Escuela Superior de Guerra ‘General Rafael Reyes Prieto’

Taller de Identificación de Riesgos de Amenazas Cibernéticas

My. Chavarro Gutiérrez Luis Alberto
My. Esmeral Madrid Diego Alejandro
My. Guerrero Cortes Alex Danny
My. Robles Ocampo Edna Giannine

Gestión de riesgos cibernéticos
Dr. Jaider Ospina Navas
Maestría en ciberseguridad y ciberdefensa

27 de febrero de 2025

Taller de Identificación de Riesgos de Amenazas. Cibernéticas

1. Definición del escenario.

Se realizara la identificación de amenazas cibernéticas de la "Universidad de Bogotá" la cual en su sistema de gestión del aprendizaje se maneja de forma hibrida en donde se aplica la presencialidad y en la nube a través de una blackboard en la cual se imparten clases virtuales y se manejan diferentes materiales académicos, en este escenario profesores y estudiantes acceden de manera remota desde diferentes ubicaciones y equipos a continuación mencionaremos algunos riesgos críticos y potenciales que identificaremos a lo largo del taller.

1.1. Riesgos críticos.

- Autenticación de usuarios y permisos de acceso.
- Servidores en la nube donde se almacenan datos de los estudiantes.
- Comunicación en tiempo real como video conferencias, foros y chat entre otros.

1.2. Riesgos potenciales.

Para identificar los activos críticos, analizamos qué elementos del sistema son esenciales para su funcionamiento y contienen información valiosa.

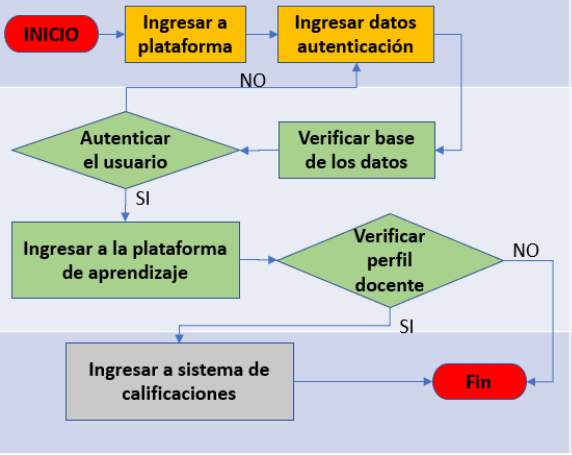
Tabla 1. Elementos del Sistema

ACTIVO	DESCRIPCIÓN	RIESGO POTENCIAL
Base de datos de usuarios	Información de estudiantes y profesores como nombres, correos, contraseñas etc.	Spoofing, information, diclossure.
Registro de calificaciones	Notas y reportes académicos.	Tampering, repudation
Sistema de autenticación	Credenciales y accesos de los usuarios.	Spoofing, elevation of privilege
Servidores en la nube	Estructura donde está la plataforma de aprendizaje.	Denia lof service

ACTIVO	DESCRIPCIÓN	RIESGO POTENCIAL
Contenido académico	Materiales de estudio, actividades y exámenes.	Information diclossure, tampering.

Fuente: Elaboración propia, de acuerdo a datos extraídos del modelo STRIDE (Pure, s.f.)

Figura1. Diagrama de Flujo de la información en el Sistema

Diagrama de Proceso	Responsable	Componentes	Tipos de Ataques
	Estudiantes y profesores	Usuario y contraseña	Tampering, DoS
	Software de aprendizaje	Base de datos, Servidores de datos académicos	Spoofing, Information Diclossure, Repudation, DoS, Elevation of privilege
	Profesores	Base de Datos de Calificaciones	Tampering, repudation

Fuente: Elaboración propia, de acuerdo a proceso que realiza la plataforma BB.

2. Análisis de riesgos.

A continuación, analizaremos las amenazas en el marco modelado STRIDE.

