PROCESO DE GESTIÓN DE FORMACIÓN PROFESIONAL INTEGRAL
FORMATO GUÍA DE APRENDIZAJE

1. IDENTIFICACIÓN DE LA GUIA DE APRENDIZAJE

- **Denominación del Programa de Formación**: Técnico en Sistemas Teleinformáticas.
- **Código del Programa de Formación**: 233101 V1.
- **Nombre del Proyecto**: Gestión de los servicios solicitados por los clientes para el soporte técnico de software, hardware y redes.
- **Fase del Proyecto**: Ejecución
- **Actividad de Proyecto**: Clasificar la infraestructura de red y equipos informáticos y solicitudes de servicio técnico presente en el entorno de trabajo
- **Competencia**: Operar herramientas informáticas y digitales de acuerdo con protocolos y manuales técnicos**.**
- **Resultados de Aprendizaje**: Planificar la información según criterios de ciberseguridad
- **Duración de la Guía**: 80 horas

2. PRESENTACIÓN

En un mundo cada vez más digitalizado, la seguridad de la información se vuelve crucial. Las políticas de seguridad, la normativa, y la gestión adecuada de datos son pilares fundamentales para proteger la integridad y confidencialidad de la información. Esta guía de aprendizaje pretende que el aprendiz explorare aspectos clave, tales como con los derechos de Habeas Data y de autor, los procesos de mejora continua y la importancia de las copias de seguridad. Que adquiera las habilidades necesarias para enfrentar los desafíos de seguridad informática y gestión de datos en el mundo actual.



Tomada de: https://acortar.link/6P8P1l

Durante el desarrollo de las actividades planteadas se realizarán prácticas basadas en la fundamentación teórica con el fin de identificar amenazas y vulnerabilidades que puedan generar incidentes que afecten la infraestructura de las redes de datos y comprometer la integridad de los mismos.

3. FORMULACIÓN DE LAS ACTIVIDADES DE APRENDIZAJE

3.1 Actividades de Reflexión inicial.

3.1.1. Reconocer aspectos fundamentales de la seguridad de la información, destacando la importancia de adoptar medidas frente a los riesgos de la seguridad y la gestión de datos.

Con la implementación de controles en la seguridad de datos en redes de telecomunicaciones, el administrador de redes debe asegurarse de gestionar las políticas que permitan blindar la seguridad de la información, como un activo fundamental de la organización.

Actividad

Para desarrollar la actividad realizará la siguiente lectura de donde extraerá las ideas principales, luego empelará **Ideogram IA**, para redactar un Prompt, que representará un **Poster** o **Afiche** alusivo a la seguridad informática. Luego en un documento en Word, con no menos de 500 palabras, redactará un escrito que responda a la siguiente pregunta: ***¿Cuál es su punto de vista acerca de la implementación de la Inteligencia artificial en procesos que involucren manejo de grandes volúmenes de información?*** *Coloque un título a su escrito. El instructor orientará la entrega de su trabajo.*

La actividad se socializará en plenaria, y con orientación del docente se tomarán algunas conclusiones para realizar el cierre de la sesión.

- **Descripción de la actividad:**
  - ✓ Realizar un afiche empleando Ideogram
  - ✓ Realizar un escrito en Word sobre seguridad informática.
- **Ambiente requerido:** Ambiente de aprendizaje presencial
- **Estrategias o técnicas didácticas activas:** Debate: Sesión de reflexión donde los estudiantes discuten las implicaciones éticas, sociales y económicas de la implementación de la Inteligencia Artificial en el manejo de datos.
- **Materiales de formación:** Computadores 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 – Video Beam, marcadores borrables, Tablero.
- **Material de apoyo:**
  - ✓ Lectura "La seguridad Infromática"
  - ✓ Link Video "Tutorial sobre Ideogram"
- **Duración de la actividad:** 5 horas**.**

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

3.2.1 Definir los principios fundamentales de la seguridad informática aplicados en situaciones reales para garantizar la protección de datos y sistemas contra amenazas y ataques.

Teniendo en cuenta que la seguridad de la información y la gestión de datos son aspectos críticos en el entorno digital actual, es fundamental comprender nuestras percepciones y experiencias previas en este ámbito.

