IFCT0109. SEGURIDAD INFORMÁTICA

MF0488_3 GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

00

DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

MF0488_3 GESTIÓN DE INCIDENTES 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

MF0488_3 GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

CONTENIDOS

1. SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES (IDS/IPS)
2. IMPLANTACIÓN Y PUESTA EN PRODUCCIÓN DE SISTEMAS IDS/IPS
3. CONTROL DE CÓDIGO MALICIOSO
4. RESPUESTA ANTE INCIDENTES DE SEGURIDAD
5. PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN
6. ANÁLISIS FORENSE INFORMÁTICO

MF0488_3 GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

CONTENIDOS

1. SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES (IDS/IPS)

1. INTRODUCCIÓN
2. CONCEPTOS GENERALES DE GESTIÓN DE INCIDENTES, DETECCIÓN DE INTRUSIONES Y SU PREVENCIÓN
3. IDENTIFICACIÓN Y CARACTERIZACIÓN DE LOS DATOS DE FUNCIONAMIENTO DEL SISTEMA
4. ARQUITECTURAS MÁS FRECUENTES DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS
5. RELACIÓN DE LOS DISTINTOS TIPOS DE IDS/IPS POR UBICACIÓN Y FUNCIONALIDAD
6. CRITERIOS DE SEGURIDAD PARA EL ESTABLECIMIENTO DE LA UBICACIÓN DE LOS IDS/IPS

MF0488_3 GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

CONTENIDOS

2. IMPLANTACIÓN Y PUESTA EN PRODUCCIÓN DE SISTEMAS IDS/IPS

1. INTRODUCCIÓN
2. ANÁLISIS PREVIO DE LOS SERVICIOS, PROTOCOLOS, ZONAS Y EQUIPOS QUE UTILIZA LA ORGANIZACIÓN PARA SUS PROCESOS DE NEGOCIO
3. DEFINICIÓN DE POLÍTICAS DE CORTE DE INTENTOS DE INTRUSIÓN EN LOS IDS/IPS
4. ANÁLISIS DE LOS EVENTOS REGISTRADOS POR EL IDS/IPS PARA DETERMINAR FALSOS POSITIVOS Y CARACTERIZARLOS EN LAS POLÍTICAS DE CORTE DEL IDS/IPS
5. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DEL IDS/ IPS NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE INTENTOS DE INTRUSIÓN
6. ESTABLECIMIENTO DE LOS NIVELES REQUERIDOS DE ACTUALIZACIÓN, MONITORIZACIÓN Y PRUEBAS DEL IDS/ IPS

MF0488_3 GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

CONTENIDOS

3. CONTROL DE CÓDIGO MALICIOSO

1. INTRODUCCIÓN
2. SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO
3. RELACIÓN DE LOS DISTINTOS TIPOS DE HERRAMIENTAS DE CONTROL DE CÓDIGO MALICIOSO EN FUNCIÓN DE LA TOPOLOGÍA DE LA INSTALACIÓN Y LAS VÍAS DE INFECCIÓN A CONTROLAR
4. CRITERIOS DE SEGURIDAD PARA LA CONFIGURACIÓN DE LAS HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO
5. DETERMINACIÓN DE LOS REQUERIMIENTOS Y TÉCNICAS DE ACTUALIZACIÓN DE LAS HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO
6. RELACIÓN DE LOS REGISTROS DE AUDITORÍA DE LAS HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGOS MALICIOSOS NECESARIOS PARA MONITORIZAR Y SUPERVISAR SU CORRECTO FUNCIONAMIENTO Y LOS EVENTOS DE SEGURIDAD
7. ESTABLECIMIENTO DE LA MONITORIZACIÓN Y PRUEBAS DE LAS HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO
8. ANÁLISIS DE LOS PROGRAMAS MALICIOSOS MEDIANTE DESENSAMBLADORES Y ENTORNOS DE EJECUCIÓN CONTROLADA

MF0488_3 GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

CONTENIDOS

4. RESPUESTA ANTE INCIDENTES DE SEGURIDAD

1. INTRODUCCIÓN
2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD
3. EXPOSICIÓN DE LAS DISTINTAS TÉCNICAS Y HERRAMIENTAS UTILIZADAS PARA EL ANÁLISIS Y CORRELACIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD
4. PROCESO DE VERIFICACIÓN DE LA INTRUSIÓN
5. NATURALEZA Y FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES TIPO CERT NACIONALES E INTERNACIONALES

MF0488_3 GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

CONTENIDOS

5. PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN

1. INTRODUCCIÓN
2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES
3. CATEGORIZACIÓN DE LOS INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES EN FUNCIÓN DE SU IMPACTO POTENCIAL
4. CRITERIOS PARA LA DETERMINACIÓN DE LAS EVIDENCIAS OBJETIVAS EN LAS QUE SE SOPORTARÁ LA GESTIÓN DEL INCIDENTE
5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES
6. GUÍA PARA LA CLASIFICACIÓN Y ANÁLISIS INICIAL DEL INTENTO DE INTRUSIÓN O INFECCIÓN CONTEMPLANDO EL IMPACTO PREVISIBLE DEL MISMO
7. ESTABLECIMIENTO DEL NIVEL DE INTERVENCIÓN REQUERIDO EN FUNCIÓN DEL IMPACTO PREVISIBLE
8. GUÍA PARA LA INVESTIGACIÓN Y DIAGNÓSTICO DEL INCIDENTE DE INTENTO DE INTRUSIÓN O INFECCIONES
9. ESTABLECIMIENTO DEL PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE LOS SISTEMAS TRAS UN INCIDENTE DERIVADO DE UN INTENTO DE INTRUSIÓN O INFECCIÓN
10. PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE
11. ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE Y LOS REGISTROS NECESARIOS PARA DOCUMENTAR EL HISTÓRICO DEL INCIDENTE

MF0488_3 GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

CONTENIDOS

6. ANÁLISIS FORENSE INFORMÁTICO

1. INTRODUCCIÓN
2. CONCEPTOS GENERALES Y OBJETIVOS DEL ANÁLISIS FORENSE
3. EXPOSICIÓN DEL PRINCIPIO DE LOCARD
4. GUÍA PARA LA RECOGIDA DE EVIDENCIAS ELECTRÓNICAS
5. GUÍA PARA EL ANÁLISIS DE LAS EVIDENCIAS ELECTRÓNICAS RECOGIDAS, INCLUYENDO EL ESTUDIO DE FICHEROS Y DIRECTORIOS OCULTOS, INFORMACIÓN OCULTA DE SISTEMA Y LA RECUPERACIÓN DE FICHEROS BORRADOS
6. GUÍA PARA LA SELECCIÓN DE LAS HERRAMIENTAS DE ANÁLISIS FORENSE

MF0488_3 GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA