**PROCESO DE GESTIÓN DE FORMACIÓN PROFESIONAL INTEGRAL**

**FORMATO GUÍA DE APRENDIZAJE**

**IDENTIFICACIÓN DE LA GUIA DE APRENDIZAJE**

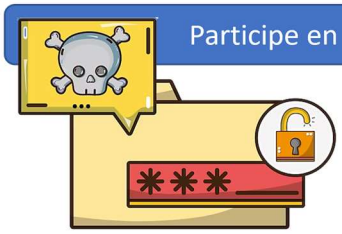
- Denominación del Programa de Formación: **SISTEMAS TELEINFORMÁTICOS**
- Código del Programa de Formación: **233108 V1**
- Nombre del Proyecto: **Optimización de los Servicios Teleinformáticos para impulsar la Conectividad en la institución educativa y/o sector empresarial seleccionado en Soacha y Municipios de influencia del CIDE**
- Fase del Proyecto: **Planeación**
- Actividad de Proyecto: Elaborar plan de mejoramiento del sistema teleinformático según estado de informe de infraestructura de la institución educativa y/o empresa seleccionada.
- Competencia: Operación de herramientas informáticas.
- Resultados de Aprendizaje Alcanzar: **220501121 RAP-03** Planificar la información según criterios de ciberseguridad.
- Duración de la Guía: 72 Horas (Netas 48 Directas 24)

**2. PRESENTACIÓN**

En un mundo cada vez más interconectado y digitalizado, la ciberseguridad se ha convertido en un aspecto fundamental para garantizar la protección de la información y la privacidad en línea. El aprendizaje en ciberseguridad ofrece una oportunidad invaluable para entender los riesgos y amenazas cibernéticas, así como para desarrollar las habilidades necesarias para prevenir y mitigar ataques informáticos. A través de este programa, los participantes explorarán conceptos clave como la protección de datos, la detección de intrusiones, la seguridad de redes y sistemas, y la gestión de incidentes de seguridad. Con un enfoque práctico y basado en escenarios reales, este proporciona las herramientas y el conocimiento necesarios para enfrentar los desafíos constantemente cambiantes del ciberespacio y proteger de manera efectiva tanto a individuos como a organizaciones contra las amenazas cibernéticas.

## 3. FORMULACIÓN DE LAS ACTIVIDADES DE APRENDIZAJE

### 3.1 Actividades de Reflexión inicial.






Participe en una mesa redonda, respondiendo los siguientes interrogantes:

1. ¿Qué entendemos por ciberseguridad y por qué es importante en nuestra vida diaria?
2. ¿Cuáles son algunas de las amenazas cibernéticas más comunes que enfrentamos como individuos y como sociedad?
3. ¿Qué medidas podemos tomar para proteger nuestra información personal en línea?
4. ¿Cómo pueden los comportamientos en línea, como compartir contraseñas o hacer clic en enlaces sospechosos, afectar nuestra seguridad cibernética?
5. ¿Cuál es el papel de la educación y la concienciación en la prevención de ataques cibernéticos?
6. ¿Cuál crees que es la responsabilidad de las empresas y organizaciones en la protección de los datos de los usuarios?
7. ¿Cómo pueden los avances tecnológicos, como el Internet de las cosas (IoT), plantear nuevos desafíos para la ciberseguridad?
8. ¿Qué podemos aprender de los incidentes de seguridad cibernética pasados para mejorar nuestra preparación y respuesta ante futuros ataques?
9. ¿Cómo podemos fomentar una cultura de ciberseguridad en nuestras comunidades y entornos de trabajo?
10. ¿Qué recursos y herramientas están disponibles para ayudarnos a proteger nuestra seguridad cibernética y dónde podemos encontrarlos?

**Ambiente requerido:** Sala de sistemas con equipos de cómputo y acceso a internet
**Materiales:** Tablero y marcadores

### 3.2 Actividades de contextualización e identificación de conocimientos necesarios para el aprendizaje.

**Entremos en contexto:** En la era digital en la que vivimos, la ciberseguridad se ha convertido en un tema de vital importancia para individuos, empresas y gobiernos por igual. Con el aumento de la conectividad a través de internet y dispositivos digitales, también han surgido nuevas amenazas cibernéticas que pueden comprometer nuestra privacidad, seguridad y bienestar en línea. Desde ataques de phishing diseñados para robar información personal hasta el malware que puede infectar nuestros dispositivos, es crucial entender los riesgos asociados con la actividad en línea y aprender cómo protegernos adecuadamente. La ciberseguridad no solo se trata de evitar amenazas externas, sino también de adoptar prácticas seguras y responsables en nuestra interacción con la tecnología. En este contexto, exploraremos los fundamentos de la ciberseguridad, desde la importancia de contraseñas seguras hasta la detección y prevención de ataques cibernéticos, para que podamos navegar por el mundo digital con confianza y seguridad.

