UNIVERSIDAD TECMILENIO

Notas de enseñanza

Ciberseguridad

LSTI2318

LBTI2518

Índice

Información general del curso

- Clave banner semestral: LSTI2318
- Clave banner bimestral/ejecutivo: LBTI2518

Competencia del certificado
Implementa técnicas y herramientas de gestión de ciberseguridad en diferentes contextos profesionales de TI, asegurando la protección de la información y el cumplimiento normativo.

Metodología semestral

- El certificado se imparte con la técnica didáctica de *Aprendizaje basado en retos*.
  - El certificado está diseñado en 18 temas para desarrollar la competencia.
  - Se desarrollan 5 actividades con rúbrica.
- La evaluación del certificado está integrada por:
  - 5 actividades
  - 1 avance de reto
  - 1 entrega final del reto
  - 1 presentación del reto

Metodología bimestral/ejecutivo

- El certificado se imparte con la técnica didáctica de *Aprendizaje basado en retos*.
  - El certificado está diseñado en 18 temas para desarrollar la competencia.
  - Se desarrollan 5 actividades con rúbrica.
- La evaluación del certificado está integrada por:
  - 5 actividades
  - 1 avance de reto
  - 1 entrega final del reto
  - 1 examen final

Evaluación semestral

Semana	Instrumento evaluador	Porcentaje
1	Actividad 1	6
2	Actividad 2	6
3	Avance del reto	25
4	Actividad 3	6
5	Actividad 4	6
6	Actividad 5	6
7	Entrega final del reto	35
8	Presentación del reto	10
Semana de Assessment		
Total		***100 puntos***

Evaluación bimestral/ejecutivo

Semana	Instrumento evaluador	Porcentaje
1	Actividad 1	6
2	Actividad 2	6
3	Avance del reto	25
4	Actividad 3	6
5	Actividad 4	6
6	Actividad 5	6
7	Entrega final del reto	35
8	Examen final	10
Semana de Assessment		
Total		***100 puntos***

Calendario semestral

Semana	Temas	Evaluable
1	1 al 3	Actividad 1
2	4 al 6	Actividad 2
3	7 al 10	Avance del reto
4	11 al 13	Actividad 3
5	14 al 17	Actividad 4
6	18 al 20	Actividad 5
7	1 al 20	Entrega final del reto
8	1 al 20	Presentación del reto

Calendario ejecutivo/bimestral

Semana	Temas	Evaluable
1	1 al 3	Actividad 1
2	4 al 6	Actividad 2
3	7 al 10	Avance del reto
4	11 al 13	Actividad 3
5	14 al 17	Actividad 4
6	18 al 20	Actividad 5
7	1 al 20	Entrega final del reto
8	1 al 20	Examen final

Bibliografía

- Ackerman, P. (2021). *Industrial Cybersecurity: Efficiently Monitor the Cybersecurity Posture of Your ICS Environment* (2ª ed.). Reino Unido: Packt.
ISBN: 9781800202092.

  Este artículo se encuentra disponible en la Biblioteca Digital, favor de acceder a la misma para su consulta:
  https://research.ebsco.com/c/bwg4dh/search/details/yctim5h6lj?db=e000xww&limiters=None&q=Industrial+Cybersecurity%3A+Efficiently+Monitor+the+Cybersecurity+Posture+of+Your+ICS+Environment+

- Arroyo, D., Gayoso, V., y Hérnandez, L. (2020). *Ciberseguridad*. España: CSIC.
ISBN: 9788400107130.

  Este artículo se encuentra disponible en la Biblioteca Digital, favor de acceder a la misma para su consulta:

https://research.ebsco.com/c/bwg4dh/search/details/wnowo6gvir?db=e000xww&limiters=None&q=Ciberseguridad

- Gupta, C., y Goyal, K. (2020). *Cybersecurity: A Self-Teaching Introduction*. Estados Unidos: Mercury Learning and Information.
ISBN: 9781683924982.

Este artículo se encuentra disponible en la Biblioteca Digital, favor de acceder a la misma para su consulta: Recuperado de https://research.ebsco.com/c/bwg4dh/search/details/re6rsflqyb?db=e000xww&limiters=None&q=Cybersecurity%3A%20A%20Self-Teaching%20Introduction

Tips importantes

1. **Relaciona los riesgos de ciberseguridad con casos reales recientes**
   - Analiza incidentes actuales como ataques de *ransomware* a hospitales, brechas de datos en bancos o hackeos a gobiernos.
     - Ejemplo: ¿Qué errores permitieron el ataque a Pemex en 2019?

💡 Tip. Comienza la clase con una noticia de ciberseguridad y plantea un breve debate sobre qué falló, cómo se pudo prevenir y qué aprenderían de ese caso como futuros profesionales.

2. Construye una narrativa desde la amenaza hasta la respuesta

- Plantea un caso base desde el inicio del curso: una empresa ficticia que enfrenta amenazas crecientes.
- En cada módulo, los estudiantes podrán hacer lo siguiente:

  - Evaluar vulnerabilidades (tema 2).
  - Proponer políticas de control (Tema 4).
  - Diseñar respuestas a incidentes (Tema 6).
  - Integrar soluciones tecnológicas (Tema 8).

💡 Tip. Usa este caso continuo como hilo conductor y pídele a los estudiantes actualizar su plan de ciberseguridad con cada nuevo tema.

3. Fomenta habilidades técnicas mediante herramientas y simulaciones

- Invita a usar plataformas como TryHackMe, Hack The Box o simuladores en línea de firewalls, phishing o malware.
  - Ejemplo de actividad: diseñar una política Zero Trust en un entorno simulado.

💡 Tip. Divide al grupo en roles de “atacantes” y “defensores” y realiza escenarios de pentesting y respuesta para fomentar el pensamiento estratégico.

4. Usa preguntas detonadoras para promover reflexión ética y estratégica

- Plantea cuestionamientos como:
    - ¿Qué responsabilidad tiene una empresa ante una fuga de datos personales?
    - ¿Qué harías si descubres una vulnerabilidad y la empresa no actúa?

💡 Tip. Conecta estos dilemas éticos con marcos normativos como el RGPD, la Ley Federal de Protección de Datos o las normas ISO 27000.

5. Cierra cada tema con aplicación profesional directa

- Finaliza cada sesión con preguntas como estas:
    - ¿Cómo aplicarías este conocimiento si fueras el CISO de una pyme?
    - ¿Qué recomendación darías a una empresa con bajo presupuesto?

💡 Tip. Usa espacios como Padlet o foros breves para que los estudiantes propongan acciones concretas que puedan implementar en sus contextos laborales o académicos.

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 Gestión de políticas de seguridad
- 7.3 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 APIs
- 15.1 Seguridad en APIs y servicios web
- 15.2 Autenticación, autorización y protección contra ataques a APIs

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 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

Herramientas

Para asegurar que aproveches al máximo tu experiencia educativa en esta modalidad de cursos, te recomendamos que revises estos **tutoriales**.

Preguntas frecuentes

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

Lo puedes reportar a la cuenta atencioncursos@servicios.tecmilenio.mx, también puedes compartir sugerencias para el contenido y actividades del curso.

