UPY BIS
UNIVERSIDAD POLITÉCNICA DE YUCATÁN

BROCHURE DE SERVICIOS

Diseñamos, evaluamos y fortalecemos tu postura de ciberseguridad con programas, pruebas y consultorías enfocadas a resultados medibles.

1.Concienciación en Ciberseguridad

Qué hacemos

Programas de formación para personal técnico y no técnico: ejecutivos, operaciones, TI y desarrollo. Enfocados en construir cultura y reducir riesgo humano.

Beneficios para tu empresa

- Menos clics en enlaces maliciosos y mejor reporte de incidentes.
- Cumplimiento con políticas internas y marcos de referencia.
- Métricas de adopción para dirección.

Alcance y actividades

- Diagnóstico de madurez cultural.
- Plan anual por perfiles (módulos de 15–30 min).
- Píldoras de micro-learning y evaluaciones.
- Comunicación interna (carteles, correos, guías rápidas).

Entregables

- Plan de formación por rol.
- Calendario de sesiones.
- Resultados de evaluaciones y recomendaciones.
- Informe ejecutivo trimestral.

Modalidades

Presencial, virtual y e-learning.

2. Campañas de Phishing Ético

Qué hacemos

Simulaciones controladas de suplantación (correo, SMS, QR, voz) para medir y mejorar la respuesta del personal.

Beneficios para tu empresa

- Entrenamiento realista y medición por área.
- Reducción de exposición a ataques.
- Reentrenamiento dirigido a quienes lo necesitan

Alcance y actividades

- Diseño de plantillas por área y nivel.
- Ejecución mensual o trimestral.
- Seguimiento de reporte y tiempo de reacción.
- Talleres de retroalimentación.

Entregables

Panel con tasas de apertura, clic y reporte.
- Informe por área con riesgos y acciones.
- Kit de comunicación preventiva.
- Plan de mejora y nueva campaña.

Modalidades

Campañas puntuales o programa continuo.

3. DevSecOps

Qué hacemos

Integramos seguridad en todo el ciclo de vida del software: diseño, desarrollo, pruebas, despliegue y operación.

Beneficios para tu empresa

- Menos vulnerabilidades en producción.
- Flujo de entrega más confiable.
- Evidencias para auditoría y cumplimiento.

Alcance y actividades

- Baselines de repositorios y pipelines CI/CD.
- Revisión de dependencias, secretos y permisos.
- Integración de SAST, análisis de dependencias y controles en PR.
- Capacitación al equipo de desarrollo.

Entregables

- Matriz de riesgos por servicio.
- Backlog de remediación priorizado.
- Políticas de ramas, PR y revisiones seguras.
- Guías de hardening para apps e infraestructura.

Modalidades

Auditoría puntual o acompañamiento continuo (enablement de squad).

4. Seguridad de Infraestructura TI y Redes

Qué hacemos

Evaluamos y fortalecemos infraestructura on-premise, nube, endpoints y redes para prevenir accesos no autorizados y ataques.

Beneficios para tu empresa

- Menos superficies de ataque.
- Continuidad operativa y protección de datos.
- Alineación con buenas prácticas de configuración.

Alcance y actividades

- Hardening de sistemas y servicios.
- Reglas de firewall y microsegmentación.
- Revisión de identidades, MFA y privilegios.
- Configuración segura en nube (CSPM y benchmarks CIS).
- Pruebas de resiliencia y recuperación.

Entregables

- Informe técnico con hallazgos clasificados por riesgo.
- Plan de cierre con responsables y plazos.
- Evidencias de remediación y verificación.
- Guía de continuidad y respaldo.

Modalidades

Assessment inicial con roadmap de 90 días o seguimiento trimestral.

5.Creación e Implementación de Políticas de Ciberseguridad

Qué hacemos

Diseñamos políticas y playbooks operativos que estandarizan la gestión de seguridad.

Beneficios para tu empresa

- Respuestas consistentes a incidentes.
- Claridad de responsabilidades por área.
- Evidencias para auditorías internas y externas.

Alcance y actividades

- Control de acceso y gestión de contraseñas. Clasificación de información y etiquetado.
- Respuesta a incidentes y notificación.
- Copias de seguridad y recuperación.
- Parcheo y gestión de vulnerabilidades.
- Uso aceptable y teletrabajo.
- Gestión de proveedores y acuerdos de nivel de servicio.

Entregables

- Políticas aprobadas por dirección.
- Procedimientos paso a paso y checklists.
- Playbooks por tipo de incidente.
- Calendario de revisión y mejora.

Modalidades

Diseño desde cero o actualización/armonización.

6. Asesoría Especializada

Qué hacemos

Consultoría para identificar riesgos, priorizar mitigaciones y fortalecer cumplimiento regulatorio.

Beneficios para tu empresa

- Visión externa experta.
- Decisiones informadas por impacto y probabilidad.
- Alineación entre negocio, legal y TI.

Alcance y actividades

Mapa de riesgos y evaluación de controles.
- Plan de mitigación con responsables.
- Sesiones ejecutivas y talleres técnicos.
- Acompañamiento en auditorías.

Entregables

Informe ejecutivo con brechas prioritarias.
- Roadmap de 30/60/90 días.
- Matriz RACI de responsabilidades.
- Bitácora de avances.

