ceti
CENTRO DE ENSEÑANZA TÉCNICA INDUSTRIAL

PROGRAMA DE ESTUDIOS

CIBERSEGURIDAD

TECNÓLOGO EN DESARROLLO DE SOFTWARE

OCTAVO SEMESTRE

EDUCACIÓN MEDIA SUPERIOR


IMPORTANTE
IMPORTANTE

Ciberseguridad. Programa de Estudios. Tecnólogo en Desarrollo de Software. Octavo Semestre, fue editado por el Centro de Enseñanza Técnica Industrial de Jalisco.

Segunda edición, 2025.

Nueva Escocia No. 1885, Col. Providencia 5ª sección, C. P. 44638, Guadalajara, Jalisco.

ÍNDICE

06
I. IDENTIFICACIÓN DEL CURSO

07
II. UBICACIÓN DE LA ASIGNATURA

09
III. DESCRIPTORES DE LA ASIGNATURA

11
IV. DESARROLLO DE LA ASIGNATURA

15
V. RECURSOS BIBLIOGRÁFICOS Y
OTRAS FUENTES DE CONSULTA

PRESENTACIÓN

El rediseño curricular del modelo educativo del tecnólogo, articula los tres componentes del Marco Curricular Común de la Educación Media Superior: i) el fundamental; ii) el ampliado; y iii) el profesional, ahora laboral, conservando este último, el enfoque basado en competencias, bajo una nueva propuesta que impulsa al CETI a mantener una estrecha vinculación con el sector productivo. El planteamiento del proceso educativo surge a partir del campo profesional, lo que permite diseñar la situación didáctica desde una problemática que pone en juego e integra las competencias del estudiantado para la transformación laboral y el aprendizaje significativo dejando a un lado, la idea del empleo.

En este sentido, la presente asignatura plantea desde su propia construcción, un proyecto integrador que va orientando el perfil de egreso y que hace explícito los conocimientos, destrezas, habilidades, actitudes y valores que las y los estudiantes aplican en los procedimientos técnicos específicos.

La asignatura de Ciberseguridad tiene la visión de consolidar los conocimientos técnicos y prácticos sobre la explotación de las vulnerabilidades en entornos organizacionales reales implementando medidas de seguridad en la infraestructura y en el software para garantizar la integridad, confidencialidad, disponibilidad, autenticación, no repudiación y responsabilidad de la información.

La seguridad informática o ciberseguridad proporciona un conjunto de medidas de protección frente a amenazas como virus, hackers y robo de identidad. Su objetivo es asegurar la infraestructura, el software e información digital contra daños, robo o posible acceso no autorizado.

A través del hacking ético, las y los estudiantes pondrán en práctica sus habilidades teórico- prácticas para simular ataques cibernéticos (pruebas de penetración) a fin de descubrir y evaluar vulnerabilidades en sistemas, redes y aplicaciones, con el objetivo de fortalecer la seguridad informática mejorando la defensa digital de una organización.

Finalmente, el análisis de vulnerabilidades (ensayo de ciberataques) permitirá a las y los estudiantes con base en las buenas prácticas y siguiendo un código de ética, proponer la implementación de medidas de seguridad para garantizar la integridad, confidencialidad, disponibilidad, autenticación, no repudiación y responsabilidad de la información digital manejada por un software y la protección de la infraestructura tomando las buenas prácticas de organismos reconocidos internacionalmente para la seguridad informática.

I. IDENTIFICACIÓN DEL CURSO

CARRERA: TECNÓLOGO EN DESARROLLO DE SOFTWARE

Modalidad:	Asignatura:	Clave:
Presencial	Ciberseguridad	-

Semestre:	Academia:	Línea de Formación:
Octavo	Infraestructura de Tecnologías de la información	Infraestructura de Tecnologías de Información y Servicios

Créditos:	Horas Semestre:	Horas Semanales:
10.80	108	6

Horas Teoría:	Horas Práctica:
3	3

Fecha de elaboración:	Fecha de última actualización:
Diciembre 2025	---

II. UBICACIÓN DE LA ASIGNATURA

ÁMBITOS DE TRANSVERSALIDAD

Relación con asignaturas respecto a Marco Curricular Común de Educación Media Superior (MCCEMS), es decir, currículum fundamental y con asignaturas del currículum laboral.

Asignatura previa / Séptimo semestre

CURRÍCULUM LABORAL

Los conocimientos adquiridos en Cómputo Nube permiten a las y los estudiantes desarrollar habilidades para implementar los servicios de red necesarios brindando solución a necesidades particulares de infraestructura para una PYME en la nube.

