



Programa de Capacitación 2026

Curso:

Cyber Risk Professional

Pensamiento Estratégico para Profesionales de Ciberseguridad

Curso a distancia

Objetivos:

Las organizaciones necesitan profesionales capaces de traducir riesgos técnicos en decisiones de negocio. Sin embargo, gran parte de la formación disponible se centra en herramientas o cumplimiento normativo, dejando en segundo plano el desarrollo del criterio profesional. Este curso fue diseñado para cerrar esa brecha.

Este es un programa especializado en gestión de riesgos de ciberseguridad, con énfasis en la evaluación de identidades privilegiadas (Privileged Access Management - PAM), el uso de inteligencia artificial como apoyo al análisis y la gestión de los riesgos asociados a ese uso.

Está dirigido a profesionales en transición hacia roles de Gestión de Riesgos y Cumplimiento (GRC), analistas de seguridad plenos y consultores junior que buscan desarrollar capacidad de análisis crítico y toma de decisiones en contextos corporativos reales.

El enfoque es profesional, pragmático y orientado a resultados medibles. La gestión de identidades privilegiadas (PAM) es el caso de estudio transversal para recorrer la identificación, análisis, cuantificación y tratamiento del riesgo. Se integran ISO/IEC 27005:2022, ISO/IEC 23894:2023 e ISO/IEC 42001:2023 con un alcance introductorio y aplicado al caso, orientado al criterio profesional.

Secretaría de Extensión Universitaria y Vinculación Tecnológica

Whatsapp +54 9 341 394-5235

seu@frro.utn.edu.ar

capacitacion@frro.utn.edu.ar

Contenidos por clase

SESIÓN 1: Fundamentos de Riesgo en Ciberseguridad

Duración: 90 minutos

Objetivo: Construir el modelo mental de la gestión de riesgos y relacionar el riesgo técnico con el impacto para el negocio, tomando ISO/IEC 27005 como referencia metodológica.

Contenido

1. Riesgo = Probabilidad x Impacto
2. Contexto, criterios de evaluación y matriz de riesgo corporativa.
3. ISO/IEC 27005:2022 y NIST RMF: enfoques complementarios. Relación con ISO/IEC 23894:2023 e ISO/IEC 42001:2023.
4. Riesgo Técnico vs Riesgo de Negocio.
5. Introducción a la cuantificación del impacto económico.

Uso de Inteligencia Artificial

- Generación de escenarios de amenazas.
- Identificación preliminar de activos y vulnerabilidades.
- Construcción asistida de matrices de riesgo.
- Validación humana de resultados y reglas de uso: datos de práctica anonimizados, sin credenciales ni información sensible.

Ejercicio Práctico 1: Análisis de un incidente utilizando logs y línea de tiempo. Identificación de amenazas, vulnerabilidades, impacto y detectabilidad.

SESIÓN 2: Evaluación Técnica de Riesgos y Acceso Privilegiado

Duración: 90 minutos

Objetivo: Identificar y evaluar riesgos de identidades privilegiadas, considerando también los riesgos del uso de IA como apoyo al análisis.

Contenido:

6. Anatomía del Riesgo de Acceso Privilegiado.
7. Movimiento lateral y escalamiento de privilegios.
8. Evaluación del estado actual de accesos privilegiados.
9. Técnicas de relevamiento de información.
10. Escenarios de riesgo corporativo y riesgos del análisis asistido por IA: introducción aplicada a ISO/IEC 23894.

Uso de Inteligencia Artificial

- Interpretación preliminar de logs y eventos.
- Generación de hipótesis sobre posibles vectores de ataque.
- Identificación inicial de riesgos.
- Contraste con evidencia: datos incompletos, errores, sesgos, exposición de información y confianza excesiva en la IA.

Ejercicio Práctico 2: Evaluación de un entorno con capturas de Active Directory, políticas y registros de auditoría anonimizados. Contraste del análisis de IA con la evidencia e identificación de un riesgo de su uso y una medida de control.

