Ciberseguridad

Guía para el profesor

Clave PTTI2211

INSTITUTO PROFESIONAL TECMILENIO

Contenido

Datos generales

Nombre: Ciberseguridad

Nivel: Profesional Asociado

Modalidad: Apilable

Clave: PTTI2212

Competencia global

Propone técnicas y herramientas de gestión de ciberseguridad en los diferentes contextos profesionales en tecnologías de la información.

Competencias esenciales

- Enfoque sistémico.

Introducción al certificado

En esta experiencia de aprendizaje realizarás un viaje esencial hacia la comprensión y la aplicación de prácticas de seguridad en el vasto y dinámico mundo digital. En un entorno donde la tecnología evoluciona a un ritmo acelerado, y con ello, las amenazas a la seguridad de los datos y sistemas, la necesidad de profesionales cualificados en ciberseguridad nunca ha sido tan crítica. Este certificado está diseñado no solo para equiparte con conocimiento técnico en ciberseguridad, sino también para inculcar actitudes y valores que son imprescindibles en la protección de la información en la era digital.

Al adentrarte en este programa, estudiarás desde los fundamentos de la ciberseguridad hasta las tendencias emergentes que modelan el futuro de la tecnología de la información y la protección de datos. A través de una cuidadosa selección de temas que incluyen la gestión de incidentes de seguridad, la explotación de vulnerabilidades, la seguridad en redes y la protección de datos en la nube, desarrollarás una comprensión profunda de los desafíos y soluciones en el campo de la ciberseguridad.

La utilidad de los conocimientos adquiridos mediante este certificado se extiende más allá de la teoría; estarás preparado para aplicar lo aprendido en situaciones reales, protegiendo activos digitales contra ataques cibernéticos, identificando vulnerabilidades en sistemas y redes, y asegurando que las prácticas de privacidad y protección de datos se mantengan en la vanguardia de las operaciones organizacionales. Además, el curso no solo se enfoca en la adquisición de habilidades técnicas, sino que también fomenta una mentalidad crítica y ética, indispensable para navegar en el complejo paisaje de la ciberseguridad con integridad y responsabilidad.

Los valores promovidos a lo largo del curso, como el compromiso ético, la responsabilidad profesional y el respeto por la privacidad y la protección de datos, son fundamentales para el desarrollo de profesionales que no solo sean competentes desde el punto de vista técnico, sino también respetuosos de las implicaciones éticas de su trabajo. La ciberseguridad no se trata solo de proteger sistemas y datos, se trata de proteger a las personas y preservar la confianza en nuestras instituciones y tecnologías.

Además, este certificado de ciberseguridad, que no solo se alinea con las más actuales necesidades del mercado, también te preparará para certificarte en Cisco Networking Academy. A lo largo del curso, cada tema que estudiarás ha sido cuidadosamente diseñado para reforzar las habilidades y los conocimientos requeridos para obtener esta certificación. Al dominar estos contenidos, no solo estarás

capacitado para enfrentarte a los desafíos prácticos del campo, sino que también estarás preparado para cumplir con los criterios exigidos por uno de los programas de certificación reconocidos en la industria de la ciberseguridad.

Información general

Metodología

Un certificado **apilable** se ha diseñado con la finalidad de impartirse a través de una metodología de flexibilidad para el aprendedor, ya que desde su diseño está estructurado para poder impartirse a través de una modalidad autodirigida, o bien, en acompañamiento de un docente con experiencia en el ámbito laboral.

La experiencia de los **certificados apilables** promueve la interacción virtual entre aprendedores localizados en diferentes campus de la Universidad Tecmilenio como una forma de enriquecer su formación, contrastando la realidad de su ciudad o región con la de otros compañeros cuando así se lo permita la disponibilidad de este, considerando que podrá tener a su disposición la experiencia docente que enriquecerá su conocimiento.

Sin embargo, se encuentran diseñados para ofrecer una experiencia autodirigida para aquellos aprendedores que por sus necesidades tengan que ajustar sus propios tiempos.

I. **Apilabilidad:** modelo nuevo de impartición que puede realizarse bajo conducción de un académico o de manera autodirigida (el diseño del certificado tiene la flexibilidad de poder impartirse en ambos casos).
II. **Duración:** un mes, equivalente a cuatro semanas efectivas.
III. **Bajo conducción de un académico:** el contenido es impartido por un docente en sesiones sincrónicas o grabadas, en las cuales se abordarán los principales conceptos asociados a las unidades de aprendizaje. El profesor ofrece seguimiento y apoyo a los aprendedores. Estas sesiones virtuales sincrónicas de 9 horas a través de una herramienta tecnológica de videoconferencia, distribuidas de 2 a 3 sesiones por semana (de 3 a 4.5 horas por sesión). La asistencia a estas sesiones de videoconferencia es muy importante, pero en caso de no poder asistir, el aprendedor tiene la posibilidad de revisar la sesión grabada.
IV. **Autodirigido:** son cursos asincrónicos sin un profesor asignado, con el contenido disponible a través de la plataforma de cursos (Canvas u otra). Los aprendedores disponen de todos los materiales para avanzar en su proceso de aprendizaje, y la retroalimentación y evaluación se realiza entre pares o de forma automatizada en los casos que la plataforma lo permita.

Bibliografía y software

Para cada módulo se sugiere material bibliográfico opcional, así como el *software* correspondiente.

Bibliografía opcional

- Ackerman, P. (2021). *Industrial Cybersecurity: Efficiently Monitor the Cybersecurity Posture of Your ICS Environment* (2ª ed.). Reino Unido: Packt. Recuperado de https://eds.p.ebscohost.com/eds/detail/detail?vid=1&sid=355a0588-8af9-4ef6-9c4c-6adb0009ea7c%40redis&bdata=JkF1dGhUeXBlPXNoaWImbGFuZz1lcyZzaXRlPWVkcy1saXZl#AN=3028133&db=nlebk
- Arroyo, D., Gayoso, V., y Hernández, L. (2020). *Ciberseguridad*. España: CSIC. Recuperado de https://eds.p.ebscohost.com/eds/detail/detail?vid=5&sid=355a0588-8af9-4ef6-9c4c-6adb0009ea7c%40redis&bdata=JkF1dGhUeXBlPXNoaWImbGFuZz1lcyZzaXRlPWVkcy1saXZl#AN=2732926&db=nlebk
- Gupta, C., y Goyal, K. (2020). *Cybersecurity: A Self-Teaching Introduction*. Mercury Learning and Information: Estados Unidos. Recuperado de https://eds.p.ebscohost.com/eds/detail/detail?vid=1&sid=09985b56-5789-4847-8df9-

f70aacc8cce0%40redis&bdata=JkF1dGhUeXBlPXNoaWImbGFuZz1lcyZzaXRlPWVkcy1saXZl#AN=2399513&db=nlebk

Software

- Oracle VirtualBox. (s.f.). *Welcome to VirtualBox.org!* Recuperado de https://www.virtualbox.org/
- Python. (s.f.). *Download the latest version for Windows*. Recuperado de https://www.python.org/downloads/

Evaluación

La evaluación consta de lo siguiente:

1. Actividades que retoman el contenido conceptual de los temas de la semana.

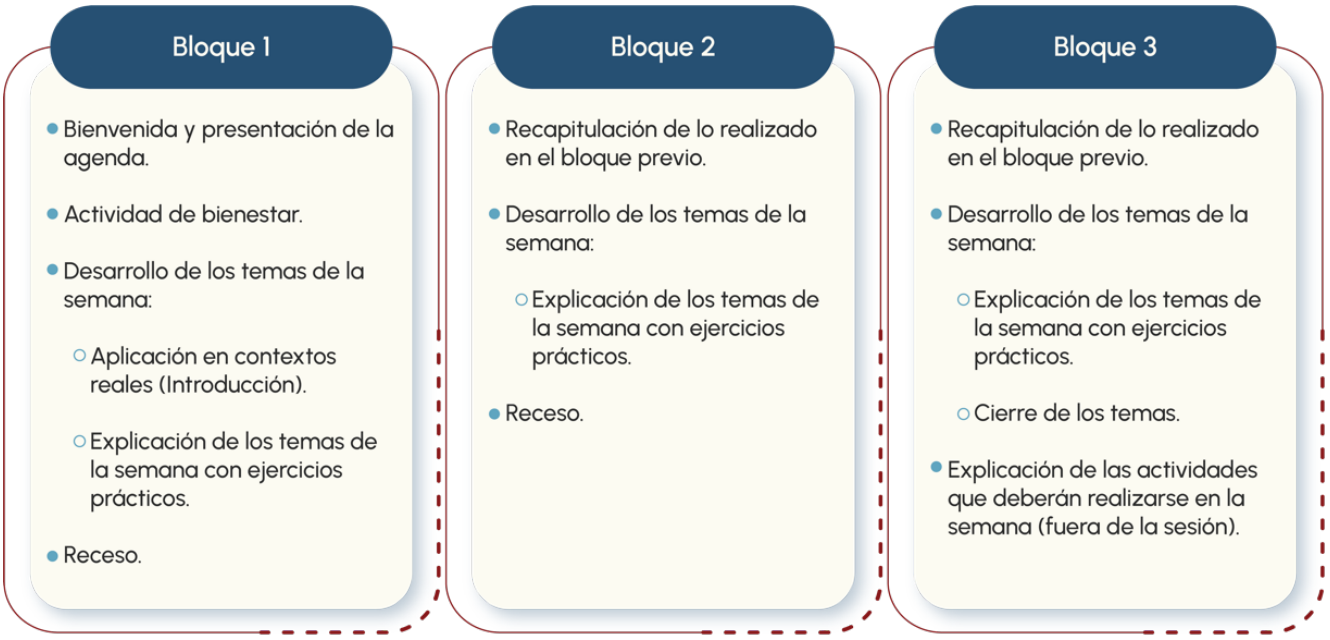
2. Proyecto con el que el participante demostrará que adquirió las habilidades y los conocimientos requeridos para acreditar el certificado. Dicho proyecto se divide en dos fases (avance y entrega final).

A continuación, puedes revisar el detalle de la evaluación:

Evaluable	Ponderación
Actividad I	10%
Avance del proyecto	30%
Actividad II	10%
Entrega final del proyecto	40%
Examen final	10%
Total	100%

Estructura de las sesiones

Las sesiones se dividen en tres bloques. Estas son las actividades que se recomienda realizar:



Antes de acudir a una sesión, es necesario que leas las explicaciones, ya que te proporcionarán los fundamentos teóricos de los temas. De igual manera, se requiere que revises las lecturas y los videos obligatorios.

Durante las sesiones sincrónicas, el docente da una breve explicación del tema, resuelve dudas y comparte las instrucciones de lo que se debe realizar fuera de dichas sesiones.

Avance y entrega final del proyecto

Las actividades, avance (fase I) y entrega final del proyecto (fase II) se han diseñado para realizarse de manera individual.

Como una forma de promover el dinamismo y la interacción de los participantes en distintos formatos, durante las sesiones, el profesor alterna intervenciones individuales, plenarias y grupales que enriquecen tus puntos de vista y, al mismo tiempo, te dan la oportunidad de presentar tus ideas y posturas en torno a los temas de clase.

Para la interacción de los participantes, se utilizan las funcionalidades de la herramienta de colaboración que permiten la creación de salas virtuales interactivas, en donde puedes compartir pantallas, documentos, videos y audios.

