

Laboratorio 27

| Amenaza | Estrategia |
|--|---|
| Ciberataques, malware y riesgos informáticos | <ul style="list-style-type: none"> - Implementar una política institucional de ciberseguridad (contraseñas seguras, VPN, autenticación de dos factores). - Capacitar a estudiantes, docentes y administrativos en ciberseguridad básica. - Realizar auditorías periódicas en los sistemas de gestión académica y servidores. |
| Cambios normativos que exijan cumplimiento técnico inmediato | <ul style="list-style-type: none"> - Establecer un comité de seguimiento legal y normativo universitario. - Mantener contacto directo con entes reguladores (ej. Ministerio de Educación). - Diseñar los sistemas académicos con arquitectura modular para facilitar adaptaciones. |
| Pérdida de talento (docente o administrativo) por ofertas externas | <ul style="list-style-type: none"> - Ofrecer programas de desarrollo profesional y académicos internos. - Fomentar un ambiente académico estimulante, con incentivos por investigación y participación en congresos. - Revisar periódicamente las escalas salariales y oportunidades de promoción. |
| Saturación de servicios por falta de automatización | <ul style="list-style-type: none"> - Digitalizar procesos académicos y administrativos (matrículas, certificados, tutorías). - Implementar sistemas de gestión universitaria (ERP académico). - Automatizar tareas repetitivas mediante chatbots o plataformas integradas. |
| Interrupción del servicio por fallos eléctricos o desastres naturales | <ul style="list-style-type: none"> - Instalar UPS y generadores en laboratorios, centros de datos y áreas críticas. - Contar con respaldo en la nube para la plataforma educativa. - Crear protocolos de continuidad académica y clases virtuales ante emergencias. |
| Inestabilidad económica global | <ul style="list-style-type: none"> - Diversificar fuentes de ingreso: programas de educación continua, convenios con empresas, servicios de investigación. - Ajustar presupuestos anualmente. - Crear fondos de contingencia y reducir dependencias únicas (ej. financiación estatal exclusiva). |
| Inestabilidad política nacional | <ul style="list-style-type: none"> - Participar activamente en redes universitarias para defensa de la autonomía. - Evaluar escenarios políticos que puedan impactar presupuestos o legislación educativa. - Mantener canales de diálogo con autoridades locales y nacionales. |

| Amenaza | Estrategia |
|---|---|
| Obsolescencia tecnológica | <ul style="list-style-type: none"> - Crear un plan de renovación tecnológica cada 3-5 años para laboratorios, salas de cómputo y servidores. - Priorizar el uso de software y plataformas con soporte activo. - Buscar convenios con empresas tecnológicas para actualización continua (ej. Microsoft, Google, Cisco). |
| Dependencia excesiva de proveedores | <ul style="list-style-type: none"> - Evitar depender de un único proveedor para servicios críticos (plataforma de clases, software de gestión, servicios en la nube). - Tener contratos con cláusulas de respaldo y salida. - Capacitar al personal técnico para poder mantener ciertos servicios en caso de emergencia. |
| Pérdida o filtración de datos sensibles (estudiantes, docentes, administrativos) | <ul style="list-style-type: none"> - Implementar cifrado de datos, respaldos automáticos y políticas de privacidad estrictas. - Capacitar a los usuarios sobre el manejo de información confidencial (expedientes, calificaciones, pagos). - Realizar pruebas de vulnerabilidad y establecer protocolos de respuesta ante incidentes. |
| Reputación afectada por redes sociales | <ul style="list-style-type: none"> - Monitorear redes sociales institucionales y menciones de la universidad con herramientas especializadas. - Establecer un comité de comunicación y protocolo de gestión de crisis. - Promover campañas de comunicación positiva sobre logros institucionales, eventos y valores. |
| Mala comunicación interna | <ul style="list-style-type: none"> - Implementar plataformas institucionales para la comunicación formal (como intranet, correos institucionales, Teams/Slack). - Fomentar la transparencia mediante boletines internos y reuniones periódicas con facultades/departamentos. - Crear canales de retroalimentación abiertos para estudiantes, docentes y administrativos. |