El aprendiz visitará el siguiente link y realizará la actividad 1 “Seguridad Informática”, la cual se socializará en clase**.** Link: https://goo.su/5jxsgUY

Ahora en este punto del desarrollo de la actividad los aprendices deberán observar el vídeo “SGSI - 01 Conceptos Básicos sobre la Seguridad de la Información”, posteriormente harán uso de una herramienta para diseño de diapositivas, donde presentarán los beneficios de la implementación de planes de seguridad en las redes de datos.

- **Descripción de la actividad:**
  - ✓ Realizar actividad 1: Definición de conceptos.
  - ✓ Realizar socialización aspectos de la seguridad de la información.
- **Evidencia:** No aplica para evidencia.
- **Instrumento de evaluación:** Cuestionario de conocimiento.
- **Ambiente requerido:** Ambiente de aprendizaje presencial.
- **Estrategias o técnicas didácticas activas: Método de indagación**: Se motiva a los aprendices a formular preguntas y buscar respuestas para construir su propio conocimiento.
- **Materiales de formación:** 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 – Video Beam, marcadores borrables, Tablero.
- **Material de apoyo:**
  - ✓ Link: https://goo.su/5jxsgUY
  - ✓ Link: “SGSI - 01 Conceptos Básicos sobre la Seguridad de la Información”
- **Duración de la actividad:** 5 horas**.**

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

3.3.1. Comprender la importancia de la planificación de la información con enfoque en ciberseguridad.

"En un mundo digital cada vez más interconectado, la seguridad de la información se ha convertido en un aspecto crucial para salvaguardar la integridad y la privacidad de los datos. En este contexto, identificar criterios efectivos de ciberseguridad se vuelve imperativo, especialmente al considerar los diversos riesgos asociados con el manejo de datos en entornos virtuales.”

Lectura: "Planificar la información según criterios de ciberseguridad".

Los participantes leerán el texto "Planificar la información según criterios de ciberseguridad" y realizarán la siguiente actividad:

Aprendizaje cooperativo: Se formarán grupos de discusión, donde los participantes compartirán sus impresiones sobre el texto y diseñarán un **juego interactivo** donde la clave será adivinar palabras claves sobre la seguridad de la información.

Realizarán una **presentación electrónica** en línea que dé respuesta a las siguientes preguntas, teniendo en cuenta la orientación del Instructor. (Equipos de trabajo de acuerdo al número de aprendices).

Preguntas:

1. ¿Por qué es importante planificar la información con un enfoque en ciberseguridad?
2. ¿Qué riesgos pueden surgir si no se consideran criterios de ciberseguridad en la planificación de la información?
3. ¿Qué medidas preventivas pueden implementarse para proteger la información de manera efectiva?

Presentación de Conclusiones: Cada grupo seleccionará a un representante para compartir las conclusiones de su discusión con el resto de los participantes. Se enfatizará en la importancia de considerar la ciberseguridad en todas las etapas de planificación y gestión de la información.

Elaboración de Propuestas: Los participantes trabajarán individualmente para elaborar propuestas concretas de cómo integrar criterios de ciberseguridad en la planificación de la información en su entorno laboral o personal. Se alentará a los participantes a ser creativos y proponer soluciones innovadoras y prácticas.

Debate y Retroalimentación: Se abrirá un espacio para el debate y la retroalimentación, donde los participantes compartirán sus propuestas y recibirán comentarios y sugerencias de mejora por parte de sus compañeros y el Instructor.

El aprendiz visitará el siguiente link y realizará las actividades propuestas: https://goo.su/QOJsB

- ✓ **1.1 Seguridad física y seguridad lógica y**
- ✓ **1.2 Delitos informáticos y legislación**

- **Descripción de la actividad:**
  - ✓ Realizar lectura sobre planificación en seguridad informática.
  - ✓ Realizar juego interactivo
  - ✓ Realizar presentación electrónica.
  - ✓ Diseñar una propuesta sobre seguridad de los datos en su entorno.
  - ✓ Participar en un debate sobre seguridad de la información.
- **Ambiente requerido:** Ambiente de aprendizaje presencial.
- **Estrategias o técnicas didácticas activas: Aprendizaje cooperativo**: Los Aprendices trabajan en grupo para diseñar la sustentación sobre Planificación de la seguridad informática.
- **Materiales de formación:** 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 – Video Beam, marcadores borrables, Tablero.
- **Material de apoyo:**
  - ✓ Link: https://goo.su/5jxsgUY
  - ✓ Documento Pdf “Conceptos sobre seguridad informática”

https://gamma.app/docs/Introduccion-a-la-seguridad-de-la-informacion-gytjnqz2ixfsqo1?mode=doc (**Presentación realizada en la IA Gamma)**

https://es.slideshare.net/alexaloaiza/seguridad-de-la-informacion-63691557

- **Evidencias de aprendizaje: Desempeño:** "Socialización _Evidencia Integral de Seguridad Informática"
- **Instrumento de evaluación:** Lista de chequeo desempeño y producto
- **Duración de la actividad:** 10 horas**.**

