

Fundamentos de ciberseguridad

Una carrera profesional en ciberseguridad

Mercado laboral

5 Minutos

Visión general del módulo

Este módulo se centra en la creciente necesidad actual de profesionales de ciberseguridad en todo el mundo. Se incluyen los siguientes temas:

- La demanda de profesionales de ciberseguridad en el mercado de trabajo actual
- Los principales atributos y habilidades que deben poseer los profesionales de ciberseguridad
- Las principales responsabilidades de los trabajos de ciberseguridad más comunes
- Las certificaciones de ciberseguridad que hay disponibles
- Recursos para obtener más información y ver las opciones que deben tenerse en cuenta para empezar una carrera profesional en ciberseguridad

Después de completar este módulo, los alumnos deberán ser capaces de:

- Resumir el mercado laboral de los profesionales de ciberseguridad
- Identificar los principales atributos y habilidades que deben poseer los profesionales de ciberseguridad
- Describir las principales responsabilidades implicadas en los puestos de trabajo típicos de ciberseguridad
- Analizar algunas de las certificaciones comunes de ciberseguridad disponibles
-

[Preferencias sobre cookies](#)

Enumere los recursos y las opciones a tener en cuenta para aquellos que comiencen una carrera en ciberseguridad

Mercado de trabajo actual

La ciberseguridad es un campo fascinante y en constante crecimiento que se encuentra en la intersección de las tecnologías establecidas y las amenazas de ciberseguridad emergentes. Como carrera profesional, requiere una amplia variedad de habilidades y características personales, algunas de las cuales puede que ya posea. Los profesionales de ciberseguridad no siempre han estudiado la típica licenciatura de cuatro años. Proviene de distintos orígenes. Puede que esté empezando su carrera, cambiando de trabajo o empezando una segunda carrera.

Si está considerando una carrera en ciberseguridad, es importante conocer el mercado de trabajo actual y las proyecciones en el futuro, las habilidades que necesita para empezar y tener éxito en un trabajo de ciberseguridad, y algunos de los puestos de trabajo más comunes. Vamos a ampliar la información sobre la gran demanda de profesionales de ciberseguridad en todo el mundo.

Si hay una tendencia que todos observamos es que la ciberseguridad es un mercado en rápido crecimiento con excelentes oportunidades profesionales. Da igual cómo haga las cuentas, en la próxima década habrá una gran necesidad de profesionales de ciberseguridad. A continuación, se muestran algunos datos clave.

Las ofertas de trabajo en ciberseguridad **crecerán un 35 %** entre 2021 y 2031, lo que supone una tasa media de crecimiento muy superior a la del resto de trabajos.

– Oficina de Estadísticas Laborales de EE. UU. (<https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm>)

Se calcula que hay **4,19 millones de profesionales de ciberseguridad en todo el mundo**, lo que significa un aumento de más de 700.000 con respecto a los datos de 2020.

– 2021 (ISC)2 Cybersecurity Workforce Study (<https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx>)

Habrá **3,5 millones de puestos ciberseguridad sin cubrir** a nivel mundial en 2025. De estos puestos vacantes, se espera que India tenga más de 1,5 millones de trabajos vacantes en ciberseguridad en 2025.

– Cybersecurity Ventures (https://cybersecurityventures.com/jobs/?utm_source=skillsbuild.org)

Las personas que trabajan en temas relacionados con ciberseguridad han mostrado **un alto grado de satisfacción con su trabajo** durante los últimos cuatro años. En 2021, el **77 %** indicaban estar satisfechos o muy satisfechos con su trabajo.

Preferencias sobre cookies

– 2021 (ISC)2 Cybersecurity Workforce Study (<https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx>)

© Copyright IBM Corporation 2022.

Principales atributos y habilidades

15 Minutos

La falta de profesionales de ciberseguridad cualificados deja muchos puestos vacantes y un déficit de competencias cada vez mayor. Puede que se esté preguntando qué conocimientos necesita para enfrentarse a las amenazas de seguridad. Si le gustan los retos y resolver problemas difíciles, esta puede ser un área de trabajo muy interesante para usted.

Vamos a explorar las características personales y los conocimientos que se necesitan para tener éxito en el campo de la ciberseguridad.

