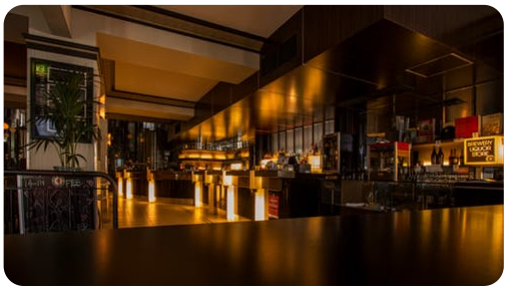

IFCT151PO. Ciberseguridad. Sector hostelería

Sku: PIT100

Horas: 150

OBJETIVOS

- 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

CONTENIDOS

Unidad 1: Conceptos básicos de ciberseguridad. • El valor de la información. • Hackers y ciberdelincuentes. • Seguridad por defecto. • Políticas y procedimientos. o Analizar la situación actual de la empresa. o Alinear el PDS con la estrategia de la empresa. o Definir los proyectos que se van a ejecutar. o Clasificar y priorizar los proyectos. o Aprobar el PDS. o Ejecución del PDS. o Certificación en seguridad. • Delitos informáticos. • Código de derecho de ciberseguridad. Examen UA 01 Actividad de Evaluación UA 01 Tiempo total de la unidad **Unidad 2: Amenazas, vulnerabilidades y riesgos.** • Tipos de amenazas. • Tipos de vulnerabilidades. o Físicas. o Naturales. o De hardware. o De software. o De almacenamiento. o De conexión. o Humanas. • Vulnerabilidades de loT. • Ingeniería social. • Malware. • Virus. Troyanos. Gusanos. Spyware. Ransomware. PUP. Key Loggers. Bots. o Virus. o Troyanos. o Gusanos. o Spyware. o Ransomware. o PUP. o Key Loggers. o Bots Examen UA 02 Actividad de Evaluación UA 02 Tiempo total de la unidad **Unidad 3: Ataques a credenciales.** • Demostración práctica del robo de credenciales de usuario. • Almacenamiento de credenciales. • Passwords de Windows. o Credenciales de Windows. o Credenciales basadas en certificados. o Credenciales genéricas. o Credenciales web. • Credenciales en caché. • Contramedidas. o Priorizar cuentas de alto valor y ordenadores. o Identificar el comportamiento normal. o Proteger contra amenazas conocidas y desconocidas. o El valor de la contención. o Establecer un modelo de contención para los privilegios de la cuenta. o Implementar prácticas administrativas. o Endurecer y restringir hosts para fines administrativos. o Consideraciones para asegurar los bosques y dominios. o Prácticas de gestión de credenciales recomendadas. o Establecer configuraciones de seguridad. o La usabilidad como característica de seguridad. o Utilizar Windows 10 con Credential Guard. o Restringir y proteger cuentas de dominio de alto privilegio. o Restringir y proteger cuentas locales con privilegios administrativos. o Restringir el tráfico de red entrante. o No permitir la navegación en Internet desde cuentas altamente privilegiadas. o Eliminar usuarios estándar del grupo de administradores locales. o Usar herramientas de

administración remota que no coloquen credenciales reutilizables en la memoria de un ordenador remoto. o Actualizar aplicaciones y sistemas operativos. o Limitar el número y uso de cuentas de dominio privilegiadas. o Asegurar y administrar los controladores de dominio. Examen UA 03 Actividad de Evaluación UA 03 Tiempo total de la unidad **Unidad 4: DOS/DDOS.** • Características. Motivación. • Víctimas. o El ataque Dyn 2016. o El ataque GitHub 2015. o El ataque Spamhaus 2013. o El ataque de Estonia 2007. o El ataque de Mafia Boy de 2000. • Ejemplos. o Clasificación según el tipo de daño o efecto provocado. o Clasificación por nivel de capa OSI. o Taxonomía por tipo de ataque. • Contramedidas. o Medidas de protección de nuestra red. o Medidas de protección en nuestra infraestructura. o Medidas de protección en nuestras aplicaciones web. Examen UA 04 Actividad de Evaluación UA 04 Tiempo total de la unidad **Unidad 5: Otros riesgos.** • Cámara web (webcam). • Estafas telefónicas. o Estafa de la llamada perdida. o Estafa de WhatsApp. o Estafa del servicio contratado. o Estafa de la tarjeta VISA. o Estafa técnicos de Microsoft. • Dispositivos USB. • Seguridad física. o Edificios, instalaciones y locales. o Autenticación y control de acceso físico. o Gabinetes de comunicación. o Medios físicos empleados para el almacenamiento y procesamiento de la información. Examen UA 05 Actividad de Evaluación UA 05 Tiempo total de la unidad **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. Examen UA 06 Actividad de Evaluación UA 06 Tiempo total de la unidad **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 loT. Necesidades específicas en cloud. • Sistemas operativos de confianza (TOS). Examen UA 07 Actividad de Evaluación UA 07 Tiempo total de la unidad **Unidad 8: Reacción frente un incidente.** • Detección. • Análisis. • Evaluación. • Clasificación de los incidentes de seguridad. o Crítico. o Muy alto. o Alto. o Medio. o Bajo. • Priorización. • Reacción. o Actividades previas al desastre. o Actividades después del desastre. Examen UA 08 Actividad de Evaluación UA 08 Tiempo total de la unidad Examen final IFCT151PO