ANDORRA DIGITAL

ANC-AD
Agència Nacional
de Ciberseguretat d'Andorra

Informe de Ciberintel·ligència

Ciberatacs al sector educatiu en el període 2023-2024

TLP: WHITE

DESEMBRE 2024

FITXA DEL DOCUMENT

Versió	Redactat/Revisat per	Aprovat per	Data aprovació	Data publicació
1.0	ANC-AD	ANC-AD	12/12/2024	16/12/2024

Registre de canvis			
Versió	Pàgines	Data Modificació	Motiu del canvi

Propietari del document	ANC-AD

ÍNDEX

1. METODOLOGIA

Aquest informe aplica els principis de Traffic Light Protocol (TLP). És un esquema creat per fomentar un intercanvi més bo d'informació delicada (però no classificada) en l'àmbit de la seguretat de la informació.

A través d'aquest esquema, d'una manera àgil i senzilla, s'indica fins on pot circular la informació més enllà del receptor immediat, i aquest ha de consultar l'Agència Nacional de Ciberseguretat d'Andorra quan cal distribuir la informació a tercers.

Codi	Com es fa servir	Com es comparteix
TLP: RED	S'ha de fer servir **TLP:RED** quan la informació està limitada a persones concretes, i podria tenir impacte en la privacitat, la reputació o les operacions si es fa servir malament.	Els receptors no han de compartir informació designada com a **TLP:RED** amb cap tercer fora de l'àmbit on va ser exposada originalment.
TLP: AMBER	S'ha de fer servir **TLP:AMBER** quan la informació ha de ser distribuïda de manera limitada, però suposa un risc per a la privacitat, la reputació o les operacions si és compartida fora de l'organització.	Els receptors poden compartir informació indicada com a **TLP:AMBER** només amb membres de la seva pròpia organització que necessiten conèixer-la, i amb clients, proveïdors o associats que necessiten conèixer-la per protegir-se a si mateixos o evitar danys. L'emissor pot especificar restriccions addicionals per compartir aquesta informació.
TLP: GREEN	S'ha de fer servir **TLP:GREEN** quan la informació és útil per a totes les organitzacions que hi participen, com també amb tercers de la comunitat o el sector.	Els receptors poden compartir la informació indicada com a **TLP:GREEN** amb organitzacions afiliades o membres del mateix sector, però mai a través de canals públics.
TLP: WHITE	S'ha de fer servir **TLP:WHITE** quan la informació no suposa cap risc de mal ús, conforme a les regles i procediments establerts per a la seva difusió pública.	La informació **TLP:WHITE** pot ser distribuïda sense restriccions, únicament subjecta a controls de copyright.

2. INTRODUCCIÓ

Les organitzacions educatives han treballat contínuament per adaptar-se a les oportunitats tecnològiques. Aquesta digitalització ha portat amb ella beneficis innumerables, com ara l'accés a recursos educatius en línia, plataformes d'aprenentatge a distància i eines per millorar la comunicació i la col·laboració entre estudiants i docents. Aquestes innovacions han transformat el panorama educatiu, i han facilitat l'aprenentatge en qualsevol moment i a qualsevol lloc.

No obstant això, la digitalització de l'educació també ha exposat el sector educatiu a una sèrie de riscos cibernètics. En ser un sector que gestiona grans volums de dades personals, financeres i d'investigació, s'ha convertit en un objectiu prioritari per als ciberdelinqüents. Segons informes recents, el sector educatiu ha experimentat un increment notable en els ciberatacs. En els darrers anys, el nombre d'escoles, instituts i universitats afectats s'ha multiplicat, cosa que reflecteix la sofisticació creixent i la freqüència d'aquestes amenaces.

Com es detalla a l'informe, els ciberatacs contra el sector educatiu poden tenir conseqüències devastadores. Entre elles hi trobem:

- **Interrupció o paràlisi de les operacions:** atacs com el programari de segrest poden interrompre completament les activitats acadèmiques, i afecta les classes, les recerques i l'accés a plataformes.

- **Robatori de dades personals:** els atacants cerquen informació delicada dels estudiants i del personal, com ara registres acadèmics, dades financeres i de salut.

- **Exfiltració de la propietat intel·lectual:** les universitats i els centres de recerca són especialment vulnerables atès el valor dels seus projectes i les seves patents de desenvolupament.

