipus de sistema de fitxers que s'utilitzarà i seleccionar-lo entre les possibles alternatives d'acord amb les necessitats de l'ús previst.
 - Definir els valors dels paràmetres habituals que cal configurar.
 - Instal·lar el sistema operatiu configurant el maquinari amb els controladors adequats per tal de garantir el funcionament correcte del sistema.
 - Instal·lar el sistema operatiu manualment.
 - Instal·lar el sistema operatiu en mode desatès.
 - Instal·lar el sistema operatiu automàticament.
 - Clonar servidors.
 - Configurar la xarxa.
 - Comprovar que la instal·lació del sistema operatiu sigui correcta mitjançant proves d'arrencada i parada i eines de diagnòstic.
 - Actualitzar el sistema operatiu.
- Conèixer i utilitzar adequadament les eines de gestió del sistema operatiu d'ús habitual.
 - Conèixer i utilitzar les eines de gestió de grups i usuaris.
 - Conèixer i utilitzar correctament les eines de gestió de permisos del sistema de fitxers.
 - Conèixer i utilitzar correctament les eines de configuració i diagnòstic de la xarxa.
 - Conèixer i utilitzar correctament les eines de gestió de serveis.
 - Conèixer i utilitzar correctament les eines de monitoratge del sistema facilitades pel fabricant del sistema.
- Protegir el sistema d'acord amb les normes definides.
 - Establir la configuració inicial d'usuaris i grups.
 - Configurar els permisos al sistema de fitxers.
 - Configurar els permisos al registre de configuracions.
 - Establir els permisos a la configuració de xarxa.
 - Revisar i desinstal·lar o inhabilitar els serveis innecessaris.
- Documentar la instal·lació.
 - Registrar el procés i les incidències produïdes, així com les mesures de resolució adoptades.
 - Detallar els valors dels paràmetres establerts.

3. Programari d'aplicació.

- Distingir els diferents tipus de programari d'aplicació segons el seu ús.
 - Conèixer els diferents paquets ofimàtics d'ús habitual.
 - Distingir les diferents funcionalitats que poden oferir les eines col·laboratives.
 - Conèixer la necessitat de servei que cobreix el programari ERP.
 - Conèixer la necessitat de servei que cobreix el programari CRM.
- Conèixer les polítiques definides a l'organització per a l'elecció i la instal·lació del programari d'aplicació.
 - Comprovar l'autorització de la instal·lació.
 - Utilitzar adequadament les llistes d'aplicacions permeses.

- Registrar la instal·lació realitzada.
- Instal·lar el programari d'aplicació d'acord amb les recomanacions del fabricant i les normes de seguretat de l'organització.
 - Comprovar els requisits del programari de manera prèvia a la instal·lació.
 - Seguir les instruccions d'instal·lació donades pel fabricant.
 - Actualitzar el programari d'aplicació.
- Comprovar que el funcionament del programari d'aplicació sigui correcte.
- Desplegar el programari d'aplicació de manera massiva i en mode desatès.

4. Automatitzacions.

- Conèixer els diferents llenguatges de programació d'ús habitual per a l'automatització de tasques.
 - Distingir l'entorn natiu de cada llenguatge de programació.
- Utilitzar un editor adequat per al desenvolupament del codi.
- Desenvolupar petits scripts per a l'execució de tasques de manteniment.
 - Conèixer els diferents llenguatges de programació d'ús més comú que es poden utilitzar en cada sistema operatiu.
 - Conèixer les ordres i estructures dels llenguatges script.
 - Utilitzar adequadament la documentació de consulta dels llenguatges script per facilitar l'escriptura correcta del codi.
 - Programar scripts per a l'execució de tasques de manteniment.
- Seleccionar el llenguatge de programació més adequat segons els requisits de la tasca que s'ha d'automatitzar i el sistema operatiu que s'utilitzarà.
- Configurar l'execució automàtica de la tasca al sistema operatiu.
 - Establir l'horari i la freqüència més adequats.
 - Configurar l'execució al sistema, comprovar que sigui correcta i observar-ne els resultats.
- Utilitzar eines d'automatització.

