SYLLABUS DE LA ASIGNATURA

ASIGNATURA	**GESTIÓN DE RIESGOS**	**NRC**	**3401**
COD	**25.S3.CIBER-4003.VR.A.3401**	**PAO**	*25.S3*
1. DATOS GENERALES			
ESCUELA	*ETEI*	**CARRERA**	*CIBERSEGURIDAD*
SEMESTRE	*Cuarto*	**CRÉDITOS**	*2.5*
HORAS COMPONENTE DOCENTE	**48**	**PRERREQUISITOS**	*HACKING ÉTICO* *SEGURIDAD EN LA RED*
HORAS COMPONENTE PRÁCTICO	**42**	**HORARIO**	*Lunes: 18:30 a 20:45* *Viernes: 18:30 a 20:00*
HORAS COMPONENTE AUTÓNOMO	**30**	**AULA/ LABORATORIO**	*Aula virtual*
PROFESOR(A)	*Jorge Luis Armijo Quito*		
CONTACTO	*jarmijo@tesa.edu.ec*		
HORARIO DE ATENCIÓN A ESTUDIANTES	*Jueves de 18:00 a 19:00 mediante videoconferencia / 0992554661*		

2. RESULTADOS DE APRENDIZAJE DE LA ASIGNATURA		NIVEL
1	Comprender los fundamentos de la gestión de riesgos en el contexto de la ciberseguridad, incluyendo los marcos de referencia y estándares relevantes.	Medio
2	Identificar y evaluar las amenazas y vulnerabilidades asociadas a los sistemas y redes, así como sus posibles impactos en la seguridad de la información.	Medio
3	Aplicar técnicas de identificación y análisis de riesgos para determinar la probabilidad y el impacto de los incidentes de seguridad en los sistemas y redes.	Medio
4	Utilizar herramientas y metodologías de evaluación de riesgos para medir y priorizar los riesgos identificados en función de su nivel de criticidad.	Medio
5	Desarrollar e implementar planes de tratamiento de riesgos, incluyendo la selección y aplicación de controles y contramedidas apropiadas.	Medio
6	Establecer procesos de monitoreo y seguimiento continuo de los riesgos para identificar cambios en el entorno de seguridad y tomar acciones correctivas en consecuencia.	Medio
7	Gestionar la evaluación de riesgos de seguridad en los sistemas y redes informáticas. Implementar medidas de seguridad para proteger los sistemas y datos contra amenazas cibernéticas. Configurar y administrar herramientas y sistemas de seguridad, como firewalls y sistemas de detección de intrusiones. Gestionar eficientemente incidentes de seguridad, incluyendo la detección, respuesta y recuperación.	Perfil de Egreso

	Evaluar y mejorar constantemente las políticas y prácticas de seguridad de una organización.	

3. OBJETIVO DE LA ASIGNATURA

El objetivo de la asignatura Gestión de Riesgos es proporcionar a los estudiantes los conocimientos y habilidades necesarios para comprender, aplicar y evaluar los principios y procesos de gestión de riesgos en el ámbito de la ciberseguridad, con el fin de identificar, evaluar y mitigar los riesgos asociados a las amenazas y vulnerabilidades en los sistemas y redes

4. CONTENIDOS DE LA ASIGNATURA

Unidad 1
DEFINICIÓN Y TIPOS DE RIESGOS EN CIBERSEGURIDAD
Unidad 2
FUNDAMENTOS DE GESTIÓN DE RIESGOS EN CIBERSEGURIDAD
Unidad 3
EVALUACIÓN Y MEDICIÓN DE RIESGOS EN CIBERSEGURIDAD
Unidad 4
CASOS PRÁCTICOS

5. METODOLOGÍA Y APLICACIÓN PRÁCTICA

Las metodologías de enseñanza utilizadas para impartir las asignaturas de TESA, fomentan la construcción del conocimiento mediante el constante intercambio de ideas y propuestas científicas y técnicas, así como experiencias entre profesores y estudiantes. En todas las asignaturas los contenidos teóricos serán vinculados con la práctica profesional y el contexto laboral donde se desempeñarán los estudiantes a futuro, procurando implementar actividades y simulaciones de diversa índole, por lo que los estudiantes deberán aprobar el aspecto teórico y el laboratorio de manera simultánea.
Se jerarquiza el aprendizaje centrado en el estudiante y basado en la filosofía de las Artes Liberales, priorizando métodos productivos como: mesas redondas, exposiciones, paneles, discusiones temáticas estudio de casos y solución de problemas en contextos reales.