Cómputo nube

III. DESCRIPTORES DE LA ASIGNATURA

1. META DE APRENDIZAJE DE LA ASIGNATURA

Evalúa la seguridad del software y hardware mediante la implementación de medidas de protección en sistemas e infraestructura de TI, con el fin de prevenir los principales ataques informáticos en un entorno organizacional.

2. COMPETENCIAS LABORALES DE LA ASIGNATURA

- Comprende la importancia de la seguridad informática para garantizar la confidencialidad, integridad, disponibilidad, autenticación, no repudiación y responsabilidad de los activos digitales ante amenazas como vulnerabilidades, filtraciones o ataques informáticos actuando con ética.
- Identifica el propósito y alcance del hacking ético mediante pruebas de penetración autorizadas para evaluar la robustez de los sistemas de información en el ámbito industrial, actuando con integridad y estricto apego al marco legal y ético establecido.
- Implementa medidas de seguridad digital para salvaguardar los atributos fundamentales de la información aplicando soluciones de software y hardware en el sector industrial con rigurosidad, responsabilidad y compromiso con la mejora continua.

3. PRODUCTO INTEGRADOR

Reporte del procedimiento del análisis de vulnerabilidades y el desarrollo de la documentación de las medidas de seguridad que se pueden implementar en un software y/o infraestructura de TI basadas en normativas internacionales.

3.1 Descripción del Producto Integrador

Reporte que contenga:

- Portada.
- Descripción del problema a resolver: Situación inicial y principales desafíos y problemas identificados.

- Solución Propuesta: Descripción de la infraestructura existente para identificar necesidades específicas.
- Proceso de implementación de la solución.
- Resultados obtenidos.
- Conclusiones.

3.2 Formado de Entrega

Reporte en formato digital o físico.

IV. DESARROLLO DE LA ASIGNATURA

UNIDAD 1. EVOLUCIÓN DE LA SEGURIDAD INFORMÁTICA.

Procesos	Contenidos	Recursos	Productos	Evaluación e instrumentos de evaluación
Comprende el marco de las evoluciones de los ataques cibernéticos para identificar su impacto y trascendencia.	Historia de la evolución de los ataques cibernéticos.	Equipo de cómputo. Material audiovisual: presentaciones, videos. Uso de pintarrón. Plataforma virtual de apoyo al aprendizaje.	Reporte de investigación de la historia de la evolución de los ataques cibernéticos.	Lista de cotejo u otro instrumento de evaluación acorde al producto.
Clasifica vectores de ataque modernos, tipos de atacantes, tipos de malware y metodologías de búsqueda de vulnerabilidades en el software e infraestructura de TI con el fin de comprender sus amenazas y alcances.	Tipos de atacantes: hacker sombrero negro, hacker sombrero blanco, hacker sombrero gris, script kiddle, hacktivistas. Tipos de ataques: malware, phishing, ingeniería social, MITM, Malware, DoS, DDoS, ISQL, NoSQLI, SSRF, XSS, CSRF, SSTI, entre otros. Documentación y búsqueda de vulnerabilidades de ciberseguridad (CVE).	Equipo de cómputo. Material audiovisual: presentaciones, videos. Uso de pintarrón. Plataforma virtual de apoyo al aprendizaje.	Reporte de investigación sobre los tipos de atacantes y sus diferencias. Cuadro sinóptico de la clasificación del malware. Reporte de investigación de los diversos tipos de ataques. Reporte de investigación y documentación de búsqueda de los CVE en la página: https://www.cve.org/	Lista de cotejo u otro instrumento de evaluación acorde al producto. Lista de cotejo u otro instrumento de evaluación acorde al producto. Lista de cotejo u otro instrumento de evaluación acorde al producto. Lista de cotejo u otro instrumento de evaluación acorde al producto.
Estructura la seguridad de punto final y el desarrollo de políticas basadas en el ciclo de vida del sistema y la recuperación de desastres para reforzar las medidas de seguridad y aplicar defensas correctivas.	Conceptos de seguridad de acceso y control de malware en dispositivos finales. Desarrollo de políticas de seguridad: normas, lineamientos y procedimientos. Planeación de continuidad operativa y recuperación de desastres.	Equipo de cómputo. Material audiovisual: presentaciones, videos. Uso de pintarrón. Plataforma virtual de apoyo al aprendizaje.	Reporte de caso de estudio para el establecimiento de políticas de seguridad, normas y procedimientos de recuperación de desastres.	Lista de cotejo u otro instrumento de evaluación acorde al producto.