¿Quién me informa de la cantidad de sesiones y tiempo de cada una en las	El líder docente te debe de proporcionar esta información.
¿En qué semanas se aplican los exámenes parciales y el examen	Consulta con tu líder 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 calificaciones en la plataforma para que los alumnos estén informados de su avance y reciban retroalimentación de parte tuya de todo lo que realizan en el curso. En banner es el registro oficial de las calificaciones de los alumnos.

Notas de enseñanza

Semana 1

Tema 1. Fundamentos de ciberseguridad

- Inicia la sesión contextualizando la importancia de la ciberseguridad en tu vida diaria y profesional. Destaca cómo la digitalización y la dependencia tecnológica han incrementado la exposición a amenazas cibernéticas, así como la necesidad de proteger los datos y sistemas críticos.
- Refuerza los principios fundamentales de la ciberseguridad (confidencialidad, integridad y disponibilidad); después, explica su aplicación práctica mediante ejemplos visuales, como el resguardo de información personal o la continuidad operativa en una empresa.
- Aborda las principales áreas de la ciberseguridad (seguridad de red, aplicaciones, información, operativa, usuario, recuperación ante desastres, móvil y *hardware*), utilizando

analogías cotidianas para facilitar la comprensión y resaltar su impacto en la protección digital.
- Explica conceptos clave como *malware*, *phishing*, *ransomware*, *firewall*, cifrado, VPN y ataques DDoS. Muestra ejemplos reales o simulados que te permitan identificar amenazas y entender el propósito de cada herramienta o técnica de defensa.
- Propón actividades prácticas, como el análisis de correos simulados para detectar intentos de phishing, incentivando la participación y el debate sobre cómo reconocer y mitigar riesgos en escenarios reales.
- Concluye reflexionando sobre la responsabilidad compartida en la protección de la información. Invita a identificar acciones concretas que puedas implementar a nivel personal y organizacional para fortalecer la seguridad digital y adaptarte al constante cambio de las amenazas.

Tema 2. Tipos de datos

- Comienza explicando la importancia de diferenciar los tipos de datos (personales, organizacionales y gubernamentales); después, comenta cómo su clasificación y protección adecuadas son esenciales para garantizar la seguridad digital individual y colectiva.
- Proporciona ejemplos claros de datos personales (nombre, dirección, datos biométricos, financieros o de salud) y enfatiza la necesidad de tomar conciencia sobre dónde y cómo se almacenan y gestionan estos datos, tanto en entornos físicos como digitales.
- Aborda los datos organizacionales y su impacto en la reputación y operación de una empresa, destacando la importancia de proteger información como la propiedad intelectual, los datos financieros y la información de empleados y clientes, cumpliendo con normativas internas de seguridad.
- Explica el proceso de clasificación de datos según su nivel de confidencialidad (público, interno, confidencial, restringido), utilizando tablas de activos y ejemplos aplicados para que los aprendedores comprendan cómo adaptar las medidas de seguridad al tipo de información y al contexto de almacenamiento (local o en la nube).
- Desarrolla una actividad práctica de clasificación de datos: analiza ejemplos y propón medidas de protección adecuadas, simulando brechas de seguridad y discutiendo estrategias para mitigar riesgos.
- Finaliza promoviendo una cultura de ciberseguridad. Destaca la importancia de la capacitación continua y la responsabilidad individual y colectiva en la protección de la información. Identifica acciones concretas para mejorar la seguridad de tus datos en distintos entornos digitales.

Tema 3. Incidentes de seguridad

- Inicia contextualizando la relevancia de la gestión de incidentes de seguridad. Señala que más de la mitad de las empresas latinoamericanas han experimentado ciberataques recientes, lo que hace indispensable que tus aprendedores desarrollen capacidades para identificar, responder y recuperarse ante incidentes como ransomware, phishing o fugas de datos.

- Explica claramente el concepto de incidente de seguridad y su impacto en la confidencialidad, integridad y disponibilidad de la información. Apóyate en ejemplos reales y destaca la necesidad de una respuesta estratégica y organizada para limitar daños y restaurar la normalidad operativa. Detalla las cinco fases críticas de un plan de respuesta a incidentes: preparación, detección y análisis, contención y erradicación, recuperación y mejora continua. Emplea diagramas y casos prácticos que ayuden a los aprendedores a visualizar y comprender cada fase del proceso.
- Demuestra el uso de herramientas para la identificación y gestión de incidentes como SIEM, XDR, análisis de *logs* o plataformas SOAR. Diseña una actividad práctica en la que los aprendedores analicen registros de Windows Defender o XProtect, detecten eventos de malware y apliquen medidas correctivas, guiándolos paso a paso.
- Refuerza la importancia de la notificación y manejo adecuado de incidentes. Explica cómo automatizar la comunicación interna y externa mediante plataformas especializadas y destaca la necesidad de cumplir con obligaciones legales y regulatorias, manteniendo la trazabilidad del proceso.
- Finaliza promoviendo la reflexión sobre una cultura organizacional proactiva. Motiva a tus aprendedores a identificar buenas prácticas para establecer protocolos efectivos de respuesta y mejorar la comunicación ante incidentes, tanto de forma individual como colaborativa.

Actividad 1

- Cerciórate de que los aprendedores comprendan a fondo la tríada CIA (confidencialidad, integridad y disponibilidad) y su relevancia práctica al analizar incidentes reales de ciberseguridad. Para ello, pídeles que seleccionen casos de 2021 a 2024 y expliquen los efectos sobre cada uno de estos principios. Esto les permitirá vincular los conceptos teóricos con escenarios del mundo real.
- Indica a los aprendedores que clasifiquen correctamente los datos comprometidos (personales u organizacionales) utilizando la "Tabla de Clasificación CNCS (2023)". Esto fortalecerá su capacidad de identificar información sensible y aplicar medidas adecuadas de protección según su criticidad.
- Asegúrate de que los aprendedores reconozcan cada fase del ciclo de respuesta a incidentes (identificación, notificación, contención, erradicación y recuperación); asimismo, deben proponer mejoras empleando herramientas SIEM como Splunk o AlienVault. De esta manera, comprenderán cómo se gestionan los incidentes en entornos reales y fortalecerán habilidades técnicas clave.
- Recuérdales estructurar adecuadamente su análisis mediante la inclusión de un diagrama de flujo de respuesta al incidente y gráficos de clasificación. Esto no solo facilitará su comprensión, sino que también desarrollará su competencia comunicativa profesional.