3.3.2. Explicar los conceptos clave acerca de la seguridad de la información, y la legislación vigente sobre delitos informáticos en Colombia.

La información es uno de los activos más valiosos para las personas y las organizaciones, por lo que su seguridad es crucial. La seguridad de la información se enfoca en proteger la confidencialidad, integridad y disponibilidad de los datos frente a amenazas como accesos no autorizados y daños intencionales. La evolución tecnológica ha incrementado los delitos informáticos, llevando a los gobiernos a reforzar sus legislaciones. En Colombia, la Ley 1273 de 2009 establece un marco legal para proteger la información y sancionar delitos como el acceso abusivo a sistemas, la interceptación de datos y el uso de software malicioso.

Para la actividad a realizar, cada aprendiz debe visitar el siguiente link https://goo.su/D1aUisT el cual le permitirá acceder a un juego de memoria educativo. Este archivo interactivo le permitirá explorar los fundamentos de la seguridad digital. Después profundizará en cada una de las proposiciones y diseñará una **infografía interactiva**, basándose en el siguiente tutorial.

Tutorial infografía con Inteligencia Artificial | ChatPDF + Canva
https://www.youtube.com/watch?v=aEIurp3NVRc

En equipos de trabajo realizará una exposición sobre el tema **Proyecto de Ley Delitos Informático en Colombia**. Esta actividad la realizarán con la orientación del instructor, quien subdividirá la información para dinamizar el trabajo.

- **Descripción de la actividad:**
  - ✓ Profundizar en los fundamentos acerca de la seguridad digital.
  - ✓ Diseñar una infografía interactiva.
  - ✓ Socializar el Proyecto de Ley Delitos informáticos en Colombia.
- **Ambiente requerido:** Ambiente de aprendizaje presencial.
- **Estrategias o técnicas didácticas activas: Exposición**: Los Aprendices trabajan en grupo para diseñar la socialización sobre la **Legislación sobre delitos informático en Colombia**.
- **Materiales de formación:** 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 – Video Beam, marcadores borrables, Tablero.
- **Material de apoyo:**
  - ✓ link https://goo.su/D1aUisT

- ✓ link https://www.youtube.com/watch?v=aEIurp3NVRc
- ✓ Documento “Ley Delitos informáticos”

- **Evidencias de aprendizaje: Socialización:** Legislación sobre delitos informático en Colombia.
- **Instrumento de evaluación:** Evaluación de conocimiento.
- **Duración de la actividad:** 10 horas**.**

3.3.3. Analizar aspectos relevantes acerca de la protección de datos personales y los derechos de autor, de acuerdo al enfoque de la aplicación de buenas prácticas en su gestión.

Protección de Datos y Derechos de Autor



1 Tomada de https://onx.la/eeff9

En la era digital, la protección de datos y los derechos de autor son esenciales en proyectos que manejan información personal y material creativo. La ley de **Habeas Data** garantiza el derecho a la privacidad y control sobre la información personal, permitiendo a los individuos conocer, actualizar y rectificar sus datos en bases de datos. Los derechos de autor protegen las obras creativas, otorgando a los creadores derechos exclusivos sobre su uso y distribución. Cumplir con estas leyes asegura la ética y legalidad del proyecto, garantizando la privacidad de las personas y el respeto a los derechos de los autores. El equilibrio entre ambas protecciones es fundamental para el manejo adecuado de la información y el reconocimiento del trabajo creativo.

Actividad

Cada aprendiz responderá las siguientes preguntas y en plenaria compartirá las respuestas de acuerdo a la orientación del instructor quien aplicará una didáctica activa.

Preguntas.

