



PROCESO DE GESTIÓN DE FORMACIÓN PROFESIONAL INTEGRAL

FORMATO GUÍA DE APRENDIZAJE

IDENTIFICACIÓN DE LA GUIA DE APRENDIZAJE

- **Denominación del Programa de Formación:** Control De La Seguridad Digital.
 - **Código del Programa de Formación:** 233103
 - **Nombre del Proyecto:** Asegurar Los Procesos De Seguridad De La Información Tanto Lógicos Y Físicos En Las Instituciones Educativas Y Empresas Del Departamento De Cauca
 - **Fase del Proyecto:** Planeación
 - **Actividad de Proyecto:** Elaborar un plan para la gestión de controles de seguridad digital para monitorizar, controlar y documentar, procesos de seguridad digital según tecnológicas y modelo de seguridad digital de la empresa Competencia
 - **Resultados de Aprendizaje Alcanzar:** 583707 - operar herramientas de control de la seguridad digital para mitigar los riesgos según procedimientos técnicos de la política de seguridad digital.
-
- **Duración de la Guía 96 horas**

2. PRESENTACIÓN

Con la esteganografía no solo es una técnica utilizada para ocultar información, sino también una disciplina que forma parte del vasto mundo de la seguridad informática, la criptografía y las tecnologías emergentes. Aprender sobre esta práctica te permitirá desarrollar habilidades que son esenciales no solo en el ámbito académico, sino también en el entorno profesional y personal.

En esta actividad, descubrirás cómo ocultar mensajes de manera segura, cómo proteger información valiosa y cómo utilizar herramientas digitales para entender y aplicar conceptos de seguridad de una forma práctica y dinámica. Guiar y organizar el aprendizaje de manera que se oriente al desarrollo integral del aprendiz



La esteganografía requiere una reflexión sobre cómo ocultar la información sin comprometer su integridad. Esto te ayudará a desarrollar una mente analítica, capaz de tomar decisiones estratégicas en situaciones que demanden seguridad o privacidad. La capacidad de pensar fuera de lo convencional es esencial al aprender esteganografía. Necesitarás encontrar formas creativas de integrar datos dentro de otros medios sin que sean detectados, lo cual es una habilidad valiosa en muchas disciplinas.

3. FORMULACIÓN DE LAS ACTIVIDADES DE APRENDIZAJE

Descripción de la(s) Actividad(es)

En esta actividad, los aprendices aprenderán a ocultar un mensaje de texto dentro de una imagen utilizando la técnica de esteganografía **LSB (Least Significant Bit)**. El objetivo es que los aprendiz comprendan cómo ocultar información de forma segura en archivos digitales y descubran cómo puede extraerse nuevamente utilizando las herramientas adecuadas.

1. **Paso 1:** Explicación teórica sobre la esteganografía y la técnica LSB. El instructor hablará sobre los fundamentos de la esteganografía y cómo la técnica LSB oculta información en los bits menos significativos de los píxeles de una imagen sin alterar su apariencia visible.
2. **Paso 2: Aplicación práctica:** Los aprendices deberán seleccionar una imagen digital en formato .png o .jpg y un mensaje de texto corto que quieran ocultar (por ejemplo, "Mensaje secreto").
3. **Paso 3:** Usar una herramienta de esteganografía como **OpenStego** o **Steghide** para esconder el mensaje en la imagen seleccionada.
4. **Paso 4:** Compartir la imagen modificada (con el mensaje oculto) con otro compañero para que intente extraer el mensaje utilizando la misma herramienta.
5. **Paso 5:** Discusión sobre cómo esta técnica puede ser utilizada en la vida real para proteger información sensible, así como los riesgos de usarla para fines malintencionados.