**ACTIVIDAD 1.** Elabore un libro de conocimientos en la herramienta https://app.bookcreator.com/, con la siguiente investigación.

el código para el ingreso será compartido por su instructor.




**Ambiente requerido:**
Sala de sistemas con equipos de cómputo y acceso a internet
**Materiales:**
Tablero y marcadores

**3.3 Actividades de apropiación del conocimiento (Conceptualización y Teorización).**

Descripción de las Actividades:

3.3.1. Ejecutar la parametrización de Seguridad en Windows 8.1, 10 o 11 según procedimiento técnicos para la Implantación de seguridad de sistemas operativo Windows para los cuales tiene aspectos importantes y particulares de seguridad o endurecimiento (hardening).
Realizar las prácticas de configuración que se encuentran en el taller que le suministrara su instructor.

3.3.2. Planificar copias de seguridad según procedimientos técnicos y criterios de seguridad.

Los cuatro (4) aprendices que realizaron el taller de hardening realizarán una planificación de las características necesarias para la realización copias de seguridad:

- Tipos de copias de seguridad.
- Discusión de ventajas y desventajas de cada tipo.
- Estrategia 3-2-1 de copias de seguridad
- Preparación de disponibilidad de recursos.
- Retención de copias y periodos.
- Controles de cifrado y protección de datos.

Puede usar el material: Copias de Seguridad “Una guía de aproximación para el empresario” disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf

**Ambiente Requerido:** Mínimo 60 metros cuadrados, materiales y herramientas requeridas.

**Materiales:** Computador funcionales de escritorio o portátiles con memoria RAM 16 GB, procesador 3.0 GHz o Superior, Disco Duro de 1 TB, Software ofimático, Red internet operativa para consultas, Unidad Flash USB. Las condiciones pueden variar, esta sujeto a disponibilidad e infraestructura disponible.

## 3.4. Actividades de transferencia del conocimiento.

**Actividad - Procesos de Copias de Seguridad**




A. Crear una Carpeta en el Sistema Operativo Windows y nombrarla “Backup”.

B. Una vez creada la anterior Carpeta deben guardar en esta Carpeta al menos cinco (5) Archivos que sean diferentes y de tipos diferentes.

C. Con la herramienta de Copia de Seguridad del Sistema Operativo Windows o cualquier otra herramienta de Copia de Seguridad, deben realizar dos (2) Procesos de Copias de Seguridad. Un (1) Backup Incremental que tenga registros de mínimo Dos (2) Horas diferentes y un (1) Backup Total de la Carpeta con sus archivos.

Nota: Para efectos de ver las versiones y los cambios de la copia incremental, se deben por favor modificar los archivos antes de hacer cada copia de seguridad (Diferentes Horas).

D. Etiquetar las copias de Seguridad creadas, con las fechas y Hora de Creación y un nombre seleccionado por ustedes, donde se debe diferenciar si la copia es Total o Incremental.

**Ambiente Requerido:** Mínimo 60 metros cuadrados, materiales y herramientas requeridas.

**Materiales:** Computador funcionales de escritorio o portátiles con memoria RAM 16 GB, procesador 3.0 GHz o Superior, Disco Duro de 1 TB, Software ofimático, Red internet operativa para consultas, Unidad Flash USB. Las condiciones pueden variar, esta sujeto a disponibilidad e infraestructura disponible.

**. ACTIVIDADES DE EVALUACIÓN**

| Evidencias de Aprendizaje | Criterios de Evaluación | Técnicas e Instrumentos de Evaluación |
|---|---|---|
| **Evidencias de Conocimiento :**<br><br>**Evidencias de Desempeño:**<br><br>Recomendaciones para el HARDENING (Endurecimiento).<br><br>**Evidencias de Producto:**<br><br>Implementación de Herramientas del Sistema Operativo para Endurecer la Seguridad del Equipo<br><br>(EndPoint) protegido | Propone procesos de mejora en el manejo de la información con base a la normativa vigente.<br><br>Aplica controles de seguridad según normativa, necesidades y restricciones de acceso a la información.<br><br>Gestiona las copias de seguridad y recuperación, según lineamientos establecidos por la empresa.<br><br>Implementa herramientas para robustecer la Seguridad en los equipos de cómputo con SO Windows. | Lista de chequeo:IE-01<br><br>Exposición Casos de Ciberseguridad<br><br>Lista de chequeo<br><br>Lista de chequeo |

**5. GLOSARIO DE TÉRMINOS**

**Antivirus :** Software que escanea un dispositivo o una red para detectar amenazas de seguridad, alertarlo y neutralizar códigos maliciosos.

