EduTech Global

Pràctica 1: Estratègia de Ciberseguretat

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

ÍNDEX

Introducció

En l'actual context digitalitzat, les organitzacions que gestionen grans volums d'informació crítica han d'adoptar mesures avançades de ciberseguretat per protegir adequadament els seus actius digitals. EduTech Global, com a plataforma educativa en línia amb presència global, afronta un repte complex i essencial en matèria de seguretat de la informació.

Aquesta pràctica té com a objectiu plantejar una estratègia integral de ciberseguretat adaptada específicament al context i les necessitats d'EduTech Global. En primer lloc, es realitzarà una anàlisi exhaustiva del model de negoci de la plataforma per entendre millor les seves necessitats específiques i el context operatiu on es desenvolupa. A continuació, es definiran detalladament els riscos i vulnerabilitats associats a les seves operacions digitals.

A partir d'aquesta anàlisi, es proposarà un model general de control d'accessos que integri els elements més efectius per protegir adequadament la informació confidencial, així com una arquitectura de xarxa robusta i segura. També es presentarà una estimació econòmica que reflecteixi els costos tant d'implementació com de manteniment d'aquesta infraestructura.

Finalment, s'abordaran les polítiques específiques de seguretat i el model detallat de control d'accessos escollit, garantint la conformitat amb regulacions internacionals com la GDPR i la FERPA. Tot això amb l'objectiu d'enfortir la plataforma davant possibles amenaces, protegint així la confiança dels usuaris i assegurant l'èxit continuat d'EduTech Global en l'àmbit de l'educació digital.

Anàlisi del Model de Negoci i Context d'EduTech Global

EduTech Global és una plataforma educativa en línia que ofereix formació des de l'educació primària fins al nivell universitari i professional, adaptant-se a diverses necessitats educatives en un context global. La seva proposta es basa en la democratització del coneixement mitjançant eines digitals accessibles que permeten als estudiants aprendre de manera flexible, independentment de la seva ubicació geogràfica.

La plataforma compta amb una extensa base de dades que inclou informació sensible d'estudiants, professors i administradors, així com un ampli catàleg de material educatiu protegit per drets d'autor. El seu model es fonamenta en oferir cursos en diverses disciplines acadèmiques, des de l'educació bàsica fins a la formació professional avançada, incloent-hi àrees com programació, ciències, matemàtiques, disseny gràfic i gestió empresarial.

Entre els elements clau destaquen:

- **Flexibilitat educativa**: Permet personalitzar l'aprenentatge, adaptant-se al ritme i preferències individuals.
- **Interactivitat**: Utilitza eines com fòrums, avaluacions interactives i contingut multimèdia per millorar l'experiència educativa.
- **Accés global**: Facilita l'accés a una educació de qualitat a estudiants de qualsevol lloc del món.
- **Gestió eficient de l'aprenentatge**: Proporciona als professors eines avançades per monitoritzar i adaptar l'ensenyament a les necessitats individuals dels alumnes.

Necessitats específiques de ciberseguretat:

EduTech Global afronta reptes específics relacionats amb la gestió segura i eficient de la informació personal, educativa i financera dels seus usuaris, havent d'assegurar:

- **Privacitat i protecció de dades personals**: Implementació de xifratge robust tant per dades en trànsit com en repòs.
- **Accessos segurs i diferenciats**: Sistemes que permetin gestionar clarament els diferents nivells d'accés segons els rols dels usuaris.
- **Compliment regulador internacional**: Garantir la conformitat amb regulacions com la GDPR (Europa) i la FERPA (EE.UU.).
- **Gestió segura de continguts educatius**: Protecció contra la pirateria mitjançant mecanismes com DRM.
- **Capacitat per gestionar trànsit elevat**: Especialment durant períodes crítics com exàmens o inscripcions massives.