SESIÓN 3: Arquitectura para la Gestión de Accesos Privilegiados (PAM)

Duración: 90 minutos

Objetivo: Comprender el rol de PAM dentro de una arquitectura de seguridad y los controles que permiten reducir los riesgos asociados a cuentas privilegiadas.

Contenido:

11. Qué problemas resuelve PAM y cuáles requieren controles complementarios.
12. Principios de mínimo privilegio (Least Privilege), Just-In-Time (JIT) y Just-Enough Administration (JEA).
13. Componentes de una solución PAM: Vault, Password Rotation, Session Recording, Password Checkout y Break Glass.
14. Integración con Active Directory, MFA, SIEM, ITSM y EDR.
15. Arquitectura de controles PAM y su relación con el tratamiento del riesgo según ISO/IEC 27005.

Uso de Inteligencia Artificial

- Análisis de documentación técnica y datasheets.
- Resumen de funcionalidades y capacidades.
- Generación de preguntas para entrevistas de relevamiento.
- Identificación de controles asociados a distintos escenarios de riesgo.

Ejercicio Práctico 3: Análisis de un entorno con cuentas privilegiadas compartidas. Identificación de controles existentes, controles faltantes y evaluación del riesgo residual.

SESIÓN 4: Evaluación de Soluciones y Toma de Decisiones Basada en Riesgo

Duración: 90 minutos

Objetivo: Aprender a seleccionar soluciones de seguridad considerando el contexto del negocio, el riesgo residual, el costo y la viabilidad de implementación.

Contenido:

16. Mapeo de riesgos a requisitos funcionales y no funcionales.
17. Evaluación comparativa de soluciones PAM.
18. Tratamiento, riesgo residual y criterios de aceptación según ISO/IEC 27005.
19. Análisis costo-beneficio (TCO) y priorización de controles.
20. Estrategias de implementación incremental y roadmap de mitigación.

Uso de Inteligencia Artificial

- Elaboración de matrices comparativas.
- Análisis de alternativas y, cuando incorporen IA, de sus riesgos y dependencia del proveedor.
- Generación de propuestas de mitigación.
- Identificación de riesgos residuales y posibles brechas.

Ejercicio Práctico 4: Evaluación comparativa de dos propuestas PAM para organizaciones con perfiles de riesgo diferentes. Justificación de la alternativa seleccionada considerando cobertura, complejidad, integración y costo.

SESIÓN 5: Comunicación Ejecutiva y Gobierno del Uso de IA

Duración: 90 minutos

Objetivo: Comunicar riesgos al negocio y definir responsabilidades, controles y seguimiento del uso de IA, con una introducción aplicada a ISO/IEC 42001 e ISO/IEC 23894.

Contenido:

21. Traducción del riesgo técnico a impacto para el negocio.

22. Recomendaciones ejecutivas y justificación de inversiones basada en riesgo.

23. ISO/IEC 23894: evaluación y tratamiento de riesgos del uso de IA en el análisis.

24. ISO/IEC 42001: introducción al sistema de gestión de IA, políticas, responsabilidades y mejora continua.

25. Aplicación al caso: autorización de uso, datos permitidos, validación humana, trazabilidad y seguimiento de errores.

Uso de Inteligencia Artificial

- Redacción asistida de informes ejecutivos.
- Adaptación del lenguaje según la audiencia.
- Validación y contraste de información.
- Registro de herramienta y modelo/versión disponible, fecha, prompt, fuentes de entrada y validación humana, sin exponer datos sensibles.

Ejercicio Práctico 5: Elaboración de un resumen ejecutivo para Dirección con apoyo de IA. Justificación de la recomendación y definición de responsables, controles y seguimiento para los riesgos de ese uso.

SESIÓN 6: Integración y Trabajo Final

Duración: 90 minutos

Objetivo: Integrar la evaluación y el tratamiento de riesgos de ciberseguridad con el análisis de los riesgos del uso de IA en un caso empresarial realista.