Tabla 2. Amenazas

Categoría	Descripción	Ejemplo	Impacto
Spoofing	Suplantación de identidad.	El atacante obtiene las credenciales de un docente y cambia calificaciones.	Alto
Tampering	Manipulación de datos.	Un estudiante logra cambiar su nota final sin autorización.	Alto
Repudiation	Negación de acciones	Un estudiante niega haber entregado una tarea por que el sistema no guarda trazabilidad.	Medio

Information diclosure	Fuga de información	Los datos personales de los estudiantes son filtrados por una deficiente configuración de permisos.	Alto
Denial of service (DoS)	Interrupción del servicio	Un ataque de este tipo satura los servidores e impide el acceso en el día de presentación de exámenes finales.	Alto
Elevation of privilege	Escala de privilegios.	Un usuario con servicios básicos explota una vulnerabilidad y obtiene accesos como administrador.	Muy Alto

Fuente: Elaboración propia, de acuerdo a datos extraídos del modelo STRIDE (Pure, s.f.)

De acuerdo a la matriz de riegos (Anexo A matriz de riesgos) los más críticos serian spoofing, information diclosure y denial of service ya que afectan directamente la integridad del sistema y la disponibilidad del mismo; las posibles soluciones deben ser tanto técnicas como administrativas mediante autenticación de multifactor, cifrado, logs de auditoría y segmentación de permisos. Estas medidas deben evaluarse constantemente toda vez que las técnicas de las amenazas evolucionan constantemente.

3. Diseño de controles de seguridad.

A continuación, se describirán las medidas de seguridad recomendadas y políticas de seguridad que se implementarán en cada uno de los componentes, iniciando por el mapeo de los controles de seguridad basado en la ISO/IEC 27001:2022 y posterior su análisis.

Tabla 3. Medidas de Seguridad Recomendadas

Control de seguridad	**Anexo A ISO/IEC 27001:2022**	**Objetivo**
Autenticación multifactor (MFA)	Control de acceso	Evitar accesos no autorizados mediante autenticaciones adicionales
Cifrado de datos (AES 256 TLS 1,3)	Cifrado y protección de datos	Proteger la confidencialidad de datos en almacenamiento y transito

Control de seguridad	Anexo A ISO/IEC 27001:2022	Objetivo
Gestión de accesos y privilegios	Control de acceso basado en roles	Limitar el acceso a información sensible solo a usuarios autorizados
Monitoreo y auditoria de logs	Registro de eventos y monitoreo	Detectar actividades sospechosas y rastrear acciones en el sistema
Protección contra ataques DoS	Protección contra amenazas externas	Prevenir la interrupción del servicio debido a ataques de denegación de servicio
Pruebas de penetración y evaluaciones de seguridad	Pruebas de seguridad de sistemas	Identificar vulnerabilidades antes de que sean explotadas por atacantes

Fuente: Elaboración propia, de acuerdo a datos extraídos del anexo A de la norma ISO/IEC 27001 (ISO/IEC, 2022).

- Portal de inicio de sesión. En este componente se recomienda habilitar una autenticación multifactor el cual evitará accesos no autorizados a la plataforma. Todos los usuarios deben registrar un segundo factor de autenticación como SMS o biometría.
- Sistema de autenticación. Se aplicará el principio de privilegios mínimos el cual ayudara a evitar escaladas de privilegios. Los usuarios solo tendrán los permisos estrictamente necesarios para su función se debe realizar revisiones periódicas de accesos con auditorias trimestrales.
- Base de datos de usuarios. Se protegerá con cifrado AES-256 para evitar fuga de información. Toda la información de los usuarios y calificaciones debe estar cifrada utilizando AES-256 en almacenamiento y TLS 1.3 en transmisión.
- Plataforma LMS. Implementación de logs de auditoria para detectar cambios y rastrear acciones de usuarios. Se debe todas las acciones criticas dentro del sistema, incluyendo inicios de sesión, modificaciones de datos y accesos administrativos, con alertas de tiempo real para actividades sospechosas.
- Base de datos de las calificaciones. Restricción de accesos para prevenir modificaciones no autorizadas.