**Autenticador:** Un método de cómo un usuario puede probar su identidad a un sistema. Puede ser una contraseña, una huella digital, un escaneo facial.

**Bot:** Un programa que puede realizar automáticamente una simple tarea repetida para alcanzar un objetivo perseguido. Algunos de los bots son maliciosos, mientras que otros pueden ser beneficiosos.

**Copia de seguridad:**Una copia de los datos físicos o virtuales para que, en caso de que se eliminen o se pierdan, el usuario pueda recuperarlos fácilmente. Funciona como parte de un plan de prevención de pérdida de datos.

**Cifrado de datos:** Una forma de proteger la información privada codificándola para que ningún tercero pueda verla o acceder a ella. Para leer el archivo codificado (cifrado), debes decodificarlo utilizando una clave de descifrado.

**Ciberataque:** Cualquier intento de violar el perímetro de seguridad de un entorno lógico. Un ataque puede enfocarse en recopilar información, dañar procesos comerciales, explotar fallas, monitorizar objetivos,

interrumpir tareas comerciales, extraer valor, causar daños a activos lógicos o físicos o utilizar recursos del sistema para respaldar ataques contra otros objetivos.

Los ciberataques pueden iniciarse mediante la explotación de una vulnerabilidad en un servicio expuesto públicamente, engañando a un usuario para que abra un archivo adjunto infeccioso o incluso provocando la instalación automatizada de herramientas de explotación a través de visitas inocentes al sitio web.

**Cracker:** Una persona que ataca un sistema informático específico, a menudo para robar o corromper información o datos confidenciales sobre una empresa o un producto.

**Hacker:** White Hat Hacker es un experto en ciberseguridad que prueba un sistema ejecutando ciberataques simulados para descubrir posibles vulnerabilidades de seguridad.

Black Hat Hacker es una persona que intenta irrumpir en un sistema informático explotando vulnerabilidades de ciberseguridad .

**Hacking de enlaces:** Una práctica potencialmente poco ética de redirigir un enlace a un sitio o ubicación de intermediario o agregador en lugar del sitio original al que parecía indicar el enlace. Por ejemplo, un servicio de agregación de noticias puede publicar enlaces que parecen apuntar a la fuente original de sus artículos publicados, pero cuando un usuario descubre esos enlaces a través de una búsqueda o redes sociales, los enlaces redireccionan al sitio de agregación y no al fuente original del artículo.

**Dirección IP:** Una dirección que identifica la conexión entre tu computadora y el proveedor de red. Tu computadora puede tener varias direcciones IP dependiendo de la cantidad de redes a las que se conecta. Además, varias computadoras pueden tener una dirección IP si están conectadas al mismo proveedor en la misma área, como en cafés o en casa.

**DLP (Prevención de pérdida de datos)**

Una colección de mecanismos de seguridad que tienen como objetivo prevenir la ocurrencia de pérdida y / o fuga de datos. La pérdida de datos ocurre cuando un dispositivo de almacenamiento se pierde o es robado, mientras que la fuga de datos ocurre cuando entidades no autorizadas poseen copias de los datos. En ambos casos, los datos son accesibles para quienes no deberían tener acceso.

**DLP** tiene como objetivo prevenir tales ocurrencias a través de diversas técnicas, como controles estrictos de acceso a los recursos, bloquear el uso de archivos adjuntos de correo electrónico, evitar el intercambio de archivos de red a sistemas externos, bloquear cortar y pegar, deshabilitar el uso de redes sociales y cifrar los datos almacenados.

**Lista negra:** Una lista de correos electrónicos u otros proveedores de servicios que difunden mensajes de spam. Las listas negras ayudan a los usuarios y empresas a evitar la avalancha de mensajes no deseados.

**Protección de datos:** Un conjunto de métodos destinados a proteger la información privada para que no caiga en las manos equivocadas.

**Phishing:**Una amplia gama de estafas cuando alguien se hace pasar por entidades confiables en un intento de obtener información. Por ejemplo, un usuario puede recibir un correo electrónico de «Google» pidiéndole que haga clic en el enlace y escriba su nombre de usuario y contraseña, o la información de la tarjeta de crédito en los campos vacíos.

**IDS (Sistema de detección de intrusiones):** Una herramienta de seguridad que intenta detectar la presencia de intrusos o la ocurrencia de violaciones de seguridad para notificar a los administradores, permitir un registro más detallado o enfocado o incluso desencadenar una respuesta como desconectar una sesión o bloquear una IP. habla a. Un IDS se considera una herramienta de seguridad más pasiva, ya que detecta compromisos después de que ya están ocurriendo en lugar de evitar que tengan éxito.