6. EVALUACIÓN

TIPO DE EVALUACIÓN	DESCRIPCIÓN GENERAL	PORCENTAJE DE LA NOTA PARCIAL
Participación	*Aportes adicionales y respuestas a preguntas realizadas en clase por parte del estudiante serán evaluados sobre 10 ptos.*	**10%**
Deberes	• *Análisis de casos de los tipos de riesgos en ciberseguridad, se debe resaltar la descripción de la temática, el propósito correspondiente y un ejemplo que evidencie lo abordado en el caso. 5 ptos.* • *Realizar un análisis comparativo entre amenazas tradicionales (ej. virus, phishing, malware básico) y amenazas emergentes (ej. ransomware, ataques a la cadena de suministro, amenazas impulsadas por IA). El trabajo debe destacar la evolución de estas amenazas, su nivel de riesgo y cómo han cambiado las estrategias de defensa en las organizaciones. 5 ptos.* • *Presentación y taller grupal de las etapas del proceso de gestión de riesgos, se resalta y describe la temática, el propósito y ejemplos que evidencien la temática seleccionada. 10 ptos.* • *Ejercicios prácticos utilizando simuladores para evidenciar vulnerabilidades en los sistemas de*	**25%**

	Información, y plasmarlo en un informe que resalte los resultados obtenidos. 5 ptos.	
Actividad	• *Discusión grupal donde los estudiantes participarán en una simulación de incidentes de ciberseguridad asumiendo distintos roles (CISO, analista, líder de respuesta, etc.). Deberán identificar amenazas, proponer acciones de mitigación y debatir en grupo las decisiones tomadas. 5 ptos.* • *Cada grupo investigará un método reconocido de evaluación de riesgos (ISO 27005, NIST SP 800-30, OCTAVE, MAGERIT, FAIR) y elaborará un ensayo breve. En clase expondrán el método y un caso práctico. 10 ptos.* • *Desarrollo de aula invertida donde los estudiantes aplicarán técnicas de medición de riesgos (matrices de impacto/probabilidad y ranking de criticidad) sobre un caso simulado. Deberán priorizar riesgos y justificar sus decisiones. 10 ptos.*	**25%**
Foro 1	• *Foro de las técnicas de identificación de riesgos, Los estudiantes seleccionarán una técnica de identificación de riesgos (ej. entrevistas, checklists, análisis de escenarios) y explicarán su aplicación en un caso real o en bibliografía académica. Posteriormente, deberán comentar al menos un aporte de un compañero con un análisis crítico. 5 ptos.* • *Foro de los riesgos en ciberseguridad que afrontan las organizaciones, los estudiantes investigaran un caso reciente de riesgo cibernético (ej. ransomware, fuga de datos, ataque a la cadena de suministro), describirá su impacto y la respuesta de la organización. Luego, debatirá con un compañero contrastando similitudes y diferencias entre casos. 5 ptos.*	**10%**
Prueba	• *Control de lectura de los tipos de riesgos en ciberseguridad. Se debe evidenciar los datos del autor, Título del texto, Introducción del texto, Desarrollo con preguntas y respuestas sobre las ideas principales, Opinión argumentada, Conclusión, Bibliografía. 5 ptos.* • *Evaluación de casos prácticos en ciberseguridad mediante la formulación de preguntas de opción múltiple y un laboratorio práctico que permitan evidenciar el avance de los estudiantes. 10 ptos.*	**15%**
	TOTAL PARCIAL	**85%**
Evaluación Final	*La evaluación final será evaluada sobre 15 ptos. y corresponde al porcentaje descrito, la misma es de carácter acumulativo con preguntas de opción múltiple, verdadero y falso, paridad*	**15%**

	y un laboratorio práctico que permitan evidenciar el avance integral de los estudiantes.	
	TOTAL	**100%**

7. SISTEMA DE EVALUACIÓN

Calificación parcial: durante el parcial el docente evaluará los siguientes criterios de manera OBLIGATORIA y obtendrá un promedio de estos. Los cuales se evalúan de manera OBLIGATORIA en la plataforma académica D2L:

- Participación en clase: El docente evaluará la atención y participación del estudiante durante la clase ya sea virtual o presencial.

