Curso de Seguridad de la Información
“Seguro te Conectás”

Este curso fue creado con el objetivo de desarrollar y fortalecer las capacidades profesionales y personales de los participantes y generar un espacio para disfrutar del encuentro entre colegas de diferentes instituciones educativas del país. Aportando herramientas que promuevan un uso seguro y responsable de las Tecnologías de la Información y la Comunicación (TIC) desde múltiples dispositivos y con diversos fines, en el curso se trabajará en torno a los aspectos más relevantes en materia de Seguridad de la Información extraídos de la campaña Seguro te Conectás.

El curso es producto del trabajo conjunto entre Agesic y MEC, partiendo del objetivo de formar a docentes y educadores en la temática y generar referentes que puedan trabajar los contenidos en los centros educativos y demás espacios de intercambio.

Objetivos del curso

- Identificar situaciones de riesgo para la Seguridad de la Información.
- Promover prácticas para un uso responsable de las TIC.
- Diseñar y desarrollar propuestas educativas orientadas al uso seguro de Internet.

Fundamentación

El curso se estructura en los siguientes módulos:

Módulo 0 – Presentación del curso
- Información y bienvenida.
- Guía de diseño del proyecto.

Módulo 1- Introducción a la Ciudadanía Digital
- ¿De qué hablamos cuando hablamos de Ciudadanía Digital?
- Tres usos de los que podemos pensar la construcción de Ciudadanía Digital
- Sensibilizar en el Uso Seguro y Responsable

Módulo 2- El valor de la información
- Sensibilizar acerca del valor que tiene la información y cómo protegerla.
- Destacar la importancia de clasificar la información y tratarla adecuadamente.
- Promover el cuidado y la protección de la privacidad de la información.

Módulo 3 - Gestión de la Seguridad de la Información
- Identificar formas de cuidar y proteger la información.

- Conocer acciones para gestionar la Seguridad de la Información propia y ajena en distintos dispositivos.

Módulo 4 - Navegación segura
- Reflexionar sobre los riesgos de seguridad que pueden presentarse en el uso de Internet.
- Explorar herramientas para prevenir riesgos y navegar en Internet de forma responsable.
- Identificar medidas de seguridad para la protección de los datos personales en el manejo de dinero y valores.
- Conocer formas de identificar y prevenir el phishing.

Módulo 5 - Redes Sociales
- Comprender qué es una red social y cuáles son las más usadas en Uruguay.
- Reconocer riesgos que se presentan en el manejo de las Redes Sociales y explorar recursos sobre su uso responsable para trabajar con los estudiantes.

Diseño del proyecto
- Diseñar un proyecto de intervención que presente una forma de abordaje de las temáticas del curso en un centro educativo o para una población determinada.
- El trabajo consistirá en la entrega del proyecto (diseño). Se evaluará su pertinencia y viabilidad en el contexto en que se piense la propuesta.

Metodología

Los cinco módulos del curso de desarrollarán en forma virtual, con 3 instancias sincrónicas (virtuales) obligatorias en el correr del curso.

Los dos primeros módulos (0 y 1) se habilitarán de manera conjunta durante la primera semana; los siguientes se irán activando de a uno por semana (ver cronograma).

Cada módulo posee pautas obligatorias que deben ser realizadas en las fechas establecidas (semana del módulo). El curso se aprobará cumpliendo con las actividades propuestas en los módulos y con la entrega del diseño del proyecto.

En los módulos habrá foros de intercambio para construir el aprendizaje colectivo entre pares. De acuerdo a los aportes de los participantes, se pretende potenciar la reflexión sobre las prácticas educativas, la integración de los recursos digitales y sus impactos en la resignificación de los roles del educador y del estudiante. Si bien las tareas se proponen a nivel individual, el trabajo en equipo, colaborativo, es considerado un valor a desarrollar de acuerdo a las posibilidades de los participantes, constituyendo una oportunidad de crecimiento profesional y personal.