Ambiente Requerido



- **Ambiente Virtual o Físico:** Puede realizarse en un laboratorio de computación, en un aula con acceso a equipos de cómputo, o de forma remota utilizando plataformas de aprendizaje en línea.
- **Conexión a Internet:** Para descargar las herramientas de esteganografía necesarias y obtener imágenes para modificar.
- **Computadoras:** Con acceso a software de esteganografía (como **OpenStego** o **Steghide**), y procesadores de texto

Materiales

- Computadora o Laptop con acceso a internet.
- Software de Esteganografía: Ej. OpenStego, Steghide (todos estos son gratuitos).
- Imagen digital: Un archivo de imagen en formato .jpg o .png (puede ser cualquier imagen simple sin derechos de autor).
- Texto secreto: Un mensaje que el estudiante quiera ocultar en la imagen (por ejemplo, "Este es un mensaje oculto").
- Instrucciones para usar las herramientas de esteganografía.
- Plataforma de comunicación (si es una actividad remota): Para que los estudiantes puedan compartir imágenes modificadas y mensajes.

Actividad 2: Detectar Información Oculta en una Imagen

Descripción de la Actividad:

Esta actividad se centra en el **análisis y detección de esteganografía**. Los estudiantes deberán aprender a identificar imágenes que han sido manipuladas para ocultar información mediante herramientas de detección. Se les presentará una imagen con datos ocultos, y deberán emplear software para descubrir el mensaje.

1. **Paso 1:** El instructor explicará cómo se puede realizar la **detección de esteganografía** utilizando herramientas como **StegExpose** o **StegSecret**.
2. **Paso 2:** Los estudiantes recibirán un conjunto de imágenes, algunas de las cuales tienen información oculta mediante esteganografía y otras no.



3. **Paso 3:** Usando las herramientas de detección, los estudiantes deberán analizar las imágenes y determinar cuáles contienen información oculta y, si es posible, extraer el mensaje.
4. **Paso 4:** Los estudiantes deberán documentar sus hallazgos, describiendo el proceso de detección y cómo llegaron a la conclusión de que una imagen contiene un mensaje oculto.
5. **Paso 5:** Reflexión grupal sobre las implicaciones de la esteganografía en la seguridad y privacidad de la información, y cómo las técnicas de detección pueden ser aplicadas en investigaciones forenses digitales.

Ambiente Requerido:

- **Ambiente Virtual o Físico:** Esta actividad se puede realizar en un aula de computación con acceso a internet o en línea, con plataformas que permitan la interacción y el intercambio de resultados.
- **Computadoras:** Equipos con acceso a las herramientas de análisis y detección de esteganografía.
- **Espacio para la reflexión grupal:** Al final de la actividad, se recomienda un espacio para compartir experiencias y conclusiones.

Materiales:

- **Computadora o Laptop** con acceso a internet.
- **Software de Detección de Esteganografía:** Ej. **StegExpose**, **StegSecret**.
- **Imágenes de prueba:** Un conjunto de imágenes que contengan mensajes ocultos, que serán proporcionadas por el instructor.
- **Instrucciones** para usar las herramientas de detección de esteganografía.
- **Preguntas guía para la reflexión:** Para estimular la discusión sobre las implicaciones de la esteganografía en el mundo real.

Actividad 3: Proyecto Final: Crear un Sistema de Esteganografía Personalizado

Descripción de la Actividad:

El objetivo de este proyecto final es que los estudiantes diseñen y creen un sistema de esteganografía personalizado, el cual combine varias técnicas de ocultación de datos en diferentes tipos de archivos (texto, imágenes, audio, etc.).



1. **Paso 1:** Los estudiantes deben investigar y decidir qué tipo de datos desean ocultar y qué tipo de archivo van a usar (puede ser una imagen, un archivo de texto o de audio).
2. **Paso 2:** Crear un prototipo de sistema que permita ocultar la información en el archivo elegido utilizando una combinación de las técnicas de esteganografía aprendidas.
3. **Paso 3:** Después de crear el sistema, los estudiantes deben probarlo con otros compañeros y asegurarse de que los mensajes puedan ser correctamente ocultados y extraídos.
4. **Paso 4:** Presentación del proyecto final, donde los estudiantes explican el proceso que siguieron, las herramientas que usaron y cómo garantizaron que la información estuviera oculta de manera segura.
5. **Paso 5:** Evaluación grupal, donde los compañeros de clase y el instructor evalúan la creatividad, la efectividad y la seguridad del sistema de esteganografía creado.

Ambiente Requerido:

- **Laboratorio de computación o ambiente remoto:** Acceso a equipos con herramientas de desarrollo y software de esteganografía.
- **Acceso a plataformas de comunicación:** Para compartir avances, resolver dudas y presentar el proyecto final.

