Cicle formatiu de grau superior
Administració de Sistemes Informàtics en la Xarxa

Desplegament curricular i criteris programàtics

Denominació del mòdul	**M11. Seguretat i alta disponibilitat**
Durada, situació i distribució setmanal	No s'assignen hores de lliure disposició. 66 hores a segon curs a raó de 2 hores setmanals presencials
Professorat	Sausan Battikh Sala. email: sausanbattikh.prof@insestatut.cat
Continguts	**UF1: Seguretat física, lògica i legislació** 1. Adopció de pautes de seguretat informàtica: 1.1 Fiabilitat, confidencialitat, integritat i disponibilitat. 1.2 Elements vulnerables en el sistema informàtic: maquinari, programari i dades. 1.3 Anàlisi de les principals vulnerabilitats d'un sistema informàtic. 1.4 Amenaces. Tipus: amenaces físiques, amenaces lògiques. 1.5 Seguretat física i ambiental. 1.6 Seguretat lògica: 1.6.1 Criptografia. 1.6.2 Llistes de control d'accés. 1.6.3 Establiment de polítiques de contrasenyes. 1.6.4 Polítiques d'emmagatzematge. 1.6.5 Còpies de seguretat i imatges de suport. 1.6.6 Mitjans d'emmagatzematge. 1.6.7 Anàlisi forense en sistemes informàtics. 2. Legislació i normes sobre seguretat: 2.1 Legislació sobre protecció de dades. 2.2 Legislació sobre els serveis de la societat de la informació i el correu electrònic. **UF2: Seguretat activa i accés remot** 1. Implantació de mecanismes de seguretat activa: 1.1 Atacs i contramesures en sistemes personals:

1.1.1 Classificació dels atacs.
1.1.2 Anatomia d'atacs i anàlisi de programari maliciós.
1.1.3 Eines preventives: instal·lació i configuració.
1.1.4 Eines pal·liatives: instal·lació i configuració.
1.1.5 Actualització de sistemes i aplicacions.
1.1.6 Seguretat en la connexió amb xarxes públiques.
1.1.7 Pautes i pràctiques segures.

1.2 Seguretat en la xarxa corporativa:

1.2.1 Monitoratge del trànsit en xarxes.
1.2.2 Seguretat en els protocols per a comunicacions sense fil.
1.2.3 Riscos potencials dels serveis de xarxa.
1.2.4 Intents de penetració.

2. Implantació de tècniques d'accés remot. Seguretat perimètrica:

2.1 Elements bàsics de la seguretat perimètrica.
2.2 Perímetres de xarxa. Zones desmilitaritzades.
2.3 Arquitectura feble de subxarxa protegida.
2.4 Arquitectura forta de subxarxa protegida.
2.5 Xarxes privades virtuals. VPN.
2.6 Beneficis i desavantatges de les VPN envers les línies dedicades.
2.7 Tècniques de xifratge. Clau pública i clau privada:

2.7.1 VPN a nivell de xarxa. SSL, IP Sec.
2.7.2 VPN a nivell d'aplicació SSH.

2.8 Servidors d'accés remot:

2.8.1 Protocols d'autenticació.
2.8.2 Configuració de paràmetres d'accés.
2.8.3 Servidors d'autenticació.

UF3: Tallafocs i servidors intermediaris

1. Instal·lació i configuració de tallafocs:

1.1 Tipus de tallafocs. Característiques. Funcions principals.
1.2 Utilització de tallafocs.
1.3 Filtratge de paquets de dades.
1.4 Instal·lació de tallafocs. Ubicació.
1.5 Regles de filtratge dels tallafocs.
1.6 Proves de funcionament. Sondeig.
1.7 Registres d'esdeveniments d'un tallafoc.

