Seguridad Informática

Formato: Asignatura

Régimen: Cuatrimestral 2° Cuatrimestre

Curso: 3 Año

División: "A"

Carrera: "Profesorado de Educación Secundaria en Informática"

N° de Plan: 737

Año: 2025

Institución: "Instituto de Formación Docente N° 13 – Nivel Superior

Profesora: Bani Natalia Maria Lourdes

Campo de la Formación Docente: Formación Específica

1- Fundamentación:

En la sociedad actual, profundamente atravesada por el uso de tecnologías digitales, la **seguridad informática** se constituye como un eje estratégico en la formación de futuros Docentes de informática. Lejos de limitarse a una dimensión técnica, la seguridad informática implica una comprensión integral de los riesgos, amenazas y responsabilidades vinculadas al uso, gestión y protección de los recursos informáticos —tanto materiales como inmateriales—, en múltiples entornos: **institucionales, educativos, personales y sociales**.

Se abordarán los conceptos fundamentales de la **ciberseguridad y la seguridad de la información**, considerando los principios que orientan su implementación: confidencialidad, integridad, disponibilidad, autenticidad e irrefutabilidad. Se reconoce que la protección de los sistemas informáticos no solo se refiere al hardware o al software, sino también a las personas, las redes, los datos y el entorno físico y legal que los rodea.

En un escenario marcado por la expansión de la **Internet de las Cosas,** el uso cotidiano de **redes sociales** y la creciente dependencia de sistemas digitales, resulta imprescindible que el futuro docente comprenda la dimensión ética, legal y social de la seguridad. Esto implica conocer y reflexionar sobre normativas vigentes, delitos informáticos, protección de datos personales, ciudadanía digital, así como los desafíos emergentes en relación al grooming, sexting, ciberbullying y muchas otras problemáticas que afectan especialmente a niñas, niños y adolescentes.

Desde un enfoque pedagógico, este espacio promueve una **formación crítica, contextualizada y actualizada**, que permita a las y los estudiantes analizar, evaluar y diseñar estrategias de seguridad aplicables tanto en entornos educativos como en otros ámbitos

institucionales. Asimismo, se enfatiza el rol del docente en la **prevención, la formación en ciudadanía digital** y la promoción de prácticas responsables y seguras en el uso de las tecnologías.

Se trata de integrar dimensiones técnicas, legales, éticas y educativas, articulando teoría y práctica, con actividades de análisis, diseño, planificación e implementación de políticas y estrategias de seguridad informática, fomentando una actitud profesional comprometida con la protección de los derechos, los datos y la integridad de las personas en el entorno digital.

2- Propósitos

- Comprender los principios fundamentales de la seguridad informática y su aplicación en diferentes contextos.
- Analizar las amenazas, vulnerabilidades y tipos de ataques que afectan a los sistemas informáticos, las redes y los datos.
- Conocer y aplicar criterios y políticas de seguridad orientadas a minimizar riesgos y garantizar la continuidad operativa de los sistemas.
- Abordar problemáticas actuales vinculadas a la ciudadanía digital: uso de redes sociales, identidad digital, huella digital, privacidad y delitos informáticos.
- Promover la incorporación de prácticas seguras en la enseñanza y en el uso cotidiano de las tecnologías por parte de docentes y estudiantes.
- Desarrollar estrategias pedagógicas para formar usuarios críticos y responsables en relación al uso de las TIC y la protección de la información.
- Diseñar propuestas didácticas que integren la seguridad informática en el marco de la educación digital, la alfabetización tecnológica y la formación ciudadana.

3- Núcleos temáticos/nudos/ejes/problemas

Eje 1- Introducción a la Seguridad Informática:

- Conceptos fundamentales: seguridad, ciberseguridad, activos de información.
- Principios de la seguridad: confidencialidad, integridad, disponibilidad, autenticidad e irrefutabilidad.

Bibliografía Obligatoria:

https://www.fortinet.com/lat/resources/cyberglossary/cia-triad

https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/cert-ar?utm_source=chatgpt.com

https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

https://www.bcra.gob.ar/SistemasFinancierosYdePagos/Ciberseguridad.asp#Riesgos%20relacionados%20con%20Tecnolog%C3%ADas%20de%20la%20Informaci%C3%B3n

https://optic.neuquen.gov.ar/seguridad-informatica/

https://fundacionsadosky.org.ar/wp-content/uploads/2023/12/Seguridad-de-la-informacion-y-ciberseguridad.pdf

https://fundacionsadosky.org.ar/wp-content/uploads/2023/12/Perfiles-en-ciberseguridad.pdf

Bibliografía Opcional

https://www.autonoma.pe/blog/principios-basicos-seguridad-informatica/#:~:text=permisos%20de%20acceso.-,6.,para%20garantizar%20el%20no%20repudio

Eje 2 - Marco legal, ética y ciudadanía digital

- Derecho informático. Propiedad intelectual. Firma digital.
- Burbujas informativas y algoritmos (Reflexión crítica sobre cómo funcionan las redes sociales y cómo condicionan lo que vemos.).
- Ciudadanía digital: identidad digital, huella digital- reputación, derecho al olvido.