Semana 2

Tema 4. Ataques y técnicas en ciberseguridad

- Inicia presentando la importancia de que los aprendedores comprendan el ciclo de vida de un ciberataque, desde el reconocimiento hasta las acciones sobre los objetivos. Relaciona esta comprensión con la capacidad de anticipar y contrarrestar tácticas maliciosas, usando ejemplos recientes como el ataque a Microsoft en 2023.
- Explica la clasificación de ciberdelincuentes según su nivel de sofisticación, desde los llamados *script kiddies* hasta los grupos APT patrocinados por estados. Esta diferenciación les permitirá diseñar estrategias de defensa adaptadas al tipo de amenaza.
- Detalla los principales tipos de malware y técnicas de infiltración vigentes, como ransomware (LockBit, Phobos), malware sin archivos, *cryptojacking*, *botnets* y ataques a contraseñas (fuerza bruta y pulverización). Destaca su evolución constante y la necesidad de medidas proactivas.
- Introduce las técnicas de análisis forense digital para investigar incidentes, incluyendo la identificación, contención, restauración y análisis de evidencias. Utiliza el caso del ataque LockBit 3.0 para ilustrar cómo se puede reconstruir una cadena de eventos y fortalecer la seguridad postincidente.
- Aborda la ingeniería social y los ataques de phishing, explicando cómo los atacantes manipulan emociones y confianza. Enseña a los aprendedores las mejores prácticas para prevenir estos ataques, como la verificación de remitentes, el uso de autenticación multifactor y la formación continua.
- Propón una actividad práctica de análisis forense básico con registros (logs) de un servidor web simulado. Los estudiantes deberán identificar patrones de ataque, IP sospechosas y elaborar recomendaciones, fomentando así la aplicación práctica de los conceptos.

Tema 5. Explotación de vulnerabilidades

- Explica la relevancia crítica de la gestión de vulnerabilidades en el panorama actual. Destaca el aumento del 37 % en los ciberataques durante 2024 y cómo la explotación de errores no corregidos, configuraciones deficientes o contraseñas débiles constituye una puerta de entrada común para incidentes graves.
- Presenta los tipos de vulnerabilidades identificados por Kaspersky (*software*, configuración, red, hardware y humanas). Utiliza ejemplos como EternalBlue, Log4Shell o XZ Utils para mostrar cómo los *exploits* aprovechan estos fallos. Enfatiza el riesgo que representan los ataques *zero-day*.
- Demuestra el proceso de identificación y explotación de vulnerabilidades con herramientas como Nmap, OWASP ZAP y Metasploit. Diseña una simulación controlada para que los aprendedores realicen un ataque sobre una aplicación web vulnerable, desde el escaneo hasta la documentación de hallazgos.
- Refuerza la importancia del parcheo prioritario (resolución de vulnerabilidades críticas en menos de 72 horas), la segmentación de redes y el modelo *Zero Trust* como medidas clave para reducir riesgos y contener ataques.
- Promueve la concienciación constante en ciberseguridad. Haz énfasis en que la combinación de tecnología, procesos y educación del usuario resulta esencial para anticipar, mitigar y responder de forma efectiva a amenazas asociadas con vulnerabilidades.
- Concluye con una reflexión sobre la priorización de recursos. Propón preguntas al grupo para debatir cómo determinar qué vulnerabilidades deben corregirse primero y cómo

complementar el parcheo con monitoreo, pruebas de penetración y políticas de mínimo privilegio.

Tema 6. Protección de datos y privacidad

- Inicia contextualizando la importancia de la protección de datos personales y la privacidad en el entorno digital actual. Destaca los riesgos derivados de la digitalización y los recientes cambios normativos en México, como la desaparición del INAI y las nuevas responsabilidades asignadas a la Secretaría Anticorrupción, lo que requiere mayor preparación en cumplimiento normativo por parte de usuarios y organizaciones.
- Explica las medidas esenciales para proteger la información, como el cifrado, las copias de seguridad, la eliminación segura de datos y las configuraciones seguras en dispositivos y redes. Asegúrate de que tus aprendedores comprendan la importancia de mantener los sistemas actualizados, utilizar contraseñas robustas, así como de activar firewalls y antivirus.
- Detalla las amenazas más comunes a la privacidad y seguridad, entre ellas phishing, malware, ransomware, *spyware* y ataques *man-in-the-middle*. Enfócate en el incremento de riesgos en dispositivos IoT y móviles; además, recomienda prácticas como el uso de Google Play Protect o la desinstalación de aplicaciones no verificadas.
- Aborda las mejores prácticas para la seguridad de redes inalámbricas y cableadas. Explica el uso de cifrado WPA3-SAE, la segmentación de red, contraseñas complejas, ocultamiento del SSID, filtrado MAC, actualización de *firmware* y uso de VPN. Diferencia los niveles de riesgo entre ambos tipos de red y enfatiza la necesidad de segmentar y controlar el acceso.
- Presenta la estrategia 3-2-1 de respaldo y recuperación, junto con los conceptos de RPO y RTO. Incorpora ejemplos actuales como el uso de *blockchain* para garantizar copias inmutables en la nube frente al ransomware.
- Guía a los aprendedores en una actividad práctica de auditoría de red doméstica. Indícales cómo identificar dispositivos conectados, analizar la configuración del *router*, implementar medidas correctivas y reflexionar sobre la aplicación del modelo Zero Trust en el hogar.

Actividad 2

- Asegúrate de que los aprendedores analicen distintos tipos de ciberataques recientes (2021-2025) e identifiquen su naturaleza, técnica utilizada e impacto. Esto les permitirá entender la lógica detrás de los ataques y prepararse mejor para anticiparlos o mitigarlos.
- Indica que simulen un ataque mediante herramientas como Metasploit o Nmap, identificando vulnerabilidades reales en entornos virtuales como Metasploitable. Esta práctica consolidará su competencia técnica para reconocer vectores de entrada y riesgos explotables.
- Motiva a los aprendedores a vincular buenas prácticas de seguridad personal y organizacional con estándares como la ISO 27001 y GDPR. Que analicen configuraciones de seguridad en sus propios dispositivos para favorecer el pensamiento crítico aplicado a su vida digital cotidiana.

- Pídeles redactar un informe técnico con una tabla resumen de ataques, vulnerabilidades y controles aplicados. Esto fomentará la síntesis analítica y su habilidad de comunicar estrategias de protección en un lenguaje profesional y estructurado.

Semana 3

Tema 7. Ciberseguridad organizacional

- Introduce el tema con el caso de Aerospacey, resaltando el impacto real de un ciberataque en una organización. Enfatiza la necesidad de una gestión integral de la ciberseguridad y cómo la ausencia de controles puede derivar en pérdidas operativas, financieras y reputacionales.
- Explica las principales tecnologías de seguridad (routers, cortafuegos, VPN, IDS/IPS, antivirus, *gateways*, MFA, *sandboxes*), detallando su función y su papel en una estrategia de defensa en capas. Emplea analogías prácticas para clarificar conceptos como segmentación de red y filtrado de tráfico.
- Aborda la gestión de políticas de seguridad. Comparte con los aprendedores cómo estas políticas funcionan a manera de reglas de tránsito en una ciudad, regulando el uso de contraseñas, correo electrónico o acceso a la información. Recalca la importancia de revisarlas y actualizarlas periódicamente.
- Resalta la capacitación continua del personal como primera línea de defensa. Explica cómo los programas de formación, simulaciones y ejercicios prácticos (como pruebas de phishing) ayudan a prevenir incidentes y fortalecer la cultura de seguridad organizacional.
- Introduce tendencias actuales como la ciberdefensa basada en inteligencia artificial, la protección en entornos híbridos y *multicloud*, además de la gestión de identidades (IAM). Subraya que la ciberseguridad es una responsabilidad compartida que requiere liderazgo en todos los niveles.
- Desarrolla una actividad práctica con firewall y análisis de tráfico usando pfSense y Wireshark. Acompaña a los aprendedores en la creación de reglas básicas, la detección de eventos y la elaboración de un informe con hallazgos y propuestas de mejora.

