23903

Universidad Nacional de General Sarmiento

Expediente N°22372/19.-

LOS POLVORINES, 23 DIC 2019

**VISTO:** el Estatuto de la Universidad Nacional de General Sarmiento; la Resolución (CS) N°2614/08, la Resolución (CIDEI) N°5779/19, el Expediente N°22372/19; y

**CONSIDERANDO:**

Que por Resolución (CS) N°2614/08 se aprueban los Lineamientos Generales para el Desarrollo de las actividades de Formación Continua en la Universidad Nacional de General Sarmiento.

Que mediante Resolución (CIDEI) N°5779/19 el Consejo del Instituto de Industria aprobó en primera instancia el dictado del Curso de Formación Continua "Seguridad en Redes Wifi".

Que los contenidos de la propuesta se ajustan a los Lineamientos Generales para el Desarrollo de las actividades de Formación Continua de la UNGS.

Que corresponde aprobar el Curso de Formación Continua "Seguridad en Redes Wifi" su estructura, contenidos y modalidad.

**POR ELLO:**

**EL VICERRECTOR EN EJERCICIO DEL RECTORADO**
**DE LA UNIVERSIDAD NACIONAL DE GENERAL SARMIENTO**
**RESUELVE:**

**ARTÍCULO N°1:** Aprobar el Curso de Formación Continua "Seguridad en Redes Wifi" cuyo programa analítico forma parte de la presente Resolución como anexo en cuatro (4) páginas.

**ARTÍCULO N°2:** Regístrese, comuníquese al Instituto de Industria, a la Dirección de Formación Continua, a la Dirección de Títulos y Planes, a Dirección General de Biblioteca y Documentación y a la Unidad de Auditoría Interna. Cumplido, archívese.

UNGS

**RESOLUCIÓN DE RECTORADO N°:** 23903

Lic. Pablo Daniel Bonaldi
Vicerrector en ejercicio del Rectorado
Universidad Nacional de General Sarmiento

Universidad Nacional de General Sarmiento

Expediente N°22372/19.-

Dirección de Formación Continua

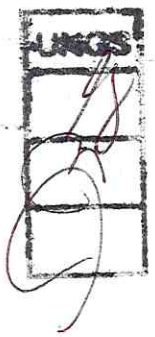
## 1- DATOS IDENTIFICATORIOS DEL PROYECTO

**Título del proyecto**: Seguridad en Redes Wifi

- **Localización de la oferta:** Dependencias de la UNGS y/u otras Instituciones por medio de convenio con la UNGS.
- **Área y/o disciplina comprendida en la capacitación**: Sistemas - Informática
- **Destinatarios:** Estudiantes de la Licenciatura en Sistemas que hayan aprobado las asignaturas Programación II y Sistemas Operativos y Redes I
- **Modalidad de la capacitación**: Presencial
- **Formato:** Curso
- **Carga horaria**: 12 horas
- **Costo**: El curso será gratuito para los/as estudiantes de la UNGS y arancelado para los/as estudiantes externos.
- **Presupuesto**: Instituto de Industria

## 2- EQUIPO CAPACITADOR

- **Nombres y apellido:** Alexis Guido Tcach Lufrano
- **N° de documento:** 39.829.633
- **Título:** Lic. Cs. Computación




- **Nombres y apellido:** Lucas Maximiliano Addisi
- **N° de documento:** 39.829.633
- **Título:** Técnico Superior en Informática

- **Apellido y Nombres:** Agustín Carlos Alexander
- **N° de documento:** 38.866.768
- **Título:** Técnico Superior en Informática



Juan María Gutiérrez 1150 (B1613GSX) Los Polvorines, Provincia de Buenos Aires, Argentina
Conmutador: 4469-7500 - (B1663ZAB) San Miguel
Centro Cultural: Julio A. Roca 850 (B1663MIR) San Miguel, Provincia de Buenos Aires, Argentina - Teléfono: 4451-7924/25
info@ungs.edu.ar - www.ungs.edu.ar

## 3- DESCRIPCIÓN DEL PROYECTO

**•Síntesis del proyecto:**

En este curso se analizarán algunos de los ataques más comunes en las redes wireless. Para ello, se introducirá al funcionamiento físico y de acceso al medio de las redes wireless. Luego, se analizarán algunos de los vectores de ataques más comunes, como por ejemplo ataques a protocolos de seguridad WEP y WPA/WPA2 o seguimiento de personas a partir de señales. El curso se cerrará con un conjunto de ataques aplicado con la finalidad de obtener credenciales de acceso a una página que así lo requiera.