2. Instal·lació i configuració de servidors intermediaris:

2.1 Tipus de servidors intermediaris. Característiques i funcions.

	2.2 Instal·lació de servidors intermediaris. 2.3 Instal·lació i configuració de clients de servidors intermediaris. 2.4 Configuració de l'emmagatzematge en memòria cau d'un servidor intermediari. 2.5 Mètodes d'autenticació en un servidor intermediari. 2.6 Configuració de filtres. **UF4: Alta disponibilitat** 1. Implantació de solucions d'alta disponibilitat: 1.1 Definició i objectius. 1.2 Anàlisi de configuracions d'alta disponibilitat. 1.2.1 Funcionament ininterromput. 1.2.3 Integritat de dades i recuperació de servei. 1.2.4 Servidors redundants. 1.2.5 Sistemes de clústers. 1.2.6 Sistemes de balanç de càrrega. 1.3 Instal·lació i configuració de solucions d'alta disponibilitat. 1.4 Virtualització de sistemes. 1.5 Possibilitats de la virtualització de sistemes. 1.6 Eines per a la virtualització. 1.7 Configuració i utilització de màquines virtuals. 1.8 Alta disponibilitat i virtualització. 1.9 Simulació de serveis amb virtualització.
Resultats d'aprenentatge i criteris d'avaluació	**UF1: Seguretat física, lògica i legislació** 1. Adopta pautes i pràctiques de tractament segur de la informació, reconeixent les vulnerabilitats d'un sistema informàtic i la necessitat d'assegurar-lo. 1.1. Valora la importància d'assegurar la privadesa, coherència i disponibilitat de la informació en els sistemes informàtics. 1.2. Descriu les diferències entre seguretat física i lògica. 1.3. Classifica les principals vulnerabilitats d'un sistema informàtic, segons la seva tipologia i origen. 1.4. Contrasta la incidència de les tècniques d'enginyeria social en els fraus informàtics. 1.5. Adopta polítiques de contrasenyes. 1.6. Valora els avantatges que suposa la utilització de sistemes biomètrics. 1.7. Aplica tècniques criptogràfiques en l'emmagatzematge i la transmissió de la informació. 1.8. Reconeix la necessitat d'establir un pla integral de protecció perimètrica, especialment en sistemes connectats a xarxes públiques. 1.9. Identifica les fases de l'anàlisi forense enfront d'atacs a un sistema.

2. Reconeix la legislació i normativa sobre seguretat i protecció de dades valorant-ne la importància.

   2.1. Descriu la legislació sobre protecció de dades de caràcter personal.
   2.2. Determina la necessitat de controlar l'accés a la informació personal emmagatzemada.
   2.3. Identifica les figures legals que intervenen en el tractament i el manteniment dels fitxers de dades.
   2.4. Contrasta l'obligació de posar a disposició de les persones les dades personals que els concerneix.
   2.5. Descriu la legislació actual sobre els serveis de la societat de la informació i de comerç electrònic.
   2.6. Contrasta les normes sobre gestió de seguretat de la informació.
   2.7. Compren la necessitat de conèixer i respectar la normativa legal aplicable.

UF2: Seguretat activa i accés remot

1. Implanta mecanismes de seguretat activa, seleccionant i executant contramesures enfront d'amenaces o atacs al sistema.

   1.1. Classifica els principals tipus d'amenaces lògiques contra un sistema informàtic.
   1.2. Verifica l'origen i l'autenticitat de les aplicacions instal·lades en un equip, així com l'estat d'actualització del sistema operatiu.
   1.3. Identifica l'anatomia dels atacs més habituals, així com les mesures preventives i pal·liatives disponibles.
   1.4. Analitza diversos tipus d'amenaces, atacs i programari maliciós, en entorns d'execució controlats.
   1.5. Implanta aplicacions específiques per a la detecció d'amenaces i l'eliminació de programari maliciós.
   1.6. Utilitza tècniques de xifrat, signatures i certificats digitals en un entorn de treball basat en l'ús de xarxes públiques.
   1.7. Avalua les mesures de seguretat dels protocols usats en xarxes sense fil.
   1.8. Reconeix la necessitat d'inventariar i controlar els serveis de xarxa que s'executen en un sistema.
   1.9. Descriu els tipus i característiques dels sistemes de detecció d'intrusions.

