Seguridad en TI

Guía para el profesor

Clave MTTI2409

Nivel Maestría

UNIVERSIDAD TECMILENIO

Contenido

Datos generales del certificado

Nombre del certificado: Seguridad en TI

Modalidad: Connect

Clave: MTTI2409

Competencia global del curso

Analiza y gestiona riesgos de seguridad en TI, aplicando estrategias, normativas y herramientas para la protección de activos digitales, la prevención de amenazas y la respuesta a incidentes, a través del desarrollo e implementación de planes de seguridad y respuesta ante incidentes en un entorno real o simulado, asegurando la continuidad del negocio y la resiliencia organizacional.

Introducción al curso

La Seguridad en TI resulta imprescindible para proteger la información y la continuidad operativa de cualquier organización moderna. Este certificado te guía, de forma progresiva y práctica, por los fundamentos que dan forma a una estrategia defensiva integral: desde los principios de confidencialidad, integridad y disponibilidad hasta la valoración de amenazas, vulnerabilidades y riesgos que ponen en alerta a los entornos corporativos contemporáneos.

A lo largo de las cuatro semanas explorarás la protección física de infraestructuras críticas, los controles de acceso, las técnicas de cifrado y los mecanismos de filtrado y monitoreo del tráfico. También aprenderás a asegurar redes locales y distribuidas, diseñar arquitecturas robustas en la nube bajo el modelo de responsabilidad compartida y aplicar buenas prácticas de desarrollo seguro basadas en los marcos de trabajo populares como OWASP y DevSecOps. El último paso te guiará por el proceso de elaboración de planes de respuesta y recuperación ante incidentes, así como con la discusión de tendencias emergentes que están transformando el panorama de la ciberseguridad.

Al finalizar esta experiencia de aprendizaje, contarás con la capacidad de identificar y mitigar amenazas en múltiples infraestructuras, diseñar controles alineados a estándares internacionales y liderar procesos de respuesta ante incidentes. Estas competencias te preparan para desempeñarte eficazmente como analista de un centro de operaciones, arquitecto de seguridad o responsable de DevSecOps, abriendo paso a certificaciones de nivel intermedio y a roles estratégicos en un mercado cada vez más competitivo.

Información general

Metodología

Este curso ha sido diseñado con la finalidad de ser impartido por un **docente líder con experiencia en el ámbito laboral,** quien compartirá contigo su conocimiento, experiencia y las mejores prácticas que realiza en su labor profesional.

La experiencia de curso promueve la interacción entre aprendedores de la Universidad Tecmilenio como una forma de enriquecer tu formación contrastando la realidad con la de otros compañeros.

Durante cada sesión, el docente transmite su experiencia y actúa como guía en el proceso de aprendizaje durante la realización de las actividades.

El curso es tetramestral y tiene una distribución semanal; en cada semana, se lleva a cabo una sesión. La asistencia a estas sesiones es muy importante para el aprendizaje.

Este curso se conforma por 8 temas y su estructura es la siguiente:

Semana	Módulo	Tema	Evaluable
1	**Módulo 1**	Tema 1	
		Tema 2	Actividad 1
2		Tema 3	
		Tema 4	Actividad 2
3	**Módulo 1**	Tema 5	
		Tema 6	Evidencia 1
4		Tema 7	
		Tema 8	Evidencia final

Bibliografía

Bibliografía opcional

- Graham, D. (2021). *Ethical Hacking: A Hands-on Introduction to Breaking In.* Estados Unidos: No starch press.
- Jason Andress. (2019). *Foundations of Information Security: A Straightforward Introduction.* Estados Unidos: No starch press

Evaluación

A continuación, puedes revisar el detalle de la evaluación:

Semana	Evaluable	Ponderación
1	Actividad 1	15
2	Actividad 2	15
3	Evidencia 1	30
4	Evidencia final	40
	Total	**100**

Estructura de las sesiones

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

Bloque 1	Bloque 2
Bienvenida y presentación de agenda.	Recapitulación de lo realizado en el bloque previo.
Actividad de bienestar.	Desarrollo de temas de la semana. • Explicación de los temas de la semana con ejercicios prácticos. • Cierre de temas.
Desarrollo de temas de la semana. • Aplicación en contextos reales (introducción). • Explicación de los temas de la semana con ejercicios prácticos.	Explicación de las actividades que deberán realizarse en la semana (fuera de la sesión).
Receso.	