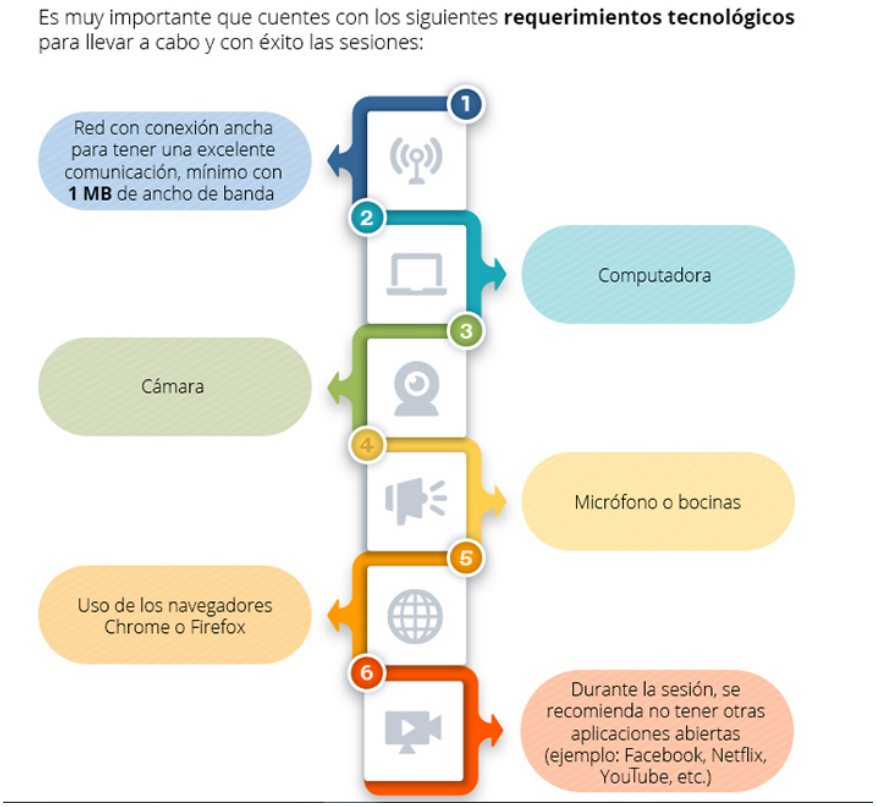
El resultado de todas las actividades, avance y entrega final del proyecto deberá entregarse a través de la plataforma tecnológica para su revisión y evaluación por parte del docente.

Es muy importante que revises el esquema de evaluación y los criterios que utilizará el docente para otorgarte una calificación. Lo anterior con la intención de que desde el inicio de la semana tengas claro el nivel de complejidad y esfuerzo que requieres para realizar las entregas semanales y garantizar tu éxito dentro del certificado.

En caso de tener dudas sobre alguna de las actividades integradoras y las fases del proyecto o del contenido, puedes contactar a tu docente a través de los medios que te indique.

Sesiones virtuales

Para la transmisión de las sesiones se utiliza una herramienta de videoconferencias. Con el fin de mejorar la calidad de dichas interacciones, se recomienda lo siguiente.



Tutoriales

Para asegurar que aproveches al máximo tu experiencia educativa en esta modalidad, te recomendamos que sigas al pie de la letra las indicaciones de tu docente, así como revisar estos tutoriales:

- ¿Cómo entrar a Canvas?
- ¿Cómo consulto mis calificaciones?
- ¿Cómo entrego mis tareas?
- ¿Cómo ingreso a la plataforma de multipresencia virtual?
- Tutoriales de Canvas para aprendedores
- ¿Cómo evalúo el desempeño de mi red?

¡Te deseamos mucho éxito!

Calendario de entregas

Semana	Tema	Actividad integradora	Proyecto
1	Tema 1. Fundamentos de ciberseguridad Tema 2. Tipos de datos Tema 3. Incidentes de seguridad Tema 4. Ataques y técnicas en ciberseguridad Tema 5. Explotación de vulnerabilidades	**Actividad I**	
2	Tema 6. Protección de datos y privacidad Tema 7. Ciberseguridad organizacional Tema 8. Cultura de seguridad en la organización Tema 9. Fundamentos de seguridad en la nube Tema 10. Seguridad de datos en la nube - Parte I		**Avance del proyecto**
3	Tema 11. Seguridad de datos en la nube - Parte II Tema 12. Seguridad en desarrollo de software - Parte I Tema 13. Seguridad en desarrollo de software - Parte II Tema 14. Seguridad en aplicaciones web Tema 15. Seguridad en APIs	**Actividad II**	
4	Tema 16. Seguridad en redes Tema 17. Seguridad perimetral Tema 18. Evaluación de riesgos Tema 19. Normativas y estándares de ciberseguridad Tema 20. Tendencias y futuro de la ciberseguridad		**Entrega final del proyecto**

Temario

Tema 1. Fundamentos de ciberseguridad
1.1 Introducción a la ciberseguridad
1.2 Conceptos básicos de ciberseguridad
1.3 Importancia de la ciberseguridad en la actualidad

Tema 2. Tipos de datos
2.1 Datos personales
2.2 Datos organizacionales
2.3 Clasificación y gestión de datos

Tema 3. Incidentes de seguridad
3.1 Identificación de incidentes de seguridad
3.2 Notificación y manejo de incidentes

Tema 4. Ataques y técnicas en ciberseguridad
4.1 Análisis de ataques cibernéticos
4.2 Identificación y clasificación de ataques
4.3 Técnicas de análisis forense
4.4 Métodos de infiltración
4.5 Ingeniería social y ataques de *phishing*

Tema 5. Explotación de vulnerabilidades
5.1 Vulnerabilidades de seguridad y *exploits*
5.2 Identificación de vulnerabilidades comunes
5.3 Exploración y explotación de vulnerabilidades

Tema 6. Protección de datos y privacidad
6.1 Seguridad de dispositivos y redes
6.2 Configuración segura de dispositivos
6.3 Seguridad de redes inalámbricas y cableadas
6.4 Respaldo y recuperación de datos

Tema 7. Ciberseguridad organizacional
7.1 Tecnologías y dispositivos de ciberseguridad
7.2 Cortafuegos, antivirus y sistemas de detección de intrusiones
7.3 Gestión de políticas de seguridad
7.4 Concientización y entrenamiento de empleados

Tema 8. Cultura de seguridad en la organización
8.1 Enfoque de ciberseguridad de Cisco
8.2 Soluciones de seguridad de Cisco
8.3 Integración de tecnologías de seguridad

Tema 9. Fundamentos de seguridad en la nube
9.1 Modelos de servicio en la nube
9.2 Riesgos y beneficios de la adopción de la nube
9.3 Estrategias de seguridad en la nube

Tema 10. Seguridad de datos en la nube - Parte I
10.1 Gestión de identidad y acceso en entornos de nube
10.2 Infraestructura como código (IaC)

Tema 11. Seguridad de datos en la nube - Parte II
11.1 Seguridad: mejores prácticas para asegurar entornos en la nube utilizando IaC

11.2 Seguridad de contenedores y orquestación

Tema 12. Seguridad en desarrollo de *software* - Parte I
12.1 Principios de desarrollo seguro
12.2 Pruebas de seguridad de aplicaciones

Tema 13. Seguridad en desarrollo de *software* - Parte II
13.1 Mejores prácticas de seguridad
13.2 Autenticación y autorización

Tema 14. Seguridad en aplicaciones web
14.1 Vulnerabilidades comunes en aplicaciones web
14.2 Protección contra ataques web
14.3 Protección contra ataques de inyecciones y XSS

Tema 15. Seguridad en API
15.1 Seguridad en API y servicios web
15.2 Autenticación, autorización y protección contra ataques a API

Tema 16. Seguridad en redes
16.1 Diseño de redes seguras
16.2 Segmentación de redes
16.3 Redes privadas virtuales (VPN) y túneles seguros

Tema 17. Seguridad perimetral
17.1 Fundamentos de seguridad perimetral
17.2 *Firewalls* y filtros de contenido
17.3 Detección y prevención de intrusiones en la red

Tema 18. Evaluación de riesgos
18.1 Identificación y análisis de riesgos
18.2 Evaluación cuantitativa y cualitativa
18.3 Cumplimiento normativo
18.4 Desarrollo de un plan de respuesta

Tema 19. Normativas y estándares de ciberseguridad
19.1 Auditoría y cumplimiento regulatorio
19.2 Derechos de autor y licencias de *software*
19.3 Cumplimiento normativo y regulaciones de privacidad
19.4 Marcos jurídicos y normativas internacionales

Tema 20. Tendencias y futuro de la ciberseguridad
20.1 Evolución de las amenazas y tecnologías de seguridad
20.2 Desafíos emergentes en ciberseguridad y oportunidades de carrera

Preguntas más frecuentes

¿En dónde o a quién le reporto un error detectado en el contenido?

Lo puedes reportar a través del botón “Mejora tu curso”, también puedes compartir sugerencias para el contenido y actividades del certificado.

¿Quién me informa de la cantidad de sesiones y el tiempo de cada sesión en las semanas?

El coordinador docente te debe proporcionar esta información.

¿En qué semanas se aplican los exámenes parciales y el examen final?

Consulta con tu coordinador docente los calendarios de acuerdo con la modalidad de impartición.

¿Tengo que capturar las calificaciones en Banner y en la plataforma educativa?

Sí, es importante que captures las calificaciones en la plataforma para que los participantes estén informados de su avance y reciban retroalimentación de parte tuya de todo lo que realizan en esta experiencia educativa. En Banner es el registro oficial de las calificaciones de los participantes.

Guía para las sesiones

Semana 1 (temas 1-5)

Bloque 1

Actividad	Descripción	Duración
Bienvenida y presentación de la agenda.	El profesor se presenta ante el grupo y da una breve introducción de los temas que se abordarán.	5 minutos.
Práctica de bienestar.	El profesor impartidor seleccionará alguna práctica del banco anexo al final de este documento para compartirla en un foro de discusión y explicarla en la sesión. Se recomienda utilizar una diferente por semana.	5 minutos.
Desarrollo de los temas de la semana: o **Aplicación en contextos reales (introducción).** o **Explicación de los temas de la semana con ejercicios prácticos.**	El profesor explicará a los participantes los contenidos con ejercicios prácticos.	40 minutos.
Receso.	Se brindará un espacio de receso para que el participante lo utilice a su beneficio.	10 minutos.

Bloque 2

Actividad	Descripción	Duración
Recapitulación de lo realizado en el bloque previo.	El profesor recapitulará de manera dinámica lo realizado en el bloque previo.	5 minutos.
Desarrollo de los temas de la semana: o **Explicación de los temas de la semana con ejercicios prácticos.**	El profesor explicará a los participantes los contenidos con ejercicios prácticos.	45 minutos.
Receso.	Se brindará un espacio de receso para que el participante lo utilice a su beneficio.	10 minutos.

Bloque 3

Actividad	Descripción	Duración
Recapitulación de lo realizado en el bloque previo.	El profesor recapitulará de manera dinámica lo realizado en el bloque previo.	5 minutos.
Desarrollo de los temas de la semana: o **Explicación de los temas de la semana con ejercicios prácticos.** o **Cierre de los temas.**	El profesor explicará a los participantes los contenidos con ejercicios prácticos y realizará un cierre de los temas correspondientes.	35 minutos.
Explicación de la actividad integradora 1. **Explicación del proyecto, con enfoque en la fase I.**	Se explicará a los participantes en qué consiste la actividad integradora 1, la cual se entrega en la semana 1. Se explicará a los participantes en qué consiste el proyecto de manera general, enfocándose en la fase 1, la cual deberán entregar en la semana 2.	10 minutos.

Notas para el profesor impartidor correspondientes a la explicación del tema 1, la cual debe considerar la realización de ejercicios prácticos durante la sesión.

Al profesor impartidor, se le recomienda lo siguiente:

1. Comenzar la clase con una discusión sobre la importancia de la ciberseguridad en el mundo actual, utilizando ejemplos de noticias recientes sobre ciberataques.
2. Explicar los conceptos básicos de ciberseguridad: amenazas, vulnerabilidades y ataques. Utilizar el cubo de McCumber para ilustrar los principios fundamentales.
3. Presentar estadísticas recientes sobre el impacto económico de los ciberataques para resaltar la relevancia del tema.
4. Incluir actividades interactivas donde los aprendedores identifiquen posibles amenazas y vulnerabilidades en escenarios hipotéticos.
5. Describir cómo ha evolucionado la ciberseguridad desde sus inicios hasta la actualidad, destacando la importancia de adaptarse a las nuevas amenazas.
6. Explicar los conceptos de confidencialidad, integridad y disponibilidad (CID) y su importancia en la protección de la información.
7. Utilizar casos reales de incidentes de seguridad, como el ataque de *ransomware* WannaCry, para ilustrar la importancia de las medidas de ciberseguridad.
8. Proporcionar una discusión detallada sobre cómo las organizaciones pueden implementar estrategias de ciberseguridad efectivas.

9. Animar a los aprendedores a reflexionar sobre cómo las prácticas de ciberseguridad pueden integrarse en su vida diaria y en sus futuras profesiones.

