Líneas de carrera y certificaciones

Hola. Este tema sobre las **certificaciones de carrera** es un complemento a lo que ya se había dejado como trabajo. Ahora veremos un resumen, algo más claro de lo que se comentó en clase o durante la exposición. Algunos puntos pueden variar, pero el objetivo es tener más claridad sobre las certificaciones y las **líneas de carrera** que existen actualmente en este rubro. Es importante tener en cuenta que el tema de **seguridad informática o ciberseguridad**, sin importar cómo se le nombre, sigue manejando los mismos principios fundamentales. Desde el inicio de las clases se comentó que existen **dos enfoques profesionales** principales en seguridad:

1. **Enfoque defensivo**
2. **Enfoque ofensivo**

1. Enfoque Defensivo

Dentro del **enfoque defensivo**, se identifican dos niveles:

A. A nivel técnico:

- Analistas de seguridad
- Ingenieros de ciberseguridad
- Especialistas en manejo de incidentes
- Threat hunters (cazadores de amenazas)
- Analistas forenses
- DevSecOps
- Auditores TI (sí, también aparecen aquí)

Importante: No todos los roles mencionados son los únicos existentes. Hay muchas variantes, pero estos son los más comunes en el mercado.

B. A nivel de gestión:

- Gestión de cumplimiento normativo
- Manejo de políticas y controles
- Oficial de seguridad de la información (CISO)

- Gerente de seguridad de la información
  (A veces similar al oficial, depende de la organización)
- Oficial de confianza digital y privacidad
  (Término más utilizado actualmente en el Estado)
- Gestión de riesgos
- Arquitecto de ciberseguridad (también para cloud)

Nota: Muchos de estos roles se pueden encontrar tanto en el sector público como en empresas privadas. En algunas instituciones, el nombramiento del "oficial de seguridad" es solo formal, sin que se cumpla un rol real o se cuente con apoyo o perfil adecuado.

Nivel técnico	Nivel de gestión
Analista/Ingniero de seguridad informática	Oficial de seguridad de información
Analista/Ingeniero de Seguridad de redes	Gerente de Seguridad de la información
Especialista en Manejo de incidentes de seguridad informática	Oficial de confianza digital y privacidad
Threat Hunting	Gestión de riesgos de seguridad de la información
SOC	Auditor de TI
DevSecOps / Seguridad en operaciones	Arquitecto de ciberseguridad
Analista forense	
Blue team	
Auditor de TI	
Arquitecto de ciberseguridad	

---

2. Enfoque Ofensivo

El **enfoque ofensivo** busca poner a prueba las defensas para identificar debilidades. Los roles más conocidos son:

- Pentesters (testers de penetración)
- Ethical hackers (hackers éticos)

- Red Team (equipos que simulan ataques reales)
- Especialistas en ingeniería social
- Especialistas en phishing
- Expertos en OSINT
- Analistas de malware

Nivel técnico	Nivel de gestión
Pentester	Oficial de seguridad de información
Ethical Hacker	Gerente de Seguridad de la información
Red teamer	…
…	

Todos estos roles, tanto ofensivos como defensivos, forman parte de un ecosistema de seguridad que busca proteger los activos de información. En muchas convocatorias laborales, los cargos pueden tener distintos nombres, pero siempre se alinean a uno u otro enfoque. También es común que los profesionales coloquen en su CV o LinkedIn etiquetas que describen sus funciones dentro de estos enfoques.

El tema de los **enfoques defensivo y ofensivo en ciberseguridad** no debe entenderse como una competencia entre ambos, sino como una **complementación necesaria**. A veces se tergiversa esta idea, como si se tratara de una competencia por ver quién detecta más o quién gana. Sin embargo, si no se trabaja en **coordinación y con una misma visión**, no se obtendrán buenos resultados. Ambos enfoques deben cooperar para fortalecer verdaderamente la seguridad.

Salarios

Entre los roles clásicos del enfoque ofensivo están los **pentesters**, tanto internos como externos. Muchas empresas e incluso instituciones públicas ya cuentan con estos profesionales dentro de sus equipos de ciberseguridad ofensiva.

Estos equipos pueden incluir:

- **Pentesters**
- **Ethical Hackers**
- **Equipos Red Team**
- **Analistas de vulnerabilidades**

Es importante notar que, aunque estos roles son similares, **no son iguales**. Cada uno tiene funciones específicas. Por ejemplo, los **equipos Red Team** realizan pruebas más complejas y menos limitadas que un pentester tradicional. A diferencia de un pentester al que se le indica qué servidores probar o qué sistemas auditar, a un **Red Team** solo se le da el **nombre del dominio o de la organización**. Su tarea es buscar cualquier forma de vulnerar la seguridad, sin restricciones previas.

En el otro extremo está el **Blue Team**, que se encarga de:

- Monitorear
- Detectar actividades sospechosas
- Reaccionar ante amenazas

Este tipo de ejercicio se conoce como un **ejercicio Red vs Blue**, y es fundamental porque muchas veces los equipos defensivos (Blue Team) **no saben** que existe una debilidad o brecha. Entonces, el Red Team ayuda a evidenciar fallos que pueden ser aprovechados para intrusiones reales.

A nivel de gestión, los roles como **gerente u oficial de seguridad de la información** siguen siendo los mismos. Sin embargo, hay diferencias en las posturas de los profesionales:

- Algunos priorizan pruebas ofensivas y de penetración para **evaluar las defensas**
- Otros prefieren una postura defensiva, enfocada en **capacitación, políticas de protección y compra de tecnologías defensivas**

Ambas posturas son válidas. Lo importante es reconocer que se trata de **enfoques complementarios**, no excluyentes.

