Postgrau en Ciberseguretat

Descripció

En la societat actual la gestió de la informació i el tractament de les dades personals es duen a terme, principalment, mitjançant la tecnologia i l'ús d'internet. Aquest procediment és, sovint, vulnerable als atacs cibernètics, que cada cop són més sofisticats i freqüents, posant en risc informació sensible i infraestructures institucionals. És per aquest motiu que la ciberseguretat s'ha convertit en un element clau per a empreses, institucions i particulars.
La necessitat de perfils qualificats en ciberseguretat és una realitat a la qual vol donar resposta aquest programa que alhora s'alinea amb l'Estratègia Nacional de Ciberseguretat del Principat d'Andorra.

Objectius

L'objectiu principal d'aquest programa és proporcionar capacitats a l'estudiantat i a les persones professionals del país per poder identificar, prevenir i respondre a les potencials amenaces cibernètiques, alhora que crear una cultura de la seguretat digital i bones pràctiques.
Els objectius específics són els següents:

- Proporcionar una formació avançada en ciberseguretat cobrint temes com la ciberintel·ligència, la seguretat web i les infraestructures, la investigació forense i la correlació de dades i anàlisi de registres d'esdeveniments.
- Desenvolupar les habilitats tècniques i pràctiques necessàries per treballar com a professionals de la ciberseguretat, incloent-hi habilitats de bastionat de sistemes, enginyeria inversa i gestió d'un centre operatiu de seguretat (SOC).
- Fomentar la recerca i el desenvolupament en el camp de la ciberseguretat, mitjançant el foment de projectes de recerca i la col·laboració amb altres investigadors i professionals del camp.

- Facilitar la inserció laboral de l'estudiantat al mercat laboral de la ciberseguretat, mitjançant la col·laboració amb empreses i organitzacions del sector i l'oferta de pràctiques professionals.

A qui va dirigit

El postgrau va dirigit a persones amb titulació universitària en l'àmbit de la informàtica o la telemàtica o amb titulació de formació professional de perfils amb estudis relacionats amb la informàtica, i professionals que puguin acreditar experiència en l'àmbit de la ciberseguretat o de la informàtica.

Per poder seguir aquest postgrau cal tenir coneixements previs en:

- Sistemes operatius: administració de sistemes operatius Windows i GNU Linux/Unix (gestió d'usuaris, sistemes de fitxers, instal·lació de paquets de programari, etc.).
- Xarxes: protocols i funcionament de xarxes (Ethernet, TCP/IP, etc.). Administració d'equips de xarxa (encaminadors, commutadors, tallafocs, etc.).
- Programació: bases de dades (SQL, MySQL, etc.) i llenguatges com C, Java, Javascript, PHP, Python i Perl, principalment.

Metodologia

Aquest postgrau combina conceptes teòrics amb recursos pràctics, així com el debat sobre situacions reals relacionades amb la matèria.

La metodologia d'aquest programa és presencial i combina les classes lectives presencials, que es faran a la Universitat d'Andorra, amb l'estudi dels materials per part dels participants, mitjançant el Campus virtual.

La llengua vehicular del postgrau és el català, però el material utilitzat pot ser en anglès.

Campus virtual

El postgrau utilitza el Campus virtual de la Universitat d'Andorra com a espai de continuïtat entre les sessions presencials. El Campus, com a entorn virtual d'aprenentatge, ofereix

diversos recursos per facilitar la comunicació, l'accés a la informació i el lliurament d'activitats.

L'aula del Campus virtual és l'espai on els i les participants trobaran la documentació i material docent de cada mòdul, podran consultar les qualificacions i accedir als calendaris del programa. Així mateix, l'aula del Campus virtual permet accedir a diversos espais de comunicació.

Coordinació acadèmica

Aleix Dorca Josa, doctor en Informàtica i màster en Seguretat informàtica (2007), és una figura destacada en el món de la tecnologia i la seguretat de la informació, amb una sòlida formació acadèmica i una extensa experiència professional. La seva trajectòria, que abasta més de dues dècades, l'ha posicionat com un expert versàtil i valuós, especialitzat en àrees com les xarxes, la seguretat i l'anàlisi de dades.

