Introducción a la ciberseguridad

Guía para el profesor

Clave PTTI2301

TECMILENIO

Contenido

Datos generales

Nombre: Introducción a la ciberseguridad

Nivel: Profesional Asociado

Modalidad: Connect

Clave: PTTI2301

Competencia global

Comprende los fundamentos de ciberseguridad y su impacto en las organizaciones para integrar el conocimiento, funcionamiento y los alcances que requieren las empresas en medidas de seguridad.

Competencias transversales

- Resolución de problemas.

Introducción

En el mundo actual, donde la información se ha convertido en uno de los activos más valiosos, la ciberseguridad es esencial para garantizar la continuidad operativa y la protección de datos en las organizaciones. Esta experiencia de aprendizaje ha sido diseñada para brindarte una comprensión profunda de los fundamentos de ciberseguridad y su impacto directo en la seguridad empresarial.

A lo largo de esta experiencia, explorarás qué es la ciberseguridad y sus principios fundamentales, centrándote en cómo proteger la confidencialidad, integridad y disponibilidad de la información. Analizarás las amenazas tanto internas como externas, y aprenderás a identificar y responder a los ataques más comunes, desde *malware* y *ransomware* hasta sofisticadas guerras cibernéticas entre naciones.

También abordarás las contramedidas necesarias para prevenir y mitigar estos ataques, incluyendo marcos de trabajo reconocidos como ISO, NIST e ITIL, así como la implementación de políticas, planes y procedimientos efectivos. Además, discutirás técnicas avanzadas de protección, como la criptografía, el uso de firewalls, y el desarrollo seguro de aplicaciones.

Al final de esta experiencia obtendrás la insignia "*Introduction to Cybersecurity*" de CISCO *Academy*.

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.

1. **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).
2. **Duración:** un mes, equivalente a cuatro semanas efectivas.
3. **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.
4. **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

Fuentes de consulta:

- Bustillos, O., y Rojas, J. (2022). Protocolo básico de ciberseguridad para pymes. *Interfases, 1*(16). Recuperado de https://doaj.org/article/9bd277a7a5b448bfa7db929697a22e1f
- Rodríguez, O., Dutari, R., Rodríguez, D., Fernández, L., Díaz, K., Quintero, J., y Chang, H. (2022). Percepción de la ciberseguridad. *Visión Antataura, 6*(2). Recuperado de https://research.ebsco.com/linkprocessor/plink?id=ca6b4796-328f-3a61-82c8-3ab3bc11dee0

Bibliografía de apoyo:

- Cisco. (s.f.). *Introducción a Ciberseguridad*. Recuperado de https://skillsforall.com/course/introduction-to-cybersecurity?courseLang=es-XL
- Del-Real, C. (2022). Panorama institucional de la gobernanza de la ciberseguridad en España. *Revista de Estudios Jurídicos y Criminológicos, 1*(6). Recuperado de https://research.ebsco.com/linkprocessor/plink?id=c021f72d-37a5-3b7b-a4a3-b3b813ca79d3

Recursos disponibles para consulta en la Biblioteca Digital: https://biblioteca.tecmilenio.mx/

Evaluación

La evaluación consta de lo siguiente:

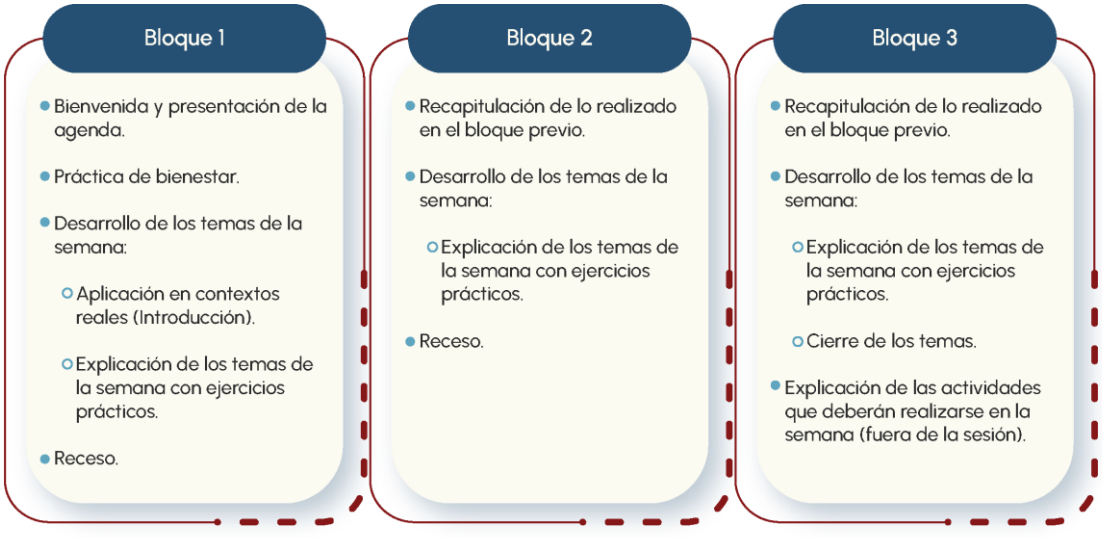
1. Actividades que retoman el contenido conceptual de los temas de la semana.
2. Proyecto con el que el participante demostrará que adquirió las habilidades y los conocimientos requeridos para acreditar el certificado. Dicho proyecto se divide en dos fases (avance y entrega final).

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.

Actividades y proyecto

Las actividades y el proyecto 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 y el proyecto realizados deberán entregarse a través de la plataforma tecnológica correspondiente 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, el proyecto o el contenido, puedes contactar a tu docente a través de los medios que te indique.