Aquest panorama destaca la importància d'enfortir les mesures de ciberseguretat en el sector educatiu, i promoure una cultura de protecció i adoptar tecnologies avançades per prevenir i mitigar riscos.

3. A QUINA MENA D'ORGANITZACIONS S'ADRECEN ELS CIBERATACS?

Tot i que les universitats són les víctimes principals de molts ciberatacs adreçats al sector educatiu no són l'únic objectiu dels delinqüents. En realitat, qualsevol institució vinculada a l'àmbit educatiu està en risc, i cap es pot considerar immune a aquestes amenaces.

3.1. Centres d'educació superior i recerca

La raó per la qual els atacs s'adrecen, principalment, a les **universitats i els centres d'ensenyament avançat i recerca**, és perquè aquests gestionen dades d'alt valor econòmic i estratègic. Això inclou dades financeres, personals i resultats de recerques que són altament atractius per als ciberdelinqüents.

3.1.1 Universitats

Es consideren un **objectiu prioritari** a causa de la seva gran dimensió, el seu nivell elevat de digitalització i l'impacte que pot generar un atac amb èxit. Els ciberatacs a les universitats poden derivar en el robatori de propietat intel·lectual d'alt valor, l'exposició de dades personals de milers de persones i la petició de rescats econòmics significatius.

3.1.2 Centres de recerca

Els centres de recerca generen **dades delicades i descobriments de gran valor**, des de desenvolupaments tecnològics fins a avenços científics. Aquesta informació es pot monetitzar a través de la venda en els mercats il·legals o es pot fer servir per obtenir avantatges competitius en sectors estratègics com ara la biotecnologia, la intel·ligència artificial o l'energia. Igualment, gestionen volums grans de dades confidencials relacionades amb els investigadors, els estudiants i els patrocinadors. Aquestes dades, que inclouen informació financera i personal, es poden fer servir en fraus, robatori d'identitat o es poden vendre al web fosc.

3.1.3 Centres de formació professional

La formació professional ha adquirit una importància creixent a Europa, i s'ha consolidat com a **peça clau en el desenvolupament laboral i econòmic**. Igualment, els centres que ofereixen aquesta mena de formació han avançat significativament en la digitalització, i han integrat eines tecnològiques a l'ensenyament. En els últims anys, s'ha popularitzat el model de formació professional a distància, que depèn completament de plataformes digitals per al seu funcionament i el seu èxit.

3.2. Educació primària, secundària i no reglada

3.2.1 Acadèmies i centres de formació

L'educació en línia s'ha convertit en un subsector molt lucratiu en el qual operen centenars d'empreses que ofereixen tota mena de cursos a través de classes virtuals i continguts digitals.

3.2.2 Instituts i escoles

Els instituts i les escoles, tant públics com privats, disposen d'infraestructures tecnològiques més complexes del que pensem. Aquests centres educatius gestionen una gran quantitat de dades delicades, especialment relacionades amb menors d'edat, cosa que n'augmenta la vulnerabilitat als ciberatacs. La digitalització i l'ús de plataformes en línia per a l'ensenyament i gestió administrativa han fet que les institucions educatives hagin de reforçar les mesures de seguretat per protegir aquesta informació valuosa i evitar incidents que puguin comprometre la privacitat i la seguretat dels estudiants.

4. FACTORS CLAU

Després d'haver explicat a quina mena d'organitzacions educatives busquen atacar els ciberdelinqüents, tot seguit s'esmenten quins són els factors que han fet que la vulnerabilitat del sector educatiu augmenti considerablement:

4.1. Factors tecnològics

- **Digitalització accelerada**: l'ús creixent de plataformes en línia per a l'ensenyament i l'administració ha ampliat la superfície d'atac, i ha exposat dades personals, acadèmiques i financeres. En fer servir les plataformes en línia per dur a terme tasques com ara les admissions a la universitat o el lliurament d'exàmens, un actor maliciós pot intervenir i interrompre aquests processos.

  Cal destacar que la COVID-19 va generar transformacions en diversos sectors, un d'ells l'educació. De manera immediata, les universitats, els instituts i les escoles van haver d'implementar mecanismes d'educació en línia per tal que milions d'alumnes poguessin acabar el curs acadèmic amb normalitat. Això va suposar la implementació d'eines i programari, i va multiplicar el nombre de dispositius des dels quals s'accedeix a la infraestructura TI de les organitzacions.

