DIRECCIÓN TÉCNICA GESTIÓN ACADÉMICA

DEPARTAMENTO DE DESARROLLO Y DISEÑO CURRICULAR

		PROGRAMA			
		Código en SIPE	Descripción en SIPE		
TIPO DE CURSO		028	Tecnólogo		
PLAN		2023			
ORIENTACIÓN		88F	Ciberseguridad		
MODALIDAD		Presencial			
AÑO		1			
SEMESTRE/ MÓDULO		2			
UNIDAD CURRICULAR		Inglés Técnico			
CRÉDITO EDUCATIVO		6			
DURACIÓN DEL CURSO		Horas totales: 64	Horas semanales: 4		Cantidad de semanas: 16
Fecha de Presentación: 6/3/2023	Nº Resolución de la DGETP	Exp. Nº	Res. Nº	Acta Nº	Fecha __/__/____

Propósitos de la unidad curricular:

La ciberseguridad se ha convertido en una área que ha cobrado relevancia dentro de las TI en la actualidad ya que es de vital importancia minimizar el nivel de riesgo al que está expuesta la información, ante amenazas o incidentes cibernéticos. El objetivo de la seguridad informática es mantener la integridad, disponibilidad, privacidad, control y autenticidad de la información manejada por computadora.

En este contexto, la evolución constante del mundo moderno y el desarrollo vertiginoso de las telecomunicaciones a nivel mundial y la globalización, conlleva a que el idioma inglés esté presente en el campo académico y profesional. Esta presencia a nivel global demanda la utilización de este idioma como vehículo de comunicación universal en el siglo XXI. En consecuencia, el conocimiento de la lengua inglesa se impone como un requisito indispensable para estudiantes, docentes, investigadores y profesionales que necesitan información completa, actualizada y veraz que les permita el descubrimiento de nuevos saberes, reflexionar acerca de los problemas de seguridad y cómo la lengua meta puede contribuir a minimizar su impacto.

A través de la unidad curricular Inglés Técnico, se pretende proporcionar al estudiante las competencias básicas para insertarse en el mundo de hoy, para que éstos comprendan las distintas situaciones, resuelvan problemas y tomen decisiones. El dominio de la lengua inglesa integra una de esas competencias puesto que es el código predominante en los ámbitos laborales y/o académicos, que no sólo le permite al educando su desarrollo cognitivo, sino el mejor conocimiento de su lengua materna.

En el transcurso de la unidad curricular, se trabajarán las competencias y estrategias para comprender textos académicos e interactuar en inglés, aspectos fundamentales para un desempeño eficaz en el mundo de las TIC. El inglés es el idioma más comúnmente empleado en la publicación de trabajos, en congresos, seminarios internacionales y en el mundo de la tecnología y la computación. Por ende, esta unidad curricular cobra importancia dentro de la currícula porque permite al futuro egresado acceder a fuentes de información de su interés de primera mano, conociendo y evaluando bibliografía publicada en lengua inglesa. A su vez, amplía su horizonte de conocimientos al investigar, comprender manuales, seguir instrucciones, leer páginas web e interactuar en inglés.

En síntesis, Inglés Técnico le permitirá al estudiante fortalecer las macrohabilidades de la lengua con el fin de favorecer una comunicación de forma efectiva en contextos diversos y complejos. Las actividades que el docente desarrolle debe atender a los procesos cognitivos específicos del estudiante en relación a la lengua meta (L2): hablar, escuchar, leer, escribir y la reflexión metalingüística.

Resultados de aprendizaje:

- Resuelve problemas mediante proyectos integrados de indagación personales y colaborativos mediados por la tecnología.
- Desarrolla habilidades, identifica conflictos y visualiza soluciones.
- Comprende e integra el lenguaje técnico-tecnológico en la lengua extranjera.
- Busca soluciones a problemas de distinta índole utilizando las herramientas digitales a su alcance.
- Conoce la administración de equipos de hardware, su mantenimiento y aseguramiento físico.
- Comprende la importancia de la ciberseguridad y reflexiona acerca de ella.
- Reconoce diferentes arquitecturas de red y sus efectos en la ciberseguridad.
- Reconoce e identifica las tecnologías de virtualización y servicios en la nube.
- Comprende las capacidades de la computación en la nube.
- Describe las posibles amenazas en la red y la forma de contrarrestar las mismas.
- Establece comparaciones entre los diferentes tipos de ciberataques.
- Explica los distintos servicios en línea.
- Identifica las distintas formas en las cuáles un sistema puede verse en riesgo de ciberataque.
- Reconoce las tendencias actuales en técnicas de ciberataque
- Identifica los conceptos básicos de los principales procesos y respuestas ante incidentes.
- Identifica y establece comparaciones entre las diferentes técnicas criptográficas.
- Reconoce las normas que los estados están creando para la protección de la información y los datos.