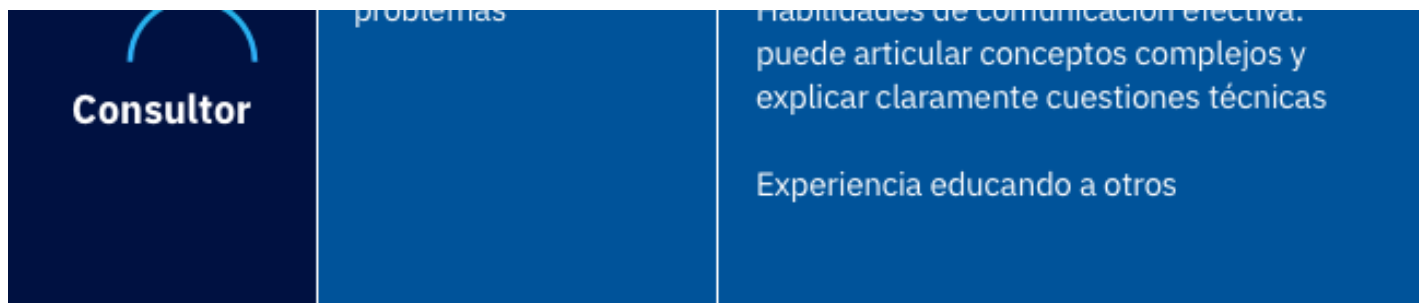
¿En qué habilidades deben centrarse los nuevos profesionales de ciberseguridad? Independientemente de la formación académica del profesional, hay algunos elementos fundamentales. Estos pueden clasificarse en dos grupos; atributos básicos y habilidades.

- Los **atributos básicos** pueden considerarse una disposición general muy útil para los profesionales de la seguridad: un conjunto de rasgos de personalidad y comportamientos adquiridos comunes.
- Las **habilidades** incluyen habilidades técnicas y relacionadas con el lugar de trabajo.

Un nuevo profesional de la seguridad puede que no tenga todas estas habilidades al principio, pero si se centra en ellas, con el tiempo podrá tener una carrera profesional más flexible y la base para puestos de liderazgo técnicos o relacionados con la empresa.

En esta tabla se muestran las habilidades y los atributos básicos que deben tener los profesionales. ¿Es su caso? Dedique un momento a revisarla.

	 Atributos centrales	 Habilidades
 Explorador	Investiga y le gustan los retos	Una comprensión innata de escenarios, riesgos y posibilidades
 Solucionador de problemas	Analítico, metódico y orientado al detalle	Experiencia práctica verificable con referencias, certificaciones y/o microcredenciales Familiaridad y cierta capacidad de codificación - para descubrir cómo construir y desarmar cosas
 Estudiante	Aprende constantemente	Conocimientos específicos del sector Capacidad de adaptarse a las tecnologías de seguridad nuevas y emergentes
 Tutor	Protector, ético y de confianza	Familiaridad con las normativas, leyes y políticas aplicables, y capacidad para interpretarlas
	Puede trabajar con otros para comprender y resolver sus problemas	Capacidad de trabajar en equipos dinámicos y diversos Preferencias sobre cookies Habilidades de comunicación efectiva:



Fuente: It's not where you start – it's how you finish: Addressing the cybersecurity skills gap with a new collar approach (<https://securityintelligence.com/events/its-not-where-you-start-its-how-you-finish-addressing-the-cybersecurity-skills-gap-with-a-new-collar-approach/>), IBM Institute for Business Value, 2017

¿Qué opina?

A continuación, se muestran algunas preguntas que debe responder. Escriba la respuesta a cada una en los recuadros. Reflexionar y escribir una respuesta es una buena forma de poner en orden sus ideas. Las respuestas son confidenciales y solo se guardan en este curso para su uso personal. Asegúrese de pulsar **Guardar texto**.

En términos de atributos básicos:

- ¿Se considera un **Explorador** de naturaleza inquisitiva y que disfruta con los retos? ¿Le gusta que cada día sea diferente y presente nuevos retos, frente a seguir una rutina?
- ¿Se considera un **Solucionador de problemas** al que le gusta observar los detalles y de carácter metódico?
- ¿Se considera un **Estudiante**, un aprendiz vitalicio al que le gusta estar al día de los últimos desarrollos, amenazas y tendencias de ciberseguridad? ¿Tiene aptitudes para crear una red de contactos y tener su propia comunidad de conocimiento (por ejemplo, colegas o participantes en conferencias)?
- ¿Se considera un **Guardián** protector y fiable? ¿Desea defender su reputación y la de su empresa para no ser el que "dejó pasar la amenaza"?
- ¿Se considera un **Asesor** al que le gusta trabajar en equipo para resolver problemas de negocio?

1. Piense en sus **atributos básicos**. ¿Qué atributos básicos tiene actualmente y qué atributos básicos le gustaría desarrollar en un futuro?

Guardar texto

En términos de habilidades:

[Preferencias sobre cookies](#)

¿Se considera un **Explorador** que puede entender los escenarios , los riesgos y los "casos hipotéticos"?

- ¿Se considera un **Solucionador de problemas** que puede aumentar sus habilidades de codificación, descubrir cómo se crean las cosas y conseguir experiencia práctica y certificaciones?
- ¿Se considera un **Estudiante** que puede aumentar sus conocimientos de seguridad y adaptarse a las tecnologías de seguridad emergentes?
- ¿Se considera un **Guardián** que puede familiarizarse y aumentar sus conocimientos sobre legislación y el respeto de los reglamentos?
- ¿Se considera un **Asesor** que puede comunicar con eficacia complejos técnicos complejos y trabajar con distintos equipos?