Módulos	Fecha	Pautas obligatorias	Puntaje
0 y 1 (10 puntos)	Miércoles 16/9/2020	Diseña y comparte un folleto sobre "¿Cómo proteger la información?".	5
		Foro: comparte una noticia vinculada a seguridad de la información.	3
		Autoevaluación del módulo.	2
2 (15 puntos)	Miércoles 30/09/2020	Diseña y comparte una propuesta didáctica que tenga como objetivo identificar vulnerabilidades de la seguridad de la información entre estudiantes.	5
		Foro: comparte alguna inquietud de los estudiantes vinculada a la ciberseguridad.	3
		Autoevaluación del módulo.	2
	Miércoles 30/09/2020 (18h)	Instancia sincrónica (videoconferencia) // ***Charla Técnica "Pishing"***	5
3 (10 puntos)	Miércoles 7/09/2020	Diseña y comparte una pequeña guía para identificar y prevenir riesgos mientras navegamos en internet.	5
		Foro: comparte un ejemplo de phishing que te haya llegado o que encuentres en las redes.	3
		Autoevaluación del módulo.	2
		Diseña y comparte una propuesta didáctica para minimizar los riesgos cuando compartimos fotografías o videos en redes sociales.	5

4 **(15 puntos)**	Miércoles 14/10/2020	Foro: compartir un riesgo que identifiques por el uso no responsable de redes sociales. Si conoces alguna experiencia, puedes compartirla.	3
		Autoevaluación del módulo.	2
	Miércoles **14/10/2020** **(18h)**	Instancia sincrónica (videoconferencia) ***Charla Técnica "Contraseñas Seguras + Las cosas por su nombre"***	5
Taller **(5 puntos)**	**Martes** **20/10/2020** **17 a 20 hrs**	Taller sobre Uso Seguro y Responsable	5
Cierre **(45 puntos)**	Domingo 25/10/2020	Entrega del diseño del proyecto.	45

Criterios de evaluación y aprobación

Diseños intermedios (5 puntos)

- Cada semana deberás entregar un diseño o pauta de trabajo referente al tema que estemos abordando, la misma te ayudará a avanzar en el diseño final del curso.

Foros (3 puntos)

- Cada semana deberás participar en los foros con la consigna propuesta.

Autoevaluaciones (2 puntos)

- Se permiten 3 intentos
- Se tomará la mejor nota obtenida
- Se aprueba con 70% del puntaje

Trabajo final (45 puntos)

Los criterios de evaluación para el proyecto serán:

- Objetivo presentado (qué problemáticas se abordan y porque)
- Público objetivo (a quién está dirigido, perfilamiento)
- Recursos a utilizar (folletos, aulas, presentaciones, personas, PC, etc.)
- Metodología de abordaje (talleres, charlas, intervenciones, etc.)
- Claridad de la propuesta
- Innovación / impacto social
- Indicadores para el cumplimiento del objetivo

Instancias sincrónicas o videoconferencias (5 puntos)

- En la semana 3 y 7; existirán instancias de reunión virtual para puesta en común e intercambio sobre los temas tratados hasta la fecha de cada instancia.
- La actividad de la semana 7 es en modalidad taller.

Talleres optativos (voluntarios): Se brindará la posibilidad de participar de 2 talleres virtuales más a los estudiantes; para cerrar con los usos para la construcción de la Ciudadanía Digital. Estos talleres son de manera voluntaria y no llevan puntos adicionales en este curso; motivamos a los estudiantes a completar el ciclo de los mismos y tener el marco general de las habilidades a desarrollar para la Ciudadanía Digital.
Los mismos se brindarán el Martes 27 de octubre (Taller de Uso Crítico y Reflexivo) y Martes 3 de noviembre (Taller de Uso Creativo y Participativo); de 17 a 20 horas.

Cantidad de horas del curso: Estimado de 30 horas (dedicación por módulos + diseño del proyecto)