Identificació de Riscos i Vulnerabilitats d'EduTech Global

Atès el context operatiu i el model de negoci d'EduTech Global, s'han identificat els següents riscos i vulnerabilitats específiques que podrien afectar la seguretat de la informació i l'operació eficient de la plataforma:

Riscos relacionats amb la protecció de dades

- **Violació de dades personals**: Possibles atacs informàtics que podrien comprometre la confidencialitat de les dades sensibles dels estudiants i del personal.
- **Incompliment de normatives de privacitat**: Possibilitat d'incompliment involuntari de normatives internacionals com GDPR i FERPA, podent comportar sancions legals i pèrdua de reputació.

Riscos associats a l'accés i control d'usuaris

- **Accessos no autoritzats**: Risc d'intrusió per part d'usuaris no autoritzats a continguts educatius protegits, afectant la integritat dels materials educatius i els ingressos econòmics.
- **Gestió deficient de permisos**: Una assignació incorrecta de permisos podria permetre accés inadequat a informació sensible per part de personal intern, professors o alumnes.

Vulnerabilitats tècniques i operatives

- **Sobrecàrrega del sistema**: Vulnerabilitat davant augments sobtats de tràfic, especialment durant períodes intensos com exàmens i matrícules, podent provocar interrupcions del servei.
- **Deficiències en el xifratge i emmagatzematge**: Possibles punts febles en el xifratge de dades en trànsit i en repòs que podrien ser explotats per atacs informàtics.

Riscos relacionats amb la propietat intel·lectual

- **Pirateria de contingut educatiu**: L'absència o insuficiència de mecanismes efectius de DRM pot facilitar la còpia no autoritzada i distribució il·legal del contingut educatiu, impactant negativament els ingressos i la reputació.

Vulnerabilitats humanes i operatives

- **Errors humans en la gestió de dades**: Errors accidentals per part dels administradors o professors que podrien exposar dades sensibles de manera no intencionada.
- **Manca de conscienciació en ciberseguretat**: Baixa formació i conscienciació en ciberseguretat per part d'usuaris i administradors podria afavorir la incidència de phishing o enginyeria social.

Model General Teòric de Control d'Accessos per EduTech Global

Per garantir una gestió segura, robusta i eficient dels recursos d'informació d'EduTech Global, proposem l'aplicació d'un model general teòric de control d'accessos basat en la combinació dels següents elements fonamentals:

Control d'Accés Basat en Rols (RBAC)

Aquest model assigna permisos d'accés segons rols específics definits dins de la plataforma (estudiants, professors, administradors). Facilita una gestió senzilla i eficient, ja que permet assignar permisos a grups amplis d'usuaris segons les seves funcions específiques.

Control d'Accés Basat en Atributs (ABAC)

Per complementar el RBAC, especialment en escenaris més complexos o dinàmics, es proposa implementar ABAC. Aquest model permet prendre decisions dinàmiques d'accés segons atributs contextuals com la localització geogràfica, tipus de dispositiu o moment d'accés.

Principi de Privilegi Mínim

Aplicació estricta d'aquest principi per garantir que cada usuari tingui exclusivament els permisos necessaris per realitzar les seves tasques, minimitzant així els riscos derivats d'accessos inadequats.

Segregació de Funcions

Establir una clara separació de rols per prevenir conflictes d'interès i reduir el risc d'errors o activitats fraudulentes internes. Per exemple, separar clarament les responsabilitats d'administració de sistemes, gestió educativa i accés a dades financeres sensibles.

Model Híbrid d'Identificació i Autenticació

- **Autenticació Multifactor (MFA)**: Incorporació obligatòria de MFA per a tots els accessos sensibles o administratius, reforçant així la seguretat d'accés.
- **Biometria selectiva**: Consideració de l'ús de biometria per garantir encara més la integritat en situacions especialment crítiques o vulnerables.

Gestió de Drets Digitals (DRM)

Implementació avançada de gestió de drets digitals per assegurar la propietat intel·lectual del contingut educatiu, impedint còpies no autoritzades i l'accés il·legítim als materials educatius.