Tema 8. Cultura de seguridad en la organización

- Comienza con el caso de Comercializadora del Norte. Muestra cómo un ciberataque puede poner en riesgo la operación y reputación de una empresa. Destaca la importancia de un enfoque integral que combine tecnología, políticas, formación y colaboración entre áreas.
- Explica el modelo de ciberseguridad de Cisco. Ayuda a los aprendedores a comprender que la seguridad moderna debe concebirse como una plataforma integrada, apoyada en inteligencia contextual, automatización y el enfoque Zero Trust.
- Profundiza en el rol del CSIRT (equipo de respuesta a incidentes de seguridad informática), abordando sus funciones clave como monitoreo, prevención, investigación forense y colaboración global. Ilustra de qué manera herramientas como Cisco XDR, Stealthwatch y Secure Endpoint permiten una respuesta ágil y coordinada.

- Subraya la importancia de la integración tecnológica. Muestra cómo la correlación de eventos entre firewalls, SIEM, herramientas de *endpoint* y soluciones *cloud* fortalece la capacidad de respuesta ante amenazas.
- Fomenta una cultura organizacional de seguridad. Recalca que la tecnología no basta: es imprescindible establecer políticas claras, capacitar al personal y promover la corresponsabilidad de todas las áreas en la gestión de la seguridad.
- Guía una actividad práctica de simulación de respuesta ante ransomware. Los aprendedores deben diseñar un plan de respuesta, integrar herramientas Cisco y reflexionar sobre la importancia de la capacitación, colaboración y mejora continua. Ajusta el nivel de dificultad según el grupo:

    - Nivel de dificultad adaptable: para estudiantes principiantes, se recomienda proporcionar una tabla parcialmente completada como guía inicial.
    - Extensión opcional: quienes cuenten con acceso a Cisco Packet Tracer pueden simular el incidente como actividad complementaria.
    - Énfasis en la cultura de seguridad: esta actividad subraya la importancia de combinar soluciones tecnológicas con procesos de capacitación y concienciación organizacional.

Tema 9. Fundamentos de seguridad en la nube

- Inicia contextualizando el auge de la migración a entornos híbridos y multicloud. Señala que esto ha incrementado los riesgos de ransomware, fugas de datos y ataques a API, haciendo de la seguridad en la nube un factor clave para la continuidad operativa.
- Explica el modelo de responsabilidad compartida. Utiliza ejemplos para diferenciar las responsabilidades del proveedor (infraestructura y redundancia) y del cliente (configuración, cifrado e identidad). Enfatiza que la mayoría de los incidentes derivan de errores del lado del cliente.
- Detalla los modelos de servicio en la nube (IaaS, PaaS y SaaS) y sus implicaciones de seguridad. Presenta casos prácticos y destaca herramientas como CASB, IAM y políticas Zero Trust para mitigar amenazas como Shadow IT y exposición de API.
- Aborda riesgos y beneficios del entorno cloud. Comenta aspectos como cumplimiento normativo, eficiencia de costos y dependencia del proveedor. Propón estrategias como automatización, monitoreo y capacitación continua para lograr un equilibrio entre innovación y protección.
- Explica las principales estrategias de seguridad en la nube: Zero Trust, MFA, cifrado integral, segmentación y automatización. Relaciona estas medidas con estándares como NIST CSF e ISO/IEC 27017; después, destaca el papel de la orquestación y la IA para escalar defensas.
- Desarrolla una actividad práctica de auditoría en un entorno multicloud. Guía el análisis de responsabilidades, riesgos y soluciones (por ejemplo, AWS IAM o Azure Policy) y fomenta el debate sobre la gestión de identidades y el rol de tecnologías emergentes**.**
- Para las actividades, intenta crear y configurar Laboratorios de Aprendizaje, las cuentas de profesor de AWS Free Tier u Oracle Cloud permiten la generación de Learner Labs.

Tema 10. Seguridad de datos en la nube - Parte I

- Introduce el tema enfatizando que migrar a la nube ofrece ventajas operativas, pero también desafíos críticos en la protección de datos y el cumplimiento normativo. Recalca la importancia de adoptar prácticas seguras desde el inicio.
- Explica los fundamentos de la gestión de identidad y acceso (IAM). Usa analogías claras, como el ingreso a un club exclusivo, para ilustrar los conceptos de identificación, autenticación, autorización y administración de accesos.
- Detalla los modelos de control de acceso más comunes, como RBAC (por roles) y ABAC (por atributos). Acompaña a tus estudiantes en la aplicación práctica de estos modelos para limitar permisos y reducir la superficie de ataque.
- Introduce la infraestructura como código (IaC) y diferencia entre los enfoques declarativo e imperativo. Explica cómo IaC mejora la eficiencia y seguridad al permitir la automatización y estandarización de configuraciones en la nube.
- Guía una actividad práctica en la que los aprendedores simulen la gestión de IAM en Google Cloud. Incluye la creación de proyectos, definición de roles personalizados, asignación de permisos y validación de políticas.
- Finaliza reflexionando sobre los retos y beneficios de la seguridad en la nube. Invita a los aprendedores a identificar amenazas comunes (como errores de configuración), así como a analizar buenas prácticas de IAM e IaC que fortalecen el cumplimiento y la protección en entornos dinámicos.
- Para las actividades, intenta crear y configurar Laboratorios de Aprendizaje, las cuentas de profesor de AWS Free Tier u Oracle Cloud permiten la generación de *Learner Labs*.

Avance del reto

- Asegúrate de que los aprendedores comprendan cómo identificar activos críticos, evaluar riesgos y aplicar marcos normativos como ISO 27001 y GDPR, al analizar el escenario de ataque en una clínica de salud. Esto fortalecerá su pensamiento analítico y estratégico ante incidentes reales.
- Indica que simulen un ataque phishing con GoPhish, analicen tráfico con Wireshark y usen Nmap para detectar dispositivos IoT vulnerables. Estas simulaciones aumentan su competencia técnica en detección de vulnerabilidades.
- Propón que diseñen una propuesta de seguridad que incluya IAM en AWS, cifrado de datos y segmentación de red. El uso de draw.io para el diagrama los ayudará a representar gráficamente soluciones integrales de ciberseguridad.

Semana 4

Tema 11. Seguridad de datos en la nube - Parte II

- Inicia contextualizando con el caso de una empresa financiera en proceso de migración a la nube. Muestra los retos de proteger datos sensibles en un entorno compartido y destaca

la necesidad de adoptar estrategias avanzadas como IaC y seguridad de contenedores para garantizar la confidencialidad, integridad y disponibilidad de la información.
- Explica las mejores prácticas de seguridad en la nube aplicadas mediante IaC. Incluye el uso de *scripts* automatizados para desplegar recursos seguros (como *buckets* S3 cifrados y con acceso limitado), la integración de controles de acceso y la automatización del cumplimiento normativo.
- Enfatiza la importancia de incorporar la seguridad desde las etapas iniciales del ciclo de desarrollo de software (SDL), identificando y mitigando riesgos antes del despliegue.
- Aborda en detalle la seguridad de contenedores y orquestación. Explica cómo el aislamiento, la gestión de imágenes, la protección en tiempo de ejecución y el monitoreo continuo previenen accesos no autorizados y amenazas como ransomware. Introduce herramientas como Kubernetes y Docker Swarm.
- Desarrolla una actividad práctica que incluya el despliegue seguro de un bucket S3 con Terraform, análisis de imágenes Docker con Trivy y aplicación de correcciones. Asegúrate de que los estudiantes documenten hallazgos y validen configuraciones.
- Refuerza la estrategia de seguridad de AWS, basada en identificar, evitar, detectar, responder y resolver incidentes. Relaciona cada paso con ejemplos de acceso, auditoría de eventos y recuperación.
- Finaliza con una reflexión sobre cómo los contenedores y la orquestación fortalecen la seguridad en la nube. Invita a los aprendedores a identificar buenas prácticas al crear IaC y a analizar cómo la combinación de tecnologías, automatización y prácticas seguras mejora la postura de seguridad.
- Para las actividades, intenta crear y configurar Laboratorios de Aprendizaje, las cuentas de profesor de AWS Free Tier u Oracle Cloud permiten la generación de Learner Labs.