Calendario de entregas

Semana	Tema	Actividad	Fase de proyecto
1	Tema 1. ¿Qué es la ciberseguridad? Tema 2. Delincuentes de la ciberseguridad Tema 3. Conociendo los ataques más comunes de ciberseguridad Tema 4. Las contramedidas para usar en ciberseguridad Tema 5. Las políticas, planes y procedimientos en ciberseguridad	1	
2	Tema 6. Las amenazas en ciberseguridad (tipos de ataques) Tema 7. Las vulnerabilidades en ciberseguridad Tema 8. Ataques a los correos electrónicos y navegadores Tema 9. Los ataques en ciberseguridad Tema 10. Ingeniería social		1
3	Tema 11. Otros virus informáticos Tema 12. *Firewall* - Controles de acceso Tema 13. Protección en la ciberseguridad por *firewall* Tema 14. Ocultamiento de datos Tema 15. Integridad garantizada	2	
4	Tema 16. Desarrollo seguro de aplicaciones Tema 17. Los cinco nueves y respuesta a incidentes Tema 18. Defensa de sistemas en dispositivos y servidores Tema 19. Vulnerabilidades y amenazas comunes a los usuarios Tema 20. Responsabilidad y leyes cibernéticas		2

Temario

1. ¿Qué es la ciberseguridad?
    1.1 Descripción y consecuencias de la ciberseguridad
    1.2 Principios fundamentales de ciberseguridad
2. Delincuentes de la ciberseguridad
    2.1 ¿Quiénes son?
    2.2 Amenazas internas y externas
3. Conociendo los ataques más comunes de ciberseguridad
    3.1 Guerras cibernéticas entre países
    3.2 Riesgos en los sistemas informáticos
4. Las contramedidas para usar en ciberseguridad
    4.1. Tríada CID
    4.2 Marcos de trabajo (ISO, NIST, ITIL)
5. Las políticas, planes y procedimientos en ciberseguridad
    5.1 Conceptos básicos
    5.2 Seguridad física (credenciales y cámaras de seguridad)
6. Las amenazas en ciberseguridad (tipos de ataques)
    6.1 ¿Qué es *malware*?
    6.2 *Ransomware*
7. Las vulnerabilidades en ciberseguridad
    7.1 Introducción
    7.2 Código malicioso
8. Ataques a los correos electrónicos y navegadores
    8.1 ¿Cuáles son? (*Spyware, adware, scareware, vishing, smishing, pharming* y *whaling*)
    8.2 Falsificación de identidad
9. Los ataques en ciberseguridad
    9.1 DoS, DDoS, falsificación de identidad [*spoofing y Man-in-the-Middle (*MitM*)*]
    9.2 Contramedidas
10. Ingeniería social
    10.1 Técnicas
    10.2 Contramedidas
11. Otros virus informáticos
    11.1 En código (inyección de SQL y Java)
    11.2 Bombas lógicas
12. *Firewall* - Controles de acceso
    12.1 ¿Qué es un *firewall*? - Estrategias y Métodos de autenticación
    12.2 Enmascaramiento de datos
13. Protección en la ciberseguridad por *firewall*
    13.1 ¿Qué es criptografía?
    13.2 Controles de acceso
14. Ocultamiento de datos
    14.1 Enmascaramiento de red
    14.2 Esteganografía y detección
15. Integridad garantizada
    15.1 Tipos de control y firmas digitales (HASH)
    15.2 Firmas digitales, certificados y validación de datos
16. Desarrollo seguro de aplicaciones
    16.1 Aplicaciones móviles seguras
    16.2 Aplicaciones web seguras
17. Los cinco nueves y respuesta a incidentes

17.1 Medidas para mejorar la disponibilidad
17.2 Respuesta ante los incidentes y recuperación tras desastre
18. Defensa de sistemas en dispositivos y servidores
18.1 Protección contra *malware* en dispositivos móviles (herramientas y criptografía de los dispositivos móviles)
18.2 Protección contra *malware* en servidores
19. Vulnerabilidades y amenazas comunes a los usuarios
19.1 Amenazas comunes a los dispositivos
19.2 Amenazas de las redes
19.3 Ética en ciberseguridad
20. Responsabilidad y leyes cibernéticas
20.1 Ciberleyes regulatorias, civiles y penales
20.2 Protección de la privacidad

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.

Semana 1

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

Al profesor impartidor se le recomienda lo siguiente:
Es importante resaltar la relevancia de la ciberseguridad utilizando ejemplos impactantes, como el ataque a Sony Pictures en 2014. Se recomienda iniciar conectando este caso con la realidad actual de los estudiantes, subrayando cómo los ciberataques afectan tanto a individuos como a organizaciones. Al detallar los tres niveles de protección —personas, organizaciones y gobiernos—, resulta esencial fomentar la participación activa de los estudiantes mediante preguntas reflexivas que les inviten a considerar la seguridad de sus propios datos y dispositivos.

Es probable que las principales dudas surjan al tratar los principios fundamentales de ciberseguridad, en particular al diferenciar entre la identidad fuera de línea y la identidad en línea. Para aclarar estas cuestiones, se recomienda el uso de ejemplos reales o simulaciones que ilustren las diferencias entre ambas identidades y las formas en que pueden ser vulneradas. Los conceptos clave que requieren una explicación más detallada incluyen los tipos de datos que deben protegerse, como los datos transaccionales y la propiedad intelectual. Como dinámica, es posible dividir a los estudiantes en grupos y asignarles el análisis de brechas de seguridad en casos empresariales. Además, se pueden utilizar videos interactivos y estudios de casos, disponibles en plataformas como Cisco Academy y CISA, para hacer la clase más dinámica.

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

Al profesor impartidor se le recomienda lo siguiente:
Es recomendable comenzar contextualizando el perfil de los ciberdelincuentes, utilizando ejemplos significativos como el ataque al RENAPER en Argentina en 2021, lo cual ayudará a conectar a los estudiantes con situaciones del mundo real. Es importante subrayar que no se requiere ser un experto para cometer ciberdelitos, un concepto que puede ser novedoso para los estudiantes. Es fundamental explicar los diferentes tipos de *hackers* (sombrero blanco, negro y gris) y los diversos actores involucrados en el cibercrimen. Esta sección puede generar dudas sobre las motivaciones de los distintos tipos de hackers y su relación con los delitos cibernéticos. Para aclarar estas dudas, se sugiere el uso de ejemplos prácticos que ilustren cómo operan y cuáles son las diferencias clave entre ellos.

Es posible que los estudiantes también encuentren confuso el concepto de amenazas internas frente a amenazas externas. Para aclarar estas diferencias, se recomienda utilizar comparaciones directas y ejemplos visuales que resalten las características de cada tipo de amenaza, tanto a nivel personal como organizacional. Los conceptos clave que deben explicarse con mayor detalle incluyen los tipos de ataques estructurados y no estructurados, así como las amenazas que afectan tanto a individuos como a organizaciones. Como dinámica, se sugiere realizar estudios de casos en pequeños grupos, donde los estudiantes identifiquen el tipo de amenaza en diversos escenarios. Además, recursos adicionales como videos explicativos o lecturas de sitios confiables, como CISA y BBVA Noticias, pueden hacer la clase más interactiva y atractiva.

