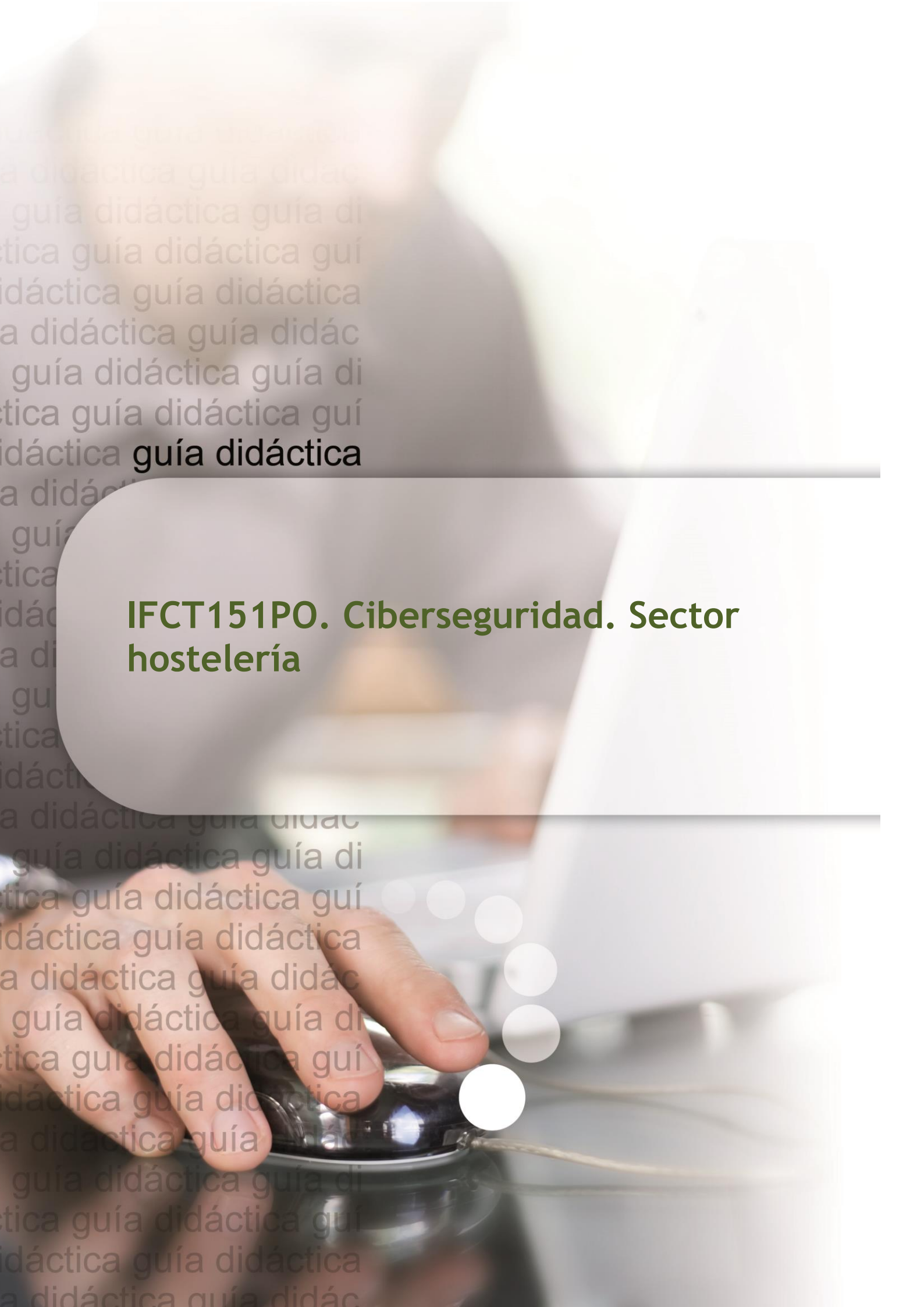

IFCT151PO. Ciberseguridad. Sector hostelería

Objetivos

Objetivo General

- Utilizar el conjunto de herramientas, políticas, conceptos y salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios.

