EduTech Global

Pràctica 2: Monitorització de Seguretat i Pla de Resposta a Incidents

---

Assignatura: Control d'Accés
Professor/a: [Joan Caubet]
Alumne: [Hamza El Haddad]

ÍNDEX

Introducció

En l'actual entorn digital, la seguretat de la informació és un pilar fonamental per a EduTech Global, una plataforma d'aprenentatge en línia que gestiona dades sensibles d'estudiants, professors i continguts educatius. Després de la implementació inicial de l'estratègia de ciberseguretat a la Pràctica 1 (on es van definir controls d'accés, arquitectura segura de xarxa i polítiques de seguretat), la junta directiva ha sol·licitat una revisió exhaustiva del model de monitorització i defensa desplegat, així com l'elaboració d'un pla integral de resposta a incidents i contingència. Aquest document aborda aquests requeriments en dos grans blocs: **Repte 1**, centrat en l'auditoria d'un actiu crític amb un escenari de base de dades vulnerable i la monitorització mitjançant un intent de monitorització amb Wazuh (sense èxit) i detecció manual mitjançant anàlisi de logs; i **Repte 2**, enfocat a dissenyar un pla complet de resposta a incidents, incloent una anàlisi de riscos, assignació de rols, fases d'actuació, gestió de comunicacions i millora contínua. L'objectiu és garantir la contínua protecció dels actius d'EduTech Global, complint amb les normatives aplicables i assegurant la confiança dels usuaris en la plataforma.

Repte 1: Auditoria d'un Actiu Crític i Monitorització de Seguretat

Context i Objectiu de l'Auditoria

La junta directiva d'EduTech Global ha expressat la seva satisfacció amb les mesures de seguretat implementades fins ara, però també ha manifestat inquietuds respecte a determinats **compliments normatius** i possibles **vulnerabilitats** encara presents. En particular, se'ns ha demanat realitzar una **auditoria detallada** dels mecanismes de monitorització i defensa del nostre entorn digital, posant especial èmfasi en els actius digitals de més valor per a l'empresa. L'objectiu principal d'aquesta auditoria és avaluar l'eficàcia dels controls actuals, detectar possibles punts febles i assegurar que es compleixen estàndards de seguretat i normatives com el RGPD (Reglament General de Protecció de Dades), FERPA (Family Educational Rights and Privacy Act) i la DMCA (Digital Millennium Copyright Act), entre d'altres.

Entre els actius crítics identificats a EduTech Global, destaquen: la **base de dades de usuaris** (amb informació personal i acadèmica d'estudiants i professors), els **repositoris de material educatiu** exclusiu, el **sistema de gestió d'identitats i autenticació** (que controla l'accés diferenciat de estudiants, professors i administradors) i la **infraestructura de servidors i xarxa** que suporta pics de trànsit en períodes crítics. Tenint en compte la sensibilitat d'aquests actius, la direcció va sol·licitar enfocar l'auditoria en assegurar la **confidencialitat, integritat i disponibilitat** d'aquests sistemes, comprovant també que els mecanismes de monitoratge detectin intents d'intrusió o usos indeguts en temps real.

Actiu Crític Auditat: Base de Dades d'Usuaris

Com a part de l'auditoria, s'ha triat la **Base de Dades d'Usuaris** com l'actiu crític principal a examinar en profunditat. Aquesta base de dades emmagatzema informació personal (nom, correu, dades financeres per a pagaments) i informació acadèmica (inscripcions, notes, contingut generat) de milers d'usuaris. Per la naturalesa d'EduTech Global, es tracta d'un actiu amb el més alt nivell de sensibilitat i valor per a l'organització, ja que una brexa en aquest sistema podria comprometre la **privacitat dels estudiants**, la **propietat intel·lectual** dels continguts educatius i la confiança en la plataforma. A més, el compliment normatiu (p. ex. RGPD i FERPA) exigeix mesures estrictes de protecció i control sobre aquestes dades.

L'auditoria de la base de dades busca **verificar l'efectivitat dels controls de seguretat aplicats** (com ara el control d'accés, l'encriptació de dades en trànsit i en repòs, i la segregació de privilegis) i testejar si el sistema és resilient front a atacs comuns. Un dels vectors d'atac més rellevants a avaluar és la **injecció SQL**, atès que és una tècnica utilitzada freqüentment per obtenir accés no autoritzat a bases de dades i que podria explotar-se si l'aplicació web no valida correctament les entrades d'usuari. Per tant, la nostra auditoria s'ha centrat en simular un escenari d'intrusió mitjançant injeccions SQL i comprovar tant la vulnerabilitat del sistema com la capacitat de la nostra plataforma de monitorització per detectar-la i alertar-nos.

Intent de Monitorització amb Wazuh i Detecció Manual mitjançant Logs

Per tal de monitoritzar els sistemes i detectar activitats malicioses durant l'auditoria, es volia desplegar la plataforma Wazuh com a eina central de seguretat. Tot i això, no es va aconseguir completar la configuració del sistema. Per aquest motiu, es va optar per una detecció manual mitjançant l'anàlisi directa dels logs del sistema (per exemple, accessos web amb tail -f /var/log/apache2/access.log). Malgrat la manca d'integració de Wazuh, es va poder identificar l'intent d'injecció SQL als registres corresponents.

Escenari d'Atac Simulat: Injecció SQL Bàsica

Per avaluar la robustesa de la base de dades, s'ha simulat un **escenari d'atac** reproduint una injecció SQL bàsica en l'aplicació web d'EduTech Global. L'escenari es va dissenyar com segueix:

Vector d'atac triat: es va suposar el rol d'un atacant extern que intenta accedir a informació confidencial de la base de dades explotant un formulari de la plataforma. Per exemple, el formulari d'inici de sessió o de cerca de la plataforma podria ser susceptible si no valida adequadament les entrades. L'atacant introdueix una cadena maliciosa com a entrada d'usuari. Un exemple típic utilitzat en la prova va ser:
' OR '1'='1

- Aquesta cadena inserida en un camp de nom d'usuari o contrasenya intenta alterar la consulta SQL original que l'aplicació enviaria a la base de dades. El propòsit és que la condició '1'='1' (sempre certa) faci que la consulta retorni tots els usuaris o permeti l'accés sense conèixer la contrasenya.

- **Execució de l'atac:** en un entorn de prova aïllat però representatiu, es va enviar la petició que contenia la injecció SQL al servidor web d'EduTech Global. La consulta maliciosa construïda d'aquesta manera va arribar al servidor de base de dades. Si el sistema fos vulnerable, la base de dades processaria la instrucció injectada. Durant l'auditoria es va observar el comportament de l'aplicació: en sistemes no protegits, aquesta injecció podria permetre iniciar sessió com a usuari sense contrasenya o extreure registres sencers de la base de dades d'usuaris.

- **Monitorització durant l'atac:** Durant la simulació, es va procedir a fer un seguiment manual dels accessos mitjançant eines bàsiques de consulta de logs com tail i grep. Es van revisar en temps real els registres d'Apache i de MySQL, on es va poder identificar clarament la petició sospitosa amb l'entrada maliciosa. Aquesta detecció manual va suplir, parcialment, la funció que hauria complert Wazuh en un entorn plenament funcional. En el moment de l'atac simulat, els registres van reflectir una entrada inusual. El **registre de la base de dades** va anotar un error de sintaxi SQL (en cas que la consulta manipulada provoqués un error) o bé una consulta vàlida però amb resultats atípics (si la injecció va reeixir a modificar la lògica de consulta).

- **Resposta immediata de l'equip (simulada):** En un escenari real, aquesta alerta hauria activat de seguida el procediment de resposta: notificació als administradors de seguretat, bloqueig temporal de l'entrada de l'IP sospitosa i inici d'una anàlisi més profunda. En el context de la prova, simplement es va confirmar la recepció de l'alerta i es va analitzar els registres correlacionats per validar els detalls de l'intent d'atac.

Registres i Alertes: Tipologia i Resultats Esperats

Durant l'auditoria, s'han recollit diferents tipus de registres (logs), els quals es van revisar manualment ja que no es van poder generar alertes automàtiques amb Wazuh com estava previst. Els registres implicats en la prova d'injecció SQL van ser:

- **Registres d'accés de l'aplicació web:** contenen les peticions HTTP realitzades a la plataforma, incloent paràmetres introduïts pels usuaris. En aquests logs es va poder veure la petició amb la cadena sospitosa ' OR '1'='1 en el camp pertinent. Normalment, una línia de registre d'accés HTTP inclou la marca de temps, l'IP de l'usuari, el recurs sol·licitat i els paràmetres. Aquí es va identificar que el paràmetre user= contenia un operador lògic i cometes no esperades, fet que ja indicava entrada potencialment maliciosa.

En resum, els registres recollits van proporcionar evidències clares de l'intent d'intrusió, avisant l'equip de seguretat de forma immediata.