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

Al profesor impartidor se le recomienda lo siguiente:
Es conveniente iniciar conectando los conceptos teóricos con ejemplos históricos como el caso del virus Stuxnet, explicando cómo este ataque transformó la forma en que se comprenden las amenazas cibernéticas. Se recomienda abordar las características de los ataques APT (amenaza persistente avanzada), los ataques DDoS y el *ransomware*, destacando las diferencias clave entre ellos. Estos conceptos pueden resultar confusos, especialmente en relación con la forma en que se infiltran y afectan los sistemas. Para aclarar esto, es útil realizar una simulación visual que ilustre cómo cada tipo de ataque se propaga y los daños que ocasiona.

Es importante estar preparado para resolver dudas relacionadas con las capas del ciberespacio (física, sintáctica y semántica), ya que es probable que los estudiantes perciban este concepto como abstracto. La mejor forma de aclarar estas dudas es mediante ejemplos visuales o interactivos que ilustren cómo un ataque puede escalar de una capa a otra. Los conceptos que requieren mayor explicación son la identificación de vulnerabilidades y los errores humanos. Se sugiere emplear estudios de casos reales o ejercicios en los que los estudiantes deban detectar posibles fallos de seguridad. Como dinámica, se pueden organizar debates sobre los riesgos de la ciberguerra, complementados con videos de National Geographic o BBC News para mostrar el impacto de estos ataques a nivel global.

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

Al profesor impartidor se le recomienda lo siguiente:

Es recomendable comenzar abordando la importancia de la seguridad de la información en el contexto de las empresas modernas, utilizando ejemplos como la pérdida de datos financieros o el robo de información sensible para subrayar los riesgos. Al explicar la tríada CID (Confidencialidad, Integridad y Disponibilidad), se sugiere enfocarse en la interrelación entre estas dimensiones, ya que los estudiantes podrían tener dudas sobre cómo se aplican en situaciones prácticas. Para aclarar este punto, es útil emplear estudios de casos reales que muestren cómo la falla en uno de los elementos afecta a los demás, generando consecuencias negativas.

Una de las áreas donde los estudiantes podrían tener más dudas es en los marcos de trabajo (ISO 27001, NIST e ITIL), especialmente al diferenciarlos y comprender cómo cada uno contribuye a la ciberseguridad. Estas dudas pueden aclararse con ejemplos visuales, como diagramas que representen las fases de implementación de estos marcos. Los conceptos que requieren mayor explicación son la definición de riesgos y las estrategias de mitigación. Como dinámica, organiza un ejercicio práctico en el que los estudiantes identifiquen y clasifiquen riesgos en un escenario ficticio, aplicando los principios de la tríada CID y los marcos de trabajo. Para hacer la clase más interactiva, se pueden usar videos explicativos como los de UniversiK, junto con recursos adicionales del NIST, para ilustrar las mejores prácticas en tiempo real.

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

Al profesor impartidor se le recomienda lo siguiente:

Es importante abordar la relación entre la creciente dependencia tecnológica de las organizaciones y la necesidad de establecer marcos formales de ciberseguridad. Se debe comenzar explicando cómo las políticas establecen directrices claras y cómo los planes y

procedimientos proporcionan pasos específicos para proteger la infraestructura y la información. Es esencial subrayar la importancia de documentar estos lineamientos de manera accesible y clara, de modo que todos los colaboradores puedan cumplirlos correctamente. Es posible que los estudiantes presenten dudas en cuanto a las diferencias entre políticas y procedimientos. Para resolver estas dudas, se recomienda utilizar ejemplos prácticos que ilustren cómo una política de seguridad de contraseñas puede transformarse en un procedimiento detallado sobre su uso y gestión.

Una de las áreas donde los estudiantes podrían necesitar mayor explicación es el concepto de autenticación multifactor y su aplicación en escenarios reales. Es importante abordar los pros y contras de esta tecnología, utilizando ejemplos como la integración de *tokens* y factores biométricos en los sistemas empresariales. Los conceptos que requieren mayor detalle incluyen los tipos de controles de acceso, tanto lógicos como físicos. Se recomienda una actividad en la que los estudiantes diseñen un plan de seguridad básico, aplicando lo aprendido sobre políticas y procedimientos.

Notas para la actividad integradora I.
Es fundamental explicar cómo las políticas, planes y procedimientos constituyen la base de una estrategia eficaz para proteger los sistemas de información en las organizaciones. Se debe destacar que las políticas ofrecen una guía clara sobre lo que se debe y no se debe hacer, mientras que los procedimientos detallan cómo aplicar esas políticas en la práctica diaria. Una parte esencial de la lección será subrayar la importancia de documentar estas normas de forma clara y comprensible, asegurando que todos los empleados sigan los mismos lineamientos. Las dudas más frecuentes suelen surgir al diferenciar entre una política y un procedimiento. Para aclarar estas dudas, se recomienda utilizar ejemplos específicos, como políticas de acceso a la información y procedimientos para gestionar contraseñas o accesos seguros.

Además, se recomienda enfatizar los mecanismos de control de acceso, tanto físicos como lógicos, especialmente en tecnologías como la autenticación multifactor. Este concepto puede ser nuevo para muchos estudiantes y generar dudas. Para aclarar estos puntos, es útil emplear casos prácticos y simulaciones que demuestren cómo la autenticación multifactor protege a las organizaciones de accesos no autorizados. Se sugiere realizar una dinámica en la que los estudiantes diseñen una política de seguridad básica para un entorno empresarial ficticio, aplicando lo aprendido sobre políticas, procedimientos y planes de respuesta ante incidentes.

Se entrega en la semana 1.

Semana 2

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

Al profesor impartidor se le recomienda lo siguiente:
Comienza la clase explicando los conceptos fundamentales del *malware*, su evolución y los distintos tipos que existen. Inicia con ejemplos actuales que conecten a los estudiantes con situaciones reales, como el caso del ransomware, resaltando el impacto que puede tener tanto en individuos como en organizaciones. Es importante subrayar que el malware no solo afecta a nivel técnico, sino también en términos financieros y de reputación. Para aclarar posibles dudas sobre

los diferentes tipos de malware (virus, gusanos, troyanos, ransomware, etc.), utiliza gráficos y ejemplos visuales que muestren cómo cada uno opera y se disemina.

Una de las áreas que puede generar más preguntas es la diferencia entre los distintos tipos de malware y cómo pueden combinarse en un ataque. Utiliza simulaciones que demuestren, por ejemplo, cómo un troyano puede llevar a la instalación de *spyware*. Los conceptos que requieren mayor detalle incluyen los métodos de prevención y las recomendaciones para evitar infecciones por malware. Como dinámica, organiza un ejercicio en el que los estudiantes identifiquen brechas de seguridad en escenarios simulados y apliquen medidas de protección.

