UTEC
Universidad Tecnológica

UNIVERSIDAD TECNOLÓGICA
CONSEJO DIRECTIVO CENTRAL PROVISORIO

RESOLUCIÓN Nº	
41	**/25**

Referencia: Plan de Estudios 2025 del BOOTCAMP EN CIBERSEGURIDAD

Montevideo, 04 de febrero de 2025.

VISTO: La propuesta elevada por la Dirección de Educación para la aprobación de un Bootcamp en Ciberseguridad.

RESULTANDO:

I. que el campo de la ciberseguridad se está volviendo cada vez más crítico a medida que la tecnología sigue avanzando y las ciberamenazas aumentan, volviendo necesario contar con los conocimientos y habilidades avanzados actualizados para proteger a las organizaciones y las personas de los ataques cibernéticos;

II. que el nuevo Bootcamp en Ciberseguridad contribuye a fortalecer el ecosistema tecnológico del país al formar profesionales competentes en un área crítica;

III. que la propuesta consiste en una formación 100% virtual, con una carga de 360 horas, para un cupo de 25 personas;

IV. que para cubrir los recursos del Bootcamp, se contará con la financiación del 100% de la Institución ANDA (fondos externos);

V. que el Área de diseño y Desarrollo Curricular y la Asesoría Jurídica de la Dirección de Educación informan favorablemente sobre la propuesta y se confirma que reglamentariamente los perfiles de ingreso, duración y créditos se adecuan a la Ordenanza de Educación Continua vigente.

CONSIDERANDO: La Educación Continua vigente, aprobada por Resolución N° 422/23 del 8 de agosto de 2023.

ATENTO: a lo precedentemente expuesto y a la atribución conferida por el artículo 16, literal F) de la Ley 19.043.

EL CONSEJO DIRECTIVO CENTRAL PROVISORIO DE LA UNIVERSIDAD TECNOLÓGICA RESUELVE:

1º. Aprobar el nuevo Bootcamp en Ciberseguridad, a impartirse en el segundo semestre de 2025, entre los meses de julio y noviembre, el que se adjunta a la presente Resolución y la integra.

2º. Aprobar la expedición de certificados en Bootcamp en Ciberseguridad a quienes cumplan con todos los requisitos establecidos en la propuesta adjunta; o en su defecto, una constancia de participación.

3°. Comuníquese y publíquese a todos los efectos.

DocuSigned by:
3616680A4368455...
Andrés D. Gil
Consejero
Universidad Tecnológica

DocuSigned by:
B12B3FE1158A46B...
Graciela Do Mato
Consejera
Universidad Tecnológica

Signed by:
5D779240B0CB4EE...
Rodolfo Silveira
Consejero
Universidad Tecnológica

Universidad Tecnológica - UTEC

Uruguay

***Bootcamps* en Habilidades Digitales**

Centro de Transformación Digital

***Bootcamp* en Ciberseguridad**

2025

Introducción de la propuesta formativa

En un contexto global donde las amenazas cibernéticas se incrementan exponencialmente, la ciberseguridad se ha convertido en una habilidad estratégica imprescindible para organizaciones de todos los sectores. En Uruguay, las empresas enfrentan un déficit significativo de personal capacitado para prevenir, detectar y mitigar riesgos en sus sistemas digitales.

Esta necesidad ha sido expresada directamente por ANDA, quien identifica la dificultad de contratar personal especializado en ciberseguridad como un desafío crítico para su operación. ANDA, que en 2024 financió exitosamente un *bootcamp* de perfil *full stack* con resultados satisfactorios, solicita ahora una formación focalizada en ciberseguridad para satisfacer esta carencia. El respaldo financiero de ANDA y su interés en replicar el modelo, orientado a cubrir esta demanda, refuerzan la pertinencia de este programa.

El modelo de *bootcamp*, caracterizado por su enfoque intensivo, 100% virtual, práctico y orientado a la empleabilidad, ha demostrado ser efectivo para formar rápidamente talento en áreas específicas. El programa diseñado tiene una duración de 16 semanas, modalidad *part-time*, lo que permite la participación de trabajadores en actividad y estudiantes que buscan especializarse sin necesariamente tener un título de grado para poder cursarlo. La planificación académica está estructurada en seis módulos integrales que combinan teoría, práctica, herramientas tecnológicas avanzadas y un proyecto final, asegurando una formación completa y orientada al mercado laboral.