- **Infraestructura deficient**: moltes institucions educatives no disposen de sistemes de seguretat avançats com ara tallafocs moderns o autenticació multifactor. En concret, les universitats s'han consolidat com els centres educatius més propensos a patir ciberatacs atès que els ciberdelinqüents aprofiten l'antiguitat dels programes informàtics per atacar-les.

- **L'Internet de les coses (IoT)**: la incorporació de dispositius connectats sense la gestió de seguretat adequada (com ara càmeres de seguretat o pissarres intel·ligents) ha obert nous punts d'entrada als atacants.

4.2. Factors econòmics

- **Pressuposts limitats**: moltes institucions no tenen els recursos necessaris per implementar mesures de seguretat robustes, amb la qual cosa augmenta l'exposició als atacs com ara la pesca i el programari de segrest.

- **Dependència d'eines gratuïtes**: moltes plataformes que es fan servir a l'educació no estan dissenyades amb estàndards de seguretat alts, i deixen exposades les dades delicades.

4.3. Factors humans

- **Manca de conscienciació:** professors, estudiants i personal administratiu solen ser la baula més dèbil de la cadena per causa de la manca de formació en ciberseguretat, cosa que facilita atacs de pesca i de programari maliciós.

- **Oblits en la gestió de contrasenyes:** l'ús de contrasenyes dèbils o la seva reutilització en múltiples plataformes continua essent un problema.

4.4. Factors específics del sector

- **Alta concentració de dades delicades:** les organitzacions educatives emmagatzemen informació personal, acadèmica i financera, cosa que les converteix en un objectiu atractiu per als ciberdelinqüents. Aquesta informació es considera d'un valor enorme: propietat industrial i intel·lectual generada per investigadors, com també dades personals de docents, personal administratiu, alumnes, exalumnes, donants i proveïdors.

- **Ecosistema descentralitzat:** la integració d'eines i aplicacions diverses dificulta la implementació de polítiques de ciberseguretat uniformes.

- **Existència de períodes crítics d'activitat:** les organitzacions educatives s'enfronten a períodes crítics al llarg de l'any, com ara l'inici de curs, el tancament de trimestres, quadrimestres o semestres, moments en els quals es fan exàmens, es lliuren treballs finals que els docents han de qualificar. Aquests períodes, caracteritzats per una alta càrrega de feina i dependència de les plataformes digitals, els aprofiten els ciberdelinqüents per dur a terme atacs que busquen maximitzar l'impacte en les institucions educatives i causar-ne disrupcions significatives a les operacions.

4.5 Altres factors

- **Proliferació de l'As-A-Service:** nombrosos grups delictius comercialitzen al web fosc serveis com ara Ransomware-as-a-Service (RaaS) i DDoS-as-a-Service, a través dels quals ofereixen eines i recursos per dur a terme atacs cibernètics sense que calgui tenir coneixements tècnics avançats. Aquests models permeten que fins i tot usuaris amb habilitats mínimes puguin dur a terme atacs de programari de segrest o DDoS mitjançant el lloguer o compra de programari maliciós preconfigurat o accés a infraestructures a punt per fer-les servir. Aquesta facilitat d'accés augmenta significativament el nombre d'atacants possible, democratitza les amenaces cibernètiques i alhora amplia l'abast d'aquestes activitats il·lícites.

5. TIPOLOGIA D'ATACS

Els ciberatacs adreçats al sector educatiu es caracteritzen per la seva adaptabilitat i manca d'un patró específic, perquè els ciberdelinqüents busquen constantment la baula més dèbil a les cadenes de seguretat de les institucions. Si un intent d'atac no té èxit en un objectiu concret, els atacants canvien ràpidament d'estratègia i d'objectiu, i prioritzen sempre les formes que comportin una resistència més petita.

Les investigacions apunten a tres països principals com els més actius d'aquesta mena de ciberdelicte. Rússia, la Xina i l'Iran. Aquests països lideren la procedència de les amenaces cibernètiques no només en l'àmbit educatiu, sinó també en sectors com ara el militar o el governamental. A més, s'han identificat nombroses activitats malicioses originades als Estats Units, Alemanya i altres països industrialitzats.