10. Concluir con una revisión de los puntos clave y preguntas para discusión o reflexión sobre el material cubierto.

11. Animar a los aprendedores a revisar el capítulo 1 (Amenazas, vulnerabilidades y ataques) del libro de apoyo para profundizar en el aprendizaje, así como revisar el módulo 1 del curso de Cisco Academy.

Notas para el profesor impartidor correspondientes a la explicación del tema 2, la cual debe considerar la realización de ejercicios prácticos durante la sesión.

Al profesor impartidor, se le recomienda lo siguiente:

1. Comenzar la clase explicando la importancia de los datos y cómo su manejo adecuado es fundamental para la ciberseguridad, utilizando ejemplos de diferentes tipos de datos personales y organizacionales.

2. Describir los diferentes tipos de datos personales, como identificadores directos, datos biométricos, datos financieros, datos de localización, información sobre salud y datos demográficos, y explicar cómo cada tipo puede ser vulnerable a diferentes amenazas.

3. Realizar una actividad en la que los aprendedores identifiquen ejemplos de datos personales en diferentes contextos (ej. redes sociales, servicios bancarios, dispositivos de salud) y discutan cómo protegerlos.

4. Explicar la importancia de la protección de datos a nivel organizacional, incluyendo datos transaccionales, propiedad intelectual y datos financieros. Utilizar ejemplos de cómo la pérdida de estos datos puede impactar una organización.

5. Describir las medidas técnicas y administrativas que pueden implementarse para proteger los datos organizacionales, como el cifrado, los controles de acceso basados en roles y las auditorías de seguridad.

6. Introducir la clasificación de datos y la gestión de la seguridad de los datos. Explicar cómo la clasificación ayuda a priorizar la protección de los datos según su sensibilidad y valor.

7. Incluir una actividad práctica en la que los aprendedores clasifiquen diferentes tipos de datos y propongan medidas de seguridad adecuadas para cada categoría.

8. Discutir la importancia de una cultura de ciberseguridad dentro de una organización, incluyendo la educación y capacitación de empleados sobre las mejores prácticas de ciberseguridad.

9. Utilizar casos reales de brechas de datos para ilustrar la importancia de las políticas de seguridad de la información y cómo pueden prevenir incidentes.

10. Concluir con una revisión de los puntos clave y preguntas para discusión o reflexión sobre el material cubierto, animando a los aprendedores a pensar en cómo aplicar estos conceptos en sus futuros roles profesionales.

11. Animar a los aprendedores a revisar el capítulo 2 (Dominios de la ciberseguridad) del libro de apoyo para profundizar en el aprendizaje, así como revisar el módulo 1.2 del curso de Cisco Academy.

Notas para el profesor impartidor correspondientes a la explicación del tema 3, la cual debe considerar la realización de ejercicios prácticos durante la sesión.

Al profesor impartidor, se recomienda lo siguiente:

1. Comenzar la clase definiendo qué es un incidente de seguridad y su importancia en el contexto de la ciberseguridad, utilizando ejemplos de incidentes recientes.

2. Describir las fases de respuesta en incidentes de seguridad: identificación, notificación y manejo. Explicar cada fase en detalle y su relevancia.

3. Explicar cómo identificar incidentes de seguridad, destacando las herramientas y técnicas como el monitoreo y análisis de *logs*, sistemas de gestión de información y eventos de seguridad (SIEM) y evaluaciones de vulnerabilidad.

4. Incluir una actividad en la que los aprendedores practiquen la identificación de incidentes en escenarios ficticios que permita la propuesta de soluciones.

5. Describir la importancia de la notificación de incidentes tanto dentro de la organización como a clientes, socios y reguladores. Explicar cómo un sistema automatizado puede optimizar este proceso.

6. Explicar el manejo efectivo de incidentes, incluyendo las etapas de contención, erradicación y recuperación. Utilizar ejemplos para ilustrar cada etapa.

7. Realizar una actividad práctica en la que los aprendedores desarrollen un plan de respuesta a un incidente de seguridad hipotético, incluyendo la identificación, notificación y manejo del incidente.

8. Discutir el impacto económico y reputacional de los incidentes de seguridad y la importancia de una respuesta rápida y efectiva para minimizar daños.

9. Utilizar casos reales de incidentes de seguridad para ilustrar las mejores prácticas en la respuesta a incidentes y cómo las organizaciones pueden aprender de estos eventos para mejorar sus estrategias de ciberseguridad.

10. Concluir con una revisión de los puntos clave y preguntas para discusión o reflexión sobre el material cubierto, animando a los aprendedores a pensar en cómo pueden aplicar estos conceptos en sus futuros roles profesionales.

11. Animar a los aprendedores a revisar el capítulo 4 (Soluciones y buenas prácticas) del libro de apoyo para profundizar en el aprendizaje, así como revisar el módulo 1.4 del curso de Cisco Academy.

Notas para el profesor impartidor correspondientes a la explicación del tema 4, la cual debe considerar la realización de ejercicios prácticos durante la sesión.

Al profesor impartidor, se le recomienda lo siguiente:

1. Comenzar la clase explicando la importancia de entender los ataques cibernéticos en el contexto actual y cómo estos pueden afectar tanto a individuos como a organizaciones.

2. Describir los diferentes tipos de atacantes (aficionados, *hackers* y hackers organizados) y sus motivaciones. Utilizar ejemplos reales para ilustrar cada tipo.

3. Explicar el ciclo de vida de un ciberataque (*cyber kill chain*), desde el reconocimiento hasta el comando y control. Utilizar diagramas para visualizar cada etapa.

4. Realizar una actividad en la que los aprendedores analicen un ciberataque hipotético, identificando las fases y proponiendo medidas de defensa en cada etapa.

5. Describir los principales tipos de *malware* (virus, gusanos, troyanos, ransomware, *spyware*, phishing, *backdoors*, *keyloggers* y bots) y sus características. Utilizar ejemplos para mostrar cómo operan.

6. Explicar las técnicas de análisis forense digital y su importancia en la investigación de incidentes de seguridad. Utilizar un caso de estudio para ilustrar el proceso forense.

7. Realizar una actividad práctica en la que los aprendedores apliquen técnicas de análisis forense para investigar un incidente de seguridad simulado.

8. Describir los métodos de infiltración como los ataques de Denegación de Servicio (DoS), el envenenamiento SEO y las botnets. Explicar cómo estos métodos pueden comprometer la seguridad de las redes y sistemas.

9. Explicar la ingeniería social y los ataques de phishing. Utilizar ejemplos de correos electrónicos de phishing para ilustrar cómo los atacantes manipulan a las víctimas.

10. Discutir las mejores prácticas para prevenir ataques de ingeniería social y phishing, incluyendo la educación y concienciación de los empleados.

11. Concluir con una revisión de los puntos clave y preguntas para discusión o reflexión sobre el material cubierto, animando a los aprendedores a pensar en cómo pueden aplicar estos conocimientos en sus futuros roles profesionales.

12. Animar a los aprendedores a revisar el capítulo 1 (Amenazas, vulnerabilidades y ataques) del libro de apoyo para profundizar en el aprendizaje, así como revisar el módulo 2.1 del curso de Cisco Academy.

Notas para el profesor impartidor correspondientes a la explicación del tema 5, la cual debe considerar la realización de ejercicios prácticos durante la sesión.

Al profesor impartidor, se le recomienda lo siguiente:

1. Comenzar la clase explicando qué son las vulnerabilidades de seguridad, utilizando ejemplos recientes y relevantes para ilustrar su impacto potencial.

2. Describir los diferentes tipos de vulnerabilidades en software y *hardware*, explicando cómo los *exploits* aprovechan estas vulnerabilidades. Utilizar casos conocidos para hacer más tangible la explicación.

3. Explicar el concepto de "exploit de día cero" y su peligrosidad. Ilustrar con ejemplos de exploits de día cero famosos y las consecuencias de su explotación.

4. Realizar una actividad en la que los aprendedores identifiquen vulnerabilidades en un sistema simulado y discutan posibles exploits que podrían ser utilizados.

5. Explicar las técnicas de ocultación y escalada de privilegios utilizadas por los atacantes para evadir detección y obtener control total sobre el sistema. Utilizar diagramas para visualizar estos conceptos.

6. Describir las estrategias para la identificación de vulnerabilidades comunes, incluyendo el monitoreo continuo, la educación y capacitación de empleados y el uso de herramientas automatizadas.

7. Realizar una actividad práctica en la que los aprendedores realicen el análisis de vulnerabilidades para identificar fallos en un sistema simulado. Revisar el video correspondiente a los temas 1-5.

8. Explicar los métodos de exploración y explotación de vulnerabilidades, diferenciando entre exploración pasiva y activa. Utilizar ejemplos para ilustrar cómo estas técnicas se aplican en la práctica.

9. Presentar un caso de estudio en el que se identifiquen y clasifiquen vulnerabilidades en un Sistema de Gestión Hospitalaria (SGH) y se desarrollen estrategias de mitigación para mejorar la seguridad del sistema.

10. Concluir con una revisión de los puntos clave y preguntas para discusión o reflexión sobre el material cubierto, animando a los aprendedores a pensar en cómo pueden aplicar estos conocimientos en sus futuros roles profesionales.

11. Animar a los aprendedores a revisar el capítulo 4 (Soluciones y buenas prácticas) del libro de apoyo para profundizar en el aprendizaje, así como revisar el módulo 2.3 del curso de Cisco Academy.

Notas para el profesor impartidor correspondientes a la explicación de la Actividad 1.

Al profesor impartidor, se le recomienda lo siguiente:

1. Explicar que esta actividad está diseñada para consolidar la comprensión de los fundamentos de la ciberseguridad a través del análisis de escenarios reales y simulados.

2. Presentar los dos escenarios de incidentes de seguridad detallados en la actividad: a) Ataque de ransomware a un sistema educativo. b) Fuga de datos en una aplicación de salud, y explicar a los aprendedores que deben elegir uno para trabajarlo a lo largo de la actividad.

3. Revisar brevemente los conceptos clave que se aplican a esta actividad, tales como tipos de datos, incidentes de seguridad, métodos de ataque y vulnerabilidades.

4. Asegúrate de que los aprendedores comprendan términos como "ransomware", "phishing", "vulnerabilidad de API" y "datos sensibles".

5. Revisar y elegir uno de los escenarios de incidentes de seguridad proporcionados.

6. Proporcionar ejemplos de medidas preventivas y de mitigación, como el uso de autenticación de dos factores, la actualización de software, la educación y capacitación en seguridad, y el uso de herramientas de análisis de vulnerabilidades.

7. Fomentar el pensamiento crítico y la discusión entre los aprendedores sobre las diferentes formas de abordar los problemas de seguridad.

8. Proporcionar retroalimentación constructiva y señale áreas que pueden necesitar más atención.

9. Resaltar los puntos clave aprendidos durante la actividad y cómo pueden aplicarse en contextos reales.

10. A continuación, se comparte la solución de la actividad como material de apoyo:

    a. **Ataque de ransomware a un sistema educativo**: una importante institución educativa ha sido víctima de un ataque de ransomware. Los atacantes han cifrado los registros académicos

y personales de aprendedores y profesores, exigiendo un rescate para la liberación de los datos. El ataque se detectó cuando los empleados no pudieron acceder a los sistemas de información estudiantil y comenzaron a recibir mensajes de los atacantes en sus pantallas.

Datos en riesgo:

- Registros académicos de estudiantes.
- Información personal de estudiantes y profesores, incluyendo nombres, direcciones y números de seguro social.

Método de ataque:

Phishing: un empleado de la institución hizo clic en un enlace malicioso contenido en un correo electrónico que parecía ser una actualización de política interna, lo que permitió a los atacantes infiltrarse en la red.

b. **Fuga de datos en una aplicación de salud**: una popular aplicación de seguimiento de salud, utilizada por millones de personas para monitorear su actividad física, nutrición y parámetros de salud, ha sufrido una brecha de seguridad. Información sensible de los usuarios, incluyendo historiales médicos, ubicaciones y detalles de pago, ha sido expuesta en un foro de hackers.

Datos en riesgo:

- Historiales médicos y de salud de los usuarios.
- Ubicaciones detalladas de los usuarios durante el ejercicio.
- Detalles de tarjetas de crédito y pagos.