Rol / Cargo	Salario promedio USD anual (USA)	Comentarios
Pentester	115,000 – 200,000	Pentester junior: 70,000 anual Pentester senior: 115,000 – 200,000 anual Ref: • https://www.cybersecurityjobs.com/penetration-tester-salary/ • https://www.payscale.com/research/US/Job=Penetration_Tester/Salary • https://www.glassdoor.com/Salaries/penetration-tester-salary-SRCH_KO0,18.htm Algunas certificaciones pueden incrementar el valor hasta 250,000.
CISO	200,000 – 300,000	Con maestria en ciberseguridad Ref.: • https://fortune.com/education/articles/cybersecurity-masters-grads-are-landing-200k-plus-pay-packages/

💰 Sueldos en seguridad informática

Una de las preguntas frecuentes es: **¿Cuánto ganan los profesionales en este campo?**

Los sueldos varían mucho, pero tomando como referencia cifras de Estados Unidos (que también sirven como base para Latinoamérica, dado que muchos trabajan de forma remota o para empresas extranjeras), se tiene lo siguiente:

Rol	**Rango salarial anual (USD)**
Pentester	$115,000 – $200,000
Junior	~ $70,000

Nota: Las brechas salariales ya no son tan marcadas porque muchos profesionales trabajan de forma global, sin importar su país de origen. Esto ha generado una **normalización salarial** entre Latinoamérica y EE.UU., al menos en este sector especializado.

💼 Ingresos, subcontratación y mercado de certificaciones en ciberseguridad

En lo que respecta a los **niveles de ingresos en ciberseguridad**, no siempre se observa una realidad uniforme. Existen **casos frecuentes de subcontratación**, donde las empresas que ganan contratos o licitaciones **no cuentan con personal especializado en su staff**, sino que

contratan a técnicos de manera puntual para ejecutar los proyectos. En muchos de estos casos, ni siquiera se contrata a profesionales calificados, sino a **practicantes**, cuyo trabajo muchas veces se limita a **ejecutar herramientas automáticas**. Como consecuencia, los **ingresos que reciben estos jóvenes son bastante reducidos**, mientras que las **ganancias para la empresa contratista son considerablemente mayores**.

En el área de gestión, la situación es distinta. Por ejemplo, un **oficial de seguridad de la información**, con una maestría especializada en ciberseguridad, puede llegar a ganar entre **200,000 y 300,000 dólares anuales**.

Estas cifras provienen de fuentes confiables de análisis de negocios, las cuales **actualizan sus datos anualmente**, ya que **los sueldos varían dependiendo de la demanda, las tecnologías emergentes y las tendencias en especialización**.

Hay páginas reconocidas que realizan **encuestas de mercado** y elaboran informes sobre:

- Los sueldos promedio en tecnología.
- Las certificaciones más demandadas.
- Las habilidades que buscan las empresas a futuro.

Es recomendable que los estudiantes **revisen estas fuentes regularmente**, para conocer las **tendencias en roles y funciones**, más allá de una simple carrera profesional.

Certificaciones

🎓 **Proliferación de certificaciones**

Ante esta demanda creciente de profesionales, el mercado **se ha saturado de certificaciones**. Existen hoy en día **decenas, incluso cientos de acreditaciones**, muchas de las cuales:

- **No son confiables**.
- **No son convenientes en costo-beneficio**.
- **No garantizan calidad ni reconocimiento real**.

Algunas certificaciones sí **facilitan el acceso al mercado laboral**, sobre todo en proyectos específicos de protección, defensa o pruebas ofensivas. Muchas empresas **exigen estas certificaciones como requisito mínimo**, por lo que el mercado **se mueve mucho en torno al "papel"**: una insignia, un badge, o un diploma puede ser determinante para ser contratado.

Sin embargo, desde hace algunos años, se ha observado que **muchas certificaciones han perdido credibilidad**, porque:

- **Los exámenes son fácilmente accesibles en internet**.
- Las preguntas **se memorizan sin comprensión real**.
- En algunos casos, incluso se **hace trampa para aprobar**, rompiendo toda ética, honestidad e incluso la legalidad.

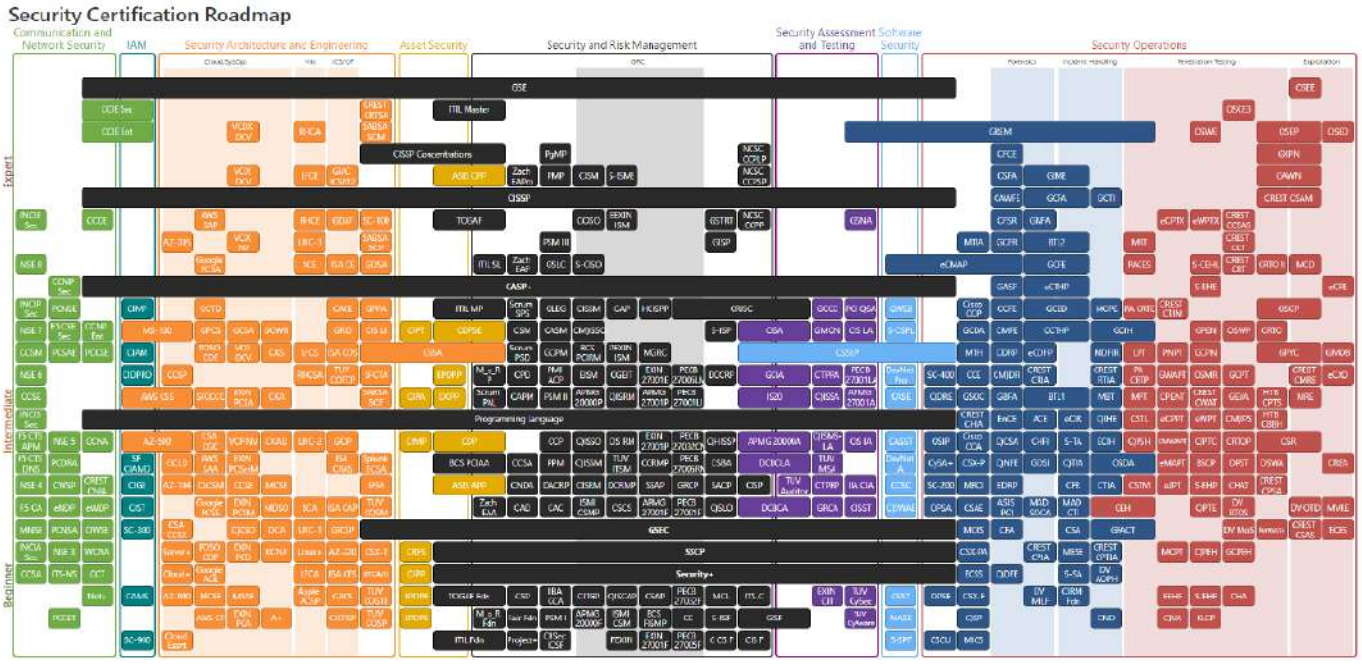
Y aunque esto no debería suceder, **es una realidad que muchas veces no se puede detener**.