1. ¿Ha escuchado alguna vez sobre la ley de Habeas Data? Si es así, ¿podría describir en qué consiste? De lo contrario consulte el tema.
2. ¿Cómo cree que la ley de Habeas Data protege la privacidad de los datos de las personas?
3. ¿Sabe qué son los derechos de autor y cómo se relacionan con la protección de la propiedad intelectual?
4. ¿Qué medidas cree que son importantes para garantizar el cumplimiento de los derechos de autor al utilizar datos o información en un proyecto?
5. ¿Cuál cree que es la importancia de respetar tanto la ley de Habeas Data como los derechos de autor en proyectos que involucran el manejo de datos e información personal?

Luego con la participación del instructor visitará el siguiente link y ampliará sus conceptos.

https://es.educaplay.com/recursos-educativos/18680613
seguridad_de_la_informacion_en_colombia.html

- **Descripción de la actividad:**
  - ✓ Profundizar en los conceptos sobre La ley de **Habeas Data.**
- **Ambiente requerido:** Ambiente de aprendizaje presencial.
- **Estrategias o técnicas didácticas activas: Debates y discusiones**: Los Aprendices trabajan en grupo para diseñar la socialización sobre La ley de **Habeas Data,** esto permitirá fomentan el intercambio de ideas y la argumentación, fortaleciendo habilidades de comunicación y pensamiento crítico.
- **Materiales de formación:** 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 – Video Beam, marcadores borrables, Tablero.
- **Material de apoyo:**
  - ✓ Link: https://es.educaplay.com/recursos-educativos/18680613 seguridad_de_la_informacion_en_colombia.html
  - ✓ Presentación electrónica: Ley 1581 de 2012
- **Evidencias de aprendizaje:** Video explicativo sobre el Habeas Data.
- **Instrumento de evaluación:** Lista de chequeo de Producto
- **Duración de la actividad:** 5 horas**.**

3.3.4. Analizar el alcance de la normatividad vigente en relación con la seguridad de la información en Colombia.

"La seguridad de la información, que suele abreviarse como InfoSec, es un conjunto de procedimientos y herramientas de seguridad que protegen ampliamente la información confidencial de la empresa frente al uso indebido, acceso no autorizado, interrupción o destrucción". (htt18)

Los aprendices tendrán la oportunidad de adquirir conocimientos sobre gestión de la seguridad de la información; para ello en equipos de trabajo, realizarán análisis casos de estudio relacionados con normativas de gestión y seguridad de la información.

Los grupos deben leer detenidamente el caso para resolver los puntos que se plantean en la actividad:



Tomado de https://www.pmg-ssi.com/2019/11/ciberataques-ransomware-amenaza-para-los-sistemas/

Caso de estudio 1.: *Mucho se ha escuchado sobre ciberataques en los últimos días. Un tema que no es nada nuevo en Colombia, pues según la firma de ciberseguridad Fortinet, tan solo en el primer semestre del año, el país recibió 5000 millones de intentos de ataques informáticos.*

Los ejemplos son numerosos: "En 2021 la Pontificia Universidad Javeriana fue víctima de uno; en 2022 el turno fue para la organización multinacional Keralty, a la que pertenece la EPS Sanitas, y Empresas Públicas de Medellín –EPM–; y la semana pasada, IFX Networks, un proveedor de servicios en la nube, sufrió un ciberataque que afectó al menos a 50 entidades estatales colombianas, incluyendo al Ministerio de Salud y Protección Social y al Consejo Superior de la Judicatura.

*El gobierno colombiano anunció que demandará a IFX Networks por los daños ocasionados por el ataque, ya que considera que hubo fallas en la seguridad de la compañía. ¿Pero por qué causa tanta preocupación y revuelo un ataque cibernético? Para empezar, ¿qué es un ciberataque? Para entenderlo de forma simple, imaginemos que nuestro computador tiene un candado digital para proteger los documentos importantes, pero alguien, sin nuestro permiso, logra abrir ese candado para ver, robar o dañar todas las cosas que están ahí dentro. "**Tomado de la internet***



Tomado de: https://x.com/CibersegLATAM/status/1729974010945925555/photo/1

En este caso, fue un ataque de ransomware, que es un tipo de ciberataque en el que los delincuentes cifran los archivos o sistemas informáticos de una víctima y luego exigen un rescate para proporcionar la clave o herramienta necesaria para desbloquear los archivos o sistemas.

En otras palabras, secuestran los datos. Los responsables de este ciberataque serían el colectivo Ransomhouse, quienes también estuvieron detrás del ataque a Keralty.

Ahora en equipos de trabajo responderán los siguientes interrogantes:

1. ¿Cuáles son las consecuencias más comunes de un ciberataque para las organizaciones afectadas?
2. ¿Qué medidas de seguridad adicionales podrían implementarse para protegerse de futuros ciberataques?
3. ¿Cómo afectan los ciberataques a la confianza y reputación de las empresas o entidades afectadas?
4. ¿Qué papel juegan las leyes y regulaciones de ciberseguridad en la prevención y respuesta a los ciberataques?
5. ¿Cuáles son las principales diferencias entre un ciberataque de ransomware y otros tipos de ataques cibernéticos?

Realizar un mapa conceptual, y preparar una sustentación de acuerdo a los siguientes temas.

- **Malware**: Qué es, tipos, cómo se identifican y controlan.
- **Suplantación de identidad** tipos de phishing, correo no deseado, cómo identificarlos y buenas prácticas.
- **Ataques TCP**: Qué son, cómo identificarlos.
- **Ataques de Día cero** e ingeniería social.
- **Directiva de seguridad** local de Windows.
- **Protección de acceso a datos** y Protección contra malware.
- **Técnicas de seguridad**

- **Protección de equipos** físicos.
- **Técnicas de mantenimiento preventivo** comunes para propósitos de seguridad.
- **Procedimientos mínimos** de solución de problemas de seguridad.

- **Descripción de la actividad:**
  - ✓ Análisis del alcance de la normatividad vigente en relación con la seguridad de la información a través de un preguntuario.
  - ✓ Diseñar mapas conceptuales sobre aspectos que comprometen la seguridad de la información.
- **Ambiente requerido:** Ambiente de aprendizaje presencial.
- **Estrategias o técnicas didácticas activas: Estudio de caso**: El aprendiz analiza un caso real o simulado, y a través de interrogantes analiza la aplicación de conceptos teóricos a situaciones concretas.
- **Materiales de formación:** 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 – Video Beam, marcadores borrables, Tablero.
- **Material de apoyo: Por definir**
- **Evidencias de aprendizaje:** Informe técnico sobre copias de seguridad.
- **Instrumento de evaluación:** Lista de chequeo de desempeño.
- **Duración de la actividad:** 10 horas**.**

3.3.5. Evaluar los servicios de Internet que permitan la investigación y el análisis crítico de los diferentes procesos, de acuerdo con las necesidades de la organización.

Los servicios de Internet son aplicaciones, plataformas o recursos en línea que proporcionan una variedad de funciones y utilidades para los usuarios. Estos servicios se utilizan para diversas actividades, como comunicación, entretenimiento, trabajo, educación, compras y más. Algunos ejemplos comunes de servicios de Internet incluyen: Redes Sociales, Correo Electrónico, Plataformas de Streaming, Herramientas de Productividad, Motores de Búsqueda, Bancos en Línea y Servicios Financieros, Educación en Línea entre otros.

En equipos de trabajo máximo 2 aprendices, visitarán el siguiente link Practiquemos: EL correo electrónico. Realizarán las actividades propuestas orientados por el Instructor.

Actividad. - Ejercicios búsqueda en Internet: Antes de realizar estos ejercicios, se recomienda repasar temas como: búsqueda avanzada en Google y almacenamiento de la información.



Tomado de: https://acortar.link/LAwrKi

Usando las opciones de búsqueda en Internet, encuentra la respuesta a estas preguntas, inserta una tabla en este espacio y consigna las respuestas. Organiza adecuadamente la información.

1. ¿Qué es un sistema operativo y cuáles son los más utilizados?
2. ¿Quién es el fundador de Facebook?
3. ¿En qué ciudad de EEUU están ubicados los servidores de Google?
4. ¿Qué es la Inteligencia Artificial?
5. ¿Cómo afecta la IA las oportunidades laborales?

Busca la siguiente información en internet. inserta una tabla en este espacio y consigna las respuestas. Organiza adecuadamente la información.