Método de ataque:

Vulnerabilidad de la API: los atacantes explotaron una vulnerabilidad no parcheada en la interfaz de programación de aplicaciones (API) de la aplicación, que permitía el acceso no autorizado a los datos de los usuarios.

Semana 2 (temas 6-10)

Bloque 1

Actividad	Descripción	Duración
Bienvenida y presentación de la agenda.	El profesor da una breve bienvenida y presenta la agenda de la sesión.	5 minutos.
Práctica de bienestar.	El profesor impartidor seleccionará alguna práctica del banco anexo al final de este documento para compartirla en un foro de discusión y explicarla en la sesión. Se recomienda utilizar una diferente por semana.	5 minutos.

Desarrollo de los temas de la semana: o **Aplicación en contextos reales (introducción).** o **Explicación de los temas de la semana con ejercicios prácticos.**	El profesor explicará a los participantes los contenidos con ejercicios prácticos.	30 minutos.
Receso.	Se brindará un espacio de receso para que el participante lo utilice a su beneficio.	10 minutos.

Bloque 2

Actividad	Descripción	Duración
Recapitulación de lo realizado en el bloque previo.	El profesor recapitulará de manera dinámica lo realizado en el bloque previo.	5 minutos.
Desarrollo de los temas de la semana: o **Explicación de los temas de la semana con ejercicios prácticos.**	El profesor explicará a los participantes los contenidos con ejercicios prácticos.	45 minutos.
Receso.	Se brindará un espacio de receso para que el participante lo utilice a su beneficio.	10 minutos.

Bloque 3

Actividad	Descripción	Duración
Recapitulación de lo realizado en el bloque previo.	El profesor recapitulará de manera dinámica lo realizado en el bloque previo.	5 minutos.
Desarrollo de los temas de la semana: o **Explicación de los temas de la semana con ejercicios prácticos.** o **Cierre de los temas.**	El profesor explicará a los participantes los contenidos con ejercicios prácticos y realizará un cierre de los temas correspondientes.	35 minutos.
Recordatorio de entrega del proyecto fase 1.	Se explicará a los participantes en qué consiste el proyecto de manera general, enfocándose en la fase 1, la cual deberán entregar en la semana 2.	10 minutos.

Notas para el profesor impartidor correspondientes a la explicación del tema 6, la cual debe considerar la realización de ejercicios prácticos durante la sesión.

Al profesor impartidor, se le recomienda lo siguiente:

1. Comenzar contextualizando la importancia de la ciberseguridad en el entorno digital actual, destacando cómo la protección de datos personales y corporativos es crucial para evitar pérdidas y accesos no autorizados.

2. Iniciar con ejemplos reales y recientes de brechas de seguridad que los aprendedores puedan haber visto en las noticias para captar su interés.

3. Detallar el funcionamiento básico de las medidas de protección como firewalls, antivirus y contraseñas y su impacto en la protección de datos.

4. Explicar detenidamente cómo se configuran y actualizan las diferentes opciones de seguridad en diversos sistemas operativos y dispositivos, ya que es la parte que podría ser más propensa a dudas. Para aclarar estas dudas, se puede recurrir a demostraciones prácticas en vivo o videotutoriales que muestren el proceso paso a paso.

5. Detallar las diferencias fundamentales entre las redes alámbricas e inalámbricas y los riesgos específicos asociados a cada una. Se debe resaltar la importancia de implementar medidas de seguridad robustas, como el uso de cifrado fuerte (WPA3 para redes inalámbricas), la configuración de firewalls y la segmentación de red para limitar el acceso a información sensible.

6. Definir y explicar de forma detallada los conceptos de principio de menor privilegio y la segmentación de red.

7. Mencionar las diferencias entre los tipos de respaldos (completo, incremental y diferencial), así como las técnicas que se utilizan actualmente para duplicar, respaldar y recuperar datos, tanto en la nube como en redes internas de la empresa. El siguiente artículo puede apoyarte en esta explicación:
   - Veritas. (s.f.). *Copias de seguridad y recuperación de datos: la guía esencial*. Recuperado de https://www.veritas.com/es/mx/information-center/data-backup-and-recovery

8. Utilizar dinámicas como estudios de caso y simulaciones de ciberataques para que los aprendedores apliquen los conceptos en situaciones reales y comprendan mejor las consecuencias de no implementar adecuadamente las medidas de seguridad.

9. Animar a los aprendedores a revisar el capítulo 1 (Amenazas, vulnerabilidades y ataques) del libro de apoyo para profundizar en el aprendizaje, así como revisar el módulo 3.1 del curso de Cisco Academy.

Notas para el profesor impartidor correspondientes a la explicación del tema 7, la cual debe considerar la realización de ejercicios prácticos durante la sesión.

Al profesor impartidor, se le recomienda lo siguiente:

1. Abordar primero el contexto y la importancia de la ciberseguridad en una organización, puedes utilizar el caso de Aerospacey que se presenta en la introducción del tema como ejemplo de las consecuencias de un ataque cibernético. Por otro lado, puedes presentar el siguiente video como ejemplo de cómo se realiza un ciberataque:
   - Cybernetips. (2017, 5 de octubre). *Demostracion de un ciberataque - © Deloitte Company* [Archivo de video]. Recuperado de https://www.youtube.com/watch?v=Vsb0x1mcNyc

2. Presentar las seis categorías de dispositivos de ciberseguridad, explicando en detalle cada uno, incluyendo sus funciones y cómo contribuyen a la protección de la red. Se recomienda prestar especial atención a los cortafuegos y las VPN, debido a su complejidad y relevancia en múltiples escenarios.

3. Utilizar diagramas y ejemplos prácticos para explicar la configuración y funcionamiento específico de dispositivos como cortafuegos y sistemas de prevención/detección de intrusiones.

4. Explicar de forma detallada conceptos como la segmentación de red, el filtrado de tráfico y los distintos tipos de cortafuegos (capa de red, transporte, aplicación, etc.).

5. Explicar la importancia de establecer un marco de normas y procedimientos que todos en la organización deben seguir para minimizar los riesgos y asegurar la integridad, disponibilidad y confidencialidad de los datos.

6. Animar a los aprendedores a revisar el capítulo 2 y 3 (Dominios de la ciberseguridad y Ámbitos de uso) del libro de apoyo para profundizar en el aprendizaje, así como revisar el módulo 4.1 del curso de Cisco Academy.

Notas para el profesor impartidor correspondientes a la explicación del tema 8, la cual debe considerar la realización de ejercicios prácticos durante la sesión.

Al profesor impartidor, se le recomienda lo siguiente:

1. Iniciar con una explicación de la importancia de contar con una cultura de seguridad integral, destacando cómo esta cultura se construye a través de medidas tecnológicas, capacitación del personal y políticas internas.

2. Contextualizar al aprendedor sobre la importancia de la cultura de seguridad integral. Para esto, puedes presentar el siguiente video, el cual presenta los 10 ataques más grandes y sus consecuencias:
    - SecurityQueen. (2021, 3 de enero). *TOP 10 Los Ataques Cibernéticos Más Grandes de la Historia - Los Mayores Ataques* [Archivo de video]. Recuperado de https://www.youtube.com/watch?v=RExgLfFzgrw

3. Enfatizar las funciones clave del CSIRT y cómo estas contribuyen a la detección, respuesta, recuperación y prevención de incidentes de seguridad. Las áreas donde los aprendedores podrían tener más dudas incluyen los detalles técnicos de las soluciones de seguridad de Cisco y la integración de tecnologías de seguridad. Estas dudas pueden ser aclaradas mediante ejemplos prácticos y estudios de caso adicionales.

4. Profundizar en las soluciones de seguridad que propone Cisco. Puedes presentar casos hipotéticos sobre vulnerabilidades que pueden presentar algunos dispositivos y pedir a los aprendedores que identifiquen qué herramienta sería la ideal para prevenir los ataques. En la siguiente liga puedes conocer la diversidad de soluciones que propone Cisco:
    - Cisco. (s.f.). *Resiliencia de la seguridad ante lo impredecible*. Recuperado de https://www.cisco.com/site/mx/es/products/security/index.html#tabs-aa1e70a88b-item-efb4f62fc5-tab

5. Animar a los aprendedores a revisar el capítulo 2 y 3 (Dominios de la ciberseguridad y Ámbitos de uso) del libro de apoyo para profundizar en el aprendizaje, así como revisar el módulo 4.3 del curso de Cisco Academy.

Notas para el profesor impartidor correspondientes a la explicación del tema 9, la cual debe considerar la realización de ejercicios prácticos durante la sesión.

Al profesor impartidor, se le recomienda lo siguiente:

1. Definir los términos IaaS, PaaS y SaaS en lo que se refiere a los servicios en la nube, explicando lo que cada uno de ellos ofrece a las organizaciones. Además, es importante que menciones las ventajas y desafíos de cada uno. Para ello, puedes consultar las siguientes ligas:
    - Google Cloud. (s.f.). *PaaS, IaaS, SaaS y CaaS: ¿en qué se diferencian?* Recuperado de https://cloud.google.com/learn/paas-vs-iaas-vs-saas?hl=es#:~:text=Cloud%20computing%20tiene%20tres%20modelos,SaaS%20(software%20como%20servicio).

    - Amazon Web Services IBERIA (España & Portugal). (2023, 24 de marzo). *Qué es la computación o informática en la nube | Conceptos de computación en la nube de AWS* [Archivo de video]. Recuperado de https://www.youtube.com/watch?v=nMfeITzWMuo

2. Mencionar, con base en tu experiencia profesional, un caso de migración de servicios a la nube, en cuanto a una empresa que sea de tu conocimiento, definiendo los pasos que se siguieron para lograr dicha implementación. Adicionalmente, se pueden presentar los siguientes ejemplos que comparte AWS.

    - AWS. (s.f.). *Clientes de la migración a la nube*. Recuperado de https://aws.amazon.com/es/cloud-migration/customers/?cloud-migration-customers-cards.sort-by=item.additionalFields.sortOrder&cloud-migration-customers-cards.sort-order=desc&awsf.industry=*all&awsf.migration-type=*all&awsf.region=*all&awsf.content-type=*all&awsf.year=*all

3. Detallar los beneficios que ofrece la computación *cloud*, puedes apoyarte en la información que ofrece IBM al respecto:
    - IBM. (s.f.). *¿Cuáles son los beneficios de la computación en la nube?* Recuperado de https://www.ibm.com/mx-es/topics/cloud-computing-benefits

4. Profundizar en los riesgos a los que se exponen los datos en la nube, así como cuáles son las responsabilidades que comparten los proveedores de servicios y los clientes. Consulta un par de proveedores de prestigio y enlista sus compromisos.

5. Animar a los aprendedores a revisar el capítulo 4 (Soluciones y buenas prácticas de ciberseguridad) del libro de apoyo para profundizar en el aprendizaje.

Notas para el profesor impartidor correspondientes a la explicación del tema 10, la cual debe considerar la realización de ejercicios prácticos durante la sesión.

Al profesor impartidor, se le recomienda lo siguiente:

1. Iniciar con una explicación clara y contextualizada sobre la importancia de la ciberseguridad en la adopción de la computación en la nube. Esto debe incluir una discusión sobre cómo la migración a la nube transforma las operaciones organizacionales e introduce nuevos desafíos de seguridad, centrándose en la protección de datos críticos.

2. Listar cuáles son los elementos que se consideran para la gestión de identidad y accesos en un entorno de nube. Puedes considerar las reflexiones ofrecidas en este panel:
    - Silicon TV. (2019, 4 de noviembre). *Gestión de identidades y acceso seguro a la nube: Una cuestión de confianza* [Archivo de video]. Recuperado de https://www.youtube.com/watch?v=JL-HgrVyEOc

3. Enfatizar en la sección de métodos de autenticación y la importancia de la autenticación multifactor, ya que es un punto en donde pueden surgir más dudas.

4. Definir, por medio de un caso de estudio basado en tu experiencia, cómo es que una empresa puede lograr una configuración de la infraestructura en la nube utilizando IaC (Infraestructura como Código). Analiza esta guía digital, que también menciona ejemplos:
    - Ionos. (2021). *Infrastructure as code (IaC)*. Recuperado de https://www.ionos.mx/digitalguide/servidores/know-how/infrastructure-as-code/

5. Incorporar actividades prácticas como ejercicios de configuración en un entorno de nube simulado, utilizando herramientas como AWS CloudFormation o Terraform para aplicar los conceptos de Infraestructura como Código (IaC).