Afortunadamente, existen profesionales que han trabajado en la creación de un **mapa mundial de certificaciones en ciberseguridad**. Este material, que también subiré como diapositiva, se actualiza periódicamente para reflejar los cambios del mercado.

En ese mapeo se pueden observar:

- Más de **400 certificaciones clasificadas**.
- **Tres niveles**:
    - Nivel **básico o de entrada** (parte inferior del gráfico)
    - Nivel **intermedio** (zona media)
    - Nivel **avanzado o experto** (zona superior)

Este trabajo fue realizado por un equipo especializado, que categorizó las certificaciones **por nivel y por fabricante**.



📄 Principales marcas en el mapa de certificaciones

Entre las marcas más representadas se encuentran:

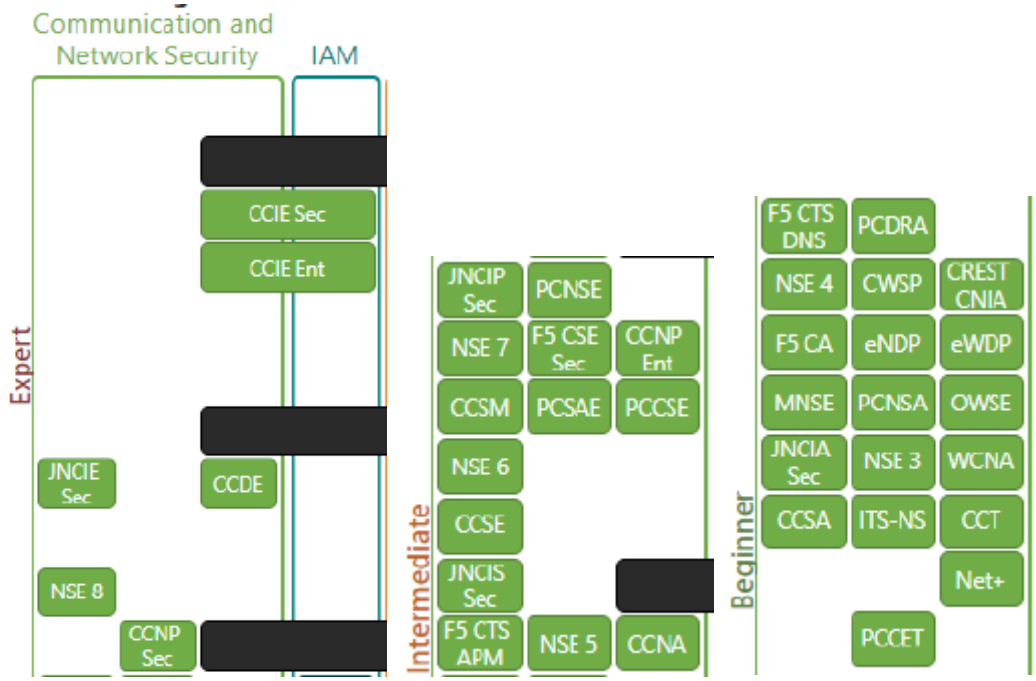
- **Cisco** (CCNA, CCNP, CCIE)
- **Juniper Networks**
- **(ISC)²** (CISSP, SSCP)
- **Fortinet** (NSE 4 al NSE 8)
- **F5 Networks**
- **Palo Alto Networks**

Estas certificaciones abarcan desde redes y firewalls hasta seguridad en la nube, siendo cada vez más relevantes en proyectos internacionales y de alta especialización.

En el **mapa de certificaciones** mencionado anteriormente, se observa la presencia de **todas las marcas más reconocidas en redes y seguridad de redes**. Estas marcas están representadas por fabricantes de:

- Cortafuegos (firewalls)
- Routers
- Switches

Estas tecnologías, fundamentales para las redes, aparecen en la **franja verde del gráfico** (zona recomendada y popular).



🔷 Certificaciones defensivas en redes

Por ejemplo, se visualiza la certificación **CCNA Security**, que no debe confundirse con la versión básica de CCNA. Esta certificación está enfocada en:

- **Seguridad en redes**
- **Enfoque defensivo**

No es una certificación ofensiva. Es decir, se centra en proteger redes, no en atacarlas.

Otra línea de certificaciones que ha ganado mucha **popularidad** últimamente es la relacionada a **Cloud Security**:

- **AWS Certified Security – Specialty**
- **AWS (Amazon Web Services)** es uno de los principales referentes en esta área.

Estas certificaciones están **orientadas exclusivamente a seguridad en la nube**, y se están posicionando fuertemente en el mercado.