6. Precio de una licencia de Office.
7. La historia de Linux. Aspectos relevantes
8. ¿Qué es un software libre y cuáles sus alcances?
9. Averigua en qué museos se encuentran los siguientes objetos y obras de arte, mostrando una imagen de los mismos, para ello diseña una tabla y consigna la información.
    - ✓ Piedra Roseta.
    - ✓ El nacimiento de Venus.
    - ✓ El Guernica.
    - ✓ Venus de Milo.
10. Agrega cada una de las páginas que consultaste a Marcadores del navegador.

Mediante el buscador de imágenes de Google, realiza las siguientes búsquedas en Internet. Organiza en una tabla los puntos propuestos y su respectiva búsqueda.

- ✓ Disco duro mecánico HHDD y una unida de estado sólido SD
- ✓ Mother board con IA
- ✓ Chip para mascotas
- ✓ Telemedicina
- ✓ Transferencia de archivos.

Copia el contenido de las siguientes búsquedas en un documento Word

- ✓ ¿Qué es la WhatsApp web?
- ✓ ¿Qué es una conexión P2P?
- ✓ ¿Qué es una cookie?
- ✓ ¿Qué es la 'unidad de estado sólido' de un computador?
- ✓ ¿A qué llaman mensajes 'fantasma?

Ejercicios de búsqueda en Internet: Busca y descarga los siguientes archivos. Guárdalos en una carpeta llamada Descarga de archivos (no los instale)

1. Manual de Outlook.
2. Acrobat Reader PDF
3. Antivirus AVG
4. Firefox
5. WinZip

El Instructor concluirá la actividad realizando una rúbrica con los aprendices, retroalimentando sobre cómo las herramientas informáticas influyen en la sociedad en general.

- **Descripción de la actividad:**
  - ✓ Evaluar a través de ejercicios prácticos el alcance que tiene los **servicios de Internet** en la manipulación de la información.
- **Ambiente requerido:** Ambiente de aprendizaje presencial.
- **Estrategias o técnicas didácticas activas: Talleres prácticos**: El Aprendiz realizará actividades prácticas que le permitan evaluar el conocimiento y habilidades en el manejo de la internet en un entorno controlado.
- **Materiales de formación:** 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 – Video Beam, marcadores borrables, Tablero.
- **Material de apoyo:** Link**:** Practiquemos: El correo electrónico
- **Evidencias de aprendizaje:** Informe en Pdf actividad servicios de internet.
- **Instrumento de evaluación:** Lista de chequeo - Evaluación de desempeño.
- **Duración de la actividad:** 10 horas**.**

3.3.6. Realizar la parametrización de Seguridad en Windows 10 o 11 según procedimiento técnicos

La seguridad en los sistemas operativos Windows 10 y 11 es fundamental para proteger datos personales y corporativos contra diversas amenazas cibernéticas. La parametrización de seguridad implica configurar adecuadamente las opciones de seguridad del sistema operativo para asegurar su integridad, confidencialidad y disponibilidad. Este proceso incluye la implementación de políticas de acceso, configuración de cortafuegos, actualizaciones de software, y uso de herramientas de seguridad integradas, garantizando un entorno robusto y protegido para los usuarios y sus datos.

Actividad: Realiza prácticas de configuración de seguridad en los sistemas operativos. Aplique la Guía de Seguridad con Windows 10 y 11 visitando el siguiente link:

Link: https://youtube.com/playlist?list=PLT0koQYMKV1ioayNc02Wnjv5X2wwBEzqf

El instructor orientará la forma como se realizará cada una de las actividades propuestas.

- ✓ Configurar el Firewall de Windows.
- ✓ Configurar Windows defender.

- ✓ Configurar Windows Update
- ✓ Navegador seguro SmartScreen
- ✓ Windows defender Offline Scanner.
- ✓ Configuración de información en redes sociales

En grupos de trabajo colaborativo de tres (3) aprendices se debe realizar un video del procedimiento aplicado para la parametrización de Seguridad en Windows, que será socializado según retroalimentación del Instructor.

