Microsoft Security

¿Por qué es necesario el aprendizaje de seguridad, cumplimiento e identidad?

Las amenazas no paran de evolucionar, por lo que la protección debe hacerlo también.

Aunque la esencia de los negocios y del trabajo ha evolucionado, las herramientas de seguridad convencionales no han sabido adaptarse a los cambios.

Esto ocurre mientras el coste de las vulneraciones sigue aumentando.

Se espera que se generen 7 millones de nuevos puestos de trabajo en el sector de la ciberseguridad en todo el mundo de aquí a 2025, pero solo contaremos con 4,2 millones de candidatos con las aptitudes necesarias. Esto genera un vacío de 2,8 millones puestos de trabajo vacantes.[1]

a. Conseguir la certificación es una ventaja notable

Más allá de que el 23 % de los especialistas en tecnología con certificación de Microsoft informan de que disfrutan de un aumento salarial que alcanza, en algunos casos, el 20 %.[2]

El aprendizaje y la certificación de seguridad, cumplimiento e identidad aumentan el valor de los alumnos considerablemente.

a. El 36 % de los profesionales de TI afirman que la certificación los ayudó a realizar tareas complejas con mayor confianza.

b. El 35 % de los profesionales de TI declaran que su influencia durante la implementación de la nube ha aumentado en comparación con la de otros compañeros de departamentos de otras tecnologías.[3]

En otras palabras, con las certificaciones de seguridad, cumplimiento e identidad, los empleados consiguen aportar más valor y recibir mejores recompensas por sus contribuciones.

¿Cómo puedo conseguir las certificaciones de seguridad, cumplimiento e identidad?

Hay dos tipos de cursos de seguridad, cumplimiento e identidad de Microsoft

Cursos de Fundamentos

a. Ayudan a obtener aptitudes sobre roles laborales del sector

b. Están dirigidos a un público amplio de diferentes segmentos de mercado

c. Básicos: no requieren tener experiencia en el área

d. Combinan conceptos teóricos y aprendizajes aplicados sobre las tecnologías de Microsoft

Cursos Role-Based

a. Se centran en aptitudes de seguridad necesarias para un trabajo concreto

Se basan en los roles de trabajo de la industria para personas que están interesadas, en transición, o que ya están en el rol laboral específico

Varios niveles de experiencia: Associate y Expert

Ofrecen conocimientos técnicos para diseñar, implementar y administrar soluciones de Microsoft

Se centran en el aprendizaje aplicado y práctico de las tecnologías de Microsoft

[1] Fuente: Microsoft launches initiative to help 25 million people worldwide acquire the digital skills needed in a COVID-19 economy, Brad Smith, Microsoft Official Blog, 20 de junio de 2020

[2] Fuente: Resolve to be a “learn it all” with new Azure Certifications, Microsoft Developer Blog, diciembre de 2018; Mike Lapierre, David Lipien, Leonel Mora, Doug Owens

[3] Microsoft Sales Training—Security, Compliance, and Identity Solution Area, Microsoft, 29 de junio de 2021

Microsoft Security

¿Qué aptitudes podría conseguir gracias a las certificaciones de seguridad, cumplimiento e identidad?

Los cursos de seguridad, cumplimiento e identidad tratan cuatro áreas de la protección

Administración de identidades y accesos

a. Proteja el acceso en un mundo conectado

b. Ofrezca los permisos de acceso adecuados a las personas correspondientes en los momentos necesarios

c. Incluye lo siguiente:

- Inicio de sesión único y autoservicio de restablecimiento de contraseña
- Autenticación multifactor y autenticación sin contraseña
- Acceso continuo
- Privileged Identity Management
- Identity Governance
- Active Directory
- Administración de aplicaciones móviles
- Administración de dispositivos móviles

Protección contra amenazas

a. Detenga ataques con Sentinel integrado, automatizado y XDR

b. Consulte informes

c. Además, podrá consultar actividades en directo, como inicios de sesión anómalos

d. Incluye lo siguiente:

- Detección y respuesta de puntos de conexión
- Plataformas de protección de puntos de conexión
- Herramientas de análisis forense
- Sistemas de prevención de intrusiones
- Administración de vulnerabilidades frente a amenazas
- Protección contra suplantación de identidad (anti-phishing)
- Análisis de comportamiento de usuarios y entidades
- Fuentes de inteligencia sobre amenazas
- Aislamiento de aplicaciones y navegadores
- Espacios aislados de archivos adjuntos
- Controles de aplicaciones

Administrador

a. Proteja la información confidencial y administre los riesgos internos con inteligencia

b. Clasifique datos y documente quién los usa, cuándo y cómo

c. Realice un seguimiento para garantizar que los datos se manipulan de manera adecuada

d. Incluye lo siguiente:

- Descubrimiento y clasificaciones de datos
- Prevención de pérdida de datos
- Administración de riesgos internos
- Seguridad de base de datos
- Cifrado de información y mensajería
- Cifrado de dispositivos
- Almacenamiento en la nube cifrado
- Administración de secretos

Seguridad en la nube

a. Protección de recursos multinube

b. Incluye lo siguiente:

- Agentes de seguridad de acceso a la nube
- Plataformas de protección de cargas de trabajo en la nube
- Administración de la posición de seguridad en la nube

Más información

www.ulearn.edu.uy
Info@ulearn.edu.uy
O Whatsapp 099550100