🔷 Certificaciones en gestión y riesgos

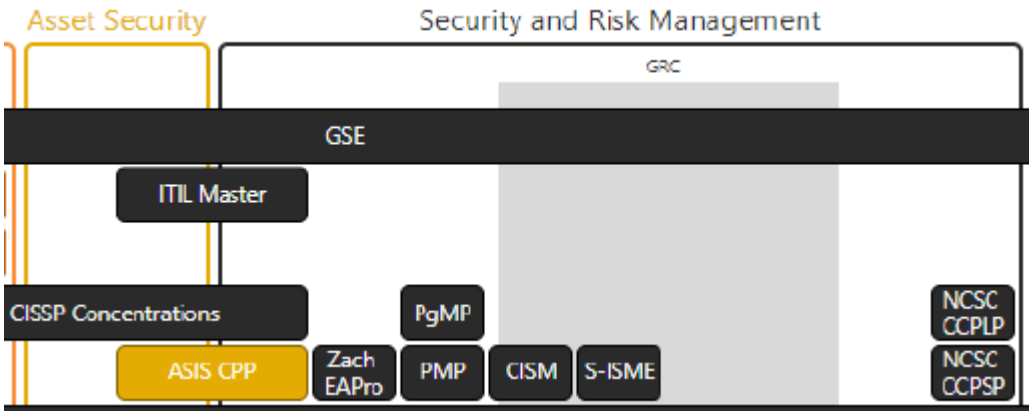
En la parte superior del gráfico (cuadros oscuros), se encuentran certificaciones orientadas a:

- **Gestión de riesgos**
- **Seguridad organizacional**

Algunas de las más representativas:

- **ITIL Master** (nivel avanzado en gestión de servicios TI)
- **GSE (GIAC Security Expert)** de **SANS Institute**
    - Esta es una certificación **transversal**, ya que cubre múltiples dominios.
    - Es considerada una de las más completas y costosas del mercado.
- **PMP (Project Management Professional)** de PMI
    - Incluye un **capítulo específico sobre análisis de riesgos**.
    - Por ello, se posiciona también dentro de la gestión de seguridad.

Estas certificaciones también están relacionadas con la gestión de TI, gobernanza y planeamiento estratégico.



🎓 Tipos de exámenes de certificación

Existen distintas **formas de obtener una certificación**, y varían en dificultad y requisitos:

Exámenes simples:

- Duración de **1 a 3 horas**.
- Se realiza un examen teórico o de selección múltiple.
- Al aprobar, se obtiene directamente la certificación.

Exámenes complejos (ej. PMP):

- Se requiere:
  - **Examen teórico supervisado (aprox. 4 horas)**.
  - **Acreditar al menos 5 años de experiencia** en gestión de proyectos.
  - **Presentar un expediente** con documentos que certifiquen esa experiencia.
- Solo después de cumplir estos requisitos, se puede obtener la certificación.

🔧 Certificaciones técnicas por operación

En la parte técnica (más operativa), se encuentran certificaciones como:

- **OSCP (Offensive Security Certified Professional)**
- **Open Security (OSEP, OSWE, etc.)**

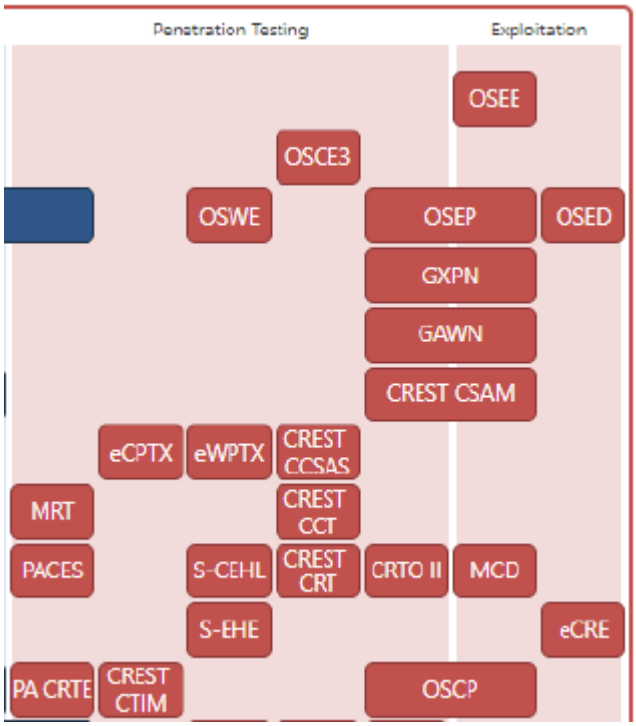
Estas certificaciones no se limitan a pruebas teóricas. En muchos casos:

- Requieren resolver **retos prácticos**.
- Se debe comprometer el sistema, demostrar habilidades técnicas reales.

- Son **altamente valoradas** por su nivel de dificultad y aplicabilidad real.

También leí que el **OSCE** está ubicado en la parte superior del mapa de certificaciones. En general, **todas las certificaciones OS** (Offensive Security) son de alto nivel técnico. Por otro lado, las certificaciones que terminan en **"HE"** o relacionadas a **SANS** son algunas de las **más costosas y complejas** del mercado.

¿A qué nos referimos con "complejas"? No basta con dar un examen y obtener la certificación. Por ejemplo, para obtener una certificación como el **GSE (GIAC Security Expert)**, ubicada en la cima del gráfico, debes haber aprobado **tres certificaciones previas del mismo nivel**. Es un proceso progresivo, no inmediato.



En cuanto a las certificaciones como **OSCE, OSWE u OSEP**, no se trata de exámenes de opción múltiple. En lugar de marcar respuestas, el examen consiste en resolver **retos prácticos**. Te dan acceso a un **laboratorio virtual** con escenarios reales y debes resolverlos por completo.