UTEC tiene la experiencia previa en la planificación y ejecución de este tipo de programas en colaboración con academias especializadas, lo que garantiza la calidad y la alineación con las expectativas del financiador. Además, la metodología del *bootcamp* incluye evaluación continua y mentorías, promoviendo una alta tasa de aprobación y una rápida inserción laboral.

El programa aborda una problemática concreta del mercado laboral uruguayo: la insuficiencia de personal capacitado en ciberseguridad. Según las proyecciones internacionales y locales, este déficit continuará creciendo en los próximos años, afectando la capacidad de las empresas para proteger sus sistemas y datos.

Este *bootcamp* no solo responde a una necesidad inmediata de ANDA, sino que también contribuye a fortalecer el ecosistema tecnológico del país al formar profesionales competentes en un área crítica. Además, como formación de capacitación continua, el

programa complementa la oferta educativa tradicional, abriendo oportunidades de desarrollo profesional a personas que deseen actualizarse o reorientar su carrera hacia un área de alta demanda, siguiendo la línea de la oferta de *bootcamps* que se viene realizando desde el 2021.

Estructura programática de la propuesta formativa

ACTIVIDAD DE UTEC-CTD			
Bootcamp en Ciberseguridad			
PROGRAMA	*Bootcamps* en Habilidades Digitales		
SEMESTRE	Ejecución segundo semestre de 2025 (julio - noviembre)		
AÑO	2025		
LUGAR	Virtual 100%		
FECHA	5/5/2025 proceso de admisión 30/07/2025 ejecución	HORARIO/S: Lun, mie y vie de 18:30 a 21.30 hs, clases sincrónicas durante 16 semanas (4 meses)	6 meses (2 meses admisión, 6 meses ejecución)
CARGA HORARIA	360 horas		
MODALIDAD	Virtual		
DEDICACIÓN (en horas)	CLASES	TRABAJO AUTÓNOMO	TRABAJO FINAL
	144	216	120 (48 de estas sincrónicas, las 120 están incluidas en las horas sincrónicas y autónomas presentadas en esta estructura)
CRÉDITOS	A definir por UTEC		
CUPOS OFRECIDOS	ESTUDIANTES UTEC	DOCENTES UTEC	CUPO EXTERNO
25			25
Es obligatorio pasar el proceso de admisión, la persona debe contar con la disponibilidad horaria.			
CRITERIO DE CUPOS	El proceso de admisión estará a cargo de UTEC, ANDA y las instituciones vinculadas a la propuesta. Se priorizará a las personas residentes en		

	departamentos del interior del país. Las etapas incluyen: una prueba, posterior acceso al prework (resolución de problemas), evaluación de disponibilidad y compromiso para realizar el bootcamp y entrevista. Por último se realiza la selección final que estará validada por UTEC y por ANDA
PÚBLICO OBJETIVO	Personas mayores de 18 años, que tengan interés en ciberseguridad y disponibilidad horaria. Con prioridad mujeres y personas que vivan en el interior.

JUSTIFICACIÓN Y PERTINENCIA

En un contexto donde las amenazas cibernéticas son cada vez más frecuentes, la ciberseguridad se posiciona como un pilar fundamental para la protección de datos, sistemas y redes. En Uruguay, como en el resto del mundo, existe una creciente demanda de profesionales capacitados para prevenir, detectar y mitigar riesgos cibernéticos. Según proyecciones, las empresas enfrentarán un déficit significativo de personal especializado en ciberseguridad para 2025.

Este programa es una respuesta a esta necesidad, brindando a los participantes las competencias necesarias para ingresar al mercado laboral o potenciar sus conocimientos actuales.

OBJETIVO GENERAL

Formar a personas para enfrentar los desafíos actuales de la ciberseguridad, brindándoles los conocimientos teóricos y prácticos necesarios para identificar, prevenir y mitigar riesgos cibernéticos en sistemas, redes y aplicaciones. Esto incluye el manejo de herramientas avanzadas, la implementación de normativas internacionales y el desarrollo de habilidades críticas y estratégicas para responder eficazmente a incidentes de seguridad, cumpliendo con estándares de la industria y fortaleciendo competencias clave para el desempeño en entornos laborales dinámicos.