Des de 2004, l'Aleix ha exercit com a IT Manager a la Universitat d'Andorra, on ha liderat la implementació i gestió de nombroses infraestructures i serveis tecnològics essencials, des de sistemes operatius i xarxes fins a serveis de correu electrònic i plataformes de videoconferència. La seva experiència també inclou projectes com la implementació d'entorn de tractament de dades massives.

Actualment, l'Aleix es dedica a la investigació tecnològica, liderant el Grup de Recerca en Tecnologia a la Universitat d'Andorra i contribuint al desenvolupament d'iniciatives innovadores. A més, comparteix el seu coneixement a través de l'ensenyament, impartint classes i seminaris sobre temes com les xarxes, la seguretat i l'anàlisi de dades. La seva reputació com a expert en el sector l'ha convertit en un referent sol·licitat, destacant per la seva capacitat d'adaptar-se a les noves tecnologies i resoldre reptes complexos.

Marc Rivero López, expert distingit en intel·ligència artificial i un professional destacat en enginyeria inversa, una combinació que li confereix un perfil excepcionalment versàtil i valuós. La seva trajectòria es caracteritza per una sòlida formació acadèmica i una àmplia experiència pràctica en intel·ligència artificial, la qual cosa li ha permès captar i mantenir l'interès del públic en nombroses conferències nacionals i internacionals.

En el seu paper clau dins dels equips CERT/CSIRT en institucions financeres de primer nivell, el Marc s'ha destacat com a Cap de Recerca. La seva sòlida formació en intel·ligència artificial ha estat un actiu fonamental en aquest context, demostrant ser un recurs inavaluable per identificar, analitzar i resoldre desafiaments complexos de seguretat.
La seva reputació com a expert en el sector l'ha convertit en un referent sol·licitat pel seu ampli coneixement, especialment en àmbits crítics com el frau, el cibercrim i els atacs dirigits. El seu lideratge ha estat clau en el desenvolupament de nombroses iniciatives de recerca, que han contribuït significativament a l'avenç del coneixement en aquestes àrees.
A més del seu èxit professional, en Marc destaca com a docent apassionat i compromès.

Albert Santisteve Prim, acumula 25 anys d'experiència en consultoria tecnològica i seguretat. Durant més de 20 anys s'ha dedicat als serveis professionals, assessorant en matèria de seguretat a empreses líders en el seus àmbits, especialment en el sector financer, tant a Espanya com a Andorra.
Durant aquest temps ha liderat equips tant nacionals com internacionals per al desenvolupament de projectes en els diferents àmbits de la ciberseguretat, ja sigui des d'una vessant més funcional com des d'una perspectiva orientada a activitats més tècniques.
Actualment és el Global CISO de Creand, lidera els equips de protecció i resposta de l'entitat en les diferents geografies on el banc té operacions. L'Albert ha intervingut com a ponent a diferents formacions especialitzades i té una reconeguda experiència com a docent, havent participat en diferents programes de postgraus i formacions executives.

Programa

El programa s'estructura en set mòduls i un treball final de postgrau:

- Mòdul 1. Governança de la seguretat (1 ECTS).
- Mòdul 2. Arquitectura de ciberseguretat (2 ECTS).
- Mòdul 3. Correlació de dades i anàlisi de *logs* (2 ECTS).
- Mòdul 4. Investigació forense i resposta a incidents (3 ECTS).
- Mòdul 5. Ciberintel·ligència (2 ECTS).
- Mòdul 6. Seguretat web i infraestructura (3 ECTS).

- Mòdul 7. Centre operatiu de servei – SOC (2 ECTS).
- Treball final de postgrau (5 ECTS).

A continuació es detalla la descripció del que es tractarà a cada mòdul.