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

Al profesor impartidor se le recomienda lo siguiente:

Comienza explicando qué es una vulnerabilidad, utilizando ejemplos del mundo real, como las fallas en procesadores (*Meltdown* y *Spectre*), para ilustrar cómo estas debilidades pueden ser explotadas. Es fundamental que los estudiantes comprendan que existen vulnerabilidades en el *hardware*, *software* y en las personas, y cómo cada una de estas puede comprometer un sistema. Se recomienda abordar cada tipo de vulnerabilidad con ejemplos claros y destacar las medidas que pueden tomarse para mitigar los riesgos. Es posible que los estudiantes tengan dudas sobre las vulnerabilidades de hardware, ya que son menos conocidas; aclara estas dudas utilizando analogías y diagramas que demuestren cómo una falla en un componente físico puede afectar todo el sistema.

Una de las áreas que puede generar confusión es la diferencia entre las vulnerabilidades de software y hardware, por lo que se recomienda utilizar estudios de caso para mostrar las implicaciones de cada una. Los conceptos que deben explicarse con más detalle incluyen el desbordamiento de búfer y las condiciones de carrera, ya que son fundamentales para comprender cómo los errores de programación pueden ser explotados. Como dinámica, puedes proponer una actividad en la que los estudiantes analicen un sistema ficticio para identificar posibles vulnerabilidades.

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

Al profesor impartidor se le recomienda lo siguiente:

Explica cómo actividades cotidianas, como enviar correos electrónicos o navegar en internet, están expuestas a diversos tipos de ataques. Es importante destacar el papel de la ingeniería social en estas amenazas, utilizando ejemplos como el *phishing* y el *pharming* para ilustrar cómo los ciberdelincuentes se aprovechan de la falta de atención de los usuarios para obtener información confidencial. Los estudiantes podrían tener dudas sobre la diferencia entre los distintos tipos de phishing (*vishing*, *smishing*, *whaling*), por lo que es recomendable usar ejemplos claros y visuales que ayuden a diferenciarlos.

Un área que puede requerir mayor explicación es el uso de *deepfakes* en ataques de phishing. Para aclarar este concepto, utiliza recursos multimedia que muestren ejemplos de deepfakes y cómo los ciberdelincuentes los utilizan para manipular a las víctimas. Los conceptos que necesitan mayor detalle incluyen las contramedidas, como la verificación de la autenticidad de los correos electrónicos y el uso de filtros de correo no deseado. Como dinámica, organiza un ejercicio práctico en el que los estudiantes identifiquen correos de phishing y evalúen los riesgos en escenarios simulados.

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

Al profesor impartidor se le recomienda lo siguiente:

Comienza explicando cómo los ataques DoS y DDoS afectan la disponibilidad de los servicios en línea, utilizando analogías sencillas como la sobrecarga de tráfico en un sitio web que impide el acceso a los usuarios legítimos. Enfatiza que estos ataques son relativamente sencillos de ejecutar, lo que aumenta su frecuencia y los convierte en una amenaza significativa para las empresas. Los estudiantes pueden tener dudas sobre la diferencia entre un DoS y un DDoS, y cómo las *botnets* juegan un papel crucial en estos últimos. Para aclarar esto, utiliza diagramas que representen cómo las botnets distribuyen los ataques desde múltiples fuentes.

Otra área que puede requerir mayor explicación es el concepto de *spoofing*, especialmente en sus diversas formas (web, correo electrónico, DNS, ARP). Es importante destacar cómo los atacantes manipulan direcciones IP o crean sitios web falsos para engañar a las víctimas y obtener información confidencial. Los conceptos que necesitan más detalle incluyen los ataques de "*man in the middle*" (MITM) y las contramedidas que pueden implementarse, como el uso de VPNs y soluciones de seguridad *endpoint*. Como dinámica, organiza un ejercicio en el que los estudiantes identifiquen un ataque DDoS o de spoofing en un caso simulado y propongan las mejores contramedidas.

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

Al profesor impartidor se le recomienda lo siguiente:

Comienza con un caso práctico para captar la atención de los estudiantes, como el ejemplo proporcionado en la introducción sobre el robo de credenciales mediante un correo electrónico falso. Esto ayudará a los estudiantes a comprender cómo las técnicas de manipulación psicológica, como el phishing, pueden comprometer la seguridad de una empresa. A lo largo de la clase, es crucial enfatizar que la ingeniería social explota las emociones humanas y la falta de conocimiento, por lo que la prevención efectiva requiere tanto medidas técnicas como educación continua. Es importante abordar las diferentes técnicas (phishing, *pretexting*, *baiting*, entre otras), utilizando ejemplos y simulaciones.

Es probable que los estudiantes encuentren confusa la diferencia entre técnicas como el phishing y el pharming, ya que ambas implican la manipulación de información. Para aclarar esto, se recomienda utilizar simulaciones visuales o diagramas que muestren cómo opera cada ataque. Los conceptos que deben explicarse en mayor detalle incluyen las contramedidas, como la autenticación multifactor, la implementación de políticas de seguridad y la cultura organizacional enfocada en la ciberseguridad. Como actividad dinámica, organiza un ejercicio en el que los estudiantes identifiquen señales de un ataque de ingeniería social en correos o mensajes ficticios.

Notas para el avance de proyecto.

Se recomienda realizar un recorrido guiado sobre cómo acceder a la plataforma **Cisco Skills for All** y enfatizar la importancia de comprender los conceptos básicos de ciberseguridad antes de iniciar el examen de certificación. Es esencial resaltar cómo las habilidades adquiridas en este curso son aplicables en escenarios laborales, abordando las amenazas cibernéticas comunes y las contramedidas que las empresas implementan para proteger su información. Un área que puede generar dudas es el uso adecuado de la plataforma de Cisco y cómo completar todos los módulos requeridos. Se deben aclarar estas inquietudes utilizando capturas de pantalla que expliquen el proceso de registro y acceso a los módulos, como se muestra en las instrucciones. Además, es

crucial explicar detalladamente la rúbrica de evaluación, para que los estudiantes comprendan cómo se medirá su progreso y qué se espera en el entregable final.

Se entrega en la semana 2.

Semana 3

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

Al profesor impartidor se le recomienda lo siguiente:
Comienza con una explicación clara sobre las vulnerabilidades y amenazas asociadas con la inyección de código SQL y el *scripting* entre sitios (XSS), dos de los ataques más comunes que enfrentan las aplicaciones web en la actualidad. Se recomienda utilizar ejemplos prácticos para mostrar cómo los atacantes emplean estas técnicas para comprometer la confidencialidad y la integridad de los sistemas. Es importante destacar que, aunque estos ataques explotan debilidades técnicas, su impacto puede ser devastador para las organizaciones, desde la pérdida de datos sensibles hasta la exposición de información personal de los usuarios.