Resultats de l'Auditoria i Conclusions del Repte 1

L'auditoria de seguretat realitzada sobre la base de dades d'usuaris ha aportat informació molt valuosa sobre l'estat de la protecció dels nostres actius crítics i l'efectivitat de les mesures de monitorització implementades com:

- **Detecció efectiva de l'atac:** Tot i no disposar d'un sistema SIEM completament operatiu, la detecció manual dels logs va permetre identificar amb èxit l'intent d'injecció SQL. Aquesta detecció mostra que, amb una anàlisi adequada, és possible detectar activitats malicioses fins i tot en absència de mecanismes automatitzats.

- **Vulnerabilitat identificada i gravetat:** Paral·lelament, el test va revelar que l'aplicació era susceptible a l'injecció SQL en el punt provat (almenys en l'entorn de prova controlat). És a dir, la vulnerabilitat existeix i podria haver estat explotada per un atacant malintencionat per accedir indegudament a dades d'usuaris. El simple fet de poder insertar ' OR '1'='1 en una consulta indica una manca de validació d'entrada o ús de consultes SQL no preparades. Aquesta és una vulnerabilitat crítica ja que compromet directament la confidencialitat de dades personals i pot infringir lleis de protecció de dades.

- **Compliment normatiu i controls associats:** Durant l'auditoria també s'ha revisat fins a quin punt les mesures actuals cobreixen les exigències normatives:

    - En termes de **RGPD**, la detecció d'un accés no autoritzat a dades personals com el simulat implica que hi ha mecanismes de registre i alerta, cosa positiva perquè facilita la notificació a autoritats i usuaris afectats dins del termini (72h) si es produís una brexa real.

    - Pel que fa a **FERPA** (protecció de dades educatives d'estudiants), assegurar la integritat de la base de dades d'estudiants és clau. L'auditoria reforça la necessitat d'endegar mesures de prevenció addicionals (com validar inputs al servidor) per protegir la privadesa dels alumnes.

    - Sobre **propietat intel·lectual (DMCA)**, un atacant que accedeixi a la base de dades podria també obtenir materials educatius exclusius. Per tant, mantenir aquests continguts segurs requereix no només control d'accés sinó també supervisió contínua d'accessos i intents sospitosos.

- **Recomanacions de millora (accions correctives):** Com a resultat de l'auditoria, es proposen les següents accions per enfortir la seguretat:

    - *Correcció de la vulnerabilitat d'injecció SQL:* Treballar conjuntament amb l'equip de desenvolupament de la plataforma per implementar una solució immediata. Això inclou validar i sanejar totes les entrades d'usuari en els formularis crítics, utilitzar consultes preparades (SQL *prepared statements*) amb paràmetres en comptes de concatenar cadenes directament a les consultes, i realitzar proves de penetració addicionals sobre altres formularis per assegurar que no hi hagi vulnerabilitats similars.

- *Implementació d'un Web Application Firewall (WAF):* Considereu desplegar un WAF davant dels servidors web de la plataforma educativa. Un WAF pot interceptar peticions HTTP malicioses (com les que contenen patrons d'injecció SQL) abans que arribin a l'aplicació, bloquejant-les automàticament. Això actuaria com a capa preventiva addicional. Ja que a la infraestructura proposada inicialment es contemplaven sistemes IPS, un WAF enfocat a aplicacions web complementaria aquesta defensa.

- *Formació i conscienciació desenvolupadors:* Traslladar els resultats d'aquesta auditoria a l'equip de desenvolupament de programari, no amb ànim de retret sinó com a **lliçó apresa**, per tal de conscienciar sobre la importància de la seguretat en el cicle de desenvolupament (Secure SDLC). Cal establir revisions de codi enfocades en seguretat, especialment en les funcionalitats de base de dades, i pot ser útil introduir eines automàtiques d'anàlisi de seguretat de codi font per detectar possibles injections i altres vulnerabilitats abans de desplegar canvis.

- *Proves periòdiques i auditoria contínua:* Institucionalitzar que aquest tipus de prova d'intrusió es realitzi regularment. És a dir, planificar auditoria de seguretat periòdica (trimestral o semestral) en què es tornin a testejar les defenses davant vectors d'atac prioritaris, incloent qualsevol vector nou que pugui sorgir. També es recomana avaluar de manera controlada altres escenaris d'atac (p. ex. phishing als administradors, elevació de privilegis internament, etc.) per garantir una postura de seguretat proactiva.

- **Altres consideracions (noves tecnologies):** La direcció va mencionar l'interès en la implementació futur d'un sistema d'Intel·ligència Artificial avançat, *"EduMind"*, per a personalitzar l'aprenentatge dels estudiants. Si bé això no forma part directament de l'escenari d'atac simulat, s'ha tingut en compte com a part de l'auditoria preventiva. La recomanació de l'equip de TI és que, abans de desplegar qualsevol sistema d'IA d'aquest tipus, es realitzi un estudi de riscos específic orientat a la seguretat i privadesa: caldria analitzar quines dades gestionaria, quins accessos tindria i com prevenir que esdevingui un nou vector d'atac. Donada la descripció gairebé **futurista** d'EduMind, és important temperar expectatives i planificar controls i limitacions de seguretat realistes. En definitiva, qualsevol nova funcionalitat o tecnologia integrada al sistema ha de passar pels mateixos estàndards d'auditoria i proves que els components actuals.

En conclusió, l'auditoria de l'actiu crític (base de dades d'usuaris) ha permès **identificar una vulnerabilitat important**. S'han proposat millores immediates per eliminar la vulnerabilitat i reforçar la seguretat global.

Repte 2: Pla de Resposta a Incidents i Contingència de Negoci

Introducció i Abast del Pla

Després de l'anàlisi de l'estat de la seguretat actual i de les vulnerabilitats identificades, EduTech Global necessita disposar d'un **Pla integral de Resposta a Incidents de Seguretat** que li permeti fer front de manera efectiva al creixent entorn d'amenaces. La junta directiva vol garanties de que existeixen **plans de prevenció i contingència** per a qualsevol incident que pugui afectar l'empresa i els seus actius més valuosos, assegurant així la continuïtat del negoci i la confiança dels usuaris en tot moment.

Objectius principals del pla:

- **Reduir el risc i l'impacte** dels incidents mitjançant la prevenció proactiva i una resposta diligent.

- **Detectar i respondre ràpidament** a qualsevol atac o brexa de seguretat, minimitzant el temps en què els sistemes romanen compromesos.

- **Mantenir la continuïtat del servei** fins i tot en situacions adverses, garantint que els processos educatius clau (classes, exàmens, inscripcions) puguin continuar o ser restablerts en el mínim temps possible.

- **Preservar la confiança** dels usuaris i el compliment normatiu, comunicant adequadament els incidents quan calgui i adoptant mesures correctives que evitin sancions i dany reputacional.

- **Fomentar la millora contínua** en la postura de ciberseguretat d'EduTech Global, aprenent de cada incident i adaptant les defenses a les noves amenaces.

Anàlisi de Riscos i Amenaces Potencials

- **Injecció SQL i fuga de dades sensibles:** Probabilitat *mitjana*, atès que ja s'ha detectat una vulnerabilitat d'aquest tipus en el nostre sistema (ara en procés de correcció) i que els atacs web són recurrents. Impacte *crític*, ja que una explotació exitosa comprometria dades personals d'usuaris i informació acadèmica, violant privadesa i regulacions (RGPD/FERPA) i afectant greument la reputació d'EduTech Global. *Nivell de risc global: ALT.*
  Mitigació: Corregir les vulnerabilitats de l'aplicació (injeccions SQL i similars) de manera prioritària, implementar un WAF i mantenir una monitorització contínua de possibles intents repetits.

- **Atac de Denegació de Servei (DDoS) durant períodes crítics:** Probabilitat *alta*, ja que les plataformes en línia sovint són objectiu de DDoS, i EduTech Global pot patir aquests atacs especialment durant èpoques d'exàmens o inscripcions (quan el

trànsit és màxim, un competidor o actor maliciós podria intentar col·lapsar el servei). Impacte *alt*, perquè la indisponibilitat de la plataforma en moments clau impediria l'accés a classes o proves, generant frustració en els usuaris i possibles pèrdues econòmiques o de credibilitat. *Nivell de risc: ALT.*
Mitigació: Preparar la infraestructura per absorbir atacs DDoS (ús de CDN i balancejadors, capacitat elàstica al núvol, sistemes d'anti-DDoS al tallafoc), i tenir un pla de contingència per comunicar als usuaris i prolongar terminis acadèmics si cal.

- **Compromís de credencials privilegiades (phishing o atac intern):** Probabilitat *alta*, ja que l'error humà és un factor crític: un administrador o professor pot ser víctima de phishing o enginyeria social, o un insider maliciós amb accés legítim podria abusar dels seus privilegis. Impacte *alt*, perquè credencials privilegiades (administradors de sistema, o comptes de professor amb accés a moltes dades) podrien utilitzar-se per extreure informació massiva, alterar notes o injectar codi maliciós en la plataforma. *Nivell de risc: ALT.*
  Mitigació: Enfortir l'autenticació (MFA obligatori per comptes d'alt privilegi), polítiques estrictes de gestió de credencials, formació regular en detecció de phishing per a tot el personal, i monitorització de l'ús de comptes privilegiats (alertes de comportament anòmal, per exemple si un compte d'admin accedeix a massa registres inusuals).

