Matriz de Gestión de Riesgos de TI – UTPL

ID	Descripción del Riesgo	Probabilidad (1-5)	Impacto (1-5)	Nivel de Riesgo (PxI)	Priorización - Ordenar de mayor a menor.	Acción de Mitigación Propuesta - Basado en estádares
R1	Dependencia de herramientas complementarias no conformes que destruyen la experiencia académica y crean pesadillas de gestión de datos.	4	5	**20**	**1**	Aprobar la **Política de Estandarización de Software** y el Catálogo oficial de TI; controles COBIT 2019 *BAI09*; revisión semestral del comité de TI.
R2	Soluciones fragmentadas compradas por departamentos sin validación del CIT, lo que resulta en "islas" tecnológicas y costos redundantes.	4	4	**16**	**2**	Aplicar la **Gestión de Demanda y Portafolio** (COBIT *EDM02 / APO05*); criterios de decisión alineados a ISO 38500.
R3	No hay trazabilidad respecto a los proyectos de TI: no existe evidencia de vinculación con las líneas estratégicas del PEI.	3	4	**12**	**3**	Crear un **Portafolio Institucional de Proyectos TI** integrado a la PMO; seguimiento por OKR/KPI y auditorías internas (ISO 21502).
R4	Duplicación e inconsistencia de datos maestros entre facultades a causa de sistemas desarticulados.	3	4	**12**	**4**	Establecer un **programa de Gobernanza de Datos y MDM** (ISO 8000) guiado por DAMA-DMBOK; nombrar *data stewards* por unidad académica.
R5	Brecha de habilidades digitales entre directivos y docentes que sabotea la adopción de tecnología alineada al PEI.	3	4	**12**	**5**	Lanzar un **Plan de Capacitación Digital** basado en *DigComp 2.2*; monitoreo semestral vía HRIS.
R6	Apps críticas corriendo versiones jurásicas sin parches: caldo de cultivo para fallos y vulnerabilidades.	3	4	**12**	**6**	Implementar un **Programa de Ciclo de Vida de Software**; parches mensuales; referencia ISO 27002 §14 y COBIT *BAI05*.
R7	Riesgo de compartir información estudiantil por plataformas no aprobadas o no verificadas por TI.	2	5	**10**	**7**	Desplegar **DLP, cifrado E2E y MFA**; controles ISO/IEC 27001 (A.5-A.8) y campaña anual de privacidad tipo GDPR.
R8	Desajuste entre licencias compradas y licencias realmente usadas, desembolsando de más o infrautilizando software.	3	3	**9**	**8**	Activar un **Software Asset Management** (ISO 19770-1); auditorías trimestrales y contratos *pay-per-use*.
R9	Dependencia de "shadow IT" gestionada por usuarios sin soporte oficial, complicando cambios y seguridad.	3	3	**9**	**9**	Campaña de **Racionalización de Herramientas**; incorporar TI emergente al CMDB (COBIT *BAI09* / ITIL v4).
R10	Cargas manuales de datos que inducen errores y corrompen la integridad de la información institucional.	3	3	**9**	**10**	Automatizar **ETL y validaciones**; política de calidad de datos ISO 8000 y prácticas DAMA-DMBOK.
R11	Punto único de fallo en el enlace WAN Loja-Quito; si cae, medio campus virtual se paraliza.	2	4	**8**	**11**	Doble carrier + **SD-WAN**, conmutación probada; alineado a ITIL v4 (Resilience) y COBIT *DSS01*.
R12	Operación de soluciones SaaS sobre-licenciadas e infrautilizadas en las inversiones de software.	3	2	**6**	**12**	Reforzar el **Programa de Gestión de Activos de Software** (ISO 19770-1); auditorías de versión trimestral y contrato *pay-per-use*.