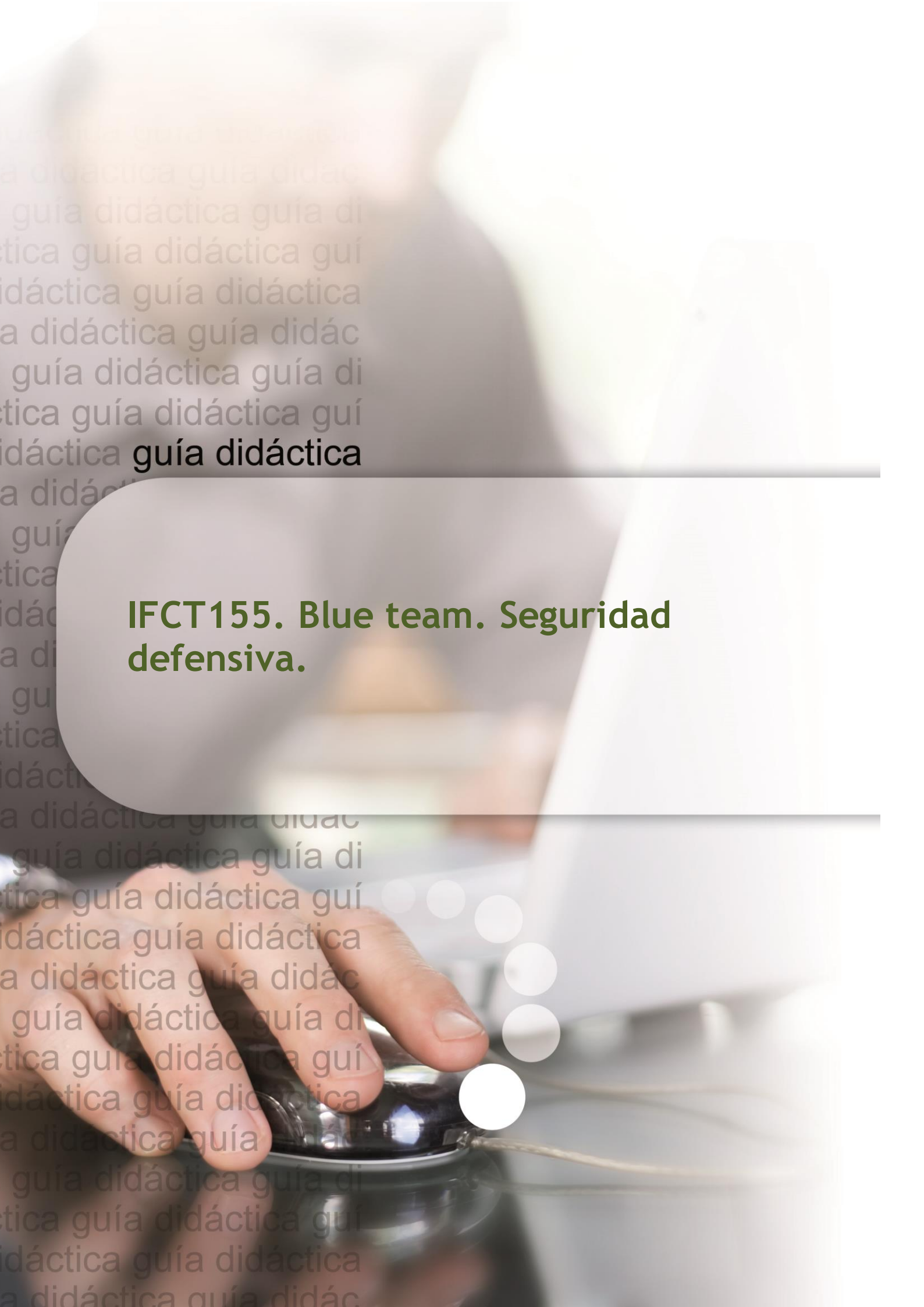

IFCT155. Blue team. Seguridad defensiva.