- **Malware/Ransomware en servidors o equips corporatius:** Probabilitat *moderada*, donat que l'amenaça de ransomware és generalitzada en tots els sectors. Un correu de phishing amb un adjunt maliciós o la descàrrega involuntària de malware podria infectar un servidor o estació de treball connectada a la xarxa. Impacte *molt alt*, ja que un ransomware podria xifrar bases de dades o continguts educatius, deixant la plataforma inutilitzable i possiblement provocant pèrdua permanent de dades si no hi ha còpies de seguretat fiables. *Nivell de risc: ALT.*
  Mitigació: Disposar de **còpies de seguretat** freqüents i emmagatzemades fora de línia (desconnectades de la xarxa principal per evitar que el malware les afecti), utilitzar programari antivirus/antimalware actualitzat en servidors i equips, segmentar la xarxa de manera que una infecció en un punt no es propagui fàcilment a tota la infraestructura, i entrenar els usuaris contra phishing per reduir la probabilitat d'infecció inicial.

- **Accessos no autoritzats per vulnerabilitats de programari (0-day, exploits desconeguts):** Probabilitat *mitjana*, ja que tot i mantenir els sistemes actualitzats, sempre existeix el risc d'exploits desconeguts (0-day) o noves vulnerabilitats en les tecnologies que fem servir (sistemes operatius, servidors web, llibreries de programació, etc.). Impacte *variable (mitjà a alt)* depenent de la naturalesa de la vulnerabilitat, però podria ser alt si permet execució remota de codi o accés a dades sensibles. *Nivell de risc: MITJÀ/ALT.*
  Mitigació: Aplicar una estratègia de *"Defensa en profunditat"*: múltiples capes de seguretat (firewalls, IPS, WAF, monitorització) de manera que fins i tot si una capa és saltada per una vulnerabilitat 0-day, altres la puguin aturar o detectar. Mantenir un procés àgil d'actualització i *patch management* per aplicar pegats tan bon punt estiguin disponibles quan es reveli una nova vulnerabilitat. Participar en comunitats de seguretat per rebre alertes tempranes de 0-days i consells de mitigació temporal

(workarounds).

- **Incompliment de normatives de seguretat o privadesa (incident legal):** Probabilitat *baixa*, ja que usualment és conseqüència d'un altre incident (per exemple una fuga de dades no gestionada correctament) més que un atac directament; però si no estem preparats per complir obligacions legals post-incident, podríem incórrer en sancions. Impacte *alt*, perquè multes per RGPD o demandes per incompliment podrien tenir costos molt elevats i danyar la continuïtat del negoci. *Nivell de risc: MITJÀ.*
  Mitigació: Assegurar que el pla de resposta inclou els procediments necessaris per complir la normativa (p. ex., notificació a autoritats i usuaris dins de termini, documentació de tot l'incident, mesures de contenció adequades per demostrar diligència). Realitzar també auditories de compliment normatiu de manera regular per detectar desviacions abans que derivin en un incident.

Altres amenaces considerades en l'anàlisi inclouen: fallades de subministrament elèctric o de comunicacions (amb impacte mitigat per sistemes SAI i proveïdors redundants de Internet), desastres naturals que afectin el centre de dades (cobert per plans de recuperació en un altre centre), i errors humans operatius (un administrador que esborri dades accidentalment, mitigat amb controls addicionals i còpies de seguretat).

Estratègies de Prevenció i Preparació

La millor manera de minimitzar l'impacte dels incidents de seguretat és **prevenir-los proactivament** o estar preparat per quan passin, i aquestes són les següents:

- **Controls d'accés robustos i diferenciats:** Mantindre i revisar periòdicament el model de control d'accés implementat (basat en rols, amb privilegi mínim i segregació de funcions) per assegurar que cada usuari només pot accedir a les dades i funcionalitats que li pertoquen. Realitzar proves d'estrès als mecanismes d'autenticació i autorització (per exemple, assegurar-se que un estudiant no pot accedir a recursos de professor ni viceversa) i revisar els permisos dels comptes de forma regular per revocar accessos obsolets.

- **Autenticació multifactor (MFA):** Exigir MFA en els accessos dels usuaris d'alt privilegi (administradors de sistema, personal de TI, etc.) i oferir-la com a opció fortament recomanada per a tots els usuaris (estudiants i professors) en els seus comptes de plataforma. Això agrega una capa addicional de seguretat per prevenir accessos no autoritzats fins i tot si es comprometen contrasenyes. En la infraestructura proposada ja es considerava la implantació d'un sistema MFA; aquest pla subratlla prioritzar-ne l'aplicació completa.

- **Parchejat i actualització contínua:** Establir un procés formal de **gestió de vulnerabilitats** i actualitzacions: mantenir un inventari de tot el programari i sistemes en ús, subscriure's a butlletins de seguretat dels fabricants i comunitats, i aplicar pegats de seguretat en el menor temps possible després de la seva disponibilitat (seguint un procediment que valori primer els sistemes crítics). Això inclou actualitzar

el sistema operatiu, el servidor de bases de dades, el servidor web, llibreries de codi i també les regles de SIEM/IPS perquè estiguin al dia front noves amenaces. Es realitzaran escanejos de vulnerabilitats periòdics per identificar components descuidats.

- **Segmentació de la xarxa i mínim accés:** Mantenir la separació de segments de xarxa tal com es va dissenyar (xarxa de bases de dades separada de la xarxa pública web, segments per a administració interna, etc.) de manera que un incident en una part no afecti totalment la resta. Per exemple, si un equip d'oficina es veu compromès per malware, la segmentació ha de limitar la possibilitat que accedeixi al segment de bases de dades sense passar per controls addicionals. També s'ha d'implementar el principi de **privilegi mínim** en serveis i comptes de sistema: els serveis han de córrer amb comptes restringits i els accessos entre servidors només els necessaris (firewalls internament configurats per permetre únicament el trànsit legítim entre capes).

- **Monitorització contínua i intel·ligent:** Consolidar l'ús de **SIEM** com a eina central de vigilància. Això significa no només tenir-lo actiu, sinó definir clarament què constitueix un esdeveniment de seguretat que requereix atenció immediata. Configurar llindars d'alerta adequats (p. ex., si es detecten més de X intents fallits d'inici de sessió en Y minuts, o si un usuari descarrega més de Z registres de dades en poc temps, etc., que el SIEM generi alertes elevades). Assignar responsables per rebre aquestes alertes 24/7. La monitorització també inclou l'ús de l'IPS de xarxa integrat al firewall per bloquejar patrons coneguts d'atac a nivell de xarxa.

- **Còpies de seguretat i recuperació:** Assegurar que existeix un esquema de **backup** robust per a les dades crítiques (bases de dades d'usuaris, continguts, etc.). S'han de realitzar còpies de seguretat de manera regular (diària per a dades crítiques, setmanal per a dades menys volàtils, etc.) i verificar periòdicament la integritat i restaurabilitat d'aquestes còpies (mitjançant simulacres de restauració). Com a mesura de prevenció, algunes còpies han d'estar *fora de línia* o almenys en un repositori segregat per evitar que un atacant que comprometi la xarxa pugui esborrar o xifrar també les backups. Aquest punt connecta amb el pla de contingència que es detallarà més endavant.

- **Programes de conscienciació i formació:** L'empresa ha d'invertir en **formació contínua del personal i usuaris** en matèria de seguretat. Això inclou sessions periòdiques per als administradors i desenvolupadors sobre noves amenaces (per exemple, recents campanyes de phishing, o tècniques d'atac emergents com el *credential stuffing*) i recordatoris de les polítiques de seguretat internes. També es poden oferir materials educatius als professors i estudiants sobre bones pràctiques de seguretat (crear contrasenyes fortes, no reutilitzar credencials, detectar correus fraudulents). Un usuari informat és la primera línia de defensa contra moltes amenaces.

- **Proves de penetració i auditories externes:** A més de les auditories internes, contractar periòdicament auditors de seguretat independents o realitzar **tests de penetració** externs. Aquests professionals poden descobrir vulnerabilitats que

l'equip intern podria passar per alt i oferir una perspectiva fresca. Idealment, fer un pentest anual integral sobre la plataforma EduTech Global, i auditories específiques si es fan canvis grans (p. ex., abans de llançar una nova funcionalitat important o després d'integrar un sistema nou com l'esmentat EduMind).

- **Normatives i estàndards de seguretat:** Desenvolupar i mantenir actualitzades les **polítiques i procediments** de seguretat de l'empresa. Això inclou tenir clar els procediments de resposta a incidents (que tractarem en detall), però també normes diàries: política de contrasenyes, política d'ús acceptable, política de seguretat per dispositius personals (BYOD) si s'escau, etc. Aquestes polítiques han d'estar alineades amb estàndards reconeguts (com ISO 27001, NIST) i amb la regulació vigent. Tots els empleats han de conèixer l'existència d'aquestes polítiques i saber on consultar-les.