5. Inventari de programari.

- Identificar els motius de la necessitat d'inventariar.
- Seleccionar adequadament els paràmetres que cal inventariar en un sistema.
- Gestionar les llicències.
 - Inventariar les llicències comprades.
 - Inventariar les llicències instal·lades.
 - Elaborar un pla de compra de llicències en funció del creixement estimat i els models de llicenciamient del programari utilitzat.
- Gestionar eines d'inventariat.
 - Utilitzar adequadament eines d'inventari per extreure informes de llicències en ús i de llicències comprades.
 - Mantenir al dia l'inventari.
 - Utilitzar eines d'inventariat automàtic.
- Inventariar la configuració de base i d'aplicació.
- Actualitzar la llista d'aplicacions permeses per usuari.

UNITAT FORMATIVA 2

Denominació: MANTENIMENT DEL PROGRAMARI

Codi: UF1894

Durada: 70 hores

Referent de competència: Aquesta unitat formativa es correspon amb l'RP2, l'RP4 i l'RP5.

Capacitats i criteris d'avaluació

C1: Planificar el suport als usuaris assegurant la màxima disponibilitat i la documentació de les tasques corresponents.

CE1.1 Definir els objectius d'un pla d'assistència tècnica i de suport a usuaris.

CE1.2 Explicar els avantatges i les característiques principals de les tècniques d'assistència remota als usuaris a través dels serveis i les eines disponibles al sistema.

CE1.3 Enumerar i descriure els problemes més comuns relatius a la implantació de programari en llocs d'usuari.

CE1.4 Enumerar i descriure els problemes més comuns relatius a dispositius de maquinari i de xarxa en llocs d'usuari.

CE1.5 Establir procediments d'instal·lació, configuració i manteniment de programari de base i d'aplicació en llocs d'usuari.

CE1.6 En diversos supòsits pràctics de planificació de suport als usuaris en un sistema degudament caracteritzat:

- Fixar procediments d'assistència basats en l'anotació sistemàtica dels problemes detectats al personal de suport.
- Documentar exhaustivament els problemes més comuns relatius als recursos de programari del sistema.
- Documentar exhaustivament els problemes més comuns relatius als recursos de maquinari del sistema.
- Planificar la formació per a l'adaptació del personal a les eines de treball.
- Configurar i utilitzar adequadament les eines d'assistència remota a l'usuari.

C2: Analitzar el sistema mitjançant tècniques de simulació i modelatge per optimitzar el rendiment.

CE2.1 Definir el concepte de simulació i explicar els avantatges d'utilització d'aquesta tècnica així com les possibles aplicacions en diferents àmbits.

CE2.2 Explicar la necessitat de representació de sistemes a través de models per poder estudiar-los posteriorment.

CE2.3 Identificar i caracteritzar adequadament els passos necessaris per a la simulació d'un sistema.

CE2.4 En un supòsit pràctic de simulació d'un sistema informàtic degudament caracteritzat:

- Formular els objectius que s'han d'assolir a través de la simulació del sistema.
- Analitzar les característiques del sistema i construir-ne un model utilitzant les eines de modelatge disponibles.
- Construir un model de simulació segons els objectius definits i el model obtingut utilitzant les eines de simulació disponibles.
- Executar el model de simulació i documentar exhaustivament les dades obtingudes.
- Analitzar els resultats de la simulació i extreure'n els punts que no funcionen o que són problemàtics del sistema.
- Ajustar la configuració del sistema per solucionar els problemes detectats i optimitzar el rendiment.
- Documentar els processos de simulació i detallar-ne els objectius, els models i els resultats obtinguts.