PP1. Portafolio de evidencias digital de la identificación de las medidas de ciberseguridad en distintos tipos de activos organizacionales.

UNIDAD 2. INTRODUCCIÓN AL HACKING ÉTICO.

Procesos	Contenidos	Recursos	Productos	Evaluación e instrumentos de evaluación
Identifica las metodologías de intrusiones con el fin de evaluar la seguridad identificando vulnerabilidades en distintos entornos.	PTES (Penetration Testing Execution Standard). OSSTMM (Open Source Security Testing Methodology Manual). NIST SP 800-115. Metodología común: 1.Reconocimiento (Reconnaissance/Foot printing) 2.Escaneo y Análisis de Vulnerabilidades 3.Obtención de Acceso (Gaining Access / Explotación) 4.Mantenimiento del Acceso (Maintaining Access / Post-Explotación) 5.Ocultamiento de Rastros y Generación de Informes (Covering Tracks / Reporting). Guía de buenas prácticas: OWASP (Open Web Application Security Project).	Equipo de cómputo. Material audiovisual: presentaciones, videos. Uso de pintarrón. Plataforma virtual de apoyo al aprendizaje.	Reporte de investigación de las metodologías de intrusiones. Cuadro comparativo de las principales diferencias entre las metodologías de intrusiones.	Lista de cotejo u otro instrumento de evaluación acorde al producto. Lista de cotejo u otro instrumento de evaluación acorde al producto.
Implementa las técnicas de intrusiones para obtener acceso no autorizado a sistemas, redes o datos.	Escaneo de red. Escaneo de puertos. Recopilación de información en base a los resultados. Identificación de posibles vulnerabilidades. Explotación de las posibles vulnerabilidades. Garantizar el acceso al equipo comprometido.	Equipo de cómputo. Material audiovisual: presentaciones, videos. Uso de pintarrón. Plataforma virtual de apoyo al aprendizaje.	Reporte de práctica de la implementación de la metodología de un ataque.	Guía de observación y/o lista de cotejo.

PP2. Portafolio de evidencias digital de la aplicación y demostración de uso de las herramientas de un proceso de pentesting.

UNIDAD 3. IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD AL SOFTWARE DE INFRAESTRUCTURA DE TI.

Procesos	Contenidos	Recursos	Productos	Evaluación e instrumentos de evaluación
Implementa las medidas de seguridad a nivel de software para proteger la integridad, confidencialidad, disponibilidad, autenticación, no repudiación y responsabilidad de la información digital.	Análisis y propuestas de la implementación de las medidas de seguridad a nivel de software en la actividad previa.	Equipo de cómputo. Material audiovisual: presentaciones, videos. Uso de pintarrón. Plataforma virtual de apoyo al aprendizaje.	Reporte de investigación del proceso de implementación de las medidas de seguridad para evitar y dar solución a las vulnerabilidades a nivel de software.	Lista de cotejo u otro instrumento de evaluación acorde al producto.
Implementa las medidas de seguridad a nivel de infraestructura de TI con el fin de asegurar un entorno estable, confiable y capaz de resistir ciberataques.	Análisis y propuestas de la implementación de las medidas de seguridad a nivel de infraestructura de TI en la actividad previa.	Equipo de cómputo. Material audiovisual: presentaciones, videos. Uso de pintarrón. Plataforma virtual de apoyo al aprendizaje.	Reporte de investigación del proceso de implementación de las medidas de seguridad para evitar y dar solución a las vulnerabilidades a nivel de infraestructura de TI.	Lista de cotejo u otro instrumento de evaluación acorde al producto.

PP3. Portafolio de evidencias digital de la implementación de las medidas de seguridad al software e infraestructura de TI.

PF. Reporte del procedimiento del análisis de vulnerabilidades y el desarrollo de la documentación de las medidas de seguridad que se pueden implementar en un software y/o infraestructura de TI basadas en normativas internacionales.