Estructura del Trabajo Final (12-16 páginas)

26. Resumen Ejecutivo.

27. Contexto del Negocio y Alcance.

28. Identificación de Activos, Amenazas y Vulnerabilidades.

29. Evaluación y Priorización de Riesgos.

30. Arquitectura de Controles y Evaluación de Soluciones.

31. Impacto Económico y Riesgo Residual.

32. Plan de Tratamiento, Responsables, Seguimiento y Roadmap de Implementación.

33. Riesgos del Uso de IA, Controles, Trazabilidad y Reflexión Crítica sobre el Análisis.

Uso de Inteligencia Artificial

- Revisión de consistencia del informe final.
- Identificación de omisiones y oportunidades de mejora.
- Asistencia en la organización y redacción del documento.
- Verificación de claridad, coherencia y calidad de la presentación ejecutiva.
- Documentación del uso de IA, sus limitaciones y la validación final por parte del participante.

Trabajo Final: Evaluación integral de riesgos con ISO/IEC 27005 como referencia. Incluir una evaluación breve de los riesgos del uso de IA apoyada en ISO/IEC 23894 y proponer responsabilidades y seguimiento tomando como referencia ISO/IEC 42001.

**Destinatarios:**

Profesionales de ciberseguridad, tecnología y consultoría que quieran fortalecer sus capacidades de gestión de riesgos y uso responsable de inteligencia artificial.

Certificación

Se otorgará certificado digital de asistencia, emitido por Universidad Tecnológica Nacional a través de la Facultad Regional Rosario.

Inicio: Lunes 26 de octubre de 2026

Días de dictado y horario: Lunes de 19:00 a 20:30 horas.

Duración: 9 horas de clases virtuales sincrónicas divididas en seis encuentros los lunes 26/10, 02/11, 09/11, 16/11, 23/11 y 30/11.

Al menos 20 horas de trabajo individual de los y las participantes con asistencia del docente.

Inversión: (Pago mediante transferencia bancaria):

Alumnos, Graduados y Docentes de UTN – CIE – Bolsa de Comercio Rosario – Centro Universitario de Firmat: \$90000 (pesos noventa mil).

Particulares y Empresas: \$110000 (pesos ciento diez mil).

(Consultar costos especiales a Empresas con tres o más asistentes)

Somos UCAP – La UTN – FRRosario está registrada como Unidad Capacitadora. Los cursos que dictamos pueden canalizarse a través del Régimen de Crédito Fiscal para capacitación.

Secretaría de Extensión Universitaria y Vinculación Tecnológica

Whatsapp +54 9 341 394-5235

seu@frro.utn.edu.ar

capacitacion@frro.utn.edu.ar



Disertantes:

Cristian Stolarowa

Licenciado en Informática. Project Management Professional (PMP). Certificaciones profesionales y formación especializada en Gestión de Riesgos, Gobierno de Seguridad, Gestión de Proyectos y Ciberseguridad. (CRISC, CISM, ISO 27001/Level 2). Formación en normas y marcos internacionales como ISO 27001, ISO 27005 y NIST. Más de 30 años liderando proyectos de tecnología, ciberseguridad y gestión del riesgo. Ex Chief Information Security Officer (CISO). Ex Líder de Gestión de Riesgos de Ciberseguridad. Project Manager en proyectos corporativos de transformación tecnológica. Perito Informático Forense.

Inscripción:

Secretaría de Extensión Universitaria y Vinculación Tecnológica

Whatsapp +54 9 341 394-5235

seu@frro.utn.edu.ar

capacitacion@frro.utn.edu.ar

Para inscribirse:

<https://forms.gle/oHjdaRKAoHkayaRZA>

Secretaría de Extensión Universitaria y Vinculación Tecnológica

Whatsapp +54 9 341 394-5235

seu@frro.utn.edu.ar

capacitacion@frro.utn.edu.ar