IFCT151PO. Ciberseguridad. Sector hostelería.

Sku: PS888

Horas: 150

Formato: HTML

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

1. CONCEPTOS BÁSICOS DE CIBERSEGURIDAD 1.1. El valor de la información 1.2. Hackers y ciberdelincuentes 1.3. Seguridad por defecto 1.4. Políticas y procedimientos 1.5. Delitos informáticos 1.6. Código de derecho de ciberseguridad **2. AMENAZAS, VULNERABILIDADES Y RIESGOS** 2.1. Tipos de Amenazas. 2.2. Tipos de vulnerabilidades. 2.3. Vulnerabilidades de IoT 2.4. Ingeniería Social 2.5. Malware 2.6. Virus 2.7. Troyanos 2.8. Gusanos 2.9. Spyware 2.10. Ransomware 2.11. PUPs 2.12. Key Loggers 2.13. Bots. **3. ATAQUES A CREDENCIALES** 3.1. Demostración práctica del robo de credenciales de usuario 3.2. Almacenamiento de credenciales 3.3. Passwords en Windows 3.4. Credenciales en caché 3.5. Contramedidas **4. DOS/DDOS** 4.1. Características 4.2. Motivación 4.3. Víctimas 4.4. Ejemplos 4.5. Contramedidas **5. OTROS RIESGOS** 5.1. Webcam 5.2. Estafas telefónicas 5.3. Dispositivos USB 5.4. Seguridad física **6. MEJORAR LA SEGURIDAD. PARTE I** 6.1. Password 6.2. Ataques por e-mail (pishing) 6.3. Seguridad en el navegador 6.4. Seguridad Wireless 6.5. VPN 6.6. Seguridad DNS 6.7. Usuarios predeterminados 6.8. Actualizaciones 6.9. Antivirus 6.10. Firewalls (cortafuegos) 6.11. Sentido Común **7. MEJORAR LA SEGURIDAD. PARTE II** 7.1. Seguridad por defecto y/o por diseño 7.2. Sistemas actualizados 7.3. Control de accesos 7.4. Gestión segura de contraseñas 7.5. Antimalware 7.6. El correo electrónico 7.7. Navegación Segura 7.8. Aplicaciones de confianza. 7.9. Copias de seguridad 7.10. Destrucción segura 7.11. Necesidades específicas en IoT 7.12. Necesidades específicas en Cloud. 7.13. Sistemas operativos de confianza (TOS) **8. REACCIÓN FRENTE UN INCIDENTE** 8.1. Detección 8.2. Análisis 8.3. Evaluación 8.4. Clasificación de los incidentes de seguridad 8.5. Priorización 8.6. Reacción