- **Descripción de la actividad:** El Aprendiz realizará en forma práctica la parametrización de la seguridad en el sistema operativo Windows.
- **Ambiente requerido:** Ambiente de aprendizaje presencial.
- **Estrategias o técnicas didácticas activas: Aprendizaje cooperativo**: Los Aprendices trabajan en pequeños grupos, apoyándose mutuamente para realizar las practicas requeridas en la parametrización de la seguridad del sistema operativo.
- **Materiales de formación:** 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 – Video Beam, marcadores borrables, Tablero.
- **Material de apoyo:** https://youtube.com/playlist?list=PLT0koQYMKV1ioayNc02Wnjv5X2wwBEzqf
- **Evidencias de aprendizaje:** Video parametrización del sistema operativo**.**
- **Instrumento de evaluación:** Lista de chequeo de producto.
- **Duración de la actividad:** 15 horas**.**

3.4 Actividades de transferencia del conocimiento.

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

Se recomienda que en Grupo de tres (3) personas, los aprendices expliquen en forma práctica 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

<u>Lineamientos para la entrega del producto</u>

- **Producto para entregar:** En los mismos grupos anteriores que expusieron, deben por favor:

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.
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.

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).

Contenido: Archivos de las Copias de Seguridad realizados.

Para hacer el envío de la evidencia remítase al área de la actividad correspondiente y acceda al espacio dispuesto para dicho proceso.

- **Descripción de la actividad:** El Aprendiz realizará en forma práctica la socialización acerca del tema copias de seguridad.
- **Ambiente requerido:** Ambiente de aprendizaje presencial.
- **Estrategias o técnicas didácticas activas: Simulaciones**: Los aprendices recrean situaciones reales en un entorno seguro, que le permitan tomar decisiones.
- **Materiales de formación:** 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 – Video Beam, marcadores borrables, Tablero.
- **Material de apoyo:**
  https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf
  https://www.youtube.com/watch?v=oFXVK8qS2xs
- **Evidencias de aprendizaje:** Copia de seguridad en Windows
- **Instrumento de evaluación:** Evaluación de desempeño y producto.
- **Duración de la actividad:** 10 horas**.**

4. ACTIVIDADES DE EVALUACIÓN

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

Fase del proyecto formativo	Actividad del proyecto formativo	Actividad de Aprendizaje	Evidencias de Aprendizaje	Criterios de Evaluación	Técnicas e Instrumentos de Evaluación
	Clasificar la infraestructura	3.1.1 Actividad de Reflexión. 3.2.1 Actividad de contextualización. 3.3.1. Comprender la importancia de la	No aplica para evidencia de aprendizaje. No aplica para evidencia de aprendizaje. **Desempeño:**	No aplica criterio de evaluación. No aplica criterio de evaluación. Aplica controles de seguridad según	**Debate.** No aplica instrumento de evaluación. **Método de indagación**. No aplica instrumento de evaluación. **Aprendizaje cooperativo.**

Ejecución	de red y equipos informáticos y solicitudes de servicio técnico presente en el entorno de trabajo	planificación de la información con enfoque en ciberseguridad. 3.3.2. Explicar los conceptos clave acerca de la seguridad de la información, y la legislación vigente sobre delitos informáticos en Colombia. 3.3.3. Analizar aspectos relevantes acerca de la protección de datos personales y los derechos de autor, de acuerdo al enfoque de la aplicación de buenas prácticas en su gestión. 3.3.4. Analizar el alcance de la normatividad vigente en relación con la seguridad de la información en Colombia. 3.3.5. Evaluar los servicios de Internet que permitan la investigación y el análisis crítico de los diferentes procesos, de acuerdo con las necesidades de la organización. 3.3.6. Realizar la parametrización de Seguridad en Windows 10 o 11 según procedimiento técnicos 3.4.1. Planificar copias de seguridad según procedimientos técnicos y criterios de seguridad.	"Socialización actividades Evidencia Integral de Seguridad Informática" **Desempeño:** Socialización: Legislación sobre delitos informático en Colombia. **Producto:** Video explicativo Habeas Data **Desempeño:** **Informe técnico:** Planificar copias de seguridad según procedimientos técnicos y criterios de seguridad. (configuración del firewall, antivirus, reglas de conexión). **Producto:** Archivos de las Copias de Seguridad creadas y etiquetadas. Video y Sistema Operativo (EndPoint) protegido: **Desempeño** Implementación de Herramientas del Sistema Operativo para Endurecer la Seguridad del Equipo **Producto**: Copia de seguridad en Windows	normativa, necesidades y restricciones de acceso a la información Aplica controles de seguridad según normativa, necesidades y restricciones de acceso a la información Propone procesos de mejora en el manejo de la información con base a la normativa vigente. Gestiona las copias de seguridad y recuperación, según lineamientos establecidos por la empresa. Implementa herramientas para mejorar la Seguridad en los equipos de cómputo con SO Windows. Propone procesos de mejora en el manejo de la información con base a la normativa vigente.	Lista de chequeo de desempeño y producto. **Exposición.** **Lista de chequeo de desempeño.** Exposición Legislación delitos informáticos en Colombia. **Debate.** **Video_ Habeas Data** Lista de chequeo de producto. **Estudio de caso.** **Informe técnico sobre copias de seguridad.** Evidencias de desempeño Lista de Chequeo de desempeño. **Talleres prácticos.** **Informe en Pdf actividad servicios de internet.** Lista de chequeo de desempeño. **Aprendizaje cooperativo** Video parametrización del sistema operativo. Lista de chequeo de producto. **Simulación** Copia de seguridad en Windows. Lista de chequeo de desempeño y producto.

