UNIVERSIDAD PERUANA UNIÓN

FACULTAD DE INGENIERIA Y ARQUITECTURA

Escuela Profesional de Ingeniería de Sistemas

Análisis de Riesgos

Curso:

Seguridad de la información

Autores:

Valle Sanca, Elias Raul
Esquivel Levano, Carla Nicolle
Flores Aguilar, Matias Urlichs
Avila Medina, Yeiser Jamber

Matos Urdanivia, Leonardo Anthony

Farfán Nuñez, Carlo Gabriel

Diaz Mendoza, Andres Rafael

Haro Ortiz, Dany Richard

Docente:

Fernando Manuel Asin Gómez

Lima, Setiembre 2025

INDICE

Tabla de contenido

1. Introducción

1.1 Propósito

Este documento desarrolla el **Análisis de Riesgos del Sistema Web Grad.IA (LMS)** de la Universidad Peruana Unión, en el marco del **Sistema de Gestión de Seguridad de la Información (SGSI)** conforme a la norma **ISO/IEC 27001:2022**.

El análisis se realiza siguiendo la metodología establecida en **ISO/IEC 27005:2018**, complementada con criterios de **OCTAVE** y **MAGERIT** para fortalecer los procesos de:

- identificación de activos,
- análisis de amenazas y vulnerabilidades,
- evaluación del riesgo,
- y definición de tratamientos y controles.

El objetivo es garantizar que Grad.IA opere bajo un enfoque de gestión de riesgos formal, controlado y alineado con las mejores prácticas internacionales en seguridad de la información.

1.2 Alcance

El análisis de riesgos considera todos los elementos clave que intervienen en la operación del LMS Grad.IA, incluyendo:

Procesos académicos y administrativos

- Gestión de cursos y contenidos.
- Evaluaciones, calificaciones y retroalimentación.
- Gestión documental y evidencias académicas.
- Administración de usuarios, roles y permisos.
- Integraciones con otros sistemas institucionales.

Infraestructura tecnológica

- Servidores locales y máquinas virtuales.
- Infraestructura de red (switches, routers, VLANs, HSRP).
- Firewall perimetral, VPN, IDS/IPS.
- Servicios en nube e infraestructura híbrida.
- Base de datos, almacenamiento y respaldos.

Actores internos y externos

- Estudiantes.
- Docentes y coordinadores.
- Administradores del LMS.
- Personal de TI (infraestructura, redes y seguridad).
- Proveedores tecnológicos asociados al sistema.

2. Identificación de Activos

Categoría	Activo	Descripción	Propietario	Valor
Hardware de enlace de red	Routers Cisco ISR, Switches Catalyst, Firewall pfSense HA	Infraestructura de red, segmentación VLAN, redundancia HSRP y seguridad perimetral	Área de TI / Redes	**Alto**
Servidores	Hosts VMware ESXi, Servidor de Base de Datos, Servidor Web Grad.IA, AD/DNS	Infraestructura de virtualización, servicios críticos del LMS, autenticación y directorio	Área de TI / Infraestructura	**Crítico**
Software	Plataforma Web Grad.IA (LMS), Active Directory, SIEM, IDS/IPS	Aplicación central del proceso académico, autenticación, monitoreo y seguridad operacional	DTI / Área TI	**Crítico**
Datos	Registros académicos, cursos, calificaciones, contenidos digitales, credenciales	Información académica, personal y sensible de estudiantes y docentes	Secretaría Académica / Escuela	**Crítico**
Personas	Estudiantes, Docentes, Coordinadores, Administradores del LMS, Área TI	Roles internos y externos que interactúan con el sistema	Dirección Académica / Escuela Profesional	**Alto**

3. Identificación de Amenazas y Vulnerabilidades

3.1 Amenazas externas:

- **Ataques DDoS contra el portal Grad.IA**, con el fin de interrumpir la disponibilidad del LMS durante periodos críticos (matrícula, evaluaciones, cierre de semestre).
- **Robo de credenciales mediante phishing**, dirigido a estudiantes, docentes o personal administrativo.
- **Explotación de vulnerabilidades en servicios web**, especialmente si existen módulos desactualizados o sin parches.
- **Ataques de fuerza bruta** contra el portal de autenticación (AD/LDAP/SSO).

- **Malware en dispositivos de usuarios** que comprometa sesiones o credenciales.
- **Acceso no autorizado desde terceros** a través de redes no confiables o dispositivos inseguros.