- Derechos del niño en la era digital (ONU y UNICEF).
- Responsabilidad Digitales
- Delitos informáticos: Sharenting -grooming, cyberbullying - sexting, - Difusión de imagen sin consentimiento
- Bienestar digital (manejo del tiempo de pantalla y estrategias de autocuidado).
- Gaming seguro y riesgos en plataformas de juego (Prevención de riesgos en juegos en línea: lenguaje tóxico, compras en juegos).- Ludopatía digital.
- Scrolling infinito y patrones oscuros (Impacto del consumo continuo de contenidos, diseño persuasivo de plataformas).

Bibliografía Obligatoria

Faro Digital: https://farodigital.org/

Chicos Net : https://www.chicos.net/

Elegí tu forma: https://www.eligetuforma.org/

Grooming Argentina: www.groomingarg.org

Pantallas Amigas: https://www.pantallasamigas.net/

https://ceibal.edu.uy/institucional/ciudadania-digital/materiales-didacticos/

https://www.unicef.org/argentina/sites/unicef.org.argentina/files/2018-04/COM-Guia_ConvivenciaDigital_ABRIL2017.pdf

https://www.unicef.org/argentina/media/24881/file/ResumenEjecutivoKidsOnline2025.pdf.pdf

Eje 3 - Tipos de amenazas y estrategias de protección

Malware: virus, troyanos, spyware, ransomware. - Criptografía y esteganografía: fundamentos y aplicaciones básicas.

Análisis de malware (introducción al análisis estático/dinámico). Seguridad física y organizacional: controles y políticas.

Bibliografía Obligatoria

https://elhacker.info/manuales/An%c3%a1lisis%20de%20malware/Analisis%20de%20malware,%20metodologia.pdf

https://es.wikipedia.org/wiki/ISO/IEC_27032

https://www.inria.cl/sites/default/files/2022-12/libro-blanco-ciberseguridad-es.pdf

Bibliografía Opcional

https://elhacker.info/manuales/Libros%20hack/RAMA%20-%20Seguridad%20y%20Alta%20Disponibilidad.pdf

Eje 4 - Seguridad en entornos específicos

Seguridad en Sistemas Operativos, Redes y Bases de Datos. Internet de las Cosas (IoT) y sus implicancias en la seguridad. Planes de contingencia y evaluación de riesgos.

Bibliografía Obligatoria:

https://es.wikipedia.org/wiki/ISO/IEC_27033

https://es.wikipedia.org/wiki/ISO/IEC_27000

https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Linea_de_investigacion_Ciberseguridad.pdf

https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=932207

https://es.wikipedia.org/wiki/Plan_de_contingencias

https://es.wikipedia.org/wiki/Plan_de_recuperaci%C3%B3n_ante_desastres

Bibliografía Opcional

https://www.fortinet.com/lat/resources/cyberglossary/iot-security

https://openaccess.uoc.edu/server/api/core/bitstreams/77cadf41-abcb-4ed7-9851-a4037e6181c2/content

4- Propuesta metodología

Se utilizarán las siguientes estrategias metodológicas:

- Aprendizaje Interactiva: la explicación y la pregunta
- Exposición dialogada que tome en cuenta las preguntas de los estudiantes para realizar un intercambio de saberes. Con apoyo visual de pizarra y proyector.
- Exposición por parte de los estudiantes de las temáticas.
- Los contenidos de cada eje temático estarán en la plataforma del campus virtual del IFD N° 13 con la finalidad que los estudiantes puedan consultar, visualizar, y descargar el material de estudio.
- Utilización de mensajería y foros para posibles consultas a través de la plataforma del campus virtual.
- La bibliografía estará también disponible en dicha plataforma mientras se desarrolle la cursada para que los estudiantes tengan acceso a la misma.
- Se trabaja en forma conjunta con la Universidad Nacional del Comahue Facultad de Informática en el acompañamiento de los Talleres EESiSeg 2025.

5- Ejes/Pautas de evaluación y Acreditación

La evaluación del estudiante será en proceso, continua y sumativa (Basada en el RAI de la institución).

Se tendrán en cuenta los siguientes cortes evaluativos.

