

PROYECTO DE CAPACITACIÓN

“Ciberseguridad aplicada a instituciones educativas de ETP”

Familia Profesional/Sector: Todas las familias profesionales

Nivel: Todos los niveles y ámbitos de la Educación Técnico Profesional

Opción pedagógica: Virtual

Síntesis

Este curso propone brindar a docentes e instructores de la Educación Técnico Profesional herramientas conceptuales y prácticas para reconocer riesgos digitales, prevenir incidentes y fortalecer la protección de la información, las cuentas, los dispositivos y los entornos tecnológicos de las instituciones educativas. La propuesta aborda la ciberseguridad desde una perspectiva educativa e institucional, considerando situaciones habituales como el phishing, la ingeniería social, el uso inseguro de contraseñas, el acceso no autorizado a cuentas, la pérdida de información, el malware, el ransomware y la exposición de datos personales.

A través de actividades prácticas, análisis de casos, recursos multimedia y situaciones simuladas, los participantes desarrollarán criterios para adoptar hábitos de seguridad digital, orientar a estudiantes y colegas y elaborar medidas básicas de prevención y respuesta aplicables a escuelas técnicas, centros de formación profesional e institutos de ETP.

Destinatarios

Docentes, instructores, equipos directivos, referentes tecnológicos, preceptores y otros agentes de instituciones de Educación Técnico Profesional interesados en fortalecer la seguridad digital institucional.

Carga horaria

40 horas reloj - 60 horas cátedra

Fundamentación

La creciente incorporación de plataformas educativas, servicios en la nube, sistemas de gestión, redes inalámbricas, dispositivos móviles, laboratorios informáticos y equipamiento conectado amplía las posibilidades de enseñanza, gestión y comunicación de las instituciones de ETP. Al mismo tiempo, incrementa la exposición a riesgos vinculados con el robo de credenciales, la



suplantación de identidad, el software malicioso, la pérdida de datos, el acceso indebido a información y otras formas de fraude digital.

En las instituciones educativas, la ciberseguridad no depende únicamente de soluciones técnicas. Una parte significativa de los incidentes puede originarse en decisiones cotidianas: reutilizar contraseñas, abrir archivos o enlaces sin verificar su procedencia, compartir credenciales, utilizar equipos sin actualizar, conectar dispositivos externos desconocidos o almacenar información sensible sin medidas adecuadas de protección. Por ello, resulta necesario desarrollar una cultura institucional de seguridad basada en la prevención, la responsabilidad compartida y la capacidad de reconocer situaciones de riesgo.

En la ETP esta necesidad adquiere particular relevancia por la presencia de laboratorios, talleres, redes, equipos informáticos y dispositivos tecnológicos utilizados con fines pedagógicos y técnico-profesionales. La formación docente en ciberseguridad permite no solo proteger recursos e información institucional, sino también incorporar prácticas responsables que puedan ser transferidas a los estudiantes y a sus futuros ámbitos laborales.

El curso propone un enfoque introductorio y aplicado. No busca formar especialistas en seguridad informática, sino ofrecer criterios, procedimientos y herramientas accesibles para prevenir incidentes frecuentes, proteger cuentas y dispositivos, realizar copias de seguridad, identificar intentos de engaño y actuar ordenadamente ante un posible incidente. De este modo, la ciberseguridad se integra como una dimensión de la ciudadanía digital, la gestión institucional y la formación profesional responsable.

Conocimientos previos requeridos

No se requieren conocimientos técnicos especializados. Se recomienda manejo básico de computadora, navegación web, correo electrónico y plataformas digitales.

Objetivos

Objetivo general

Brindar a los participantes herramientas conceptuales y prácticas para reconocer riesgos de ciberseguridad, adoptar medidas preventivas y promover prácticas seguras en el uso de cuentas, datos, dispositivos, redes y servicios digitales de las instituciones de Educación Técnico Profesional.

Objetivos específicos

- Comprender los conceptos básicos de ciberseguridad y su importancia en las instituciones educativas de ETP.



**Ministerio de
Capital Humano**
República Argentina

**Secretaría
de Educación**

inet

Instituto Nacional de
Educación Tecnológica

- Identificar amenazas frecuentes, especialmente phishing, ingeniería social, malware, ransomware y suplantación de identidad.
- Aplicar buenas prácticas para la creación y administración de contraseñas y el uso de autenticación multifactor.
- Reconocer medidas básicas para proteger dispositivos, redes, archivos, datos personales y cuentas institucionales.
- Incorporar estrategias de copia de seguridad, actualización y recuperación de información.
- Desarrollar criterios básicos de actuación y comunicación ante incidentes de seguridad.
- Promover una cultura institucional de prevención y uso responsable de los recursos digitales.

Contenidos

Unidad 1. Ciberseguridad en las instituciones educativas

Objetivo. Comprender los principios básicos de la ciberseguridad y reconocer los principales activos digitales y riesgos presentes en una institución de ETP.