Tot seguit s'expliquen els mètodes més comuns:

5.1 Enginyeria social

En el terreny de l'educació, les tècniques d'enginyeria social poden servir per accedir a equips de professors, investigadors o alumnes i robar informació, prendre el control dels dispositius i endinsar-se en les xarxes de les organitzacions per complir els objectius delictius. Igualment, també es poden produir fraus del CEO contra personal de les institucions educatives per cometre fraus econòmics a través de pagaments fraudulents. Exemple d'això és el cas ocorregut dins del sistema universitari de Dakota del Nord, que va estar a punt de patir un frau de més de 5 milions de dòlars a finals d'octubre de 2023. Les transaccions fraudulentes es van poder aturar a l'últim moment.

Pesca

Els correus electrònics fraudulents, dissenyats per enganyar els usuaris i obtenir-ne les credencials o les dades personals, són una de les eines que es fan servir més.

5.2 Programari de segrest

Els atacs de programari de segrest representen una de les amenaces principals per a les organitzacions educatives. Aquests ciberatacs, que xifren les dades i exigeixen pagaments pel seu alliberament, poden causar una disrupció significativa en les activitats acadèmiques, interrompre l'accés a informació crítica i alhora comprometre la integritat dels sistemes. En molts casos, els atacants busquen obtenir beneficis econòmics mitjançant el segrest de dades valuoses, com ara investigacions, informació financera o dades personals d'estudiants i personal.

5.3 Atacs DDoS

Tot i que els atacs de denegació de servei (DDoS) són més comuns en sectors com el sanitari, inclosos hospitals vinculats a universitats, també es poden fer servir contra plataformes i llocs web d'institucions educatives. Aquesta mena d'atacs busca sobrecarregar els servidors, i impedir que els usuaris legítims accedeixin als serveis en línia. Encara que els DDoS solen ser més freqüents en organitzacions de salut, la seva capacitat per interrompre l'accés a sistemes vitals fa que les entitats de l'àmbit educatiu també en siguin objectius potencials.

5.4 Ús de dominis falsos

La creació de llocs web fraudulents que imiten plataformes educatives ha crescut significativament, i ha facilitat la recol·lecció d'informació personal d'estudiants i docents.

6. ESTADÍSTIQUES CLAU

Tot seguit, es presenten dades de ciberatacs a organitzacions educatives corresponents als anys 2023 i 2024.

6.1 Dades de ciberatacs el 2023

Segons dades de Statista, el 2023 els sectors de l'educació i la recerca van encapçalar la llista dels més afectats pels ciberatacs, i van assolir xifres alarmants.

6.1.1 Dades globals 2023

D'acord amb l'estudi de Check Point Research, el 2023 es va observar un **increment en els ciberatacs adreçats a institucions educatives i de recerca a nivell global**. Aquest sector s'ha posicionat com l'objectiu principal dels ciberdelinqüents, i ha superat per un marge ample altres sectors com ara el militar, el governamental o el sanitari. Aquesta tendència destaca la vulnerabilitat creixent del sector educatiu.

Al llarg de l'any, es va informar d'una **mitjana setmanal de 1.780 incidents cibernètics**, dels quals **1.537 van estar relacionats amb filtracions de dades delicades**, segons l'Informe d'Investigació de Filtracions de Dades (DBIR) de Verizon. Això representa un increment del 258 % en el nombre total d'atacs en comparació amb el 2022 i un augment impactant del 546 % en els casos específics de violacions de dades.

Durant el **primer semestre del 2023**, les institucions educatives i de recerca es van enfrontar a una **mitjana de 2.256 ciberatacs setmanals**, xifra que supera sectors crítics com ara el militar (1.759 atacs registrats com a mitjana setmanal) i el sanitari. Aquest increment, que representa un augment de l'11 % respecte del 2022, posa de manifest el creixement de les amenaces en el sector educatiu i la recerca.

Més del 79 % de les institucions d'educació superior i el 80 % de les de primària han estat víctimes d'atacs de programari de segrest. Aquestes xifres mostren un increment significatiu en comparació amb l'any anterior, quan els percentatges eren del 64 % i 56 %, respectivament, i reflecteixen l'amenaça creixent que representa aquesta mena de ciberatac per al sector educatiu.

6.1.2 Dades Europa 2023

Segons el mateix estudi, **el nombre de ciberatacs adreçats a institucions educatives i de recerca a Europa va augmentar un 11 % en comparació amb el mateix període de l'any 2022**. En contrast, l'Amèrica Llatina va experimentar un creixement més moderat, amb un increment del 4 %. Això posiciona Europa com la regió amb el creixement més gran en incidents d'aquesta mena durant el període analitzat.