Arquitectura de Xarxa Proposada per EduTech Global

Per protegir adequadament els recursos digitals d'EduTech Global i garantir la integritat i confidencialitat de les dades, proposem la següent arquitectura de xarxa segura:

Components Principals:

- **Zona Pública (DMZ):**
    - Servidors web accessibles públicament per als usuaris finals, amb balancejadors de càrrega per gestionar pics d'activitat.
    - Sistemes de mitigació d'atacs DDoS per protegir davant altes càrregues durant períodes crítics.
- **Zona Privada (Intranet)**:
    - Contindrà servidors d'aplicacions i bases de dades sensibles, només accessibles mitjançant canals segurs i autenticació multifactor.
    - Sistemes de control d'accessos robustos per gestionar rols específics (estudiants, professors, administradors).
- **Zona d'Administració**:
    - Àrea exclusiva per a administradors i gestors de TI, protegida amb mesures de seguretat addicionals com accés VPN dedicat i monitorització contínua.

Dispositius de Seguretat:

- **Firewall de nova generació (NGFW)**:
    - Supervisió avançada del trànsit de xarxa, detecció d'amenaces en temps real i protecció contra intrusions.
- **Sistema de Prevenció d'Intrusions (IPS)**:
    - Integrat amb el firewall per bloquejar automàticament activitats sospitoses o malicioses.
- **Servidor VPN**:
    - Permetrà accessos remots segurs i protegits, especialment per administradors i professors amb accés a dades sensibles.
- **Balancejadors de càrrega (Load Balancers)**:
    - Distribució eficaç del trànsit per assegurar alta disponibilitat, especialment durant períodes de tràfic intens.

Comunicacions Segures:

- **Xifratge de dades en trànsit** mitjançant TLS/SSL.
- **Xifratge de dades en repòs** mitjançant protocols avançats de xifrat AES.

Monitoratge i Auditoria:

- Sistemes centralitzats per al monitoratge continu, identificant en temps real possibles vulnerabilitats i incidents.
- Realització periòdica d'auditories de seguretat per validar la integritat i eficàcia de la infraestructura.

Proposta Econòmica d'Implementació per EduTech Global

A continuació es detalla la proposta econòmica d'implementació per EduTech Global, especificant clarament els costos inicials de dispositius i hores de treball, així com les despeses anuals estimades per al manteniment de la infraestructura de ciberseguretat proposada.

Cost Inicial dels Dispositius

Component	Quantitat	Cost Unitari (€)	Cost Total (€)
Firewall de nova generació (NGFW)	2	8.000 €	16.000 €
Sistema de Prevenció d'Intrusions (IPS)	1	5.000 €	5.000 €
Balancejadors de càrrega	2	3.000 €	6.000 €
Servidors VPN	2	2.500 €	5.000 €
Sistema DRM avançat	1	8.000 €	8.000 €
Software MFA (llicència anual inicial)	1	2.000 €	2.000 €
Total			**40.000 €**

Cost Inicial en Hores de Treball

Tasca	Hores	Cost/hora (€)	Cost Total (€)
Configuració inicial de la xarxa	40	60 €	2.400 €
Instal·lació de dispositius	50	60 €	3.000 €
Proves inicials de seguretat	30	50 €	1.500 €
Formació inicial (usuaris i administradors)	40	50 €	2.000 €

Total Hores Inicials: **7.500 €**

Cost Anual de Manteniment

Activitat	Hores anuals	Cost/hora (€)	Cost Total (€)
Monitorització i resposta a incidents	200	50 €	10.000 €
Actualització periòdica del sistema	50	50 €	2.500 €

Auditoria anual de seguretat	20	100 €	2.000 €
Formació contínua en seguretat	30	50 €	1.500 €

Total Cost Manteniment Anual: **8.000 €**

Resum Econòmic

- **Cost inicial total** (dispositius + treball inicial): **48.500 €**
- **Cost Anual de Manteniment**: **8.500 €**

Polítiques de Seguretat per EduTech Global

A continuació es detallen les polítiques de seguretat proposades per EduTech Global, estructurades en tres fases: avaluació de necessitats, disseny de polítiques específiques i pla d'implementació.