Actividades y evidencias

Las actividades y evidencias han sido diseñados para realizarse de manera individual. Por ende, para promover el dinamismo y la interacción de los participantes en distintos formatos, el profesor alternará (durante las sesiones) intervenciones individuales, plenarias y grupales que enriquezcan los puntos de vista del aprendedor.

Todas las actividades y evidencias deberán entregarse por medio de la plataforma tecnológica, para que el profesor pueda hacer la respectiva revisión y evaluación. Es crucial que el aprendedor revise el esquema de evaluación y los criterios que se utilizarán, con el fin de que tenga claro el nivel de complejidad y esfuerzo requerido para realizar las entregas semanales, con lo cual garantizará el éxito en el curso.

En caso de que el aprendedor tenga dudas sobre alguna actividad o contenido del programa, podrá contactar al profesor a través de los medios indicados.

Sesiones virtuales

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

Tutoriales

Para asegurar que el aprendedor aproveche al máximo su experiencia educativa, se le recomienda que siga las indicaciones del docente, así como la revisión de los siguientes tutoriales:

- **¿Cómo ingreso a la plataforma de multipresencia virtual?**
- **Tutoriales de Canvas para participantes.**
- **¿Cómo evalúo el desempeño de mi red?**

Calendario de entregas de los aprendedores

Semanas	Módulos	Temas	Actividades	Proyecto
1	Módulo 1	Tema 1		
		Tema 2	Actividad 1	
2		Tema 3		
		Tema 4	Actividad 2	
3	Módulo 2	Tema 5		
		Tema 6		Evidencia 1
4		Tema 7		
		Tema 8		Evidencia final

Temario del curso

Semana 1
1. Introducción a la seguridad en TI
2. Seguridad física y lógica

Semana 2
3. Gestión de vulnerabilidades y amenazas
4. Seguridad en redes y comunicaciones

Semana 3
5. Seguridad en la nube y en sistemas distribuidos
6. Seguridad en el desarrollo de aplicaciones

Semana 4
7. Gestión de incidentes y recuperación
8. Tendencias emergentes y el futuro de la ciberseguridad

Preguntas más frecuentes

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

Cualquier incidencia se puede reportar directamente haciendo clic en el botón “Mejora tu curso” que se encuentra en la parte superior derecha de la pantalla en la plataforma de Canvas.

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

El coordinador docente te debe proporcionar esta información.

¿En qué semana se aplica 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 calificaciones en la plataforma para que los aprendedores estén informados de su avance y reciban retroalimentación de tu parte sobre todo lo que realizan en el certificado. El banner es el registro oficial de las calificaciones de los aprendedores.

Guía general para las sesiones

Bloque 1

Actividad	Descripción
Bienvenida y presentación de agenda.	El profesor se presenta ante el grupo y da una breve introducción al certificado.
Práctica de bienestar.	El profesor impartidor seleccionará alguna práctica de bienestar para aplicarla en la sesión. Se recomienda utilizar una diferente por sesión.
Desarrollo de los temas de la semana: ○ **Aplicación en contextos reales (introducción).** ○ **Explicación de los temas de la semana con ejercicios prácticos.**	El profesor explicará los contenidos con ejercicios prácticos.
Receso.	Se brindará un espacio de receso para que el aprendedor lo utilice en su beneficio.

Bloque 2

Actividad	Descripción
Recapitulación del bloque previo.	De manera dinámica, el profesor recapitulará lo realizado en el bloque previo.
Desarrollo de los temas de la semana: ○ **Explicación de los temas de la semana con ejercicios prácticos.** ○ **Cierre de temas.**	El profesor explicará los contenidos con ejercicios prácticos y realizará un cierre de los temas correspondientes.
Explicación sobre lo que deberá realizarse fuera de la sesión: • **Actividades, evidencias, exámenes, etc.**	Se brindará una breve explicación de las tareas correspondientes a la semana, las cuales se deberán realizar de forma individual.

Semana 1

Notas para el profesor impartidor correspondientes a la explicación del tema 1 (favor de considerar la realización de ejercicios prácticos durante la sesión).

