PROCESO DE GESTIÓN DE FORMACIÓN PROFESIONAL INTEGRAL

FORMATO GUÍA DE APRENDIZAJE

IDENTIFICACIÓN DE LA GUIA DE APRENDIZAJE

- Denominación del Programa de Formación: Desarrollo de habilidades digitales para experiencias seguras en linea
- Código del Programa de Formación: 23310013
- Competencia: Implementar el sistema de seguridad de la información según modelo y estándares técnicos
- Resultados de Aprendizaje Alcanzar:
    - Realizar un uso adecuado y responsable de los recursos tecnológicos para garantizar la integridad de la persona
    - Aplicar las estrategias de ciberseguridad conforme a los recursos y servicios digitales utilizados
    - Preparar las estrategias de ciberseguridad de acuerdo a los recursos informáticos utilizados
- Duración de la Guía: 48 hrs

2. PRESENTACIÓN

¡Bienvenidos al curso de Desarrollo de Habilidades Digitales para Experiencias Seguras en Línea! En este emocionante programa, nos sumergiremos en el fascinante mundo de las habilidades digitales esenciales para navegar de manera segura y efectiva en el ciberespacio. En un entorno donde la tecnología evoluciona rápidamente, es crucial adquirir destrezas que no solo nos permitan aprovechar al máximo las oportunidades en línea, sino también resguardarnos de posibles amenazas. Este curso ha sido diseñado para dotar a los participantes con las herramientas prácticas y conocimientos necesarios para navegar con confianza, protegiendo su información personal y manteniendo experiencias en línea seguras.

A lo largo de este viaje educativo, exploraremos temas como la gestión de contraseñas, la conciencia de la privacidad, la detección de fraudes en línea y las mejores prácticas para evitar ciberataques. Además, abordaremos la importancia de la ética digital y cómo construir una presencia en línea positiva. Nuestro enfoque práctico incluirá ejercicios interactivos, estudios de casos y discusiones grupales para asegurar una

comprensión profunda y la aplicación práctica de las habilidades adquiridas. Al finalizar el curso, no solo estarán equipados con habilidades digitales avanzadas, sino que también se convertirán en defensores activos de la seguridad en línea, contribuyendo a un entorno digital más seguro y colaborativo.

Así que, ¡prepárense para sumergirse en el mundo digital con confianza y seguridad! Este curso será un viaje emocionante hacia el fortalecimiento de sus habilidades digitales y la construcción de una presencia en línea sólida y segura. ¡Bienvenidos a la era digital segura del siglo XXI! *(Máximo 10 renglones)*

3. FORMULACIÓN DE LAS ACTIVIDADES DE APRENDIZAJE

Los aprendices pueden realizar un ejercicio práctico de evaluación de contraseñas, donde aprendan a crear y fortalecer contraseñas seguras. Esto incluiría el uso de herramientas y estrategias para generar contraseñas robustas y la comprensión de la importancia de la diversidad de caracteres.
Exploración de Herramientas Antivirus:

Los aprendices pueden iniciar una exploración y comparación de diversas herramientas antivirus disponibles. Los participantes pueden instalar y probar versiones de prueba gratuitas, evaluando su facilidad de uso, capacidad de detección y características de protección. Esto proporcionará una comprensión práctica de las herramientas disponibles para proteger dispositivos digitales.

4. ACTIVIDADES DE EVALUACIÓN

Tome como referencia la técnica e instrumentos de evaluación citados en la guía de Desarrollo Curricular

Evidencias de Aprendizaje	Criterios de Evaluación	Técnicas e Instrumentos de Evaluación
Evidencias de Conocimiento: MOD01 Actividad Didactica	La actividad planteada consiste en organizar dos columnas, en una se deben poner los términos y en otra columna aparte las definiciones, el objetivo es que el aprendiz haga la unión entre término y definición, de esta manera podrá hacer un repaso general	**Lista de chequeo**

	del desarrollo de este primer componente formativo.	
MOD02 Actividad Didactica	Afianzar algunos de los conceptos más importantes de la ciberseguridad y las redes sociales.	
MOD03 Actividad Didactica **Evidencias de Desempeño:** **Evidencias de Producto:**	Apropiar conocimientos de los riesgos y amenazas a los cuales se exponen los usuarios digitales al hacer uso de las nuevas herramientas tecnológicas.	

5. GLOSARIO DE TÉRMINOS

Contraseña Segura: Secuencia de caracteres que protege el acceso a cuentas en línea.

Autenticación de Dos Factores (A2F): Método que añade una capa extra de seguridad, generalmente un código temporal, para verificar la identidad del usuario.

Privacidad Digital: Protección y control de la información personal en línea para evitar su uso no autorizado.

Phishing: Técnica engañosa que busca obtener información confidencial, como contraseñas, haciéndose pasar por entidades confiables.

Firewall: Barrera de seguridad que controla el tráfico de red para prevenir accesos no autorizados y proteger contra amenazas en línea.

Ciberseguridad: Prácticas y medidas para proteger sistemas, redes y datos contra ataques cibernéticos.

Malware: Software malicioso diseñado para dañar o infiltrarse en sistemas informáticos sin el consentimiento del usuario.