Sumari

1. Plans de manteniment.

- Conèixer la utilitat i les funcions dels plans de manteniment.
 - Mantenir actualitzat el programari.
 - Gestionar l'antivirus.

- Formar els usuaris en les tasques de manteniment corresponents.
- Optimitzar el sistema de fitxers.
- Dissenyar, desenvolupar i documentar el pla de manteniment.
 - Dissenyar els manteniments proactius.
 - Documentar els manteniments reactius.
- Gestionar els problemes freqüents.
 - Localitzar i documentar els problemes freqüents.
 - Resoldre els casos de problemes freqüents.
 - Dotar els usuaris dels mitjans necessaris per poder resoldre per si mateixos els problemes freqüents.
 - Aturar la causa arrel dels problemes freqüents.
- Utilitzar el coneixement adquirit amb l'experiència.
 - Consultar les bases de dades de coneixement d'acord amb les normes establertes a l'organització.
 - Actualitzar les bases de dades de coneixement amb informació nova derivada de les activitats de manteniment.
- Atendre l'usuari.
 - Registrar les sol·licituds dels usuaris i prioritzar-ne adequadament la resolució.
 - Informar l'usuari de l'estat de resolució de la seva sol·licitud i del temps estimat de resolució.
 - Formar l'usuari en els procediments i canals adequats per a la sol·licitud de servei i notificació d'incidents, així com en les possibles solucions que s'han d'aplicar davant de l'aparició de problemes freqüents.
- Actualitzar el sistema i mantenir-lo al dia amb les versions adequades segons les funcionalitats requerides i els requisits de seguretat del sistema.
 - Actualitzar el sistema operatiu.
 - Actualitzar les aplicacions.
 - Aplicar pedaços al sistema operatiu.
 - Aplicar pedaços a les aplicacions.

2. Optimització de l'ús dels recursos.

- Comprovar l'adequació del rendiment del sistema a les necessitats de l'organització.
 - Seleccionar els paràmetres que cal mesurar per comprovar el rendiment del sistema.
 - Establir el monitoratge necessari per mesurar el rendiment del sistema.
 - Representar gràficament el rendiment del sistema, interpretar-lo i determinar l'adequació o no a les necessitats de l'organització.
 - Proposar les millores necessàries per incrementar el rendiment.
- Utilitzar les eines de modelatge per predir el rendiment del sistema d'acord amb les previsions d'increment de càrrega del sistema.
- Efectuar proves de càrrega per comprovar l'escalabilitat del sistema i la seva adequació a les necessitats presents i futures de l'organització.
 - Seleccionar les eines adequades per a la realització de les proves de càrrega en funció dels serveis que es prestaran.
 - Dissenyar i implementar el pla de proves de càrrega.
 - Dur a terme les proves de càrrega sense provocar problemes de disponibilitat del servei en el sistema en producció.
 - Representar i interpretar el resultat de les proves de càrrega.

UNITAT FORMATIVA 3

Denominació: AUDITORIES I CONTINUÏTAT DEL NEGOCI

Codi: UF1895

Durada: 50 hores

Referent de competència: Aquesta unitat formativa es correspon amb l'RP6 i l'RP7.

Capacitats i criteris d'avaluació

C1: Analitzar i definir les polítiques de realització de còpies de seguretat i de recuperació de dades en funció de les especificacions de seguretat.

CE1.1 Classificar els diferents tipus de sistemes de còpia de seguretat basant-se en el suport emprat, en la topologia o l'arquitectura i en els sistemes admesos (fitxer, partició de disc i base de dades, entre d'altres).

CE1.2 Descriure els nivells de còpies de seguretat i explicar-ne les diferències.

CE1.3 Associar la política de realització de còpies als sistemes implicats i justificar les decisions complint la normativa vigent en matèria de protecció de dades de caràcter personal.