Si postulas a una certificación ofensiva (por ejemplo, como pentester), se espera que puedas:

- Acceder a los sistemas.
- Identificar vulnerabilidades.
- Explotarlas.
- Obtener evidencia clara.

No basta con encontrar una simple “banderita” (flag) como ocurre en algunos retos básicos. Esa es solo una parte del examen. La evaluación concluye con la **elaboración de un informe técnico completo**, en el que debes documentar:

- Todas las vulnerabilidades encontradas.
- La forma en que fueron explotadas.
- Las pruebas y evidencias respectivas.

Estos informes pueden **variar significativamente** de un postulante a otro. Por ejemplo:

- Un informe puede reportar 10 vulnerabilidades.
- Otro puede identificar 25, 30 o incluso 40.

La evaluación no se basa solo en la cantidad, sino en:

- **La calidad del análisis.**
- **La documentación de los pasos realizados.**
- **La profundidad de la explotación.**

Todo esto se valora en conjunto para determinar si apruebas o no. Además, este tipo de examen es **100% práctico** y de larga duración. Por ejemplo, el examen del **OSCP** tiene una duración de **24 horas**.

Tú eliges cuándo comenzar. Si empiezas a las 12 del mediodía, tienes hasta las 12 del día siguiente para completar el laboratorio y resolver todos los retos planteados. Es un examen exigente y realista, orientado a medir habilidades técnicas en condiciones similares a un entorno profesional.

Aunque los exámenes de certificaciones como **OSCP, OSWE o OSEP** tienen una duración de 24 horas, **no son libres ni autónomos**. De hecho, están **altamente supervisados**.

Durante el examen:

- Debes tener **cámara y micrófono encendidos** todo el tiempo.
- Hay **supervisores remotos** que se turnan cada 4 horas para vigilar la sesión.
- Se registra absolutamente todo: si conversas, si mueves la mirada, si escribes fuera de la pantalla, etc.

Antes de empezar:

- Te solicitan hacer un **barrido completo con la cámara** del entorno donde te encuentras.
- Tu **escritorio debe estar limpio**, sin ningún otro dispositivo a la vista.
- Tu equipo debe ser de uso exclusivo y estar en un ambiente **cerrado, silencioso y libre de distracciones**.

También, los supervisores pueden **tomar control remoto de tu máquina** para asegurarse de que no estés utilizando herramientas indebidas ni recibiendo ayuda externa. Esto se hace porque existen casos donde los postulantes intentan **comunicarse con terceros** durante el examen, por ejemplo a través de chats ocultos.

⏱️ Pausas y medidas antifraude

Es posible **pausar el examen para comer, ir al baño o descansar**, pero se debe **coordinar previamente**. Cuando te ausentas de la cámara, la sesión se **suspende automáticamente**. Esto implica que:

- No puedes continuar avanzando fuera de cámara.
- No puedes dejar la sesión abierta e irte.

Estas **ventanas de inactividad** son críticas, ya que podrían ser utilizadas por algunas personas para **recibir ayuda externa**. Por eso la supervisión es tan estricta.
De hecho, **ya se han detectado casos de fraude**, y los postulantes han sido **baneados permanentemente** sin posibilidad de volver a obtener la certificación.

📜 El informe: parte clave del examen

Al finalizar el examen práctico, se debe presentar un **informe técnico detallado**, que:

- Documente cada paso realizado.
- Presente evidencias de las vulnerabilidades encontradas y explotadas.
- Explique el proceso de forma clara, estructurada y en inglés (no se permite usar solo traductor automático).

Este informe es **una parte fundamental del examen**, y su calidad influye directamente en la nota final. No basta con encontrar una vulnerabilidad: debes demostrar que comprendes lo que hiciste, cómo lo hiciste y cuál es su impacto.

📆 Tiempos según certificación

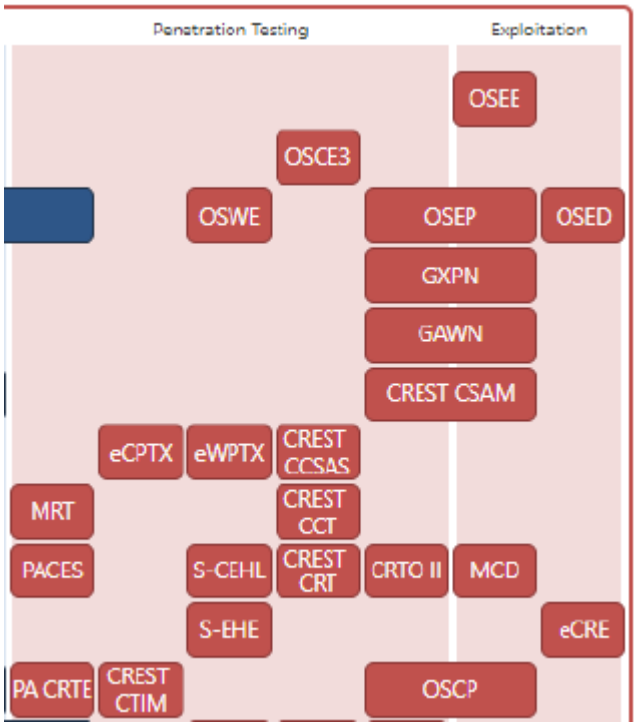
Cada certificación tiene su propia estructura de tiempos:

- **OSCP**:
    - 24 horas para completar el laboratorio.
    - Inmediatamente después, **24 horas para entregar el informe**.

- Es un examen muy intenso; si después de las primeras 8 horas no logras avances, **la frustración puede jugarte en contra**.

- **OSEP / OSWE (los "W")**:
  - Dispones de **7 días para completar el laboratorio**.
  - Luego, tienes otros **7 días adicionales para entregar el informe**.
  - Esta modalidad permite una mejor gestión del tiempo, pero sigue siendo exigente.

