0. Nombre de la experiencia educativa

Introducción a la Ciberseguridad

1. Modalidad

Curso taller en línea

2. Valores de la experiencia educativa

2.1 Horas de teoría	2.2 Horas de práctica	2.3 Total de horas	2.4 Valor en créditos
15	30	45	4

(15 horas teoría: 2 créditos) (15 horas prácticas: 1 crédito)

3. Fecha

3.1 Elaboración	3.2 Modificación
20 de julio 2020	

4. Nombre de los académicos que participaron en la elaboración y/o modificación.

Zenaida Ávila Águila, Josefina Conejo Vega, Patricia del Carmen San Martín Sicré, Marbella Crystal Velasco Hernández, María Karin Rosenkran Sáenz, Miguel Ángel Barradas Gerón, Gerardo Contreras Vega, Urbano Francisco Ortega.

5. Descripción

La experiencia educativa “Introducción a la Ciberseguridad” se concibe como un Curso-taller orientado al desarrollo de competencias en ciberseguridad en el uso diario de computadoras y teléfonos celulares. Forma parte del Programa de Formación de Académicos (ProFA) y tiene una duración de 45 horas, distribuidas en 30 horas presenciales y 15 extra clase, con un valor de 4 créditos. Algunos saberes que desarrollará son identificación de amenazas en el uso de la computadora personal, el uso del celular y en la navegación web que le permitan minimizar los ataques y riesgos al usar estos dispositivos. La metodología de trabajo es el aprendizaje basado en problemas (ABP), los alumnos a través de problemas conocen la forma en que los cibercriminales se aprovechan de la confianza de los usuarios para intentar engañarlos y así acceder a información confidencial.

6. Justificación

Actualmente, la seguridad de la información, protección y recuperación de los datos de una empresa, organización y personas han tomado importancia fundamental en las actividades que se realizan día con día, sobre todo por la alta demanda de servicios en línea y por el incremento en delincuentes que utilizan la computadora e Internet para cometer actos ilícitos; por lo que es necesario conocer acerca de la forma en que actúan estas personas y así desarrollar mecanismos de prevención, protección y recuperación de datos e información a las empresas, organizaciones y personas que lo requieran.

7. Unidad de competencia

El participante conceptualiza elementos utilizados por cibercriminales para acceder, obtener, eliminar su información, a partir de la observación y comparación de

elementos claves utilizados en la navegación en Internet a través de una computadora o teléfono celular, en un clima de respeto, honestidad, discreción, curiosidad intelectual, tolerancia, creatividad y responsabilidad.

8. Articulación de los ejes

A través de la conceptualización de elementos de seguridad de la información y de los elementos utilizados por cibercriminales (teórico), el participante identifica, usa y prueba herramientas de software que le permiten reducir riesgos de seguridad cuando utiliza un dispositivo de cómputo y navega en Internet (Heurístico), a través del trabajo con responsabilidad, honestidad, discreción, tolerancia, respeto y curiosidad (Axiológico).

9. Saberes

9.1 Teóricos	9.2 Heurísticos	9.3 Axiológicos
• Fundamentos de cyberseguridad ◦ Importancia de la seguridad de la información ◦ Conceptos ◦ Principales amenazas • Mentalidad y Hábitos en la red ◦ Hábitos de la seguridad de la información ◦ Funcionamiento de Internet ◦ La importancia de las actualizaciones de software ◦ Respaldos ◦ Borrado y baja de equipo de cómputo. • Autenticación ◦ Tipos de autenticación ◦ Autenticación de un factor ◦ Autenticación multifactor ◦ Ejemplos de autenticación • Cifrado ◦ Conceptos ◦ Tipos de cifrado ◦ Cifrado simétrico ◦ Cifrado asimétrico	• Identificación de hábitos de navegación en Internet • Utilización de software para autenticación de un factor. • Utilización de software para autenticación multifactor. • Cifrado simétrico de archivos. • Cifrado asimétrico de archivos. • Firma digital de documentos. • Verificación de la integridad de archivos. • Comprobación de la fortaleza criptográfica de una contraseña. • Comprobación del riesgos de utilizar programas que no cifran información. • Uso de herramientas para disminuir amenazas en la computadora. • Uso de herramientas para disminuir amenazas en el celular. • Uso de herramientas para disminuir amenazas en la	Responsabilidad en la entrega de evidencias. Honestidad y discreción en el manejo de información confidencial. Creatividad para la identificación de engaños. Tolerancia a la diversidad de opiniones. Disposición para trabajo en equipo. Respeto por el trabajo de los demás. Curiosidad para entender el funcionamiento de los sistemas de cómputo.

