



Universidad Nacional de Asunción

CONSEJO SUPERIOR UNIVERSITARIO

www.una.py

C. Elect.: sgeneral@rec.una.py

Telefax: 595 - 21 - 585540/3, 585546

CP: 2160, San Lorenzo - Paraguay

Campus de la UNA, San Lorenzo - Paraguay

Acta N° 13 (A.S. N° 13/16/06/2021)

Resolución N° 0353-00-2021

UNIVERSIDAD NACIONAL DE ASUNCIÓN Dirección General de Extensión Universitaria Proyecto de extensión universitaria

1. Datos Generales del programa

- 1.1. Facultad Politécnica.
- 1.2. HackCamp.
- 1.3. Dirección de Tecnología de la Información y Comunicación
Dirección Académica - Movilidad Académica y Pasantía
- 1.4. Bootcamp.

2. Antecedentes y Justificación:

En los últimos años ha habido una evolución tecnológica sin precedentes, muchos de los procesos clásicos o tradicionales que se venían realizando de manera manual, en la actualidad son realizados de forma automatizada utilizando infraestructura tecnológica y sistemas informático, por lo que la sociedad actual se ha hecho dependiente de estos sistemas y esta tecnología para la gestión de sus infraestructuras críticas, esto incluye a centrales de energía, hospitales, laboratorios, bancos, financieras, etc.

Esta rápida evolución, y el hecho de que esta tecnología y estos sistemas sean altamente vulnerables a ataques maliciosos, deja en evidencia el gran riesgo al que nos enfrentamos al no contar con mecanismos que nos permitan defendernos y dar respuesta a este tipo de incidentes, y Paraguay no se encuentra ajeno a esto, ya que la pandemia del COVID-19 ha forzado el incremento del uso de la tecnología y la automatización de procesos permitiendo la agilización de los mismos. En la actualidad se puede encontrar una gran cantidad de amenazas como ataques a la red, el secuestro de datos, ingeniería social, etc.

Este hecho ha ocasionado que la perspectiva de la seguridad cambie y cobre un papel especialmente importante haciendo que las organizaciones inviertan recursos para crear departamentos sólidos que garanticen la ciberseguridad.

Hoy en día, el perfil de ciberseguridad es uno de los más buscados por las empresas e instituciones, la infraestructura tecnológica y los sistemas de dichas organizaciones son parte clave para su desarrollo y funcionamiento, por lo que conocer las amenazas,

vulnerabilidades y cómo realizar la mitigación oportuna de los riesgos actuales es fundamental.

Este proyecto pretende promover el desarrollo de habilidades en el campo de la ciberseguridad de manera a que las organizaciones se encuentren preparadas para enfrentar los riesgos actuales y concientizar sobre la importancia de la seguridad digital.

3. Objetivo General

- Incrementar el conocimiento de ciberseguridad a través de una jornada completa de Conferencias y una Competencia intensa, inmersiva y segura.

4. Objetivos específicos

- Dar a conocer la importancia de la ciberseguridad, sus diferentes ramas de actuación e impacto actual en las empresas públicas y privadas
- Presentar las principales técnicas defensivas y ofensivas que son empleadas en la actualidad por los profesionales del sector.
- Proveer un entorno seguro y controlado para que puedan ser aplicados los conocimientos adquiridos a través de una competencia simulada.

5. Implementación

Se pretende la realización de una capacitación intensiva de corta duración, denominado Bootcamp, enfocado a la adquisición de conocimientos en el área de ciberseguridad. En un Bootcamp el aprendizaje se realiza en un entorno donde se recrean situaciones reales, lo que permite al participante aplicar los conocimientos adquiridos en un espacio seguro y controlado.

Como ya se había mencionado anteriormente, este proyecto busca contribuir con el fortalecimiento de las habilidades necesarias para hacer frente a los requerimientos actuales de seguridad, para ello se pretende implementar el aprendizaje a través de la realización de un Bootcamp.