En exámenes como el **OSEP**, puede suceder que en los primeros días no logres acceder a la aplicación objetivo. En esos casos, es importante revisar las notas y pruebas, reintentar, y si es necesario, solicitar reprogramación del informe.



Exigencia extrema en exámenes OS: 48 horas sin descanso

Una de las grandes exigencias de las certificaciones ofensivas como el **OSCP** es que **muchos postulantes no duermen durante el proceso**. ¿Por qué?

- El examen práctico dura **24 horas continuas**, en las que debes comprometer y vulnerar sistemas en un laboratorio real.
- Pero después de eso, tienes otras **24 horas para elaborar y entregar el informe técnico**.

Es decir, en el caso extremo, podrías pasar **hasta 48 horas sin dormir**, lo cual genera un nivel alto de **estrés, cansancio y presión mental**.

Entre todas las certificaciones disponibles en el ámbito de ciberseguridad ofensiva, hay una clasificación no oficial pero bastante consensuada en la comunidad técnica. Esta clasificación **no es estrictamente formal**, sino una recopilación basada en lo que se observa en el **mercado, la comunidad técnica y la demanda empresarial**.

Las más **valoradas por la comunidad técnica**, debido a su dificultad, realismo y cercanía con entornos reales, son:

- **OSCP** (Offensive Security Certified Professional)
- **OSCE**
- **OSWE** (Web Exploitation)

Estas son certificaciones ofrecidas por **Offensive Security**.

🌎 Firmas más reconocidas en certificaciones ofensivas

Las **cuatro principales empresas** que dominan el mercado de certificaciones ofensivas son:

1. **Offensive Security**
2. **EC-Council** (creadores del CEH – Certified Ethical Hacker)
3. **Mile2** (creadores de CPTE)
4. **eLearnSecurity** (empresa italiana con certificaciones como eWPT, eCPPT, eJPT)

En cuanto a **certificaciones disponibles en universidades**, muchas academias, incluida la nuestra, ofrecen acceso a la certificación **CEH (Certified Ethical Hacker)**.

Nota: A pesar de estar en un entorno académico, **no se otorgan gratuitamente**, ya que son certificaciones comerciales.

📈 ¿Qué pide el mercado?

El mercado laboral y de servicios de ciberseguridad **valora especialmente** estas certificaciones:

- **CEH** (por ser la más antigua y mediáticamente difundida)
- **OSCP**
- **CPTE**
- **eWPT**
- **PPTS**
- **PTX**

De hecho, en **licitaciones públicas o privadas**, se puede requerir que el postulante cuente con al menos **tres de estas certificaciones**, dependiendo de la complejidad del proyecto o servicio.

Certificaciones a nivel defensivo

En el enfoque **defensivo**, ocurre algo similar al ofensivo. También hay certificaciones muy valoradas por la comunidad profesional. ¿Y cómo sabemos cuáles son más valoradas?

Cuando uno **está realmente involucrado en el campo**, comienza a interactuar con profesionales especializados, participa en **eventos, congresos, conferencias** y espacios de trabajo donde se comparte experiencia. En esos entornos se discute, **se debate** y se recomienda constantemente cuáles son las certificaciones **más relevantes y atractivas**.

Certificaciones más valoradas por la comunidad		Certificaciones más valoradas por el "mercado"		Certificaciones más valoradas por medios	
Técnico	Gestión	Técnico	Gestión	Técnico	Gestión
OSCP	CISSP	OSCP	CISM	CHE	CISM
OSCE3	CISM	CHE	CISSP	OSCP	CISSP
OSCW		C|PTE		C|PTE	
eCPPTx		eWPT			
eWPTx		eCPPT			
eCPPT					
eWPT					
CHE					
C|PTE					

👨💼 **Certificaciones en gestión**

En el ámbito de gestión, las certificaciones **no cambian tanto** como en el técnico. Las más posicionadas siguen siendo:

- **CISSP**
- **CISM**
- **ISO/IEC 27001**
- **PMP (Project Management Professional)**

Estas certificaciones se mantienen **estables en el mercado**, sin tantas variaciones ni tendencias influidas por redes sociales.

Percepción (Defensiva)

🎓 **Certificaciones de Cisco (defensiva)**

Una de las certificaciones más conocidas y exigentes en este campo es la **CCIE (Cisco Certified Internetwork Expert)**, que es **una de las más difíciles de obtener**.

🔷 **Certificaciones de Cisco:**

- **CCNA Security**:
  Disponible actualmente solo en inglés. Es una certificación accesible, con un examen de selección múltiple y simulaciones prácticas básicas.
    - Duración: 90 minutos o hasta 2 horas.
- **CCNP**:
  Es un examen más largo, alrededor de 2 horas y media a 3 horas, con contenido práctico más complejo.
- **CCIE**:
  Esta es la certificación más avanzada. Incluye:
    - Examen teórico.
    - Examen práctico.
    - Ambos se deben rendir **presencialmente** en las **instalaciones oficiales de Cisco**, por ejemplo, en Estados Unidos.

En el examen práctico:

- Te instalan una red completa con **routers, switches, topologías complejas**.

- Debes **resolver problemas reales** durante un examen que puede durar hasta **8 horas continuas**.
- Todo el examen es en inglés.

Además, **la certificación tiene una validez de solo 2 años**. Luego, debes **rendir nuevamente** para renovarla.

¿Por qué se requiere renovación?
Porque las tecnologías evolucionan constantemente y si no te mantienes activo en el campo, esa certificación pierde su sentido práctico.