6. Animar a los aprendedores a revisar el capítulo 4 (Soluciones y buenas prácticas de ciberseguridad) del libro de apoyo para profundizar en el aprendizaje.

Notas para el avance del proyecto (fase I).

Al profesor impartidor, se le recomienda lo siguiente:

1. Sugerir a los aprendedores que hagan una búsqueda de las empresas que están cotizando en la bolsa de valores, muchas de estas organizaciones contienen sitios institucionales públicos donde explican el tipo de infraestructura que puedan contener. De igual manera, puedes explicarles cómo utilizar inteligencia artificial regenerativa para poder crear escenarios de empresas ficticias y proponerlo para el escenario de practica del proyecto.

2. Explicar a los aprendedores que en lo que respecta a la simulación de ataque, no se busca como tal que haga alguna practica de *hacking* ético, solamente hay que contextualizar un escenario donde se vea atacado uno de los activos de la información. Para ello, se sugiere que pueda realizar una búsqueda de casos de estudio donde hayan sucedido ataques a empresas.

3. Guiar a los aprendedores en el desarrollo de un pequeño plan de acción de protección a los datos. Para ello, se pueden compartir experiencias profesionales, o bien, mostrar algunos de estos recursos:

    - CiscoLatam. (2021, 9 de junio). *Cómo crear un plan de respuesta contra ataques DDoS* [Archivo de video]. Recuperado de https://www.youtube.com/watch?v=0nNKT4RgS4w
    - Olimpia IT. (2021, 3 de noviembre). *¿Sabes qué hacer en caso de un ataque cibernético?* [Archivo de video]. Recuperado de https://www.youtube.com/watch?v=rDQ8njC4SX8

Semana 3 (temas 11-15)

Bloque 1

Actividad	Descripción	Duración
Bienvenida y presentación de la agenda.	El profesor da una breve bienvenida y presenta la agenda de la sesión.	5 minutos.

Práctica de bienestar.	El profesor impartidor seleccionará alguna práctica del banco anexo al final de este documento para compartirla en un foro de discusión y explicarla en la sesión. Se recomienda utilizar una diferente por semana.	5 minutos.
Desarrollo de los temas de la semana: o **Aplicación en contextos reales (introducción).** o **Explicación de los temas de la semana con ejercicios prácticos.**	El profesor explicará a los participantes los contenidos con ejercicios prácticos.	30 minutos.
Receso.	Se brindará un espacio de receso para que el participante lo utilice a su beneficio.	10 minutos.

Bloque 2

Actividad	Descripción	Duración
Recapitulación de lo realizado en el bloque previo.	El profesor recapitulará de manera dinámica lo realizado en el bloque previo.	5 minutos.
Desarrollo de los temas de la semana: o **Explicación de los temas de la semana con ejercicios prácticos.**	El profesor explicará a los participantes los contenidos con ejercicios prácticos.	45 minutos.
Receso.	Se brindará un espacio de receso para que el participante lo utilice a su beneficio.	10 minutos.

Bloque 3

Actividad	Descripción	Duración
Recapitulación de lo realizado en el bloque previo.	El profesor recapitulará de manera dinámica lo realizado en el bloque previo.	5 minutos.

Desarrollo de los temas de la semana: o **Explicación de los temas de la semana con ejercicios prácticos.** o **Cierre de los temas.**	El profesor explicará a los participantes los contenidos con ejercicios prácticos y realizará un cierre de los temas correspondientes.	35 minutos.
Explicación de la actividad integradora 2	Se explicará a los participantes en qué consiste la actividad integradora 2, la cual se entrega en la semana 3.	10 minutos.

Notas para el profesor impartidor correspondientes a la explicación del tema 11, la cual debe considerar la realización de ejercicios prácticos durante la sesión.

Al profesor impartidor, se recomienda lo siguiente:

1. Introducir los conceptos clave de IaC y su importancia en la seguridad en la nube. Resaltar cómo IaC facilita la automatización y consistencia en la configuración de infraestructuras seguras.

2. Demostrar el uso de herramientas como Terraform, CloudFormation y Ansible en la gestión segura de infraestructuras. Proveer ejemplos prácticos de *scripts* y configuraciones.

3. Fomentar la discusión sobre los beneficios de IaC para la seguridad, como la reproducibilidad y la detección temprana de vulnerabilidades. Presentar estudios de caso reales donde IaC haya mejorado la seguridad.

4. Realizar actividades prácticas que involucren la implementación de políticas de seguridad automatizadas mediante IaC. Utilizar ejercicios que permitan a los aprendedores configurar reglas de firewall, gestionar accesos y realizar escaneos de seguridad.

5. Explicar cómo integrar la seguridad en el ciclo de vida del desarrollo de software (SDLC) utilizando IaC. Discutir el SDL (*Secure Development Lifecycle*) y cómo IaC puede contribuir a cada fase.

6. Definir claramente qué son los contenedores y las herramientas de orquestación como Kubernetes y Docker. Explicar su rol en la mejora de la seguridad a través de la microsegmentación y la automatización.

7. Mostrar cómo se implementan y configuran las políticas de seguridad en contenedores. Proveer ejemplos de políticas de seguridad en Kubernetes, como el uso de RBAC y políticas de seguridad de Pod.

8. Destacar la importancia de la monitorización y auditoría continua en entornos de contenedores. Introducir herramientas y prácticas para la monitorización y auditoría efectiva.

9. Realizar actividades prácticas que involucren el despliegue seguro de contenedores y la configuración de políticas de seguridad. Organizar laboratorios donde los aprendedores puedan desplegar contenedores, configurar políticas y monitorear su seguridad.

10. Facilitar la discusión sobre los beneficios y desafíos de la seguridad en entornos de contenedores y orquestación. Promover el análisis de escenarios reales de seguridad en contenedores y la resolución de problemas.

11. Explorar casos de uso y ejemplos prácticos de seguridad en contenedores y orquestación. Presentar ejemplos de implementaciones exitosas y discutir las lecciones aprendidas.

12. Animar a los aprendedores a revisar el capítulo 2 (Dominios de la ciberseguridad) del libro de apoyo para profundizar en el aprendizaje.

Notas para el profesor impartidor correspondientes a la explicación del tema 12, la cual debe considerar la realización de ejercicios prácticos durante la sesión.

Al profesor impartidor, se le recomienda lo siguiente:

1. Iniciar la sesión destacando la relevancia del tema. Puedes utilizar el caso de Equifax para subrayar las graves consecuencias de las vulnerabilidades en el código. Además, es importante destacar cómo una pequeña vulnerabilidad puede tener un impacto masivo en una organización.

2. Guiar a los aprendedores a través de las fases del SDLC y enfatizar la necesidad de incorporar prácticas de seguridad en cada etapa del ciclo de vida del desarrollo de software, desde la planificación hasta el mantenimiento. Asimismo, se debe explicar cómo la seguridad debe ser una parte integral desde el principio.

3. Explicar detalladamente las metodologías DevSecOps, CLASP y SSDF, presentándolas como marcos estructurados que mejoran la seguridad del software. Aclarar cómo cada uno proporciona herramientas y prácticas específicas para integrar la seguridad de manera efectiva.

4. Simplificar los conceptos más importantes, enfocándose en los principios de desarrollo seguro y la aplicación práctica de las pruebas de seguridad. Utilizar ejemplos prácticos y ejercicios que permitan a los aprendedores identificar y mitigar vulnerabilidades en un entorno controlado.

5. Utilizar estudios de caso adicionales o simulaciones de ataques y facilitar la realización de pruebas de seguridad en aplicaciones ficticias. Por otro lado, se pueden utilizar recursos como tutoriales en línea, herramientas de simulación de ciberataques y plataformas de aprendizaje interactivo para complementar la enseñanza.

6. Promover discusiones sobre los desafíos y estrategias de implementación de DevSecOps. Esto ayudará a consolidar los conocimientos y a desarrollar una mentalidad de seguridad entre los aprendedores.

7. Planificar ejercicios de codificación en los que los aprendedores deban aplicar prácticas de seguridad, como la sanitización de entradas y la gestión de excepciones.

9. Demostrar el uso de herramientas de análisis estático y dinámico e introducir a los aprendedores a herramientas como SonarQube para análisis estático y ZAP para análisis dinámico, y guiarlos en su uso práctico.

10. Evaluar el impacto de vulnerabilidades en escenarios controlados. En este punto se puede simular un ataque en un entorno de prueba para mostrar a los aprendedores las consecuencias de no seguir prácticas seguras, seguido de una discusión sobre cómo mitigar tales riesgos.

Notas para el profesor impartidor correspondientes a la explicación del tema 13, la cual debe considerar la realización de ejercicios prácticos durante la sesión.

Al profesor impartidor, se le recomienda lo siguiente:

1. Resaltar la importancia de la seguridad en la industria tecnológica, utilizando ejemplos reales como el incidente de seguridad de Twitter en 2022.

2. Explicar detalladamente el concepto de "*Security by Design*", enfatizando la integración de medidas de seguridad desde el inicio del ciclo de vida del desarrollo de software (SDLC).

3. Ejemplificar, mediante diagramas de flujo, cómo funcionan los procesos de autenticación y autorización, ya que es un punto en donde los aprendedores podrían tener más dudas.

4. Utiliza ejemplos y casos prácticos para explicar los conceptos de "principio de menor privilegio", "desarrollo defensivo" y "pruebas de penetración". Puedes utilizar herramientas como "TryHackme" para realizar simulaciones.

Notas para el profesor impartidor correspondientes a la explicación del tema 14, la cual debe considerar la realización de ejercicios prácticos durante la sesión.

Al profesor impartidor, se le recomienda lo siguiente:

1. Contextualizar a los aprendedores sobre la importancia de la ciberseguridad en la era digital. Para fomentar la participación, puedes pedirles que compartan si conocen algún ataque cibernético importante que haya sucedido en los últimos años.

2. Explicar detalladamente las vulnerabilidades comunes en aplicaciones web, como Cross-Site Scripting (XSS), inyección SQL y Cross-Site Request Forgery (CSRF), utilizando ejemplos prácticos para ilustrar cómo estos ataques pueden comprometer la seguridad de las aplicaciones.

3. Enfatizar la importancia de medidas preventivas como la validación de entradas, el uso de cortafuegos de aplicaciones web (WAF) y la autenticación multifactor (MFA).

4. Ejemplificar las principales vulnerabilidades que presenta OWASP utilizando algún laboratorio interactivo.

5. Detallar las diversas técnicas de protección como validación de entrada, sanitización de datos, uso de API seguras, *Content Security Policy* (CSP) y cifrado de datos. Explicar cada técnica con ejemplos prácticos.

6. Animar a los aprendedores a revisar el capítulo 4 (Soluciones y buenas prácticas de ciberseguridad) del libro de apoyo para profundizar en el aprendizaje.

Notas para el profesor impartidor correspondientes a la explicación del tema 15, la cual debe considerar la realización de ejercicios prácticos durante la sesión.

Al profesor impartidor, se le recomienda lo siguiente:

1. Explicar la importancia y los riesgos asociados a la exposición de datos sensibles a través de API. Es fundamental enfatizar cómo las API facilitan la interacción entre diferentes sistemas, utilizando ejemplos prácticos como la obtención de datos meteorológicos por una aplicación móvil.

2. Detallar los tipos de API (SOAP, RPC, WebSocket, REST), sus características y casos de uso, permitiendo a los aprendedores comprender cómo y cuándo utilizar cada una.

3. Discutir las prácticas avanzadas de seguridad en API, tales como la validación y sanitización de datos, la comunicación segura mediante HTTPS y la implementación de mecanismos de autenticación y autorización robustos como OAuth y JWT.

4. Utilizar diagramas de flujo que muestren cómo se procesan las solicitudes y respuestas de autenticación y autorización en diferentes tipos de API y casos prácticos que ejemplifiquen el uso de OAuth en aplicaciones reales.

5. Utilizar plataformas interactivas, como OWASP ZAP para escanear vulnerabilidades y enriquecer la experiencia educativa.

Notas para el profesor impartidor correspondientes a la explicación de la Actividad 2.