CE1.4 A partir d'un supòsit pràctic en què es dona un escenari de sistemes d'emmagatzematge d'informació en el pla d'explotació d'una organització:

- Estimar el volum d'informació que cal copiar per unitat de temps.
- Identificar àrees d'emmagatzematge dels suports utilitzats per a les còpies de seguretat.
- Planificar l'accés autoritzat als suports.
- Mantenir el registre d'informació pel que fa al contingut, les versions i la ubicació dels fitxers de dades.
- Organitzar l'inventari dels mitjans d'emmagatzematge i els fitxers emmagatzemats.
- Verificar que les còpies de seguretat rebin el mateix nivell de seguretat que els fitxers originals.

C2: Aplicar procediments d'auditoria utilitzant les tècniques i eines adequades per garantir els paràmetres de funcionament del sistema informàtic.

CE2.1 Enumerar i explicar els objectius de l'habilitació d'auditories del sistema.

CE2.2 Classificar per prioritat els esdeveniments del sistema i de les aplicacions susceptibles de ser auditats per mantenir un funcionament òptim del sistema.

CE2.3 Determinar per a cada esdeveniment detectat la necessitat de dur a terme accions correctives i, en cas afirmatiu, establir-les.

CE2.4 En un supòsit pràctic d'aplicació de procediments d'auditoria en un sistema degudament caracteritzat:

- Establir les polítiques d'auditoria de manera adequada per evitar sobrecarregar el funcionament del sistema i afectar-ne el rendiment.
- Seleccionar una llista d'esdeveniments per auditar que proporcionin informació útil: inici i detecció de serveis, accessos a recursos, connexió i desconnexió d'usuaris, esdeveniments d'aplicacions i esdeveniments del sistema.
- Fixar les accions correctives necessàries associades als esdeveniments detectats.
- Aplicar i integrar les eines disponibles al sistema segons el pla d'auditoria establert.
- Establir alarmes per ressaltar la detecció d'esdeveniments prioritaris o crítics.
- Utilitzar les eines disponibles per a la planificació, la definició i la implementació d'auditories.
- Analitzar els registres d'auditoria i extreure'n informació sobre el funcionament i l'estat del sistema per a l'elaboració de l'informe d'auditoria.

- Interpretar la documentació tècnica del sistema i les eines d'auditoria.

Sumari

1. Còpies de seguretat.

- Tipificar les dades segons les necessitats de còpia.
- Distingir els diferents tipus de còpies, establint les diferències entre còpies completes, incrementals i diferencials, així com els avantatges i inconvenients de cadascuna i les combinacions més habituals.
- Definir correctament els períodes de retenció d'acord amb les normes de seguretat de l'empresa, amb les necessitats segons el tipus de dades i amb la legislació vigent.
- Dimensionar les còpies de seguretat.
 - Establir la mida de còpia completa d'acord amb les dades que s'han de copiar i l'ocupació estimada al dispositiu de còpies.
 - Establir la mida de les còpies en funció del temps i d'acord amb la política de còpies que s'utilitzarà.
- Establir la política de còpies de l'organització.
 - Definir el pla de còpies i indicar el tipus de còpia que s'ha de fer, l'hora de programació, la finestra de còpia i el període de conservació.
 - Revisar l'adequació de la política de còpies a les normes de l'organització i a la legalitat vigent.
- Proposar els dispositius de còpia i els suports més adequats d'acord amb les necessitats de l'organització.
 - Conèixer les diferents alternatives possibles per als dispositius de còpia.
 - Raonar la millor adequació de cada alternativa a les necessitats de l'organització.
- Dur a terme les còpies de seguretat segons els procediments i les polítiques vigents a l'organització.
 - Implementar i configurar les còpies de seguretat.
 - Programar i executar les còpies de seguretat.
 - Verificar les còpies de seguretat duent a terme restauracions i documentar el temps de restauració i el resultat obtingut.
- Gestionar el cicle de vida dels suports.
 - Salvaguardar els suports de còpia mantenint-los en unes condicions òptimes per a la conservació.
 - Externalitzar les còpies.
 - Destruir els suports un cop finalitzat el seu cicle de vida útil d'acord amb les normes de seguretat de l'empresa i garantint la impossibilitat d'extreure'n informació.
- Documentació dels plans de recuperació.
 - Dissenyar els passos necessaris per efectuar una restauració completa d'un sistema en producció.
 - Documentar les restauracions que cal executar per restablir un sistema en producció després d'un problema greu.

