# IFCT0109. SEGURIDAD INFORMÁTICA
# MF0488_3 GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

# RESUMEN FINAL

# 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

# CONTENIDOS

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

# RESUMEN

UN **INCIDENTE DE SEGURIDAD** ES *CUALQUIER EVENTO QUE PUEDE AFECTAR A LA INTEGRIDAD, CONFIDENCIALIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN*. TAMBIÉN SE PUEDE DEFINIR COMO *UN EVENTO NO DESEADO QUE PUEDE COMPROMETER SIGNIFICATIVAMENTE LAS OPERACIONES DE UNA ORGANIZACIÓN Y AMENAZAR SU SEGU*RIDAD.

HAY NUMEROSOS TIPOS DE INCIDENTES DE SEGURIDAD:

- ACCESOS NO AUTORIZADOS
- CÓDIGO MALICIOSO
- DENEGACIÓN DE SERVICIO
- INTENTOS DE INFORMACIÓN DE UN SISTEMA
- USO DEFICIENTE DE LOS RECURSOS TECNOLÓGICOS
- ETC.

PARA CADA UNO DE ELLOS LAS ORGANIZACIONES DEBEN TOMAR UNA SERIE DE MEDIDAS QUE LOS CORRIJAN, LOS PREVENGAN O, COMO MÍNIMO, LOS DETECTEN.

# RESUMEN

LA **GESTIÓN DE INCIDENTES** TIENE COMO OBJETIVO LA *ORGANIZACIÓN DE LOS RECURSOS PARA QUE ESTAS MEDIDAS SEAN APLICADAS DE UN MODO EFICIENTE*.

PARA ELLO SE PUEDE UTILIZAR EL *VISOR DE EVENTOS* DE **WINDOWS** O *UNA SERIE DE COMANDOS* EN **LINUX** QUE OFRECEN UNA VISIÓN DE LOS DIFERENTES ARCHIVOS DE REGISTRO DE EVENTOS.

UNA VEZ YA SE CONOCE CÓMO LOCALIZAR LOS EVENTOS QUE OCURREN EN UN SISTEMA, ES BÁSICA LA IMPLANTACIÓN DE **SISTEMAS DE PREVENCIÓN DE INTRUSIONES** O DE **SISTEMAS DE DETECCIÓN DE INTRUSIONE**S COMO COMPLEMENTO A LAS DEMÁS MEDIDAS DE SEGURIDAD DE LA ORGANIZACIÓN.

# RESUMEN

UNA VEZ DECIDIDO EL SISTEMA IDS/IPS A IMPLANTAR, OTRA DE LAS DECISIONES FUNDAMENTALES QUE INFLUIRÁN EN EL SISTEMA DE SEGURIDAD DE UNA ORGANIZACIÓN ES ELEGIR **LA UBICACIÓN** DE ESTOS SISTEMAS. ATENDIENDO A *CRITERIOS DE ASUNCIÓN DE RIESGOS Y GRADO DE CONFIANZA.*

# CONTENIDOS

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

## RESUMEN

**LOS SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES** SON UNA POTENTE HERRAMIENTA PARA EVITAR POSIBLES ATAQUES QUE PUEDEN PRODUCIRSE EN LA INFRAESTRUCTURA DE RED DE LA ORGANIZACIÓN.

SON SISTEMAS COMPLEJOS Y MUY ESPECIALIZADOS, POR LO QUE ES VITAL QUE **LAS ORGANIZACIONES REALICEN UN ANÁLISIS PREVIO DE SUS INFRAESTRUCTURAS, SERVICIOS, EQUIPOS, ZONAS Y PROTOCOLOS** UTILIZADOS PARA DETERMINAR EL SISTEMA A IMPLANTAR, SUS CARACTERÍSTICAS Y CONFIGURACIONES Y SU LOCALIZACIÓN DENTRO DE SUS INSTALACIONES O A TRAVÉS DE ENTORNOS VIRTUALES.

## RESUMEN

UNA VEZ YA TOMADA LA DECISIÓN SOBRE EL SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES QUE SE VA A IMPLANTAR EN UNA ORGANIZACIÓN **DEBEN DECIDIRSE QUÉ POLÍTICAS DE CORTE DE ATAQUES SE VAN A APLICAR** CUANDO SE DETECTE ALGUNA INTRUSIÓN DISTINGUIENDO ENTRE **POLÍTICAS DE RESPUESTA PASIVA** (CUANDO EL SISTEMA SE LIMITA A INFORMAR DE LOS DETALLES DE LA INTRUSIÓN) Y **POLÍTICAS DE RESPUESTA ACTIVA** (CUANDO EL SISTEMA ADEMÁS DE INFORMAR TOMA MEDIDAS QUE FRENEN EL ATAQUE).