Al profesor impartidor, se le recomienda lo siguiente:

1. Explicar que esta actividad consiste en presentar el examen final del curso "Introducción a la Ciberseguridad" de Cisco Networking Academy.
2. Antes de que presenten el examen, preguntar a los aprendedores si hay alguna duda y animarlos a repasar el contenido de la plataforma para ampliar y profundizar su aprendizaje sobre la ciencia de datos.
3. Guiar a los aprendedores por la plataforma de Cisco para que puedan ubicar el apartado donde se encuentra el examen final.

Semana 4 (temas 16-20)

Bloque 1

Actividad	Descripción	Duración
Bienvenida y presentación de la agenda.	El profesor da una breve bienvenida y presenta la agenda de la sesión.	5 minutos.
Práctica de bienestar.	El profesor impartidor seleccionará alguna práctica del banco anexo al final de este documento para compartirla en un foro de discusión y explicarla en la sesión. Se recomienda utilizar una diferente por semana.	5 minutos.
Desarrollo de los temas de la semana: o **Aplicación en contextos reales (introducción).** o **Explicación de los temas de la semana con ejercicios prácticos.**	El profesor explicará a los participantes los contenidos con ejercicios prácticos.	40 minutos.
Receso.	Se brindará un espacio de receso para que el participante lo utilice a su beneficio.	10 minutos.

Bloque 2

Actividad	Descripción	Duración
Recapitulación de lo realizado en el bloque previo.	El profesor recapitulará de manera dinámica lo realizado en el bloque previo.	5 minutos.
Desarrollo de los temas de la semana: o **Explicación de los temas de la semana con ejercicios prácticos.**	El profesor explicará a los participantes los contenidos con ejercicios prácticos.	45 minutos.
Receso.	Se brindará un espacio de receso para que el participante lo utilice a su beneficio.	10 minutos.

Bloque 3

Actividad	Descripción	Duración
Recapitulación de lo realizado en el bloque previo.	El profesor recapitulará de manera dinámica lo realizado en el bloque previo.	5 minutos.
Desarrollo de los temas de la semana: o **Explicación de los temas de la semana con ejercicios prácticos.** o **Cierre de los temas.**	El profesor explicará a los participantes los contenidos con ejercicios prácticos y realizará un cierre de los temas correspondientes.	35 minutos.
Recordatorio de entrega del proyecto, fase 2. **Recordatorio del examen final.**	El profesor recordará a los participantes la entrega de la fase 2 del proyecto. El profesor recordará a los participantes el examen final.	10 minutos.

Notas para el profesor impartidor correspondientes a la explicación del tema 16, la cual debe considerar la realización de ejercicios prácticos durante la sesión.

Al profesor impartidor, se le recomienda lo siguiente:

1. Realizar alguna practica donde los aprendedores puedan conocer la importancia del diseño de redes seguras. Puedes utilizar Cisco Packet Tracer para explicar el perímetro de la red y la segmentación de redes. Si desconoces el uso de Cisco Packet Tracer, puedes revisar el siguiente curso:

- Cisco Academy. (s.f.). *Introducción a Cisco Packet Tracer.* Recuperado de https://skillsforall.com/es/launch?id=ec0847b7-e6fc-4597-bc31-38ddd6b07a2f&tab=curriculum&view=d8d86845-f4c6-584c-ae59-7c1ef4f26eb3

2. Mostrar a los aprendedores cómo realizar la instalación de una VPN. Se puede utilizar la VPN que se muestra en el ejemplo del tema, o bien, algún otro tipo de VPN. Incluso, se puede descargar la

   VPN gratuita de ProtonVPN y con ello explicar a los aprendedores cómo es que funcionan las VPN, por ejemplo, al anonimizar la dirección de internet (IP) en la navegación.

3. Para descargar y crear una cuenta gratuita de ProtonVPN, revisa el siguiente *link*:
   - Proton VPN. (s.f.). *VPN suiza de gran velocidad que protege su privacidad.* Recuperado de https://account.protonvpn.com/es/signup?plan=free&currency=USD&ref=upsell

4. Reforzar el objetivo del tema, que es que los aprendedores entiendan los riesgos que pueden encontrarse al no diseñar una red segura, así como saber que robustecer la seguridad puede protegerlos a ellos y a las organizaciones.

5. Animar a los aprendedores a revisar el capítulo 4 (Soluciones y buenas prácticas de ciberseguridad) del libro de apoyo para profundizar en el aprendizaje.

Notas para el profesor impartidor correspondientes a la explicación del tema 17, la cual debe considerar la realización de ejercicios prácticos durante la sesión.

Al profesor impartidor, se le recomienda lo siguiente:

1. Recordar que el objetivo de este tema es ayudar a los aprendedores a conocer la importancia de crear barreras de protección en el perímetro de la red.

2. Utilizar **Cisco Packet Tracer** para simular el funcionamiento y operación de un firewall físico de cisco.

3. Utilizar y ejemplificar el uso de firewalls basado en el Host, ya sea en Windows o en ambiente Linux. Para ello, puedes crear algunas reglas para bloquear una aplicación, por ejemplo, navegador de internet y verificar este bloqueo al acceder a la aplicación e intentar realizar una consulta en internet.

4. Hacer una presentación del uso de los sistemas de detección de intrusiones (IDS) y de los sistemas de prevención de intrusos (IPS). Si lo consideras prudente, puedes realizar la instalación de Snort, un potente y robusto IDS e IPS. Puedes tomar ideas del siguiente video:
   - Wild IT Academy. (2023, 10 de agosto). *Implementación de Snort en Windows |CEHv12| Wild IT Academy* [Archivo de video]. Recuperado de https://www.youtube.com/watch?v=uakiR0jM0Y4

5. Animar a los aprendedores a revisar el capítulo 4 (Soluciones y buenas prácticas de ciberseguridad) del libro de apoyo para profundizar en el aprendizaje.

Notas para el profesor impartidor correspondientes a la explicación del tema 18, la cual debe considerar la realización de ejercicios prácticos durante la sesión.

Al profesor impartidor, se le recomienda lo siguiente:

1. Guiar a los aprendedores para que sean capaces de crear evaluaciones de riesgos asertivas para prever posibles amenazas, así como para crear planes de recuperación.

2. Exponer un caso de estudio, o bien, pedirles que realicen una investigación sobre un ataque real de ciberseguridad y, posteriormente hacer una evaluación, donde se tome en cuenta qué mecanismos existían sobre:

    - Protección de datos
    - Mitigación de riesgos
    - Estándares de la industria

3. Ejemplificar, con base en su experiencia, cómo la correcta evaluación de riesgos puede proteger a las organizaciones y cómo gracias a esta practicas será mucho más asertivo el reaccionar ante un incidente de ciberseguridad.

4. Animar a los aprendedores a revisar el capítulo 4 (Soluciones y buenas prácticas de ciberseguridad) del libro de apoyo para profundizar en el aprendizaje.

Notas para el profesor impartidor correspondientes a la explicación del tema 19, la cual debe considerar la realización de ejercicios prácticos durante la sesión.

Al profesor impartidor, se le recomienda lo siguiente:

1. Explicar las diferentes normas y regulaciones internacionales que existen como las normas ISO, así como el GDPR, CCPA y APPI, ya que son fundamentales en el ámbito de la ciberseguridad. Además, se pueden utilizar guías y recursos disponibles en línea para mejorar la seguridad en el uso de redes y dispositivos en el contexto educativo por citar un ejemplo.

2. Incorporar casos de estudio y ejemplos reales para ilustrar cómo las normativas y estándares se aplican en situaciones prácticas.

3. Fomentar la participación con herramientas interactivas como cuestionarios, juegos de rol y simulaciones de toma de decisiones.

4. Organizar debates en clase sobre temas actuales relacionados con la ciberseguridad y cómo las normativas internacionales afectan a las decisiones empresariales y gubernamentales.

5. Mencionar cómo la legislación mexicana hace frente a los requerimientos internacionales. Para ello, se pueden mencionar las leyes de:
    - **Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO)**
    - **Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)**

6. Consultar el siguiente proyecto de una ley de ciberseguridad:
    - Fuentes, S. (2024). *Ley de Ciberseguridad en México: Conoce la nueva Ley*. Recuperado de https://www.deltaprotect.com/blog/ley-de-ciberseguridad-mexico

Notas para el profesor impartidor correspondientes a la explicación del tema 20, la cual debe considerar la realización de ejercicios prácticos durante la sesión.

Al profesor impartidor, se le recomienda lo siguiente:

1. Realizar un repaso breve sobre la ciberseguridad.

2. Hacer algunas aportaciones con base en su experiencia sobre los siguientes temas:
    - **Tendencias actuales en ciberseguridad**
        - **Inteligencia Artificial (IA) y Aprendizaje Automático (ML)**: cómo los algoritmos de IA y ML están transformando la detección y respuesta a amenazas.

- ***Blockchain***: la importancia del blockchain para la seguridad de la información y cómo está siendo adoptado en diferentes sectores.
- **IoT y sus desafíos**: el impacto del Internet de las Cosas en la ciberseguridad y las medidas para proteger estos dispositivos.

- **El futuro de la ciberseguridad**
  - **Generative AI**: la adopción de IA generativa como herramienta de ciberseguridad.
  - **Brecha de talento**: la necesidad de expertos en seguridad y cómo abordarla.
  - **Regulaciones y gobierno**: cómo las regulaciones afectan la gestión de la ciberseguridad.

3. Enriquecer estos temas invitando a los aprendedores a que revisen la siguiente lectura:
   - Banafa, A. (2023). *El futuro de la ciberseguridad. Previsiones y tendencias*. Recuperado de https://www.bbvaopenmind.com/tecnologia/mundo-digital/futuro-ciberseguridad-previsiones-tendencias/

Notas para la segunda entrega del proyecto final (fase 2).

Al profesor impartidor, se le recomienda lo siguiente:

1. Hacer una demostración de cómo se descargan e instalan las máquinas virtuales. Kali Linux servirá como herramienta principal para realizar las pruebas de seguridad, mientras que BadStore actuará como un servidor web vulnerable corriendo en un sistema Linux.
2. Mencionar a los aprendedores que revisen el video de la semana 2 para que repasen el proceso de instalación. Además, se puede mostrar el siguiente video como apoyo en este proceso:
   - DevGuardian Code. (2022, 24 de marzo). *Herramienta ligera para realizar pruebas de Seguridad Web - BadStore* [Archivo de video]. Recuperado de https://www.youtube.com/watch?v=esYRRzzbX84
3. Explicar que no es necesario asignar numerosa memoria RAM o almacenamiento a las máquinas virtuales. Sigue las recomendaciones mínimas proporcionadas en los sitios de descarga.
4. Hacer énfasis en que las máquinas virtuales se deben configurar en modo “Bridge” para que compartan el mismo direccionamiento IP que la red local. Esto facilita la comunicación entre las máquinas virtuales y su máquina *host*. Los aprendedores deben conectarse a una red doméstica estable y preferentemente conectada mediante cables ethernet (LAN) para evitar problemas de conectividad.
5. Guiar a los aprendedores en la configuración de sus máquinas virtuales y resolver cualquier duda que tengan. Además, es importante recordarles que accedan a la página web de BadStore utilizando la IP privada del servidor en su navegador (por ejemplo, http://[IP PRIVADA]).
6. Motivar a los aprendedores a que lean el manual proporcionado, ya que esto les ayudará a entender y visualizar las vulnerabilidades presentes en BadStore.
7. Proporcionar retroalimentación sobre las soluciones y la investigación realizada por los aprendedores. Aunque no hay respuestas incorrectas, es crucial señalar fallas en la investigación o prácticas erróneas.
8. Recordar a los aprendedores que deben documentar las tácticas de obtención de información utilizadas y cómo aplicaron esta información en su laboratorio para encontrar vulnerabilidades.

9. Explicar a los aprendedores que, basándose en las vulnerabilidades y riesgos identificados en BadStore, deben diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) para una empresa ficticia. Esto incluye la identificación de activos críticos y la evaluación de riesgos y amenazas.