Objetivos Específicos

- Conocer y comprender el valor de la información y de la seguridad informática.
- Estudiar la figura del hacker y del ciberdelincuente.
- Conocer y saber aplicar los principales estándares de la seguridad de la información, así como sus políticas y procedimientos.
- Explicar los diferentes tipos de delitos informáticos.
- Estudiar los tipos de amenazas que reciben los sistemas informáticos.
- Conocer las vulnerabilidades de los sistemas informáticos y de Internet of the Things (IoT).
- Definir la ingeniería social y las técnicas que emplea.
- Profundizar en el conocimiento de los diferentes tipos de programas maliciosos (malware).
- Conocer qué son las credenciales y qué valor tienen dentro de una empresa u organización.
- Estudiar el almacenamiento de credenciales.
- Explicar qué son las credenciales en caché.
- Saber aplicar las contramedidas adecuadas contra los ataques a credenciales.
- Conocer las características de los ataques DoS y DDoS.
- Explicar las diferentes motivaciones que tienen los ciberdelincuentes para realizar los ataques.
- Exponer diferentes ejemplos de víctimas y de ataques.
- Estudiar las contramedidas aplicables a los ataques DoS y DDoS.
- Conocer los riesgos que conlleva utilizar una cámara web (cámara web) y las pautas que se deben seguir para asegurarla.
- Explicar los diferentes tipos de estafas telefónicas.
- Aprender los riesgos asociados al uso de un dispositivo USB.
- Estudiar aspectos relacionados con la seguridad física.

- Conocer los riesgos que conlleva utilizar una cámara web (cámara web) y las pautas que se deben seguir para asegurarla.
- Explicar los diferentes tipos de estafas telefónicas.
- Aprender los riesgos asociados al uso de un dispositivo USB.
- Estudiar aspectos relacionados con la seguridad física.
- Conocer los riesgos que conlleva utilizar una cámara web (cámara web) y las pautas que se deben seguir para asegurarla.
- Explicar los diferentes tipos de estafas telefónicas.
- Aprender los riesgos asociados al uso de un dispositivo USB.
- Estudiar aspectos relacionados con la seguridad física.
- Conocer los riesgos que conlleva utilizar una cámara web (cámara web) y las pautas que se deben seguir para asegurarla.
- Explicar los diferentes tipos de estafas telefónicas.
- Aprender los riesgos asociados al uso de un dispositivo USB.
- Estudiar aspectos relacionados con la seguridad física.

Contenidos

IFCT151PO. Ciberseguridad. Sector hostelería	Tiempo estimado

Unidad 1: Conceptos básicos de ciberseguridad.
• El valor de la información.
• Hackers y ciberdelincuentes.
• Seguridad por defecto.
• Políticas y procedimientos.
  ○ Analizar la situación actual de la empresa.
  ○ Alinear el PDS con la estrategia de la empresa.
  ○ Definir los proyectos que se van a ejecutar.
  ○ Clasificar y priorizar los proyectos.
  ○ Aprobar el PDS.
  ○ Ejecución del PDS.
  ○ Certificación en seguridad.
• Delitos informáticos.
• Código de derecho de ciberseguridad.
	15 horas

Examen UA 01	**30 minutos**
Actividad de Evaluación UA 01	**30 minutos**
Tiempo total de la unidad	**16 horas**

Unidad 2: Amenazas, vulnerabilidades y riesgos.
• Tipos de amenazas.
• Tipos de vulnerabilidades.
  ○ Físicas.
  ○ Naturales.
  ○ De hardware.
  ○ De software.
  ○ De almacenamiento.
  ○ De conexión.
  ○ Humanas.
• Vulnerabilidades de IoT.
• Ingeniería social.
• Malware.
• Virus. Troyanos. Gusanos. Spyware. Ransomware. PUP. Key Loggers. Bots.
  ○ Virus.
  ○ Troyanos.
  ○ Gusanos.
  ○ Spyware.
	21 horas