Objetivo general

- Adquirir las competencias básicas para el desarrollo de una seguridad defensiva en procesos de ciberseguridad.

Objetivos específicos

- Comprender el funcionamiento general de las redes IP en entornos corporativos.
- Identificar servicios, protocolos y equipos que intervienen en la comunicación de red.
- Analizar mecanismos de segmentación, direccionamiento, enrutamiento y traducción de direcciones.
- Aplicar criterios básicos de documentación, inventariado y organización de infraestructuras de red.
- Analizar el despliegue y bastionado de sistemas para reducir la superficie de ataque desde las fases iniciales de implantación.
- Identificar activos, servicios corporativos, dependencias y riesgos asociados a infraestructuras en producción.
- Configurar medidas de protección en sistemas Windows, Linux, redes perimetrales, firewalls y zonas de seguridad.
- Aplicar mecanismos de cifrado, autenticación y securización de servicios para proteger aplicaciones y datos en tránsito.
- Identificar ataques, anomalías e indicadores de compromiso mediante el análisis de registros, tráfico de red y actividad en sistemas.
- Aplicar procedimientos de monitorización, auditoría y respuesta ante incidentes para contener, erradicar y recuperar servicios afectados.
- Diferenciar tecnologías de detección como IDS, IPS, HIDS, NIDS, SIEM y EDR, atendiendo a su ámbito de visibilidad y despliegue.

- Correlacionar eventos procedentes de distintos sistemas para interpretar patrones sospechosos y apoyar la toma de decisiones defensivas.
- Analizar la planificación estratégica de la seguridad corporativa desde una perspectiva alineada con los objetivos de negocio.
- Diseñar políticas, normativas internas y controles de acceso que protejan sistemas, identidades y datos sensibles.
- Aplicar medidas de seguridad en entornos Cloud, servicios SaaS y escenarios de continuidad del negocio.
- Evaluar la evolución de la seguridad mediante métricas, KPIs, revisión de madurez y actualización continua de planes.
- Comprender la estructura, funciones y modelos de operación de un Centro de Operaciones de Seguridad, diferenciando sus componentes humanos, tecnológicos y procedimentales.
- Aplicar criterios de clasificación, priorización y triaje para gestionar alertas de seguridad con menor ruido operativo y mayor coherencia en la respuesta.
- Analizar flujos de trabajo, logs, telemetría e hipótesis de caza para detectar comportamientos anómalos y amenazas que no hayan generado alertas evidentes.
- Evaluar la eficacia operativa del SOC mediante métricas, revisión de procesos, coordinación interdepartamental y mejora continua.

Contenidos

IFCT155. Blue team. Seguridad defensiva	Tiempo estimado
MÓDULO 1: Blue Team. Seguridad defensiva	
Unidad 1: Fundamentos de sistemas y redes IP. 1. Conocimiento de los sistemas y redes IP. 1.1. Redes y direccionamiento IP. 1.2. Servidores IP. 1.3. Creación de zonas en redes privadas. 1.4. Virtualización de servidores. 1.5. Topologías y arquitecturas de red. 1.6. Protocolos esenciales de red (ARP, ICMP y TCP/UDP). 1.7. Introducción al direccionamiento IPv6 y coexistencia con IPv4. 1.8. NAT y técnicas de traducción de direcciones. 1.9. Segmentación y aislamiento mediante VLAN. 1.10. Servicios esenciales de red: DHCP y DNS. 1.11. Enrutamiento básico y configuración de gateways. 1.12. Equipamiento de red: switches, routers y puntos de acceso. 1.13. Documentación, inventariado y mapas de red.	
Cuestionario de autoevaluación UA 01	**30 minutos**
Actividad de Evaluación UA 01	**45 minutos**
Tiempo total de la unidad	**10 horas**
Unidad 2: Despliegue seguro y bastionado de infraestructuras. 1. Análisis del despliegue y bastionado de sistemas. 1.1. Servicios corporativos en producción. 1.2. Creación del firewall. 1.3. Protección de comunicaciones. 2. Evaluación inicial del entorno. 2.1. Identificación de activos y dependencias. 2.2. Análisis de riesgos en sistemas y servicios. 3. Bastionado de sistemas. 3.1. Endurecimiento de sistemas Windows.	