Modalidades

Bolsas de horas o proyectos por objetivo.

7. DAST — Pruebas Dinámicas de Seguridad de Aplicaciones

Qué hacemos

Analizamos aplicaciones web y APIs en ejecución para detectar fallas explotables en tiempo real: XSS, inyección SQL, fallas de autenticación y autorización, exposición de información, cabeceras inseguras y abuso de lógica de negocio.

Beneficios para tu empresa

- Complementa pruebas estáticas y revisiones manuales.
- Detecta problemas que emergen solo en entornos reales.
  Reduce riesgos antes del lanzamiento o durante operación.
-

Alcance y actividades

- Definición de objetivos y activos.
- Configuración de entorno de pruebas o staging.
  Escaneo dinámico y pruebas dirigidas autenticadas.
- Validación de falsos positivos y priorización por riesgo.
- Re-pruebas para verificación de cierre.
-

Entregables

- Informe ejecutivo con impacto en negocio.
  Reporte técnico con evidencias y PoC.
- Recomendaciones precisas por vulnerabilidad.
- Certificado de cierre por versión y alcance.
-

Modalidades

Evaluación puntual (pre-release) o monitoreo continuo integrado en CI/CD.

8. Pentesting (Pruebas de Penetración)

Qué hacemos:

Simulaciones controladas y autorizadas de ataques reales contra sistemas, redes, aplicaciones y dispositivos tecnológicos para identificar vulnerabilidades antes de que sean explotadas por actores maliciosos.

Beneficios para tu empresa

- Prevención de brechas de seguridad al detectar vulnerabilidades antes de que sean aprovechadas.
- Cumplimiento con regulaciones y auditorías (ISO 27001, PCI DSS, GDPR, entre otras).
- Reducción de pérdidas económicas y reputacionales por incidentes de ciberseguridad.
- Fortalecimiento de la postura de seguridad mediante evidencias técnicas y planes de remediación.
- Confianza y resiliencia digital ante clientes, socios y usuarios finales.

Alcance y actividades

- Pentesting de aplicaciones web
- Pentesting de redes internas y externas
- Pruebas en entornos de producción y/o pre-producción (según acuerdo)
- Explotación controlada, pruebas manuales y automatizadas
- Recomendaciones de corrección y priorización de vulnerabilidades
- Informe detallado con hallazgos, evidencias, grado de riesgo y plan de mitigación.

Entregables

- Informe técnico detallado con hallazgos, evidencias, riesgo y plan de mitigación.
- Resumen ejecutivo para dirección con impacto en negocio y acciones recomendadas.
- Certificado de evaluación con fecha, alcance y resultados principales.
- Repruebas y validaciones posteriores para verificar correcciones implementadas.

Modalidades

- Evaluación puntual: auditoría completa o dirigida antes de lanzamientos, migraciones o auditorías externas.
- Programa continuo: servicio recurrente trimestral o semestral para monitorear nuevas vulnerabilidades.
- Acompañamiento especializado: integración de un Red Team Hyperlab para entornos críticos o regulados.

9. Forensía Digital

Qué hacemos

Realizamos investigaciones técnicas especializadas para recolectar, preservar, analizar y presentar evidencia digital después de un incidente de seguridad. Nuestro equipo utiliza metodologías forenses reconocidas (NIST, ISO/IEC 27037, SANS) para determinar qué ocurrió, cómo, cuándo, por quién y con qué impacto, garantizando la integridad de la información y la trazabilidad del proceso.

Beneficios para tu empresa

- Identificación precisa de causas y responsables ante incidentes de seguridad.
- Cumplimiento regulatorio y soporte legal con evidencia válida y cadena de custodia documentada.
- Reducción de riesgos y tiempo de respuesta, evitando reincidencias por desconocimiento del ataque.
- Lecciones aprendidas que fortalecen la postura de seguridad institucional.
- Soporte especializado para reportes ante autoridades, aseguradoras o auditorías.

Alcance y actividades

- Recolección segura de evidencias digitales (logs, discos duros, redes, dispositivos móviles).
- Preservación de integridad y cadena de custodia conforme a estándares internacionales.
- Análisis técnico de malware, intrusiones o filtraciones de datos.
- Reconstrucción completa del incidente: cronología, vectores de ataque y alcance del daño.
- Apoyo en reportes oficiales o cumplimiento normativo, cuando sea requerido.
- Recomendaciones y plan de medidas correctivas con base en hallazgos y buenas prácticas.

Entregables

- Informe técnico forense con evidencias, hallazgos, impacto y trazabilidad.
- Resumen ejecutivo con implicaciones legales, regulatorias y estratégicas.
- Registro de cadena de custodia y bitácora de acciones realizadas.
- Reporte de lecciones aprendidas y recomendaciones preventivas.

Modalidades

- Respuesta a incidentes: servicio inmediato ante un evento detectado.
- Investigación post-incidente: análisis retrospectivo para reconstruir los hechos y generar evidencia legal.
- Servicio preventivo: preparación de protocolos, herramientas y personal para futuras investigaciones.

Conéctate con nuestro equipo y comienza a construir una empresa más cibersegura.

unidad-de-ciberseguidad

Cyber@upy.edu.mx
hyperlab@upy.edu.mx

UNIVERSIDAD POLITECNICA YUCATAN

#WeDesign TheFuture