Materiales:

- **Computadora o Laptop** con acceso a internet.
- **Software de Desarrollo:** Dependiendo del tipo de proyecto (por ejemplo, un entorno de programación si se utiliza código para crear un sistema).
- **Software de Esteganografía:** Ej. **OpenStego**, **Steghide**, **Audacity** (si se trabaja con audio).
- **Instrucciones y guías** para el desarrollo del proyecto.

Resumen de las Actividades:

1. **Actividad 1:** Ocultar un mensaje en una imagen utilizando la técnica LSB.
 - **Ambiente:** Aula de computación o trabajo remoto.



- **Materiales:** Computadoras, software de esteganografía, imágenes digitales, texto.
2. **Actividad 2:** Detectar mensajes ocultos en imágenes.
- **Ambiente:** Aula de computación o trabajo remoto.
 - **Materiales:** Computadoras, software de detección de esteganografía, imágenes con datos ocultos.
3. **Actividad 3:** Crear un sistema de esteganografía personalizado.
- **Ambiente:** Aula de computación o trabajo remoto.
 - **Materiales:** Computadoras, software de esteganografía, herramientas de desarrollo.

Tomando como referencia la planeación pedagógica y las orientaciones para elaborar guías de aprendizaje citado en la guía de desarrollo curricular.

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 : Evidencia 1: Responder correctamente a preguntas teóricas en un examen escrito sobre los conceptos fundamentales de la esteganografía (tipos de esteganografía, historia, aplicaciones, herramientas, etc.) Evidencia 2: Participación activa en una discusión en clase donde se analicen casos reales de uso de esteganografía (por ejemplo, en el contexto de la seguridad	Dominio de los conceptos fundamentales: El estudiante debe conocer las definiciones y características de las técnicas de esteganografía. Comprensión de la aplicación de la esteganografía: El estudiante debe ser capaz de identificar los usos prácticos de la esteganografía en diversos contextos, como la seguridad informática, la protección de datos, etc. Uso adecuado de la terminología técnica: El estudiante debe emplear términos como "ocultación",	Examen escrito con preguntas de opción múltiple, verdadero/falso, y de desarrollo. Rúbricas para evaluar la precisión y profundidad en las respuestas.



informática y la protección de datos).	"mensaje escondido", "herramientas de detección", etc., de manera precisa y correcta.	
<p>Evidencias de Desempeño</p> <p>Evidencia 1: Realizar un análisis de imágenes para detectar esteganografía, utilizando herramientas de detección como Steghide o StegExpose.</p> <p>Evidencia 2: Creación de un proyecto práctico, como un sistema básico de esteganografía que permita ocultar y extraer información en imágenes o audios</p>	<p>Habilidad técnica: El estudiante debe demostrar capacidad para utilizar correctamente herramientas y técnicas de esteganografía para ocultar y extraer información. Resolución de problemas: El estudiante debe ser capaz de resolver problemas prácticos relacionados con la detección y ocultación de mensajes.</p> <p>Rigor en el proceso: El estudiante debe seguir correctamente los pasos y procedimientos para la detección de esteganografía o la creación de sistemas.</p>	<p>Ejercicio práctico de detección de esteganografía en imágenes.</p> <p>Observación directa del desempeño del estudiante mientras utiliza herramientas de esteganografía.</p> <p>Rúbricas de desempeño para evaluar la ejecución práctica.</p>
<p>Evidencias de Producto:</p> <p>Evidencia 1: Presentación de un proyecto final que consiste en un sistema de esteganografía que oculta y extrae mensajes de archivos de imágenes, audios o textos.</p> <p>Evidencia 2: Creación de un informe detallado que explique cómo se desarrolló el sistema de esteganografía, las herramientas utilizadas y la justificación de las decisiones tomadas durante el proceso.</p>	<p>Funcionalidad del producto: El sistema debe funcionar correctamente, permitiendo ocultar y extraer información de manera efectiva.</p> <p>Calidad del producto final: El producto debe ser presentado de forma clara, profesional, y debe ser capaz de cumplir su propósito sin errores.</p> <p>Innovación y creatividad: El proyecto debe mostrar creatividad en el uso de las técnicas de esteganografía y proponer una solución innovadora o interesante.</p>	<p>Informe escrito que describa el proceso y los resultados del proyecto de esteganografía.</p> <p>Presentación del producto final para demostrar la funcionalidad y el uso de la herramienta.</p> <p>Rúbricas de evaluación de producto para evaluar tanto el funcionamiento como la calidad y creatividad del producto.</p>