Certificaciones más valoradas por la comunidad		Certificaciones más valoradas por el "mercado"		Certificaciones más valoradas por medios	
Técnico	Gestión	Técnico	Gestión	Técnico	Gestión
CCIE Sec.	CISSP	CCIE Sec.	CISM	NSE7	CISM
PCNSE (Palo Alto)	CISM	PCNSE (Palo Alto)	CISSP	PCNSA	CISSP
NSE8 (Fortinet)		NSE8 (Fortinet)	ISO 27001	CCNA Sec.	ISO 27001
CCNP Sec.		NSE7		AWS CSS	
CCNA Sec.		CCNA Sec.		CCNP Sec.	
PCNSA		CCNP Sec.			
NSE7		PCNSA			
CyberOps		CyberOps			

🧠 **Influencia de los medios y la comunidad**

Hay una **brecha entre lo que valora la comunidad técnica y lo que posicionan los medios o fabricantes**. Por ejemplo:

- La comunidad técnica suele valorar más certificaciones como **OSCP**, por su dificultad y nivel realista.
- Sin embargo, en redes sociales, influencers y campañas publicitarias tienden a **posicionar más al CEH**, por ser más mediática y accesible.

Esto genera **una pugna constante** entre la percepción técnica (basada en mérito y exigencia) y la percepción mediática (basada en visibilidad y marketing).

📌 Certificaciones: Perspectivas y niveles

Bueno, repasando el tema de las **certificaciones**, podemos decir que este panorama incluye muchísimas opciones. Aunque no todas están listadas aquí, si observamos el **mapa o ruta de certificaciones** presentado previamente, vemos que existen **numerosas especialidades**, tanto en seguridad ofensiva como defensiva.

Muchos profesionales optan por **no rendir** esta certificación, a pesar de su prestigio, porque:

- No trabajan en una empresa que requiera ese nivel.
- **El costo es elevado**.
- **No aprovecharían realmente el conocimiento adquirido** si no están en el rubro específico de diseño y arquitectura de redes.

Por eso, la **CCIE** está más orientada a:

- Arquitectos de redes de alto nivel.
- Profesionales que trabajan directamente con fabricantes como **Cisco, Microsoft, Google**, etc.
- Personal que participa en la **generación de tecnología** a gran escala.

🔒 Otras marcas defensivas populares

Entre las más **alcanzables** y también valoradas por el mercado, destacan:

- **Palo Alto Networks**
- **Fortinet (certificaciones NSE)**
- **Cisco (CCNA, CCNP)** nuevamente

Estas certificaciones son más accesibles para quienes desean trabajar en el campo de **infraestructura, seguridad perimetral, administración de firewalls y redes seguras**.

🗂️ En gestión, las certificaciones se mantienen estables

A diferencia del ámbito técnico, en el área de **gestión de la seguridad de la información**, las certificaciones **no cambian tanto con el tiempo**. Las más reconocidas siguen siendo las mismas y se mantienen estables en el mercado.

🎯 Diferencias de enfoque en el rol de oficial de seguridad

Como comentábamos hace un momento, el **oficial de seguridad** sigue siendo el mismo rol en esencia; sin embargo, **las posturas pueden variar** dependiendo del enfoque, la formación y las exigencias del entorno. Estas diferencias se notan en qué certificaciones valoran más tanto **el mercado como los medios especializados**.

🔝 Certificaciones más valoradas por el mercado

Entre las más reconocidas y recurrentes en los entornos técnicos y mediáticos se encuentran:

- **CCIE** (Cisco)
- **Fortinet** (NSE)
- **Palo Alto Networks**
- **Panw**
- **Cisco CCNP / CCNA**

Estas marcas suelen **aparecer constantemente entre las primeras posiciones** en rankings, publicaciones y ofertas laborales. Fortinet y Palo Alto, por ejemplo, son muy populares en redes sociales y entornos profesionales, y aparecen repetidamente en certificaciones defensivas.

☁️ Auge de la seguridad en la nube (Cloud Security)

Un aspecto que **aún no se refleja completamente en las diapositivas** (porq están basadas en datos del año pasado), pero que está ganando fuerza, es el **tema de Cloud Security**.

Especialmente con **AWS (Amazon Web Services)**, cuyas certificaciones de seguridad están tomando relevancia significativa en los campos de **ciberseguridad general**. Incluso se podría decir que AWS ya compite por las primeras posiciones en el mercado actual.

🔒 Certificaciones de gestión

En cuanto a la **gestión de la seguridad**, también existen certificaciones importantes y accesibles, como:

- **ISO/IEC 27001 – Líder Auditor**
- **PMP (Project Management Professional)**

En el caso de **ISO 27001 Líder Auditor**, puedo compartir desde la experiencia que es una de las certificaciones **más fáciles de obtener** dentro del área de gestión:

- El examen dura aproximadamente **90 minutos**.
- Si has leído el material y tienes buen criterio, **no debería ser difícil**.
- Se basa más en **sentido común** y comprensión general del estándar.

📘 Exámenes teóricos y prácticos: diferencias

También existen otras certificaciones como la **7001**, que tienen un examen de:

- **60 minutos**
- **40 preguntas**

Algunas preguntas pueden parecer complicadas si **no tienes experiencia práctica**, ya que requieren análisis situacional.

Una **característica de los exámenes más complejos** (como PMP o certificaciones de gestión avanzadas) es que **no basta con memorizar conceptos**. Las preguntas presentan **casos reales**, donde: **Todas las respuestas pueden ser correctas**, pero debes seleccionar la **más adecuada al contexto**.En estos casos, debes **entender bien el escenario** y tener clara la teoría que justifique tu elección. No se trata de descartar respuestas obvias como en otros exámenes, sino de **identificar la opción óptima según el caso planteado**.

Por otro lado, los exámenes **más simples o básicos**, como algunos de tipo "control X", son más directos y no presentan tanto nivel de análisis. Y por supuesto, los **exámenes prácticos**, como los de Offensive Security, ya son otro nivel completamente diferente.