2. Piense en sus **habilidades**. ¿Qué habilidades tiene actualmente y qué habilidades le gustaría desarrollar en un futuro?

Guardar texto

Áreas de habilidades que debe desarrollar

Los profesionales de ciberseguridad tienen distintos orígenes, algunos de ellos provienen del campo de TI y otros de campos totalmente diferentes. La clave es **desarrollar** un conjunto de habilidades técnicas relevantes y relacionadas con el lugar de trabajo que puedan ofrecerle los conocimientos básicos necesarios para su puesto en ciberseguridad. A continuación, se muestran algunas áreas de habilidades que debe considerar. No es una lista exhaustiva, cubre las habilidades básicas a tener en cuenta.

Área de habilidades	Descripción
Administración del sistema	Para los sistemas operativos Linux, UNIX y/o Windows, debe conocer los aspectos básicos de la instalación, la configuración y el mantenimiento de los sistemas de cliente y servidor. Debe conocer los modelos subyacentes para la gestión de usuarios, los permisos, los sistemas de archivos y los scripts de mandato.
Administración de red	Debe conocer los protocolos como, por ejemplo, TCP/IP, FTP y SMTP. En concreto, debe saber qué significan y cómo se utilizan a nivel práctico.
Servicio al cliente	Necesita saber interactuar con clientes para ayudarles en el diagnóstico y la remediación de los problema de seguridad.
Comunicaciones	Necesita saber comunicar de forma sucinta, utilizando comunicación verbal y escrita, información técnica sobre incidentes de seguridad y la remediación de dichos incidentes.

Preferencias sobre cookies

Área de habilidades	Descripción
Aptitud para la investigación	Necesita tener curiosidad y disposición para detectar y sondear el comportamiento inusual. Esto puede demostrarse con experiencia en la resolución de problemas de TI o en un campo completamente distinto como, por ejemplo, la inteligencia militar. La clave es demostrar la iniciativa de realizar el trabajo de detección necesario para llegar al fondo de las situaciones sospechosas.

Cualquiera que trabaja en ciberseguridad debe ser imaginativo y poder encontrar soluciones rápidamente para que las infracciones no se conviertan en problemas masivos para una organización. Recuerde que pensando creativamente es como los ciberatacantes entraron en primer lugar. Un profesional de ciberseguridad debe ser igualmente creativo para averiguar cómo entraron en el sistema.

En general, tener habilidades técnicas, ser crítico, interactuar con personas y tener la "mentalidad de un detective" le ayudarán a lograr el éxito.

Puestos de trabajo de ciberseguridad

25 Minutos

Los profesionales de ciberseguridad están en la línea de frente de la defensa contra ciberdelitos para proteger sistemas vitales de amenazas internas y externas como, por ejemplo, malware, hackers e ingeniería social.

Todas las organizaciones tienen algún tipo de necesidad de seguridad de la información. Los datos deben protegerse en cualquier lugar. La ciberseguridad abarca muchos sectores. Las instituciones financieras, así como los sectores del gobierno, el sector educativo y los minoristas son algunos de los principales actores debido a su tamaño.

Hay muchas oportunidades de ciberseguridad diferentes, y en dichas áreas hay decenas de puestos que requieren distintas habilidades y experiencia. Algunos puestos pueden requerir viajar, mientras que otros se desempeñan en una ubicación fija como, por ejemplo, un centro de operaciones de seguridad (SOC). Este equipo centralizado supervisa una organización en busca de posibles incidentes de seguridad, los investiga y (si es necesario) los remedia. En esta lección, analizaremos algunos de los puestos más interesantes de ciberseguridad.

Centro de operaciones de seguridad (SOC)



Nota: hay muchos más puestos de trabajo en el campo de la ciberseguridad. No es una lista completa. Los puestos de trabajo varían por compañía y área de seguridad, así como por nombre. Estos son algunos de los puestos más comunes.

Analista SOC

En el centro de operaciones de seguridad (SOC) de la compañía, hay un **nivel de entrada** denominado el **analista SOC**.

- También se conoce como analista de ciberseguridad o analista de priorización.
- Este puesto es "reactivo", ya que el analista SOC responde a alertas individuales e investiga, como si fuera un detective, a partir de unas pruebas. Puede ver referencias a un analista SOC como un puesto de "Nivel 1". Los niveles con un número cada vez mayor se utilizan para indicar los niveles de responsabilidad y los requisitos de experiencia correspondientes. También puede ver referencias a un puesto "Junior".

¿Qué hacen durante un día típico?