Mòdul 1. Governança de la seguretat

En aquest mòdul es tractaran els principis, marcs de referència i millors pràctiques per establir i mantenir una estructura de govern de seguretat robusta i efectiva dins d'una organització. S'exploraran temes crítics com el desenvolupament de polítiques i procediments de seguretat que s'alineen amb els objectius empresarials, la definició i l'assignació de rols i responsabilitats, la gestió proactiva de riscos, el compliment de normatives i estàndards rellevants (tant internacionals com locals) i el mesurament continu de l'exercici de la seguretat.

A més, s'explorarà la importància de desenvolupar una estratègia de seguretat coherent i alineada amb els objectius empresarials. L'estudiant aprendrà a plantejar plans directors de seguretat que estableix un full de ruta clar per a la implementació d'iniciatives de seguretat a curt, mitjà i llarg termini, assegurant l'assignació adequada de recursos i el seguiment continuat del progrés.

Després de cursar aquest mòdul, l'estudiant hauria de ser capaç de:

- Desenvolupar i mantenir un marc de govern de seguretat.
- Gestionar proactivament els riscos de ciberseguretat.
- Entendre el compliment de normatives i estàndards rellevants.
- Dissenyar mètriques i indicadors per mesurar l'efectivitat del govern de la seguretat.
- Conèixer els fonaments d'una estratègia de ciberseguretat.

Mòdul 2. Arquitectura de ciberseguretat

Aquest mòdul ofereix l'oportunitat d'adquirir habilitats pràctiques per gestionar diferents sistemes de seguretat, implementant escenaris de ciberseguretat amb eines avançades de fabricants líders al camp. Els temes inclouen protecció de xarxes mitjançant Next Generation

Firewalls (NGFW), protecció de punts finals mitjançant Advanced Endpoint Protection i arquitectures avançades de ciberseguretat, així com eines pràctiques de *threat hunting*.
És un mòdul amb un alt contingut pràctic, on l'estudiant treballarà amb tecnologies reals proporcionades per fabricants líders.
En acabar el mòdul, l'estudiant podrà:

- Dissenyar i configurar polítiques de seguretat a FW.
- Implementar i gestionar solucions de protecció d'*endpoints*.
- Dissenyar infraestructures de ciberseguretat integrades.
- Planificar la disposició de components (*firewalls*, sistemes de prevenció d'intrusions, EDR, SIEM) per crear un ecosistema de defensa en profunditat.
- Realitzar activitats de *threat hunting*.
- Administrar escenaris reals amb eines de fabricants líders.

Mòdul 3. Correlació de dades i anàlisi de *logs*

El mòdul de Correlació de dades i anàlisi de logs se centra en les solucions d'administració d'esdeveniments i tractament d'informació de seguretat. S'hi inclouen aspectes relacionats amb el monitoratge de xarxes i la recol·lecció d'alertes i registres de seguretat de diferents aplicacions i equipaments de xarxa. L'estudiant aprendrà a utilitzar eines que li permetin consolidar la informació obtinguda durant una auditoria de seguretat, extreure'n conclusions i generar informes.
El contingut del mòdul inclou:

- Introducció a la monitorització i correlació. Tecnologies SIEM.
- *Logging*
- Esdeveniments de seguretat
- Cicle de vida d'un esdeveniment
- Configuració
- *Reporting*
- Fabricants

En acabar el mòdul, l'estudiant haurà de ser capaç de:

- Realitzar la configuració i el desplegament d'un sistema SIEM.

- Gestionar de manera local i remota els *logs* d'un sistema.
- Crear regles per a la correlació d'esdeveniments.
- Generar informes de seguretat.
- Interpretar els esdeveniments, alarmes i informes oferts per un sistema SIEM.