4. GLOSARIO DE TÉRMINOS

1. Esteganografía

Definición: Técnica de ocultar información dentro de otros archivos o medios de comunicación, de tal manera que su presencia no sea evidente para una persona no informada. A diferencia de la criptografía, la esteganografía no oculta el contenido, sino que oculta la existencia del contenido.

5. 2. Criptografía

Definición: Técnica de cifrar datos para hacerlos ilegibles para personas no autorizadas. A diferencia de la esteganografía, la criptografía tiene como objetivo ocultar el contenido del mensaje, no su existencia.

6. 3. Imagen de portada (Cover Image)

Definición: En esteganografía, se refiere al archivo en el que se oculta el mensaje. Puede ser una imagen, un archivo de audio, un video o un texto.

7. 4. Mensaje oculto (Hidden Message)

Definición: Información o datos que se encuentran insertados dentro del archivo de portada (por ejemplo, una imagen) utilizando técnicas de esteganografía.

8. 5. Método de sustitución

Definición: Técnica de esteganografía que sustituye ciertos bits de la imagen de portada con los bits del mensaje oculto. Es un enfoque común y simple de esteganografía.

9. 6. LSB (Least Significant Bit)

Definición: Es el bit menos significativo de un byte de información. En la esteganografía, los datos del mensaje oculto se insertan en los bits menos significativos de los píxeles de una imagen para hacer que los cambios sean casi imperceptibles.

10. 7. Herramienta de esteganografía

Definición: Software utilizado para ocultar y extraer mensajes de un archivo. Algunos ejemplos son **Steghide**, **OpenStego**, **QuickStego**, entre otros.

11. 8. Esteganálisis

Definición: El proceso de detectar y descifrar mensajes ocultos dentro de archivos. Los esteganalistas buscan patrones anómalos en los archivos de portada que puedan indicar la presencia de información oculta.

12. 9. Esteganografía en imágenes (Image Steganography)

Definición: Es una forma de esteganografía en la que los datos ocultos se incrustan



en las imágenes digitales. Los cambios en los píxeles de la imagen son mínimos y no perceptibles a simple vista.

13. **10. Esteganografía en audio (Audio Steganography)**

Definición: Técnica que oculta datos en archivos de audio. Esta técnica suele emplear el principio de modificación de los bits menos significativos del archivo de audio para ocultar la información sin afectar la calidad del sonido.

14. **11. Esteganografía en video (Video Steganography)**

Definición: Similar a la esteganografía en imágenes, pero los datos se ocultan en un archivo de video. Se puede ocultar la información en los fotogramas del video o en los audios asociados a este.

15. **12. Esteganografía en texto (Text Steganography)**

Definición: Técnica que oculta mensajes dentro de textos. Puede utilizarse el espaciado de palabras, las mayúsculas, las letras o la codificación de caracteres para ocultar la información.

16. **13. Algoritmo de esteganografía**

Definición: Un conjunto de reglas o procedimientos matemáticos utilizados para insertar o extraer mensajes ocultos de un archivo de portada.

17. **14. Detección de esteganografía (Steganalysis)**

Definición: El proceso y las técnicas utilizadas para detectar la presencia de información oculta en archivos que parecen normales, como imágenes, sonidos o videos. Se buscan patrones o irregularidades que puedan indicar que el archivo ha sido manipulado.

18. **15. Hashing**

Definición: Proceso de generar un valor único (hash) a partir de un archivo o mensaje. En esteganografía, el hashing se puede utilizar para verificar la integridad del mensaje oculto y garantizar que no haya sido alterado.

19. **16. Canal de comunicación (Communication Channel)**

Definición: El medio o archivo en el que se transmite el mensaje oculto. En esteganografía, esto puede ser una imagen, un video, un archivo de audio, un texto, entre otros.