Los estudiantes podrían tener más dudas sobre las diferencias entre SQLi y XSS, especialmente en cómo se ejecutan y qué tipo de datos comprometen. Para aclarar esto, utiliza diagramas y simulaciones de ataques que muestren cómo cada uno afecta tanto a las aplicaciones como a los usuarios. Los conceptos que deben explicarse con mayor detalle incluyen las contramedidas, como el uso de *firewalls* de aplicaciones web (WAF), la actualización continua del software y la validación de las entradas de los usuarios. Como dinámica, organiza un taller donde los estudiantes practiquen la identificación de posibles vulnerabilidades en el código y propongan soluciones para mitigarlas.

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

Al profesor impartidor se le recomienda lo siguiente:
Comienza explicando la importancia de los firewalls como una primera línea de defensa en la protección de redes empresariales. Es recomendable utilizar el ejemplo presentado en la introducción, donde una empresa financiera implementa un *firewall* para prevenir accesos no autorizados, ilustrando cómo estas herramientas ayudan a mitigar riesgos. Es crucial enfatizar los diferentes tipos de firewall, desde los tradicionales de filtrado de paquetes hasta los de próxima generación, explicando cómo cada uno cumple funciones específicas en el contexto de la seguridad de la información. Se recomienda hacer un recorrido por las principales funcionalidades, incluyendo el filtrado de tráfico, la segmentación de redes y la auditoría de registros.

Es probable que los estudiantes tengan dudas sobre cómo funcionan los firewalls de inspección con estado y los de próxima generación, especialmente en relación con la inspección profunda de paquetes. Para aclarar estos puntos, se recomienda utilizar diagramas que muestren cómo los firewalls analizan el tráfico y toman decisiones sobre qué datos bloquear o permitir. Los conceptos que necesitan mayor detalle incluyen las estrategias de segmentación de red y el enmascaramiento de datos, que son esenciales para proteger la información sensible en entornos de pruebas o producción. Como dinámica, organiza un ejercicio práctico en el que los estudiantes configuren un firewall en un entorno simulado y apliquen políticas de acceso.

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

Al profesor impartidor se le recomienda lo siguiente:
Comienza explicando la relevancia de los firewalls como parte esencial de una estrategia de ciberseguridad en las organizaciones. Destaca que los firewalls actúan como barreras que filtran el tráfico entre redes confiables y no confiables, protegiendo los recursos internos de accesos no autorizados y ataques cibernéticos. Es crucial que se explique el funcionamiento de los firewalls a través de reglas de filtrado de paquetes, inspección con estado y firewalls de próxima generación, utilizando ejemplos claros y aplicables al entorno empresarial.

Los estudiantes podrían tener dudas sobre las diferencias entre los diversos tipos de firewalls y los métodos de autenticación que emplean. Para aclarar estos conceptos, utiliza diagramas que ilustren cómo se manejan las conexiones a través de los firewalls y cómo se toman decisiones de bloqueo o permiso según las políticas de seguridad establecidas. Los conceptos que requieren mayor detalle incluyen las estrategias de segmentación de red y el uso de firewalls de próxima generación para protección avanzada contra ataques. Como dinámica, organiza un ejercicio práctico en el que los estudiantes configuren un firewall en un entorno virtual, aplicando diferentes reglas de acceso y monitoreando el tráfico bloqueado.

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

Al profesor impartidor se le recomienda lo siguiente:

Comienza explicando la importancia del enmascaramiento de red (NAT) y la esteganografía como herramientas clave para proteger la información en un entorno de ciberseguridad. Utiliza ejemplos prácticos, como el uso de NAT para ocultar las direcciones IP internas de una empresa, lo que permite proteger los dispositivos conectados a la red de amenazas externas. Aclara cómo estas técnicas funcionan como capas adicionales de seguridad, proporcionando una barrera contra posibles ataques y aumentando la confidencialidad de los sistemas.

Es probable que los estudiantes presenten dudas en cuanto a las diferencias entre el enmascaramiento mediante NAT y la esteganografía, así como los distintos modos de NAT (estático, dinámico y con sobrecarga). Para aclarar estas diferencias, utiliza diagramas que ilustren cómo funciona cada técnica y cómo se aplican en diferentes escenarios. Los conceptos que requieren mayor detalle son las limitaciones de NAT en cuanto al rendimiento y las vulnerabilidades que presenta, así como las técnicas de esteganografía más avanzadas. Como dinámica, organiza una actividad en la que los estudiantes analicen imágenes o archivos en busca de datos ocultos mediante esteganografía.

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

Al profesor impartidor se le recomienda lo siguiente:

Explica los conceptos clave relacionados con la firma digital, los algoritmos hash y los certificados digitales. Comienza destacando la importancia del uso de los hashes en ciberseguridad para garantizar la integridad de los datos. Utiliza un ejemplo práctico de cómo se genera un hash mediante algoritmos como SHA-256, explicando cómo este proceso asegura que cualquier cambio en los datos sea detectable. Enfatiza que el hash es una herramienta de uso cotidiano en la protección de contraseñas y en tecnologías como *blockchain*.

Es probable que los estudiantes tengan dudas sobre el funcionamiento de las firmas digitales y el proceso de validación de documentos electrónicos. Para aclarar estos conceptos, desglosa cada paso del proceso, desde la generación de un hash hasta la encriptación con claves públicas y privadas, utilizando diagramas visuales que ilustren el proceso. Los conceptos que requieren mayor detalle incluyen la diferencia entre firmas digitales y firmas electrónicas tradicionales, así como las aplicaciones prácticas de los certificados digitales. Como dinámica, se sugiere organizar un ejercicio en el que los estudiantes validen un documento firmado digitalmente utilizando herramientas disponibles en línea.

Notas para la actividad integradora II.
Divide la clase en dos partes. En la primera, es fundamental explicar en detalle los diferentes tipos de códigos maliciosos, como virus, malware y ransomware, destacando cómo afectan tanto a organizaciones como a personas. Utiliza ejemplos reales de incidentes de seguridad, como el ataque de ransomware a Colonial Pipeline, para ilustrar cómo estos códigos maliciosos pueden interrumpir operaciones, causar pérdida de datos y poner en riesgo información confidencial. Se recomienda enfatizar la importancia de la ciberseguridad preventiva para mitigar estos riesgos.

