

Curso **Fortinet NSE4 BootCamp**

Plan de Estudio



6C



**COMUNICACIÓN
INTEGRAL**
Haciendo futuro con ideas.

Descripción

LEl Curso Fortinet NSE4 BootCamp está diseñado para formar profesionales altamente competentes en la implementación, configuración y administración de soluciones avanzadas de seguridad de red utilizando dispositivos FortiGate, bajo el sistema operativo FortiOS 7.2.

Este programa ofrece una experiencia intensiva y práctica, orientada a dominar las herramientas y metodologías necesarias para proteger infraestructuras tecnológicas empresariales y entornos de Proveedores de Servicios de Seguridad Gestionada (MSSP).

A través de una combinación de sesiones teórico-prácticas, laboratorios técnicos y simulaciones reales, los participantes desarrollarán la capacidad de diseñar entornos de red seguros, aplicar políticas de seguridad, gestionar VPNs, realizar diagnósticos avanzados y responder ante incidentes de ciberseguridad.

El curso prepara de manera directa para la certificación internacional Fortinet NSE 4 – FortiOS 7.2, reconocimiento que valida el dominio profesional en la gestión, monitoreo y operación de dispositivos FortiGate, respaldando la capacidad del participante para proteger redes empresariales frente a amenazas complejas y dinámicas.





Dirigido a:

- Profesionales de redes, seguridad informática y ciberseguridad que buscan especializarse en el uso de dispositivos Fortinet FortiGate.
- Administradores de sistemas y especialistas en infraestructuras tecnológicas empresariales que gestionan entornos de alta disponibilidad y seguridad.
- Consultores y técnicos que laboran en empresas de telecomunicaciones o Proveedores de Servicios de Seguridad Gestionada (MSSP).
- Personal de TI responsable de la configuración, mantenimiento y supervisión de redes seguras en instituciones públicas o privadas.
- Candidatos que desean obtener la certificación internacional Fortinet NSE 4, fortaleciendo su perfil profesional y ampliando sus oportunidades laborales en el ámbito global.





¿Qué aprenderás?

- Implementar y configurar redes seguras avanzadas mediante dispositivos FortiGate.
- Gestionar infraestructuras con seguridad redundante y control de acceso centralizado.
- Configurar y administrar VPNs IPsec de sitio a sitio para conexiones seguras entre redes.
- Implementar estrategias de ciberseguridad que incluyan proxy web, filtrado de contenido y políticas de protección de datos.
- Integrar autenticación e inicio de sesión único (SSO) para usuarios en redes empresariales.
- Diagnosticar y resolver problemas de seguridad y conectividad en entornos empresariales complejos.
- Prepararse eficazmente para el examen de certificación Fortinet NSE 4 – FortiOS 7.2, con dominio práctico de escenarios operativos y configuraciones reales.

Incluye

- Clases en vivo.
- Videos tutoriales.
- Clases grabadas para repaso
- Recursos descargables.
- Acceso en diferentes dispositivos.
- Actividades para desarrollar habilidades.
- Autoevaluación de habilidades.
- Tutores online para resolver tus dudas.
- Certificado de participación.

¿Qué necesitas?

- Computador o tablet.
- Acceso a internet.

Contenido

Unidad I: Introducción a la certificación y al Fortinet FortiGate

- Introducción a la certificación y al dispositivo Fortinet FortiGate: arquitectura, funcionalidades, modos de operación.
- Configuración inicial del FortiGate: interfaces, zonas, administración, licencias, registro.

Unidad II: Arquitectura de Seguridad Avanzada y Fortinet Security Fabric

Arquitectura de Seguridad Avanzada

- Concepto de Fortinet Security Fabric y sus principales ventajas.
- Interconectan los diferentes componentes de la infraestructura de seguridad.
- Beneficios de la visibilidad y control centralizado en un entorno corporativo.



Segmentación, VDOMs y Alta Disponibilidad

- Configurar segmentación de red para aumentar la seguridad y el control.
- Funcionamiento de los VDOMs y su aplicación en entornos multi-tenant.
- Escenarios básicos de Alta Disponibilidad para asegurar la continuidad operativa.

Unidad III: Políticas de Firewall y Reglas de Inspección

Políticas de Firewall

- Políticas de firewall para controlar el tráfico de red.
- Configurar reglas de direccionamiento y aplicar inspecciones básicas.
- La efectividad de las reglas aplicadas y realizar ajustes según las necesidades de la organización.

Inspección de Contenido y Protección Avanzada

- Implemento de políticas de filtrado web y control de aplicaciones para gestionar el uso de recursos.
- Configurar mecanismos de detección de malware y amenazas mediante antivirus.
- Ajuste y configuraciones de IPS/IDS y protección DoS para mitigar riesgos de intrusión y ataques de saturación.

Unidad IV: Fundamentos de NAT

Fundamento de NAT

- Qué es NAT y su importancia en la administración de redes
- Diferencia y los principales tipos de NAT y sus aplicaciones.
- Escenarios en los que NAT resulta imprescindible para la seguridad y conectividad.

Configuración de NAT en FortiGate

- Configuración y reglas de NAT en FortiGate para distintos escenarios de red.
- Implementación de políticas de enmascaramiento para proteger la red interna.
- Verificación y validar la conectividad después de aplicar configuraciones de NAT.