◦ Cifrado híbrido ◦ Integridad de archivos ◦ Firmas digitales ◦ Blockchian ◦ Redes privadas virtuales ◦ SSL • Privacidad ◦ Derechos ARCO ◦ Ley de protección de datos personales en posesión de particulares ◦ Leyes de transparencia y acceso a la información federal y estatal • Seguridad del sistema operativo ◦ Principales amenazas ◦ Medidas de protección y mitigación de riesgos • Seguridad web ◦ Identificación de riesgos, amenazas y vulnerabilidades ◦ Medidas de protección • Seguridad móvil ◦ Permisos y aplicaciones ◦ Riesgos • Medidas de protección	navegación web. • Identificación de vulnerabilidades, amenazas y engaños en la red.	

10. Estrategias metodológicas

10.1 De aprendizaje:	**10.2 De enseñanza:**
- Lecturas de material relacionado con seguridad de la información. - Participación en foros de discusión sobre ataques, engaños y medidas de protección. - Resolución de problemas relacionados con seguridad.	- Presentación de casos prácticos sobre amenazas en el uso de la computadora, celular y navegación web. - Exposiciones teóricas por parte del maestro. - Presentaciones de retos para identificación de vulnerabilidades y malas prácticas.

11. Apoyos educativos

11.1 Recursos	11.2 Materiales
• Plataforma de aprendizaje EMINUS • Clases sincronas con la herramienta que EMINUS proporciona o alguna otra como TEAMS. • Acceso a Internet • Software: o Sistema operativo Windows, GNU/Linux o MacOS o Programas antivirus, antimalware o Navegador web o Sistema operativo Android o IOS o Software de seguridad o Para virtualizar sistemas operativos	• Leyes y manuales en disponibles en línea. • Manuales de uso de los programas a utilizar. • Libros de seguridad en cómputo. • Material del curso en la plataforma EMINUS.

12. Evaluación del desempeño

12.1 Evidencia(s) de desempeño	12.2 Criterios de desempeño	12.3 Ámbito(s) de aplicación	12.4 Porcentaje
Actividades en foro	Concretas, claras, precisas, sin faltas de ortografía.	Plataforma virtual	**20 %**
Reportes de problemas y prácticas	Completas, claras, sin faltas de ortografía y en tiempo	Plataforma virtual	**40 %**
Reporte de actividad integradora	Completas, claras, sin faltas de ortografía y en tiempo	Plataforma virtual	**40 %**
			100 %

13. Acreditación

Para acreditar esta EE el participante deberá haber presentado con suficiencia cada evidencia de desempeño, es decir, que en cada una de ellas haya obtenido cuando menos el 70 %.

14. Fuentes de información

14.1 Básicas

ISO/IEC. (2018). *ISO/IEC Information technology—Security techniques—Information security management systems—Overview and vocabulary*. ISO/IEC. https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip

Diccionario de Protección de Datos Personales Conceptos Fundamentales – Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) Primera Edición, Noviembre 2019

Ley Federal de Protección de Datos personales en posesión de los Particulares - http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Ley Estatal de Protección de Datos Personales en Posesión de Sujetos obligados para el Estado de Veracruz - http://ivai.org.mx/DatosPersonales/Archivos/Normatividad/gaceta298_LEY_DE_DATOS_PERS

ONALES.pdf

Llamas Covarrubias I. N. y Llamas Covarrubias J. Z. (2018). Internet, ¿Arma o Herramientas? Recuperado de http://www.publicaciones.cucsh.udg.mx/kiosko/2018/internet_arma_o_herramienta_Ebook.pdf

Retzkin, S. (2018). Hands-On DarkWeb Analysis. Estados Unidos de América. Editorial: Packt Publishing Limited

Khawaja, Gus (2018). Practical web Penetration Testing. Estados Unidos de América. Editorial: Packt Publishing Limited

14.2 Complementarias

GPG for Win Download. Recuperado de https://gpg4win.org/download.html Visitada mayo 2020.

The offical Social Engineering Portal – Security Trhough Education. Recuperado de https://www.social-engineer.org/ Visitada mayo 2020.

Anón. 2012. “iOS vs Android. La batalla por la seguridad y la privacidad”. *Sozpic*. Recuperado el 21 de mayo de 2020 (https://www.sozpic.com/seguridad-y-privacidad-ios-vs-android/).

Anón. s/f. “Guía de seguridad en redes sociales”. 10. Disponible en https://www.is4k.es/sites/default/files/contenidos/materiales/Campanas/is4k-guia-rrss.pdf