Anexo 1. Rúbrica del avance del proyecto (fase I)

	Nivel de desempeño			
Criterios de evaluación	Altamente competente 100%-86%	Competente 85%-70%	Aún sin desarrollar la competencia 69%-0%	%
1. Preparación y configuración de infraestructura.	20 – 18 La infraestructura está configurada con detalle y precisión, utilizando herramientas avanzadas de IaC o simuladores; incluye políticas de seguridad robustas y bien documentadas.	17 - 15 La infraestructura está configurada adecuadamente, con uso correcto de herramientas de IaC o simuladores; las políticas de seguridad son básicas pero efectivas.	14 - 0 La infraestructura presenta configuraciones incorrectas o incompletas; las políticas de seguridad son inexistentes o inadecuadas.	20
2. Identificación y clasificación de datos.	30 - 27 Los datos están identificados y clasificados con precisión, reflejando una comprensión clara de la sensibilidad y prioridad de protección.	26 - 23 La mayoría de los datos están correctamente identificados y clasificados; hay alguna confusión en cuanto a sensibilidad y prioridad.	22 - 0 La identificación y clasificación de datos es inadecuada, con muchos errores o datos no clasificados.	30
3. Creación de medidas de seguridad.	30 - 27 Las medidas de seguridad propuestas son exhaustivas, innovadoras y cubren todos los posibles ataques y vulnerabilidades identificados.	26 - 23 Las medidas de seguridad son adecuadas y cubren la mayoría de los posibles ataques y vulnerabilidades.	22 - 0 Las medidas de seguridad son insuficientes o inapropiadas, dejando muchas vulnerabilidades sin abordar.	30
4. Análisis y presentación de resultados.	20 -18 La presentación es clara, profesional y detallada; incluye contexto, metodología, resultados clave, análisis de riesgos y recomendaciones bien fundamentadas.	17 - 12 La presentación es clara y profesional, con la mayoría de los elementos requeridos; algunas áreas carecen de detalle o claridad.	11 - 0 La presentación es confusa, incompleta o no profesional, omitiendo varios elementos clave como el análisis de riesgos y recomendaciones.	20
			TOTAL	**100%**

Anexo 2. Rúbrica de la entrega final del proyecto (fase II)

	Nivel de desempeño			
Criterios de evaluación	Altamente competente 100%-86%	Competente 85%-70%	Aún sin desarrollar la competencia 69%-0%	%
1. Familiarización con Kali Linux.	20 - 18 Navega y utiliza la interfaz de Kali Linux de manera eficiente, mostrando comprensión completa del entorno y la configuración de red en modo *bridge* e identificación de IP privada sin errores.	17 - 15 Navega y utiliza la interfaz de Kali Linux con comprensión básica, configurando la red en modo bridge e identificando la IP privada con algunos errores menores.	14 - 0 Muestra poca o ninguna familiarización con la interfaz de Kali Linux, con dificultades significativas para navegar y utilizar el entorno, y no logra configurar la red o identificar la IP privada correctamente.	20
2. Escaneo y análisis de vulnerabilidades.	30 - 27 Utiliza Nmap y Burp Suite para identificar y documentar todos los servicios, puertos abiertos y vulnerabilidades en BadStore de manera precisa y detallada.	26 - 23 Utiliza Nmap y Burp Suite para identificar y documentar la mayoría de los servicios, puertos abiertos y vulnerabilidades en BadStore con algunos errores menores.	22 - 0 No logra utilizar Nmap y Burp Suite adecuadamente para identificar y documentar los servicios, puertos abiertos y vulnerabilidades en BadStore.	30
3. Investigación de vulnerabilidades.	30 - 27 Realiza un análisis exhaustivo de las vulnerabilidades detectadas, proporcionando una documentación detallada y precisa de los hallazgos y su impacto potencial.	26 - 23 Realiza un análisis básico de las vulnerabilidades detectadas, con una documentación mayormente completa, pero con algunas faltas de detalle o precisión.	22 - 0 No realiza un análisis adecuado de las vulnerabilidades detectadas, o la documentación es insuficiente y carece de precisión.	30
4. Diseño del SGSI.	20 - 18 Identifica y documenta todos los activos críticos de la organización, evaluando riesgos y amenazas de manera detallada y precisa, e integra de manera completa y coherente la información de los activos y la	17 - 12 Identifica y documenta la mayoría de los activos críticos de la organización, evaluando los riesgos y amenazas con algunos errores o faltas de detalle, e integra la mayoría de la información de los activos y la infraestructura en el	11 - 0 No identifica o documenta adecuadamente los activos críticos de la organización, ni evalúa correctamente los riesgos y amenazas, y no integra adecuadamente la información de los activos y la	20

	infraestructura en el SGSI.	SGSI con algunas incoherencias.	infraestructura en el SGSI.	
			TOTAL	**100%**

Prácticas de bienestar

Práctica 1

Nombre de la práctica	Un momento para respirar.
Descripción de la práctica	Aprender a respirar por la nariz y a tranquilizar tu mente.
Palabras clave	Fortalezas de carácter, autorregulación.
Instrucciones para el aprendedor	La autorregulación, también percibida como control, es una fortaleza de carácter muy importante dentro de la psicología positiva. Este concepto implica regular lo que uno siente y hace, ser disciplinado, así como mantener un control sobre los apetitos y, especialmente, sobre las emociones. En la actualidad vivimos situaciones muy estresantes que provocan que nuestra reacción instintiva y natural ante ellas sea estallar en ira. Pero, las consecuencias de este comportamiento no solo se quedan en nosotros, sino que también pueden llegar a afectar a terceros. A continuación, se presenta un ejercicio que te ayudará a cultivar la fortaleza de autorregulación: 1. Toma dos minutos de tu tiempo, siéntate en un lugar cómodo, donde no haya mucho ruido que te pueda distraer. 2. Escucha música de relajación (crea tu propio ambiente de meditación). 3. Comienza a respirar y exhalar por nariz. 4. Trata de que tu respiración y exhalación dure el mismo tiempo. 5. Fija tu mente en tu respiración, en cómo entra y sale el aire de tu cuerpo. Así durante dos minutos. Te recomendamos que si durante este periodo algún pensamiento (olvidé algo en la oficina, más tarde tengo que hacer tal actividad, etc.) llega a tu mente, solo déjalo pasar y regresa a la concentración en tu respiración. Al finalizar los dos minutos sentirás paz en tu ser. Comienza a hacer este ejercicio de respiración y meditación todos los días y poco a poco vas aumentando los minutos de este.
Fuente	Conferencia Rosalinda Ballesteros.

Práctica 2

Nombre de la práctica	Fomentando la atención plena.
Descripción de la práctica	Llevarás a cabo breves ejercicios de meditación para fomentar la atención plena en tus actividades diarias.

Palabras clave	Atención plena, fortalezas de carácter, autorregulación.
Instrucciones para el aprendedor	La meditación es una herramienta que ayuda a mejorar el desempeño de cualquier persona, ya que fomenta el desarrollo de la atención plena en una sola actividad. Para fomentar la atención plena y lograr cada vez más estar en una zona de concentración mientras realizas tus actividades cotidianas, puedes llevar a cabo los siguientes ejercicios de meditación: Encuentra en algún momento del día cinco minutos para ti, siéntate en un lugar cómodo, donde no tengas distracciones. 1. Haz tres respiraciones profundas por la nariz y exhala por la nariz. 2. Comienza a hacer un repaso de tu día, de lo que más te acuerdes, por ejemplo, te levantaste, ¿qué hiciste?, ¿desayunaste?, ¿te bañaste?, ¿diste los buenos días?, etcétera. Si desayunaste, ¿qué fue lo que desayunaste?, ¿te gustó?, ¿tomaste tu alimento despacio o apurado? Si estabas apurado, ¿qué era lo que te tenía en esa situación? 3. Sigue meditando en lo que te acuerdes: ¿te molestase con alguien?, ¿por qué?, ¿qué fue lo que pasó?, ¿crees que era posible haber reaccionado de alguna manera más pacífica? Con este ejercicio te darás cuenta de que reaccionamos o hacemos cosas de manera automática. Algunas veces si estamos más conscientes y presentes, podemos tener otra actitud sin que alguna situación nos afecte demasiado.
Fuente	Eby, D. (s.f.). *Creativity and Flow Psychology*. Recuperado de http://talentdevelop.com/articles/Page8.html

Práctica 03

Nombre de la práctica	Experiencias difíciles.
Descripción de la práctica	En esta práctica podrás analizar las estrategias que seguiste para afrontar problemáticas y cómo aprendiste de tales sucesos.
Palabras clave	Resiliencia.
Instrucciones para el aprendedor	Todos hemos pasado por situaciones complejas, no solo en lo laboral, sino también en el ámbito familiar y personal. La manera en que enfrentamos dichos obstáculos es muy diferente, algunas personas continúan con su vida sin problema alguno, a otras tantas se les complica esa transición, también hay quienes no pueden sobreponerse a las experiencias difíciles. > La resiliencia es la capacidad de reponerse tras la adversidad, de recuperarse después de vivir experiencias difíciles, dolorosas o traumáticas. Para algunos la resiliencia implica no solo salir adelante después de una situación muy dura, sino incluso crecer o ser mejor a raíz de esta experiencia. (Tarragona, 2012) La siguiente práctica te ayudará a fomentar esta importante cualidad:

	1. Crea una tabla con tres columnas y cinco filas. 2. En la primera columna escribe un evento difícil o desagradable al que te hayas enfrentado en tu vida. 3. En la segunda columna menciona cuáles son tus creencias sobre esa adversidad. 4. En la tercera columna describe las consecuencias que tiene esa creencia. 5. Cuando termines, lee toda la tabla y reflexiona sobre cómo te ha cambiado cada evento y cómo lo enfrentaste. 6. Escribe al final cómo enfrentarías cada evento hoy en día.
Fuente	• Metodología ABC. • Fundamentos de psicología positiva.

Práctica 04

Nombre de la práctica	Concentrarse en lo positivo.
Descripción de la práctica	Analizarás sucesos que te hayan ocurrido recientemente, buscando orientar el análisis hacia las consecuencias positivas.
Palabras clave	Resiliencia y esperanza.
Instrucciones para el aprendedor	¿Qué es lo primero que piensas cuando recibes una noticia inesperada?, o bien, ¿qué te imaginas cuando un acontecimiento complejo se presenta ante ti? La mayoría de las personas automáticamente se concentra en el peor de los escenarios independientemente del tipo de noticia que reciban. Martin Seligman sugiere hacer un breve ejercicio para fomentar la resiliencia y la esperanza con base en la premisa antes señalada: 1. Piensa en una noticia reciente que hayas recibido y que creas que es negativa para ti. 2. Luego de analizarla, haz una tabla con tres columnas. En la primera, señala cuál sería el peor de los escenarios posibles que pudieran resultar de esa noticia; en la segunda columna señala cuál sería el mejor de los escenarios posibles, y en la última, cuál es el escenario que realmente tiene mayor probabilidad de ocurrir. 3. Reflexiona sobre los tres escenarios, ¿cómo enfrentarías cada uno de ellos? Procura repetir este ejercicio cada vez que sientas que te enfrentas a una situación complicada. Hacerlo te dará perspectiva y te ayudará a cultivar tu resiliencia.
Fuente	Seligman, M. (2011). *Building Resilience*. Recuperado de https://hbr.org/2011/04/building-resilience

Práctica 05

Nombre de la práctica	Crecimiento postraumático.
Descripción de la práctica	En esta práctica harás un recuento de las situaciones difíciles a las que te has enfrentado y reflexionarás sobre lo positivo que surgió de ellas.
Palabras clave	Resiliencia.
Instrucciones para el aprendedor	La resiliencia es la capacidad de reponerse tras la adversidad, de recuperarse después de vivir experiencias difíciles, dolorosas o traumáticas. Para algunos la resiliencia implica no solo salir adelante después de una situación muy dura, sino incluso crecer o ser mejor a raíz de esta experiencia. (Tarragona, 2012) La siguiente práctica te ayudará a fomentar esta importante cualidad: 1. Escribe acerca de un momento en el que enfrentaste una adversidad significativa o pérdida. 2. Primero escribe acerca de las puertas que se te cerraron debido a esa adversidad o pérdida, ¿qué perdiste? 3. Después escribe acerca de las puertas que se abrieron al termino o como secuela de esa adversidad o pérdida. 4. ¿Hay nuevas maneras de actuar, pensar o relacionarse que son más probables de suceder ahora?
Fuente	• Ejercicio contribuido por Taylor Kreiss de University of Pennsylvania Positive Psychology Center, y basado en el libro: A Primer in Positive Psychology de Christopher Peterson.