Equip de Resposta a Incidents: Rols i Responsabilitats

Una resposta a incidents efectiva requereix un equip coordinat, amb rols clarament definits perquè, en moments de crisi, cada membre sàpiga què s'espera d'ell i quines decisions pot prendre, per això la composició de l'**Equip de Resposta a Incidents (ERI)** i les responsabilitats de cada rol són les següents:

- **Responsable de Resposta a Incidents (Incident Manager):** Aquest serà usualment el CISO o el cap de seguretat de l'empresa. La seva funció és **coordinar tot el procés de resposta** un cop es declara un incident. Pren decisions com ara quan escalar l'incident a la direcció, si cal aïllar parts de la xarxa, i assegura que cada rol compleix les seves tasques. És el punt de contacte principal entre l'equip tècnic i la direcció de l'empresa durant l'incident. També és qui, un cop tancat l'incident, lidera la reunió de post-mortem per analitzar-lo i impulsar millores.

- **Analistes de Seguretat / Operadors SOC:** Són tècnics especialitzats que **monitoritzen els sistemes** (per exemple, supervisant el panell de SIEM i altres eines) i que inicialment detecten i analitzen l'incident. Quan salta una alerta crítica, un analista de seguretat valida si és un veritable incident o un fals positiu, recull evidències (logs, captures de pantalla, hash de fitxers sospitosos, etc.) i informa el Responsable de Resposta a Incidents. Durant la resposta, poden realitzar investigacions forenses en calent, com ara identificar l'abast de la intrusió, l'origen de l'atac i seguiment de les activitats de l'atacant dins del sistema.

- **Equip Tècnic de Suport (Administradors de sistemes / Desenvolupadors):** Aquest grup s'encarrega d'**aplicar les mesures tècniques de contenció i eradicació**. Per exemple, si cal desconnectar un servidor de la xarxa, els administradors de sistemes ho duen a terme; si cal aplicar un pegat d'emergència a l'aplicació per tancar una vulnerabilitat explotada, els desenvolupadors de la plataforma ho implementen immediatament. També són responsables de restaurar serveis afectats (per exemple, recuperar dades de backup, reconstruir un servidor nou si cal) durant la fase de recuperació. Han de seguir les indicacions i prioritats marcades pel Responsable d'Incidents i col·laborar estretament amb els analistes de seguretat per assegurar que les accions tècniques no interfereixin amb la recollida

d'evidències o investigació (hi ha d'haver comunicació: p. ex., "puc reiniciar aquest servidor compromès ara?" un analista hauria d'haver extret abans els logs necessaris).

- **Enllaç de Comunicacions (Portaveu Intern/Extern):** Persona encarregada de la **gestió de comunicació** durant l'incident. Pot ser algú de l'equip de comunicació corporativa o relacions públiques. La seva tasca és coordinar els missatges que es donen tant a l'interior de l'empresa (als empleats, direcció, etc.) com a l'exterior (usuaris, mitjans de comunicació, autoritats) seguint el pla de comunicació. Treballa colze a colze amb el Responsable de Resposta a Incidents per entendre l'abast i impacte de l'incident i preparar comunicats acurats i a temps. També gestiona les consultes entrants (per exemple, si premsa contacta o molts usuaris truquen reportant problemes).

- **Representant Legal/Compliment Normatiu:** En incidents greus, especialment aquells que impliquin **dades personals compromeses o requeriments legals**, és important involucrar algú del departament legal o de compliment (com ara el Delegat de Protecció de Dades si n'hi ha). Aquest rol assessora sobre les obligacions legals: per exemple, si s'ha produït una fuga de dades personals, indicaria els passos per notificar l'Agència de Protecció de Dades i els afectats. També revisa els comunicats públics des d'un punt de vista legal per minimitzar risc de litigis. Si cal emprendre accions legals (p. ex. denúncia a autoritats policials), ell s'encarrega de coordinar-les.

- **Equip Directiu / Comitè de Crisi:** Encara que no formen part de l'ERI en el sentit operatiu, en casos d'incidents crítics (de gran impacte), es formarà un petit comitè amb membres de la direcció (CEO, CTO, etc.) per estar informats en tot moment i prendre decisions estratègiques que van més enllà de l'àmbit tècnic. Per exemple, decidir aturar totalment el servei temporalment per protegir dades, aprovar despeses extraordinàries (com contractar experts externs en forense o comunicació), o fins i tot considerar implicacions legals greus. El Responsable d'Incidents actua de pont entre l'ERI i aquest comitè, facilitant informació i recomanant accions. La direcció, al seu torn, dona suport institucional a les decisions de l'ERI i assegura que la resposta a l'incident s'alinea amb els interessos globals de l'empresa.

- **Contactes externs de suport:** Tot i que no són "rols" interns, cal tenir identificats i pre-establerts contactes amb entitats externes que podrien ajudar en la resposta a incidents: per exemple, una empresa especialitzada en ciberseguretat/forense digital a qui es pugui trucar si l'incident depassa les capacitats internes, o el CERT (equip de resposta a emergències cibernètiques) nacional per notificar incidents greus, o fins i tot les forces de l'ordre (Mossos d'Esquadra o unitats policials especialitzades en delictes informàtics) en cas d'atacs deliberats criminals. Al pla, aquests contactes es llisten amb telèfons d'emergència i persones de referència, per no perdre temps cercant informació durant la crisi.

Fases d'Actuació del Pla de Resposta a Incidents

El procediment de resposta a incidents de seguretat es pot estructurar en diverses **fases sequencials**, inspirades en les millors pràctiques i estàndards internacionals, per tant aquestes son la **Preparació**, **Detecció i Anàlisi**, **Contenció**, **Eradicació**, **Recuperació** i **Aprenentatge/Millora**:

1. **Preparació:** Aquesta fase prèvia ja s'ha exposat en gran mesura en les estratègies de prevenció. Inclou totes les accions *antecedents* que asseguren que, quan es produeixi un incident, l'organització està llesta per respondre. Durant la preparació s'elaboren els plans (com aquest document mateix), es defineixen rols (com s'ha fet més amunt), es dota l'equip de les eines necessàries (sistemes de monitoratge, eines forenses, accessos d'emergència, checklists), i s'entrena el personal en simulacres d'incident. És fonamental que abans que passi res, **tothom sàpiga a qui avisar i què fer inicialment**: per exemple, tenir clar quins contactes trucar a les 3 de la matinada si salta una alerta crítica, o on està el document pas a pas per apagar un servidor de bases de dades sense fer malbé les dades. En el context d'EduTech Global, la fase de preparació significa que ja tenim el SIEM vigilant, que l'equip està format en l'ús d'aquesta eina, que les còpies de seguretat estan al dia, i que disposem d'un llistat actualitzat de tots els sistemes amb els seus responsables. També implica que s'han creat **procediments d'emergència abreujats** (per exemple, guions de "què fer si es detecta una fuga de dades massiva"), de manera que no es comenci de zero en ple caos.

2. **Detecció i Anàlisi:** Aquesta és la fase en què **identifiquem un potencial incident i el diagnostiquem**. Pot començar de diverses maneres: a) a través d'una alerta de seguretat automàtica que indica comportament anòmal; b) mitjançant la notificació d'un usuari o empleat que reporta algun fet (per exemple, un professor indica que veu contingut estrany, o un usuari diu que ha rebut un correu d'EduTech sospitós demanant-li contrasenya – possible phishing); c) o fins i tot per observació manual d'un administrador. Un cop saltada l'alarma, els **analistes de seguretat** agafen el relleu: confirmen si realment és un incident de seguretat. Això implica recollir informació: revisar els logs implicats, reunir evidències del que ha passat, determinar l'abast – quin(s) sistema(es) està(n) afectat(s), des de quan, i quin és l'impacte fins al moment. Si tornem a l'escenari simulat del Repte 1: la fase de detecció va ser l'arribada de l'alerta d'injecció SQL; l'anàlisi consistiria a veure si l'intent va tenir èxit o no (per exemple, revisant logs de la base de dades per veure si es va retornar informació que no tocava, o si l'usuari maliciós va aconseguir algun accés). Un cop confirmat que és un incident (en aquest cas, un intent d'intrusió actiu), l'analista ho comunica immediatament al Responsable d'Incidents i a l'equip ERI, i ja es passa a activar la resposta. **Classificació de l'incident:** com a part de l'anàlisi inicial, es categoritza la gravetat i tipus d'incident (p. ex., *"Intrusió crítica en base de dades, possible fuga de dades personals"* o *"Atac DDoS en curs, degradant el servei"*); això ajuda a decidir quina resposta escalar.

3. **Contenció:** Un cop s'ha identificat un incident i abans no es desenvolupi més, cal posar-hi **contenció per limitar els danys immediats**. La contenció pot ser temporal

o permanent:

- En incidents com una intrusió a la base de dades, la contenció podria consistir en **aïllar el servidor afectat**: per exemple, treure temporalment el servidor de la xarxa (desconnectar-lo o blocar-li l'accés des d'Internet) per evitar que l'atacant segueixi extraient dades. En paral·lel, es podria tallar l'accés a la funcionalitat compromesa de l'aplicació (per exemple, deshabilitar temporalment el formulari vulnerable).