Tal com assenyala Chekpoint Research, aquest creixement podria estar relacionat amb la digitalització creixent del sector educatiu i la seva alta dependència de les plataformes en línia. Els ciberdelinqüents sembla que estan explotant aquestes eines, que fan servir els estudiants i

els professors per compartir materials i exàmens, per accedir a grans quantitats d'informació confidencial, com ara registres personals i dades financeres dels alumnes.

6.1.3 Dades Espanya 2023

El mateix estudi indica que Espanya va informar d'una **mitjana de 1.252 ciberatacs setmanals**, cosa que mostra una lleugera reducció interanual del 8 % respecte de l'any anterior, tot i que continua estant per sobre de la mitjana europea en alguns períodes.

6.1.4 Dades Regne Unit 2023

Un estudi del govern del **Regne Unit** fet durant el 2023 va revelar que el **85 % de les universitats enquestades van informar que havien identificat atacs maliciosos en els últims 12 mesos**. Aquesta dada situa les universitats com les entitats educatives més afectades per aquesta mena d'incidents i destaca la importància d'enfortir les mesures de ciberseguretat en el sector per protegir els seus sistemes i informació crítica enfront d'amenaces en evolució constant. A les escoles secundàries i primàries s'han identificat menys ciberatacs, 63 % i 41 %, respectivament.

6.2 Dades de ciberatacs el 2024

En el primer semestre de 2024, el sector educatiu va continuar essent un dels objectius principals dels ciberatacs a nivell global.

6.2.1 Dades globals 2024

Segons l'informe de Check Point Research comentat prèviament, entre el gener i el juliol de 2024, el sector educatiu i de recerca a nivell global va registrar 3.086 atacs per setmana, cosa que representa un increment del 37 % en comparació amb el mateix període de l'any anterior. A Espanya es va registrar una mitjana de 1.491 ciberatacs setmanals. La regió Àsia-Pacífic (APAC) va liderar en volum d'atacs amb 6.002 atacs setmanals per institució, seguida d'Europa i Amèrica del Nord.

A més, l'estudi assenyala que, durant el mes de juliol, es van identificar 12.234 dominis nous relacionats amb escoles, cosa que evidencia el creixement en la digitalització del sector educatiu a nivell mundial. Si bé aquest creixement beneficia les institucions i els docents, també és, sens dubte, un atractiu per als ciberdelinqüents.

6.2.2 Dades Europa 2024

En el context europeu, segons Check Point Research, la regió ocupa el tercer lloc a nivell global en incidents cibernètics, amb una mitjana de 2.084 atacs per setmana, cosa que representa un augment del 18 % respecte del mateix període del 2023.

Comparativament, la regió Àsia-Pacífic va liderar en volum de ciberatacs, i va assolir 6.002 atacs setmanals per organització en el mateix període, mentre que Amèrica del Nord va registrar l'increment interanual més gran amb un alarmant 127 % de creixement.

Aquest panorama subratlla com Europa, tot i que menys afectada en termes absoluts que Àsia-Pacífic, s'enfronta a una acceleració preocupant en el ritme d'incidents, cosa que posa en relleu la necessitat de reforçar les defenses cibernètiques en tots els nivells del sector educatiu i de recerca. La dependència creixent d'eines digitals i plataformes en línia amplifica la vulnerabilitat de les institucions enfront d'amenaces sofisticades i persistents.

6.2.3 Dades Espanya 2024

Entre gener i finals de juliol de 2024, Espanya ha registrat una mitjana de 1.491 ciberatacs setmanals per institució educativa segons dades proporcionades per Check Point Software. Aquest panorama a Espanya s'emmarca en una tendència global d'increment en els atacs contra l'educació i la recerca.

7. CASOS RELLEVANTS

Tot seguit, es presenten casos ocorreguts de ciberatacs a organitzacions educatives dintre de l'àmbit europeu.

