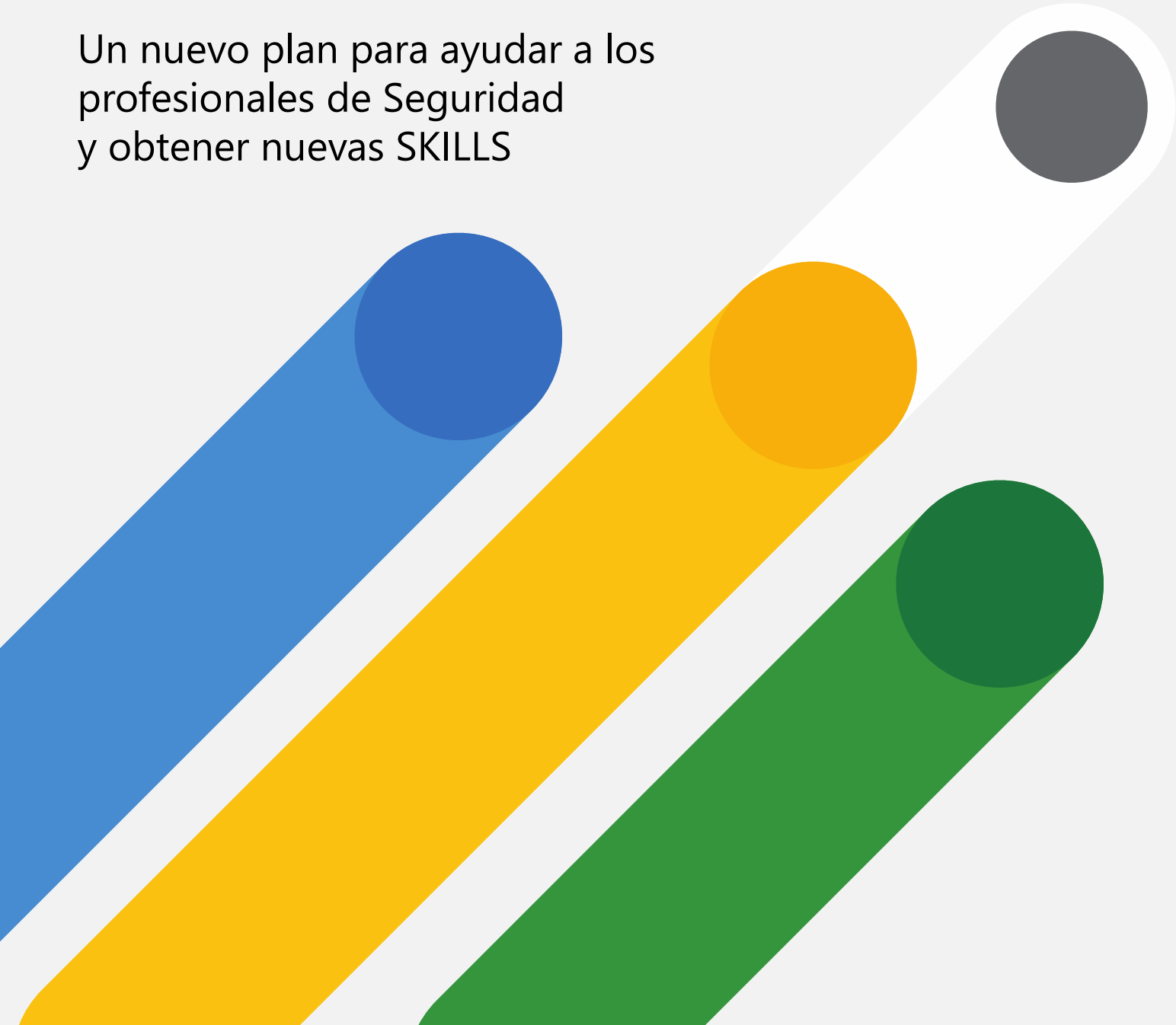
Consulting & Training

Microsoft Security

Plan de ayuda para la mejora de la seguridad

Un nuevo plan para ayudar a los profesionales de Seguridad y obtener nuevas SKILLS



Introducción:
El reto de la ciberseguridad y nuevas oportunidades

Las últimas noticias acerca de ciberataques de tipo ransomware, han aumentado en un 27%. Además, actualmente estamos viviendo en un contexto de ciberguerra internacional debido al conflicto de Ucrania, siendo necesario:

Aumentar el número de profesionales expertos en ciberseguridad y con aptitudes para defender y asegurar los sistemas más críticos. En este momento no contamos con profesionales suficientes.

Demanda de profesionales

Estos son los datos: entre 2020 y 2025 se generarán 7 millones de trabajos en el sector de la seguridad y privacidad en todo el mundo [1].

7 000 000

de nuevos trabajos en ciberseguridad en todo el mundo, pero solo 4,2 millones de candidatos con las aptitudes necesarias

Comparemos esa cifra con los 4,2 millones de especialistas de seguridad que estimamos hay disponibles.

El resultado es un vacío de 2,8 millones de puestos de trabajo[2].