- Asegúrate de que los aprendedores comprendan la diferencia entre seguridad de la información, seguridad informática y ciberseguridad. Organiza una actividad de clasificación en equipos, donde analicen situaciones reales y determinen qué tipo de seguridad se ve comprometida, promoviendo así un entendimiento contextualizado y aplicado de cada concepto.
- Invita a los aprendedores a diseñar un esquema visual que represente las capas de seguridad (física, lógica y organizacional), incorporando ejemplos de controles asociados a cada una. Esta actividad fomenta la integración conceptual y el reconocimiento de cómo las capas se articulan para ofrecer una protección integral.
- Promueve el análisis crítico de los tipos de controles de seguridad (preventivos, proactivos, de detección y de respuesta) y su relación con los escenarios de riesgo.
- Propicia una actividad de simulación donde los estudiantes identifiquen activos, amenazas, vulnerabilidades y riesgos en un caso práctico, utilizando plantillas para el análisis. Esto refuerza la comprensión del modelo de análisis de riesgo alineado con ISO/IEC 27005.
- Asegúrate de que los aprendedores analicen el paradigma de Confianza Cero y los principios de diseño seguro (mínimos privilegios, defensa en profundidad, etc.). Propón un debate sobre cómo estos principios impactan el diseño de sistemas actuales en comparación con enfoques tradicionales, fortaleciendo su capacidad para tomar decisiones técnicas informadas.

Notas para el profesor impartidor correspondientes a la explicación del tema 2 (favor de considerar la realización de ejercicios prácticos durante la sesión).

- Asegúrate de que los aprendedores comprendan la importancia de la seguridad física en la protección de la información. Realiza una dinámica en la que diseñen un plan básico de protección para un centro de datos ficticio, considerando acceso físico, videovigilancia, control ambiental y destrucción de activos.
- Propón una actividad donde los estudiantes ejemplifiquen la implementación del modelo AAA (autenticación, autorización y auditoría) en distintos contextos organizacionales. Esto puede realizarse mediante diagramas de flujo que muestren cómo se aplica este modelo en sistemas de recursos humanos, financieros o educativos.
- Fomenta el análisis comparativo entre cifrado simétrico y asimétrico, su uso en protocolos como HTTPS, VPN y almacenamiento. Para ello, pide a los aprendedores que construyan una tabla de selección de cifrado con base en escenarios concretos (comercio electrónico, bases de datos, backups).
- Asegúrate de que los aprendedores comprendan la función de firewalls, IDS/IPS y monitoreo de tráfico.
- Solicita a los estudiantes un trabajo colaborativo donde evalúen la arquitectura de seguridad de una organización real o simulada, proponiendo mejoras basadas en normas ISO/IEC 27001 y 27002. Esto les permitirá vincular teoría con práctica y desarrollar pensamiento estratégico en ciberseguridad.

Notas para el profesor impartidor correspondientes a la actividad 1.

- La calificación de esta actividad se asignará en función del porcentaje de avance y desempeño que obtengas en el curso **Getting Started with Cybersecurity**. A continuación, se detalla la relación entre el porcentaje alcanzado en el curso y la calificación asignada.

Porcentaje de calificación del curso IBM Cloud Essentials	Calificación
0%	0
1% a 20%	50
21% a 50%	70
51% a 69%	80
70% a 100%	100

Semana 2

Notas para el profesor impartidor correspondientes a la explicación del tema 3 (favor de considerar la realización de ejercicios prácticos durante la sesión).

- Asegúrate de que los aprendedores comprendan la diferencia entre políticas, normas, procedimientos y estándares en seguridad. Puedes organizar una actividad en la que analicen ejemplos reales de documentos organizacionales y los clasifiquen, fortaleciendo así su comprensión estructural y jerárquica.
- Promueve una discusión en equipos sobre la importancia de las políticas de seguridad y su impacto en la cultura organizacional. Pide a los aprendedores que redacten un fragmento de política enfocada en control de accesos o uso de dispositivos personales, enfatizando la claridad, el enfoque preventivo y la viabilidad de cumplimiento.
- Invita a los aprendedores a comparar las principales normativas internacionales, como ISO/IEC 27001, NIST, GDPR y LFPDPPP, identificando similitudes, diferencias y casos de aplicación. Esta actividad puede estructurarse como una matriz comparativa y análisis de un caso empresarial donde apliquen dichas normativas.
- Fomenta la reflexión sobre las consecuencias legales y reputacionales del incumplimiento de normativas de seguridad, proponiendo un estudio de caso sobre una empresa sancionada.

Notas para el profesor impartidor correspondientes a la explicación del tema 4 (favor de considerar la realización de ejercicios prácticos durante la sesión).