[Preferencias sobre cookies](#)

- **Supervisan** el tráfico de red del sistema para detectar la actividad sospechosa que pueda indicar la presencia de hackers o malware, por ejemplo, troyanos y ransomware (secuestro de datos).
- **Investigan** las alertas desencadenadas por la herramienta de Supervisión de Sucesos e Incidentes de Seguridad (SIEM) (por ejemplo, **IBM Security QRadar** (<https://www.ibm.com/security/security-intelligence/qradar>)) cuando detecta sucesos sospechosos para determinar si la alerta es un falso positivo (una falsa alarma) o un verdadero positivo (un incidente de seguridad de la vida real que debe solucionarse). Si es una alerta de verdadero positivo, debe identificar el contexto, la causa y los usuarios afectados.
- **Evalúan** la gravedad del incidente de seguridad y asignan la valoración de riesgo correspondiente a los incidentes (por ejemplo, gravedad baja o alta).
- **Escalan** los incidentes de gravedad alta al experto en incidentes.

¿Cuál sería un ejemplo de lo que hace un analista SOC?

Supongamos que llega una alerta a la herramienta SIEM. El analista SOC determina que está relacionada con una infección de malware en el sistema de uno de los directivos de la organización. Después de la investigación, el analista SOC concluye que es un verdadero positivo. Como es un ataque que afecta a un directivo que tiene acceso a información muy confidencial, el analista SOC le asigna una severidad alta.

¿Cuáles son las habilidades necesarias para este puesto de trabajo?

- Habilidades de administración de sistemas y redes de sistemas.
 - Por ejemplo, ¿cómo fluye la conexión a través de una dirección IP y cómo fluye a través de una red, un direccionador y los dispositivos asociados con la red? ¿Cómo se administra un servidor Windows y un servidor Linux? ¿Qué es un servidor de bases de datos? ¿Cómo se consultan y se interpretan los registros del sistema de todos los sucesos y transacciones de un dispositivo, direccionador, cortafuegos, etc.?

Nota: este puesto no requiere habilidades de programación de sistemas. La codificación no es un requisito para este rol.

Experto en incidentes

A continuación, también en SOC, hay un puesto de trabajo de **nivel medio** denominado **experto en incidentes**.

- También se conoce como analista de respuestas a incidentes.

-

Preferencias sobre cookies

Este puesto determina si una alerta notificada es un ataque a una organización o una amenaza persistente en la red de una empresa, y garantiza su solución.

¿Qué hacen durante un día típico?

- **Determinan** el alcance de un incidente de ciberseguridad. Por ejemplo, si se detecta malware en la estación de trabajo de una persona en un departamento de recursos humanos, ¿se ha propagado a otros sistemas de ese departamento? ¿Se ha propagado a otras partes de la empresa? ¿Se ha contenido el comportamiento malicioso con las defensas automatizadas (por ejemplo, el software antivirus y los cortafuegos) o se han comprometido activos de la empresa?
- **Planifican la solución** en función del alcance del incidente de ciberseguridad. Esto implica investigar la naturaleza del incidente (por ejemplo, qué tipo de comportamiento malicioso busca el malware) y determinar cómo se debe responder a él.
- **Implementan la solución** con los equipos adecuados, por ejemplo, abriendo incidencias de TI para recrear una imagen de los sistemas infectados, formando a los usuarios finales sobre cómo evitar pulsar archivos adjuntos de correo de suplantación de identidad, o comunicando la gravedad de una infracción de datos a los directivos correspondientes cuanto antes.

¿Cuál sería un ejemplo de lo que hace un experto en incidentes?

Supongamos que se notifica un incidente de malware de gravedad alta en el ordenador de un directivo. El experto en incidentes determina si hay otros empleados afectados por el malware, cómo se debe responder al incidente y colabora con otros para conseguir su solución.

¿Cuáles son las habilidades necesarias para este puesto de trabajo?

- Habilidades de administración de sistemas y redes de sistemas.
- Familiaridad con la empresa y las políticas corporativas (por ejemplo, datos, privacidad, leyes)
- Habilidades de solución para seleccionar las acciones correctivas adecuadas, técnicas y no técnicas

Cazador de amenazas

A continuación, también en SOC, hay un puesto de trabajo de **nivel medio** denominado **cazador de amenazas**.

- También se conoce como analista de amenazas.
- Este puesto es "proactivo", ya que el cazador de amenazas realiza búsquedas para estar actualizado sobre las últimas amenazas, cómo han evolucionado y las reglas de código para desencadenar alertas en la herramienta SIEM para la empresa.

¿Qué hacen durante un día típico?

Preferencias sobre cookies

- **Investigan de forma proactiva** el "panorama de amenazas" mediante una supervisión continua de distintos recursos de amenaza, por ejemplo, **IBM X-Force Exchange** (<https://exchange.xforce.ibmcloud.com/>).
- **Evalúan** qué amenazas nuevas y emergentes suponen el máximo riesgo para su organización, en función de criterios como los sectores de destino, las vulnerabilidades explotadas y las tácticas utilizadas por las amenazas.
- **Responden** a estas amenazas de la siguiente manera:
 - Implementando cambios de configuración del sistema.
 - Programando la automatización en herramientas de seguridad para detectar automáticamente la actividad que es característica de estas amenazas.
 - Sensibilizando a la organización de los posibles ataques.