Tema 12. Seguridad en desarrollo de software - Parte I

- Comienza con el caso de Equifax (2017), donde una vulnerabilidad no atendida provocó una brecha masiva de datos. Usa este ejemplo para subrayar la importancia de integrar la seguridad desde el inicio del ciclo de vida del software.
- Explica los principios del desarrollo seguro. Introduce enfoques como seguridad por diseño y metodologías DevSecOps, donde la seguridad es responsabilidad de todo el equipo. Apóyate en ejemplos de automatización de pruebas y trabajo colaborativo.
- Detalla los modelos de referencia más relevantes, como CLASP y SSDF. Compara sus enfoques y muestra cómo pueden guiar la integración de la seguridad en proyectos nuevos o existentes. Utiliza tablas comparativas para ilustrar roles, actividades y buenas prácticas.
- Aborda las pruebas de seguridad de aplicaciones. Diferencia entre análisis estático (SAST), dinámico (DAST), composición de software (SCA) y pruebas de penetración. Explica cuándo y cómo aplicarlas para detectar vulnerabilidades antes del despliegue.
- Utiliza herramientas como OWASP ZAP y SonarQube para ejemplificar el proceso. Distingue entre pruebas internas, externas, anunciadas y encubiertas.
- Guía a los aprendedores en una actividad con WebGoat, OWASP ZAP y SonarQube. Deben explotar una vulnerabilidad (por ejemplo, SQLi), corregir el código y validar la solución con un nuevo escaneo.

- Cierra con una reflexión sobre cómo equilibrar la entrega ágil de software con pruebas exhaustivas de seguridad. Fomenta el debate sobre la formación continua de los equipos de desarrollo.

Tema 13. Seguridad en desarrollo de software - Parte II

- Abre la sesión con el caso de una *fintech* sancionada tras un ataque de ransomware y el incumplimiento del GDPR. Relaciónalo con incidentes como el de Twitter (2022) para evidenciar las consecuencias de fallos en autenticación y autorización.
- Expón las mejores prácticas de seguridad en el desarrollo de software. Incluye enfoques como *security by design,* DevSecOps y la gestión automatizada de vulnerabilidades mediante SAST, DAST o SBOM.
- Presenta una tabla con buenas prácticas que ayude a los estudiantes a interiorizar acciones clave para reducir riesgos y fomentar una cultura de seguridad.
- Detalla el proceso de respuesta a vulnerabilidades en el desarrollo seguro: identificación, análisis, priorización, corrección y validación. Usa ejemplos visuales para mostrar de qué manera herramientas como IaC, IA/ML y automatización de parches fortalecen la resiliencia.
- Profundiza en los modelos y protocolos actuales de autenticación y autorización. Explica las diferencias conceptuales y técnicas; asimismo, introduce métodos como MFA, biometría y autenticación sin contraseña, además de protocolos como OAuth 2.0, OIDC y SAML.
- Complementa con ejemplos de RBAC, ABAC y PBAC para limitar el acceso y prevenir escaladas de privilegios.
- Propón una actividad con OWASP Juice Shop. Los aprendedores deben implementar autenticación, auditar el sistema, explotar y corregir fallos de RBAC, así como validar la protección con ZAP. Refuerza el uso del *checklist* de seguridad.
- Finaliza con una reflexión sobre el equilibrio entre seguridad y experiencia de usuario. Invita a debatir cómo la automatización y la formación continua influyen en la eficacia de las prácticas de autenticación.

Actividad 3

- Asegúrate de que los aprendedores configuren entornos seguros en la nube usando Terraform, cifrando buckets S3 y validando que no sean públicos. Esto consolidará su dominio de la IaC aplicado a la protección de datos.
- Indica que analicen contenedores Docker usando Trivy y que documenten el proceso de actualización de imágenes vulnerables; así, fortalecerán su competencia para asegurar pipelines de desarrollo.

- Pide que implementen autenticación JWT en API simuladas y validen los accesos con pruebas automatizadas. Esta actividad les permitirá integrar principios de desarrollo seguro desde las primeras fases del ciclo de vida del software.
- Sugiere crear un diagrama de arquitectura segura donde se evidencie el flujo de datos protegidos. Este ejercicio mejora su comprensión visual del entorno digital y permite una mejor planeación de controles técnicos.

Semana 5

Tema 14. Seguridad en aplicaciones web

- Contextualiza con el caso de Marriott International (2018), donde una vulnerabilidad expuso los datos de 500 millones de usuarios. Muestra cómo las brechas en aplicaciones web pueden afectar la reputación y generar sanciones legales.
- Explica las principales vulnerabilidades según OWASP Top 10: inyección SQL, XSS, CSRF, fallos de control de acceso, criptografía débil, uso de componentes obsoletos, configuraciones incorrectas, fallos de autenticación y registro insuficiente. Usa ejemplos visuales para clarificar.
- Detalla las técnicas de protección: validación de entradas, consultas parametrizadas, codificación de salidas, uso de WAF, autenticación multifactor, cifrado de datos y gestión de sesiones. Destaca la necesidad de seguridad desde el diseño y la actualización constante de componentes.
- Realiza una demostración con DVWA (*Damn Vulnerable Web App*). Acompaña a los aprendedores en la identificación y explotación de vulnerabilidades como XSS o SQLi, así como en la aplicación de medidas correctivas con herramientas como Burp Suite o SQLMap.
- Refuerza la importancia de la capacitación continua. Promueve debates sobre cómo mantener el equilibrio entre experiencia de usuario y seguridad; además, enseña cómo estar al día frente a amenazas emergentes.
- Concluye con una actividad de checklist de verificación. Asegúrate de que los estudiantes hayan configurado DVWA, identificado vulnerabilidades, aplicado mitigaciones y comprendido la diferencia entre autenticación y autorización.

Tema 15. Seguridad en APIs

- Inicia con el caso de Experian (2021) y un ejemplo de una *startup* de salud. Muestra cómo una vulnerabilidad en la autenticación de una API puede poner en riesgo datos sensibles y la reputación de una organización.
- Explica los tipos principales de API (REST, SOAP, RPC y WebSocket) y sus características técnicas. Utiliza analogías visuales para facilitar la comprensión del rol de las API como puentes entre sistemas.