- Asegúrate de que los aprendedores comprendan los principios de la tríada CIA (confidencialidad, integridad, disponibilidad) y su aplicación en la arquitectura de redes.
- Propón una actividad de análisis en la que los aprendedores identifiquen los controles técnicos (firewalls, IDS/IPS, cifrado) aplicables a cada capa del modelo OSI y TCP/IP. Esto puede apoyarse con diagramas que ilustren la protección por capas y su rol en la defensa en profundidad.

- Promueve un estudio comparativo entre los modelos Confianza Cero, SASE, SSE y redes definidas por software (SDN). Pide a los estudiantes que justifiquen qué modelo sería más adecuado para un escenario específico (empresa con trabajo remoto, banco digital, etc.).
- Invita a los aprendedores a analizar ataques comunes como DoS, sniffing o exfiltración, y vincularlos con las estrategias de mitigación. Esto puede estructurarse como una tabla de amenazas vs. controles y promoverá una visión táctica de la protección en redes.
- Proporciona una práctica guiada donde configuren una VPN de acceso remoto (usando simuladores como Packet Tracer o GNS3) y diseñen una arquitectura de segmentación lógica con políticas de microsegmentación. Esta actividad permite integrar conceptos y habilidades técnicas en un contexto práctico.

Notas para el profesor impartidor correspondientes a la actividad 2.

- Asegúrate de que los aprendedores seleccionen un ciberataque ampliamente documentado y de alto impacto (ej. SolarWinds, WannaCry, Colonial Pipeline), cuya reconstrucción permita analizar tanto la seguridad física como lógica. Recomiéndales verificar la disponibilidad de fuentes técnicas actualizadas y confiables para sustentar su investigación.
- Indica que la cronología del ataque debe incluir los eventos clave desde la intrusión inicial hasta la recuperación, integrando actores, objetivos, técnicas y afectaciones. Esto permitirá contextualizar adecuadamente el incidente y facilita el análisis forense de sus etapas.
- Solicita que identifiquen fallas específicas: debilidades en accesos físicos, configuraciones inseguras, software obsoleto, ausencia de segmentación o errores humanos. Pide que clasifiquen estas fallas como físicas, lógicas o humanas, y expliquen cómo se interrelacionaron para facilitar el ataque.
- Asegúrate de que el informe aplique de manera correcta un marco de análisis como la cadena de ataque Cyber Kill Chain o MITRE ATT&CK. Esto permitirá estructurar la narrativa del ataque y comprender la progresión de la amenaza desde el reconocimiento hasta la exfiltración.
- Promueve que las estrategias propuestas se vinculen con los aprendizajes de las semanas 1 y 2, incluyendo medidas de seguridad física, controles técnicos (firewalls, IDS, VPNs, segmentación), y prácticas organizacionales.
- Insiste en que las recomendaciones sean contextualizadas, viables y aplicables a organizaciones similares a la afectada, con base en su tamaño, sector y recursos disponibles. Esto fomenta un análisis estratégico y realista.
- Verifica que el entregable tenga una estructura clara, use lenguaje técnico apropiado, incorpore referencias con formato APA Tecmilenio y cumpla con la extensión requerida (6 a 8 cuartillas). Sugiere la revisión cruzada entre pares antes de la entrega final.

Semana 3

Notas para el profesor impartidor correspondientes a la explicación del tema 5 (favor de considerar la realización de ejercicios prácticos durante la sesión).

- Asegúrate de que los aprendedores comprendan las fases del ciclo de gestión de incidentes: preparación, detección, análisis, contención, erradicación, recuperación y lecciones aprendidas. Puedes proponer un mapa mental colaborativo en el que identifiquen tareas, herramientas y roles asociados a cada etapa.
- Promueve el análisis de casos reales de respuesta a incidentes (como ataques de ransomware en hospitales o filtraciones de datos en instituciones financieras) para ejemplificar la aplicación de las fases y facilitar la comprensión del proceso completo.

- Solicita a los aprendedores que diseñen un plan básico de respuesta a incidentes para una empresa ficticia, incluyendo roles, canales de comunicación, protocolos de contención y actividades de recuperación. Esta actividad favorece la conexión entre teoría y aplicación práctica.
- Invita a reflexionar sobre la importancia de registrar, documentar y evaluar cada incidente para fortalecer la resiliencia organizacional. Puedes usar como base el marco NIST SP 800-61r2, disponible en español.