¿Cuál sería un ejemplo de lo que hace un cazador de amenazas?

Supongamos que se ha anunciado una amenaza de ransomware (secuestro de datos) completamente nueva. El cazador de amenazas investigará esta amenaza e implementará la automatización para evitar que la amenaza penetre en la organización y detectarla si intenta penetrar.

¿Cuáles son las habilidades necesarias para este puesto de trabajo?

- Habilidades de administración de sistemas y redes de sistemas.
- Conocer las fuentes de información de amenazas e implementar la automatización para detectar el comportamiento sospechoso

Nota: los cazadores de amenazas a menudo tienen experiencia en otros puestos de seguridad, por ejemplo, analista SOC, experto en incidentes, en pruebas de penetración o analista de pruebas de vulnerabilidad.

Posible progresión profesional

Es posible entrar en la profesión de la ciberseguridad sin un título si se empieza en un puesto de TI de nivel de entrada. A continuación, deberá ascender hasta llegar a un puesto de ciberseguridad.

En términos de progresión profesional, se pueden dar varios escenarios. Por ejemplo:

- Puede empezar como administrador de sistemas y, con el tiempo, hacer un cambio lateral a un puesto de analista SOC.
- Puede empezar como un analista SOC y continuar en ese puesto durante mucho tiempo.
- Puede empezar como un analista SOC y quizás convertirse en jefe de equipo SOC o avanzar hasta convertirse en un experto en incidentes.

Preferencias sobre cookies

Puede desempeñar una combinación de las responsabilidades de un analista SOC, un experto en incidentes y un cazador de amenazas.

- Como analista SOC, puede realizar un cambio lateral a un administrador de sistemas o un puesto de administrador de gestión de identidad y acceso (IAM).

Nota: esto dependerá de la madurez de la empresa. Las organizaciones más maduras pueden contratar los tres puestos de trabajo (analista SOC, experto en incidentes y analista de amenazas). Una organización menos madura puede tener una persona dedicada a una combinación de los tres puestos de trabajo.

Puestos de trabajo adicionales

A continuación, se muestran algunos puestos para familiarizarse con ellos.

Expanda cada puesto de trabajo para ver una descripción.

Asesor de seguridad



- Un puesto de nivel de entrada o nivel medio que es responsable de solucionar problemas de ciberseguridad bajo la dirección de un asesor experto.
- Realiza tareas que son necesarias durante el ciclo de vida de un proyecto.
- A menudo se contrata fuera de la empresa como fuente de conocimientos técnicos.
- Hay muchas especializaciones, por ejemplo, asesor de estrategia, asesor de operaciones, etc.

Administrador de seguridad



- Un puesto de nivel medio que también trabaja en el SOC, aunque es bastante diferente al puesto de analista SOC.
- Como un administrador de sistemas, este puesto trabaja con herramientas de seguridad como SIEM.
- Mantiene las herramientas de seguridad mediante la aplicación de parches y su ajuste para garantizar su buen rendimiento.
- Escribe scripts para automatizar las tareas en los sistemas de seguridad.

Preferencias sobre cookies

No investiga incidentes.

Administrador de Gestión de Identidad y Acceso (IAM)



- Un puesto de nivel de entrada o nivel medio que da soporte a distintos grupos en una compañía.
 - Responsable de gestionar autoridades y privilegios del sistema/aplicación, gestionar el inicio de sesión único, informar sobre aplicaciones y trabajar con desarrolladores para implementar prestaciones de gestión de identidad y acceso para nuevas aplicaciones.
 - Debe tener competencias sobre el uso de herramientas IAM y administración de redes.
-

Probador de penetración



- Un puesto más avanzado que emula a los cibercriminales.
 - Responsable de probar un sistema, una red o una aplicación para buscar las vulnerabilidades de seguridad que puede explotar un hacker.
 - A menudo se contrata fuera de la empresa para "infiltrarse" en el sistema de la empresa y proporcionar un nivel de control de calidad y evaluación externa.
-

Administrador móvil



- Un puesto de nivel de entrada que gestiona la protección de seguridad de los dispositivos móviles de los empleados.
 - Necesita conocimientos de administrador de sistemas.
-

Analista de conformidad



- Un puesto de nivel de entrada en una gran empresa que realiza auditorías internas para ver si la compañía está siguiendo sus políticas de seguridad y de privacidad y si cumple la legislación local.
- También ayuda a las organizaciones a estar preparadas para las auditorías externas, que son necesarias dependiendo del sector (por ejemplo, atención sanitaria, finanzas, etc.).

¡NO SE LO PIERDA!

Este sitio web muestra varios casos interesantes de personas que tienen perfiles y trayectorias profesionales totalmente diferentes en ciberseguridad. Vea cómo han empezado o han progresado.