2. Legislació vigent.

- Conèixer les lleis vigents relacionades amb el tractament de dades.
 - Legislació vigent en matèria de protecció de dades de caràcter personal.
 - Legislació vigent en matèria de comerç electrònic.
 - Legislació vigent en matèria de protecció de la propietat intel·lectual.
- Enumerar els punts principals a tenir en compte.

3. Alternatives a les còpies.

- Conèixer les diferències entre la salvaguarda de dades i la disponibilitat del

- servei.
- Enumerar les alternatives per garantir la disponibilitat del servei.
 - Dissenyar alternatives en clúster.
 - Dissenyar alternatives basades en emmagatzematge extern.
 - Dissenyar alternatives basades en còpies d'imatges.
- Indicar els avantatges i els inconvenients de les alternatives per garantir la disponibilitat del servei sobre les còpies de seguretat.

4. Plans d'auditoria.

- Descriure els objectius dels plans d'auditoria.
 - Distingir les auditories segons el tipus i l'aplicació (de rendiment, de seguretat, de millora contínua, d'optimització d'ús).
- Descriure el perfil de l'auditor.
- Auditar el sistema.
 - Dissenyar el pla d'auditoria.
 - Utilitzar eines d'auditoria.
 - Documentar el resultat de l'auditoria.

Orientacions metodològiques

Formació a distància:

Unitats formatives	Durada total de les unitats formatives en hores	Nombre màxim d'hores susceptibles de formació a distància
Unitat formativa 1 – UF1893	90	45
Unitat formativa 2 – UF1894	70	35
Unitat formativa 3 – UF1895	50	30

Seqüència:

Per accedir a les unitats formatives 2 i 3 cal haver superat la unitat formativa 1.

Les unitats formatives 2 i 3 es poden programar de manera independent.

Criteris d'accés per als alumnes

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

MÒDUL FORMATIU 3

Denominació: SEGURETAT EN EQUIPS INFORMÀTICS

Codi: MF0486_3

Nivell de qualificació professional: 3

Associat a la unitat de competència: UC0486_3: Assegurar els 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 i 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 tallafoç de servidor i reflectir la informació de seguretat rellevant.

CE4.4 Partint d'un supòsit pràctic d'instal·lació d'un tallafoç 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 tallafoç implementat.
- Executar el pla de proves i redactar les correccions necessàries per corregir les deficiències detectades.

Sumari

1. Criteris generals comunament acceptats sobre seguretat dels equips informàtics.

- Model de seguretat orientada a la gestió del risc relacionat amb l'ús dels sistemes d'informació.
- Relació de les amenaces més freqüents, els riscos que impliquen i les salvaguardes més habituals.
- Salvaguardes i tecnologies de seguretat més habituals.
- La gestió de la seguretat informàtica com a complement de salvaguardes i mesures tecnològiques.

2. Anàlisi d'impacte de negoci.

- Identificació de processos de negoci suportats per sistemes d'informació.
- Valoració dels requeriments de confidencialitat, integritat i disponibilitat dels processos de negoci.
- Determinació dels sistemes d'informació que suporten els processos de negoci i requeriments de seguretat.

3. Gestió de riscos.

- Aplicació del procés de gestió de riscos i exposició de les alternatives més freqüents.
- Metodologies comunament acceptades d'identificació i anàlisi de riscos.
- Aplicació de controls i mesures de salvaguarda per obtenir una reducció del risc.