LA SIGUIENTE FASE EN LA DETECCIÓN Y PREVENCIÓN DE INTRUSIONES CONSISTE EN **ANALIZAR LOS EVENTOS QUE HA REGISTRADO EL IDS/IPS** Y QUE HA CALIFICADO COMO ATAQUES.

## RESUMEN

ESTOS SISTEMAS NO SON PERFECTOS Y PUEDE SER QUE HAYA FALSOS POSITIVOS Y FALSOS NEGATIVOS. POR ELLO, LAS ORGANIZACIONES **DEBEN CONFIGURAR SUS SISTEMAS** PARA QUE EL NÚMERO DE ERRORES SEA EL MÍNIMO POSIBLE **CONSIGUIENDO UN EQUILIBRIO ENTRE LA SENSIBILIDAD DEL SISTEMA Y LA CANTIDAD DE DATOS A INSPECCIONAR** SEGÚN SUS REQUERIMIENTOS Y NECESIDADES.

**LOS REGISTROS DE AUDITORÍA EN UN IDS/IPS** SON AQUELLOS EN LOS QUE SE REGISTRAN EVENTOS REALIZADOS POR LOS USUARIOS EN UN SISTEMA Y FACILITAN INFORMACIÓN TANTO DE LOS USUARIOS COMO DE LOS DEMÁS DETALLES DEL EVENTO REALIZADO.

## RESUMEN

UNA VEZ DEFINIDAS LAS POLÍTICAS DE ACTUACIÓN Y ANALIZADOS LOS REGISTROS DE AUDITORÍA, LOS ADMINISTRADORES DE LA ORGANIZACIÓN YA TIENEN SUFICIENTE INFORMACIÓN PARA COMPROBAR LA EFICACIA DEL SISTEMA DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES.

AUN ASÍ, SIEMPRE SERÁ NECESARIO EL ESTABLECIMIENTO **DE PRUEBAS Y ACTUALIZACIONES PERIÓDICAS DEL SISTEMA IMPLANTADO** QUE GARANTICEN QUE NO HAY NINGUNA MERMA DE EFICACIA MEDIANTE LA COMPROBACIÓN DE UNA SERIE DE INDICADORES **COMO EL RENDIMIENTO, LA COMPLETITUD, LA PRECISIÓN, LA TOLERANCIA A FALLOS Y EL TIEMPO DE RESPUESTA DEL SISTEMA**.

# CONTENIDOS

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

# RESUMEN

LA INSEGURIDAD DE LOS EQUIPOS ELECTRÓNICOS HA IDO AUMENTANDO CON EL TIEMPO POR LA GRAN CANTIDAD DE INTENTOS Y ATAQUES QUE SE PRODUCEN A DIARIO Y A SU ALTA CAPACIDAD Y VELOCIDAD DE PROPAGACIÓN POR LAS NUEVAS TECNOLOGÍAS DE COMUNICACIÓN.

UN TIPO DE ATAQUE MUY COMÚN SON LOS **CÓDIGOS MALICIOSOS**, PARA LOS CUALES EXISTEN SISTEMAS DE DETECCIÓN Y CONTENCIÓN: **IDS/IPS, ANTIVIRUS Y CORTAFUEGOS**.

LA ELECCIÓN DE LOS SISTEMAS DE DETECCIÓN Y CONTENCIÓN PUEDE VARIAR EN FUNCIÓN DE LA TIPOLOGÍA DE LA INSTALACIÓN DE RED DE LA ORGANIZACIÓN Y DE LAS VÍAS DE INFECCIÓN QUE SE PRETENDEN CONTROLAR.

# RESUMEN

SIN EMBARGO, EN EL INSTANTE DE DECIDIR QUÉ HERRAMIENTAS Y SISTEMAS DE PROTECCIÓN IMPLANTAR EN LA ORGANIZACIÓN HAY QUE TENER EN CUENTA LAS RECOMENDACIONES DE LA **NORMA ISO 27001**, EN LA QUE SE DESCRIBEN UNA SERIE DE PROCEDIMIENTOS DE CONCIENCIACIÓN DE USUARIOS EN CUANTO A SEGURIDAD Y TAMBIÉN LAS RECOMENDACIONES SOBRE LOS REQUERIMIENTOS Y LAS TÉCNICAS DE ACTUALIZACIÓN PARA LAS HERRAMIENTAS DE CONTENCIÓN Y CONTROL DE CÓDIGO MALICIOSO.