Un Bootcamp es una metodología de enseñanza que se caracteriza por brindar un aprendizaje intensivo e inmersivo, enfocándose en conocimientos específicos sobre un área, se trata de aprender haciendo (Learning by doing). El principal objetivo de un bootcamp es preparar a sus participantes para dar respuesta a las necesidades reales del mercado laboral.

Hackcamp estará compuesto por dos fases principales:

La primera, en la que se impartirán por medio de charlas y talleres todos los conocimientos propuestos para esta primera edición.

La segunda, la cual permitirá la aplicación de todos los conocimientos adquiridos, a

través de una competencia entre equipos. Dicha competencia consistirá básicamente en la aplicación de técnicas defensivas y ofensivas. Por lo que un equipo deberá cumplir el rol de Red team, esto quiere decir que buscará atacar al otro, tratando de encontrar sus vulnerabilidades y explotarlas. Sin embargo, el otro equipo, cumplirá el rol de Blue Team, es decir, tratará de defenderse buscando fortificar sus defensas para evitar que los ataques del otro equipo ocasionen una denegación de sus servicios o mitigar sus efectos. Ganará el equipo que haya logrado obtener el mayor puntaje.

6. Resultados esperados

Incrementar el nivel de conocimiento de los participantes en el área de la ciberseguridad a través de la práctica de técnicas defensivas (Blue team) y ofensivas (Red team) en un entorno controlado.

7. Metas

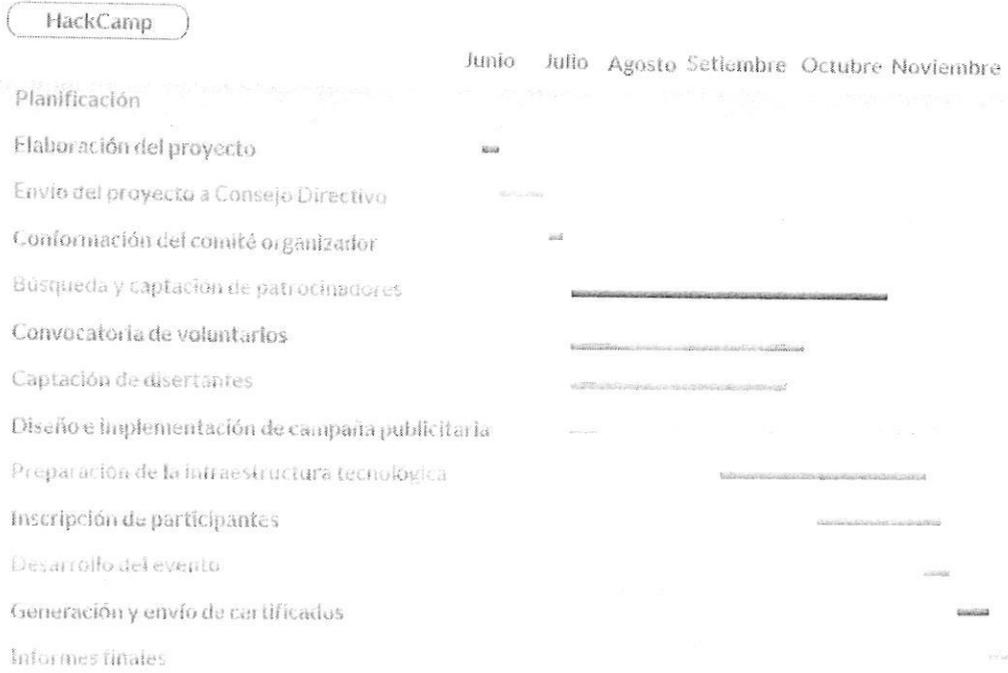
Medir y llevar a la práctica los conocimientos adquiridos a través de la competencia entre equipos.