🔗 **SecurityIntelligence: Voices of Security** (<https://securityintelligence.com/series/voices-of-security/>)

Este es el final de la lección. Asegúrese de seleccionar el recuadro "Actividad finalizada" para realizar un minicuestionario y demostrar los conocimientos que ha adquirido en esta lección. Se mostrarán tres escenarios prácticos para identificar el tipo correcto de puesto de ciberseguridad. Esto es necesario para terminar la lección.

Información sobre certificaciones

10 Minutos

Hay muchas certificaciones vigentes relacionadas con la ciberseguridad y muchas otras en desarrollo. Para estar al día en estas cualificaciones, deben estudiarse.

Las certificaciones pueden ser específicas del producto o pueden estar relacionadas con conceptos del sector. Las certificaciones existen en la industria para permitir el mantenimiento de estándares relacionados con las habilidades y el conocimiento. Los puestos que requieren cualificaciones específicas tienden a ser más especializados. Si un puesto requiere un determinado conjunto de habilidades, puede ver las certificaciones que se listan en su oferta de empleo.

Tener una certificación puede aumentar la gama de puestos de trabajo disponibles y ser una buena forma de demostrar determinados niveles de competencia cuando se solicita un trabajo.

Vamos a analizar varias de las certificaciones más comunes que hay disponibles en este campo.

Nota: algunas de estas certificaciones son para profesionales del sector con años de experiencia. Son cualificaciones en las que puede trabajar años después de conseguir un puesto relacionado con la seguridad. Se incluyen aquí para resaltar el progreso de la trayectoria.

Expanda cada certificación para aprender información clave.

CompTIA Security+



Esta es una certificación global que valida las habilidades de línea base que necesitan los profesionales para ejecutar funciones básicas de seguridad y seguir una carrera en seguridad de TI.

- Es la mejor certificación para los puestos de trabajo de ciberseguridad de nivel de entrada.
- La certificación CompTIA Security+ está destinada a estos puestos de trabajo: administrador del sistema, administrador de red, administrador de seguridad, probador de penetración o auditor de TI junior, especialista de seguridad, asesor de seguridad e ingeniero de seguridad.
- La experiencia recomendada es tener CompTIA Network+ y dos años de experiencia en administración de TI centrada en la seguridad.

Puede encontrar más información sobre CompTIA Security+.

(<https://www.comptia.org/certifications/security>)

CompTIA Cybersecurity Analyst (CySA+)



- Esta es una certificación del personal de TI que aplica la analítica del comportamiento de redes y dispositivos para evitar, detectar y combatir amenazas de ciberseguridad.
- CySA+ es la certificación de analista de seguridad más actualizada que cubre amenazas persistentes avanzadas en un entorno de ciberseguridad posterior a 2014.
- La certificación CompTIA CySA+ está destinada a estos tres puestos de trabajo: analista de seguridad TI, analista SOC, analista de vulnerabilidades, especialista en ciberseguridad, analista de información de amenazas, ingeniero de seguridad, analista de ciberseguridad y supervisor de seguridad.
- La experiencia recomendada es tener Network+, Security+ o conocimientos equivalentes. Un mínimo de 3-4 años de experiencia práctica en seguridad de la información o relacionada. Aunque no hay ningún requisito previo, CySA+ debe seguir la certificación CompTIA Security+ o una experiencia equivalente, y tiene un foco técnico y práctico.

Puede encontrar más información sobre CompTIA Cybersecurity Analyst (CySA+).

(<https://www.comptia.org/certifications/cybersecurity-analyst>) b

Biblioteca de Infraestructura de TI (ITIL)



- ITIL es una infraestructura aceptada globalmente de prácticas recomendadas de Gestión de servicios de TI (ITSM).
- El esquema de certificación ITIL proporciona un enfoque modular a la infraestructura ITIL. Hay una estructura por capas de varias certificaciones, por ejemplo, del nivel básico al nivel maestro. Esto ofrece flexibilidad relacionada con las distintas disciplinas y áreas de ITIL, y la capacidad de dedicar estudios a áreas clave de interés.

Preferencias sobre cookies

Hay certificaciones de nivel de entrada que solo son relevantes si un determinado puesto las requiere.

Puede encontrar más información sobre la certificación Biblioteca de Infraestructura de TI (ITIL). (<https://www.axelos.com/certifications/itil-service-management>)

Hacker ético certificado (CEH)



- Un Hacker ético certificado es un profesional cualificado que conoce y sabe cómo buscar puntos débiles y vulnerabilidades en los sistemas de destino, y utiliza los mismos conocimientos y herramientas que un hacker malicioso, pero de manera legal y legítima para evaluar la infraestructura de seguridad de los sistemas de destino.
- La credencial CEH certifica a las personas en la disciplina de seguridad de red específica de Hackeo ético desde una perspectiva independiente del proveedor.
- Este programa respetado y de confianza puede beneficiar a cualquier profesional de ciberseguridad.