UNA VEZ DECIDIDAS LAS HERRAMIENTAS A IMPLANTAR SUELE SUCEDER QUE EL NÚMERO DE HERRAMIENTAS ES MUY ELEVADO Y RESULTA UNA TAREA ARDUA LLEVAR A CABO UN CONTROL MANUAL DE ESTAS.

# RESUMEN

COMO SOLUCIÓN A ESTA PROBLEMÁTICA HAY VARIAS APLICACIONES ENCARGADAS DE GESTIONAR LA INFRAESTRUCTURA DE HERRAMIENTAS DE DETECCIÓN DE LA ORGANIZACIÓN OFRECIENDO ESTADÍSTICAS QUE PERMITEN CONOCER SU EFICACIA, LA EVOLUCIÓN DE DETECCIÓN DE CÓDIGOS MALICIOSOS Y LAS MEDIDAS QUE SE HAN IDO TOMANDO EN CADA UNA DE LAS DETECCIONES.

PARA TERMINAR, OTRO TIPO DE HERRAMIENTAS MUY ÚTILES PARA COMBATIR LOS CÓDIGOS MALICIOSOS SON LAS HERRAMIENTAS QUE GENERAN ENTORNOS DE EJECUCIÓN CONTROLADA Y LOS DESENSAMBLADORES.

# CONTENIDOS

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

# RESUMEN

LA **GESTIÓN DE INCIDENTES** ES LA PARTE DE LA SEGURIDAD QUE SE ENCARGA DE ASIGNAR LOS RECURSOS A LA PREVENCIÓN, DETECCIÓN Y CORRECCIÓN DE INCIDENTES QUE AFECTEN A LA SEGURIDAD DE LA INFORMACIÓN. ESTA GESTIÓN CONLLEVA UNA SERIE DE PASOS A SEGUIR:

**PREPARACIÓN Y PREVENCIÓN, DETECCIÓN Y NOTIFICACIÓN, ANÁLISIS PRELIMINAR, CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN, INVESTIGACIÓN Y ACTIVIDADES POSTERIORES**.

TODOS ESTOS PASOS AYUDAN A LAS ORGANIZACIONES A OBTENER MÁS INFORMACIÓN DEL INCIDENTE, EVALUAR LOS DAÑOS CAUSADOS, TOMAR MEDIDAS AL RESPECTO Y A CONSEGUIR LLEGAR AL PUNTO INICIAL EN EL MENOR TIEMPO POSIBLE.

# RESUMEN

CON LA RECOLECCIÓN DE INFORMACIÓN SE CONSIGUE ANALIZAR TODO EL PROCEDIMIENTO LLEVADO A CABO POR EL INCIDENTE Y ELABORAR MEDIDAS PREVENTIVAS EVITANDO QUE SE VUELVA A PRODUCIR.

POR SU PARTE, **LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN BASADA EN EL ANÁLISIS Y CORRELACIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (CON HERRAMIENTAS SIM, SEM Y SIEM)** FACILITARÁ AL RESPONSABLE DE SEGURIDAD EL CONOCIMIENTO DE TODO LO QUE SUCEDE EN LOS EQUIPOS A TIEMPO REAL Y ASÍ, CONSEGUIR ESTABLECER MEDIDAS DE CONTENCIÓN MÁS EFECTIVAS Y RÁPIDAS EN CUANTO SE DETECTE ALGÚN INDICIO DE INCIDENTE DE SEGURIDAD.

# RESUMEN

UNA VEZ DETECTADO Y ELIMINADO EL INCIDENTE Y RESTAURADA LA SITUACIÓN ORIGINAL DEBE PROCEDERSE A **LA INVESTIGACIÓN Y VERIFICACIÓN DEL INCIDENTE** CON EL FIN DE ELABORAR UN **INFORME FINAL** QUE CONTENGA ASPECTOS FUNDAMENTALES ACERCA DE LAS CAUSAS Y CONSECUENCIAS PRODUCIDAS POR EL INCIDENTE, LA EVALUACIÓN DE LA TOMA DE DECISIONES Y ACTUACIONES LLEVADAS A CABO POR EL EQUIPO DE RESPUESTA A INCIDENTES, EL ANÁLISIS DE LAS POLÍTICAS DE SEGURIDAD Y EL ANÁLISIS DE LAS DIRECTRICES DE LA ORGANIZACIÓN.