Notas para el profesor impartidor correspondientes a la explicación del tema 6 (favor de considerar la realización de ejercicios prácticos durante la sesión).

- Asegúrate de que los aprendedores comprendan que la seguridad debe integrarse desde la etapa de diseño. Propón una dinámica donde identifiquen amenazas en una arquitectura básica y apliquen los principios del desarrollo seguro (mínimos privilegios, defensa en profundidad, etc.).
- Promueve la exploración del OWASP Top 10 como herramienta de análisis y prevención. Puedes dividir al grupo en equipos y asignar a cada uno un riesgo del listado para investigar y presentar con ejemplos, controles de mitigación y casos reales.
- Fomenta el uso del ciclo SSDLC y sus prácticas asociadas (requisitos seguros, codificación segura, pruebas automatizadas y manuales). Puedes pedirles que documenten cómo integrarían estas fases en un proyecto ágil real.
- Propicia el análisis comparativo de herramientas de análisis estático (SAST), dinámico (DAST), de composición (SCA) e interactivo (IAST), y su integración en pipelines DevSecOps.
- Asegúrate de que los aprendedores analicen un caso forense de falla de seguridad (como Equifax o SolarWinds), reconstruyendo sus fases e identificando fallos evitables desde el desarrollo. Esto les permitirá extraer aprendizajes y fortalecer su pensamiento crítico frente al diseño de aplicaciones.

Notas para el profesor impartidor correspondientes a la evidencia 1.

- Asegúrate de que los aprendedores seleccionen un caso empresarial viable (real o ficticio) que cumpla con los requisitos mínimos: red local, servidor, aplicación crítica y personal con distintos niveles de acceso. Puedes guiarlos en la construcción del caso ficticio si no conocen una empresa adecuada.
- Indica que deben elaborar un inventario técnico detallado, organizando los activos por tipo (hardware, software, datos, personas) e indicando su criticidad. Propón el uso de una plantilla estructurada que les facilite visualizar los componentes clave y su relación con los procesos organizacionales.
- Promueve la identificación de amenazas clasificadas por origen (externo/interno), tipo (física/lógica) e impacto. Pide que ejemplifiquen al menos cinco vulnerabilidades, incluyendo debilidades técnicas (puertos abiertos, contraseñas inseguras) y humanas (ingeniería social, desconocimiento de protocolos).
- Asegúrate de que los aprendedores diseñen una estrategia integral que contemple controles físicos (acceso restringido, videovigilancia), controles lógicos (firewalls, cifrado, políticas de actualizaciones) y medidas de segmentación y monitoreo.
- Solicita que el informe incluya esquemas o diagramas que expliquen visualmente la arquitectura de la red y las zonas protegidas. Puedes sugerir herramientas como draw.io, Lucidchart o diagramas hechos a mano digitalizados, siempre que sean claros y pertinentes.

- Comenta la importancia de usar un lenguaje técnico claro, citar fuentes confiables, estructurar el informe en secciones (diagnóstico, vulnerabilidades, propuesta) y revisar ortografía y formato antes de entregarlo en PDF.

Semana 4

Notas para el profesor impartidor correspondientes a la explicación del tema 7 (favor de considerar la realización de ejercicios prácticos durante la sesión).

- Asegúrate de que los aprendedores comprendan los modelos de servicio en la nube (IaaS, PaaS, SaaS) y sus implicaciones en la responsabilidad compartida. Propón una dinámica donde analicen los riesgos y controles necesarios para cada modelo, vinculándolo con proveedores reales (AWS, Azure, GCP).
- Invita a identificar amenazas específicas en entornos virtualizados y en la nube, como “VM escape”, configuración errónea de buckets o acceso no autorizado a API. Pide que describan estas amenazas con ejemplos reales o simulados para comprender su funcionamiento y consecuencias.
- Promueve el análisis de buenas prácticas de configuración segura en servicios en la nube.
- Fomenta el uso de herramientas de escaneo automatizado y monitoreo continuo como CSPM, CWPP o SIEM. Puedes pedir que investiguen herramientas como Prisma Cloud o Microsoft Defender for Cloud y expongan su funcionamiento básico.
- Asegúrate de que los aprendedores entiendan el principio de mínima exposición en la configuración de redes, roles y almacenamiento. Una práctica sugerida es que diseñen políticas de control de acceso granular (IAM) para un escenario simulado.
- Sugiere analizar el impacto de la soberanía de los datos y las regulaciones locales sobre el despliegue de servicios en la nube. Esto puede estructurarse en un debate sobre cómo GDPR o LFPDPPP condicionan la arquitectura y gobernanza de datos.