Práctica 06

Nombre de la práctica	La mejor versión de ti mismo.
Descripción de la práctica	Escribe acerca de la mejor versión posible de ti mismo durante al menos 20 minutos.
Palabras clave	Emociones positivas, fortalezas de carácter, autorregulación y esperanza.
Instrucciones para el aprendedor	Imagina que dentro de 20 años has crecido en todas las áreas o maneras que te gustaría crecer y las cosas te han salido tan bien como te las imaginaste. • ¿Cómo es esa mejor versión de ti mismo? • ¿Qué hace él o ella cotidianamente? • ¿Qué dicen los demás acerca de él o ella? No es necesario que compartas este escrito, ya que el objetivo de esta reflexión es enfocarse en la experiencia que viviste mientras reflexionabas en esa mejor versión posible de ti mismo.

Fuente	• Ejercicio contribuido por Taylor Kreiss de University of Pennsylvania Positive Psychology Center, y basado en el libro A Primer in Positive Psychology de Christopher Peterson.

Práctica 07

Nombre de la práctica	Obtener lo que quieres.
Descripción de la práctica	Reflexionarás sobre alguna meta que desees alcanzar y propondrás una forma de conseguirla.
Palabras clave	Logro, involucramiento, fortalezas de carácter, esperanza, autorregulación, metas y objetivos a largo plazo.
Instrucciones para el aprendedor	Tener una idea clara de lo que deseas lograr a corto, mediano y largo plazo es de suma importancia, pues te ayuda a seguir un camino trazado previamente. Para que puedas generar esta guía, responde las siguientes preguntas: 1. ¿Qué quieres lograr? Al trazar tu meta, procura que esta sea específica, medible, alineada, realista, retadora y con una fecha para lograrla. Piensa en algo y utiliza el método SMART para definirla. 2. ¿Qué te impide que lo tengas en este momento? 3. ¿Qué sufrimiento estás experimentando en tu vida por no tenerlo en este momento? 4. ¿Qué placer, involucramiento, relación, significado o logro tendrías en tu vida si tuvieras eso en este momento? 5. ¿Qué hábitos te detienen o no te dejan avanzar hacia eso que quieres? 6. ¿Qué nuevos hábitos podrías generar para ayudarte a obtener lo que quieres? 7. ¿Qué dos cosas podrías hacer para romper con los hábitos que no te permiten avanzar hacia lo que quieres y generar hábitos nuevos? 8. ¿Te comprometes a hacer esas dos cosas? Si es así, ¿cuándo las harás? Escribe tus resultados en un sitio donde puedas verlos constantemente.
Fuente	• Ejercicio contribuido por Taylor Kreiss de University of Pennsylvania Positive Psychology Center, y basado en el libro A Primer in Positive Psychology de Christopher Peterson.

Práctica 08

Nombre de la práctica	Felicidad en el trabajo.
Descripción de la práctica	Reflexionarás sobre las distintas dimensiones de tu vida cotidiana, enfocando el análisis a cómo fomentar un estado de ánimo y relaciones positivos en el ámbito laboral.
Palabras clave	Involucramiento, emociones positivas, relaciones positivas.
Instrucciones para el aprendedor	Elegir conscientemente maneras de incrementar la felicidad en el trabajo puede hacer la diferencia en cómo nosotros nos sentimos y qué tan bien

	nos desempeñamos. En lugar de quejarnos del trabajo, ¿por qué no pensar en cómo podemos obtener mayor felicidad de lo que hacemos? Estar más involucrados en lo que hacemos contribuye a nuestra felicidad y bienestar, y nos lleva a un mejor desempeño y productividad. A manera de reflexión, responde las siguientes preguntas que están enfocadas en distintas dimensiones de tu vida: • **Dar:** ¿cómo estoy apoyando a mis colaboradores, compañeros, líderes, proveedores y clientes? • **Relaciones:** ¿cómo puedo mejorar mis relaciones en el trabajo?, ¿cómo logro un balance entre la vida laboral y familiar? • **Ejercicio:** ¿cómo puedo integrar la actividad física dentro de mis actividades diarias?, ¿cómo aseguro que estoy comiendo bien y descansando lo suficiente? • **Conciencia:** ¿cómo puedo construir momentos de atención plena en mi día laboral? • **Ensayo:** ¿qué habilidades estoy construyendo?, ¿qué cosas nuevas he experimentado? • **Dirección:** ¿cuáles son mis metas laborales hoy, esta semana, este año?, ¿cómo caben y contribuyen estas con mis metas de vida y me ayudan a desarrollar mis competencias en la construcción de mis relaciones y cómo contribuyo con lo anterior a ayudar a otros?, ¿cómo se pueden alinear mis metas laborales con las de mi equipo y la organización? • **Resiliencia:** ¿cuáles son mis tácticas para lidiar con los retos difíciles en el trabajo?, ¿me estoy enfocando en lo que puedo controlar?, ¿necesito pedir ayuda a otros?, ¿hay alguien a mi alrededor que requiere de mi ayuda? • **Emoción:** ¿qué cosas, aunque sean pequeñas, puedo encontrar que me pueden hacer sentir bien en mi trabajo hoy?, ¿qué me ha hecho sonreír?
Fuente	Tomado del Catálogo de actividades para profesores.

Práctica 9

Nombre de la práctica	Interacciones positivas.
Descripción de la práctica	Reflexionarás sobre las cualidades positivas que aprecias de las personas con las que interactúas diariamente.
Palabras clave	Relaciones positivas.
Instrucciones para el aprendedor	Puedes obtener mayor gozo de los momentos que compartes con tus colegas si te tomas el tiempo para pensar en lo que valoras y aprecias de ellos. Diversas investigaciones muestran que enfocarse en lo positivo que sucede diariamente ayuda a incrementar nuestra felicidad y lo mismo aplica a todas nuestras relaciones cercanas.

	El psicólogo John Gottman sugiere que, para tener relaciones felices con alguna persona, es necesario aspirar a tener cinco interacciones positivas por cada interacción negativa que se tenga con ella. Enfócate en tus compañeros y/o colegas y piensa en las siguientes preguntas. En cada caso, anota ejemplos específicos. 1. ¿Qué te atrajo de tus compañeros cuando se conocieron? 2. ¿Qué cosas han disfrutado al hacerlas juntos? 3. ¿Qué cosas realmente aprecias de ellos en este momento? 4. ¿Cuáles son sus fortalezas? Ahora, lo más importante es que cuando estés con tus compañeros te tomes el tiempo para darte cuenta y reconocer estas cualidades, sus fortalezas y las cosas que ellos hacen que realmente aprecies, así como los momentos agradables que han compartido. Piensa en estas declaraciones: • "Realmente me encanta cuando ellos...". • "Son tan buenos para...". • "Viéndolos hacer..., me recuerda ese fantástico día cuando nosotros...". Aunque realizar dicho análisis con todas las personas que conoces resulta poco práctico, puedes usar los mismos principios para mejorar tus relaciones en general. Por ejemplo, antes de pasar tiempo con alguien tómate un momento para pensar en aquellas cosas que te gustan, aprecias o admiras de esa persona o cómo te hacen sentir bien. Asimismo, después de pasar tiempo con esa persona, piensa en las cosas que apreciaste o lo que disfrutaste del tiempo que pasaron juntos.
Fuente	Basado en el Catálogo de actividades para profesores.

Práctica 10

Nombre de la práctica	Las fortalezas se muestran en nuestras historias.
Descripción de la práctica	Reflexionarás sobre las fortalezas de carácter que aplicaste en una situación.
Palabras clave	Fortalezas de carácter.
Instrucciones para el aprendedor	Antes de comenzar el ejercicio, ¿sabes cuáles son las fortalezas de carácter? Consulta la descripción de las 24 fortalezas de carácter en la siguiente liga: **El siguiente enlace es externo a la Universidad Tecmilenio, al acceder a este considera que debes apegarte a sus términos y condiciones.** http://www.viacharacter.org/www/Character-Strengths/VIA-Classification Luego de que leas cuáles son las fortalezas de carácter, realiza lo que se pide a continuación:

	1. Describe detalladamente, mediante un texto, una anécdota en la que hayas llevado a cabo alguna acción de la mejor manera posible, o bien, que hayas actuado por encima de lo ordinario. Procura enfocarlo al entorno laboral. 2. Puede ser cualquier suceso que te haya marcado por la manera en que te desenvolviste. 3. Señala en tu descripción: ¿qué ocurrió?, ¿qué papel jugaste en el suceso?, ¿qué acciones llevaste a cabo que fueron de utilidad para ti y para los demás? 4. Luego de que hayas terminado de escribir, lee tu texto y subraya las palabras y oraciones que te den una idea sobre cómo usaste cualquiera de las 24 fortalezas de carácter. 5. Observa y clasifica cuáles son las fortalezas que usaste en tu anécdota. Reflexiona sobre el impacto que estas pueden tener en tu desempeño cotidiano.
Fuente	Niemiec, R. (2016). *How to Assess Your Strengths: 5 Tactics for Self-Growth*. Recuperado de https://www.psychologytoday.com/us/blog/what-matters-most/201603/how-assess-your-strengths-5-tactics-self-growth

Práctica 11

Nombre de la práctica	Tus fortalezas en los ojos del otro.
Descripción de la práctica	En la práctica podrás reflexionar sobre la percepción que otros tienen sobre tus fortalezas de carácter.
Palabras clave	Fortalezas de carácter.
Instrucciones para el aprendedor	¿Recuerdas alguna ocasión en la que hablaste con algún colega y este te reveló algo positivo que piensa de ti? Cuando esto ocurre, usualmente deja huella en nuestros comportamientos y acciones, pues nos damos cuenta de que las personas tienen percepciones sobre nuestras fortalezas que nosotros mismos no vislumbramos. Haz lo siguiente: 1. Piensa sobre alguna vez que algún compañero de trabajo te compartió lo que piensa de ti y que te haya sorprendido. 2. Piensa en lo siguiente: ¿qué fue lo que te llamó más la atención?, ¿qué fortalezas vio en ti que pensaste que no tenías tan desarrolladas? 3. Por último, señala en un texto por qué consideras que esta revelación te causó tanto impacto, así como la manera en que te ayudó a cultivar tus fortalezas de carácter.
Fuente	Niemiec, R. (2016). *How to Assess Your Strengths: 5 Tactics for Self-Growth*. Recuperado de https://www.psychologytoday.com/us/blog/what-matters-most/201603/how-assess-your-strengths-5-tactics-self-growth

Práctica 12

Nombre de la práctica	Plantea tus objetivos como metas de aproximación y replantea tus metas de evitación.
Descripción de la práctica	Con base en lo que plantea Grenville (2012), en la práctica podrás definir diferentes tipos de metas y encontrar la mejor manera de conseguirlas.
Palabras clave	Objetivos, metas y planes.
Instrucciones para el aprendedor	La autora Bridget Grenville-Cleave (2012) comenta que en el establecimiento de metas es importante distinguir los tipos de metas que hay y menciona dos: 1. Metas de aproximación (*approach*): son las metas con resultados positivos (deseables, placenteros, benéficos o que nos gustaría tener) y hacia las cuales trabajamos. 2. Metas de evitación (*avoidance*): son las metas con resultados negativos (indeseables, dolorosos, dañinos, o nos disgustan) y en las cuales trabajamos para evitarlas. Ejemplo: **Meta de aproximación:** • Ser más eficiente. • Ser amigable y extrovertido en reuniones. • Asumir el rol de líder en el trabajo. **Meta de evitación:** • Dejar de aplazar. • Dejar de ser tan tímido en las reuniones. • No pasar desapercibido en el trabajo. Las investigaciones que se han realizado respecto a estos tipos de metas muestran que perseguir metas de evitación resulta en un detrimento del bienestar. Estos descubrimientos sugieren que el establecer metas de aproximación o replantear las metas de evitación es benéfico. Reflexiona lo siguiente: • ¿Qué tipo de metas te has planteado tú? • ¿Hay algunas metas que puedas replantear en una forma más positiva? • ¿Cuándo las tendrás listas?
Fuente	Grenville, B. (2012). *GOAL-SETTING SECRETS*. Recuperado de http://positivepsychologynews.com/news/bridget-grenville-cleave/2012013120696