2. Implanta tècniques segures d'accés remot a un sistema informàtic, interpretant i aplicant el pla de seguretat.

   2.1. Descriu escenaris típics de sistemes amb connexió a xarxes públiques en els quals es precisa fortificar la xarxa interna.
   2.2. Classifica les zones de risc d'un sistema, segons criteris de seguretat perimètrica.
   2.3. Identifica els protocols segurs de comunicació i els seus àmbits d'utilització.

2.4. Configura xarxes privades virtuals mitjançant protocols segurs a diferents nivells.
2.5. Implanta un servidor com a passarel·la d'accés a la xarxa interna des d'ubicacions remotes.
2.6. Identifica i configura els possibles mètodes d'autenticació en l'accés d'usuaris remots a través de la passarel·la.
2.7. Instal·la, configura i integra en la passarel·la un servidor remot d'autenticació.

UF3: Tallafocs i servidors intermediaris

1. Implanta tallafocs per a assegurar un sistema informàtic, analitzant les seves prestacions i controlant el tràfic cap a la xarxa interna.

   1.1. Descriu les característiques, tipus i funcions dels tallafocs.
   1.2. Classifica els nivells en els quals es realitza el filtratge de tràfic.
   1.3. Planifica la instal·lació de tallafocs per limitar els accessos a determinades zones de la xarxa.
   1.4. Configura filtres en un tallafocs a partir d'un llistat de regles de filtratge.
   1.5. Revisa els registres d'esdeveniments de tallafocs, per verificar que les regles s'apliquen correctament.
   1.6. Prova diferents opcions per implementar tallafocs, tant de programari com de maquinari.
   1.7. Diagnostica problemes de connectivitat en els clients provocats pels tallafocs.
   1.8. Elabora documentació relativa a la instal·lació, configuració i utilització de tallafocs.

2. Implanta servidors intermediaris, aplicant criteris de configuració que garanteixin el funcionament segur del servei.

   2.1. Identifica els tipus de servidors intermediaris, les seves característiques i funcions principals.
   2.2. Instal·la i configura un servidor cau.
   2.3. Configura els mètodes d'autenticació en el servidor intermediari.
   2.4. Configura un servidor intermediari en manera transparent.
   2.5. Utilitza el servidor intermediari per establir restriccions d'accés web.
   2.6. Soluciona problemes d'accés des dels clients al servidor intermediari.
   2.7. Realitza proves de funcionament del servidor intermediari, monitorant la seva activitat amb eines gràfiques.
   2.8. Configura un servidor intermediari en mode invers.
   2.9. Elabora documentació relativa a la instal·lació, configuració i ús de servidors intermediaris.

UF4: Alta disponibilitat

1. Implanta solucions d'alta disponibilitat emprant tècniques de virtualització i configurant els entorns de prova.

	1.1. Analitza supòsits i situacions en les quals es fa necessari implementar solucions d'alta disponibilitat. 1.2. Identifica solucions de maquinari per assegurar la continuïtat en el funcionament d'un sistema. 1.3. Avalua les possibilitats de la virtualització de sistemes per implementar solucions d'alta disponibilitat. 1.4. Implanta un servidor redundant que garanteixi la continuïtat de serveis en casos de caiguda del servidor principal. 1.5. Implanta un sistema de balanç de càrrega a l'entrada de la xarxa interna. 1.6. Implanta sistemes d'emmagatzematge redundant sobre servidors i dispositius específics. 1.7. Avalua la utilitat dels sistemes de clústers per augmentar la fiabilitat i productivitat del sistema. 1.8. Analitza solucions de futur per a un sistema amb demanda creixent. 1.9. Esquematitza i documenta solucions per a diferents supòsits amb necessitats d'alta disponibilitat.
Temporització Calendari 0,	

Unitats Formatives	Hores mín.	Durada prevista	Setmana Data inicial	Setmana Data final
UF 1	16	16	21/09/21	12/11/21
UF 2	16	16	13/11/21	25/01/22
UF 3	19	21	26/01/22	08/04/22
UF 4	15	14	09/04/22	03/06/22

Avaluació	L'avaluació del Mòdul serà continuada i basada en una sèrie de notes individuals obtingudes a partir d'exàmens, treballs i pràctiques. Cada Unitat Formativa dins del Mòdul s'avaluarà separadament de la resta.
	
