Roadmap de Implementación de Ciberseguridad – Universidad Popular del Cesar

Jesús Rodrigo Toro Navarro

Seguridad informática

Universidad Popular del Cesar

Valledupar, Cesar

Amenaza	Estrategia para Contrarrestarla	Plazo de Implementación
1. Ciberataques, malware y riesgos informáticos crecientes	- Firewall de nueva generación.- Antimalware actualizado y análisis de comportamiento.- Simulacros de phishing y capacitaciones.	Corto plazo (0–6 meses)
2. Cambios normativos exigentes y repentinos	- Seguimiento legal y normativo con alertas.- Adopción de marcos normativos (ISO 27001, GDPR, etc.).- Manual de respuesta rápida ante exigencias externas.	Mediano plazo (6–12 meses)
3. Pérdida de talento TIC por ofertas externas	- Planes de carrera y bienestar laboral.- Programas de formación continua con certificación.- Banco de conocimiento institucional.	Mediano plazo (6–12 meses)
4. Fallos eléctricos o desastres naturales	- UPS y generadores eléctricos para data center.- Replicación en la nube.- Pruebas semestrales de contingencia.	Largo plazo (12–18 meses)
5. Dependencia de personal clave	- Transferencia de conocimiento.- Rotación de roles técnicos.- Uso de sistemas de gestión documental.	Corto-Mediano plazo
6. Dificultad para actualizar software	- Contratos de mantenimiento y soporte.- Migración progresiva a sistemas SaaS.- Política de obsolescencia tecnológica.	Mediano-Largo plazo
7. Ingeniería social y suplantación de identidad	- Talleres prácticos de concienciación.- Políticas claras de verificación de identidad.- Validación de acceso por MFA.	Corto plazo
8. Acceso no autorizado a datos sensibles	- Control de accesos basado en roles (RBAC).- Registro de auditoría y monitoreo continuo.- Cifrado de base de datos y comunicaciones.	Corto-Mediano plazo
9. Uso indebido de dispositivos personales (BYOD)	- Política clara de BYOD.- Soluciones MDM (Mobile Device Management).- Segmentación de red para invitados.	Mediano plazo
10. Exposición de información en la nube sin control	- Herramientas CASB (Cloud Access Security Broker).- Configuración segura de servicios en la nube.- Revisión periódica de accesos y permisos.	Mediano-Largo plazo
11. Saturación de servicios por falta de automatización	- Automatización de tareas repetitivas con scripts o herramientas RPA.- Monitoreo de rendimiento.- Balanceadores de carga.	Mediano plazo