7.1 Institut Nacional de Recerca de Tecnologia Agrària i Alimentària (INIA)

- **Data**: 12 de novembre de 2024.
- **Tipus d'atac**: programari de segrest.
- **Actor d'amenaça**: no identificat.
- **Detalls de l'incident**: es creu que el vector d'entrada del ciberatac va ser un USB infectat, cosa que va iniciar el segrest de dades per programari de segrest. Quan es va detectar l'atac, es van aplicar mesures de prevenció per evitar una possible propagació a altres equips, cosa que va permetre contenir-lo i limitar-lo. Per recomanació del Centre d'Operacions de Ciberseguretat (COCS) es va tallar la xarxa principal i secundària i es van aïllar màquines, servidors, commutadors i encaminadors, per prevenir una possible propagació.
- **Impacte a les operacions**: l'incident va afectar les operacions científiques i administratives, i va complicar comandes de materials i cures essencials per als animals de recerca. Els empleats (més de 600) es van quedar sense accés als ordinadors, a Internet ni a les dades emmagatzemades a la xarxa interna.
- **Una altra informació a destacar**: cal ressaltar que l'INIA és part del CSIC i és un referent en recerques agrícoles, ramaderes i mediambientals. Igualment, treballa amb tècniques avançades com ara l'edició genètica CRIPR (seqüències repetitives presents a l'ADN dels bacteris). També exerceix un rol clau en la conservació d'espècies en perill. Aquest ciberatac és el primer en la història de l'institut, segons la seva direcció, tot i que el CSIC va patir ciberatacs el 2022.

7.2 Universitat de Ciències Aplicades de Frankfurt

- **Data**: 16 de juliol de 2024.
- **Tipus d'atac**: no identificat.
- **Actor d'amenaça**: no identificat.
- **Detalls de l'incident**: els ciberdelinqüents van aconseguir accedir a part de la infraestructura informàtica de la universitat. Com a mesura de seguretat immediata, es va bloquejar l'accés extern als sistemes informàtics i es van apagar alguns serveis. També es va limitar la infraestructura de comunicacions. La universitat va contactar amb les autoritats i es va posar en marxa per recuperar els serveis afectats.

- **Impacte a les operacions**: la universitat (que té al voltant de 15.000 alumnes) va interrompre diversos serveis, com ara ascensors, inscripció a Internet, comunicació externa (no era accessible per correu electrònic ni per telèfon).

7.3 Universitat Complutense de Madrid

- **Data**: 10 de maig de 2024.
- **Tipus d'atac**: no identificat.
- **Actor d'amenaça**: no identificat.
- **Detalls de l'incident**: l'accés es va produir a través de la plataforma informàtica Gestió Integral de Pràctiques Externes (GIPE), desenvolupada pel personal de la mateixa Universitat Complutense des de l'any 2011 i allotjada als seus servidors. La naturalesa exacta de la filtració encara no s'ha determinat i tampoc se sap la quantitat d'usuaris afectats. La recomanació immediata als afectats va ser la de modificar totes les seves contrasenyes, especialment si estaven basades en dades personals que haguessin estat compromeses. Entre elles hi ha el nom, l'adreça postal, la data de naixement, la titulació feta, el correu electrònic, el DNI/passaport.
- **Impacte a les operacions**: des de la universitat asseguren que no els consta que s'haguessin filtrat contrasenyes dels usuaris, però van recomanar als seus alumnes que les modifiquessin.

7.4 Universitat Catòlica de València

- **Data**: 10 de maig de 2024.
- **Tipus d'atac**: programari de segrest.
- **Actor d'amenaça**: Grup de programari de segrest INC.
- **Detalls de l'incident**: els ciberdelinqüents van aconseguir xifrar informació de dades identificatives i econòmiques, informació acadèmica i professional, detalls d'ocupació i dades de salut. El grup de programari de segrest INC va afegir la universitat a la seva pàgina de filtracions i va amenaçar d'alliberar 1,5 TB de dades si no rebien el rescat demanat a la institució. Després de detectar l'incident, la universitat el va notificar tot seguit a la Policia Nacional espanyola i a l'Agència Espanyola de Protecció de Dades (AEPD). Igualment, va començar a col·laborar amb experts de seguretat cibernètica i les autoritats competents per gestionar la situació. Les accions que es van implementar van ser:
    - Protecció de la informació: es van adoptar mesures immediates per garantir la seguretat de les dades dels usuaris afectats.
    - Contenció de l'incident: es va treballar en la mitigació de l'atac per evitar la seva propagació a altres sistemes.

- Restauració de sistemes: es van reparar els servidors afectats i es va restaurar l'operativitat.

- **Impacte a les operacions:** malgrat la gravetat de l'atac, l'activitat acadèmica no es va interrompre. Els serveis de la universitat van assolir nivells alts de funcionalitat, i van assegurar la continuïtat en la prestació de serveis a estudiants i personal.