○ Ransomware. ○ PUP. ○ Key Loggers. ○ Bots.	
Examen UA 02	**30 minutos**
Actividad de Evaluación UA 02	**30 minutos**
Tiempo total de la unidad	**22 horas**
Unidad 3: Ataques a credenciales. • Demostración práctica del robo de credenciales de usuario. • Almacenamiento de credenciales. • Passwords de Windows. ○ Credenciales de Windows. ○ Credenciales basadas en certificados. ○ Credenciales genéricas. ○ Credenciales web. • Credenciales en caché. • Contramedidas. ○ Priorizar cuentas de alto valor y ordenadores. ○ Identificar el comportamiento normal. ○ Proteger contra amenazas conocidas y desconocidas. ○ El valor de la contención. ○ Establecer un modelo de contención para los privilegios de la cuenta. ○ Implementar prácticas administrativas. ○ Endurecer y restringir hosts para fines administrativos. ○ Consideraciones para asegurar los bosques y dominios. ○ Prácticas de gestión de credenciales recomendadas. ○ Establecer configuraciones de seguridad. ○ La usabilidad como característica de seguridad. ○ Utilizar Windows 10 con Credential Guard. ○ Restringir y proteger cuentas de dominio de alto privilegio. ○ Restringir y proteger cuentas locales con privilegios administrativos. ○ Restringir el tráfico de red entrante. ○ No permitir la navegación en Internet desde cuentas altamente privilegiadas. ○ Eliminar usuarios estándar del grupo de administradores locales. ○ Usar herramientas de administración remota que no coloquen credenciales reutilizables en la memoria de un ordenador remoto.	**26 horas**

○ Actualizar aplicaciones y sistemas operativos. ○ Limitar el número y uso de cuentas de dominio privilegiadas. ○ Asegurar y administrar los controladores de dominio.	
Examen UA 03	**30 minutos**
Actividad de Evaluación UA 03	**30 minutos**
Tiempo total de la unidad	**27 horas**
Unidad 4: DOS/DDOS. • Características. Motivación. • Víctimas. ○ El ataque Dyn 2016. ○ El ataque GitHub 2015. ○ El ataque Spamhaus 2013. ○ El ataque de Estonia 2007. ○ El ataque de Mafia Boy de 2000. • Ejemplos. ○ Clasificación según el tipo de daño o efecto provocado. ○ Clasificación por nivel de capa OSI. ○ Taxonomía por tipo de ataque. • Contramedidas. ○ Medidas de protección de nuestra red. ○ Medidas de protección en nuestra infraestructura. ○ Medidas de protección en nuestras aplicaciones web.	**17 horas**
Examen UA 04	**30 minutos**
Actividad de Evaluación UA 04	**30 minutos**
Tiempo total de la unidad	**18 horas**
Unidad 5: Otros riesgos. • Cámara web (webcam). • Estafas telefónicas. ○ Estafa de la llamada perdida. ○ Estafa de WhatsApp. ○ Estafa del servicio contratado. ○ Estafa de la tarjeta VISA. ○ Estafa técnicos de Microsoft. • Dispositivos USB. • Seguridad física. ○ Edificios, instalaciones y locales.	**14 horas**

○ Autenticación y control de acceso físico. ○ Gabinetes de comunicación. ○ Medios físicos empleados para el almacenamiento y procesamiento de la información.	
Examen UA 05	**30 minutos**
Actividad de Evaluación UA 05	**30 minutos**
Tiempo total de la unidad	**15 horas**
Unidad 6: Mejorar la seguridad. Parte I. • Password. • Ataques por correo electrónico (phishing). • Seguridad en el navegador. • Seguridad inalámbrica (Wireless). • VPN. • Seguridad DNS. • Usuarios predeterminados. Actualizaciones. • Antivirus. Cortafuegos (firewalls). • Sentido común.	**16 horas**
Examen UA 06	**30 minutos**
Actividad de Evaluación UA 06	**30 minutos**
Tiempo total de la unidad	**17 horas**
Unidad 7: Mejorar la seguridad. Parte II. • Seguridad por defecto y/o por diseño. • Sistemas actualizados. • Control de accesos. Gestión segura de contraseñas. • Antimalware. • El correo electrónico. Navegación segura. • Aplicaciones de confianza. • Copias de seguridad. Destrucción segura. • Necesidades especiales en IoT. Necesidades específicas en cloud. • Sistemas operativos de confianza (TOS).	**17 horas**
Examen UA 07	**30 minutos**
Actividad de Evaluación UA 07	**30 minutos**
Tiempo total de la unidad	**18 horas**

Unidad 8: Reacción frente un incidente.
 	
• Detección.
• Análisis.
• Evaluación.
• Clasificación de los incidentes de seguridad.
  ○ Crítico.
  ○ Muy alto.
  ○ Alto.
  ○ Medio.
  ○ Bajo.
• Priorización.
• Reacción.
  ○ Actividades previas al desastre.
  ○ Actividades después del desastre.
	15 horas

Examen UA 08	**30 minutos**
Actividad de Evaluación UA 08	**30 minutos**
Tiempo total de la unidad	**16 horas**
Examen final IFCT151PO	**1 hora**
8 unidades	**150 horas**