Notas para el profesor impartidor correspondiente a la explicación del tema 8 (favor de considerar la realización de ejercicios prácticos durante la sesión).

- Asegúrate de que los aprendedores identifiquen cómo la inteligencia artificial está redefiniendo los mecanismos defensivos y ofensivos en ciberseguridad.
- Promueve la comprensión de los desafíos de seguridad en IoT y dispositivos móviles. Proponles que construyan una matriz de vulnerabilidades vs. controles, usando como base los estándares NIST SP 800-213, ETSI EN 303 645 y MDM.
- Solicita que analicen el impacto de la computación cuántica sobre la criptografía actual. Puedes pedir que expliquen en equipos la diferencia entre criptografía post-cuántica (PQC) y distribución cuántica de claves (QKD), usando ejemplos de algoritmos como Kyber y Dilithium.
- Invita a reflexionar sobre los dilemas éticos y regulatorios que surgen con la automatización y vigilancia digital. Puedes guiar un debate con base en principios como la privacidad diferencial, la responsabilidad algorítmica y la gobernanza global del ciberespacio.
- Promueve una perspectiva crítica y anticipatoria: pide a los aprendedores que redacten una breve política de seguridad para un entorno de 2030, integrando IA, IoT, criptografía avanzada y principios éticos.

Notas para el profesor impartidor correspondientes a la evidencia final.

- Asegúrate de que los aprendedores comprendan que esta fase simula la gestión de una amenaza reciente y deben elegirla con base en fuentes confiables como OpenSSF, SANS ISC o Securelist. Oriéntalos para que seleccionen amenazas con documentación técnica clara, como malware dirigido a VPNs, explotación de APIs o paquetes maliciosos en repositorios.
- Indica que el análisis debe incluir origen, vectores, objetivos y métodos técnicos de la amenaza, así como una evaluación precisa de la exposición de la organización definida en la Fase I. Esto implica revisar puntos como puertos vulnerables, falta de autenticación o configuraciones débiles que permitan el ingreso de la amenaza.
- Promueve el uso de los controles propuestos en la Fase I para explicar cómo se habría detectado o mitigado el ataque. Pide que justifiquen dos controles adicionales (como SIEM, honeypots o soluciones EDR) en función de las características de la amenaza seleccionada.
- Asegúrate de que la simulación del proceso de respuesta cubra las etapas de detección, contención y recuperación, y que se ilustre cómo interactuarían los diferentes actores internos y externos. Sugiere apoyarse en guías como las de NIST SP 800-61r2 o ejemplos de respuesta de CERTs nacionales.
- Indica que la sección de “lecciones aprendidas” debe incluir reflexiones basadas en el desempeño simulado y proponer al menos dos mejoras puntuales a la estrategia diseñada en la Fase I. Esto promueve el pensamiento crítico y la mejora continua en entornos reales de ciberseguridad.
- Comenta la importancia de integrar el reporte completo en un solo documento PDF, con redacción técnica clara, diagramas explicativos si es necesario, referencias en formato APA y coherencia entre ambas fases.
- Puedes sugerir la revisión cruzada del informe entre compañeros antes de la entrega, para detectar áreas de mejora y asegurar la claridad en la exposición del análisis.

Rubricas de evaluación

Actividad 1

Seguridad en TI

Rúbrica de Evaluación.

Calificación basada en el curso Getting Started with Cybersecurity.

La calificación de esta actividad se asignará en función del porcentaje de avance y desempeño que obtengas en el curso **Getting Started with Cybersecurity**. A continuación, se detalla la relación entre el porcentaje alcanzado en el curso y la calificación asignada:

Porcentaje de calificación del curso IBM Cloud Essentials	Calificación
0%	0
1% a 20%	50
21% a 50%	70
51% a 69%	80
70% a 100%	100