- Deberes: Pueden ser de carácter individual o grupal, enviados a casa, con el objetivo de reforzar lo aprendido en clase, estos pueden ser:
  - Investigaciones
  - Trabajos didácticos y prototipos
  - Estudios de caso
  - Ensayos y demás

- Actividades en clase: Pueden ser de carácter individual o grupal, son realizados en clases, entre las actividades pueden estar:
  - Prácticas e informes
  - Exposiciones
  - Trabajos en grupo
  - Estudios de caso
  - Mesas redondas
  - Otras actividades en clase

- Foros de discusión: En la plataforma académica D2L, el docente generará espacios abiertos para la discusión de temas específicos, con el propósito de que los estudiantes interactúen intercambiando ideas, teorías y opiniones, promoviendo un debate sano y ampliando el criterio y visión del estudiante.

- Pruebas parciales: Son pruebas cortas, que evalúan unidades en específico, nunca de carácter acumulativo.

Se incluyen en esta categoría:
  - Controles de lectura
  - Lecciones orales o escritas no acumulativas.

Proyecto Final/Examen Final: La evaluación final puede ser un proyecto o un examen, de carácter acumulativo, que pretende evaluar los resultados de aprendizaje adquiridos por el estudiante a lo largo de la asignatura. Puede ser de carácter práctico, teórico o ambos.

El docente definirá qué actividades son estrictamente individuales y cuáles son de valoración grupal, de ser este el caso diseñará los mecanismos para que la evaluación sea totalmente justa, objetiva, transparente y mida también el aporte de cada estudiante en el trabajo.

Descripción de la calificación final:

CALIFICACIÓN		VALORACIÓN	PUNTAJE
PARCIAL	**Participación**	10%	10 puntos
	Deberes	25%	25 puntos
	Actividades	25%	25 puntos

	Foros	10%	10 puntos
	Pruebas	15%	15 puntos
Evaluación Final		15%	15 puntos
Total		**100%**	**100 puntos**

Asistencia: Para aprobar la asignatura, el estudiante regular debe cumplir con un mínimo del **75% de asistencia** a las horas de clase tanto presenciales como virtuales sincrónicas de la asignatura, lo que significa que un estudiante puede ausentarse un máximo de 2 veces durante el semestre sin penalidad.
Con la segunda falta injustificada el estudiante perderá los puntos correspondientes a participación, a discreción del profesor.
Si el estudiante se ausenta de manera injustificada por más de 2 ocasiones, obtendrá automáticamente una F y reprobará la asignatura, sin posibilidad alguna de apelación.

Para que la asignatura sea considerada aprobada, el estudiante debe cumplir con lo establecido tanto para la calificación final como para la asistencia.

8. ESCALA Y EQUIVALENCIA DE VALORACIÓN CALIFICACIÓN FINAL

CALIFICACIÓN	INTERPRETACIÓN	RANGO	PROMEDIO GPA
A	Excelente	91 a 100	4
B	Bueno	81 a 90.99	3
C	Regular	71 a 80.99	2
D	Deficiente	61 a 70.99	1
F	Reprobado	Igual o menor a 60.99	0

9. BIBLIOGRAFÍA

UNIDADES	BIBLIOGRAFÍA
Unidad 1	*Moreno García, M. (2022). Gestión de incidentes de ciberseguridad: (1 ed.). RA-MA Editorial. https://elibro.net/es/lc/tesa/titulos/222669*
Unidad 3	*Moreno García, M. (2022). Gestión de incidentes de ciberseguridad: (1 ed.). RA-MA Editorial. https://elibro.net/es/lc/tesa/titulos/222669*
Unidad 4	*Arroyo Guardeño, D. Gayoso Martínez, V. & Hernández Encinas, L. (2020). Ciberseguridad: (ed.). Editorial CSIC Consejo Superior de Investigaciones Científicas. https://elibro.net/es/lc/tesa/titulos/172144*
Unidad 5	*Deutsch, V. E. (2022). Ciberseguridad para directivos: riesgos, control y eficiencia de las tecnologías de la información: (1 ed.). LID Editorial España. https://elibro.net/es/lc/tesa/titulos/269669*

10. ENLACES RECOMENDADOS

- Canal Once. (25 de 03 de 2024). Canal Once. Obtenido de Canal Once: *https://www.youtube.com/watch?v=SzE2ydciRwA*
- IBM. (12 de 08 de 2024). IBM. Obtenido de IBM: *https://www.ibm.com/es-es/topics/cybersecurity*
- Amazon. (05 de 12 de 2024). AWS. Obtenido de AWS: *https://aws.amazon.com/es/what-is/cybersecurity/*
- YOUTUBE. (11 de 02 de 2023). Youtube. Obtenido de Youtube: *https://www.youtube.com/watch?v=z6Tr9bxBHNk*
- *Virtual Training Lteam. (04 de 07 de 2019). Virtual Training Lteam. Obtenido de Virtual Training Lteam: https://www.youtube.com/watch?v=k5gblbzHeFI*