3.2 Amenazas internas

- **Accesos indebidos por privilegios mal asignados** (falta de segmentación de roles RBAC).
- **Errores humanos** en la gestión de cursos, carga de calificaciones o administración de usuarios.
- **Filtración involuntaria de datos** por uso de correos personales, dispositivos no autorizados o almacenamiento externo.
- **Manipulación de notas o contenidos** por usuarios con permisos excesivos.
- **Desconfiguración accidental de servidores o servicios críticos** por personal técnico sin procesos formales de cambio.
- **Uso de contraseñas compartidas** entre asistentes o docentes.

3.3 Vulnerabilidades

- **Contraseñas débiles o sin políticas robustas**, ausencia de **MFA** obligatorio.
- **Servidor o plataforma mal configurada**, con puertos expuestos o permisos débiles.
- **Falta de endurecimiento (hardening)** del firewall, base de datos, AD o servidores web.
- **Validaciones manuales sin trazabilidad**, generando ausencia de auditoría de cambios.
- **Dependencia del factor humano** sin mecanismos automáticos de control.
- **Respaldo no verificado o no probado regularmente**, lo que compromete la recuperación.
- **Logs insuficientes o sin centralización**, dificultando la detección temprana de incidentes.
- **Ausencia de monitoreo continuo o SIEM**, exponiendo el sistema a ataques no detectados.
- **Uso de dispositivos personales (BYOD)** sin políticas de seguridad definidas.

4. Matriz de Riesgos

4.1 Criterios de evaluación

- **Impacto:** Bajo, Medio, Alto, Crítico.

- **Probabilidad:** Baja, Media, Alta.
    - **Nivel de Riesgo:** Bajo, Medio, Alto, Crítico.

Activo	Amenaza	Vulnerabilidad	Impacto (1-5)	Probabilidad (1-5)	Nivel de riesgo (lxp)	Clasificación
Sistema **Web Grad.IA (LMS)**	Denegación de servicio (DoS)	Falta de WAF y monitoreo	5	3	15	Alto
	Denegación de servicio distribuido (DDoS)	Autenticación débil, contraseñas reutilizadas	4	2	8	Bajo
	Inyección SQL	Dependencias desactualizadas	4	3	12	Medio
Servidor de Base de Datos	Ataque ransomware	Software antivirus desactualizado en la red	5	3	10	Alto
	Acceso no autorizado	Puertos innecesarios abiertos	5	3	15	Alto
Servicio correo Institucional	Phishing dirigido	Contraseñas débiles, sin MFA	5	3	15	Alto
Servicio DNS	Spoofing de DNS	falta de DNSSEC. Redirección masiva a sitios maliciosos	4	2	8	Bajo
Servicio DHCP	Rogue DHCP.	Falta de segmentación. ataques de tipo "man-in-the-middle"	4	2	8	Bajo
Informes confidenciales de la organización	Exposición de informes confidenciales	Control de acceso inadecuado	4	4	16	Alto
	Acceso interno no autorizado	Roles mal definidos	4	4	16	Alto
Credenciales	Uso de credenciales por personal	Procesos de gestión de identidades	5	3	15	Alto

	no autorizado	deficientes (IAM)				
	Almacenamiento inseguro de credenciales	Repositorios sin encriptación	5	3	15	Alto
Evaluadores	Phishing	Usuarios sin capacitación en ciberseguridad. Ingeniería Social	5	5	25	Alto
Estudiantes						

4.2 Método cuantitativo de Análisis de Riesgo

Activo	Valor Económico (Soles)	Justificación	Probabilidad de ataque (% ARO)	ALE
Sistema **Web Grad.IA (LMS)**	S/ 80,000.00	Desarrollo, soporte, reputación institucional	30%	S/24,000.00
Servidor de Base de Datos	S/ 150,000.00	Pérdida de datos críticos, multas por privacidad	30%	S/45,000.00
Servicio de Correo Institucional	S/ 20,000.00	Comunicación institucional y operaciones diarias	15%	S/3,000.00
Credenciales	S/ 150,000.00	Compromiso total de servicios.	15%	S/22,500.00
Evaluadores / Estudiantes	S/ 40,000.00	Datos personales, reputación y cumplimiento normativo	40%	S/16,000.00

4.3 Criterios de evaluación

Activo	Riesgo	Controles de Seguridad	Justificación	Acciones de Solución
Sistema **Web Grad.IA (LMS)**	Servicio caído y saturado por ataque DoS al sistema **Web Grad.IA (LMS)**	A.8.21 Seguridad de la red	Garantiza la Disponibilidad de los servicios y sistemas	Prevención: Implementar un sistema de Detección y Prevención de