- **Trabaja Práctico expositivo Evaluativo**, individual con sus respectivas instancias de recuperación.
- Se evaluará la participación activa para el desarrollo de los talleres articulados con la Facultad de Informática (UNCO) EESiSeg 2025.
- **Trabajo Práctico Final, individual,** se desarrollará el diseño de una clase teniendo en cuenta los contenidos de seguridad informática.
- Todos los trabajos a realizar se deberán subir a la plataforma Campus Virtual del IFD N° 13 y en ese mismo espacio recibirán

la retroalimentación y formas de recuperación en caso de no acreditar dicha instancia

Todos estos contenidos y temáticas se evaluarán teniendo en cuenta los siguientes criterios

- Expresión oral adecuada a las temáticas y situaciones comunicativa en clases
- Claridad y fundamentación para la exposición de las temáticas
- Manejo de contenidos abordados
- Participación pertinente tanto para los trabajos y producciones dentro del aula como así también con los talleres EESiSeg 2025.
- Responsabilidad y respeto en todo momento entre pares y hacia la docente.
- Seguridad Informática posee formato de asignatura por lo que: Para la acreditación del espacio se tendrá en cuenta la normativa vigente del RAI que establece en su inciso 6.1.

6.1.1. APROBADO cuando el/la estudiante reúne el requisito de asistencia 60 % y obtiene nota igual o superior a 4 (cuatro) puntos en todas las instancias acreditables propuestas en la Planificación y/o programa.

El/la estudiante que cumpliese entre el 50 y el 60 % de asistencia siempre que sus ausencias estén debidamente justificadas tendrá derecho a una instancia de recuperación integradora para los espacios curriculares que conllevan examen final, pudiendo de esa manera conservar la condición de regularidad en el espacio.

6.1.2. Si el/la estudiante obtuviera en alguna de las instancias acreditables una nota entre uno (01) y seis (06) podrá acceder a una instancia de recuperación, no perdiendo por ello la posibilidad de promoción. La nota del recuperatorio quedará como única validez del proceso evaluativo, sin necesidad de promediarse con la calificación del mismo corte evaluativo recuperado, ni sometida a ninguna instancia de revalidación ulterior.

6.2 PROMOCIÓN: para acceder a esta instancia, los requisitos son:

• Cumplir con un mínimo de 75 % de asistencia.

• Aprobar con un mínimo de 7 (siete) puntos todas las instancias acreditables.

8.3.2 LIBRE: Se constituye en la tercera modalidad de acreditación.

• Los programas que se utilizarán para los exámenes libres serán, en tanto se presenten las actualizaciones del año en curso, los programas del ciclo lectivo anterior.

• El examen libre comprenderá dos instancias, escrita, donde deberá desarrollar un trabajo domiciliario. Solo si resultara aprobada esta primera instancia, podrá pasar a la instancia oral, en la que deberá exponer la temática enmarcada en el programa y hacer frente a las preguntas y desafíos propuestos por el tribunal evaluador.

Es requisito que el\la estudiante asista a la mesa examinadora en el horario estipulado con: DNI (original), permiso de examen, programa de examen libre o regular. Contar con los recursos necesarios para la exposición y defensa del trabajo (computadora, caños, equipo de audio, etc).

Instituto de Formación Docente N° 13 Nivel Superior
Seguridad Informática
Profesora de Educación Secundaria en Informática
Asignatura – 2° Cuatrimestre – Plan: 737 – 3 Año "A" – 2025
Prof. Bani Natalia – Formación Específica

Seguridad Informática

(Programa de Examen Libre 2025)

Eje 1- Introducción a la Seguridad Informática:

- Conceptos fundamentales: seguridad, ciberseguridad, activos de información.
- Principios de la seguridad: confidencialidad, integridad, disponibilidad, autenticidad e irrefutabilidad.

Bibliografía Obligatoria:

https://www.fortinet.com/lat/resources/cyberglossary/cia-triad

https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/cert-ar?utm_source=chatgpt.com

https://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

https://www.bcra.gob.ar/SistemasFinancierosYdePagos/Ciberseguridad.asp#Riesgos%20relacionados%20con%20Tecnolog%C3%ADas%20de%20la%20Informaci%C3%B3n

https://optic.neuquen.gov.ar/seguridad-informatica/

https://fundacionsadosky.org.ar/wp-content/uploads/2023/12/Seguridad-de-la-informacion-y-ciberseguridad.pdf

https://fundacionsadosky.org.ar/wp-content/uploads/2023/12/Perfiles-en-ciberseguridad.pdf

Bibliografía Opcional

https://www.autonoma.pe/blog/principios-basicos-seguridad-informatica/#:~:text=permisos%20de%20acceso.-,6.,para%20garantizar%20el%20no%20repudio