1. Avaluació de Necessitats

L'avaluació es fonamenta en identificar els requisits específics d'EduTech Global, contemplant les normatives internacionals (GDPR, FERPA), protecció de dades personals i educatives, així com la protecció dels drets de propietat intel·lectual dels continguts educatius. Això implica:

- Recollida d'informació interna (auditories, informes d'incidents, retroalimentació).
- Col·laboració multidisciplinària amb departaments com TI, Recursos Humans, Legal i Finances.
- Anàlisi de riscos per prioritzar les àrees crítiques vulnerables.

2. Disseny de Polítiques

Les polítiques proposades inclouen:

- **Política de Privacitat i Protecció de Dades**: Compliment estricte de la GDPR i la FERPA, incloent-hi protocols detallats per a la gestió i tractament de dades personals.
- **Política d'Accés**: Definició clara dels nivells d'accés segons els rols d'estudiants, professors i administradors, aplicant autenticació multifactor.
- **Política de DRM (Gestió de Drets Digitals)**: Mecanismes robustos per evitar la distribució il·legal de continguts educatius.
- **Política de Resposta a Incidents**: Procediments detallats per identificar, comunicar, gestionar i resoldre incidents de seguretat de manera ràpida i eficaç.

3. Pla d'Implementació

Aquest pla es divideix en les següents fases clau:

- **Comunicació**: Informació clara i detallada sobre les noves polítiques a tot el personal i usuaris.
- **Capacitació i formació**: Sessions específiques per assegurar que tots els usuaris comprenguin i apliquin correctament les polítiques.
- **Implementació gradual**: Cronograma clar per a la transició als nous procediments, minimitzant l'impacte sobre l'operativa diària.
- **Monitorització contínua**: Auditoria constant per assegurar l'eficàcia i adaptació a canvis normatius i operatius.

Model de Control d'Accessos per EduTech Global

A continuació es presenta el model específic seleccionat per EduTech Global, detallant com es gestionaran les identitats, permisos i com s'implementaran aquests mecanismes dins la plataforma.

1. Elecció del Model de Control d'Accessos

S'ha seleccionat un model híbrid combinant principalment el Control d'Accessos Basat en Rols (RBAC) i el Control d'Accessos Basat en Atributs (ABAC), per assegurar la flexibilitat i robustesa requerides per EduTech Global:

- **RBAC**: Ideal per gestionar eficientment permisos associats a rols fixos com estudiants, professors i administradors.
- **ABAC**: Utilitzat per accedir de manera més granular en situacions específiques o contextos dinàmics (localització, dispositius, períodes específics).

2. Disseny de l'Esquema de Gestió d'Identitats i Permisos

Es definiran clarament tres grups principals d'usuaris amb permisos específics:

- **Estudiants**:
    - Accés únicament al material dels cursos matriculats i recursos públics.
    - Sense accés a informació administrativa o continguts restringits.
- **Professors**:
    - Accés a materials de cursos propis, informació dels estudiants assignats i eines per personalitzar continguts i avaluacions.
    - Sense accés a dades financeres ni informació personal no relacionada amb la seva funció.
- **Administradors**:
    - Accés complet per gestionar la plataforma, usuaris, permisos, continguts i aspectes financers.
    - Implementació obligatòria d'autenticació multifactor (MFA).

3. Aplicació i Integració del Model

- **Configuració inicial**:
    - Integració amb un sistema centralitzat de gestió d'identitats (IdM) com LDAP o Active Directory.
    - Definició clara i documentada dels rols i atributs per configurar permisos.
- **Implementació tècnica**:
    - Configuració de polítiques d'accés detallades als servidors web, aplicacions, bases de dades i sistemes administratius segons el model RBAC i ABAC.