🎓 Certificaciones: entre la experiencia real y el valor ético

En el mundo de la ciberseguridad, tanto a nivel **de infraestructura** como en el ámbito **de gestión**, las certificaciones requieren diferentes niveles de preparación y experiencia.

Por ejemplo:

- En certificaciones como **CISM**, similares al **PMP**, se exige **acreditar al menos 5 años de experiencia en gestión de la seguridad de la información** para poder acceder a ellas.

Esto muestra que **no todas las certificaciones son iguales**, ni garantizan automáticamente competencia profesional. Tener una certificación **no siempre significa que ya "la hiciste"**. Puede ayudarte, sí, pero quienes estamos en el rubro sabemos distinguir cuáles certificaciones tienen verdadero valor y cuáles han perdido peso debido a **su facilidad de obtención o falta de rigurosidad**.

Mi consejo es que, al rendir un examen de certificación —en este u otro rubro— lo hagan **como un desafío personal**, no solo como un requisito laboral.
Es decir, que se trate de **probarse a uno mismo** que puede lograrlo por mérito, sin necesidad de

hacer trampa, sin buscar atajos, sin memorizar preguntas de internet, ni recurrir a otras personas para que lo rindan por ustedes.

Lamentablemente, hemos visto casos incluso de **suplantación**, de personas que pagan para que alguien más les rinda el examen. Esto ocurre en todo tipo de evaluaciones, incluso en certificaciones internacionales como PMP, y **nadie está exento de que pueda pasar**.

⚠️ El lado oscuro: certificados sin sustento real

Hay una frase común entre quienes buscan aparentar experiencia sin tenerla:

“Ahora lo certificamos a fulanito, ya tiene su certificado.”

Este tipo de prácticas **son auditables**, al menos en organizaciones serias como **PMI**, que puede auditar de forma aleatoria para comprobar si realmente se cumplen los requisitos.

Pero la realidad es que **hay muchos que no valoran la ética ni la honestidad**, y aún así son los primeros en publicar en redes sociales frases como:

"¡Ya obtuve mi certificación!"

Cuando en realidad nadie sabe cómo la obtuvieron. Y es aquí donde se pierde el verdadero sentido del esfuerzo y la competencia profesional.

📉 ¿Certificaciones infladas?

Sí, el mercado **aún pide certificaciones** como parte de los procesos de selección, no solo en ciberseguridad, sino en prácticamente **todo lo relacionado a tecnología**. Un simple **badge digital** o un certificado de plataformas como **Google, Microsoft, Azure, AWS**, ya es un punto a favor en un CV.

Sin embargo, hoy en día estas ofertas se han **proliferado en exceso**. Hay cursos gratuitos por todos lados, y personas que **obtienen certificados semanalmente**, uno tras otro:

- Curso A, curso B, curso C…
- Cada día publican que aprobaron un nuevo módulo.

Pero luego uno se pregunta:

“¿Realmente está aplicando lo que aprendió? ¿Está trabajando en ese campo?”

Muchas veces, la respuesta es no. Solo están **acumulando certificados**, sin desarrollo profesional real detrás.

📄 Duración y renovación de certificaciones

—¿Alguna pregunta, muchachos?

—Sí, profesor, ¿cuánto tiempo duran las certificaciones? ¿Se pueden renovar o hay que hacer todo el proceso de nuevo?

La respuesta es: **depende de la certificación**.

🛡️ Certificaciones sin vencimiento

Por ejemplo, **OSCP** es una certificación **permanente**: una vez obtenida, **no caduca**.

🔁 Certificaciones con renovación obligatoria

En cambio, otras como las de **Cisco** (CCNA, CCNP, etc.) tienen una **vigencia de 3 años**. Para renovarlas, debes **volver a rendir el examen** y así mantener activa tu certificación.

- Si no lo haces, **no pierdes la certificación**, pero esta quedará **no vigente**, es decir, ya no estás certificado de manera **activa**.

💡 Otras formas de renovación: PDUs

Algunas certificaciones permiten renovar **acumulando puntos**, conocidos como **PDUs (Professional Development Units)**.

Por ejemplo, en el caso del **PMP (Project Management Professional)**:

- La certificación dura **3 años**.
- Debes **acumular 60 PDUs** durante ese período.

Puedes obtener PDUs mediante:

- Participación en **conferencias de gestión de proyectos**.
- **Dirección o ejecución de proyectos reales**.
- **Dictado de clases** o redacción de contenido sobre gestión de proyectos.

Al juntar los puntos, pagas la renovación y mantienes tu certificación activa. Yo, por ejemplo, tengo mi PMP desde 2013, y la he renovado varias veces así.

🔄 Ejemplo con Cisco

En el caso de Cisco:

- Si obtienes el **CCNA**, después de 3 años puedes optar por rendir un **examen superior** como el **CCNP**.

- Al aprobar el CCNP, tu certificación CCNA también se **renueva automáticamente**.

Cisco ha incorporado también el **sistema de PDUs** (como lo hace PMI), en el que puedes sumar puntos asistiendo a conferencias, cursos, foros especializados, o incluso escribiendo libros.

💰 ¿Negocio o necesidad?

Muchas veces, la renovación de certificaciones responde más a un **modelo comercial** que a una necesidad técnica. Los fabricantes de tecnología **necesitan mantener a los profesionales dentro de su ecosistema**.

Nosotros —los estudiantes, egresados y docentes— somos su **mejor herramienta de marketing**. Si todos aquí aprendiéramos únicamente tecnología de Cisco, lo más probable es que, al salir al mercado laboral, recomendemos o trabajemos con **productos de Cisco**.

Por eso, en nuestra institución **no nos casamos con una sola marca**, sino que apostamos por una **formación diversa**, abarcando múltiples tecnologías y certificaciones. Así ustedes tienen **más opciones para elegir**.