V. RECURSOS BIBLIOGRÁFICOS Y OTRAS FUENTES DE CONSULTA DE LA UAC

Recursos Básicos

- Cano, J. (2016). Inseguridad de la información - Una visión estratégica. México. Alfaomega, Ra-Ma.
- Gómez, A. (2011). Enciclopedia de la seguridad informática - 2ª Edición. México. Alfaomega Grupo Editor.
- Common Vulnerability Enumeration (CVE) 2025. cve.org. Recuperado el 21 de enero de 2026, Consultado: https://www.cve.org/
- Espino, L. (2016). Criptografía. Edición Kindle. Recuperado 30 de enero de 2026, Consultado:https://www.amazon.com.mx/Criptograf%C3%ADa-Luis-Espino-ebook/dp/B01M8MYR8R
- Walker, M. (2019). CEH Certified Ethical Hacker All-in-One Exam Guide, Fourth Edition. Formatos: McGraw-Hill Education ISBN-13 978-1260454550 Tapa/Pasta blanda; McGraw Hill ISBN-13 978-1260454567 Edition Kindle (English Edition). Recuperado 30 de enero de 2026, Consultado: https://www.amazon.com.mx/Certified-Ethical-Hacker-Guide-Fourth/dp/126045455X
- Maymi, F.; Harris, S. (2021). Cissp All-In-One Exam Guide, Ninth Edition. Formatos: Editorial McGraw-Hill Companies ISBN-13 978-1260467376 Tapa/Pasta dura; Editorial McGraw Hill ISBN-13 978-1260467369 Edición Kindle (English Edition); Editorial McGraw Hill-Ascent Audio ISBN-13 979-8212450928 & ISBN-13 979-8212450911. Recuperado 30 de enero de 2026, Consultado: https://www.amazon.com.mx/Cissp-All-One-Guide-Ninth/dp/1260467376/ref=asc_df_1260467376?mcid=2604f282e7c63d7099db008ee54a4600&tag=gledskshopmx-20&linkCode=df0&hvadid=709846689729&hvpos=&hvnetw=g&hvrand=18288257894198572994&hvpone=&hvptwo=&hvqmt=&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=9138765&hvtargid=pla-1247391367904&psc=1&language=es_MX&gad_source=1
- Hook, D.; Eaves, J. (2023). Java Criptography: Tools and Techniques. Formatos: ISBN: 9798372121782 Tapa/Pasta blanda & Edición Kindle. Recuperado 30 de enero de 2026, Consultado: https://www.amazon.com/Java-Cryptography-David-Geoffrey-Hook/dp/B0BRH1H7GP#

Recursos complementarios

- Pacheco, F. y Jara, H. (2013). Hackers al descubierto. Buenos Aires: Creative Andina Corp.
- González, L. y De Fuentes, J. (2010). Sistemas seguros de acceso y transmisión de datos. LC editorial.
- Fuster, A.; Muñoz, J.; Hernández, L.; Martín, A.; Montoya, F. (2016). Criptografía, protección de datos y aplicaciones
- Guía para estudiantes y profesionales. México. Alfaomega, Ra-Ma.
- Junior Cybersecurity Analyst 2026. netacad.com. Recuperado el 22 de enero de 2026, Consultado: https://www.netacad.com/career-paths/cybersecurity?courseLang=en-US
- Ethical hacker 2026. Netacad.com. Recuperado el 22 de enero de 2026, Consultado: https://www.netacad.com/courses/ethical-hacker?courseLang=en-US
- OWASP 2026. Owasp.org. Recuperado el 22 de enero de 2026, Consultado: https://owasp.org/www-project-top-ten/
- Congreso de la Unión. (2025). Ley general de transparencia y acceso a la información. DOF 20-03-2025. Recuperado el 22 de enero de 2026 en http://www.diputados.gob.mx/LeyesBiblio/pdf/LGTAIP.pdf
- Congreso de la Unión. (2025). Ley federal de derecho de autor. DOF 14-11-2025. Recuperado el 22 de enero 2026 en https://www.diputados.gob.mx/LeyesBiblio/pdf/LFDA.pdf

Fuentes de consulta utilizadas

- Cámara de Diputados del H. Congreso de Unión. (30 de septiembre de 2019). Ley General de Educación. https://www.diputados.gob.mx/LeyesBiblio/pdf/LGE.pdf

- Diario Oficial de la Federación. (20 de septiembre de 2023). Acuerdo secretarial 17/08/22 y 09/08/23. https://www.dof.gob.mx/nota_detalle.php?codigo=5699835&fecha=25/08/2023

- Gobierno de México. (7 de septiembre de 2023). Propuesta del Marco Curricular Común de la Educación Media Superior. https://educacionmediasuperior.sep.gob.mx/propuestaMCCEMS

AGRADECIMIENTOS

El Centro de Enseñanza Técnica Industrial agradece al cuerpo docente por su participación en el diseño curricular:

Miriam Nayeli Anastasio Saiz.

Jorge Alberto Chamorro Martínez.

Francisco Javier González Cibrián.

Ramses Delgado Díaz.

Juan Carlos Hernández Velázquez.

Luz Araceli García Beltrán.

Rodolfo Ulyses Vázquez Cárdenas.