Temas. Ciberseguridad: conceptos fundamentales. Confidencialidad, integridad y disponibilidad de la información. Activos digitales institucionales. Amenazas, vulnerabilidades y riesgos. Datos personales y datos institucionales. Responsabilidades de los usuarios. Cultura de seguridad y prevención en contextos educativos.

Actividad de la unidad. Cuestionario diagnóstico y análisis guiado de situaciones de riesgo presentes en una institución educativa.

Unidad 2. Ingeniería social, phishing y fraudes digitales

Objetivo. Reconocer técnicas de manipulación y engaño utilizadas para obtener información, credenciales o acceso a sistemas, desarrollando criterios para detectar comunicaciones sospechosas.

Temas. Ingeniería social. Phishing, smishing y otras formas de engaño. Suplantación de identidad. Señales de alerta en correos, mensajes, códigos QR, archivos adjuntos y enlaces. Verificación de remitentes y direcciones web. Fraudes mediante cuentas comprometidas. Buenas prácticas de comunicación y reporte.

Actividad de la unidad. Análisis de casos simulados de phishing e ingeniería social. Identificación de señales de alerta y propuesta de acciones seguras.

Unidad 3. Protección de cuentas, dispositivos, redes y datos

Objetivo. Aplicar medidas básicas para reducir el riesgo de accesos no autorizados, pérdida de información e infección de dispositivos.



Temas. Contraseñas robustas y frases de contraseña. Gestores de contraseñas. Autenticación multifactor (MFA/2FA) y códigos de un solo uso (OTP). Actualizaciones y parches. Malware y ransomware. Antivirus y protección integrada. Permisos de usuario. Redes Wi-Fi y conexiones seguras. Uso de pendrives y dispositivos externos. Copias de seguridad: principios básicos y regla 3-2-1. Protección de datos personales y almacenamiento seguro.

Actividad de la unidad. Revisión de una lista de buenas prácticas y elaboración de recomendaciones para proteger una cuenta, un equipo y la información institucional.

Unidad 4. Prevención y respuesta institucional ante incidentes

Objetivo. Desarrollar criterios básicos para prevenir, registrar, comunicar y responder ante incidentes de ciberseguridad en una institución educativa.

Temas. Qué es un incidente de seguridad. Indicadores de compromiso. Primeras acciones ante una cuenta comprometida, malware, ransomware, pérdida o robo de un dispositivo y filtración de información. Qué hacer y qué evitar. Preservación básica de evidencias. Canales internos de comunicación. Roles y responsabilidades. Inventario básico de activos. Políticas y protocolos institucionales. Concientización de docentes y estudiantes.

Actividad de la unidad. Resolución colaborativa de un caso de incidente y elaboración de una secuencia de actuación institucional.

Unidad 5. Trabajo final

Objetivo. Integrar los contenidos del curso mediante la elaboración de una propuesta concreta de mejora de la ciberseguridad aplicable a una institución de ETP.

Temas. Diagnóstico básico de riesgos. Priorización de problemas. Medidas preventivas. Concientización. Procedimientos de actuación. Diseño de recomendaciones contextualizadas para la comunidad educativa.

Actividad de la unidad. Elaboración de un “Plan básico de ciberseguridad para una institución de ETP”.

Trabajo final

El trabajo final consistirá en la elaboración de un “Plan básico de ciberseguridad para una institución de ETP”, presentado en un documento de texto (Word o PDF). La propuesta deberá recuperar los contenidos trabajados y adecuarlos a una institución educativa real o hipotética.

El documento deberá contener los siguientes apartados:

1. Caracterización breve de la institución y de sus principales recursos digitales.
2. Identificación de al menos cinco riesgos o situaciones problemáticas vinculadas con la ciberseguridad.



3. Priorización de los riesgos según su posible impacto y probabilidad.
4. Propuesta de medidas preventivas para cuentas, dispositivos, redes, datos y copias de seguridad.
5. Procedimiento básico de actuación ante un incidente seleccionado.
6. Propuesta breve de concientización destinada a docentes, estudiantes u otros integrantes de la comunidad educativa.
7. Reflexión final sobre la importancia de construir una cultura institucional de ciberseguridad.

Cronograma de la capacitación (de cursada, actividades y evaluaciones)

Módulo	Título	Tema / Actividad	Tipo de contenido	Modalidad	Clase
1	Ciberseguridad en las instituciones educativas	Conceptos básicos, activos, amenazas, vulnerabilidades y riesgos. Cuestionario diagnóstico y análisis de situaciones.	Teórico / práctico	Virtual	1
2	Ingeniería social, phishing y fraudes digitales	Phishing, suplantación, enlaces, adjuntos y QR. Análisis de casos simulados.	Teórico / práctico	Virtual	2
3	Protección de cuentas, dispositivos, redes y datos	Contraseñas, MFA/2FA, malware, actualizaciones, Wi-Fi, datos y copias de seguridad. Actividad de buenas prácticas.	Teórico / práctico	Virtual	3
4	Prevención y respuesta ante incidentes	Primeras acciones, comunicación, roles y protocolo básico. Resolución de caso.	Teórico / práctico	Virtual	4
Trabajo final	Evaluación final	Elaboración de un Plan básico de ciberseguridad para una institución de ETP.	Teórico / práctico	Virtual	5

Plataforma de dictado

La propuesta se desarrollará mediante el campus virtual del CENET. La tutoría acompañará el proceso de aprendizaje a través de los recursos de comunicación disponibles en la plataforma. Se habilitarán foros para consultas, intercambio de experiencias y socialización de producciones.