Además, se espera que el número de trabajos del sector de la ciberseguridad aumente en más del doble entre ahora y 2025.

2x Más del doble de trabajos en ciberseguridad para 2025

El déficit de especialistas en ciberseguridad cualificados no para de expandirse.

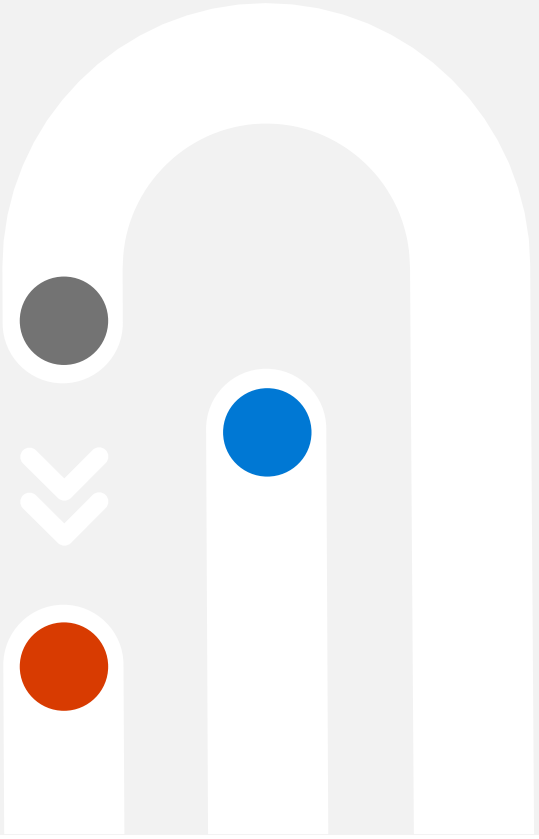
Esta falta de aptitudes ya supone un coste de dinero.

71 % de los empresarios ha sufrido daños por el déficit de cibertalentos[3]

Estos son trabajos de futuro con algunos de los mejores salarios del sector de la tecnología

Algunos serán trabajos a tiempo completo en ciberseguridad, como en los puestos de director jefe de Seguridad de la Información, o CISO.

Otros puestos combinarán la ciberseguridad con otras funciones de TI.



[1] Industry Skills Report2021, Coursera
[2] A Resilient Cybersecurity Profession Charts the Path Forward, (ISC)2 Cybersecurity Workforce Study, 2021, (ISC)2, 2021
[3] 3 Key Statistics from Global Cybersecurity Outlook 2022, Swiss Cyber Institute, 10 de marzo de 2022

Microsoft Security

Mejora tus skills en seguridad:

Los pasos para ampliar tus skills en seguridad en la nube, cumplimiento e identidad

Para llevar sus conocimientos al siguiente nivel y ocupar uno de esos puestos vacantes, será necesario un plan de formación teórica y practica.

Aquí encontrará 3 pasos para comenzar su recorrido hacia el aprendizaje de las aptitudes de seguridad, cumplimiento e identidad que necesita.

Además, con la ayuda de Microsoft Learn, dispondrá de la estructura y los recursos necesarios para ayudarle a usted y a su equipo a medida que amplíen sus aptitudes técnicas.

1

Familiarícese con el mapa de aptitudes y sus hitos

- Puede encontrar recorridos de aprendizaje de aptitudes recomendados y las pistas para alumnos en el manual Recorrido de seguridad, cumplimiento e identidad.

2

Identifique las aptitudes, de las básicas a las más avanzadas, que necesita

- Ajuste su ruta de aprendizaje de aptitudes con la dirección planeada de su carrera y sus siguientes pasos.
- Verá que cada ruta está diseñada para ayudar a decidir cuál debe ser su punto de partida y qué pasos se deben dar en función de su rol o sus proyectos específicos.

3

Reúna sus recursos

- Cuando haya decidido qué ruta es la más adecuada, encontrará cursos, oportunidades de aprendizaje y otra información importante que ayudará a su equipo a alcanzar el éxito.

Microsoft Security

Sus opciones de certificación de seguridad, cumplimiento e identidad

1

Microsoft Certified: Fundamentos de seguridad, cumplimiento e identidad

Para estudiantes, usuarios profesionales o profesionales de TI

- Esta certificación de Fundamentos le ofrece una amplia variedad de temas relacionados con el sector creciente de la ciberseguridad.
- Se trata de un primer paso hacia la certificación Advanced Role-Based de operaciones de seguridad, administración de identidades y accesos y protección de la información.

2

Microsoft Certified: Security Operations Analyst Associate

- Colabore con las partes interesadas organizativas para proteger los sistemas tecnológicos de la organización.
- Ayude a reducir los riesgos para la organización al corregir rápidamente los ataques activos en el entorno, asesorar sobre mejoras en las prácticas de protección contra amenazas y dirigir las infracciones de las directivas organizativas a las partes interesadas apropiadas..