- En cas d'un atac DDoS, la contenció seria **filtrar el trànsit** maliciós: aplicar regles al tallafoc o al proveïdor de serveis perquè descartin les peticions de les IP origen de l'atac, augmentar capacitat si és possible per diluir l'atac, i possiblement activar un servei anti-DDoS tercer. Aquí la contenció busca mantenir operatiu el servei encara que sigui amb rendiment degradat.

- Si es tracta d'un malware/ransomware detectat en un servidor, la contenció seria **desconnectar immediatament aquest servidor de la xarxa** i possiblement apagar-lo (si ja està xifrant fitxers, s'intenta evitar que es propagui o que xifri unitats de xarxa). També pot implicar revocar credencials si es sospita que han estat robades (per exemple, si s'ha comprovat que un compte d'administrador ha estat compromès, es canvia o bloqueja la contrasenya de seguida).

- En qualsevol cas, la contenció té també un vessant de **seguretat de l'evidència**: cal fer-ho de manera controlada per no destruir evidències necessàries per a l'anàlisi. Per exemple, abans de reiniciar o apagar un servidor compromès, l'analista ha d'haver recollit la informació volàtil crucial (processos en execució, connexions de xarxa actives, memòria, etc., si és possible), o fer una imatge de disc si es tracta d'un forense posterior. Aquest equilibri entre tallar l'incident i preservar evidència forma part de l'expertesa de l'equip de seguretat.

- A EduTech Global, s'han de tenir preparades eines de contenció ràpida: scripts per bloquejar accessos, comptes d'emergència per entrar als sistemes i fer tancaments, etc. La contenció és potser la fase més crítica perquè és on es pot evitar que un incident passi de molest a catastròfic. Un cop l'incident està contingut (l'atacant sense accés, el malware aturat, etc.), es pot respirar una mica i passar a la següent fase.

4. **Eradicació:** Un cop estabilitzada la situació, cal **eliminar la causa de l'incident** i qualsevol rastre de l'atac dels sistemes. La diferència amb contenció és que la contenció potser només ha posat un pedaç temporal (per exemple, treure un servidor de producció), però ara cal solucionar l'arrel del problema.

    - En el cas d'una vulnerabilitat explotada (com l'injecció SQL), l'eradicació consistirà a **corregir la vulnerabilitat**: aplicar el pegat de programari, reconfigurar el sistema, o actualitzar el que calgui. En el nostre exemple, això significaria arreglar el codi de l'aplicació perquè no accepti més aquella

injecció (p. ex., sanititzar l'input o posar la consulta preparada) abans de tornar a posar el servidor en producció. També pot incloure passos com instal·lar pegats de seguretat si l'atac va aprofitar un bug del sistema operatiu o del SGBD.

- Si l'incident era un malware, l'eradicació és **eliminar el malware** de tots els sistemes afectats: fer escanejos complets, reimaginar màquines si cal per estar segurs que no queda cap *backdoor*, i actualitzar signatures antivirus perquè no reentri.

- Si hi va haver comptes compromesos, l'eradicació és **canviar o revocar credencials**, assegurant que l'atacant ja no tingui cap accés. També revisar configuracions d'accés per evitar que la mateixa tècnica (p. ex., phishing) pugui ser tan efectiva de nou.

- Altres tasques d'eradicació: esborrar o neutralitzar codi maliciós inserit (per exemple, si l'atacant va deixar un *web shell* a la plataforma, cal trobar-lo i eliminar-lo), sanejar bases de dades si van ser corrompudes (assegurar integritat de les dades), etc.

- Durant aquesta fase és molt important que la solució implementada no introdueixi nous problemes. Sovint es fan proves abans de declarar completada l'eradicació: per exemple, testejar que la vulnerabilitat ja no és explotable (repetint l'exploit en un entorn de prova) o que el malware ja no reapareix. A EduTech Global, l'eradicació serà fruit del treball conjunt dels admins i desenvolupadors, seguint les prioritats marcades. Només un cop satisfets que l'amenaça s'ha eliminat es passa a recuperar la normalitat.

5. **Recuperació:** Aquesta fase consisteix a **restaurar els sistemes i serveis a la normalitat** assegurant-nos que l'incident no es repeteix immediatament. Si durant contenció es van apagar o aïllar sistemes, ara cal tornar-los a posar en funcionament de manera controlada.

    - En un cas de ciberatac tipus intrusió, potser es decideix reinstal·lar des de zero un servidor compromès per confiança, aplicant-li després les correccions abans de reconnectar-lo a la xarxa de producció. Un cop fet, es reintegra i es comprova que tot funciona (testing complet de l'aplicació).

    - Si hi va haver pèrdua o corrupció de dades, és en aquesta fase quan es fan **restauracions de backup**. Per exemple, si un ransomware va xifrar la base de dades, un cop eliminat el malware (eradicació) es restaura la base de dades des de la còpia de seguretat més recent no afectada i es verifica la consistència. És possible que es perdi alguna dada recent si el backup no és totalment al dia, però és preferible a mantenir dades xifrades i inaccessibles.

    - En un atac DDoS, la recuperació seria monitoritzar la finalització de l'atac i anar retirant mesures temporals un cop s'estigui segur que el trànsit torna a nivells normals. Per exemple, reactivar serveis opcionals que s'havien

desconnectat per alleugerir càrrega, o reobrir registres si s'havien tancat preventivament.

- Abans de tornar a la normalitat plena, l'equip de seguretat pot fer un **escaneig final** als sistemes per cerciorar-se que no queden portes del darrere ni usuaris estranys creats durant l'incident. També cal mantenir un monitoratge intensiu en els primers dies posteriors a la recuperació, per detectar qualsevol símptoma que l'atac reapareix (de vegades, atacants tornen a intentar aprofitar la mateixa bretxa, per això és crucial haver-la resolt).

- La recuperació no es considera completa fins que: tots els serveis funcionen correctament, els usuaris poden fer servir la plataforma sense problemes, s'ha confirmat que les dades estan integres, i els temps de resposta i rendiment són òptims. Aleshores es pot declarar l'incident com a resolt/desactivat i procedir a la darrera fase.

6. **Aprenentatge i Millora (Post-Incident):** Un cop acabada la gestió immediata, és imprescindible dedicar temps a **analitzar l'incident a fons** i extreure'n lliçons. Aquesta fase de vegades s'anomena *"lessons learned"*. A EduTech Global es convocarà una reunió post-mortem amb tots els involucrats (membres del ERI i direcció si escau) per revisar:

   - **Causes arrel** de l'incident: Què va permetre que passés? (p. ex., "no es va actualitzar un component X a temps", o "l'usuari va caure en phishing perquè no havia tingut prou formació", etc.).

   - **Eficàcia de la resposta:** Com va funcionar el pla? Es va detectar l'incident prou aviat? Les comunicacions internes van ser fluids? Es van seguir els procediments o hi va haver confusió? Cada responsable sabia què fer? Es va contenir prou ràpid? Qualsevol problema o retard identificat aquí s'ha de documentar i corregir en el pla per al futur.

   - **Dany real sofert:** Quant data es va perdre o exposar? Quin va ser l'impacte en usuaris (temps d'inactivitat, etc.)? Això és important també per actualitzar l'anàlisi de riscos: si un tipus d'incident va ser més costós de l'esperat, cal pujar-li la prioritat o replantejar mesures preventives.

   - **Actualització de documentació i mesures:** Un resultat d'aquesta fase és actualitzar el **pla de resposta a incidents** si cal, incorporant-hi els ajustos detectats. També actualitzar altres polítiques o procediments relacionats. Per exemple, arran d'un incident es podria decidir "cal implementar una prova de phishing semestral als empleats" si es va veure que el factor humà va fallar, i això es reflecteix en el pla de conscienciació. O "cal contractar un servei de monitoratge 24h" si l'incident va ocórrer fora de l'horari i va trigar hores a ser notat.

- **Informe final i comunicació:** Es prepara un informe complet de l'incident, que pot ser compartit amb la direcció i altres parts interessades. Si és exigible per llei o per compromís amb els usuaris, es farà un comunicat públic transparent explicant en termes generals què va passar i quines mesures s'han pres per evitar que torni a succeir (per exemple, després d'una fuga de dades, és habitual informar els usuaris afectats de quines dades van ser exposades i oferir ajuda com supervisió de crèdit si s'escau, etc.).

- **Seguiment:** Potser caldrà fer un seguiment de certs aspectes: si s'han de notificar entitats reguladores, assegurar-se que es faci; si es va obrir una investigació policial, cooperar subministrant logs i proves; si es van prometre millores a clients, complir-les en el termini dit.