11. POLÍTICAS

Todas las asignaturas de TESA están sujetas al Reglamento General de Estudiantes, a las normas de ética de aprendizaje, ética de la investigación y ética del comportamiento que constan en el Código de Ética, así como a las políticas y procedimientos de la institución; por tanto:

▪ En todas las clases virtuales, los estudiantes deben encender de manera **OBLIGATORIA** sus cámaras; en caso de no hacerlo, esto será tomado como **INASISTENCIA**.
▪ La participación es sumamente importante, no se podrá, bajo ningún motivo, chatear o realizar actividades ajenas a la clase; si el estudiante incurre en dicha falta, perderá puntos correspondientes a **PARTICIPACIÓN**.
▪ El docente, de manera **OBLIGATORIA**, deberá tomar asistencia en **TODAS** sus clases, ya sean virtuales o presenciales, a través de la plataforma D2L.
▪ Se considera retraso a clases a partir de los **5 minutos**. Tres atrasos de **hasta 10 minutos** al inicio de la clase presencial o virtual, contarán como **1 INASISTENCIA**.
▪ Cada atraso **superior a 10 minutos** al inicio de la clase presencial o virtual se considerará automáticamente como **INASISTENCIA**.
▪ El **ABANDONO** de la clase virtual o presencial, previo al fin de esta, constituye **INASISTENCIA** a dicha clase.
▪ En caso de que la inasistencia sea por motivos comprobables como: calamidad, accidente o enfermedad comprobable mediante certificado, este deberá ser validado y sellado, hasta **UNA SEMANA DESPUÉS** de ocurrido el evento, por parte del Director de Carrera, para poder ser presentado a los docentes. Pasado el tiempo establecido, **NO** se podrá justificar dicha falta.
▪ Los estudiantes que se ausenten al **EXAMEN FINAL**, podrán recuperarlo hasta una semana después de la fecha establecida, **SÓLO CON JUSTIFICACIÓN** médica o calamidad doméstica (duelo familiar) verificada por la Dirección de Carrera.
▪ **BAJO NINGUNA CIRCUNSTANCIA**, los deberes o trabajos pueden ser recibidos por el profesor por e-mail o WhatsApp, únicamente pueden ser entregados a través de la plataforma académica **D2L**.
▪ Los trabajos y deberes **NO SERÁN RECIBIDOS** después de la fecha establecida, si no existe una justificación comprobada. Dependerá del profesor, si acepta o no dicho trabajo y la justificación en caso de existir.
▪ Todos los ensayos, investigaciones, artículos, etc. deberán ser realizados siguiendo la **Normativa APA 7ma edición**. Los docentes deberán exigir y controlar el estricto cumplimiento de dichas normas, así como el contenido de la siguiente información en la portada del documento:

- o Código y nombre de la asignatura
- o Código, nombre y apellido del estudiante
- o Título del trabajo de acuerdo con lo que consta en el apartado 7 del presente documento
- o Fecha de entrega (Día-Mes-Año)

▪ El Tecnológico San Antonio cuenta un sistema avanzado para la **DETECCIÓN DE PLAGIO** y autoplagio, integrado a la plataforma D2L, y TODOS los trabajos sin excepción, serán revisados con esta herramienta, por ello, más del **20% de similitud** entre trabajos de estudiantes de este u otro grupo, o de publicaciones en el internet se tomará como **plagio**, lo cual constituye una falta **MUY GRAVE** dentro de la institución y será penalizado acorde a los lineamientos establecidos en el Código de Ética de TESA.
▪ Esta institución considera también el **autoplagio** como una falta **MUY GRAVE**. No se puede reproducir parcial o totalmente los trabajos realizados para una asignatura y presentarlos en otra. En caso de incurrir en esta falta será penalizado en la calificación del trabajo, acorde a los lineamientos establecidos en el Código de Ética de TESA.
▪ TESA considera también el uso de herramientas de **Inteligencia Artificial** como una falta **MUY GRAVE**. En caso de incurrir en esta falta será penalizado en la calificación del trabajo, acorde a los lineamientos establecidos en el Código de Ética de TESA.
▪ El docente se compromete a calificar trabajos, informes y exámenes en un plazo **no superior a 15 días** después de entregados o rendidos, los que estarán subidos a la plataforma virtual D2L en el mismo plazo.