    - Configuració i desplegament de sistemes MFA per assegurar autenticació forta.
- **Integració amb la plataforma existent**:
    - Proves exhaustives per garantir que el sistema funcioni correctament sense afectar negativament l'experiència d'usuari.

3. Aplicació i Integració del Model

- **Formació contínua**:
    - Sessions periòdiques per assegurar que tots els usuaris coneixen el funcionament del model.
- **Monitoratge continu**:
    - Implementació de mecanismes de supervisió i alertes automatitzades per detectar anomalies d'accés o possibles abusos.
- **Auditories periòdiques**:
    - Realització regular d'auditories per identificar i corregir desviacions o vulnerabilitats.

Conclusions

En aquesta pràctica hem dissenyat una estratègia integral de ciberseguretat adaptada específicament a les necessitats d'EduTech Global, considerant el seu context educatiu global, les necessitats particulars de protecció de dades sensibles, i les normatives internacionals pertinents.

L'anàlisi detallat ha permès identificar clarament els riscos i vulnerabilitats específiques de la plataforma, establint una arquitectura de xarxa segura que integra components tecnològics avançats com Firewalls NGFW, IPS, sistemes VPN i DRM, així com l'ús obligatori d'autenticació multifactor.

A nivell econòmic, la proposta ofereix una estimació clara dels costos inicials d'implementació i els costos recurrents associats al manteniment, essent una inversió equilibrada que assegura una alta disponibilitat, integritat i confidencialitat de les dades i serveis.

Les polítiques dissenyades asseguren el compliment estricte de les regulacions GDPR i FERPA, a més de garantir la privacitat i seguretat de dades dels usuaris d'acord amb estàndards globals. El model híbrid de control d'accessos (RBAC combinat amb ABAC) proporciona la flexibilitat i robustesa necessàries per gestionar eficaçment els accessos dels diferents perfils d'usuaris, prevenint així possibles violacions internes i externes.

Finalment, aquesta estratègia proporciona un marc robust i escalable que no només reforça la seguretat actual d'EduTech Global, sinó que també està preparat per adaptar-se eficaçment a futurs reptes tecnològics i reguladors, garantint així la continuïtat operativa, la confiança dels usuaris i la solidesa del negoci a llarg termini.

Bibliografia

1. **Agència Espanyola de Protecció de Dades – GDPR**
   https://www.aepd.es/es/prensa-y-comunicacion/blog/guia-reglamento-general-proteccion-datos
2. **Family Educational Rights and Privacy Act (FERPA)**
   https://studentprivacy.ed.gov/
3. **PCI Security Standards Council (PCI-DSS)**
   https://www.pcisecuritystandards.org/document_library
4. **National Institute of Standards and Technology (NIST) - Control d'Accessos (RBAC i ABAC)**
   https://csrc.nist.gov/publications/detail/sp/800-162/final
5. **OWASP - Principi de Privilegi Mínim**
   https://cheatsheetseries.owasp.org/cheatsheets/Least_Privilege_Cheat_Sheet.html
6. **Introducció a l'Autenticació Multifactor (MFA) - Microsoft Security**
   https://www.microsoft.com/security/blog/2020/11/19/multi-factor-authentication-how-to-protect-online-accounts/
7. **Introducció als Firewalls de nova generació (NGFW)**
   https://www.fortinet.com/resources/cyberglossary/next-generation-firewall-ngfw
8. **Introducció a l'IPS (Sistema de Prevenció d'Intrusions)**
   https://www.cisco.com/c/es_es/products/security/ips-explained.html
9. **Què és la Gestió de Drets Digitals (DRM)?**
   https://www.investopedia.com/terms/d/digital-rights-management.asp
10. **Cybersecurity and Infrastructure Security Agency (CISA) - Seguretat de xarxes i arquitectura segura**
    https://www.cisa.gov/free-cybersecurity-services-and-tools
11. **Realitat Augmentada aplicada a l'Educació (exemple)**
    https://www.edutopia.org/article/how-teachers-can-start-using-ar-classroom/