# RESUMEN

PARA ESTABLECER ESTAS MEDIDAS Y HERRAMIENTAS HAY UNA SERIE DE ORGANIZACIONES NACIONALES E INTERNACIONALES CONOCIDAS COMO **CERT O CENTROS DE RESPUESTA A INCIDENTES DE SEGURIDAD EN TECNOLOGÍAS** DE LA INFORMACIÓN ENCARGADAS DE DISEÑAR MEDIDAS PREVENTIVAS Y REACTIVAS, MANTENER BASES DE DATOS DE INCIDENTES ACTUALIZADAS Y, EN GENERAL, DE APOYAR Y OFRECER INFORMACIÓN VALIOSA A LAS ORGANIZACIONES QUE LES AYUDEN A ELABORAR UN PLAN DE GESTIÓN DE INCIDENTES DE MAYOR CALIDAD.

# CONTENIDOS

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

# RESUMEN

**LAS INTRUSIONES** SON UN CONJUNTO DE EVENTOS OCURRIDOS CUANDO UN USUARIO INTENTA ACCEDER AL SISTEMA SIN AUTORIZACIÓN POR VARIOS MOTIVOS.

LAS ORGANIZACIONES DEBEN SER CAPACES DE **ESTABLECER UNA SERIE DE HERRAMIENTAS Y CONTROLES** QUE PREVENGAN LA APARICIÓN DE ESTOS INTRUSOS Y EVITEN SU ACCESO.

AUN ASÍ, **CUANDO SE DETECTA UNA POSIBLE INTRUSIÓN** ES NECESARIO LLEVAR A CABO UNA SERIE DE PASOS ESTABLECIDOS PARA QUE SE GESTIONE DEL MODO MÁS EFICIENTE POSIBLE.

# RESUMEN

SE COMIENZA CON LA **RECOLECCIÓN DE INFORMACIÓN ADICIONAL** PARA COMPROBAR SI LA AMENAZA ES REAL O POR EL CONTRARIO ES UNA FALSA ALARMA.

EN EL CASO DE SER UNA AMENAZA REAL SE DEBE PROCEDER A **UN ANÁLISIS DE LA INCIDENCIA Y A SU CLASIFICACIÓN** SEGÚN CRITERIOS DE CRITICIDAD DE LOS RECURSOS E IMPACTO POTENCIAL EN LA ORGANIZACIÓN.

ATENDIENDO A ESTA CLASIFICACIÓN SE DEBERÁN **DEFINIR LOS TIEMPOS MÁXIMOS DE CONTENCIÓN Y RESOLUCIÓN DEL INCIDENTE**, DEBIENDO RESOLVERSE EN MENOR TIEMPO A MEDIDA QUE AUMENTA LA PRIORIDAD DE LA INCIDENCIA.

# RESUMEN

UNA VEZ TOMADAS LAS MEDIDAS CORRECTIVAS Y RESUELTA LA INCIDENCIA DEBE VALORARSE LA POSIBILIDAD DE **COMUNICAR SU OCURRENCIA A TERCEROS** QUE PUEDAN VERSE IMPLICADOS POR LA UTILIZACIÓN DE SUS DATOS.

PARA CONCLUIR Y UNA VEZ RESUELTO EL PROBLEMA Y REALIZADAS LAS COMUNICACIONES PERTINENTES SE PROCEDERÁ AL **CIERRE DEL INCIDENTE**, REGISTRANDO TODA LA INFORMACIÓN SOBRE SU EVOLUCIÓN, LAS MEDIDAS QUE SE HAN TOMADO, LOS ERRORES COMETIDOS Y SUS SOLUCIONES PARA AUMENTAR LA EFICIENCIA ANTE INCIDENCIAS FUTURAS.

# RESUMEN

UN CORRECTO REGISTRO DEL INCIDENTE PERMITIRÁ A LAS ORGANIZACIONES **OBTENER UN APRENDIZAJE DE LAS ACCIONES TOMADAS QUE CONSIGA EVITAR NUEVOS INCIDENTES** QUE SEAN SIMILARES A LOS YA SUCEDIDOS, REDUCIÉNDOSE ASÍ TIEMPO Y DAÑOS PRODUCIDOS.

# CONTENIDOS

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

## RESUMEN

DEBIDO A LA PRESENCIA CRECIENTE DE INCIDENTES DE SEGURIDAD SURGIERON LAS **HERRAMIENTAS DE ANÁLISIS FORENSE DIGITAL**.