Mòdul 4. Investigació forense i resposta a incidents

Aquest mòdul formarà a l'estudiant en com dur a terme investigacions forenses efectives i comprendre com obtenir resultats òptims i evidències digitals vàlides en procediments legals. El mòdul inclou l'estudi de les tècniques i les eines necessàries per investigar objectius compromesos, des de la localització i l'extracció d'evidències digitals fins a la utilització d'aquestes proves en accions legals. L'estudiant aprendrà com utilitzar eines especialitzades i seguir protocols establerts per fer investigacions forenses de manera eficient i efectiva, així com analitzar i presentar les seves troballes de manera clara i concisa. A més, se li ensenyarà sobre les lleis i normatives relacionades amb la ciència forense i com aplicar-les a les seves investigacions.

En acabar el mòdul, l'estudiant haurà de ser capaç de:

- Dur a terme investigacions forenses efectives, seguint protocols establerts i utilitzant eines especialitzades.
- Comprendre com obtenir resultats òptims i evidències digitals vàlides que es puguin utilitzar en procediments legals.
- Analitzar i presentar les troballes de les investigacions forenses de forma clara i concisa, facilitant-ne la comprensió i l'ús en accions legals.
- Conèixer i aplicar les lleis i normatives relacionades amb la ciència forense en les seves investigacions, assegurant que es compleixen els requisits legals pertinents.

Mòdul 5. Ciberintel·ligència

El mòdul de ciberintel·ligència introdueix l'estudiant al voltant de la ciberseguretat. S'examinen els tipus d'amenaces existents a les xarxes, com el frau, el *phishing* i el *malware* i s'hi inclouen casos pràctics per analitzar les contramesures existents.

Els objectius d'aquest mòdul són adquirir una visió completa de la relació entre la ciberintel·ligència i l'administració de la seguretat dels sistemes d'informació, identificar diferents models d'anàlisi de la informació i el seu context, gestionar la informació obtinguda mitjançant ciberintel·ligència d'acord amb el risc, fomentar la capacitat de reflexió sobre la cibercriminalitat i desenvolupar la capacitat crítica, discussió i lliure expressió.

- Identificar i comprendre els diferents tipus d'amenaces existents a les xarxes.
- Adquirir una visió completa de la relació entre la ciberintel·ligència i l'administració de la seguretat dels sistemes d'informació, entenent com la ciberintel·ligència pot contribuir a una gestió més efectiva de la seguretat.
- Conèixer i aplicar diferents models d'anàlisi de la informació i el seu context.
- Gestionar la informació obtinguda mitjançant ciberintel·ligència d'acord amb el nivell de risc associat.

Mòdul 6. Seguretat web i infraestructura

Aquest mòdul proporciona els coneixements necessaris perquè l'estudiant sigui capaç de fer auditories de seguretat de serveis i aplicacions web per detectar problemes de seguretat i implementar solucions de prevenció i millora. S'aborda com dur a terme programari web segur i com fer front al disseny d'infraestructures robustes. També s'hi inclou una introducció a la matèria de *hacking ètic*, descrivint les tecnologies i mètodes emprats actualment per a la realització de tests de penetració i d'auditories de seguretat. En aquest mòdul s'ensenya a identificar vulnerabilitats en xarxes, sistemes i aplicacions, establir els riscos associats a cada vulnerabilitat i definir les accions correctives que siguin necessàries. A més, s'hi inclouen pràctiques diàries associades a cadascuna de les explicacions clau del temari, simulant vulnerabilitats reals en sistemes per aplicar els coneixements apresos i ús de les eines.

- Comprendre i aplicar els conceptes i les tècniques del *hacking ètic* per dur a terme tests de penetració i auditories de seguretat de manera ètica i responsable.
- Realitzar auditories de seguretat en serveis i aplicacions web.
- Identificar vulnerabilitats en xarxes, sistemes i aplicacions, avaluar els riscos associats i definir les accions correctives necessàries per mitigar-los.

- Conèixer els principis de desenvolupament de programari web segur aplicant les millors pràctiques i mesures de prevenció adequades.
- Dissenyar serveis robustos i resilients, tenint en compte els aspectes clau de la seguretat.