Seguridad en TI

Rúbrica de evaluación para Actividad 2

Nivel de desempeño				
Criterios de evaluación	**Altamente competente (100%–86%)**	**Competente (85%–70%)**	**Aún sin desarrollar la competencia (69%–0%)**	%
1. Profundidad del análisis del ataque	25 – 23 puntos	22 – 19 puntos	18 – 0 puntos	25
	Incluye los cuatro elementos solicitados (cronología, actores, objetivos y métodos del ataque), con explicaciones técnicas fundamentadas en al menos tres fuentes confiables, y relaciones causales claras entre elementos.	Incluye al menos tres de los cuatro elementos solicitados, con explicaciones generales y con apoyo limitado en fuentes o con vínculos causales poco desarrollados.	Incluye dos o menos elementos, o presenta información incompleta, con errores de interpretación, sin respaldo en fuentes verificables o sin análisis técnico.	
	25 – 23 puntos	22 – 19 puntos	18 – 0 puntos	25

2. Identificación y análisis de vulnerabilidades (ciclo de vida de la amenaza)	Identifica y describe tres o más vulnerabilidades (físicas, lógicas o humanas), explicando su función dentro del ciclo de vida de la amenaza con base en Cyber Kill Chain o MITRE ATT&CK. Relaciona cada vulnerabilidad con una etapa concreta del ataque.	Identifica dos vulnerabilidades, describe su función de forma general y establece una relación parcial con el ciclo de vida de la amenaza.	Identifica una vulnerabilidad o ninguna, o no vincula correctamente las vulnerabilidades con el ciclo de vida del ataque.	
3. Propuestas de prevención realistas y argumentadas	25 – 23 puntos Presenta tres o más estrategias de seguridad física y lógica que pueden implementarse en entornos reales, argumentadas con base en las vulnerabilidades detectadas, tecnologías disponibles y prácticas de ciberseguridad.	22 – 19 puntos Presenta dos estrategias con explicación general. Las propuestas están relacionadas con el ataque, pero no están suficientemente justificadas o carecen de viabilidad técnica clara.	18 – 0 puntos Presenta una estrategia o ninguna, o las propuestas no se relacionan con las vulnerabilidades identificadas ni están justificadas con base técnica.	25
4. Claridad, estructura y formato del informe	25 – 23 puntos El informe incluye los cinco apartados solicitados: descripción del ataque, análisis de vulnerabilidades, ciclo de vida, estrategias y lecciones aprendidas. Tiene una extensión de 6 a 8 cuartillas y aplica correctamente el formato APA Tecmilenio, con un máximo de 2 errores menores.	22 – 19 puntos El informe incluye al menos cuatro de los cinco apartados, cumple parcialmente con la extensión (5 o 9 cuartillas) o presenta entre 3 y 5 errores en el formato APA.	18 – 0 puntos El informe presenta tres apartados o menos, tiene problemas estructurales, no cumple con la extensión mínima (menos de 5 cuartillas), o contiene más de 5 errores en el formato APA.	25
			TOTAL	100

Seguridad en TI

Rúbrica de evaluación para Evidencia 1

Nivel de desempeño				
Criterios de evaluación	**Altamente competente (100%–86%)**	**Competente (85%–70%)**	**Aún sin desarrollar la competencia (69%–0%)**	%
1. Identificación de activos críticos y su relación con la operación	20 – 18 puntos Elabora un inventario con al menos 5 activos críticos, cada uno con descripción técnica y explicación de su función en los procesos clave de la organización.	17 – 15 puntos Elabora un inventario con entre 3 y 4 activos críticos. Las descripciones incluyen funciones generales, y al menos un activo carece de vinculación clara con los procesos.	14 – 0 puntos Elabora un inventario con menos de 3 activos críticos, o las descripciones no establecen relación con los procesos de la organización.	20
2. Evaluación de amenazas y vulnerabilidades	25 – 23 puntos Clasifica mínimo 4 amenazas y 5 vulnerabilidades, cubriendo seguridad física, lógica y humana. Incluye análisis de impacto y riesgo para cada elemento.	22 – 19 puntos Identifica al menos 3 amenazas y 3 vulnerabilidades. Describe su impacto de forma general, sin clasificar todos los elementos por tipo o nivel.	18 – 0 puntos Presenta menos de 3 amenazas o vulnerabilidades, o el análisis omite clasificación por tipo o nivel, o presenta errores técnicos en más de un elemento.	25
3. Propuesta de estrategia de seguridad integral	30 – 27 puntos Formula una estrategia con al menos 6 controles distribuidos entre seguridad física, lógica y de comunicaciones. Cada control se justifica técnicamente con base en los riesgos identificados.	26 – 23 puntos Presenta una estrategia con entre 3 y 5 controles, algunos sin vinculación clara con los riesgos identificados. Al menos dos controles carecen de justificación técnica específica.	22 – 0 puntos Incluye menos de 3 controles, o la estrategia no está relacionada con el diagnóstico previo y carece de justificación técnica.	30
4. Sustento técnico y uso de conceptos	15 – 13 puntos Aplica correctamente al menos 5 conceptos técnicos, marcos de referencia o normativas, integrándolos de forma coherente en el	12 – 10 puntos Utiliza entre 3 y 4 conceptos técnicos, de los cuales al menos uno no está claramente explicado o no se relaciona	9 – 0 puntos Utiliza menos de 3 conceptos, o al menos dos presentan errores técnicos o aplicaciones incorrectas.	15