Los materiales de estudio, recursos audiovisuales, actividades, cuestionarios y consignas estarán disponibles en el aula virtual. Las entregas y devoluciones se gestionarán mediante la misma plataforma, junto con el registro de las calificaciones obtenidas.



Bibliografía

Agencia de Acceso a la Información Pública. (2024, 26 de enero). Recomendaciones de la AAIP para proteger datos personales en Internet. Argentina.gob.ar.
<https://www.argentina.gob.ar/node/414527>

UNESCO. (2023). Informe de seguimiento de la educación en el mundo 2023: Tecnología en la educación: ¿Una herramienta en los términos de quién? Informe GEM 2023 en español
Agencia de Acceso a la Información Pública. (s. f.). Protección de datos personales. <https://www.argentina.gob.ar/aaip/datospersonales>

Argentina.gob.ar. (s. f.). Seguridad en internet: guía para familias y docentes.
<https://www.argentina.gob.ar/node/216925>

Educ.ar. (s. f.). Ciudadanía digital: seguridad y uso responsable de internet.
<https://www.educ.ar/>

Instituto Nacional de Ciberseguridad de España. (s. f.). Recursos para educadores.
<https://www.incibe.es/menores/educadores>

Oficina de Seguridad del Internauta. (s. f.). Copias de seguridad. Instituto Nacional de Ciberseguridad de España. <https://www.osi.es/>

Evaluación

Para acreditar el curso de capacitación, los participantes deberán cumplir con las actividades propuestas en el aula virtual y aprobar el trabajo final.

Diagnóstica: se realizará una valoración inicial de los saberes y prácticas de seguridad digital mediante una encuesta o cuestionario de inicio.

Formativa: durante el desarrollo del curso se considerará la participación en las actividades, el análisis de casos y la aplicación progresiva de medidas de prevención. Al finalizar cada unidad, los participantes deberán completar la actividad propuesta.

Final: se realizará mediante la elaboración de un Plan básico de ciberseguridad para una institución de ETP, en el que se integren el diagnóstico de riesgos, las medidas preventivas, un procedimiento de respuesta y una propuesta de concientización.

Criterios de evaluación

Criterios de evaluación
Identifica de manera pertinente los principales riesgos y vulnerabilidades presentes en el contexto institucional seleccionado.
Propone medidas preventivas claras, viables y coherentes para proteger cuentas, dispositivos, redes, datos e información institucional.



El procedimiento de respuesta ante incidentes presenta una secuencia ordenada de acciones y distingue adecuadamente qué hacer y qué evitar.
La propuesta de concientización se adecua a los destinatarios y promueve prácticas concretas de seguridad digital.
El trabajo final integra los contenidos del curso, utiliza vocabulario específico y presenta una propuesta contextualizada y aplicable a la ETP.
La participación en el aula virtual evidencia reflexión, intercambio y apropiación progresiva de los contenidos.

Capacitador

Gabriel Maximiliano Roca

Gabrielmaximilianoroca24@gmail.com

Licenciado en Tecnología Educativa. Analista de Sistemas de Computación y Analista Programador. Profesor de Educación Secundaria en Informática y Profesor de Tecnología. Especialista en Educación y TIC.

Cuenta con amplia trayectoria docente y de gestión en Educación Técnico Profesional, particularmente en el campo de la informática y las tecnologías digitales. Se ha desempeñado como Administrador de Redes, profesor de Computación y Programación, Sistemas Digitales, Bases de Datos, Ingeniería de Software y Seguridad Informática, así como en diferentes funciones de conducción dentro de instituciones de ETP.

Posee formación específica vinculada con seguridad y ciudadanía digital, ciberseguridad para docentes, tecnologías de la información, redes y entornos digitales. Su trayectoria combina conocimientos técnicos con formación pedagógica y experiencia en la incorporación de tecnologías a los procesos educativos.

Desde 2021 se desempeña como disertante en capacitaciones docentes y desde 2023 ejerce funciones de Vicerrector en la Escuela Técnica Carmen Molina de Llano, articulando su experiencia en gestión educativa, Educación Técnico Profesional y tecnologías digitales.



**Ministerio de
Capital Humano**
República Argentina

**Secretaría
de Educación**

inet

Instituto Nacional de
Educación Tecnológica