Laboratorio 27 – Estrategia de Ciberseguridad

Universidad Popular del Cesar

1. Definición de Objetivos de Ciberseguridad

Objetivo: Establecer metas claras y alcanzables alineadas con la estrategia institucional de la Universidad Popular del Cesar.

Metas específicas:
- Reducir el puntaje de riesgo en los servidores académicos y administrativos en un 40% durante los próximos seis meses.
- Implementar autenticación multifactor (MFA) en todos los accesos críticos en un plazo de tres meses.
- Establecer auditorías trimestrales de configuraciones y vulnerabilidades.
- Garantizar copias de seguridad automatizadas diarias con pruebas mensuales de restauración.
- Realizar campañas de sensibilización en ciberseguridad dos veces por semestre.

Alineación estratégica:
Estas metas respaldan la transformación digital institucional, el cumplimiento normativo y la continuidad operativa en entornos virtuales de aprendizaje y administración.

2. Desarrollo de la Estrategia Integral

La estrategia integral incluye medidas técnicas, organizativas y de formación, estructuradas de la siguiente manera:

Medidas técnicas:
- Configuración de firewalls en el datacenter central y facultades descentralizadas.
- Implementación de sistemas de detección y prevención de intrusos (IDS/IPS).
- Automatización de copias de seguridad con replicación en la nube.
- Segmentación de redes por facultad/rol de usuario.

Medidas organizativas:
- Establecimiento de un comité de ciberseguridad institucional.
- Definición de roles y responsabilidades claras para incidentes TI.
- Elaboración de manuales de procedimiento para incidentes de seguridad.

Capacitación:
- Capacitaciones semestrales a funcionarios y docentes.

- Talleres prácticos para estudiantes en protección de identidad digital y redes.

3. Roadmap de Implementación

Fase 1: Diagnóstico y Planificación (0–3 meses)
- Evaluación inicial de riesgos: identificación de activos críticos, análisis de amenazas y vulnerabilidades, clasificación de riesgos.
- Inventario y clasificación de activos: hardware, software, redes, datos, usuarios.
- Cumplimiento normativo: revisión de estándares como ISO 27001, NIST, GDPR y brechas.
- Definición de política de seguridad institucional.
- Creación del Comité de Seguridad de la Información.

Fase 2: Implementación de Controles Básicos (3–6 meses)
- Implementación de control de acceso: contraseñas robustas y MFA.
- Gestión de identidades (IAM).
- Instalación de antivirus, antimalware y EDR.
- Configuración de firewall perimetral y segmentación de red.
- Aplicación de actualizaciones y parches automatizados.
- Diseño e implementación de estrategia de respaldo 3-2-1.

Fase 3: Formación, Monitoreo y Fortalecimiento (6–12 meses)
- Capacitación continua al personal: simulacros y ejercicios de concienciación.
- Implementación de SIEM para correlación de eventos y centralización de logs.
- Pruebas de penetración y escaneo de vulnerabilidades.
- Políticas para uso seguro de dispositivos móviles (BYOD).
- Auditorías internas periódicas.

Fase 4: Madurez y Respuesta Avanzada (12–24 meses)
- Plan de respuesta ante incidentes (IRP) y formación de CSIRT.
- Capacidades de análisis forense digital.
- Clasificación de la información y prevención de fuga de datos (DLP).
- Ejercicios de Red Team vs Blue Team.
- Implementación de capacidades de ciberinteligencia.
- Iniciativas de certificación en estándares internacionales.

Fase 5: Gobierno y Cultura de Seguridad (24+ meses)
- Integrar la ciberseguridad en la estrategia institucional con KPIs definidos.
- Promover cultura organizacional de seguridad (gamificación, incentivos).
- Simulacros de crisis cibernética y mejora continua.
- Auditorías externas y certificación de terceros.

Matrix DOFA Universidad Popular del Cesar

FORTALEZAS	**OPORTUNIDADES**
- Personal capacitado y con experiencia en soporte, redes y sistemas.	- Acceso a recursos del Estado para modernización tecnológica.
- Infraestructura básica instalada (red, servidores, data center).	- Convenios con universidades y empresas para prácticas, capacitaciones o transferencias tecnológicas.
- Presencia activa en proyectos institucionales estratégicos.	- Adopción de nuevas tecnologías (nube, virtualización, IA).
- Uso de plataformas educativas como Moodle o Teams.	- Financiamiento de proyectos mediante convocatorias TIC.
- Implementación de normas de seguridad (respaldo, antivirus, roles).	- Creciente interés institucional por la transformación digital.
-Cultura de aprendizaje continuo del personal técnico.	- Participación en redes académicas nacionales e internacionales de ciberseguridad.
- Políticas de acceso por roles en sistemas administrativos.	- Implementación de certificaciones internacionales (ISO 27001, NIST)
- Red de contactos con otras instituciones educativas para apoyo técnico.	- Desarrollo de programas académicos especializados en ciberseguridad.
- Capacidad de adaptación rápida a nuevas tecnologías por parte del equipo.	- Alianzas estratégicas con proveedores tecnológicos para obtener descuentos educativos.
- Conocimiento interno de los procesos académicos y administrativos.	- Creación de diplomados en ciberseguridad y gestión TI.
DEBILIDADES	**AMENAZAS**
- Recursos limitados para renovación de equipos y licencias.	- Ciberataques, malware y riesgos informáticos crecientes.
- Falta de manuales actualizados de procedimientos.	- Cambios normativos que exijan cumplimiento técnico inmediato.
- Dependencia de pocos funcionarios clave.	- Pérdida de talento por ofertas laborales externas.
- Baja inversión histórica en mantenimiento preventivo.	- Saturación de servicios por falta de automatización.
- Dificultad para actualizar software institucional.	- Interrupción del servicio por fallos eléctricos o desastres.
- Ausencia de un plan formal de continuidad del negocio	- Filtración de datos personales de estudiantes y funcionarios
- Falta de monitoreo 24/7 de la infraestructura crítica	- Suplantación de identidad en sistemas virtuales.

- Limitada capacitación del personal en ciberseguridad avanzada.	- Uso de software pirata o sin soporte en áreas académicas.
- Carencia de herramientas de análisis de vulnerabilidades automatizadas.	- Desinformación y ataques sociales dirigidos a usuarios administrativos.
- Insuficiente documentación de incidentes de seguridad previos.	- Pérdida o robo de información por accesos no autorizados.