	diagnóstico y propuesta.	directamente con la estrategia propuesta.		
5. Claridad y calidad del informe	10 – 8 puntos Incluye portada, índice, introducción, desarrollo, conclusiones, referencias y al menos un recurso gráfico. No contiene errores ortográficos o de redacción.	7 – 5 puntos Incluye al menos 5 de los 7 elementos formales esperados. Presenta entre 1 y 3 errores ortográficos o gramaticales. Puede faltar un recurso gráfico.	4 – 0 puntos Incluye menos de 5 elementos formales. Presenta más de 4 errores ortográficos o gramaticales, y omite recursos gráficos.	10
			TOTAL	100

Rúbrica Seguridad en TI

Evidencia Final

Nivel de desempeño				
Criterios de evaluación	**Altamente competente (100%–86%)**	**Competente (85%–70%)**	**Aún sin desarrollar la competencia (69%–0%)**	%
1. Análisis de la amenaza seleccionada	20 – 18 puntos Describe origen, naturaleza técnica, objetivos y al menos un vector de ataque. Identifica 3 o más puntos específicos de exposición en la organización, relacionados con infraestructura o procesos.	17 – 15 puntos Describe origen, naturaleza técnica y al menos un vector de ataque. Identifica 1 o 2 puntos de exposición en la organización con relación parcial al caso.	14 – 0 puntos Omite uno o más elementos requeridos (origen, naturaleza, vectores). Identifica 1 punto o ninguno, sin establecer relación con el caso.	20
2. Evaluación de detección y controles	25 – 23 puntos Explica cómo se detectaría la amenaza utilizando al menos un control existente. Propone 2 controles adicionales,	22 – 19 puntos Explica la detección con al menos un control existente. Propone 1 o 2 controles adicionales, pero sin detallar su	18 – 0 puntos No explica la detección adecuadamente o los controles adicionales son irrelevantes o están ausentes.	25

	describiendo su función, tecnología y cómo mitigan la amenaza seleccionada.	función o vinculación con la amenaza.		
3. Uso de IA en la simulación del impacto	15 – 13 puntos Formula un prompt con al menos 3 elementos (alcance, tipo de daño, activos afectados). Incluye captura de la respuesta generada por IA y describe el impacto considerando procesos críticos.	12 – 10 puntos El prompt incluye 2 elementos clave. Se presenta la captura y una descripción parcial del impacto, con relación limitada al caso.	9 – 0 puntos El prompt es incompleto o no incluye la captura. La descripción del impacto es ausente o irrelevante para el contexto de la organización.	15
4. Simulación de respuesta organizacional	30 – 27 puntos Describe las tres etapas (detección, contención y recuperación). Asocia al menos una herramienta específica por etapa (ej. SIEM, EDR, XDR) y menciona 3 actores clave, indicando sus funciones.	26 – 23 puntos Describe dos etapas. Menciona herramientas en alguna de ellas y uno o dos actores clave, pero sin detallar sus funciones o coordinación.	22 – 0 puntos Describe una etapa de forma incompleta. No menciona herramientas específicas ni actores clave implicados.	30
5. Lecciones aprendidas y mejoras	10 – 8 puntos Expone 2 lecciones claras derivadas del análisis y simulación, y 2 mejoras específicas a la estrategia de seguridad, indicando su efecto directo sobre la postura organizacional.	7 – 5 puntos Presenta una lección y una mejora, o dos elementos sin explicar su aplicabilidad ni impacto en la estrategia.	4 – 0 puntos No presenta lecciones o mejoras, o bien son vagas y no se vinculan con el análisis realizado.	10
			TOTAL	100