IFCT0109. SEGURIDAD INFORMÁTICA

MF0489_3 SISTEMAS SEGUROS DE ACCESO Y TRANSMISIÓN DE DATOS

00

DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

MF0489_3 SISTEMAS SEGUROS DE ACCESO Y TRANSMISIÓN DE DATOS

OBJETIVOS GENERALES

ESTE MÓDULO FORMATIVO SE ENCUENTRA DENTRO DEL CERTIFICADO DE PROFESIONALIDAD **IFCT0109. SEGURIDAD INFORMÁTICA**, CUYO OBJETIVO GENERAL ES:

- GARANTIZAR LA SEGURIDAD DE LOS ACCESOS Y USOS DE LA INFORMACIÓN REGISTRADA EN EQUIPOS INFORMÁTICOS, ASÍ COMO DEL PROPIO SISTEMA, PROTEGIÉNDOSE DE LOS POSIBLES ATAQUES, IDENTIFICANDO VULNERABILIDADES Y APLICANDO SISTEMAS DE CIFRADO A LAS COMUNICACIONES QUE SE REALICEN HACIA EL EXTERIOR Y EN EL INTERIOR DE LA ORGANIZACIÓN

MF0489_3 SISTEMAS SEGUROS DE ACCESO Y TRANSMISIÓN DE DATOS

OBJETIVOS ESPECÍFICOS

LOS OBJETIVOS ESPECÍFICOS DE ESTE MÓDULO SON:

- EVALUAR LAS TÉCNICAS DE CIFRADO EXISTENTES PARA ESCOGER LA NECESARIA EN FUNCIÓN DE LOS REQUISITOS DE SEGURIDAD EXIGIDOS.
- IMPLANTAR SERVICIOS Y TÉCNICAS CRIPTOGRÁFICAS EN AQUELLOS SERVICIOS QUE LO REQUIERAN SEGÚN ESPECIFICACIONES DE SEGURIDAD INFORMÁTICA.
- UTILIZAR SISTEMAS DE CERTIFICADOS DIGITALES EN AQUELLAS COMUNICACIONES QUE REQUIERAN INTEGRIDAD Y CONFIDENCIALIDAD SEGÚN ESPECIFICACIONES DE SEGURIDAD.
- DISEÑAR E IMPLANTAR SERVICIOS DE CERTIFICACIÓN DIGITAL SEGÚN NECESIDADES DE EXPLOTACIÓN Y DE SEGURIDAD INFORMÁTICA.

MF0489_3 SISTEMAS SEGUROS DE ACCESO Y TRANSMISIÓN DE DATOS

CONTENIDOS

1. CRIPTOGRAFÍA
2. APLICACIÓN DE UNA INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)
3. COMUNICACIONES SEGURAS

MF0489_3 SISTEMAS SEGUROS DE ACCESO Y TRANSMISIÓN DE DATOS

CONTENIDOS

1. CRIPTOGRAFÍA

1. INTRODUCCIÓN
2. PERSPECTIVA HISTÓRICA Y OBJETIVOS DE LA CRIPTOGRAFÍA
3. TEORÍA DE LA INFORMACIÓN
4. PROPIEDADES DE LA SEGURIDAD QUE SE PUEDEN CONTROLAR MEDIANTE LA APLICACIÓN DE LA CRIPTOGRAFÍA: CONFIDENCIALIDAD, INTEGRIDAD, AUTENTICIDAD, NO REPUDIO, IMPUTABILIDAD Y SELLADO DE TIEMPOS
5. ELEMENTOS FUNDAMENTALES DE LA CRIPTOGRAFÍA DE CLAVE PRIVADA Y DE CLAVE P3ÚBLICA
6. CARACTERÍSTICAS Y ATRIBUTOS DE LOS CERTIFICADOS DIGITALES
7. IDENTIFICACIÓN Y DESCRIPCIÓN DEL FUNCIONAMIENTO DE LOS PROTOCOLOS DE INTERCAMBIO DE CLAVES USADOS MÁS FRECUENTEMENTE
8. ALGORITMOS CRIPTOGRÁFICOS MÁS FRECUENTEMENTE UTILIZADOS
9. ELEMENTOS DE LOS CERTIFICADOS DIGITALES, LOS FORMATOS COMÚNMENTE ACEPTADOS Y SU UTILIZACIÓN
10. ELEMENTOS FUNDAMENTALES DE LAS FUNCIONES RESUMEN Y LOS CRITERIOS PARA SU UTILIZACIÓN
11. REQUERIMIENTOS LEGALES INCLUIDOS EN LA LEY 59/2003, DE 19 DE DICIEMBRE, DE FIRMA ELECTRÓNICA
12. ELEMENTOS FUNDAMENTALES DE LA FIRMA DIGITAL, LOS DISTINTOS TIPOS DE FIRMA Y LOS CRITERIOS PARA SU UTILIZACIÓN
13. CRITERIOS PARA LA UTILIZACIÓN DE TÉCNICAS DE CIFRADO DE FLUJO Y DE BLOQUE
14. PROTOCOLOS DE INTERCAMBIO DE CLAVES
15. USO DE HERRAMIENTAS DE CIFRADO TIPO PGP, GPG O CRYPTOLOOP

MF0489_3 SISTEMAS SEGUROS DE ACCESO Y TRANSMISIÓN DE DATOS

CONTENIDOS

2. APLICACIÓN DE UNA INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)

1. INTRODUCCIÓN
2. IDENTIFICACIÓN DE LOS COMPONENTES DE UNA PKI Y SU MODELO DE RELACIONES
3. AUTORIDAD DE CERTIFICACIÓN Y SUS ELEMENTOS
4. POLÍTICA DE CERTIFICADO Y DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (CPS)
5. LISTA DE CERTIFICADOS REVOCADOS (CRL)
6. FUNCIONAMIENTO DE LAS SOLICITUDES DE FIRMA DE CERTIFICADOS (CSR)
7. INFRAESTRUCTURA DE GESTIÓN DE PRIVILEGIOS (PMI)
8. CAMPOS DE CERTIFICADOS DE ATRIBUTOS, INCLUYEN LA DESCRIPCIÓN DE SUS USOS HABITUALES Y LA RELACIÓN CON LOS CERTIFICADOS DIGITALES
9. APLICACIONES QUE SE APOYAN EN LA EXISTENCIA DE UNA PKI

MF0489_3 SISTEMAS SEGUROS DE ACCESO Y TRANSMISIÓN DE DATOS

CONTENIDOS

3. COMUNICACIONES SEGURAS

1. INTRODUCCIÓN
2. DEFINICIÓN, FINALIDAD Y FUNCIONALIDAD DE REDES PRIVADAS VIRTUALES
3. PROTOCOLO IPSEC
4. PROTOCOLOS SSL Y SSH
5. SISTEMAS SSL VPN
6. TÚNELES CIFRADOS
7. VENTAJAS E INCONVENIENTES DE LAS DISTINTAS ALTERNATIVAS PARA LA IMPLANTACIÓN DE LA TECNOLOGÍA DE VPN

MF0489_3 SISTEMAS SEGUROS DE ACCESO Y TRANSMISIÓN DE DATOS