- Detalla los principales riesgos: autenticación y autorización deficientes, exposición excesiva de datos, ausencia de cifrado, errores de configuración y ataques de inyección. Apóyate en ejemplos actuales y tablas de riesgos para facilitar su identificación.
- Presenta las mejores prácticas de seguridad en API:

    - Implementar autenticación y autorización robustas (OAuth 2.0, JWT, RBAC, MFA).
    - Usar HTTPS/TLS para cifrar datos en tránsito.
    - Validar y sanear entradas.
    - Aplicar limitación de tasas de solicitud y monitoreo.
    - Realizar auditorías periódicas.
    - Configurar encabezados HTTP y emplear WAF.

- Organiza una actividad integral: guía a los aprendedores en el consumo y análisis de una API REST, la implementación de autenticación con JWT y OAuth 2.0, la detección de vulnerabilidades con Postman y OWASP ZAP, así como la simulación de protección con WAF.
- Finaliza con una reflexión sobre la distinción entre autenticación y autorización. Invita al grupo a debatir cómo mantener la seguridad sin sacrificar la usabilidad; después, comenta cómo mantenerse al día ante la evolución de amenazas y técnicas de ataque.

Tema 16. Seguridad en redes

- Contextualiza la sesión destacando el aumento de ciberataques, la proliferación de dispositivos IoT y la creciente complejidad de entornos híbridos. Señala que el 87 % de las brechas tienen origen en errores de configuración o segmentación, lo que hace indispensable fortalecer la resiliencia de la red.
- Explica los principios fundamentales del diseño de redes seguras: defensa en profundidad, enfoque Zero Trust, microsegmentación y monitoreo continuo. Utiliza ejemplos de hospitales o bancos para ilustrar cómo estas arquitecturas aíslan amenazas y protegen datos sensibles.
- Compara los distintos enfoques de segmentación: tradicional (VLAN y subredes), microsegmentación y segmentación basada en identidad. Ayuda a tus aprendedores a visualizar cómo estas estrategias reducen el movimiento lateral de los atacantes y facilitan el cumplimiento normativo.
- Profundiza en la protección de dispositivos de borde. Detalla la importancia del *hardening*, la actualización de firmware, el uso de TLS 1.3 y la autenticación multifactor en routers, firewalls, gateways VPN y dispositivos IoT.
- Recomienda buenas prácticas en la implementación y gestión de VPN modernas, empleando protocolos robustos como WireGuard u OpenVPN. Refuerza la necesidad de controlar los accesos remotos con autenticación avanzada.
- Desarrolla una actividad práctica que incluya la configuración de VLAN en Cisco Packet Tracer, la simulación de un ataque lateral con Kali Linux y la auditoría del tráfico con Wireshark y Nmap. Asegúrate de que los aprendedores verifiquen la contención de amenazas.
- Finaliza con una reflexión sobre resiliencia adaptativa. Invita al grupo a debatir cómo priorizar la microsegmentación, responder a ataques sin interrumpir operaciones críticas y equilibrar la automatización defensiva con el control humano.

Tema 17. Seguridad perimetral

- Contextualiza con el escenario actual del trabajo remoto, IoT y cloud. Explica que el perímetro tradicional se ha disuelto y que hoy la primera línea de defensa debe ser dinámica, adaptativa y guiada por principios de Zero Trust e inteligencia artificial aplicada a la ciberdefensa.
- Describe los componentes esenciales de la seguridad perimetral. Integra elementos físicos (muros, CCTV, sensores, iluminación y control de acceso) con tecnologías digitales como firewalls de próxima generación, sistemas IDS/IPS, VPN y gateways web seguros.
- Muestra ejemplos de infraestructuras críticas en salud, finanzas o industria para ilustrar el impacto operativo de una brecha en el perímetro.
- Explica la evolución de los firewalls: desde filtros de paquetes hasta soluciones NGFW con inspección profunda, control de aplicaciones, inteligencia de amenazas y segmentación.
- Subraya la importancia de mantener una configuración precisa, reglas actualizadas y auditorías frecuentes para reducir el riesgo de errores humanos o fallos ante cambios en la red.
- Aborda los sistemas IDS/IPS. Diferencia entre detección y prevención, así como entre enfoques basados en firmas o anomalías. Explica cómo se integran con soluciones SIEM para una correlación efectiva de eventos.
- Realiza una demostración con Snort y Nmap. Guía a los aprendedores en la simulación de un ataque, la configuración de reglas y el bloqueo de IP sospechosas.
- Cierra reforzando las mejores prácticas: segmentación, privilegios mínimos, actualización de firmas, filtrado web y DNS, autenticación multifactor, monitoreo continuo y respuesta planificada.
- Promueve una reflexión final sobre el papel de la inteligencia artificial, la automatización y la *deception technology* en la evolución de la seguridad perimetral.

Actividad 4

- Asegúrate de que los aprendedores apliquen OWASP ZAP para analizar vulnerabilidades críticas (como XSS o inyección SQL) en aplicaciones como DVWA, documentando vectores de ataque e impacto; de esta manera, se familiarizarán con los riesgos más comunes del desarrollo web.
- Indica que protejan API simuladas mediante mecanismos como JWT, OAuth 2.0 y validación de entradas. Esto reforzará su competencia para implementar API resilientes frente a ataques comunes.
- Pide que diseñen una red segmentada en Packet Tracer con VLAN diferenciadas y acceso remoto seguro por VPN, aplicando el principio de mínimo privilegio. Esto permitirá que visualicen cómo se construyen entornos defensivos robustos.
- Propón la configuración de un firewall pfSense y la integración de Snort para detectar ataques. Esto les brindará experiencia en seguridad perimetral y los preparará para detectar y mitigar accesos no autorizados.
- Para la organización del laboratorio, asegúrate de que los alumnos tengan acceso a:

  - Máquina virtual con DVWA (IP preconfigurada, por ejemplo, 192.168.1.100).
  - Credenciales predeterminadas de DVWA (*admin/password*).
  - Recomiéndales usar Kali Linux (preinstalado con OWASP ZAP, Nmap y Metasploit).

- En cuanto a la gestión del tiempo, considera asignar tiempos fijos por actividad:

  - 20 minutos para escaneo con ZAP.
  - 15 minutos para configuración de API.
  - 25 minutos para diseño de red y pfSense.

- Para solucionar problemas comunes, toma en cuenta lo siguiente:

  - Si OWASP ZAP no detecta DVWA, verifica que el proxy esté en localhost:8080 y añade DVWA a "Sitios incluidos".
  - Si pfSense no bloquea tráfico, revisa el orden de reglas (las más restrictivas primero).

- Para el ejemplo de autenticación JWT con Node.js, puedes tomar como base el siguiente código (con la libertad de realizar tus propias adaptaciones):

```
const express = require('express');
const jwt = require('jsonwebtoken');
const app = express();
const SECRET_KEY = 'clave_secreta';

app.post('/login', (req, res) => {
  const { user, pass } = req.body;
  if (user === 'admin' && pass === 'Password123!') {
    const token = jwt.sign({ user }, SECRET_KEY, { expiresIn: '1h' });
    res.json({ token });
  } else {
    res.status(401).send('Credenciales inválidas');
  }
});

app.get('/api/protected', (req, res) => {
  const token = req.headers.authorization?.split(' ')[1];
  if (!token) return res.sendStatus(401);
  jwt.verify(token, SECRET_KEY, (err, decoded) => {
    if (err) return res.sendStatus(403);
    res.json({ data: 'Información confidencial' });
  });
});

app.listen(3000, () => console.log('API en http://localhost:3000'));
```

- Rate Limiting con Express. Instalar express-rate-limit:

```
npm install express-rate-limit
```

- Añadir a la API:

```
const rateLimit = require('express-rate-limit');
const limiter = rateLimit({ windowMs: 60 * 1000, max: 100 });
app.use(limiter);
```

- Pruebas con Postman:

  - ¿Enviar solicitudes sin token? Debe retornar 401.
  - ¿Exceder 100 requests/minuto? Debe retornar 429.

- Para configurar pfSense y Snort para bloquear tráfico malicioso, puedes basarte en el siguiente ejemplo:

  - Regla en pfSense para bloquear tráfico no autorizado. Ir a Firewall > Rules > LAN:

    - Acción: Block.
    - Protocolo: TCP/UDP.
    - Origen: VLAN IoT.
    - Destino: VLAN Interna.
    - Puertos: Any.

  - Regla personalizada en Snort para detectar escaneos de puertos:

    - Editar /etc/snort/rules/local.rules:

```
alert tcp any any -> $HOME_NET any (msg:"Escaneo de Puertos SOSPECHOSO"; flags:S; detection_filter: track by_src, count 5, seconds 10; sid:1000001; rev:1;)
```

  - Reiniciar Snort:

```
sudo service snort restart
```

  - Simulación de ataque desde Kali Linux:

```
nmap -sS <IP_DVWA>
```

- Verificar alertas en Snort (/var/log/snort/alert).

Semana 6

Tema 18. Evaluación de riesgos

- Inicia con el caso de Lainer Tech. Muestra cómo incluso una empresa con buena reputación puede ser víctima de ciberataques si no realiza evaluaciones de riesgos periódicas y bien estructuradas.
- Explica los pasos esenciales de la gestión de riesgos: identificación de activos, análisis de amenazas y vulnerabilidades, evaluación del impacto y consolidación del riesgo. Usa ejemplos visuales para facilitar la priorización de recursos según la criticidad.
- Diferencia entre evaluación cualitativa y cuantitativa. Explica que la primera se basa en escalas descriptivas y juicio experto, mientras que la segunda utiliza datos para tomar decisiones fundamentadas.
- Destaca que ambos enfoques pueden complementarse para una gestión eficaz.
- Subraya la relevancia del cumplimiento normativo en este proceso. Incluye referencias a GDPR, NIS 2 u otras regulaciones; después, muestra cómo alinear políticas internas con estándares cambiantes fortalece la confianza del cliente y la reputación de la organización.
- Relaciona la evaluación de riesgos con cada fase del plan de respuesta a incidentes. Explica cómo la documentación clara y la colaboración entre áreas fortalecen la capacidad de recuperación.
- Organiza una actividad práctica de simulación con matriz de riesgos. Los aprendedores deberán clasificar activos, priorizar amenazas y tomar decisiones alineadas con niveles de riesgo y cumplimiento.
- Cierra con una reflexión sobre las lecciones aprendidas y la mejora continua de planes de respuesta.

Tema 19. Normativas y estándares de ciberseguridad

- Abre con ejemplos recientes de sanciones a empresas por incumplimiento de normativas como GDPR o la Ley de Ciberresiliencia de la UE. Usa estos casos para enfatizar la necesidad de mantenerse actualizado ante los marcos regulatorios globales.
- Explica la diferencia entre normativas, leyes y estándares. Señala que las primeras establecen requisitos legales, mientras que los segundos ofrecen marcos técnicos para la implementación y auditoría de medidas de seguridad.
- Cita ejemplos clave como ISO 27001:2022, NIST CSF 2.0 o el marco de IA de ENISA.
- Detalla el proceso y los beneficios de una auditoría de ciberseguridad. Muestra cómo estas revisiones permiten identificar vulnerabilidades, evaluar políticas y prevenir sanciones.

- Introduce conceptos como auditorías dinámicas, inteligencia artificial aplicada al monitoreo continuo y preparación para la resiliencia cuántica.
- Expón la relevancia de la gestión de licencias de software. Enseña los tipos de licencias más comunes y por qué el uso de software sin licencia incrementa los riesgos y posibles sanciones.
- Recomienda el uso de herramientas de gestión de licencias y promueve la formación ética en entornos digitales.
- Muestra los principales desafíos del cumplimiento en 2025: conflictos regulatorios entre jurisdicciones, vigilancia proactiva, cumplimiento cuántico e integración de IA.
- Propón una actividad práctica de auditoría normativa. Guía al grupo en la selección de una empresa real, la aplicación de un checklist GDPR/CCPA, la revisión de licencias y la elaboración de un plan de remediación priorizado.

Tema 20. Tendencias y futuro de la ciberseguridad

- Abre la sesión con el caso de Andrés, víctima de un ciberataque sorpresa, para destacar que incluso organizaciones avanzadas pueden ser vulneradas. Recalca que hoy se valora más la resiliencia y la capacidad de adaptación que la simple prevención.
- Explica la evolución de las amenazas: desde virus primitivos hasta ransomware de triple extorsión, ataques a la cadena de suministro, malware con IA o *deepfakes* biométricos. Usa una línea cronológica para visualizar los riesgos emergentes.
- Detalla las tecnologías defensivas más actuales. Incluye firewalls con IA, SIEM avanzados, segmentación dinámica, criptografía poscuántica, blockchain para integridad de datos y automatización de respuestas.
- Aborda los desafíos que plantean la IA ofensiva, las vulnerabilidades en IoT, el ransomware cuántico o los ataques a infraestructuras críticas.
- Relaciona estos riesgos con la necesidad de colaboración intersectorial, formación constante y cumplimiento normativo proactivo.
- Muestra las oportunidades laborales emergentes en el área: especialistas en IA aplicada a seguridad, arquitectos de resiliencia cuántica, analistas de amenazas en IoT o gestores de respuesta ante ransomware.
- Menciona certificaciones como CAISP, QSSE, CRRM o IoTSP y fomenta el desarrollo profesional continuo.
- Organiza una actividad de simulación ante un ataque de ransomware con dilema ético. Los aprendedores deberán diseñar un plan de recuperación, justificar decisiones y proponer medidas preventivas.
- Cierra con una reflexión sobre el rol individual en la construcción de un entorno digital resiliente. Invita a los aprendedores a identificar cómo pueden contribuir desde su función profesional a fortalecer la seguridad colectiva.

Actividad 5

- Asegúrate de que los aprendedores completen el curso "*Introduction to Cybersecurity*" de Cisco Networking Academy, lo cual les permitirá consolidar sus conocimientos básicos en ciberseguridad de manera estructurada y con aval externo.

- Indica que deben evidenciar su progreso mediante capturas del examen final aprobado y de la insignia digital. Esto fomentará su responsabilidad en el aprendizaje autónomo y fortalecerá su portafolio profesional.
- Refuerza la importancia de adquirir certificaciones reconocidas en la industria para demostrar dominio técnico ante empleadores y comunidades especializadas en ciberseguridad.

