



SEGURIDAD INFORMÁTICA

Duración: 40 horas reloj

Modalidad: virtual con encuentros sincrónicos por zoom

Ciclo lectivo: 2026

Convocatoria: 1era

Inicio: 10 de marzo 2026

Finalización: 30 de abril 2026

Presentación

En la actualidad, la seguridad informática se ha convertido en una necesidad fundamental para todas las personas, independientemente de su nivel de conocimientos técnicos. Las estafas digitales, el robo de identidad, el phishing y el fraude mediante redes sociales, bancos y billeteras virtuales se han multiplicado en los últimos años.

Este curso propone brindar herramientas prácticas y accesibles para reconocer amenazas, actuar de manera preventiva y responder correctamente ante incidentes. No se requieren conocimientos previos. La propuesta está orientada a usuarios cotidianos que necesitan proteger su información personal, financiera y familiar mientras utilizan computadoras, celulares, aplicaciones bancarias y redes sociales.

El curso combina conceptos esenciales con ejercicios reales y actividades de análisis para desarrollar criterios sólidos que permitan detectar estafas y minimizar riesgos.

Objetivos

- Desarrollar competencias básicas en seguridad informática, proporcionando conocimientos fundamentales que permitan comprender las principales amenazas digitales actuales y su impacto en la vida cotidiana.
- Fortalecer la capacidad de prevención y detección de estafas digitales, mediante la identificación de señales de alerta en correos electrónicos, mensajes, redes sociales, plataformas bancarias y sitios web.
- Promover prácticas seguras en el uso de dispositivos y servicios digitales, brindando herramientas concretas para la protección de datos personales, la gestión segura de cuentas y la correcta actuación ante incidentes de seguridad informática.



Contenidos

Unidad 1: Introducción a la Seguridad Informática

- Definición de seguridad informática: confidencialidad, integridad y disponibilidad.
- Principales amenazas actuales: malware, phishing, ingeniería social.
- Por qué todos somos potenciales víctimas: panorama actual en Argentina.
- Ejemplos reales de estafas digitales.

Unidad 2: Phishing, Smishing y Vishing

- Estafas por correo electrónico: señales de alerta.
- Smishing: fraudes mediante SMS (AFIP, bancos, envíos, MercadoPago).
- Vishing: llamadas fraudulentas y manipulación psicológica.
- Cómo analizar enlaces, remitentes y páginas clonadas.
- Práctica guiada: detección de phishing real.

Unidad 3: Seguridad en Redes Sociales y Mensajería

- Robo de cuentas de WhatsApp: técnicas utilizadas y prevención.
- Privacidad y protección en Instagram, Facebook y WhatsApp.
- Estafas de compras falsas, perfiles falsos, Marketplace y catfishing.
- Exposición excesiva de datos personales en redes.
- Configuración guiada de verificación en dos pasos.

Unidad 4: Seguridad Financiera Digital

- Estafas bancarias y con billeteras virtuales (MercadoPago, homebanking).
- Falsos comprobantes de pago y fraudes con QR.
- Compras online seguras: cómo identificar sitios legítimos.
- Contraseñas seguras y autenticación multifactor.
- Buenas prácticas para transferencias y operaciones.



Unidad 5: Protección de Dispositivos y Redes

- Buenas prácticas de uso de computadoras y celulares.
- Señales de malware, apps peligrosas y permisos indebidos.
- Antivirus, actualizaciones y copias de seguridad.
- Seguridad en redes WiFi hogareñas y routers.
- Checklist de seguridad personal.

Unidad 6: Cómo Actuar Ante Estafas y Recuperación de Cuentas

- Procedimiento inmediato ante un fraude o intento de estafa.
- Canal de denuncias oficiales: Policía, UFECL, entidades bancarias.
- Recuperación de cuentas: WhatsApp, Instagram, Gmail, MercadoPago.
- Elaboración de un “Plan Personal de Ciberseguridad”.

Metodología

Este curso es de modalidad virtual y tiene una duración de dos meses. Asimismo, está planteado un (1) encuentro sincrónico al finalizar cada unidad con el equipo de tutoría para facilitar el desarrollo de los temas a abordar. En dicho encuentro se realizará una exposición teórica como también la explicación de algún caso práctico o ejercicio. Las clases sincrónicas serán por zoom. Los contenidos están desarrollados en unidades didácticas, que contemplan palabras claves, material de lectura obligatoria y de apoyo, actividades de evaluación diseñadas por el docente junto con propuestas de reflexión y análisis orientadas a poner en práctica los conocimientos adquiridos.

Todos los recursos disponibles en el campus podrán ser descargados por los participantes y alojados en sus respectivos dispositivos electrónicos.

El día de inicio del curso cada alumno recibirá sus datos de ingreso (usuario y contraseña) que le permitirán acceder a los materiales.

El campus virtual está articulado sobre una plataforma entorno Moodle, que es un sistema de gestión que propicia y promueve la construcción de comunidades de aprendizaje de la que participan los docentes, los tutores y los alumnos participantes. Tiene una interfaz de navegador de tecnología sencilla que simplificará sus recorridos didácticos.

La propuesta educativa propicia la construcción de comunidades de aprendizaje conformadas por personas geográficamente distantes pero que comparten esta experiencia en un entorno virtual, y así podrán de manera compartida recorrer un trayecto formativo que les permita adquirir nuevas herramientas para su desarrollo laboral.

Evaluación / Condiciones de aprobación



Una vez abierto el curso, el estudiante podrá acceder con su usuario y contraseña al campus virtual e ir descargando el material como así también realizando las tareas que el equipo de tutoría vaya proponiendo a lo largo de la cursada.

La aprobación del mismo combinará la evaluación de los siguientes factores:

- Realización de las actividades que se propongan.
- Participación en foros.
- 75% de asistencia a las clases sincrónicas.
- Aprobación de la instancia final de evaluación integral.

Una vez aprobado el curso, la plataforma requerirá al cursante responder una encuesta relacionada a la experiencia de aprendizaje transitada y una vez respondida se podrá descargar el certificado que es digital con formato para impresión y avalado por UTEDYC.