**Malware (software malicioso):** Un código malicioso diseñado para dañar computadoras y sistemas. Existen muchos tipos de programas de malware con diferentes objetivos: robar o borrar información del usuario, robar capacidades informáticas, espiar o destruir un programa.

**Ransomware:** Un tipo de programa malicioso (malware) que cifra los datos para que la víctima no pueda acceder a ellos sin la clave de descifrado. Para obtener uno, la víctima debe pagar un rescate, generalmente dentro de un período designado. Puede ver cómo se ve el ransomware a continuación.

**Ransomcloud:** Un tipo especial de ransomware, diseñado para cifrar correos electrónicos y archivos adjuntos en la nube.

**Rootkit:** Un tipo de malware que se utiliza para infiltrarse en el sistema y robar información de la empresa. Puede ser muy complicado de detectar porque el malware gana control sobre el sistema operativo y se disfraza. Algunas empresas detectan fugas de datos después de meses o incluso años.

**Spyware:**Malware que espía en la computadora para recopilar información sobre un producto, una empresa o una persona. Los objetivos pueden ser diferentes: vender esta información a quienes puedan beneficiarse de ella, como anunciantes, competidores, empresas de datos; para obtener la información bancaria y las contraseñas, etc. Los programas espía más difundidos son los registradores de pulsaciones de teclas y los troyanos.

**Spear phishing:** Una forma de ataque de ingeniería social que está dirigido a víctimas que tienen una relación digital existente con una entidad en línea, como un banco o un sitio web minorista. Un mensaje de spear phishing suele ser un correo electrónico, aunque también hay mensajes de texto y ataques de spear phishing VoIP, que se parecen exactamente a una comunicación legítima de una entidad de confianza.

El ataque engaña a la víctima para que haga clic en un hipervínculo para visitar el sitio web de una empresa y luego sea redirigida a una versión falsa del sitio web operado por los atacantes. El sitio web falso a menudo se verá y funcionará de manera similar al sitio legítimo y se centrará en que la víctima proporcione sus credenciales de inicio de sesión y posiblemente otra información de identidad personal.

El objetivo de un ataque de suplantación de identidad (spear phishing) es robar información de identidad con el fin de tomar el control de la cuenta o el robo de identidad.

**Troyano:**Una forma de código malicioso que parece un archivo, programa o aplicación legítimos, pero que en realidad está diseñado para controlar la computadora y los datos del usuario. Por lo general, es difícil de detectar hasta que los daños y las pérdidas son importantes. Puede borrar, espiar y pedir dinero por razones aparentemente legítimas.

**Virus:**Un tipo de malware que tiene como objetivo infectar y dañar un archivo, un sistema o una red. El programa de virus generalmente se adjunta a un archivo o aplicación de apariencia inofensiva, lo que elimina la sospecha al hacer que parezca válido y seguro. Algunos virus pueden replicarse.

**Gusano:** Un tipo de malware autorreplicante que, cuando se infecta en una computadora, tiene como objetivo propagarse por la red para infectar a otros. Un gusano puede multiplicarse para «comerse» los recursos de una computadora, o ser agudizado para robar y eliminar datos del usuario y provocar un caos generalizado en el sistema. Los gusanos llegan a través de vulnerabilidades del sistema o haciendo clic en archivos adjuntos maliciosos.

**Zombie:**Término relacionado con el concepto malicioso de una botnet. El término zombi se puede utilizar para hacer referencia al sistema que aloja el agente de malware de la botnet o al propio agente de malware. Si es lo primero, el zombi es el sistema que está cegando al realizar tareas según las instrucciones de un pirata informático externo y remoto. Si es lo último, el zombi es la herramienta que está realizando acciones maliciosas como inundación de DoS, transmisión de SPAM, escuchas en llamadas VoIP o falsificación de resoluciones de DNS como miembro de una botnet.

## 6. REFERENTES BILBIOGRÁFICOS


https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf
https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf
https://ciberseguridad.com/guias/recursos/glosario-terminos/


## 7. CONTROL DEL DOCUMENTO

| | Nombre | Cargo | Dependencia | Fecha |
|---|---|---|---|---|
| **Autor (es)** | Ing.German Eduardo Homez Rodríguez | Instructor | Articulación con la Educación Media | Marzo 01 de 2024 |

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

| | Nombre | Cargo | Dependencia | Fecha | Razón del Cambio |
|---|---|---|---|---|---|
| **Autor (es)** | | | | | |