12. CRONOGRAMA DE ACTIVIDADES

FECHA	TEMA O TRABAJO EN CLASE	ACTIVIDAD EVALUADA

Semana N°1 25/08/2025	Presentación de Syllabus, políticas y dinámica de la asignatura. **Unidad 1:** DEFINICIÓN Y TIPOS DE RIESGOS EN CIBERSEGURIDAD • Definición y tipos de riesgos. • Conceptos básicos de riesgo en ciberseguridad.	
Semana N°1 29/08/2025	• Clasificación de riesgos (operacionales, técnicos, humanos, estratégicos). Análisis de casos recientes.	Deber 1
Semana N°1	**Asincrónico:** Análisis de los ataques sobre phishing, ingeniería social, Hacking de contraseñas.	
Semana N°2 01/09/2025	• Principales amenazas y su evolución. • Tendencias globales de riesgos cibernéticos.	
Semana N°2 05/09/2025	• Factores que influyen en los riesgos: humanos, tecnológicos, normativos. Discusión guiada.	Deber 2
Semana N°2	**Asincrónico:** Riesgos ocultos cuando la infraestructura tecnológica falla.	
Semana N°3 08/09/2025	**Unidad 2:** FUNDAMENTOS DE GESTIÓN DE RIESGOS EN CIBERSEGURIDAD • Introducción a marcos de referencia: ISO 27005, NIST, ENISA.	Deber 3
Semana N°3 12/09/2025	• Etapas del proceso de gestión de riesgos.	
Semana N°3	**Asincrónico:** Análisis de los riesgos derivados del factor humano en ciberseguridad (errores, negligencia, ingeniería social).	

Semana N°4
15/09/2025
	• Herramientas para la gestión de riesgos:
	  ○ Matrices de impacto
	  ○ Análisis cualitativo y cuantitativo.
	• Mitigación de riesgos.
		Deber 4

Semana N°4 19/09/2025	• Roles y responsabilidades en la gestión de riesgos • Dinámica de simulación.	Actividad 1
Semana N°4	**Asincrónico:** Estudio de procesos para la gestión de riesgos en instituciones públicas y privadas.	
Semana N°5 22/09/2025	**Unidad 3:** EVALUACIÓN Y MEDICIÓN DE RIESGOS EN CIBERSEGURIDAD • Métodos y Técnicas de evaluación de riesgos	Actividad 2
Semana N°5 26/09/2025	• Medición del impacto y priorización de riesgos. Taller práctico.	Actividad 3
Semana N°5	**Asincrónico:** Revisión de herramientas para la detección de vulnerabilidades.	
Semana N°6 29/09/2025	• Niveles de riesgos y criterios de aceptación. **Unidad 4:** CASOS PRÁCTICOS EN ESCENARIOS SIMULADOS	Foro 1
Semana N°6 03/10/2025	• Simulación de gestión de riesgos	Prueba 1
Semana N°6	**Asincrónico:** Análisis de simulador para la gestión de riesgos	
Semana N°7 06/10/2025	• Evaluación de riesgos en infraestructura simulada. Identificación de controles efectivos	Foro 2

Semana N°7 10/10/2025	• Evaluación de la efectividad de los controles implementados. • Debate en clase.	Prueba 2
Semana N°7	**Asincrónico:** Proceso para proteger la información de las organizaciones.	
Semana N°8 13/10/2025	• Repaso general de conceptos, herramientas y prácticas. • Preparación de examen final.	
Semana N°8 17/10/2025	• Evaluación Final	Evaluación Final
Semana N°8	**Asincrónico:** Análisis de vulnerabilidades más comunes	

13. ELABORACIÓN, REVISIÓN Y APROBACIÓN

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Profesor	**Decano de Escuela/ Dirección de Carrera**	**Vicerrectorado Académico**
Firmado electrónicamente por: JORGE LUIS ARMIJO QUITO Validar únicamente con FirmaEC Jorge Armijo	Santiago Rojas	Katiuska Espinoza
Fecha: 25/08/2025	Fecha: 25/08/2025	Fecha: 25/08/2025

Este PEA fue revisado por el Decanato de Planificación Académica y aprobado por el Vicerrectorado Académico del Tecnológico San Antonio TESA, por lo que todos los profesores que dicten la asignatura deben regirse a este programa y sus políticas. En caso de que sea necesario realizar cambios/ajustes al plan de estudio, debe solicitarlo a Vicerrectorado Académico para su aprobación y actualización en el sistema de Diseño Curricular.