- Servidor en la nube. Se incluyen firewalls y balanceos de carga para mitigar ataques (DoS) para garantizar la disponibilidad del sistema.

Tabla 3. Medidas de Seguridad Recomendadas

Control de Seguridad	**Amenaza Mitigada**
Autenticación multifactor	Spoofing
Cifrado AS-256 y TLS 1.3	Information diclosure
Auditoria de logs	Repudation y tampering
Gestión de privilegios	Elevation of privilege
Firewalls y balanceo de carga	Denial of service

Fuente: Elaboración propia, de acuerdo a datos extraídos del anexo A de la norma ISO/IEC 27001 (ISO/IEC, 2022).

Conclusiones y recomendaciones.

El análisis de riesgos realizado demuestra que es de importancia tener un buen sistema de seguridad en entornos híbridos ya que la digitalización del aprendizaje ha convertido a las plataformas LMS en objetivos de ciberataques, esta gestión de riesgos es fundamental y nos sirve para garantizar la disponibilidad, integridad y confidencialidad de la información básica. Un ataque exitoso en contra de la plataforma virtual podría comprometer la privacidad de profesores y estudiantes, alterar las calificaciones de forma fraudulenta y causar un sin número de interrupciones en el servicio afectando el proceso educativo.

El análisis realizado con el método STRIDE revelo que las amenazas más críticas del sistema incluyen suplantación de identidad (Spoofing), modificación de datos (Tampering), filtración de información (information diclossure) y ataques de negación de servicio (DoS). Es por esto que se recomienda implementar medidas de seguridad con el fin de mejorar significativamente la seguridad con diseños como es la aplicación de autenticación multifactor, cifrado AES-256, auditoria de logs, una gestión estricta de privilegios y protección contra ataques (DoS), se requiere que este proceso sea dinámico requiriendo evaluaciones periódicas, monitoreo constante y capacitación del personal mitigando los riesgos de manera efectiva.

También es importante establecer políticas de gestión de privilegios con el fin de reducir la posibilidad de escalada de privilegios implementando el principio de privilegios mínimos (PoLP) y realizar trimestralmente auditorias de accesos. Se recomienda activar unos monitores y auditoria de registros en donde se detecten actividades sospechosas y mejorar la trazabilidad configurando alertas en tiempo real para cuando se tengan intentos de accesos no autorizados y cambios en clasificaciones.

Por ultimo se recomienda realizar evaluaciones de seguridad y pruebas de penetración donde el objetivo es identificar vulnerabilidades antes de que sean explotadas, realizando pruebas de penetración periódicas y auditorias de seguridad para fortalecer infraestructura. Capacitar a los usuarios de la plataforma en buenas prácticas de seguridad con el fin de reducir los errores humanos que puedan facilitar ataques implementando campañas sobre seguridad en contraseñas, phishing y gestión de accesos.

Referencias.

DataSunrise. (s.f.). Modelo de Amenazas STRIDE. Recuperado el 23 de febrero del 2025 de https://www.datasunrise.com/es/centro-de-conocimiento/modelo-de-amenazas-stride/

IBM. (s.f.). ¿Qué es la gestión de riesgos cibernéticos? IBM. Recuperado el 23 febrero del 2025. https://www.ibm.com/mx-es/topics/cyber-risk-management

IBM. (s.f.). Supported security ciphers. IBM Documentation. Recuperado el 23 de febrero del 2025. https://www.ibm.com/docs/es/flashsystem-5x00/8.7.0?topic=levels-security-supported-security-ciphers

Pure Storage. (s.f.). ¿Qué es el modelo de amenaza STRIDE? Pure Storage. Recuperado el 23 de febrero del 2025. https://www.purestorage.com/es/knowledge/stride-threat-model.html.

ISO/IEC. (2022). Seguridad de la información, ciberseguridad y protección de la privacidad — Sistemas de gestión de la seguridad de la información — Requisitos (3ª ed.). Organización Internacional de Normalización.