8. Cronograma y presupuesto

8.1. Presupuesto

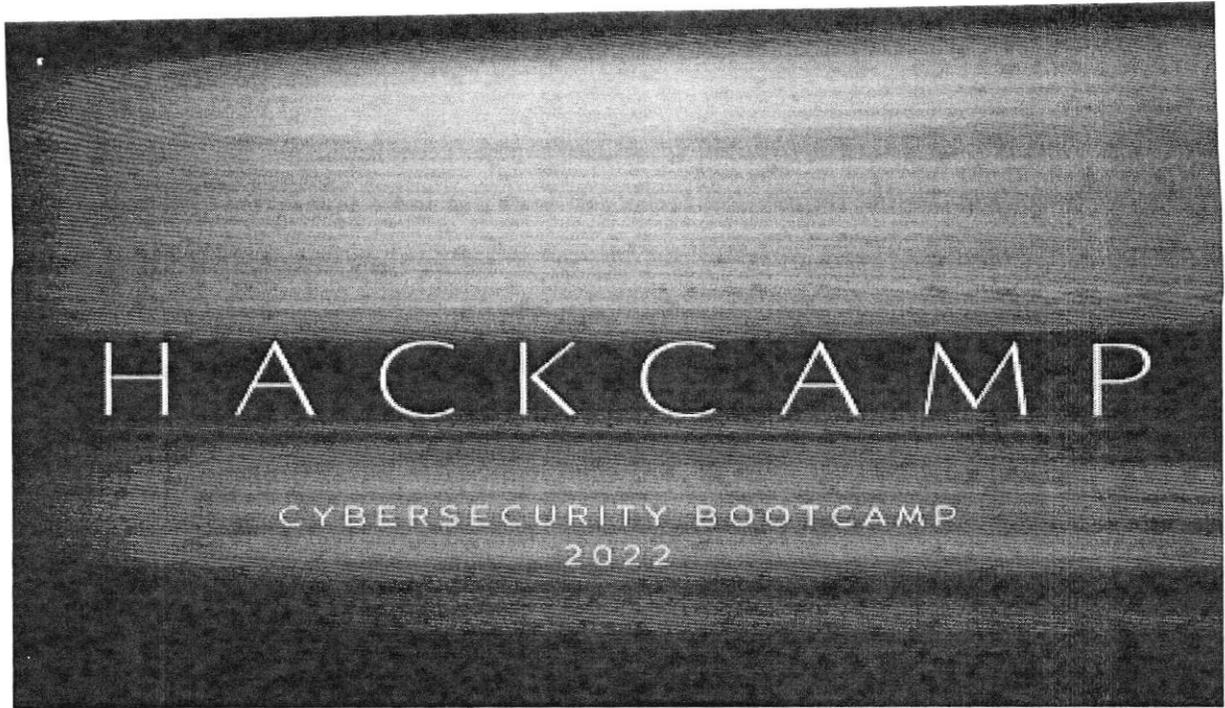
Ítem	Descripción	Cantidad	Unidad	Fuente Recursos			Total
				Institucional	Propio	Donaciones	
1	Estudiante voluntario	200	1	X			200
2	Funcionario	10	1	X			10
3	Speaker	5				ad honorem	5
4	Computadora	10	1	X			10
5	Impresora	1	1	X			1
6	Hojas para impresión	250	1	X			250
7	Toner	1	1	X			1
8	Equipo de comunicación	3	1	X			3
9	Local del evento	1	1			X	1
10	Mesa	20	1	X			20
11	Silla	40	1	X			40
12	Micrófono	2	1	X			2
13	Parlante	2	1	X			2
14	Proyector	1	1	X			1
15	merchandising	200	1			X	200
TOTAL							746

8.2.1. Cronograma



9. Referencias Bibliográficas (Formato APA)

Elaboración propia



22 JUNIO

Dirección de Tecnología de la Información y Comunicación

Dirección Académica - Coordinación de Movilidad Académica y Pasantías

Creado por:

- Mag. Fátima Barrios Villagra
- Prof. Msc. Liduvina Vega de Urizar

En los últimos años ha habido una evolución tecnológica sin precedentes, esta rápida evolución, y el hecho de que esta tecnología sean altamente vulnerables a ataques maliciosos, deja en evidencia el gran riesgo al que nos enfrentamos al no contar con mecanismos que nos permitan defendernos y dar respuesta a este tipo de incidentes, y Paraguay no se encuentra ajeno a esto, ya que la pandemia del COVID-19 ha forzado el incremento del uso de la tecnología y la automatización de procesos permitiendo la agilización de los mismos. En la actualidad se puede encontrar una gran cantidad de amenazas como ataques a la red, el secuestro de datos, ingeniería social, etc.