Sergio Antonio Ellerbracke Román

Clara Gabriela García Durán.

Andrés Figueroa Flores.

Angelberto Rosales Mayorga.

Edgar Matías Aldana.

Equipo Técnico Pedagógico

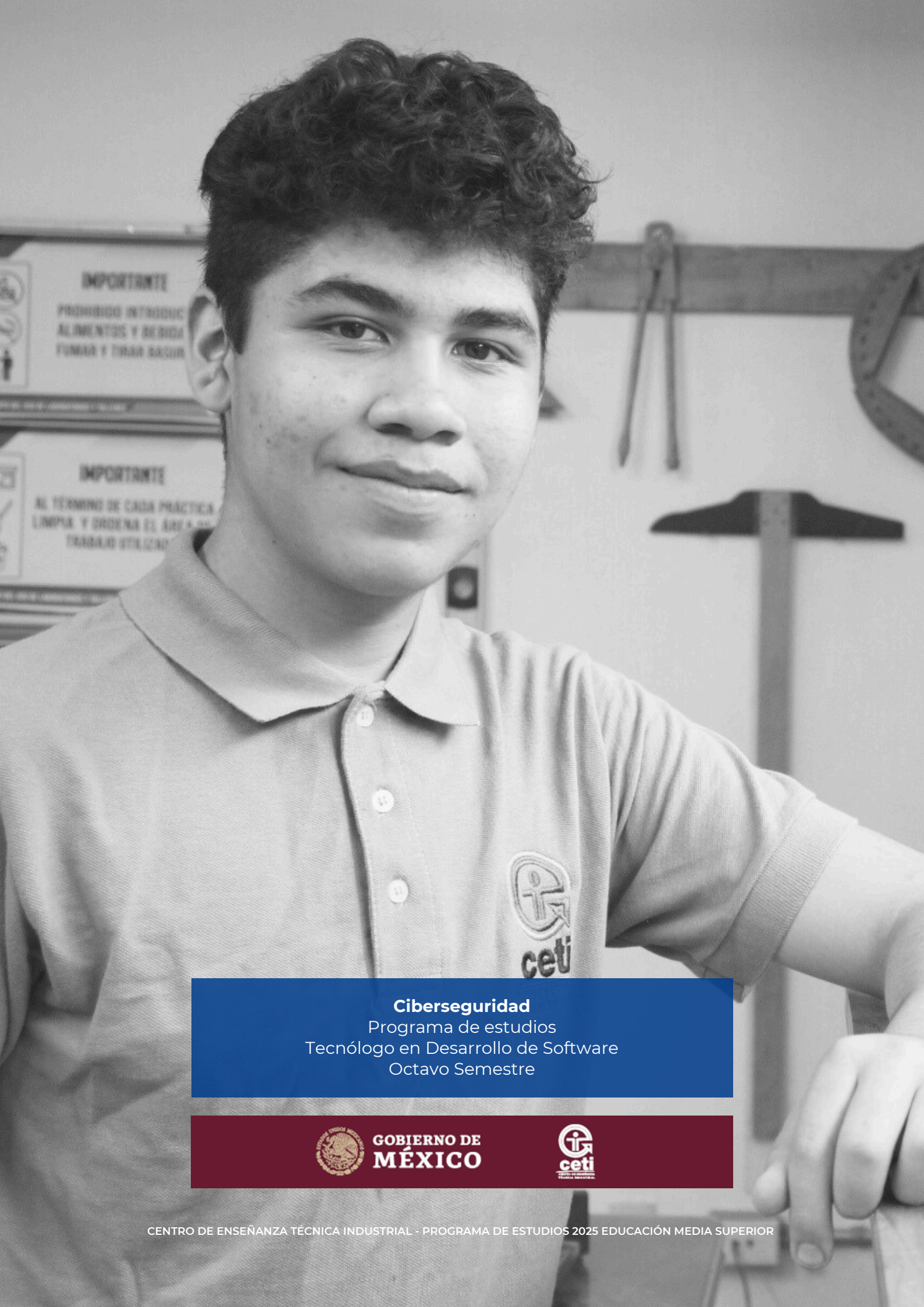
Cynthia Isabel Zatarain Bastidas.

Ciara Hurtado Arellano.

Rodolfo Alberto Sánchez Ramos.

Janeth Poleth Álvarez Duarte

Raquel Abigail Díaz Díaz



Ciberseguridad

Programa de estudios
Tecnólogo en Desarrollo de Software
Octavo Semestre

GOBIERNO DE MÉXICO

ceti