**•Fundamentación:**

El uso de dispositivos electrónicos que se conectan a redes wireless es masivo. La mayoría de las personas cuentan con teléfonos inteligentes o computadoras portátiles, los cuales accede a Internet a través de una conexión wifi. Sin embargo, pocos advierten los riesgos que puede traer aparejado conectarse a redes inalámbricas públicas o la utilización de protocolos de seguridad vulnerables. Este curso, brindará los conocimientos básicos para entender el funcionamiento de las redes Wifi, conocer los ataques más comunes en este tipo de redes y cómo mitigar estas contingencias.

**•Objetivos:**

El objetivo de este curso es que los/as estudiantes adquieran un marco teórico para entender cómo funcionan las técnicas de ataques de redes Wireless (más recurrentes) y los protocolos de seguridad en Redes Wifi.

- **Contenidos**

  1. Modelo OSI

  Se introducirá al modelo conceptual que caracteriza y estandariza las funciones de interconexión de sistemas de computación, sin importar la organización de los componentes internos ni la tecnología implementada.

  2. Capa Física

  Se explicará la capa física, vinculada a cómo son trasmitidos a través de medios físicos como el aire

  3. Capa MAC

  Explicación de la capa de Acceso al medio, aquella por la cual se encarga de controlar el hardware responsable de la interacción con el medio de transmisión



Juan María Gutiérrez 1150 (B1613GSX) Los Polvorines, Provincia de Buenos Aires, Argentina
Conmutador: 4469-7500 - (B1663ZAB) San Miguel
Centro Cultural: Julio A. Roca 850 (B1663MIR) San Miguel, Provincia de Buenos Aires, Argentina - Teléfono: 4451-7924/25
info@ungs.edu.ar - www.ungs.edu.ar

4. CSMA CA/CD

Se entenderá cuál es la importancia del protocolo Carrier-sense Múltiple Access para verificar la presencia de tráfico antes de la transmisión en un medio compartido.

5. 802.11

Se introducirá a la estandarización regulada por la IEEE de las redes Wifi. Se explicarán los tipos de redes y la estructura de los frames de paquetes Wifi.

6. Protocolos de seguridad Wifi

Se explicarán los protocolos más utilizados para la seguridad de redes Wifi. Estos son, el protocolo WEP y el protocolo WPA/WPA2.

7. Sniffing/Seguimiento de personas

Se introducirán conceptos para el seguimiento de personas a partir de los datos que emiten los dispositivos móviles que estas pueden llevar consigo.

8. Caso Práctico WEP Attack

Caso práctico en clases de cómo se puede vulnerar una red Wifi protegida a partir del protocolo WEP utilizando la suite de herramientas de Aircrack-ng.

9. WPA2 Attack

Se explicará la nueva vulnerabilidad descubierta en protocolos WPA/WPA2 llamada KRACK. Aquí, se profundizará sobre detalles técnicos de este protocolo y se explicará que vulnerabilidad aprovecha el ataque.

10. Caso Práctico: Deuth Attack + Evil Twin + DNS Poissoning

Para finalizar el curso, se realizará una demostración de un conjunto de ataques con el fin de la obtención de contraseñas. Además, se ahondará con detalles en cada uno de los ataques y las vulnerabilidades que aprovechan.

- **Duración y carga horaria**
  12 horas en 4 encuentros de 3 hs.



Juan María Gutiérrez 1150 (B1613GSX) Los Polvorines, Provincia de Buenos Aires, Argentina
Conmutador: 4469-7500 - (B1663ZAB) San Miguel
Centro Cultural: Julio A. Roca 850 (B1663MIR) San Miguel, Provincia de Buenos Aires, Argentina - Teléfono: 4451-7924/25
info@ungs.edu.ar - www.ungs.edu.ar

**•Evaluación:**

Se realizará un trabajo práctico integrador del curso al final del mismo.

**•Bibliografía:**


- Tanenbaum, A. S. (2003). *Redes de computadoras*. Pearson educación.
- Scambray, J., McClure, S., & Kurtz, G. (2000). *Hacking exposed*. McGraw-Hill Professional.
- Vanhoef, M., & Piessens, F. (2017, October). Key reinstallation attacks: Forcing nonce reuse in WPA2. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1313-1328). ACM.


- **Certificación**

Certificación de asistencia, con una asistencia mínima del 75% del total de las clases.



Juan María Gutiérrez 1150 (B1613GSX) Los Polvorines, Provincia de Buenos Aires, Argentina
Conmutador: 4469-7500 - (B1663ZAB) San Miguel
Centro Cultural: Julio A. Roca 850 (B1663MIR) San Miguel, Provincia de Buenos Aires, Argentina - Teléfono: 4451-7924/25
info@ungs.edu.ar - www.ungs.edu.ar