20. **17. Clave de esteganografía (Steganographic Key)**

Definición: Una clave que se utiliza en algunos métodos de esteganografía para cifrar o descifrar el mensaje oculto. No todos los métodos de esteganografía requieren de una clave, pero algunos la utilizan para asegurar el mensaje.

21. **18. Método de difusión (Spread Spectrum)**

Definición: Técnica de esteganografía en la que los datos se dispersan en varias



partes del archivo de portada, lo que dificulta la detección del mensaje oculto al alterar varias partes del archivo, como los píxeles de una imagen.

22. **19. Watermarking (Marca de agua)**

Definición: Similar a la esteganografía, pero con la diferencia de que el propósito es **proteger la propiedad intelectual** y asegurar la integridad de un archivo. A menudo se usa en imágenes o videos para agregar una marca visible o invisible que identifique la autoría o propiedad.

23. **20. Seguridad en esteganografía**

Definición: Medidas adoptadas para proteger la información oculta en un archivo de ser detectada o modificada. Incluye el uso de cifrado, herramientas avanzadas de esteganografía y técnicas de ocultación seguras.

24. **21. Esteganografía adaptativa**

Definición: Técnica de esteganografía en la que los datos se insertan en el archivo de portada de manera dinámica, adaptándose a las características del archivo de acuerdo con su contenido y estructura.

25. **22. Esteganografía visual (Visual Cryptography)**

Definición: Técnica que permite dividir un mensaje en partes visuales que, cuando se combinan correctamente, revelan el contenido completo. Aunque no es estrictamente esteganografía en su definición más clásica, es una forma de ocultar información visualmente.

26. **23. Esteganografía reversible (Reversible Steganography)**

Definición: Tipo de esteganografía en la que el archivo de portada puede ser completamente restaurado a su estado original después de extraer el mensaje oculto. Esto se logra utilizando técnicas que no alteran permanentemente el archivo.

27. **24. Payload (Carga útil)**

Definición: El mensaje o los datos ocultos en el archivo de portada utilizando técnicas de esteganografía. El "payload" es lo que realmente se quiere transmitir.

28. **25. SNR (Signal-to-Noise Ratio - Relación señal-ruido)**

Definición: Es una medida de la cantidad de "ruido" (información alterada) en comparación con la señal original en un archivo que ha sido modificado por esteganografía. Un SNR alto indica que el archivo modificado es difícil de distinguir del original.

6. REFERENTES BIBLIOGRÁFICOS



Anderson, R., & Petitcolas, F. A. P. (2001). *On the Limits of Steganography*. In *Information Hiding: Techniques for Steganography and Digital Watermarking* (pp. 1-26). Artech House.

- **Resumen:** Este libro aborda técnicas de esteganografía, incluyendo su historia y las limitaciones inherentes a los métodos de ocultación de información en los archivos. Los autores exploran tanto el uso legítimo de la esteganografía como los desafíos y las contramedidas contra el esteganálisis.

Kessler, G. C. (2013). *An Overview of Steganography Techniques*. *International Journal of Computer Applications*, 56(10), 1-6.

- **Resumen:** En este artículo, el autor ofrece una visión general de las técnicas de esteganografía, enfocándose en la ocultación de información en imágenes, videos y archivos de audio, y discute las herramientas más utilizadas.

Fridrich, J. (2010). *Digital Image Steganography*. Springer Science & Business Media.

- **Resumen:** Este libro profundiza en la esteganografía digital, con un enfoque particular en la ocultación de información en imágenes digitales. Fridrich discute métodos avanzados y las aplicaciones de esteganografía en la era moderna.

Zhao, X., & Kuo, C. C. J. (2004). *A Survey of Image Steganography and Steganalysis*. *Journal of Visual Communication and Image Representation*, 15(4), 1-9.

7. CONTROL DEL DOCUMENTO

	Nombre	Cargo	Dependencia	Fecha
Autor (es)	Sandra Yineth Macias	Instructir	Comercio y Servicios	5/11/2024

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



	Nombre	Cargo	Dependencia	Fecha	Razón del Cambio
Autor (es)					