Gestió de la Comunicació durant els Incidents

Comunicar de manera adequada pot mitigar danys reputacionals, mantenir la confiança dels usuaris i evitar malentesos o especulacions, per tant, els protocols de comunicació són els següents:

- **Comunicació interna (dins de l'equip i empresa):** Des del moment en què es detecta un incident, l'Incident Manager ha d'assegurar que tots els membres pertinents de l'ERI estan informats i coordinats (a través d'un canal segur, ja sigui un xat xifrat d'empresa, trucades, etc.). S'utilitzarà una llista de distribució d'emergència o grup de missatgeria específic per incidents on es donaran actualitzacions freqüents. A més, segons la gravetat, es notificarà la direcció executiva de forma resumida (per exemple, *"Hem detectat un accés no autoritzat a la base de dades, estem actuant, us mantindrem informats cada hora"*). És important evitar filtracions d'informació inexacta: s'indicarà al personal que l'incident està sent gestionat i que no divulguin res per compte propi. Si l'incident impacta operativament (p. ex., s'ha de desconnectar un servei intern), també es comunica als empleats de l'empresa perquè ho sàpiguen i, si cal, ajudin amb contingències (com ara atendre trucades de clients preocupats, etc.).

- **Comunicació externa (usuaris, clients, autoritats):** Depenent del tipus d'incident, caldrà informar entitats fora de l'empresa:

    - *Notificació a usuaris afectats:* Si hi ha hagut una **violació de dades personals** o informació sensible d'usuaris, el RGPD obliga a notificar els afectats sense demora injustificada quan la brexa pot comportar un alt risc pels seus drets. Per tant, EduTech Global enviaria comunicacions (correus electrònics segurs, per exemple) a tots els usuaris involucrats explicant què ha passat a grans trets, quines dades els concerneixen s'han vist compromeses i oferint recomanacions (canvi de contrasenya, vigilància de comptes, etc.). El to ha de ser transparent i proactiu, mostrant empatia i explicant les mesures preses per solucionar-ho.

- *Notificació a autoritats reguladores:* Igualment sota RGPD, si l'incident suposa fuga de dades personals, s'ha de notificar a l'autoritat de protecció de dades (APD) en menys de 72 hores. El representant legal prepararà aquest informe formal, que inclou la naturalesa de la informació robada, el nombre de afectats, les conseqüències i mesures adoptades. En casos d'atacs greus, també es pot notificar a forces de l'ordre; per exemple, si va ser un sabotatge o un atac d'extorsió (ransomware amb petició de rescat), convé informar la policia.

- *Comunicació pública i premsa:* Si l'incident té transcendència pública (per exemple, la plataforma ha estat caiguda diverses hores per un DDoS en ple període d'exàmens, i molts ho comenten a xarxes), o si implica dades de moltes persones, és millor **controlar el relat** abans no es filtrin històries incompletes. S'emetrà una nota de premsa o publicació al web oficial i xarxes socials d'EduTech Global admetent l'incident de forma transparent, indicant que s'està investigant i les mesures dutes a terme, i que es proporcionarà més informació quan estigui disponible. Cal evitar donar més detalls dels necessaris (sobretot tècnics que puguin ajudar altres atacants), però sí transmetre compromís amb la seguretat i penediment per les molèsties. Per exemple: *"Aquest matí la nostra plataforma ha patit una incidència de seguretat que ha provocat la interrupció temporal del servei. El nostre equip tècnic ha contingut la incidència i està treballant per restablir completament les funcionalitats. Mantindrem informada la comunitat un cop conclogui la investigació. La seguretat dels nostres usuaris és la nostra màxima prioritat i ja hem pres mesures addicionals per evitar que torni a succeir."* Aquest tipus de comunicats ajuden a frenar especulacions i mostrar control de la situació.

- *Canals de suport als usuaris:* Si l'incident afecta el funcionament, s'habilitarà un canal d'informació constant per als usuaris, com ara una pàgina d'estat en línia actualitzada o una línia telefònica especial, on puguin consultar novetats i temps estimat de recuperació. En cas de fuga de dades, també es pot establir un email o hotline perquè els usuaris fagin preguntes i sels respongui personalment les seves preocupacions.

- **Coherència i rapidesa:** Totes les comunicacions han de ser **consistents** entre elles i emeses en temps oportú. Per això, l'Enllaç de Comunicacions treballa el missatge en conjunt per diferents audiències, però mantenint el mateix contingut bàsic. També és vital no esperar massa: en seguretat, la percepció del públic pot empitjorar si sembla que l'empresa ha amagat l'incident. Millor comunicar aviat allò que es conegui, i després actualitzar a mesura que se sàpiguen més detalls, que no pas deixar un silenci prolongat.

- **Després de l'incident:** Un cop resolt, comunicar el tancament i les mesures preses és igualment important. Agrair la paciència dels usuaris, informar que els serveis tornen a la normalitat i que s'han implementat millores (sense entrar en detalls que exposin la seguretat). Això tanca el cicle de comunicació i restaura la confiança.

Pla de Contingència i Continuïtat del Negoci

Mentre el pla de resposta a incidents se centra en lidiar amb l'incident en sí, el **Pla de Contingència** complementa aquesta resposta enfocant-se en garantir que l'empresa pugui continuar operant o reprendre operacions tan aviat com sigui possible. És a dir, contempla escenaris en què un incident greu podria fer inútil l'entorn habitual i caldrien alternatives per mantenir els serveis essencials.

- **Identificació de processos crítics i requisits de disponibilitat:** S'ha determinat que els serveis més crítics a preservar són: la plataforma d'aula virtual (accés a materials, lliçons en línia), el mòdul d'exàmens i avaluacions, i el sistema d'inscripció de cursos. Aquests processos tenen uns **objectius de temps de recuperació (RTO)** molt curts (idealment menys de 1 o 2 hores en cas de caiguda) i un **objectiu de punt de recuperació (RPO)** també molt baix (no es poden perdre dades d'avaluacions o inscripcions, potser com a màxim les de uns pocs minuts). Això estableix la base per planificar la redundància i recuperació de dades.

- **Infraestructura redundant i recuperació de desastres:** En la mesura del possible, es manté una infraestructura **redundant**:

    - Servidors en clúster o rèplica: la base de dades d'usuaris podria tenir una rèplica en temps real en un servidor secundari o al núvol, de manera que si el servidor principal falla (ja sigui per un atac o per qualsevol fallada), el servei pot commutar al secundari. Igualment, els servidors d'aplicacions es poden tenir en configuració d'equilibrat de càrrega actiu-actiu, de forma que la fallada d'un no interrompi el servei.

    - Còpies de seguretat fora de seu: a part dels backups locals, mantenir còpies en un entorn geogràficament separat (per exemple, en un cloud segur o en un centre de dades diferent). Això protegeix davant desastres físics o incidents que comprometin totalment la xarxa local.

    - Pla de recuperació de desastres (DR): document que indica com restaurar tot el sistema en un entorn nou en cas de destrucció de l'actual. Inclou tenir scripts d'infraestructura-com-a-codi per redeployar servidors al núvol si cal, disposar de llicències, claus i instal·ladors a mà, etc. És un escenari extrem però ha de ser considerat (p. ex., un atac massiu combinat amb sabotatge físic que deixés inoperants els servidors on resideix la plataforma).

    - SAI i protecció elèctrica: per esgotivitat, també es contempla tenir Sistemes d'Alimentació Ininterrompuda i generadors per evitar caigudes per talls elèctrics, i línies de comunicació alternatives per si falla la principal d'internet.

- **Procediments de continuïtat durant un incident:** Sovint, encara que hi hagi redundància, un incident pot requerir operar en **mode degradat** durant un temps. El pla defineix com es treballaria en aquests casos. Per exemple:

- Si la base de dades principal està desconnectada per un atac i es tarda unes hores en restaurar-la, potser es decideix posar la plataforma en mode "només lectura" utilitzant la darrera còpia de seguretat (avisant els usuaris que els canvis no es guardaran fins a nou avís). Això almenys permet consultar materials encara que no es puguin entregar tasques noves.

- Si el sistema d'exàmens queda inutilitzat el dia d'una prova important, el pla de contingència podria contemplar alternatives com habilitar temporalment una eina externa de qüestionaris o, si cal, ajornar l'examen enviant notificacions massives als afectats i ampliant terminis. Són decisions de negoci/acadèmiques que han d'estar predefinides per no improvisar en calent.

- En cas d'un atac DDoS prolongat, treballar amb el proveïdor per re-rutar trànsit, però si malgrat tot el servei està inestable, tenir una pàgina web estàtica de contingència allotjada en un proveïdor extern on els usuaris puguin almenys veure comunicats i instruccions (per exemple, una pàgina senzilla que informi que *"la plataforma està patint dificultats tècniques, estem treballant en la recuperació, mentre tant podeu accedir a materials urgents en aquest altre enllaç provisional..."*). D'aquesta manera es manté la comunicació i certa funcionalitat mínima.

- Mantenir priorització de recursos: el pla també defineix que, en situacions de recursos limitats, es prioritzaran els serveis de més valor. Per exemple, si només podem mantenir un servidor en línia, prioritzarem la base de dades d'usuaris i portal de curs sobre serveis secundaris com el portal públic de màrqueting.