Puede encontrar más información sobre el Hacker ético certificado (CEH). (<https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/>)

Profesional de seguridad de sistemas de información certificado (CISSP)



- La certificación CISSP valida las habilidades y experiencia de un profesional para diseñar, implementar y gestionar de manera eficaz un programa de ciberseguridad.
- Está especialmente indicada para profesionales de seguridad, gestores y directivos con experiencia interesados en proporcionar sus conocimientos en una amplia variedad de principios y prácticas de seguridad, por ejemplo, en los siguientes puestos: director de seguridad de la información, director de seguridad, analista de seguridad, arquitecto de seguridad, asesor de seguridad, etc.
- **Nota:** se requieren cinco años de experiencia.

Puede encontrar más información sobre el Profesional de seguridad de sistemas de información certificado (CISSP). (<https://www.isc2.org/Certifications/CISSP>)

Gestor certificado de seguridad de la información (CISM)



-

ISACA ofrece la certificación CISM para que los profesionales demuestren su experiencia probada en distintas facetas, y su capacidad de entender problemas de gestión de seguridad complejos y de difícil solución para las empresas.

- Recientes estudios independientes clasifican constantemente CISM como una de las certificaciones de TI mejor pagadas y más buscadas.
- **Nota:** se requieren cinco años de experiencia.

Puede encontrar más información sobre el Gestor certificado de seguridad de la información (CISM). (<https://www.isaca.org/credentialing/cism>)

Permiso de seguridad

Además de las certificaciones, muchos puestos en organizaciones y agencias gubernamentales que trabajan en el sector público pueden requerir que las personas pasen un conjunto de verificaciones de antecedentes. Estas varían según el país y tienen distinto nivel dependiendo de la confidencialidad del puesto de trabajo. Si se requiere un permiso de seguridad, generalmente se resaltarán en la oferta de empleo.

En algunos países, si una persona ya posee un permiso de seguridad emitido previamente, el proceso de nueva solicitud se simplifica ligeramente. O al menos la persona es más probable que pase las verificaciones necesarias. Debido a los costes relacionados con determinadas verificaciones y la reticencia de las personas o la incapacidad de verificar sus antecedentes, hay una prima de salario medible para aquellos con permisos de seguridad.

Recursos útiles y guía de inicio

10 Minutos

Esperamos que este curso le resulte informativo, interesante y educativo. Puede ser una parte de su recorrido por la seguridad cibernética. Esta lección le proporcionará inspiración para futuras exploraciones.

Recursos útiles

Primero, aquí tiene algunos recursos que puede consultar, marcar y tener en cuenta si desea investigar más sobre la seguridad cibernética y estar en contacto con los desarrollos prácticos más recientes. Se trata de una lista supervisada. Hay muchas organizaciones y sitios web para revisar, en función de sus intereses.

Nota: Estos recursos son sitios web reconocidos por el sector, en inglés. Puede consultar estos recursos y Preferencias sobre cookies

cualquier otro que sea útil y pueda descubrir en su idioma.

Organizaciones de ciberseguridad

- El **NIST (National Institute of Standards and Technology)** (<https://www.nist.gov/topics/cybersecurity>) es una unidad del Departamento de Comercio de los EE.UU que hace el mantenimiento de los estándares de medición. Tiene un programa para implementar la seguridad cibernética práctica y la privacidad a través de la participación y la aplicación efectiva de estándares y prácticas recomendadas necesarias para que los EE.UU. adopten prestaciones de seguridad cibernética.
- El **NCSC (National Cyber Security Centre)** (<https://www.ncsc.gov.uk>) es la máxima autoridad del Reino Unido en cuestiones de ciberseguridad. El sitio web contiene muchos documentos de asesoramiento y orientación para sectores específicos.
- La **OWASP (Open Web Application Security Project)** (https://www.owasp.org/index.php/Main_Page) es una organización benéfica internacional sin fines de lucro, enfocada a la mejora de la seguridad del software. Proporciona una fuente neutral de información sobre prácticas recomendadas, y actúa también como organismo activo que defiende los estándares abiertos.
- La **ISSA (Information Systems Security Association)** (<https://www.issa.org/>) es una organización sin fines de lucro centrada en la seguridad de la información. Está comprometida con la promoción de un mundo digital seguro. La mayoría de los recursos de la ISSA son para miembros. Puede echar un vistazo a las ventajas derivadas de convertirse en miembro y ver si existen centros locales cerca de usted. Busque si hay un centro local cerca de usted y eche un vistazo al sitio web del centro.
- La **WiCyS (Women in Cybersecurity)** (<https://www.wicys.org/about>) es una organización sin fines de lucro con sede en los Estados Unidos para miembros que se dedica a reunir a las mujeres del sector de la ciberseguridad de ámbitos diversos, como el académico, la investigación y la industria, para compartir conocimientos, experiencias, contactos y tutorización.
- El **FIRST (Forum of Incident Response and Security Teams)** (<https://www.first.org/>) es un foro global y un reconocido líder mundial en respuesta a incidencias. FIRST proporciona documentos actualizados de prácticas recomendadas, publicaciones, etc.