En la segunda parte, profundiza en las tácticas utilizadas en los ataques a correos electrónicos, como el phishing, spoofing y spear-phishing. Es probable que los estudiantes tengan dudas sobre cómo distinguir entre estas técnicas y cómo se ejecutan en la práctica. Para aclarar estos conceptos, utiliza ejemplos de correos falsos y realiza un análisis conjunto con los estudiantes, destacando los indicadores que revelan un ataque. Los conceptos que deben explicarse con mayor detalle incluyen cómo los atacantes utilizan la ingeniería social para manipular a los usuarios. Como dinámica, organiza un ejercicio práctico en el que los estudiantes identifiquen correos maliciosos y propongan medidas preventivas.

Se entrega en la semana 3.

Semana 4

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

Al profesor impartidor se le recomienda lo siguiente:
Explica la importancia de la seguridad en cada etapa del ciclo de desarrollo de software, tanto en aplicaciones móviles como web. Comienza con ejemplos prácticos, como el impacto de brechas de seguridad en aplicaciones populares, para ilustrar la gravedad de no implementar medidas de ciberseguridad desde el diseño hasta el despliegue. Es fundamental destacar las diferencias entre las fases del desarrollo de aplicaciones móviles y web, así como las herramientas y técnicas utilizadas para mitigar riesgos en cada etapa, como el análisis de vulnerabilidades y la autenticación multifactor.

Es probable que los estudiantes presenten dudas sobre cómo prevenir ataques como el Cross-Site Scripting (XSS) o la inyección SQL en aplicaciones web. Para aclarar estos conceptos, utiliza ejemplos de código y simula ataques para demostrar cómo estas vulnerabilidades pueden ser explotadas. Los conceptos que requieren mayor detalle son las pruebas de penetración y la

validación de entradas para evitar ataques. Como dinámica, se sugiere organizar un ejercicio en el que los estudiantes auditen una aplicación ficticia en busca de vulnerabilidades comunes y propongan mejoras.

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

Al profesor impartidor se le recomienda lo siguiente:

Comienza explicando el concepto de "cinco nueves" (99.999% de disponibilidad) y su relevancia en la ciberseguridad, especialmente para garantizar la continuidad operativa de los servicios críticos. Es fundamental que los estudiantes comprendan que la disponibilidad total es un ideal casi inalcanzable, pero las empresas deben esforzarse por acercarse lo más posible para evitar tiempos de inactividad, que pueden ser extremadamente costosos. Utiliza ejemplos de infraestructuras críticas, como bancos o plataformas de comercio electrónico, para ilustrar el impacto financiero y reputacional que incluso minutos de inactividad pueden tener. Se recomienda enfatizar la importancia de invertir en redundancia, conmutación por error y soluciones automatizadas para alcanzar una alta disponibilidad.

Una parte del tema que puede generar más dudas es el proceso para implementar un Plan de Recuperación ante Desastres (DRP). Para aclarar estas dudas, utiliza un enfoque práctico, explicando cómo se establecen los objetivos de tiempo de recuperación (RTO) y los puntos de recuperación (RPO), que determinan el tiempo máximo tolerable para restaurar operaciones críticas y la cantidad de datos que puede perderse sin afectar gravemente a la organización. Los conceptos que requieren mayor detalle incluyen las diferencias entre los distintos tipos de planes de recuperación, como la virtualización y la recuperación en la nube. Como dinámica, organiza un ejercicio en el que los estudiantes diseñen un plan de recuperación para un entorno simulado, asegurando la alineación con los RTO y RPO.

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

Al profesor impartidor se le recomienda lo siguiente:

Explica la importancia crítica de proteger tanto dispositivos móviles como servidores, ya que ambos son objetivos constantes en el ámbito de la ciberseguridad. Comienza destacando los tipos de malware que afectan a estos sistemas y cómo los ataques pueden comprometer la integridad, confidencialidad y disponibilidad de los datos almacenados. Enfatiza que las amenazas varían entre dispositivos móviles y servidores, por lo que las estrategias de protección deben diferenciarse. Para los dispositivos móviles, es fundamental hablar sobre criptografía y el uso de soluciones de seguridad confiables para mitigar los riesgos.

Es probable que los estudiantes presenten dudas sobre cómo aplicar medidas de protección, como la implementación de llaves SSH en servidores o el uso de software de criptografía en dispositivos móviles. Para aclarar estas dudas, utiliza ejemplos de configuraciones prácticas de servidores y simula el proceso de autenticación segura en un entorno controlado. Los conceptos que requieren mayor detalle son la protección de datos mediante cifrado y las herramientas de prevención de intrusiones, como IDS e IPS. Como dinámica, organiza un ejercicio práctico en el que los estudiantes configuren medidas de seguridad básicas en un servidor simulado y protejan datos en un dispositivo móvil ficticio mediante criptografía.

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

Al profesor impartidor se le recomienda lo siguiente:

Explica las diferencias entre vulnerabilidades y amenazas, utilizando ejemplos cotidianos que los estudiantes puedan comprender, como aplicaciones maliciosas o contraseñas débiles. Es importante resaltar que las vulnerabilidades representan debilidades en los sistemas, mientras que las amenazas son acciones que explotan esas vulnerabilidades. Puedes referirte a casos reales de ataques como el phishing o ransomware, explicando cómo los ciberdelincuentes aprovechan las vulnerabilidades para infiltrarse en redes o dispositivos. También se debe destacar la importancia de las actualizaciones de software para corregir vulnerabilidades conocidas.

Es probable que los estudiantes presenten dudas sobre cómo protegerse frente a estas amenazas en su vida diaria. Para aclarar esto, utiliza ejemplos prácticos, como la configuración de contraseñas seguras, la autenticación multifactor y el uso de redes wifi seguras. Los conceptos que requieren mayor detalle incluyen las amenazas en redes inalámbricas y locales, así como las buenas prácticas para evitar ser víctimas de ataques de malware o phishing. Como dinámica, organiza un ejercicio práctico en el que los estudiantes identifiquen posibles vulnerabilidades en una red simulada y propongan soluciones para mitigarlas.

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

Al profesor impartidor se le recomienda lo siguiente:

Explica la importancia de las regulaciones y leyes que rigen la ciberseguridad, haciendo énfasis en cómo estas leyes protegen tanto a individuos como a organizaciones de los delitos informáticos. Se recomienda iniciar con un panorama general de las ciberleyes en México, mencionando la Ley Federal de Protección de Datos Personales y los delitos informáticos tipificados en el Código Penal Federal. Utiliza ejemplos como el caso del ataque al SPEI en 2018 para ilustrar las implicaciones legales de no cumplir con estas normativas. Es importante que los estudiantes comprendan que las leyes cibernéticas no solo castigan a los ciberdelincuentes, sino que también imponen responsabilidades sobre las empresas para proteger la privacidad y seguridad de los datos de sus usuarios.