3.2. Endurecimiento de sistemas Linux. 4. Protección perimetral. 4.1. Diseño de arquitecturas de red seguras. 4.2. Segmentación de red y zonas de seguridad. 4.3. Filtrado avanzado y políticas de firewall. 5. Seguridad en servicios y comunicaciones. 5.1. Securización de servicios expuestos a Internet. 5.2. Configuración segura de protocolos y cifrado.	
Cuestionario de autoevaluación UA 02	**30 minutos**
Actividad de Evaluación UA 02	**45 minutos**
Tiempo total de la unidad	**12 horas**
Unidad 3: Detección de amenazas, análisis y respuesta ante incidentes. 1. Detección de ataques y respuestas ante incidencias. 1.1. Análisis y detección de ataques a servidores. 1.2. Monitorización de servicios críticos. 1.3. Herramientas de detección. 1.4. Auditoría informática. 1.5. Respuesta ante incidencias y procedimientos de actuación. 2. Técnicas de detección y análisis. 2.1. Identificación de indicadores de compromiso. 2.2. Análisis de comportamiento anómalo y patrones sospechosos. 2.3. Correlación de eventos mediante plataformas SIEM. 2.4. Análisis de tráfico de red para detección de amenazas. 3. Sistemas y tecnologías de detección. 3.1. IDS/IPS: funcionamiento y despliegue. 3.2. Detección basada en host (HIDS). 3.3. Detección basada en red (NIDS). 3.4. EDR y protección avanzada de endpoints.	
Cuestionario de autoevaluación UA 01	**30 minutos**
Actividad de Evaluación UA 01	**45 minutos**
Tiempo total de la unidad	**11 horas**

Unidad 4: Gestión avanzada de la seguridad en la organización. 1. Planificación estratégica de la seguridad corporativa. 2. Diseño de políticas y normativas internas de seguridad. 3. Gestión de identidades y accesos (IAM). 4. Seguridad en entornos cloud y servicios SaaS. 5. Protección y control de datos sensibles. 6. Gestión de la continuidad del negocio. 6.1. Plan de continuidad de negocio (BCP). 6.2. Plan de recuperación ante desastres (DRP). 7. Supervisión y evolución de la seguridad. 7.1. Definición de métricas y KPIs de ciberseguridad. 7.2. Evaluación periódica del nivel de madurez de la organización. 7.3. Actualización y revisión continua de planes de seguridad.	
Cuestionario de autoevaluación UA 02	**30 minutos**
Actividad de Evaluación UA 02	**45 minutos**
Tiempo total de la unidad	**9 horas**
Unidad 5: Operaciones de seguridad y gestión del SOC. 1. Estructura y funciones de un Centro de Operaciones de Seguridad (SOC). 2. Modelos de SOC: interno, híbrido y externalizado. 3. Gestión de alertas y priorización. 3.1. Clasificación de alertas por criticidad. 3.2. Métodos de triaje y reducción de ruido. 4. Flujos operativos dentro del SOC (workflow). 5. Gestión avanzada de logs y telemetría de seguridad. 6. Técnicas de Threat Hunting. 6.1. Hipótesis de caza y fuentes de información. 6.2. Procedimientos manuales y asistidos. 7. Coordinación con otros equipos (TI, red, legal, dirección). 8. Revisión periódica de la eficacia operativa del SOC.	
Cuestionario de autoevaluación UA 02	**30 minutos**

Actividad de Evaluación UA 02	**45 minutos**
Tiempo total de la unidad	**7 horas**
Examen final	**1 hora**
1 módulo / 5 unidades	**50 horas**