UTN.BA
UNIVERSIDAD TECNOLÓGICA NACIONAL
FACULTAD REGIONAL BUENOS AIRES

Prevención de ransomware con IA

Información General

Fecha de inicio: 17/11/2026

Frecuencia: Semanal

Carga horaria por clase: 120 min

Presentación

Taller online e intensivo de dos semanas para equipos sin áreas especializadas en ciberseguridad, en particular cooperativas y organizaciones medianas y pequeñas. Cada organización parte de un análisis previo de ciberseguridad hecho solo con información pública, y sus hallazgos reales se usan como ejemplos de trabajo durante las cuatro sesiones. Los participantes aprenden a usar chats de inteligencia artificial para entender el informe, priorizar riesgos, resolverlos (correo, sitio web, DNS, accesos expuestos) y verificar el resultado con una nueva medición. La última sesión incluye una autoevaluación guiada de lo que el análisis externo no alcanza a ver (copias de respaldo, cuentas y permisos, actualizaciones, segunda autenticación) y un informe para la dirección. Metodología 100% práctica: la explicación no supera los 20 minutos por sesión y el resto es trabajo en laboratorio con acompañamiento docente.

Objetivos Generales

Que el personal técnico de cada organización pueda reducir su exposición al ransomware y a otros ataques, utilizando herramientas de inteligencia artificial para diagnosticar, priorizar, corregir y verificar problemas de seguridad sobre su propia infraestructura, con criterio y de forma segura.

Objetivos Específicos

- Interpretar con ayuda de IA un informe de ciberseguridad elaborado con información pública y priorizar los hallazgos por riesgo.
- Configurar la autenticación del correo (SPF, DKIM y DMARC) y publicar el contacto de seguridad (security.txt).
- Corregir problemas del sitio web y del DNS: cabeceras de seguridad, archivos expuestos, subdominios huérfanos y certificados vencidos.
- Restringir accesos expuestos (paneles de administración, webmail, sistemas de gestión) y activar la segunda autenticación.
- Verificar cada mejora con una nueva medición y detectar los errores de la IA.
- Realizar una autoevaluación interna guiada (respaldos, cuentas, actualizaciones, equipos y

proveedores) y elaborar un informe para la dirección.
- Aplicar reglas de uso seguro de la IA: información sensible, trabajo solo sobre el propio dominio y nada en producción sin verificar.

Destinatarios

- Personal técnico de cooperativas y organizaciones sin áreas especializadas en ciberseguridad.
- Responsables de sistemas, administradores de TI y proveedores de servicios.
- Integrantes de la conducción que quieran sumar formación con aval universitario.

Requisitos Previos

- Manejo básico de computadora e internet
- Acceso (propio o del proveedor) a la configuración del DNS y del sitio web de la organización
- Autorización firmada para colaborar en eventuales pruebas de penetración.

Plan de Estudios

Módulo 1: Resultados inmediatos:

- Se realizará un diagnóstico por empresa participante y se identificarán los hallazgos. Se definirá un plan de trabajo para atacar los problemas/hallazgos típcos

Módulo 2: Confianza:

- Se resuelven hallazgos del sitio y del DNS con el mismo método.

Módulo 3: Profundidad:

- Se cierran accesos expuestos, que ya tocan sistemas críticos.

Módulo 4: Lo que falta:

- Autoevaluación guiada por IA sobre copias de respaldo, cuentas y permisos, actualizaciones, segunda autenticación y equipos.

Bibliografía

- Guías de trabajo y prompts propios de cada laboratorio (material de la cátedra)
- Ley 25.326 de Protección de los Datos Personales.
- Documentación oficial de SPF, DKIM y DMARC (RFC 7208, RFC 6376 y RFC 7489).