4. Pla d'implantació de seguretat.

- Determinació del nivell de seguretat existent dels sistemes respecte al necessari d'acord amb els requeriments de seguretat dels processos de negoci.
- Selecció de mesures de salvaguarda per cobrir els requeriments de seguretat dels sistemes d'informació.
- Guia per a l'elaboració del pla d'implantació de les salvaguardes seleccionades.

5. Protecció de dades de caràcter personal.

- Principis generals de la protecció de dades de caràcter personal.
- Infraccions i sancions previstes en la legislació vigent en matèria de protecció de dades de caràcter personal.
- Identificació i registre dels fitxers amb dades de caràcter personal utilitzats per l'organització.
- Elaboració del document de seguretat requerit per la legislació vigent en 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'altres, 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, els serveis i els 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.
- 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 DE PRÀCTIQUES PROFESSIONALS NO LABORALS DE GESTIÓ DE SISTEMES INFORMÀTICS

Codi: MP0398

Durada: 80 hores

Capacitats i criteris d'avaluació

C1: Identificar els components de maquinari del sistema, distingir-ne les característiques i detallar els paràmetres i els procediments d'instal·lació.

CE1.1 Detallar les característiques tècniques i els procediments d'instal·lació i configuració dels components de maquinari d'un sistema informàtic segons les especificacions de funcionalitats donades.

CE1.2 Definir i classificar els diferents tipus de dispositius perifèrics segons el seu propòsit, i descriure les diferents tècniques de comunicació utilitzades i les tecnologies disponibles en controladors d'entrada/sortida.

CE1.3 Identificar i classificar els diferents dispositius físics disponibles per connectar el sistema a través d'una xarxa de comunicacions.

C2: Aplicar procediments de seguretat i de condicionament ambiental per garantir la integritat del sistema i l'entorn adequat segons les especificacions i els requisits dels sistemes que s'instal·laran.

CE2.1 Interpretar les especificacions tècniques dels dispositius i el pla de seguretat per adequar-ne la instal·lació i ubicació física i aconseguir-ne un rendiment òptim.

CE2.2 Avaluar la instal·lació de la xarxa elèctrica, assegurant-se que la seva capacitat sigui suficient i que els equips disponibles siguin els adequats per connectar tots els dispositius de maquinari i presentin un funcionament òptim.

C3: Planificar el suport als usuaris assegurant la màxima disponibilitat i la documentació de les tasques corresponents.

CE3.1 Definir els objectius d'un pla d'assistència tècnica i de suport a usuaris.

CE3.2 Enumerar i descriure els problemes més comuns relatius a la implantació de programari en llocs d'usuari.

CE3.3 Enumerar i descriure els problemes més comuns relatius a dispositius de maquinari i de xarxa en llocs d'usuari.

CE3.4 Establir procediments d'instal·lació, configuració i manteniment de programari de base i d'aplicació en llocs d'usuari.

C4: Analitzar i definir les polítiques de realització de còpies de seguretat i de

recuperació de dades en funció de les especificacions de seguretat.

CE4.1 Classificar els diferents tipus de sistemes de còpia de seguretat basant-se en el suport emprat, en la topologia o l'arquitectura i en els sistemes admesos (fitxer, partició de disc i base de dades, entre d'altres).

CE4.2 Descriure els nivells de còpies de seguretat i explicar-ne les diferències.

CE4.3 Associar la política de realització de còpies als sistemes implicats i justificar les decisions complint la normativa vigent en matèria de protecció de dades de caràcter personal.

C5: Participar en els processos de treball de l'empresa seguint les normes i instruccions establertes al centre de treball.

CE5.1 Comportar-se de manera responsable tant en les relacions humanes com en les laborals.

CE5.2 Respectar els procediments i les normes del centre de treball.

CE5.3 Emprendre amb diligència les tasques segons les instruccions rebudes, intentant que s'adeqüin al ritme de treball de l'empresa.

CE5.4 Integrar-se en els processos de producció del centre de treball.

CE5.5 Fer ús dels canals de comunicació establerts.

CE5.6 Respectar en tot moment les mesures de prevenció de riscos, salut laboral i protecció del medi ambient.

Sumari

1. Posada en producció de nous sistemes.

- Revisió de la documentació d'instal·lació de sistemes i suggeriment de possibles millores.
- Instal·lació de servidors d'acord amb les normes de l'organització.
- Instal·lació de programari d'aplicació als servidors.
- Desinstal·lació dels serveis en desús.
- Establiment de la seguretat en el nivell de servidor als servidors instal·lats.
- Disseny i configuració del monitoratge dels sistemes instal·lats.
- Configuració de l'auditoria del sistema d'acord amb les normes de l'organització.
- Inventari dels nous sistemes posats en producció.
- Configuració de còpies de seguretat dels sistemes instal·lats.

2. Monitoratge i rendiment dels sistemes.

- Revisió de la documentació de monitoratge del rendiment i capacitat dels sistemes en producció.
- Revisió de la documentació de monitoratge del consum elèctric i mediambiental dels sistemes en producció.
- Revisió de la documentació d'auditoria dels sistemes en producció.
- Comportament dels sistemes en producció d'acord amb les càrregues de treball futures esperades.

3. Atenció als usuaris.

- Revisió de la documentació de suport a usuaris corporatius.
- Atenció als usuaris corporatius.
- Millores dels procediments i la documentació d'atenció a usuaris.

4. Còpies de seguretat i restauració del servei.

- Revisió de la documentació de còpies de seguretat de l'organització.
- Procediments de recuperació de servidors de producció en equips de proves, registre dels resultats i elaboració de propostes de millora dels procediments o

les polítiques de còpies.

5. 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 requerida en l'àmbit de la unitat de competència
MF0484_3: Administració del maquinari d'un sistema informàtic.	• Llicenciat/ada, enginyer/a, arquitecte/a o títol de grau corresponent, o altres títols equivalents. • Diplomats/ada, enginyer/a tècnic/a, arquitecte/a tècnic/a o títol de grau corresponent, o altres títols equivalents.	2 anys
MF0485_3: Administració del programari d'un sistema informàtic.	• Llicenciat/ada, enginyer/a, arquitecte/a o títol de grau corresponent, o altres títols equivalents. • Diplomats/ada, enginyer/a tècnic/a, arquitecte/a tècnic/a o títol de grau corresponent, o altres títols equivalents.	2 anys
MF0486_3: Seguretat en equips informàtics.	• Llicenciat/ada, enginyer/a, arquitecte/a o títol de grau corresponent, o altres títols equivalents. • Diplomats/ada, enginyer/a tècnic/a, arquitecte/a tècnic/a o títol de grau corresponent, o altres títols equivalents.	2 anys

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

Espai formatiu	Superfície m ² 15 alumnes	Superfície m ² 25 alumnes
Aula taller d'informàtica	45	75

Espai formatiu	M1	M2	M3
Aula de gestió	X	X	X
Aula tècnica informàtica	X	X	X

Espai formatiu	Equipament
Aula de gestió	– Equips audiovisuals. – PC instal·lats en xarxa, canó de projecció i Internet. – Programari específic de l'especialitat. – Dues pissarres per escriure amb retolador. – Paperògraf. – Material d'aula. – Taula i cadira per al formador. – Taula i cadires per als alumnes.
Aula tècnica informàtica	– Bastidors. – Condicionament de fred. – SAI. – Servidors instal·lats en xarxa. – Equips d'emmagatzematge extern. – Dispositius de còpia de seguretat. – Programari de còpia de seguretat. – Programari de monitoratge. – Connexió amb la xarxa de l'aula de gestió. – Connexió a Internet.

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'estris, 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'adreça a persones amb discapacitat, caldrà fer les adaptacions i els ajustos necessaris per assegurar que hi participin en condicions d'igualtat.