7.5 Consell Superior de Recerques Científiques (Espanya)

- **Data:** 16 i 17 de juliol de 2022.

- **Tipus d'atac:** programari de segrest.

- **Actor d'amenaça:** no identificat.

- **Detall de l'incident:** el ciberatac d'origen rus va encriptar part de la informació que gestionava tant el mateix Consell com els seus centres. El 18 de juliol es va activar el protocol marcat pel Centre d'Operacions de Ciberseguretat (COCS) i el Centre Criptològic Nacional (CCN) per evitar que l'atac es generalitzés.

- **Impacte a les operacions:** el ciberatac va provocar la paràlisi del centre més gran de recerca d'Espanya, que va tardar un mes a recuperar la normalitat. Els 149 centres, instituts i seus territorials del CSIC van restablir progressivament la connectivitat. El ciberatac va causar un mal reputacional enorme i moltíssimes pèrdues econòmiques.

7.6 Altres ciberatacs més antics dintre d'Europa

- **Universitat de Maastricht, Països Baixos (24 de desembre de 2019):** va ser atacada amb un programari de segrest i l'incident va ser descrit com a greu per la mateixa universitat. Els equips Windows van quedar inaccessibles i alguns llocs de la universitat, inclòs el portal d'estudiants, van caure de manera temporal.

- **Universitat de Còrsega, França (maig 2019):** la Universitat de Còrsega va ser víctima d'un programari de segrest Dharma, que va paralitzar part dels seus servidors. El criptovirus va xifrar tots els arxius (inclosos els arxius del sistema), cosa que va impedir que els ordinadors infectats poguessin funcionar. Els ciberdelinqüents es van oferir a desbloquejar els sistemes a canvi d'un rescat.

- **Diverses universitats a Itàlia (2019):** es van registrar diversos incidents que van afectar la Universitat de Campània Luigi Vanvitelli, la Universitat de Siena, la Universitat per a Estrangers Dante Alighieri, la Universitat IUAV de Venècia, la Universitat de Milà, la Universitat Politècnica de Bari i la Universitat de Salento. Els atacs els va llançar el grup Anonymous i es van publicar un total de 1700 pàgines que contenien dades personals, carnets d'identitat, passaports, números de telèfon i adreces de correu electrònic de professors i estudiants. Els ciberatacs a universitats italianes van continuar el 2020, però una gran part van formar part d'una campanya de conscienciació del grup LulZSec per evidenciar les vulnerabilitats de seguretat de les universitats.

8. ACTORS D'AMENAÇA

Malgrat que en molts dels ciberincidents no s'ha pogut determinar la seva autoria, un dels actors d'amenaça sobre els que sí que hi ha constància és INC. Ramsom Grup, tal com s'ha esmentat en el cas de la Universitat Catòlica de València.

8.1 Inc. Ransom Group

L'actor d'amenaça Inc. Ramson és una organització emergent en l'àmbit del programari de segrest que ha guanyat notorietat des de la seva aparició el juliol de 2023. Aquest grup ha estat relacionat amb ciberatacs adreçat a múltiples sectors, inclosos l'educatiu, el governamental i l'empresarial, i ha destacat pel seu ús de tàctiques avançades i una estructura operativa organitzada.

- **Àlies: INC ransomware, GOLD IONIC, salfetka, Inc. Ransom, Inc. Ransomware Group.**
- **Vist per primera vegada:** juny 2023.
- **Vist per última vegada**: agost 2024.
- **Descripció:** aquest grup es posiciona com un adversari i un proveïdor d'analistes de ciberseguretat, i ofereix serveis com ara assistència de desxifratge, accés inicial i orientació sobre seguretat de la xarxa a canvi de pagaments de rescat.

  El grup d'amenaces continua, un període previ de setmanes, emfatitzant la recopilació exhaustiva d'informació i el mapatge de la infraestructura abans d'executar atacs de programari de segrest.

  Inc. Ramson fa servir una estratègia indiscriminada, adreçada als sectors d'educació, salut, govern i tecnologia a nivell mundial per aconseguir un impacte financer generalitzat. Aquest grup gestiona un blog a la xarxa TOR on publica informació periòdica relacionada amb els seus ciberatacs duts a terme amb èxit.