Una parte del tema que puede generar más dudas es la diferencia entre los diversos tipos de delitos informáticos y cómo se aplican las sanciones legales. Aclara conceptos como el acceso no autorizado, fraude digital y la Ley Olimpia, utilizando ejemplos prácticos para ilustrar las consecuencias de estos delitos. Los conceptos que requieren mayor detalle son las medidas de protección de la privacidad y las implicaciones legales para las empresas que incumplen con las regulaciones de ciberseguridad. Como dinámica, se sugiere organizar un debate donde los estudiantes analicen casos recientes de delitos informáticos y propongan estrategias de cumplimiento legal.

Notas para la actividad integradora II.

Guía a los estudiantes en un análisis profundo de casos de ciberataques de alto perfil, como los mencionados en las instrucciones (ej. Uber y Cambridge Analytica). El enfoque debe estar en comprender cómo las empresas gestionan las advertencias previas y las crisis durante los ataques, así como el impacto en clientes, socios y la imagen pública. Enfatiza que el objetivo no es solo describir los eventos, sino reflexionar sobre las lecciones aprendidas y cómo pueden aplicarse para mejorar la ciberseguridad en los entornos laborales y educativos de los estudiantes.

Es probable que los estudiantes presenten dudas sobre cómo evaluar las respuestas empresariales ante los ataques y qué aspectos clave deben considerar para desarrollar estrategias de

ciberseguridad. Aclara estos puntos proporcionando ejemplos de análisis críticos sobre las medidas implementadas por las empresas. Los conceptos que requieren mayor detalle incluyen la identificación de contramedidas eficaces y la planificación de respuestas ante incidentes. Como dinámica, se sugiere que los estudiantes trabajen en grupos para realizar un análisis conjunto de un caso y diseñen un cronograma de implementación de mejoras de seguridad en su propio contexto.

Se entrega en la semana 4.

Anexo 1. Rúbricas de evaluación

Rúbrica de la actividad I

Nivel de desempeño				
Criterios de evaluación	**Altamente competente** **100%-86%**	**Competente** **85%-70%**	**Aún sin desarrollar la competencia** **69%-0%**	%
1. Identificación de elementos clave	25 – 21 puntos	20 – 18 puntos	17 – 0 puntos	**25**
	Identifica y destaca los elementos clave que respaldan la importancia de la ciberseguridad en la sociedad moderna.	Identifica los elementos clave que respaldan la importancia de la ciberseguridad en la sociedad moderna pero no destaca correctamente de acuerdo con su importancia.	Muestra dificultades para identificar y destacar los elementos clave que respaldan la importancia de la ciberseguridad en la sociedad moderna.	
2. Organización lógica	15 – 11 puntos	10 – 8 puntos	7 – 0 puntos	**15**
	La organización lógica de los elementos identificados en el diseño conceptual está presentada de manera coherente y estructurada.	La organización lógica de los elementos identificados en el diseño conceptual está presentada de manera coherente, pero no estructurada.	Tiene dificultades para organizar lógicamente los elementos identificados en el diseño conceptual, tanto en términos de coherencia como de estructuración.	
3. Claridad y comprensión fundamentales de la ciberseguridad	10 – 8 puntos	7 – 5 puntos	4 – 0 puntos	**10**
	El diseño conceptual es claro y fácil de comprender para cualquier persona que lo vea, y comunica de manera efectiva los aspectos clave.	El diseño conceptual es claro, pero no fácil de comprender para cualquier persona que lo vea.	El diseño conceptual no es claro ni fácil de comprender para cualquier persona que lo vea.	

4. Investigación y recopilación de información	25 – 21 puntos	20 – 18 puntos	17 – 0 puntos	**25**
	Muestra calidad y profundidad de la investigación realizada para identificar y comprender las tres consecuencias importantes de la vulnerabilidad cibernética.	Demuestra calidad, pero poca profundidad de la investigación realizada para identificar y comprender las tres consecuencias importantes de la vulnerabilidad cibernética.	Poca calidad y profundidad de la investigación realizada para identificar y comprender las tres consecuencias importantes de la vulnerabilidad cibernética.	
5. Descripción detallada	15 – 11 puntos	10 – 8 puntos	7 – 0 puntos	**15**
	Capacidad del participante para describir detalladamente cómo estas consecuencias afectan a las personas, empresas u organizaciones. Deben proporcionarse ejemplos concretos si es posible.	Capacidad del participante para describir detalladamente cómo estas consecuencias afectan a las personas, empresas u organizaciones. No presenta ejemplos concretos.	Se le dificulta al participante describir detalladamente cómo estas consecuencias afectan a las personas, empresas u organizaciones. No presenta ejemplos concretos.	
6. Fundamentación en fuentes confiables	10 – 8 puntos	7 – 5 puntos	4 – 0 puntos	**10**
	La exploración de las consecuencias está respaldada por fuentes confiables y se citan adecuadamente. La información debe ser precisa y verificable.	La exploración de las consecuencias está respaldada por fuentes confiables, pero no se citan adecuadamente.	La exploración de las consecuencias no está respaldada por fuentes confiables y no se citan adecuadamente.	
			TOTAL	100

Rúbrica del avance de proyecto

	Nivel de desempeño			
Criterios de evaluación	**Altamente competente** **100%-86%**	**Competente** **85%-70%**	**Aún sin desarrollar la competencia** **69%-0%**	%
Avance del curso de CISCO Academy.	100 – 86 puntos	85 – 70 puntos	69 – 0 puntos	**100**
	El documento en Word contiene capturas de pantalla que muestran un avance de mínimo el 86 % de los módulos, el examen de certificación y la obtención de la insignia digital. El formato y la estructura son impecables.	El documento en Word contiene capturas de pantalla que muestran un avance del 70 al 85 % de los módulos, el examen de certificación y la obtención de la insignia digital. El formato es adecuado, con leves errores.	El documento en Word presenta capturas de pantalla que muestran un avance menor al 70 % de los módulos, el examen de certificación, o la insignia digital. El formato es deficiente y afecta la claridad del entregable.	
			TOTAL	**100%**