Unidad V: Métodos de Autenticación e Integración con AD

- Principales métodos de autenticación en FortiGate.
- Integración de la autenticación de usuarios con Active Directory.
- Implementación FSSO para simplificar la gestión de usuarios en entornos corporativos.

Acceso Seguro mediante Portal Cautivo y SSL VPN

- Configuración de un portal cautivo para la autenticación de usuarios en la red.
- Implementación una SSL VPN en FortiGate para acceso remoto seguro.
- Validación del acceso y la seguridad en escenarios de usuarios internos y externos.

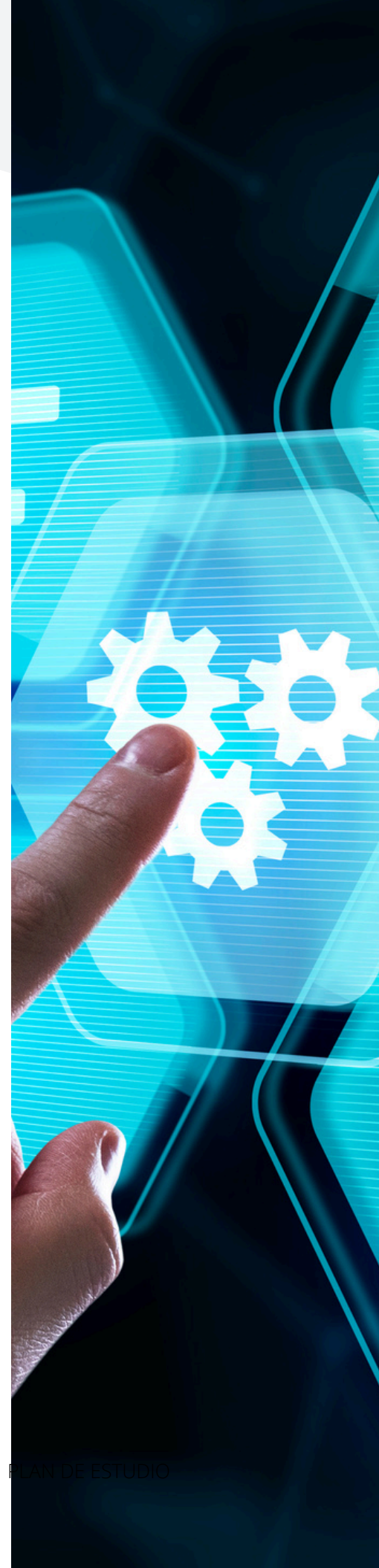
Unidad VI - A: Gestión de Logs, Alertas y Trazas

Gestión de Logs

- Habilitación y gestión logs en FortiGate.
- Configuraciones alertas para la detección temprana de eventos críticos.
- Trazas de red para identificar fallos o comportamientos anómalos.

Herramientas de Supervisión y Diagnóstico en FortiGate

- Utilizar comandos básicos en CLI para diagnóstico de red.
- Supervisar el rendimiento del dispositivo desde la GUI.
- Aplicar técnicas de troubleshooting para resolver incidencias en la infraestructura.



Unidad VII: Fundamentos de Certificados Digitales y Fundamentos de Certificados Digitales

Fundamentos de Certificados Digitales

- Qué es un certificado digital y cómo funciona el estándar X.509.
- El papel de los certificados en la autenticación y el cifrado.
- Escenarios donde los certificados son necesarios para la seguridad de la red.
- Infraestructura de Clave Pública (PKI) y Gestión en FortiGate
- El concepto de PKI y su importancia en la gestión de claves y certificados.
- Configuración de certificados digitales en FortiGate.
- Administración certificados emitidos por autoridades certificadoras para fortalecer la seguridad en comunicaciones y accesos.

Unidad VIII: Diseño de Infraestructura de Red Avanzada

Diseño de Infraestructura de red avanzada

- Los principios de una red en capas y sus beneficios.
- Implementación esquemas de redundancia para garantizar alta disponibilidad.
- Configuración y diferenciación rutas estáticas y dinámicas en FortiGate.

Túneles Seguros y Conectividad VPN

- Configuración de túneles IPsec y SSL en FortiGate.
- Implementación una VPN site-to-site para interconectar diferentes sedes.
- Configuración de una VPN cliente para acceso remoto seguro.



Soluciones empresariales

- Presencial o virtual
- Grupos online 6+ participantes
- InHouse desde 10 participantes
- Contenidos personalizados
- Plataforma interactiva moderna

Modalidad

100% Virtual

Duración

6 semanas
25 horas

Inversión

RD\$25,000.00

Forma de pago

Depósito o transferencia



Transacciones bancarias

Banreservas: Cuenta corriente: 9601879916 a nombre de CI Comunicación Integral, SRL.

RNC: 131805851.

Correo electrónico: ci.comunicacionintegral@gmail.com

**Para completar el proceso de inscripción debes enviar el comprobante de la transacción vía correo electrónico, indicando tu nombre, datos del curso pagado.*

Contacto

Oficina: 809-476-9975

WhatsApp: 829-773-9975

Calle Ana Teresa Paradas No. 10, Mirador Sur, Santo Domingo, República Dominicana.

Certificado

En el **Curso en Fortinet NSE4 BootCamp**, te puedes certificar cuando completes los reportes de actividades y estudios de casos, desarrollo de proyecto que evidencian los conocimientos adquiridos.



