TIC

TALENTO TECH

**Integrador**
Intermedio

# MAPA DE RUTA

## MISIÓN 1

Curso: Ciberseguridad

## Objetivo de la misión

Campista, en esta primera misión aprenderás sobre la configuración de un entorno de red segura, utilizando protocolos criptográficos, técnicas criptográficas en reposo y en tránsito; despliegue de operaciones de filtrado a partir de cortafuegos y sistemas de detección de intrusiones, así como la definición de políticas de ciberseguridad basadas en estas estrategias.

# HABILIDADES DIGITALES

01

**Entender y desplegar protocolos seguros:** Conocimiento profundo de los protocolos de seguridad, tales como HTTPS, SSL/TLS, IPsec, SSH, entre otros, y la capacidad de implementarlos correctamente para proteger la comunicación y los datos en tránsito.

02

**Configurar servicios básicos de filtrado y detección de intrusiones:** Configura y administra sistemas de filtrado, como firewalls, y sistemas de detección de intrusiones (IDS) y prevención de intrusiones (IPS). Esto incluye la creación de reglas de filtrado de tráfico, la detección de actividades sospechosas y la respuesta a posibles amenazas.

# Competencias

01

**Diseñar arquitecturas de redes seguras:** Planificar y diseñar infraestructuras de red que incorporen principios de seguridad desde el inicio. Esto incluye la segmentación de redes, el uso de zonas de desmilitarización (DMZ), la implementación de controles de acceso y otras medidas de protección.

02

**Configurar y administrar firewalls y VPNs:** Instalar, configurar y gestionar firewalls y redes privadas virtuales (VPNs) para proteger los perímetros de la red y asegurar la comunicación segura entre distintas ubicaciones y usuarios remotos.

03

**Aplicar técnicas de seguridad y reconocer la norma ISO-27001:** Conocer y la aplicar diversas técnicas de seguridad, así como el entendimiento y la implementación de los requisitos de la norma ISO/IEC 27001, que establece un marco para la gestión de la seguridad de la información.

## Contenidos

### Tema 1: Arquitectura de Redes Seguras

*Diseño de Arquitecturas de Redes Seguras*

01

- Principios de diseño (defensa en profundidad, separación de funciones).
- Segmentación de redes y zonas de seguridad.
- Implementación de redes perimetrales y DMZ.
- Evaluación de necesidades de seguridad en redes (análisis de tráfico).

*Herramientas y Tecnologías para Redes Seguras*

- Sistemas de detección y prevención de intrusiones (IDS/IPS).
- Uso de VPNs para conexiones seguras (protocolos, tipos).
- Técnicas de cifrado de datos en tránsito (SSL, TLS).
- Monitoreo y análisis de logs de seguridad.

02

### Tema 2: Configuración de Firewalls y VPNs

*Fundamentos de Firewalls*

01

- Tipos de firewalls (de red, de host, de aplicación).
- Configuración básica y avanzada de firewalls.
- Reglas y políticas de filtrado de tráfico.
- Monitoreo y mantenimiento de firewalls (logs, alertas).

*Fundamentos de VPNs*

- Tipos de VPNs (site-to-site, remote access).
- Protocolos de VPN (IPsec, SSL/TLS).
- Configuración y gestión de VPNs en entornos empresariales.
- Pruebas de conexión y resolución de problemas.

02

### Tema 3: Normas y Técnicas de Seguridad de la Información

*Confidencialidad, Integridad y Disponibilidad de la Información*

01

- Técnicas de aseguramiento de la información (cifrado, control de acceso).
- Protección de datos en reposo y en tránsito.
- Gestión de identidades y accesos (IAM).