Eje 2 - Marco legal, ética y ciudadanía digital

- Derecho informático. Propiedad intelectual. Firma digital.
- Burbujas informativas y algoritmos (Reflexión crítica sobre cómo funcionan las redes sociales y cómo condicionan lo que vemos.).
- Ciudadanía digital: identidad digital, huella digital- reputación, derecho al olvido.
- Derechos del niño en la era digital (ONU y UNICEF).
- Responsabilidad Digitales
- Delitos informáticos: Sharenting -grooming, cyberbullying - sexting, - Difusión de imagen sin consentimiento
- Bienestar digital (manejo del tiempo de pantalla y estrategias de autocuidado).
- Gaming seguro y riesgos en plataformas de juego (Prevención de riesgos en juegos en línea: lenguaje tóxico, compras en juegos).- Ludopatía digital.
- Scrolling infinito y patrones oscuros (Impacto del consumo continuo de contenidos, diseño persuasivo de plataformas).

Bibliografía Obligatoria

Faro Digital: https://farodigital.org/

Chicos Net : https://www.chicos.net/

Elegí tu forma: https://www.eligetuforma.org/

Grooming Argentina: www.groomingarg.org

Pantallas Amigas: https://www.pantallasamigas.net/

https://ceibal.edu.uy/institucional/ciudadania-digital/materiales-didacticos/

https://www.unicef.org/argentina/sites/unicef.org.argentina/files/2018-04/COM-Guia_ConvivenciaDigital_ABRIL2017.pdf

https://www.unicef.org/argentina/media/24881/file/ResumenEjecutivoKidsOnline2025.pdf.pdf

Eje 3 - Tipos de amenazas y estrategias de protección

Malware: virus, troyanos, spyware, ransomware. - Criptografía y esteganografía: fundamentos y aplicaciones básicas.

Análisis de malware (introducción al análisis estático/dinámico). Seguridad física y organizacional: controles y políticas.

Bibliografía Obligatoria

https://elhacker.info/manuales/An%c3%a1lisis%20de%20malware/Analisis%20de%20malware,%20metodologia.pdf

https://es.wikipedia.org/wiki/ISO/IEC_27032

https://www.inria.cl/sites/default/files/2022-12/libro-blanco-ciberseguridad-es.pdf

Bibliografía Opcional

https://elhacker.info/manuales/Libros%20hack/RAMA%20-%20Seguridad%20y%20Alta%20Disponibilidad.pdf

Eje 4 - Seguridad en entornos específicos

Seguridad en Sistemas Operativos, Redes y Bases de Datos. Internet de las Cosas (IoT) y sus implicancias en la seguridad. Planes de contingencia y evaluación de riesgos.

Bibliografía Obligatoria:

https://es.wikipedia.org/wiki/ISO/IEC_27033

https://es.wikipedia.org/wiki/ISO/IEC_27000

https://selloeditorial.unad.edu.co/images/Documentos/ciberseguridad/Linea_de_investigacion_Ciberseguridad.pdf

https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=932207

https://es.wikipedia.org/wiki/Plan_de_contingencias

https://es.wikipedia.org/wiki/Plan_de_recuperaci%C3%B3n_ante_desastres

Bibliografía Opcional

https://www.fortinet.com/lat/resources/cyberglossary/iot-security

https://openaccess.uoc.edu/server/api/core/bitstreams/77cadf41-abcb-4ed7-9851-a4037e6181c2/content

Metodología Trabajo Domiciliario:

Pautas y Evaluación: Se considera el desarrollo basado en la bibliografía dada en la asignatura. El examen libre será de manera oral a modo de defensa del trabajo escrito, la misma deberá ser dada con el apoyo de una presentación multimedia.

Criterios de presentación: El trabajo deberá contener una portada, tipografía adecuada, redacción clara y cuidado de la ortografía. Deberá tener coherencia en el desarrollo de cada punto, al igual que la justificación conceptual, partiendo de una producción propia.

Fecha de entrega: 15 días antes de la fecha de mesa de examen correspondiente, como se estipula en el RAI institucional.

Consignas:

De acuerdo a las temáticas dadas en Seguridad informática desarrolle una de ellas

- ✔ Deberá desarrollar un plan de clases en base al diseño curricular del nivel medio.
- ✔ Desarrollar la temática con los conceptos, pautas de prevención y normas de actuar a la temática.
- ✔ Video corto y adecuado de acuerdo al año de nivel secundaria basado al plan de clases
- ✔ Actividades áulicas para dichos estudiantes

- ✔ Actividades parentales.
- ✔ Detallar en el mismo Recursos, metodología, contenidos, bibliografía, temporización.