IFCT0109. SEGURIDAD INFORMÁTICA

MF0487_3 AUDITORÍA DE SEGURIDAD INFORMÁTICA

00

DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

MF0487_3 AUDITORÍA DE SEGURIDAD INFORMÁTICA

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

MF0487_3 AUDITORÍA DE SEGURIDAD INFORMÁTICA

OBJETIVOS ESPECÍFICOS

- ANALIZAR Y SELECCIONAR LAS HERRAMIENTAS DE AUDITORÍA Y DETECCIÓN DE VULNERABILIDADES DEL SISTEMA INFORMÁTICO IMPLANTANDO AQUELLAS QUE SE ADECUEN A LAS ESPECIFICACIONES DE SEGURIDAD INFORMÁTICA..
- APLICAR PROCEDIMIENTOS RELATIVOS AL CUMPLIMIENTO DE LA NORMATIVA LEGAL VIGENTE.
- PLANIFICAR Y APLICAR MEDIDAS DE SEGURIDAD PARA GARANTIZAR LA INTEGRIDAD DEL SISTEMA INFORMÁTICO Y DE LOS PUNTOS DE ENTRADA Y SALIDA DE LA RED DEPARTAMENTAL.

MF0487_3 AUDITORÍA DE SEGURIDAD INFORMÁTICA

CONTENIDOS

1. CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE AUDITORÍA INFORMÁTICA
2. APLICACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL
3. ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN
4. USO DE HERRAMIENTAS PARA LA AUDITORÍA DE SISTEMAS
5. DESCRIPCIÓN DE LOS ASPECTOS SOBRE CORTAFUEGOS EN AUDITORÍAS DE SISTEMAS INFORMÁTICOS
6. GUÍAS PARA LA EJECUCIÓN DE LAS DISTINTAS FASES DE LA AUDITORÍA DE SISTEMA DE INFORMACIÓN

MF0487_3 AUDITORÍA DE SEGURIDAD INFORMÁTICA

CONTENIDOS

1. CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE AUDITORÍA INFORMÁTICA

1. INTRODUCCIÓN
2. CÓDIGO DEONTOLÓGICO DE LA FUNCIÓN DE AUDITORÍA
3. RELACIÓN DE LOS DISTINTOS TIPOS DE AUDITORÍA EN EL MARCO DE LOS SISTEMAS DE LA INFORMACIÓN
4. CRITERIOS A SEGUIR PARA LA COMPOSICIÓN DEL EQUIPO AUDITOR
5. TIPOS DE PRUEBAS A REALIZAR EN EL MARCO DE LA AUDITORÍA. PRUEBAS SUSTANTIVAS Y PRUEBAS DE CUMPLIMIENTO
6. TIPOS DE MUESTREO A APLICAR DURANTE EL PROCESO DE AUDITORÍA
7. UTILIZACIÓN DE HERRAMIENTAS TIPO CAAT (COMPUTER ASSISTED AUDIT TOOLS)
8. EXPLICACIÓN DE LOS REQUERIMIENTOS QUE DEBEN CUMPLIR LOS HALLAZGOS DE AUDITORÍA
9. APLICACIÓN DE CRITERIOS COMUNES PARA CATEGORIZAR LOS HALLAZGOS COMO OBSERVACIONES O NO CONFORMIDADES
10. RELACIÓN DE LAS NORMATIVAS Y METODOLOGÍAS RELACIONADAS CON LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN COMÚNMENTE ACEPTADAS

MF0487_3 AUDITORÍA DE SEGURIDAD INFORMÁTICA

CONTENIDOS

2. APLICACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

1. PRINCIPIOS GENERALES DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL
2. NORMATIVA EUROPEA RECOGIDA EN LA DIRECTIVA 95/46/CE
3. NORMATIVA NACIONAL RECOGIDA EN EL CÓDIGO PENAL, LEY ORGÁNICA PARA EL TRATAMIENTO AUTOMATIZADO DE DATOS (LORTAD), LEY ORGÁNICA DE PROTECCIÓN DE DATOS (LOPD) Y REGLAMENTO DE DESARROLLO DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS (RD 1720/2007)
4. IDENTIFICACIÓN Y REGISTRO DE LOS FICHEROS CON DATOS DE CARÁCTER PERSONAL UTILIZADOS POR LA ORGANIZACIÓN
5. EXPLICACIÓN DE LAS MEDIDAS DE SEGURIDAD PARA LA PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL RECOGIDAS EN EL REAL DECRETO 1720/2007
6. GUÍA PARA LA REALIZACIÓN DE LA AUDITORÍA BIENAL OBLIGATORIA DE LEY ORGÁNICA 15-1999 DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