- **Responsabilitats i decisió de declaració de desastre:** Ha de quedar clar qui i quan es "premen els botons" de contingència. Per exemple, el Responsable d'Incidents pot recomanar passar al centre de dades alternatiu, però segurament aquesta decisió l'aprovarà la direcció un cop avaluat que la interrupció serà llarga. El pla estableix triggers: *"Si transcorregudes 2 hores des de l'inici de l'incident no s'ha pogut restablir el servei principal, es considerarà invocar el pla de recuperació de desastres i migrar a la infraestructura de contingència"*. També llista qui executa tècnicament aquesta migració i com s'informa els usuaris.

- **Documentació de continuïtat i tests:** Tota aquesta planificació ha d'estar documentada i, important, **provada prèviament**. Igual com es fan simulacres d'incident, cal fer simulacres de contingència: per exemple, un cop l'any fer una restauració simulada de tot el sistema en entorn de test només a partir de backups, per veure quant es triga i què falla; o provar durant un cap de setmana de baix ús de commutar voluntàriament al servidor secundari per comprovar que realment la rèplica funciona. Aquests exercicis revelaran problemes insospitats i donaran confiança que en cas real el pla funcionarà.

Millora Contínua de la Seguretat i el Pla

La seguretat informàtica no és un assoliment estàtic sinó un **procés dinàmic**. Tant les amenaces com la pròpia empresa evolucionen constantment: poden aparèixer noves tecnologies, es desenvolupen nous vectors d'atac, i alhora EduTech Global pot ampliar serveis o funcionalitats que requereixin revisar els enfocaments de seguretat. Per això, un component final però essencial del pla és establir una **millora contínua**.

Per tant, els mecanismes de millora contínua inclouen:

- **Revisió periòdica del Pla de Resposta a Incidents:** Cal programar, com a mínim anualment, una revisió completa del present pla. Això implicarà repassar tots els apartats (riscos, rols, contactes, procediments) i actualitzar-los segons l'experiència dels incidents soferts i canvis en l'organització. Si, per exemple, l'empresa creix i es crea un nou departament, potser cal incloure'l en la cadena de comunicació; si s'adopta una nova eina de monitoratge, incorporar-la al procés; etc. També assegurar-se que els noms i telèfons de contacte són actuals.

- **Simulacres i exercicis regulars:** A banda dels incidents reals, és molt recomanable fer **drills** o simulacres controlats per posar a prova l'equip i el pla. Es poden fer *table-top exercises* (exercicis de taula) on es proposa un escenari hipotètic i es discuteix què faria cadascú, o fins i tot simulacions en viu (amb acord previ de la direcció) on l'equip tècnic rep una alerta simulada i ha d'actuar com si fos real. Després, s'avalua el rendiment i es detecten mancances: potser es veu que no sabien on estava un telèfon d'emergència, o que van trigar massa a analitzar perquè una eina no estava ben configurada, etc. Aquestes pràctiques entrenen l'equip i alhora serveixen per polir detalls del pla.

- **Actualització tecnològica contínua:** La integració de noves eines que millorin la seguretat ha de ser un esforç constant. Per exemple, podríem estudiar la incorporació de sistemes de detecció basats en intel·ligència artificial que aprenguin el patró normal d'ús de la plataforma i alertin d'activitats inusuals més enllà de les regles predefinides. També, si en el futur es desenvolupa el sistema *EduMind* d'IA educativa, caldrà incloure'l tant en monitoratge (logs de decisions de la IA, etc.) com en els plans de resposta (què fer si hi ha un mal funcionament o exploit a la IA). La seguretat ha d'anar de bracet amb la innovació: per cada nova feature, pensar en els riscos associats i com es controlaran.

- **Recollida d'indicadors i metriques:** Per avaluar la millora, es definiran alguns **KPIs de seguretat**. Per exemple: número d'incidents per trimestre (esperem que disminueixi o almenys que els greus disminueixin), temps de resposta mitjà des de detecció fins contenció, temps de recuperació mitjà, nombre de vulnerabilitats crítiques obertes detectades en escanejos, etc. Es farà seguiment d'aquests indicadors en reunions de seguretat i es fixaran objectius (p. ex., reduir el temps de detecció a menys de 15 minuts de mitjana). Si els objectius no es compleixen, analitzar per què i introduir millores (més personal, millor formació, eines diferents...).

- **Cultura de seguretat i aprenentatge:** Promoure una cultura on els **empleats comparteixin les incidències o quasi-incidents** (p. ex., algú rep un phishing però se n'adona, igualment que ho comuniqui per aprendre'n tots) sense por a represàlies, sinó veient-ho com oportunitat d'aprenentatge. També mantenir-se al dia amb la comunitat de ciberseguretat, assistint a conferències, obtenint certificacions, aprenent de casos d'altres organitzacions. Això permetrà anticipar-se a noves tendències d'amenaces i tenir el pla preparat per a escenaris que potser encara no hem viscut però són potencials.

Conclusions

Al llarg d'aquesta Pràctica s'han abordat amb detall els dos reptes proposats per la direcció d'EduTech Global, amb l'objectiu de reforçar la protecció del nostre entorn digital. En el primer repte, centrat en l'auditoria d'un actiu crític, s'ha dut a terme una anàlisi exhaustiva de la base de dades d'usuaris, on s'ha detectat una vulnerabilitat rellevant d'injecció SQL. Tot i que inicialment es pretenia utilitzar Wazuh com a eina de monitorització, problemes tècnics van impedir-ne el desplegament efectiu. Malgrat això, la detecció de l'intent d'intrusió es va poder dur a terme mitjançant una revisió manual dels logs, que va proporcionar evidències clares de l'activitat sospitosa. Aquesta auditoria ha estat clau per corregir punts febles concrets i, alhora, per enfortir l'alineament del sistema amb la normativa vigent i les bones pràctiques de seguretat..

En el **Repte 2 (Pla de Resposta a Incidents i Contingència)** hem desenvolupat un pla integral que prepara EduTech Global per fer front a una varietat d'incidents, des de ciberatacs deliberats fins a contratemps operatius, assegurant que la continuïtat de l'educació en línia que oferim als nostres usuaris no es vegi compromesa. S'han definit clarament els procediments a seguir, els rols de cada membre de l'equip en situacions crítiques, i les mesures de comunicació i contingència per minimitzar l'impacte tant en l'organització com en els nostres estudiants i docents. El pla s'ha concebut de manera alineada amb els estàndards internacionals i amb una visió de millora constant, cosa que ens permetrà adaptar-nos davant nous reptes de seguretat en el futur.

En conjunt, les accions realitzades i planificades consoliden la **postura de seguretat** d'EduTech Global. Hem passat de tenir un model teòric i unes mesures inicials (Pràctica 1) a verificar en la pràctica la seva eficàcia i a dotar l'organització d'un marc robust per reaccionar quan les defenses es vegin posades a prova. Amb això, EduTech Global reforça el seu compromís amb la seguretat i la confiança: tant els usuaris poden sentir-se més segurs utilitzant la nostra plataforma, com la direcció pot estar tranquil·la sabent que la protecció dels actius digitals i la continuïtat del negoci estan planificades i sota control.

La seguretat és un viatge continu, però els passos donats en aquesta pràctica representen un avanç significatiu cap a una **infrastructura educativa en línia segura, resilient i confiable**, mantenint EduTech Global a l'avantguarda com a plataforma líder en educació en línia en un món ple de reptes cibernètics. Hem establert una base sòlida perquè, passi el que passi, l'aprenentatge dels nostres usuaris continuï sense interrupcions i amb la garantia que les seves dades i experiència estan protegides al màxim nivell possible.

Annex: Captures de pantalla

Figura 1: Captura de la pàgina SQL Injection de DVWA abans de l'execució de l'atac. A la part esquerra s'observa el formulari vulnerable on s'ha introduït el payload d'injecció (1' OR '1'='1) en el camp "User ID". En aquest punt, l'usuari maliciós està a punt d'enviar la petició amb la condició alterada. A la dreta, la consola del servidor mostra la sessió MySQL i configuracions prèvies (per exemple, les ordres per atorgar privilegis a l'usuari dvwa sobre la base de dades), preparant l'entorn perquè l'aplicació funcioni i permeti la prova.

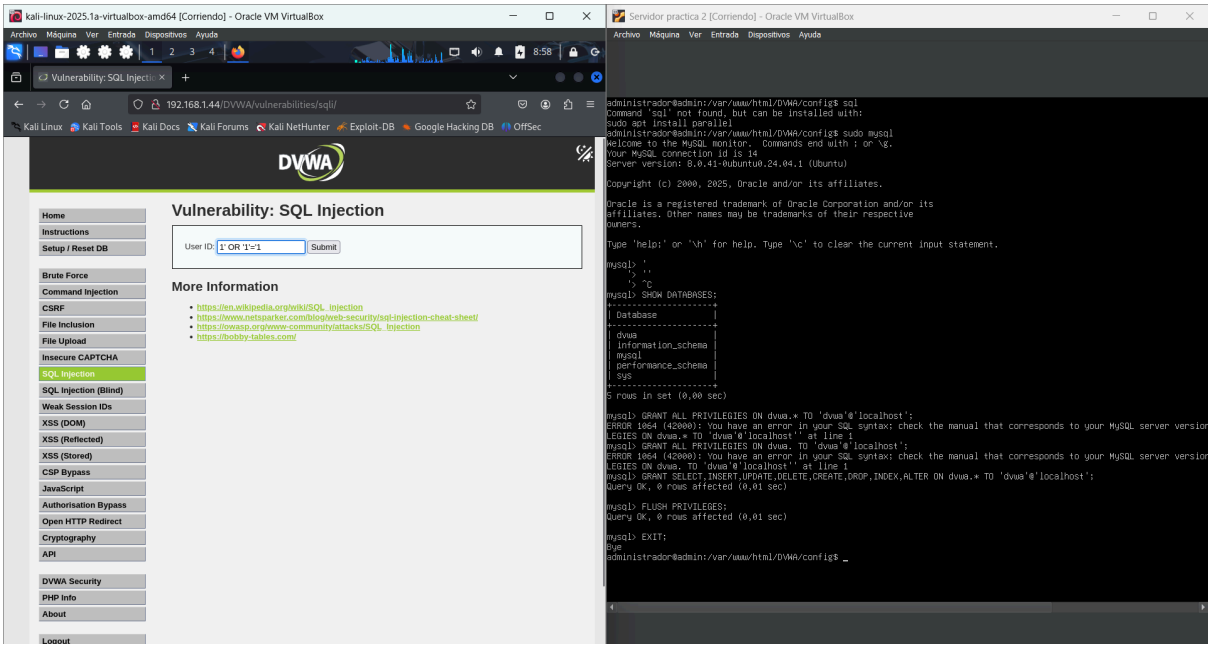

Figura 2: Resultat de la injecció SQL a DVWA. Després d'enviar el payload, la pàgina retorna múltiples entrades de la base de dades d'usuaris. Es poden veure diversos ID d'usuari amb els seus noms i cognoms (en vermell a la interfície de DVWA), incloent l'administrador i usuaris de prova. El fet que es mostrin tots aquests resultats confirma que la consulta SQL original ha estat manipulada amb èxit per incloure una condició sempre certa, extraient tots els registres. En un entorn real, aquesta fuga de dades suposaria una greu violació de seguretat, ja que informació sensible de múltiples usuaris queda exposada.

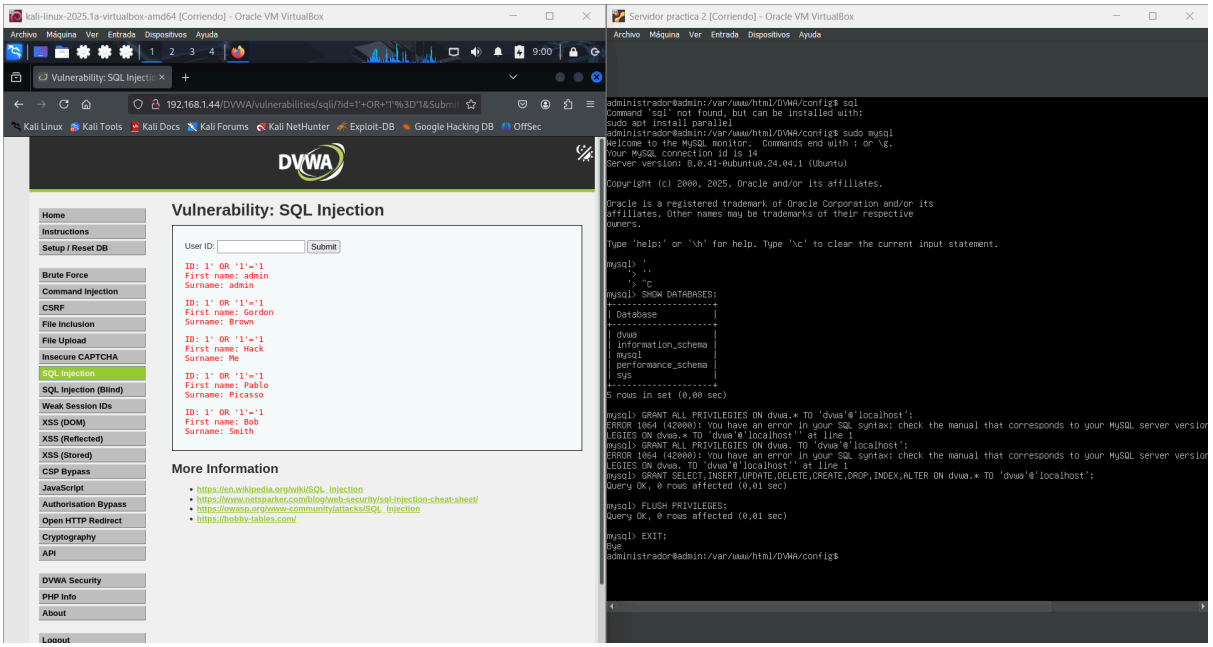

Figura 3: Registre d'accés d'Apache capturat durant l'atac (extracte). A la finestra de la dreta es mostra la sortida de la comanda tail -f /var/log/apache2/access.log al servidor durant la simulació. S'hi destaca la petició GET provenint de la IP de l'atacant (192.168.1.43) cap al recurs vulnerable, amb el paràmetre id manipulat (id=1' OR '1'='1) codificat en URL. El servidor respon amb codi 200 (OK), indicant que ha processat la petició. Aquesta línia de log és un indicador clar de l'intent d'injecció SQL i, en un desplegament de monitorització operatiu, hauria generat una alerta. La supervisió manual del registre en aquest cas ha permès comprovar que l'atac quedava registrat.

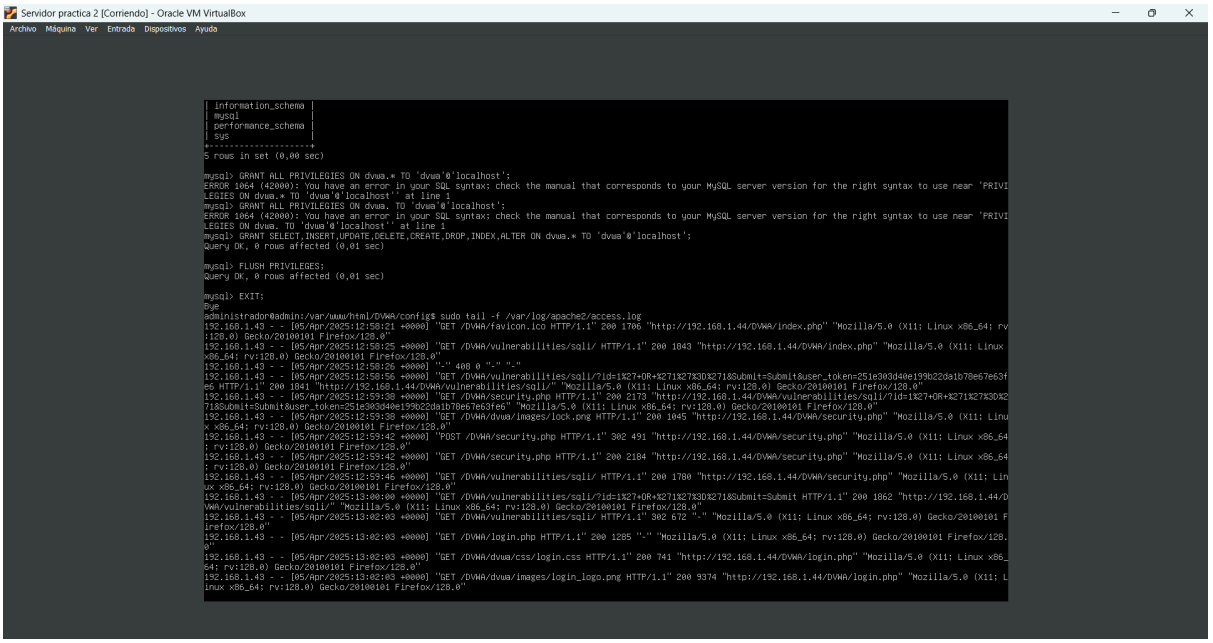

Figura 4: Intent d'accés als registres de Wazuh sense èxit. En aquesta captura es veu la consola del servidor en intentar llegir el fitxer de log de l'indexador de Wazuh (/var/log/wazuh-indexer/wazuh-indexer.log). El sistema retorna un missatge d'error indicant que el fitxer no existeix, la qual cosa reflecteix que el component Wazuh Indexer (encarregat d'emmagatzemar i indexar els esdeveniments) no està funcionant o instal·lat correctament. Aquesta limitació ha impedit disposar de les funcionalitats completes de detecció automàtica durant la prova, ressaltant la necessitat de configurar adequadament totes les parts de la plataforma SIEM. Aquesta limitació evidencia que Wazuh no va estar operatiu durant la prova, cosa que va obligar a fer la detecció de manera manual.