Red Virtual Privada (VPN): Herramienta que crea un túnel cifrado para asegurar la conexión a internet, protegiendo la privacidad y la seguridad en línea.

Actualización de Software: Proceso de instalar las últimas versiones de programas para corregir vulnerabilidades y mejorar la seguridad.

Etiqueta Digital: Comportamiento ético en línea que refleja una presencia digital positiva y respetuosa en redes sociales y plataformas en línea.

Rastreo de Cookies: Recopilación de información del usuario mediante cookies, pequeños archivos de texto, con el fin de personalizar la experiencia en línea, aunque plantea preocupaciones de privacidad.

Sextorsión: Amenaza que involucra el chantaje a través de la publicación de material sexualmente explícito, a menudo obtenido ilegalmente.

Backup en la Nube: Almacenamiento de copias de seguridad de datos en servidores remotos, garantizando la recuperación de información en caso de pérdida o daño.

Educación en Ciberseguridad: Formación para aumentar la conciencia sobre amenazas cibernéticas y promover prácticas seguras en línea.

Filtro de Contenido: Herramienta que bloquea o filtra el acceso a ciertos sitios web o contenido en línea, especialmente útil para padres y educadores.

Huella Digital: Rastro único dejado por la actividad en línea de un individuo, incluyendo publicaciones, comentarios y búsquedas, que puede ser rastreado.

Software Antivirus: Aplicación diseñada para detectar, prevenir y eliminar software malicioso, protegiendo dispositivos contra amenazas en línea.

Criptomoneda: Moneda digital que utiliza la criptografía para garantizar transacciones seguras y controlar la creación de nuevas unidades.

Control Parental: Herramienta que permite a los padres limitar el acceso y supervisar la actividad en línea de sus hijos para garantizar un entorno digital seguro.

Desinformación: Difusión deliberada de información falsa en línea con el objetivo de engañar, confundir o influenciar a la audiencia.

Seguridad de la Cámara Web: Prácticas y herramientas para proteger la privacidad al controlar y limitar el acceso a la cámara web de un dispositivo.

Hacker Ético: Profesional de la seguridad informática que utiliza sus habilidades para identificar y corregir vulnerabilidades, contribuyendo a mejorar la seguridad en línea.

Autenticación Biométrica: Método de seguridad que utiliza características físicas o comportamentales únicas, como huellas dactilares o reconocimiento facial, para verificar la identidad.

Derechos Digitales: Conjunto de derechos relacionados con la privacidad, propiedad y acceso a datos digitales y servicios en línea.

Redes Sociales Seguras: Prácticas para proteger la información personal al utilizar plataformas de redes sociales y ajustar configuraciones de privacidad.

Certificado SSL/TLS: Protocolo de seguridad que asegura la comunicación cifrada entre un navegador web y un servidor, esencial para la protección de datos durante la transmisión.

Seguridad en Transacciones en Línea: Medidas para proteger las transacciones financieras realizadas a través de internet, incluyendo cifrado seguro y autenticación de dos factores.

Navegación Anónima: Práctica de ocultar la identidad y actividad en línea mediante el uso de herramientas como VPNs y navegadores privados.

Ingeniería Social: Tácticas utilizadas para manipular a individuos con el fin de obtener información confidencial, a menudo a través de engaños psicológicos en línea.

Ransomware: Tipo de malware que cifra datos en un dispositivo y exige un rescate para restaurar el acceso, destacando la importancia de la prevención y la seguridad en línea.

6. REFERENTES BILBIOGRÁFICOS

Cano, J. (2011). Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global. Sistemas (Asociación Colombiana de Ingenieros de Sistemas), 119, 4-7.

Cynthus (2020). ¿Qué hay de nuevo en COBIT® 2019? https://www.cynthus.com.mx/que-hay-de-nuevo-en-cobit-2019/

NIST (s.f). Framework for Improving Critical Infrastructure Cybersecurity https://www.businesswire.com/news/home/20180522005533/en/HITRUST%C2%AE-Provides-NIST-Cybersecurity-Framework-Certification

Soriano, M. (2014). Seguridad en redes y seguridad de la información. Obtenido de http://improvet.cvut. https://www.academia.edu/40156122/Seguridad_en_redes_y_seguridad_de_la_informaci%C3%B3n

Avance Jurídico Casa Editorial Ltda. (2021). Leyes desde 1992 - Vigencia expresa y control de constitucionalidad [Ley 1273 de 2009]. Senado de la República de Colombia. http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Bastidas, H. (2021). Gestión de contraseñas. https://www.youtube.com/watch?v=WuO1Fu38yPk

Bastidas, H. (2021). Huella digital. https://www.youtube.com/watch?v=-p5HezBeYQE

Interpol. (s.f). Huellas dactilares. https://www.interpol.int/es/Como-trabajamos/Policia-cientifica/Huellas-dactilares

7. CONTROL DEL DOCUMENTO

	Nombre	**Cargo**	**Dependencia**	**Fecha**
Autor (es)	**Sergio David Muñoz Vela**	**Instructor**	**Centro de Comercio y Servicios**	**29 de Noviembre de 2023**

8. CONTROL DE CAMBIOS (diligenciar únicamente si realiza ajustes a la guía)

	Nombre	**Cargo**	**Dependencia**	**Fecha**	**Razón del Cambio**

Autor (es)					