				Intrusiones (IDS/IPS) y configurar reglas para identificar y bloquear automáticamente patrones de tráfico anómalo
	Explotación de vulnerabilidades de inyección SQL en el sistema **Web Grad.IA (LMS)** debido a dependencias desactualizadas.	A.8.28 Codificación segura	El desarrollo seguro incluye validación de entradas y pruebas para identificar fallos antes de desplegar a producción	Mitigación: Configurar un Web Application Firewall (WAF) en el front-end para inspeccionar el tráfico entrante. Prevención: Usar los métodos del ORM, evitar concatenar string SQL
Servicio de Base de datos	Pérdida de datos en el servidor de base de datos debido a un ataque de ransomware, aprovechando el software antivirus desactualizado en la red	A.8.7 Protección contra el malware	Mitigar la pérdida de datos causada por un ataque de *ransomware* en el Servicio de Base de Datos	Control/Red: Segmentar la red para aislar el servidor de base de datos de la red de endpoints de usuario final. Restringir el tráfico solo a puertos y protocolos necesarios.
	Pérdida de Confidencialidad , Integridad mediante la explotación de puertos innecesarios abiertos en el Servidor de Base de Datos para obtener acceso no autorizado.	A.8.21 Seguridad de la red	Evitar el acceso no autorizado al Servidor de Base de Datos a través de puertos innecesarios abiertos, la organización debe establecer reglas claras sobre cómo funciona su red	Detección/Monitoreo: Ejecutar escaneos de vulnerabilidades y puertos (ej. usando Nmap) periódicamente (semanal o mensualmente) al servidor de base de datos

Servicio correo institucional	Compromiso de cuentas de correo institucional mediante un ataque de phishing dirigido, aprovechando contraseñas débiles o ausencia de MFA.	A.6.3 Concientización y formación sobre seguridad de la información	Garantizar que las personas sean conscientes de sus responsabilidades en materia de seguridad y cumplirlas.	Control: Establecer y Compartir una política de contraseñas robusta que exija una longitud mínima (ej. 12-14 caracteres), prohíba el uso de contraseñas previamente comprometidas.
Informes confidenciales de la organización	Exposición de información académica o personal contenida en informes operativos debido a un control de acceso mal gestionado	A.5.10 Uso aceptable de la información y otros activos asociados	Garantizar que la información y otros activos asociados se protejan, utilicen y gestionen adecuadamente.	Detección: Revisar y auditar periódicamente las Listas de Control de Acceso (ACLs) en los repositorios de informes. Eliminar inmediatamente cualquier acceso que ya no sea necesario
	Acceso no autorizado a los informes confidenciales por parte de empleados o personal autorizado incorrectamente debido a una gestión inadecuada de roles.	A.5.15 Control de acceso	Establecer reglas para controlar el acceso a la información de acuerdo con la necesidad del saber.	Definir y documentar formalmente los roles de acceso y los permisos. Cada rol debe mapearse directamente a un conjunto mínimo y específico de permisos necesarios para una función labora
Credenciales	Uso indebido de credenciales por parte de personas no autorizadas debido a procesos de gestión de			

	identidades deficientes.			
	Exposición y robo de credenciales debido al almacenamiento inseguro en repositorios sin encriptación.	A.8.24 Uso de la Criptografia	Evitar la exposición y robo de credenciales debido a un almacenamiento inseguro.	Implementar un Almacén de Credenciales Centralizado (ej. Secret Manager con AWS Secrets Manager). Todas las credenciales deben ser eliminadas de archivos de configuración y código fuente
Evaluadores/Estudiantes	Compromiso de cuentas de evaluadores y estudiantes por captura de credenciales mediante correos/mensajes de phishing, aprovechando el bajo conocimiento en seguridad	A.6.3 Concientización y formación sobre seguridad de la información	Enfocarse en el factor humano, que es el blanco de la amenaza de phishing. Al capacitar y concientizar a los usuarios sobre cómo reconocer correos maliciosos y proteger sus credenciales.	Diseñar un programa de formación obligatoria de seguridad de la información específico para evaluadores y estudiantes al inicio de cada ciclo o año académico, haciendo énfasis en cómo reconocer el phishing y los ataques de ingeniería social.

5. Plan de Tratamiento de Riesgos

- Controles técnicos: MFA, RBAC, cifrado AES-256, WAF, IDS/IPS, segmentación VLAN.
- Controles organizativos: políticas de seguridad ISO 27001/27002, capacitación, auditorías semestrales.
- Controles físicos: acceso restringido al CPD, CCTV, racks cerrados.
- Continuidad: respaldos 3-2-1, pruebas de restauración trimestrales, RTO ≤ 2h, RPO ≤ 15min.

6. Referencias Normativas

- ISO/IEC 27001:2022 – Sistemas de Gestión de Seguridad de la Información.
- ISO/IEC 27002:2022 – Controles de seguridad de la información.
- ISO/IEC 27005:2018 – Gestión de riesgos de seguridad de la información.
- NIST Cybersecurity Framework (CSF).
- ITIL v4 – Gestión de servicios TI.