3

Microsoft Certified: Identity and Access Administrator Associate

- Obtenga las aptitudes para diseñar, implementar y operar los sistemas de administración de identidades y accesos de una organización mediante Azure Active Directory.
- Administre tareas como, por ejemplo, proporcionar acceso con autenticación y autorización seguras a las aplicaciones empresariales.
- También aprenderá aptitudes para la solución de problemas, supervisión y creación de informes para el entorno de identidades y accesos.

4

Microsoft Certified: Information Protection Administrator Associate

- Esta certificación ofrece la preparación para afrontar la responsabilidad de convertir los requisitos y controles de cumplimiento normativo en una implementación técnica.
- Recibirá preparación para asistir a los propietarios del control de la organización para conseguir y conservar el cumplimiento e implementar tecnologías compatibles con los controles y directivas necesarios para satisfacer los requisitos normativos de su organización.

Ver certificaciones de seguridad

https://bit.ly/3as9XEr

Microsoft Security

Sus opciones de certificación de seguridad, cumplimiento e identidad

5

Microsoft Certified: Azure Security Engineer Associate

- Administre la posición de seguridad, identifique y solucione las vulnerabilidades, lleve a cabo el modelado de amenazas, implemente la protección contra amenazas y responda a las escalaciones de los incidentes de seguridad.
- Este curso le ofrece las herramientas para administrar la seguridad y los accesos, implementar la protección de la plataforma y administrar sus operaciones de seguridad.

6

Microsoft Certified: Administrador asociado de seguridad de Microsoft 365

- Aprenda a proteger de manera proactiva los entornos de Microsoft 365 Enterprise e híbridos, a implementar y administrar las soluciones de seguridad y cumplimiento, a responder contra las amenazas y a aplicar el gobierno de datos.
- Administre las características de gobierno y cumplimiento dentro de Microsoft 365.
- Contará con la preparación para implementar y administrar la identidad, los accesos, además de la protección contra amenazas y la protección de la información.

Ver certificaciones de seguridad

https://bit.ly/3as9XEr

Microsoft Security

Security, Compliance, and Identity

SC-900: Microsoft Security, Compliance, and Identity Fundamentals

Este curso proporciona conocimientos de nivel básico sobre los conceptos de seguridad, cumplimiento e identidad y las soluciones de Microsoft relacionadas basadas en la nube.

• Conceptos básicos de seguridad, cumplimiento e identidad
• Funcionalidades de las soluciones de administración de identidades y acceso de Microsoft
• Soluciones de seguridad de Microsoft
• Administración de cumplimiento en Microsoft

Más información >

AZ-500: Microsoft Azure Security Technologies

Este curso proporciona a los profesionales de seguridad de TI el conocimiento y las habilidades necesarias para implementar controles de seguridad.

• Estrategias de gobierno empresarial que incluyen control de acceso basado en roles, políticas de Azure y bloqueos de recursos.
• Implementar una infraestructura de Azure AD que incluya usuarios, grupos y autenticación multifactor.
• Azure AD Identity Protection, incluidas las políticas de riesgo, el acceso condicional y las revisiones de acceso.
• Azure AD Privileged Identity Management, incluidos los roles de Azure AD y los recursos de Azure.

Más información >

MS-500: Microsoft 365 Security Administration

En este curso aprenderá cómo asegurar el acceso de los usuarios a los recursos de su organización.

•Administrar el acceso de usuarios y grupos en Microsoft 365.
•Explicar y administrar Azure Identity Protection.
•Planificar e implementar Azure AD Connect.
•Administrar identidades de usuario sincronizadas.
•Explicar y usar el acceso condicional.
•Describir los vectores de amenazas de ciberataques.

Más información >

cas Consulting & Training

Microsoft Security

Security, Compliance, and Identity

SC-200: Microsoft Security Operations Analyst

Aprenda a investigar y buscar amenazas, respondiendo mediante Microsoft Sentinel, Microsoft Defender for Cloud y Microsoft 365 Defender.

• Microsoft Defender para punto de conexión puede corregir los riesgos de su entorno.
• Administrar un entorno de Microsoft Defender para punto de conexión
•Configurar reglas de reducción para evitar ataques en dispositivos con Windows

Más información >

SC-300: Microsoft Identity and Access Administrator

Este curso proporciona a los profesionales de la identidad y el acceso de TI, junto con los profesionales de la seguridad de TI, los conocimientos y las habilidades necesarias para implementar soluciones de administración de identidades basadas en Microsoft Azure AD, y las tecnologías de identidades conectadas.

• Solución de administración de identidades
• Soluciones de administración de acceso y autenticación
• Administración del acceso para aplicaciones
• Planear e implementar una estrategia de gobernanza de identidad

Más información >

SC-400: Microsoft Information Protection Administrator

En este curso aprenderá cómo asegurar el acceso de los usuarios a los recursos de su organización.

•Administrar el acceso de usuarios y grupos en Microsoft 365.
•Explicar y administrar Azure Identity Protection.
•Planificar e implementar Azure AD Connect.
•Administrar identidades de usuario sincronizadas.
•Explicar y usar el acceso condicional.
•Describir los vectores de amenazas de ciberataques.

Más información >

cas Consulting & Training

Microsoft Security