Rúbrica de la actividad II

Nivel de desempeño				
Criterios de evaluación	**Altamente competente 100%-86%**	**Competente 85%-70%**	**Aún sin desarrollar la competencia 69%-0%**	%
1. Investigación de códigos maliciosos	25 – 21 puntos	20 – 18 puntos	17 – 0 puntos	**25**
	Profundidad en la investigación realizada sobre los tipos de códigos maliciosos, como virus, *malware* y *ransomware*. Debe demostrarse una comprensión sólida de estos conceptos.	Poca profundidad en la investigación realizada sobre los tipos de códigos maliciosos, como virus, malware y ransomware. Debe demostrarse una comprensión sólida de estos conceptos.	Se le dificulta la profundidad en la investigación realizada sobre los tipos de códigos maliciosos, como virus, malware y ransomware. No demuestra una comprensión sólida de estos conceptos.	
2. Descripción de impactos	15 – 11 puntos	10 – 8 puntos	7 – 0 puntos	**15**
	Capacidad del participante para describir con precisión y de manera detallada cómo estos códigos pueden afectar a organizaciones y personas. Deben destacarse los posibles impactos, como la pérdida de datos, la disrupción de operaciones y el robo de información confidencial.	Capacidad del participante para describir con precisión y de manera detallada cómo estos códigos pueden afectar a organizaciones y personas. No se destacan los posibles impactos, como la pérdida de datos, la disrupción de operaciones y el robo de información confidencial.	Se le dificulta describir con precisión y de manera detallada cómo estos códigos pueden afectar a organizaciones y personas. No se destacan los posibles impactos, como la pérdida de datos, la disrupción de operaciones y el robo de información confidencial.	
3. Uso de ejemplos	10 – 8 puntos	7 – 5 puntos	4 – 0 puntos	**10**
	Inclusión de ejemplos concretos o casos reales para ilustrar los efectos de los códigos maliciosos. Los	Inclusión de ejemplos poco concretos o casos reales para ilustrar los efectos de los códigos maliciosos.	Se le dificulta la inclusión de ejemplos concretos o casos reales para ilustrar los efectos	

	ejemplos deben ser pertinentes y ayudar a los demás a comprender mejor los conceptos.	Los ejemplos deben ser pertinentes y ayudar a los demás a comprender mejor los conceptos.	de los códigos maliciosos.	
4. Investigación de tácticas de ataque	25 – 21 puntos	20 – 18 puntos	17 – 0 puntos	**25**
	Calidad y amplitud de la investigación realizada sobre las tácticas comunes utilizadas en los ataques a correos electrónicos, como el *phishing*, el *spoofing* y el *spear-phishing*.	Calidad, pero poca amplitud de la investigación realizada sobre las tácticas comunes utilizadas en los ataques a correos electrónicos, como el phishing, el spoofing y el spear-phishing.	Se le dificulta la calidad y amplitud de la investigación realizada sobre las tácticas comunes utilizadas en los ataques a correos electrónicos, como el phishing, el spoofing y el spear-phishing.	
5. Descripción detallada	15 – 11 puntos	10 – 8 puntos	7 – 0 puntos	**15**
	Capacidad del participante para describir detalladamente cómo se ejecutan estas tácticas, desde la creación de mensajes engañosos hasta el uso de enlaces y archivos adjuntos maliciosos. Debe demostrarse un conocimiento sólido de los procesos involucrados.	Capacidad del participante para describir detalladamente cómo se ejecutan estas tácticas, desde la creación de mensajes engañosos hasta el uso de enlaces y archivos adjuntos maliciosos. Pero sus descripciones son demasiado cortas.	Se le dificulta describir detalladamente cómo se ejecutan estas tácticas, desde la creación de mensajes engañosos hasta el uso de enlaces y archivos adjuntos maliciosos.	
6. Ejemplos específicos	10 – 8 puntos	7 – 5 puntos	4 – 0 puntos	**10**
	Inclusión de ejemplos específicos que ilustren cómo funcionan estas tácticas y cómo pueden engañar a las personas. Los ejemplos deben ser claros y pertinentes para ayudar a otros	Inclusión de ejemplos específicos que ilustren cómo funcionan estas tácticas y cómo pueden engañar a las personas. Pero los ejemplos no son claros y pertinentes para ayudar a otros	Se le dificulta la inclusión de ejemplos específicos que ilustren cómo funcionan estas tácticas y cómo pueden engañar a las personas.	

	a comprender las amenazas.	a comprender las amenazas.		
			TOTAL	**100**

Rúbrica de la entrega final del proyecto

Nivel de desempeño				
Criterios de evaluación	**Altamente competente** **100%-86%**	**Competente** **85%-70%**	**Aún sin desarrollar la competencia** **69%-0%**	%
1. Investigación.	20 - 18	17 - 15	14 - 0	**20**
	Se seleccionaron noticias bien documentadas y relevantes, con fuentes confiables y citadas correctamente.	Se seleccionaron noticias relevantes, aunque algunas fuentes pueden no ser las más adecuadas o la documentación es limitada.	Se seleccionaron noticias inadecuadas o poco relevantes, con fuentes poco confiables o sin citar correctamente.	
2. Análisis y descripción del evento.	25 - 23	22 - 20	19 - 0	**25**
	Se describe y analiza el evento de manera detallada, incluyendo amenazas, riesgos, contramedidas y responsabilidades.	El evento se describe y analiza adecuadamente, aunque falta detalle en algunos aspectos importantes.	La descripción y el análisis del evento son incompletos o carecen de detalles clave.	
3. Evaluación de la respuesta y gestión de crisis.	25 - 23	22 - 20	19 - 0	**25**
	Se presenta un análisis profundo de la respuesta de la empresa y de su gestión de la crisis, destacando fortalezas y áreas de mejora.	El análisis es adecuado, aunque podría beneficiarse de mayor profundidad o de una consideración más detallada de algunos aspectos críticos.	El análisis es superficial y no aborda de manera adecuada la respuesta de la empresa ni la gestión de la crisis.	
4. Reflexión sobre el impacto mundial y conclusiones.	15 - 13	12 - 10	9 – 0	**15**
	La reflexión es profunda, demuestra un entendimiento claro del impacto global del ciberataque y ofrece	La reflexión es adecuada y demuestra un entendimiento general del impacto, aunque las	La reflexión es superficial, carece de profundidad y las conclusiones no están bien	

	conclusiones bien fundamentadas.	conclusiones podrían estar más elaboradas.	fundamentadas en el análisis previo.	
5. Elaboración del cronograma y reporte final.	15 - 13	12 - 10	9 - 0	**15**
	El cronograma y el reporte son completos, bien organizados y detallados, cumpliendo con todos los puntos requeridos de manera coherente.	El cronograma y el reporte son adecuados, aunque podrían beneficiarse de mayor especificidad, estructura o detalle en algunas áreas.	El cronograma y el reporte son incompletos, desorganizados o carecen de claridad y detalle, sin cubrir todos los puntos requeridos.	
			TOTAL	**100%**

Anexo 2. 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 sólo 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