Este hecho ha ocasionado que la perspectiva de la seguridad cambie y cobre un papel especialmente importante haciendo que las organizaciones inviertan recursos para crear departamentos sólidos que garanticen la ciberseguridad.

Hoy en día, el perfil de ciberseguridad es uno de los más buscados por las empresas e instituciones, la infraestructura tecnológica y los sistemas de dichas organizaciones son parte clave para su desarrollo y funcionamiento, por lo que conocer las amenazas, vulnerabilidades y cómo realizar la mitigación oportuna de los riesgos actuales es fundamental.

Este proyecto pretende promover el desarrollo de habilidades en el campo de la ciberseguridad de manera a que las organizaciones se encuentren preparadas para enfrentar los riesgos actuales y concientizar sobre la importancia de la seguridad digital.

La Dirección de Tecnología de la Información y Comunicación en conjunto con la Coordinación de Movilidad Académica y Pasantías (MAP) de la Facultad Politécnica de la UNA, propone la realización de una capacitación intensiva de corta duración enfocada a la adquisición de conocimientos en el área de ciberseguridad, que conste de dos fases principales:

- La primera, en la que se impartirán por medio de charlas y talleres todos los conocimientos propuestos para esta primera edición.
- La segunda, la cual permitirá la aplicación de todos los conocimientos adquiridos, a través de una competencia entre equipos. Dicha competencia consistirá básicamente en la aplicación de técnicas defensivas y ofensivas. Por lo que un equipo deberá cumplir el rol de Red team, esto quiere decir que buscará atacar al otro, tratando de encontrar sus vulnerabilidades y explotarlas. Sin embargo, el otro equipo, cumplirá el rol de Blue Team, es decir, tratará de defenderse buscando fortificar sus defensas para evitar que los ataques del otro equipo ocasionen una denegación de sus servicios o mitigar sus efectos. Ganará el equipo que haya logrado obtener el mayor puntaje.

La actividad será abierta a la participación de profesionales del ámbito tecnológico y estudiantes tanto de la Facultad Politécnica como de otras universidades.

Cada Empresa participante contará con un stand, una mesa y dos sillas disponibles para su muestra.

Durante la jornada se podrá entregar a los profesionales y estudiantes afiches, revistas y publicaciones para dar a conocer productos y proyectos que las empresas desarrollan.

Esta actividad busca, a través de una experiencia inmersiva, incrementar el nivel de conocimiento de los participantes en el área de la ciberseguridad a través de la práctica de técnicas defensivas (Blue team) y ofensivas (Red team) en un entorno controlado.

Nuestros OBJETIVOS:

- Incrementar el conocimiento de ciberseguridad a través de una jornada completa de Conferencias y una Competencia intensa, inmersiva y segura.
- Dar a conocer la importancia de la ciberseguridad, sus diferentes ramas de actuación e impacto actual en las empresas públicas y privadas.
- Presentar las principales técnicas defensivas y ofensivas que son empleadas en la actualidad por los profesionales del sector.
- Proveer un entorno seguro y controlado para que puedan ser aplicados los conocimientos adquiridos a través de una competencia simulada.

HackCamp

Primera edición

Fecha propuesta: Miércoles 16 de noviembre

Horario: 09:00 a 17:00

Lugar : A confirmar

Responsables : MAG. FÁTIMA BARRIOS VILLAGRA
Directora de Tecnología de la Información y Comunicación (DTIC)
MAG. LIDUVINA VEGA DE URIZAR
Coordinadora de Movilidad Académica y Pasantías (CMP)