

ÍNDICE 32120 IFCT102 CIBERSEGURIDAD EN EL TRABAJO

TEMA 1 DEFINICIÓN DE LOS MÉTODOS DE ACCESO REMOTO

- 1.1. Concepto, beneficios y riesgos del acceso remoto
- 1.2. Métodos de acceso remoto en el trabajo

TEMA 2 CONTEXTUALIZACIÓN DEL TELETRABAJO

- 2.1. Concepto y ventajas del teletrabajo
- 2.2. Herramientas tecnológicas para el teletrabajo

TEMA 3 IDENTIFICACIÓN DE LAS PRINCIPALES AMENAZAS PARA LOS TERMINALES DE TELETRABAJO

- 3.1. Introducción a las amenazas en el teletrabajo
- 3.2. Malware y software malicioso
- 3.3. Ataques de ingeniería social y phishing
- 3.4. Vulnerabilidades en redes y conexiones remotas
- 3.5. Amenazas en dispositivos personales y corporativos
- 3.6. Ataques a aplicaciones y servicios en la nube

TEMA 4 IDENTIFICACIÓN DE LAS PRINCIPALES MEDIDAS PARA PREVENIR AMENAZAS. RECOPIACIÓN DE EVIDENCIAS

- 4.1. Seguridad en el acceso en remoto
- 4.2. Seguridad en los equipos de trabajo
- 4.3. Seguridad en dispositivos móviles
- 4.4. Técnicas y recursos para el análisis de los datos

TEMA 5 PROTECCIÓN DE DATOS EN LOS TERMINALES DE TELETRABAJO

- 5.1. Protección de datos en el teletrabajo y su normativa
- 5.2. Seguridad en el almacenamiento y transmisión de datos
- 5.3. Control de accesos y autenticación segura Cifrado de datos en discos duros, USBs y dispositivos móviles.
- 5.4. Prevención de fugas de información (Data Loss Prevention, DLP)

TEMA 6 UTILIZACIÓN DE COPIAS DE SEGURIDAD EN DISPOSITIVOS DE TELETRABAJO

- 6.1 Copias de seguridad y su clasificación
- 6.2. Métodos y soportes de almacenamiento de copias de seguridad
- 6.3. Políticas y estrategias de copias de seguridad en teletrabajo
- 6.4. Seguridad en las copias de seguridad

ANEXO

- Glosario de términos
- Bibliografía
- Supuestos prácticos