	NOTA DE CADA UNITAT FORMATIVA (avaluació contínua, primera convocatòria):
	
	● 30%: mitjana proves teòriques i pràctiques, que es desglossa així:
	  ● 15% Examen teòric
	  ● 15 %Examen pràctic
	
	Si es posa únicament un dels exàmens (per exemple l'examen teòric) llavors el 30% de la nota de la UF recaurà en aquest.
	
	● 70%: mitjana de les pràctiques i treballs.
	
	Caldrà tenir una nota mínima de 4 a l'examen teòric i pràctic. També caldrà tenir una nota mínima de 4 en la mitjana de les pràctiques i treballs per poder fer la mitjana ponderada. És obligatori entregar totes les pràctiques i treballs.
	
	En cada UF, la pèrdua de l'avaluació pot ser per:
	
	a) Superació del 20% d'hores de faltes d'assistència sobre el número total d'hores de la Unitat Formativa.
	b) El no lliurament en temps i forma de les pràctiques, treballs o activitats demanats a cada UF.
	c) La no superació dels mínims exigits en els controls/pràctiques de la UF.
	
	Això anterior donarà com a resultat la recuperació de la UF en convocatòria 2a Ordinària al juny. Per tant, no hi haurà cap altre possibilitat de recuperació durant el curs, tret de casos excepcionals que s'estudiaran de manera particular.
	
	NOTA FINAL DEL MÒDUL: Per poder aprovar el mòdul i obtenir nota, les cinc Unitats Formatives hauran d'estar aprovades de manera individual.
	
	La qualificació Final del Mòdul professional s'obté segons la següent ponderació:
	
	$$Q_{MP} = 0.24 \cdot Q_{UF1} + 0.24 \cdot Q_{UF2} + 0.28 \cdot Q_{UF3} + 0.24 \cdot Q_{UF4}$$

Recuperació	

	Si un alumne opta per recuperar el mòdul en la segona convocatòria ordinària, haurà de recuperar totes aquelles UF's que no hagi aprovat al llarg del curs. Se'l considerarà aprovat en una determinada UF si obté una nota igual o superior a 5. Per cada UF es posaran uns treballs de recuperació, que poden no ser els mateixos que les pràctiques de l'avaluació contínua. Aquests treballs de recuperació, en volum, no seran tan extensos com a l'avaluació contínua. S'hauran de presentar com a molt tard abans del dia de l'examen de la segona convocatòria. En cas de no presentar-se (o presentar-se fora de termini), no es superarà la recuperació de la UF en segona convocatòria. Caldrà tenir una nota mínima de 4 en l'examen per poder fer la mitjana ponderada amb les pràctiques. Per altra banda, també caldrà tenir una nota mínima de 4 en la mitjana de les pràctiques de recuperació. La distribució de la nota de cada unitat formativa serà el mateix que a la primera convocatòria (veure apartat anterior). En cas de superar la UF a la segona convocatòria, serà aquesta la nota final de la UF. En cas de suspendre la segona convocatòria, cal fer constar el següent cas: ● Si la nota de la segona convocatòria és superior a la de la primera convocatòria, la nota final serà la de la segona convocatòria. ● Si la nota de la segona convocatòria és inferior a la de la primera convocatòria, la nota final serà una mitja de les dues. En cas que a l'avaluació de final de curs un alumne tingui només una unitat formativa suspesa (després de realitzar les dues convocatòries corresponents al curs), es podrà procedir a la seva compensació (aprovar la unitat formativa amb una nota de 5) si es compleixen els següents requisits: ● La nota de la unitat formativa suspesa ha de ser superior o igual a 4. ● La mitjana ponderada segons els criteris d'avaluació de les diferents unitats formatives (amb la nota de la unitat formativa suspesa) queda amb una nota final igual o superior a 5.
Avaluació en condicions especials	En les activitats d'avaluació de cada UF es prendran les mesures pertinents per atendre a la diversitat de l'alumnat, atenent les recomanacions marcades al Projecte Educatiu del Centre i de la Junta d'Avaluació.