Mòdul 7. Centre operatiu de servei - SOC

El mòdul del centre operatiu SOC i resposta a incidents dona els coneixements a l'estudiant sobre la gestió d'un centre d'operacions de seguretat (SOC), que és un equip d'experts en ciberseguretat que monitoritza i gestiona la seguretat d'una xarxa de TI. Els temes que s'aborden en el mòdul inclouen les funcions i serveis comuns del SOC, els models d'entitats i les seves funcions, habilitats per respondre a incidents de seguretat i ús d'eines de resposta a incidents, així com la importància de seguir la cadena de custòdia de les evidències adquirides. A més, el mòdul inclou les pràctiques i exercicis perquè l'estudiant pugui aplicar allò que ha après en situacions reals.

- Comprendre les funcions i els serveis comuns d'un centre d'operacions de seguretat (SOC)
- Conèixer els diferents models d'entitats existents en un SOC i les seves funcions específiques
- Adquirir habilitats per respondre de manera efectiva a incidents de seguretat, aplicant les millors pràctiques i utilitzant les eines de resposta a incidents més adequades en cada situació.
- Comprendre i seguir correctament la cadena de custòdia de les evidències adquirides durant la gestió d'incidents de seguretat, per garantir la integritat i admissibilitat de les proves en cas de ser necessàries en processos legals.

Treball de fi de postgrau

El Treball Final de postgrau és una oportunitat important per posar en pràctica els coneixements adquirits al llarg del programa de postgrau en Ciberseguretat. Dur a terme un projecte d'aquesta naturalesa permet a l'estudiant demostrar que ha adquirit els coneixements necessaris per enfrontar els desafiaments de la ciberseguretat al món real. A

més, el projecte dona l'oportunitat d'aplicar la seva creativitat i habilitats tècniques per resoldre problemes concrets en el camp de la ciberseguretat.

Durada i calendari

El programa té una càrrega de 20 crèdits europeus i es desenvolupa d'octubre del 2026 a juny del 2027. Aquesta càrrega representa una dedicació per part de l'estudiant equivalent a 600 hores, incloent les classes lectives, les lectures, la preparació de les classes, les pràctiques i la preparació, elaboració i defensa del treball final.

Les classes lectives presencials representen 162 hores i es faran a la Universitat d'Andorra els dimarts i els dijous de les 17.00 h a les 20.00 h.

Procés d'avaluació

Per poder superar l'avaluació cal haver assistit a un mínim del 80% de les classes lectives.

L'avaluació consisteix en l'obtenció d'una qualificació igual o superior a 5 en la mitjana de la puntuació de les activitats pràctiques que s'organitzin a cada mòdul i en la presentació i superació del Treball final de postgrau.

Titulació

Les persones que superin el sistema d'avaluació previst al programa i que disposin d'una titulació universitària reconeguda a Andorra al nivell 6A o superior del Marc Andorrà de Qualificacions, obtindran un diploma de postgrau en Ciberseguretat per la Universitat d'Andorra.

En cas que no es disposi de la titulació universitària descrita al paràgraf anterior s'obtindrà un diploma d'aprofitament en Ciberseguretat expedit per la Universitat d'Andorra.

Grups reduïts

El nombre màxim d'estudiants és de 20, fet que permet que puguin gaudir d'una atenció personalitzada. En cas que hi hagi més de 20 preinscripcions el procés de selecció serà per ordre d'inscripció.

El curs s'anul·larà si no hi ha un mínim de 15 inscripcions.

Preinscripció i matrícula

Preinscripció: fins al 21 de setembre del 2026.

Matrícula: fins al 28 de setembre del 2026.

Preu: 2.400 euros. Aquest preu representa el 80% del cost de la matrícula, donat que Creand Fundació en finança el 20% restant.

Formulari de preinscripció

Més informació

Universitat d'Andorra

Plaça de la Germandat, núm. 7

AD600 Sant Julià de Lòria

Tel.: +376 743 000

A/e: euniversitaria@uda.ad

Web: http://www.uda.ad

Amb el suport de

ANC-AD Agència Nacional de Ciberseguretat d'Andorra

Creand© Fundació