Semana 7

Entrega del reto

- Cerciórate de que los aprendedores implementen soluciones técnicas avanzadas que incluyan IaC con Terraform, pruebas de API con Burp Suite y simulación de ataques APT29 con Metasploit. Esto demostrará su dominio completo del ciclo de seguridad ofensiva y defensiva.
- Pide que diseñen un plan de respuesta a incidentes que contemple aislamiento, recuperación y revocación de accesos comprometidos; así, reforzarán su competencia en gestión de crisis tecnológicas.
- Sugiere que auditen políticas de seguridad en Azure usando marcos como NIST SP 800-53 e ISO 27001. Esta integración de cumplimiento normativo los prepara para entornos corporativos exigentes.
- Asegúrate de que presenten los resultados mediante una presentación ejecutiva y reporte técnico profesional, con métricas de impacto y retorno de inversión. Esto los prepara para comunicar eficazmente su propuesta a distintos públicos.

Semana 8

Presentación del reto (versión bimestral)

- Explica que esta presentación representa el cierre de un ciclo formativo integral donde el aprendedor demuestra competencias técnicas en ciberseguridad y habilidades de comunicación ejecutiva. La audiencia esperada (autoridades académicas, representantes de instituciones tecnológicas y de salud) exige claridad, rigor técnico y visión estratégica.
- Subraya que el enfoque de la presentación es profesionalizante, es decir, más que describir lo que se hizo, se busca comunicar valor: ¿cuál fue el problema?, ¿cómo se resolvió?, ¿qué evidencia técnica sustenta la solución?, ¿qué impacto tuvo?
- Orienta la organización de la presentación en cuatro bloques clave:
    - Diagnóstico: explicar el escenario del ataque (ransomware), los sistemas afectados y las brechas detectadas.
    - Simulaciones y defensa: mostrar las pruebas realizadas (APT29, phishing, escaneo), el diseño del entorno de pruebas y las herramientas utilizadas.

- Implementación y resultados: explicar cómo se aplicaron medidas como hardening, BitLocker, VLANs y mostrar métricas de mejora.
- Cierre estratégico: reflexión sobre aprendizajes, retos, cumplimiento normativo, y propuestas futuras.

- Sugerencia técnica: pide que cada diapositiva tenga un enfoque visual claro (una idea por slide), que combinen textos breves con gráficos, capturas de herramientas (Nmap, Wireshark, GoPhish, Metasploit, etc.), y que el uso del color respete una plantilla sobria y profesional.
- Prepara a los estudiantes para responder preguntas técnicas que podrían surgir durante la exposición:

  - ¿Por qué seleccionaron APT29 como modelo de ataque?
  - ¿Qué implicaciones tiene el uso de BitLocker en entornos clínicos?
  - ¿Qué normativas se incumplían antes del ataque?
  - ¿Cómo midieron la mejora en ciberresiliencia?

Examen final (versión bimestral)

Recomienda a los aprendedores que hagan notas para repasar o realizar alguna actividad, como en Kahoot, Menti, etc., de tal manera que evalúen su nivel de comprensión de los temas.

Rúbricas

Cada actividad y proyecto se evalúa mediante rúbricas específicas. Puedes consultarlas en la sección "Actividades y Proyectos", dentro del apartado "Criterios de Evaluación" del certificado programado en CANVAS. Estas rúbricas aseguran una retroalimentación clara y consistente, permitiendo a los aprendedores comprender con precisión las expectativas y los aspectos que deben mejorar. Además, al objetivar la calificación, el uso de rúbricas promueve un proceso de evaluación más justo y transparente, sirviendo como una herramienta valiosa tanto para el aprendizaje del aprendedor como para la labor docente.

Prácticas de bienestar

Práctica 1

<table>
<tr><td>Nombre de la práctica</td><td>Identificar patrones de comunicación</td></tr>
<tr><td>Descripción de la práctica</td><td>Identificarás patrones en la manera en que te comunicas con tus familiares, compañeros o colegas. Trazarás una estrategia para mejorarlo.</td></tr>
<tr><td>Palabras clave</td><td>Emociones positivas, resiliencia, perspectiva.</td></tr>
<tr><td>Instrucciones para el participante</td><td>Martin Seligman señala que existen cuatro formas de abordar la comunicación con otra persona:

<table>
<tr><td>1. Activa destructiva

Señalar aspectos negativos de un evento o una conversación.</td><td>4. Activa constructiva

Apoyo auténtico y con entusiasmo.</td></tr>
<tr><td>2. Pasiva destructiva

Ignorar el evento o la conversación.</td><td>3. Pasiva constructiva

Apoyo breve, sin seguimiento o por compromiso.</td></tr>
</table>

Seligman señala que es sumamente importante cultivar la retroalimentación activa constructiva, ya que esta ayuda a que tu interlocutor experimente emociones positivas y se concentre en sus fortalezas, no en sus debilidades. Ahora reflexiona por un momento, ¿cuáles son los tipos de respuestas que más escuchas diariamente?

1. Durante dos días, haz el ejercicio de observación y señala en qué clasificación caen las conversaciones que has tenido.
2. Posteriormente, piensa en cómo te han hecho sentir cada tipo de participación.
3. Aplica lo que aprendiste luego de este análisis a las siguientes conversaciones que entables. Posteriormente, vuelve a reflexionar sobre cómo te has sentido.
4. Lo ideal es buscar siempre estar en el cuadrante de la retroalimentación activa constructiva. Si descubres que usualmente las conversaciones se inclinan hacia otro cuadrante, trata de establecer por qué.
5. Establece una estrategia que te ayude a mejorar tu comunicación.</td></tr>
<tr><td>Fuente</td><td>Fuente: Seligman, M. (2011). Building Resilience. Recuperado de https://hbr.org/2011/04/building-resilience</td></tr>
</table>

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, inhala 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 3

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 4

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 5

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 6

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 7

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 8

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	¿Cuáles son tus fortalezas de carácter?
Descripción de la práctica	A través de esta actividad descubrirás cuáles son tus principales fortalezas de carácter.
Palabras clave	Fortalezas de carácter, test VIA.
Instrucciones para el participante	1. Ingresa **http://www.viacharacter.org/Survey/Account/Register** y regístrate con los datos que solicita la página para que puedas tener acceso al test VIA. Una vez que obtuviste el registro, procede a realizar el test (las instrucciones están en inglés, pero el test está en español). Al momento en que se desplieguen tus resultados, obsérvalos bien, analízalos, y posteriormente redacta un reporte en el cual desarrolles los siguientes puntos: a. Análisis de los resultados obtenidos, en términos de qué tanto coinciden con tu personalidad. Describe cuáles de esas fortalezas coinciden con tu personalidad, y analiza cuáles son tus áreas de oportunidad (las 5 fortalezas al final de la lista) sobre las que debes de continuar trabajando. b. Explica qué medidas prácticas (plan de acción) podrías considerar tomar para continuar desarrollando dichas fortalezas, y trabajar en la mejora de tus áreas de oportunidad. c. Incluye una conclusión donde redondees el análisis de los resultados y los expliques en términos de los contenidos del curso vistos en este tema.
Fuente	Curso: El líder desde adentro.

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 (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