OBJETIVOS DE APRENDIZAJE (“LEARNING GOALS”)

- Incorporar conocimientos fundamentales en ciberseguridad que permitan a los participantes comprender y aplicar medidas de protección en sistemas, redes y aplicaciones.
- Desarrollar habilidades prácticas mediante la implementación y gestión de herramientas avanzadas como NMAP, Wireshark y Metasploit, y la simulación de escenarios reales.
- Adquirir conocimientos sobre normativas internacionales y nacionales de ciberseguridad, tales como ISO 27001, NIST para asegurar el cumplimiento de estándares de la industria.
- Desarrollar el pensamiento crítico y estratégico para identificar, mitigar y responder efectivamente a incidentes de ciberseguridad.
- Fortalecer competencias en ciberinteligencia utilizando técnicas OSINT para la recolección y análisis de datos relevantes.
- Desarrollar habilidades blandas clave, como el trabajo en equipo, la comunicación efectiva y la autorregulación del aprendizaje, esenciales para el desempeño en entornos laborales dinámicos.

METODOLOGÍA

El *bootcamp* utiliza una combinación de:

- Clases sincrónicas en línea con aprendizaje colaborativo.
- Prácticas y proyectos basados en escenarios reales.
- Mentorías personalizadas para acompañar el aprendizaje.

Se promueve el uso de herramientas digitales de ciberseguridad como NMAP, Wireshark y OSINT, con acceso a entornos simulados para experimentación.

CONTENIDOS

Módulo I: Fundamentos básicos, Conceptos clave, redes y sistemas operativos.

Módulo II: Redes y servidores, Seguridad en redes y administración cloud.

Módulo III: Pentesting y análisis, Técnicas de ataque y defensa (Red/Blue Team).

Módulo IV: OSINT y ciberinteligencia, Herramientas para recolección de datos.

Módulo V: Normativa y riesgos. Gestión de riesgos y cumplimiento normativo.

Módulo VI: Proyecto Final: Auditoría y estrategias de Ciberseguridad.

EVALUACIÓN

Se evaluará el programa mediante un proyecto final cuya escala será Aprobado/No aprobado.

En el proyecto se evalúan habilidades técnicas sobre el contenido brindado en el *bootcamp* y blandas como el trabajo en equipo, la comunicación, la resolución de problemas, etc.

REQUISITOS PARA LA CERTIFICACIÓN

Para obtener el certificado, los participantes deben:

- Asistir al 85% de las clases.
- Completar el 80% de los proyectos y ejercicios requeridos.
- Aprobar el proyecto final, integrando los conocimientos adquiridos.

Quienes no aprueben el programa mediante el método de aprobación definido, recibirán una constancia de participación.

CONSTANCIA/CERTIFICACIÓN OTORGADA

Constancia de participación en *Bootcamp* en Ciberseguridad.

Certificado en *Bootcamp* en Ciberseguridad.

BIBLIOGRAFÍA o MATERIAL COMPLEMENTARIO

Andress, J., & Winterfeld, S. (2017). *Cybersecurity for Beginners*. CreateSpace Independent Publishing Platform.

CIS (Center for Internet Security). (2023). *CIS Controls for Effective Cyber Defense*. Center for Internet Security.

DOCENTES RESPONSABLES Y PERFIL ACADÉMICO PROFESIONAL

Anahí Lacava - Docente encargada de Habilidades Digitales. Líder de los proyectos de *bootcamps* ejecutados desde UTEC con *partners* desde el 2021 hasta la fecha. Contadora con posgrados varios en tecnologías. Trabaja hace más de 6 años en proyectos de tecnología.

Mail: anahi.lacava@utec.edu.uy

DOCENTE **REFERENTE**	Matías Camargo - Licenciado en Informática, con posgrado en seguridad de sistemas y redes, así como en robótica e inteligencia artificial. Docente y Coordinador del Posgrado en ciberseguridad de UTEC, trabaja hace más de 6 años en ciberseguridad. Mail: jorge.camargo@utec.edu.uy
DOCENTE/S DE LA ACTIVIDAD	A contratar
OTRAS INSTITUCIONES/ ORGANIZACIONES CONTRAPARTES	
ANDA Contrataciones pendientes	