



## Asignatura Insignia Ciberseguridad

Para evaluar el módulo de “Introducción y estándares de Ciberseguridad” los alumnos deberán elaborar un documento con las siguientes reglas:

1. De manera individual y personal, sin usar herramientas de inteligencia artificial.
2. No hay límite en la extensión del documento, pero su valor debería rondar entre 10 y 20 páginas.
3. Utilizar la plantilla de un documento científico publicado en la IEEE de una conferencia. La última versión se puede consultar en:
  - a. <https://www.ieee.org/conferences/publishing/templates.html>
4. La fecha de entrega límite es 15 días naturales después de la última clase. Por ejemplo, para el semestre 2025-A, la fecha límite es el 19 de marzo del 2025 a las 23:59 hrs.
5. El documento tiene que ser enviado al correo electrónico [racostab@ipn.mx](mailto:racostab@ipn.mx) con copia al correo [racosta@cic.ipn.mx](mailto:racosta@cic.ipn.mx) y en la sección Asunto poner una cadena separada por comas y formada con los siguientes datos:
  - a. “Insignia Ciber”
  - b. Año-Semestre con letra A y B para el primero y segundo semestre respectivamente
  - c. Nombre completo empezando por los nombres.

Por ejemplo: “Insignia Ciber, 2025-A, Raúl Acosta Bermejo”

6. El documento será revisado con varias herramientas de TICs para verificar su originalidad (no exista plagio). En particular se usará Turnitin y el porcentaje de similitud debe ser a lo más del 30%.
7. El objetivo del documento es realizar un ensayo sobre uno de los estándares (o manuales o guías o mejores prácticas, etc.) de la **Tabla 1**, en el cual deben:
  - a. Enunciar y explicar en qué casos se usa el estándar. Haga un mapa mental o conceptual: no lo incluya en el documento ya que será un documento anexo (imagen PNG de alta resolución).
  - b. Analizar con otros estándares que hagan lo mismo en relación con los elementos más fundamentales como definiciones, modelos, etc.
  - c. Comparar a detalle con otros estándares que traten temas similares, enunciando diferencias y en qué casos se usan esas diferencias.
  - d. Por último, explicar cómo lo aplicarían a un pequeño ejemplo para entenderlo. El caso más sencillo es que consideren la red de su casa.

El incumplimiento de las reglas tiene como consecuencia una penalización en la calificación final del módulo y en algunos casos la anulación del trabajo (calificación de cero).



No	Tema
1	CIS Controls
2	ISO 27001
3	ISSAF
4	MAGERIT
5	MITRE ATT&CK
6	MITRE CVE CWE
7	NIST Cybersecurity Maturity Model
8	OSSTM
9	OWASP
10	GDPR

**Tabla 1.** Lista de estándares a utilizar.

Elaborado:

- Por Raúl Acosta Bermejo.
- Ciudad de México a 5 de febrero de 2025.
- Versión 1.0

===== FIN DEL DOCUMENTO =====



## Temario del Módulo

No	Unidad
1	Introducción a la Ciberseguridad
	Definición de ciberseguridad y conceptos del área
	Estándares de TICs y de Ciberseguridad
	SANS: Capacitación y certificaciones
2	ISO 27001
	NIST: CSF
3	MITRE ATT&CK
	MITRE CVE CWE
	MITRE Defense, IA, etc.
4	OSSTM
	CIS Controls
5	OWASP
	ISSAF
	MAGERIT
6	GDPR