IFCT0109. SEGURIDAD INFORMÁTICA

MF0486_3. SEGURIDAD EN EQUIPOS INFORMÁTICOS

00

DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

MF0486_3. SEGURIDAD EN EQUIPOS INFORMÁTICOS

CONTENIDOS

1. CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE SEGURIDAD DE LOS EQUIPOS INFORMÁTICOS
2. ANÁLISIS DE IMPACTO DE NEGOCIO
3. GESTIÓN DE RIESGOS
4. PLAN DE IMPLANTACIÓN DE SEGURIDAD
5. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL
6. SEGURIDAD FÍSICA E INDUSTRIAL DE LOS SISTEMAS. SEGURIDAD LÓGICA DE SISTEMA
7. IDENTIFICACIÓN DE SERVICIOS
8. ROBUSTECIMIENTO DE SISTEMAS
9. IMPLANTACIÓN Y CONFIGURACIÓN DE CORTAFUEGOS

MF0486_3. SEGURIDAD EN EQUIPOS INFORMÁTICOS

CONTENIDOS

1. CRITERIOS GENERALES COMÚNMENTE ACEPTADOS SOBRE SEGURIDAD DE LOS EQUIPOS INFORMÁTICOS

1. INTRODUCCIÓN
2. MODELO DE SEGURIDAD ORIENTADA A LA GESTIÓN DEL RIESGO RELACIONADO CON EL USO DE LOS SISTEMAS DE INFORMACIÓN.
3. RELACIÓN DE LAS AMENAZAS MÁS FRECUENTES, LOS RIESGOS QUE IMPLICAN Y LAS SALVAGUARDAS MÁS FRECUENTES
4. SALVAGUARDAS Y TECNOLOGÍAS DE SEGURIDAD MÁS HABITUALES
5. LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA COMO COMPLEMENTO A SALVAGUARDAS Y MEDIDAS TECNOLÓGICAS

MF0486_3. SEGURIDAD EN EQUIPOS INFORMÁTICOS

CONTENIDOS

2. ANÁLISIS DE IMPACTO DE NEGOCIO

1. INTRODUCCIÓN
2. IDENTIFICACIÓN DE PROCESOS DE NEGOCIO SOPORTADOS POR SISTEMAS DE INFORMACIÓN
3. VALORACIÓN DE LOS REQUERIMIENTOS DE CONFIDENCIALIDAD, INTEGRIDAD, Y DISPONIBILIDAD DE LOS PROCESOS DE NEGOCIO
4. DETERMINACIÓN DE LOS SISTEMAS DE INFORMACIÓN QUE SOPORTAN LOS PROCESOS DE NEGOCIO Y SUS REQUERIMIENTOS DE SEGURIDAD

MF0486_3. SEGURIDAD EN EQUIPOS INFORMÁTICOS

CONTENIDOS

3. GESTIÓN DE RIESGOS

1. INTRODUCCIÓN
2. APLICACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS Y EXPOSICIÓN DE LAS ALTERNATIVAS MÁS FRECUENTES
3. METODOLOGÍAS COMÚNMENTE ACEPTADAS DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS
4. APLICACIÓN DE CONTROLES Y MEDIDAS DE SALVAGUARDA PARA OBTENER UNA REDUCCIÓN DEL RIESGO

MF0486_3. SEGURIDAD EN EQUIPOS INFORMÁTICOS

CONTENIDOS

4. PLAN DE IMPLANTACIÓN DE SEGURIDAD

1. INTRODUCCIÓN
2. DETERMINACIÓN DEL NIVEL DE SEGURIDAD EXISTENTE DE LOS SISTEMAS FRENTE A LA NECESARIA, EN BASE A LOS REQUERIMIENTOS DE SEGURIDAD DE LOS PROCESOS DE NEGOCIO
3. SELECCIÓN DE MEDIDAS DE SALVAGUARDA PARA CUBRIR LOS REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN
4. GUÍA PARA LA ELABORACIÓN DEL PLAN DE IMPLANTACIÓN DE LAS SALVAGUARDAS SELECCIONADAS

MF0486_3. SEGURIDAD EN EQUIPOS INFORMÁTICOS

CONTENIDOS

5. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

1. INTRODUCCIÓN
2. PRINCIPIOS GENERALES DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL
3. INFRACCIONES Y SANCIONES CONTEMPLADAS EN LA LEGISLACIÓN VIGENTE EN MATERIA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL
4. IDENTIFICACIÓN Y REGISTRO DE LOS FICHEROS CON DATOS DE CARÁCTER PERSONAL UTILIZADOS POR LA ORGANIZACIÓN
5. ELABORACIÓN DEL DOCUMENTO DE SEGURIDAD REQUERIDO POR LA LEGISLACIÓN VIGENTE EN MATERIA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