MF0487_3 AUDITORÍA DE SEGURIDAD INFORMÁTICA

CONTENIDOS

3. ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN

1. INTRODUCCIÓN AL ANÁLISIS DE RIESGOS
2. PRINCIPALES TIPOS DE VULNERABILIDADES, FALLOS DE PROGRAMA, PROGRAMAS MALICIOSOS Y SU ACTUALIZACIÓN PERMANENTE, ASÍ COMO CRITERIOS DE PROGRAMACIÓN SEGURA
3. PARTICULARIDADES DE LOS DISTINTOS TIPOS DE CÓDIGO MALICIOSO
4. PRINCIPALES ELEMENTOS DEL ANÁLISIS DE RIESGOS Y SUS MODELOS DE RELACIONES
5. METODOLOGÍAS CUALITATIVAS Y CUANTITATIVAS DE ANÁLISIS DE RIESGOS
6. IDENTIFICACIÓN DE LOS ACTIVOS INVOLUCRADOS EN EL ANÁLISIS DE RIESGOS Y SU VALORACIÓN
7. IDENTIFICACIÓN DE LAS AMENAZAS QUE PUEDEN AFECTAR A LOS ACTIVOS IDENTIFICADOS PREVIAMENTE
8. ANÁLISIS E IDENTIFICACIÓN DE LAS VULNERABILIDADES EXISTENTES EN LOS SISTEMAS DE INFORMACIÓN QUE PERMITIRÍAN LA MATERIALIZACIÓN DE AMENAZAS, INCLUYENDO EL ANÁLISIS LOCAL, ANÁLISIS REMOTO DE CAJA BLANCA Y DE CAJA NEGRA

MF0487_3 AUDITORÍA DE SEGURIDAD INFORMÁTICA

CONTENIDOS

3. ANÁLISIS DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN

9. OPTIMIZACIÓN DEL PROCESO DE AUDITORÍA Y CONTRASTE DE VULNERABILIDADES E INFORME DE AUDITORÍA
10. IDENTIFICACIÓN DE LAS MEDIDAS DE SALVAGUARDA EXISTENTES EN EL MOMENTO DE LA REALIZACIÓN DEL ANÁLISIS DE RIESGOS Y SU EFECTO SOBRE LAS VULNERABILIDADES Y AMENAZAS
11. ESTABLECIMIENTO DE LOS ESCENARIOS DE RIESGO ENTENDIDOS COMO PARES ACTIVO-AMENAZA SUSCEPTIBLES DE MATERIALIZARSE
12. -DETERMINACIÓN DE LA PROBABILIDAD E IMPACTO DE MATERIALIZACIÓN DE LOS ESCENARIOS
13. ESTABLECIMIENTO DEL NIVEL DE RIESGO PARA LOS DISTINTOS PARES DE ACTIVO Y AMENAZA
14. DETERMINACIÓN POR PARTE DE LA ORGANIZACIÓN DE LOS CRITERIOS DE EVALUACIÓN DEL RIESGO, EN FUNCIÓN DE LOS CUALES SE DETERMINA SI UN RIESGO ES ACEPTABLE O NO
15. RELACIÓN DE LAS DISTINTAS ALTERNATIVAS DE GESTIÓN DE RIESGOS

MF0487_3 AUDITORÍA DE SEGURIDAD INFORMÁTICA

CONTENIDOS

4. USO DE HERRAMIENTAS PARA LA AUDITORÍA DE SISTEMAS

1. INTRODUCCIÓN
2. HERRAMIENTAS DEL SISTEMA OPERATIVO
3. HERRAMIENTAS DE ANÁLISIS DE RED, PUERTOS Y SERVICIOS TIPO.
4. HERRAMIENTAS DE ANÁLISIS DE VULNERABILIDADES
5. ANALIZADORES DE PROTOCOLOS
6. ANALIZADORES DE PÁGINAS WEB
7. ATAQUES DE DICCIONARIO Y FUERZA BRUTA

MF0487_3 AUDITORÍA DE SEGURIDAD INFORMÁTICA

CONTENIDOS

5. DESCRIPCIÓN DE LOS ASPECTOS SOBRE CORTAFUEGOS EN AUDITORÍAS DE SISTEMAS INFORMÁTICOS

1. INTRODUCCIÓN PRINCIPIOS GENERALES DE CORTAFUEGOS
2. COMPONENTES DE UN CORTAFUEGOS DE RED
3. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD
4. ARQUITECTURAS DE CORTAFUEGOS DE RED
5. OTRAS ARQUITECTURAS DE CORTAFUEGOS DE RED

ESTO ES TODO