5. GLOSARIO DE TÉRMINOS

Ciberseguridad: La seguridad informática, también conocida como ciberseguridad, es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, y especialmente la información contenida en una computadora o circulante a través de las redes de computadoras.

Confidencialidad: Consiste en que la información no debe llegar a personas u organizaciones que no estén autorizadas.

Controles de seguridad: La virtualización utiliza el software para imitar las características del hardware y crear un sistema informático virtual. Esto permite a las organizaciones de TI ejecutar más de un sistema virtual, y múltiples sistemas operativos y aplicaciones, en un solo servidor.

Disponibilidad: La información debe poder ser accedida en cualquier momento que se requiera, por las personas autorizadas

Integridad: La información debe mantenerse íntegra y sin modificaciones por parte de personas no autorizadas.

Malware: Se relaciona con software dañino que afecta los dispositivos, de lograrse materializar se podría generar perdida de información, incluso monitorear las acciones que se estén haciendo en el dispositivo de forma silenciosa sin que el usuario se entere.

Phishing: Consiste en suplantar la identidad de una persona o una entidad, la principal vía de ataque es el envío de emails, por eso la importancia de verificar los remitentes, enlaces y archivos adjuntos que parezcan sospechosos o de dudosa procedencia.

6. REFERENTES BILBIOGRÁFICOS

- Del Poder Judicial, A. V. (2017, April 07). Análisis e Interpretación de los Controles - Anexo "A" ISO 27001. Youtube. Retrieved from https://www.youtube.com/watch?v=YlMxx-LbUWM
- Guía para la implementación del Principio de Responsabilidad Demostrada (Accountability) | Superintendencia de Industria y Comercio. (2022, December 07). Retrieved from https://www.sic.gov.co/noticias/guia-para-la-implementacion-del-principio-de-responsabilidad-demostrada
- Informática pa novatos. (2022, december 07). Curso de seguridad doméstica con Windows 10. Youtube. Retrieved from https://www.youtube.com/playlist?list=PLT0koQYMKV1ioayNc02Wnjv5X2wwBEzqf
- Instituto nacional de ciberseguridad. (2018). Copias de Seguridad. "Una guía de aproximación para el empresario". Retrive from https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf
- Incibe. Protege tu empresa – Blog - (2008, agosto) – «Como Pedro por su casa»: ¿a quién dejas acceder a tus sistemas? (1/2) https://www.incibe.es/protege-tuempresa/blog/como-pedro-por-su-casa-01
- Incibe. Protege tu empresa – Blog - (2008, agosto) – «Como Pedro por su casa»: ¿a quién dejas acceder a tus sistemas? (2/2) https://www.incibe.es/protege-tuempresa/blog/como-pedro-por-su-casa-02
- Quanti Media Group. (2021, November 04). ¿Qué es la norma ISO 27001? | Quanti Lightboard Series. Youtube. Retrieved from https://www.youtube.com/watch?v=iZNUDnf7QgQ
- Ti, L. C. (2020, October 12). ESTRUCTURA DE LA NORMA ISO 27001 2013. Youtube. Retrieved from https://www.youtube.com/watch?v=NoFccA90D7E

7. CONTROL DEL DOCUMENTO

	Nombre	Cargo	Dependencia	Fecha
Autor (es)	**Jaime Rodrigo Saucedo** **Adriana Patricia Salazar**	**Instructor** **Instructora**	**CEAI**	**2/07/2024**

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

	Nombre	Cargo	Dependencia	Fecha	Razón del Cambio
Autor (es)					
Autor					