- **Modus operandi:** el grup fa servir tècniques tradicionals de programari de segrest, com ara l'encriptació de dades delicades, juntament amb l'extracció d'informació crítica que després es fa servir com a moneda de canvi per extorsionar les organitzacions afectades. Han estat assenyalats per atacar sistemes vulnerables i explotar credencials compromeses per penetrar a les xarxes protegides.

9. MESURES RECOMANADES

Tal com s'ha explicat al llarg de l'informe, els ciberatacs a les organitzacions educatives poden comprometre la seguretat de les dades d'estudiants i professors, interrompre l'aprenentatge i exposar informació d'índole diversa. Davant d'aquests desafiaments, és fonamental que les organitzacions educatives implementin una sèrie de mesures de ciberseguretat per protegir-se i protegir la seva comunitat. Tot seguit es presenten algunes recomanacions clau:

- **Protecció de dades:** la protecció de dades ha de ser una prioritat per a les organitzacions educatives. Les dades personals dels estudiants, com els noms, adreces, registres acadèmics i altra informació delicada, han d'estar protegides contra l'accés no autoritzat i les bretxes de seguretat. La implementació de polítiques de seguretat cibernètica i l'educació del personal i els estudiants sobre les millors pràctiques en línia són passos essencials per garantir un entorn segur.

- **Implementació d'autenticació multifactor (MFA):** l'autenticació multifactor afegeix una capa addicional de seguretat en requerir més d'una forma de verificació per accedir a sistemes i plataformes educatives. Això fa que sigui més difícil per als atacants accedir a comptes, fins i tot si arriben a aconseguir les contrasenyes.

- **Actualització regular de programari:** és crucial mantenir tots els sistemes i aplicacions actualitzats amb els últims pedaços de seguretat. Les vulnerabilitats en el programari obsolet són una de les portes d'entrada principals per als ciberdelinqüents.

- **Ús de xarxes segures**: fomentar l'ús de xarxes privades virtuals (VPN) i assegurar-se que les connexions wifi institucionals estiguin adequadament protegides amb contrasenyes robustes i xifratge.

- **Mantenir una xarxa privada independentment:** relacionat amb el punt anterior, és important tenir una xarxa independent d'aquella que fan servir i gestionen els alumnes o visitants.

- **Monitoratge i resposta a incidents:** és essencial disposar d'un equip especialitzat que supervisi contínuament les xarxes i els sistemes de la institució a la recerca de possibles amenaces i respongui de manera efectiva en cas d'incidents. És molt important identificar, contenir i expulsar els actors maliciosos, com també recuperar la normalitat en el menor temps possible i garantir la continuïtat de les activitats.

- **Auditories de seguretat:** això inclou seguretat web, aplicacions mòbils, dispositius IoT i infraestructures al núvol de manera periòdica per detectar qualsevol debilitat que pugui posar en risc les organitzacions educatives.

- **Gestió de vulnerabilitats:** tant en aplicacions com infraestructura tecnològica, per reduir la ciberexposició d'una organització i escometre la resolució de les vulnerabilitats trobades.

- **Identificació de vulnerabilitats:** dur a terme una anàlisi regular de vulnerabilitats emergents que puguin afectar els actius digitals de l'organització.

- **Desplegar tecnologia EDR o XDR**: que proporcioni protecció addicional a llocs de treball i servidors, i fer-ne *hunting* proactiu.

- **Educació i conscienciació**: els docents, estudiants i la comunitat educativa en general han de ser conscients dels riscos cibernètics i de les millors pràctiques per evitar-los. Per a això, es proposa posar en marxa programes de formació regulars en ciberseguretat per tal de prevenir possibles errades humanes.

- **Test d'enginyeria social**: amb l'objectiu de formar i conscienciar el personal i avaluar-ne el nivell de maduresa enfront d'aquesta classe d'amenaces.

- **Test DoS**: per tal de comprovar la capacitat de resiliència de l'organització davant d'atacs de denegació de servei contra els seus sistemes.

10. CLÀUSULA DE CONFIDENCIALITAT

Aquest document és propietat de l'Agència Nacional de Ciberseguretat d'Andorra. Tota la informació que conté és confidencial, aquesta informació s'actualitzarà regularment per reflectir els possibles canvis dels productes i no podrà ser copiada o revelada a terceres persones sigui totalment o en part, sense consentiment previ exprés de l'Agència Nacional de Ciberseguretat d'Andorra.