Publicaciones y plataformas de ciberseguridad

- **Cybersecurity Ventures** (<https://cybersecurityventures.com/>) es responsable de **Cybercrime Magazine**. Cybersecurity Ventures es el investigador líder mundial de la economía cibernética global y una fuente de confianza de datos, cifras y estadísticas de seguridad cibernética. Proporciona los últimos datos del mercado de cibereconomía, ideas y predicciones innovadoras a una audiencia global de profesionales de ciberseguridad.
- **Security Intelligence** (<https://securityintelligence.com/>) es un sitio que proporciona análisis e información de todo el sector de la ciberseguridad. Encontrará las últimas noticias, investigaciones, podcasts, etc.
- **SC Media** (<https://www.scmagazine.com/about-sc-media/>) comparte orientación y conocimiento de expertos de la industria, características detalladas y noticias actuales, así como revisiones de productos independientes

Preferencias sobre cookies

en varias formas de contenido en asociación con y para ejecutivos de seguridad de la información de alto nivel y sus equipos técnicos.

- **Wired Threat Level** (<https://www.wired.com/category/threatlevel/>) es una serie de artículos de seguridad cibernética de la revista **Wired** (<https://www.wired.com/>).
- **IBM X-Force Exchange** (<https://exchange.xforce.ibmcloud.com/>) es una plataforma de inteligencia de amenazas públicas que asesora en relación con alertas sobre nuevos ataques, vulnerabilidades y campañas. Proporciona una vista geográfica en tiempo real de la actividad de amenazas en directo. Puede buscar o enviar un archivo para analizar, mantener sus propias investigaciones y ver lo que otros comparten.

Blogs de ciberseguridad

- **Krebs on Security** (<https://krebsonsecurity.com/>) es una colección de blogs sobre seguridad informática y delitos cibernéticos creados por Brian Krebs, periodista estadounidense de investigación.
- **Graham Cluley** (<https://www.grahamcluley.com/>) es una colección de blogs con noticias actuales, opiniones y consejos sobre seguridad informática escritos por Graham Cluley, conferenciante y analista independiente británico.
- El blog **Recorded Future** (<https://www.recordedfuture.com/blog/>) proporciona análisis de inteligencia de amenazas cibernéticas, perspectivas de la industria, novedades de la empresa Recorded Future, etc.

Introducción al sector

¿Qué viene a continuación? ¿Qué puede hacer para iniciarse en la industria de la ciberseguridad? Dependiendo de su interés y experiencia, si está considerando la posibilidad de iniciar una carrera en ciberseguridad, puede explorar estas diferentes opciones.

- **¡Amplíe sus conocimientos!** Cuanto más se familiarice con la ciberseguridad, más posibilidades tendrá para explorar. Intente hacer un seguimiento de sus intereses y descubra nuevos roles y sectores que quizás no haya tenido en cuenta antes.
- **¡Siga aprendiendo!** Este es el principio de su experiencia de aprendizaje. Puede seguir aprendiendo buscando en línea temas adicionales sobre seguridad cibernética y tomando en consideración algunos de estos recursos de formación.
 - El **CyboC (Cyber Security Body Of Knowledge)** (<https://www.cybok.org/>) tiene como objetivo ser un organismo integral de conocimiento para informar y apuntalar la formación y la capacitación profesional para el sector de seguridad cibernética. Sirve como una excelente guía de referencia para temas de seguridad.
 - El **SANS Institute** (<https://www.sans.org/>) es una institución cooperativa de investigación y formación. La base de SANS es un gran número de profesionales de seguridad en diversas organizaciones globales, desde corporaciones hasta universidades, que trabajan juntas para ayudar a toda la comunidad de seguridad de la información. SANS es una fuente de confianza de dimensiones importantes para la **formación en seguridad de la información** (<https://www.sans.org/find-training/>) y la **certificación de seguridad** (<https://www.giac.org/>).

•

Preferencias sobre cookies

La **IBM Security Learning Academy** (<https://www.securitylearningacademy.com/>) proporciona formación técnica gratuita sobre los productos de IBM Security. Puede explorar el **catálogo de cursos** (<https://www.securitylearningacademy.com/local/navigator/index.php>) y diseñar su propio currículum al inscribirse en ellos.

- Tenga en cuenta que deberá crear una cuenta con un ID de IBM.
- El **Instituto Nacional de Estándares y Tecnología (NIST)** (<https://www.nist.gov/itl/applied-cybersecurity/nice/resources/online-learning-content>) ofrece contenido para el aprendizaje sobre ciberseguridad en línea gratuito o de bajo coste a estudiantes y profesionales.
- ¡Y esté atento a las nuevas ofertas formativas de este programa!
- **¡Explore nuevas oportunidades!** Si está buscando empleo, puede comenzar a explorar el mercado de trabajo. Consulte las ofertas de trabajo para identificar las ofertas y calificaciones más habituales. Hágase una idea de qué trabajos podrían resultarle atractivos en el futuro y trabaje para cumplir sus requisitos.