Saberes estructurantes de la unidad curricular:

Thematic Unit 1: What is cybersecurity?
Se detallan a continuación los temas a abordar dentro de la unidad temática. A partir de la unidad el docente podrá a su vez trabajar con temas de interés que surjan por parte de los estudiantes. Los temas son los siguientes: ● Cybersecurity definition and use ● The Internet of things ● Impact of cybersecurity ● The CIA triad
Contenidos: ● Definición de ciberseguridad ● Acrónimos ● Internet de las cosas ● Confidencialidad, Integridad y Accesibilidad (CIA)

Thematic Unit 2: The ABCs of cryptography
Se detallan a continuación los temas a abordar dentro de la unidad temática. A partir de la unidad el docente podrá a su vez trabajar con temas de interés que surjan por parte de los estudiantes. Los temas son los siguientes: ● Cryptology, cryptography and cryptanalysis ● Why is encryption important? ● Basic crypto systems ● Advanced cryptography
Contenidos: ● Diferencia entre criptología, criptografía y criptoanálisis ● Sistemas de encriptación ● Encriptación y desencriptación ● Avances en el área de la criptografía

Thematic Unit 3: Software security
Se detallan a continuación los temas a abordar dentro de la unidad temática. A partir de la unidad el docente podrá a su vez trabajar con temas de interés que surjan por parte de los estudiantes. Los temas son los siguientes: ● Common security problems ● Databases security ● SQL injection, types of SQLi and prevention ● Hardening
Contenidos: ● Problemas en el área de la seguridad ● Bases de datos y seguridad de los mismos ● Inyección SQL, tipos de infiltración de código intruso y su prevención ● Proceso de reducción de vulnerabilidades.

Estrategias metodológicas:

Los contenidos se deben trabajar en base a temas. El marco ideal para el desarrollo de los temas son las unidades temáticas, partiendo de un tema general relacionado con la orientación del curso. El docente jerarquizará aquellos temas de cada unidad para trabajar en forma particular de acuerdo a las características del grupo y a los acuerdos logrados con los docentes del curso. El docente diseñará y secuenciará las actividades que considere adecuadas para el logro de los objetivos del curso, teniendo en cuenta que el estudiante adquiera las competencias lingüísticas y comunicativas necesarias.

El docente al enseñar deberá ser ecléctico lo que implica escoger las estrategias de enseñanza que mejor se ajusten a las necesidades e intereses de los estudiantes.

Evaluación

La evaluación se realizará de acuerdo al reglamento vigente. No obstante, conviene destacar que la evaluación, concebida como parte del proceso de enseñanza y de aprendizaje, debe ser continua y fundamentalmente formativa. Se sugiere la incorporación de diferentes técnicas, instrumentos y herramientas para la recolección de información sobre los aprendizajes de los

estudiantes y sus singularidades, y que permitan tomar decisiones fundamentadas al docente. Asimismo, se sugiere desarrollar las instancias de evaluación en distintos formatos.

Bibliografía de referencia para el docente

Angel M.Y. Lin (2016). *Language Across the Curriculum & CLIL in English as an Additional Language (EAL) Contexts*. Springer Science+Business Media

Anthony, L. (2018). *Introducing English for Specific Purposes*. Routledge.

Clark, K. (2022) *Cybersecurity for Beginners*

Cornish, P (2022) *The Oxford Handbook of Cyber Security*

Dauti, D. (2022). *Windows Server 2022 Administration Fundamentals.* Packt. 3rd Edition.

Du, W. (2022). *Computer Security: A Hands-on Approach (Computer & Internet Security).* Syracuse University. 3rd Edition.

Gregory, G. & Chapman, C. M. (2013). *Differentiated Instruction Strategies: One size does not fit all.* Corwin Press.

Harding, K. (2007). *English for Specific Purposes*. Oxford University Press.

Hein, T., Nemeth, E., Snyder, G., Whaley, B., & Mackin, D. (2017). *UNIX and Linux System Administration Handbook.* Addison-Wesley Professional. 5th Edition.

Julian, M. (2017). *Practical Monitoring: Effective Strategies for the Real World*. O'Reilly. 1st Edition.

Kim, G., Debois, P., Willis, J., & Humble, J. (2021). *The DevOps Handbook: How to Create World-Class Agility, Reliability, & Security in Technology Organizations.* IT Revolution Press. 2nd Edition.

Lightbown, P., & Spada, N. M. (2017). *How languages are learned*. Oxford University Press.

Paar, C., Pelzl, J., Preneel, B. (2014). *Understanding Cryptography: A Textbook for Students and Practitioners.* Springer. 10th Edition.