MF0486_3. SEGURIDAD EN EQUIPOS INFORMÁTICOS

CONTENIDOS

6. SEGURIDAD FÍSICA E INDUSTRIAL DE LOS SISTEMAS. SEGURIDAD LÓGICA DE SISTEMAS

1. INTRODUCCIÓN
2. DETERMINACIÓN DE LOS PERÍMETROS DE SEGURIDAD FÍSICA
3. CRITERIOS DE SEGURIDAD PARA EL EMPLAZAMIENTO FÍSICO DE LOS SISTEMAS INFORMÁTICOS
4. EXPOSICIÓN DE ELEMENTOS MÁS FRECUENTES PARA GARANTIZAR LA CALIDAD Y CONTINUIDAD DEL SUMINISTRO ELÉCTRICO A LOS SISTEMAS INFORMÁTICOS. CRITERIOS DE SEGURIDAD PARA EL EMPLAZAMIENTO FÍSICO DE LOS SISTEMAS INFORMÁTICOS
5. REQUERIMIENTOS DE CLIMATIZACIÓN Y PROTECCIÓN CONTRA INCENDIOS APLICABLES A LOS SISTEMAS INFORMÁTICOS
6. ELABORACIÓN DE LA NORMATIVA DE SEGURIDAD FÍSICA E INDUSTRIAL PARA LA ORGANIZACIÓN
7. SISTEMAS DE FICHEROS MÁS FRECUENTEMENTE UTILIZADOS

MF0486_3. SEGURIDAD EN EQUIPOS INFORMÁTICOS

CONTENIDOS

6. SEGURIDAD FÍSICA E INDUSTRIAL DE LOS SISTEMAS. SEGURIDAD LÓGICA DE SISTEMAS

8. ESTABLECIMIENTO DEL CONTROL DE ACCESOS DE LOS SISTEMAS INFORMÁTICOS A LA RED DE COMUNICACIONES DE LA ORGANIZACIÓN
9. CONFIGURACIÓN DE POLÍTICAS Y DIRECTIVAS DEL DIRECTORIO DE USUARIOS
10. ESTABLECIMIENTO DE LAS LISTAS DE CONTROL DE ACCESO (ACL) A FICHEROS
11. GESTIÓN DE ALTAS, BAJAS Y MODIFICACIONES DE USUARIOS Y LOS PRIVILEGIOS QUE TIENEN ASIGNADOS
12. REQUERIMIENTOS DE SEGURIDAD RELACIONADOS CON EL CONTROL DE ACCESO DE LOS USUARIOS AL SISTEMA OPERATIVO
13. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL SISTEMA OPERATIVO NECESARIOS PARA MONITORIZAR Y SUPERVISAR EL CONTROL DE ACCESOS
14. ELABORACIÓN DE LA NORMATIVA DE CONTROL DE ACCESOS A LOS SISTEMAS INFORMÁTICOS

MF0486_3. SEGURIDAD EN EQUIPOS INFORMÁTICOS

CONTENIDOS

7. IDENTIFICACIÓN DE SERVICIOS

1. INTRODUCCIÓN
2. IDENTIFICACIÓN DE LOS PROTOCOLOS, SERVICIOS Y PUERTOS UTILIZADOS POR LOS SISTEMAS DE INFORMACIÓN
3. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE PUERTOS Y SERVICIOS ABIERTOS PARA DETERMINAR AQUELLOS QUE NO SON NECESARIOS
4. UTILIZACIÓN DE HERRAMIENTAS DE ANÁLISIS DE TRÁFICO DE COMUNICACIONES PARA DETERMINAR EL USO REAL QUE HACEN LOS SISTEMAS DE INFORMACIÓN DE LOS DISTINTOS PROTOCOLOS, SERVICIOS Y PUERTOS

MF0486_3. SEGURIDAD EN EQUIPOS INFORMÁTICOS

CONTENIDOS

8. ROBUSTECIMIENTO DE SISTEMAS

1. INTRODUCCIÓN
2. MODIFICACIÓN DE LOS USUARIOS Y CONTRASEÑAS POR DEFECTO DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN
3. CONFIGURACIÓN DE LAS DIRECTIVAS DE GESTIÓN DE CONTRASEÑAS Y PRIVILEGIOS EN EL DIRECTORIO DE USUARIOS
4. ELIMINACIÓN Y CIERRE DE LAS HERRAMIENTAS, UTILIDADES, SERVICIOS Y PUERTOS PRESCINDIBLES
5. ACTUALIZACIÓN DE PARCHES DE SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS
6. PROTECCIÓN DE LOS SISTEMAS DE INFORMACIÓN FRENTE A CÓDIGO MALICIOSO
7. GESTIÓN SEGURA DE COMUNICACIONES, CARPETAS COMPARTIDAS, IMPRESORAS Y OTROS RECURSOS COMPARTIDOS DEL SISTEMA
8. MONITORIZACIÓN DE LA SEGURIDAD Y EL USO ADECUADO DE LOS SISTEMAS DE INFORMACIÓN

MF0486_3. SEGURIDAD EN EQUIPOS INFORMÁTICOS

CONTENIDOS

9. IMPLANTACIÓN Y CONFIGURACIÓN DE CORTAFUEGOS

1. INTRODUCCIÓN
2. RELACIÓN DE LOS DISTINTOS TIPOS DE CORTAFUEGOS POR UBICACIÓN Y FUNCIONALIDAD
3. CRITERIOS DE SEGURIDAD PARA LA SEGREGACIÓN DE REDES EN EL CORTAFUEGOS MEDIANTE ZONAS DESMILITARIZADAS/DMZ
4. UTILIZACIÓN DE REDES PRIVADAS VIRTUALES/VPN PARA ESTABLECER CANALES SEGUROS DE COMUNICACIONES
5. DEFINICIÓN DE REGLAS DE CORTE EN LOS CORTAFUEGOS
6. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL CORTAFUEGOS, NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE SEGURIDAD
7. ESTABLECIMIENTO DE LA MONITORIZACIÓN Y PRUEBAS DEL CORTAFUEGOS

MF0486_3. SEGURIDAD EN EQUIPOS INFORMÁTICOS