SE TRATA DE UNA DISCIPLINA DENTRO DE LA SEGURIDAD INFORMÁTICA QUE *SE ENCARGA DE ANALIZAR LOS INCIDENTES DE SEGURIDAD Y LOS DELITOS DIGITALES A POSTERIORI PARA RECONSTRUIR LOS HECHOS Y CONSEGUIR DETECTAR AL ATACANTE Y AVERIGUAR CÓMO HA ACCEDIDO A LOS EQUIPOS*.

LOS USOS Y OBJETIVOS DE ESTOS ANÁLISIS SON DE LO MÁS VARIADOS Y PUEDEN UTILIZARSE TANTO PARA APORTAR PRUEBAS PARA INVESTIGAR DELITOS DE FRAUDE CON COMPAÑÍAS DE SEGUROS, COMO PARA REALIZAR INVESTIGACIONES CON ÓRDENES JUDICIALES, ENTRE OTROS.

## RESUMEN

PARA DESARROLLAR LAS TÉCNICAS DE ANÁLISIS FORENSE DIGITAL DEBE SEGUIRSE UNA METODOLOGÍA CON UNAS **FASES** PERFECTAMENTE DEFINIDAS**: ESTUDIO PRELIMINAR, RECOPILACIÓN DE EVIDENCIAS, ANÁLISIS DE EVIDENCIAS Y ELABORACIÓN DE INFORMES CON LOS RESULTADOS.**

CON LA CORRECTA APLICACIÓN DE ESTAS FASES Y UN MANTENIMIENTO ADECUADO DE LA CADENA DE **CUSTODIA DE LAS EVIDENCIAS** (QUE IMPIDA QUE LA INFORMACIÓN RECOPILADA SE MODIFIQUE Y PUEDA LLEVAR A RESULTADOS ERRÓNEOS) SE PUEDE LLEGAR A DESCUBRIR EL ORIGEN DEL ATAQUE, LOCALIZAR AL ATACANTE E, INCLUSO, TOMAR MEDIDAS LEGALES CONTRA ESTE PARA EXIGIRLE RESPONSABILIDAD POR LOS DAÑOS CAUSADOS.

## RESUMEN

POR ESTE MOTIVO, LOS DISTINTOS ATACANTES CADA VEZ UTILIZAN TÉCNICAS MÁS SOFISTICADAS PARA OCULTAR SUS HUELLAS Y EVITAR SER DESCUBIERTOS.

AUN ASÍ, SE PUEDEN ENCONTRAR EN EL MERCADO VARIAS HERRAMIENTAS (TANTO DE PAGO, COMO GRATUITAS Y PARA VARIOS SISTEMAS OPERATIVOS) QUE CONSIGUEN RECOGER EVIDENCIAS Y DETECTAR AL CULPABLE CON BASTANTE PROBABILIDAD.

# ACTIVIDADES

- ACTIVIDAD 01. USO DE ARMITAGE
- ACTIVIDAD 02. USO DE LA HERRAMIENTA NIKTO
- ACTIVIDAD 03. USO DE JOHN THE RIPPER
- ACTIVIDAD 04. USO DE CONTRASEÑAS
- ACTIVIDAD 05. ATAQUES DE INGENIERÍA SOCIAL
- ACTIVIDAD 06. ARP SPOOFING MAN IN THE MIDDLE Y DNS SPOOFING
- ACTIVIDAD 07. EXPLOTAR VULNERABILIDAD (E1)
- ACTIVIDAD 08. ATAQUE DE PHISING
- ACTIVIDAD 09. PREVENCIÓN DE PÉRDIDA DE DATOS (DLP)
- ACTIVIDAD 10. USO DE HERRAMIENTA OPENVAS

# ACTIVIDADES

- ACTIVIDAD 11. ATAQUE DE DENEGACIÓN DE SERVICIO
- ACTIVIDAD 12. USO DE OPNSENSE
- ACTIVIDAD 13. GESTIÓN DE CIBERINCIDENTES
- ACTIVIDAD 14. INSTALAR IDS-IPS SURICATA (E2)
- ACTIVIDAD 15. HERRAMIENTAS DE ANÁLISIS FORENSE INFORMÁTICO
- ACTIVIDAD 16. PRUEBAS ANTIMALWARE (E3)

# ANEXOS

- SITIOS WEB VULNERABLES Y VULNERABILIDADES MÁS FRECUENTES
- INGENIERÍA SOCIAL
- EXPLOTAR VULNERABILIDAD
- FUGA DE INFORMACIÓN Y PREVENCIÓN DE PÉRDIDA DE DATOS (DLP)
- ARP SPOOFING, MAN IN THE MIDDLE Y DNS SPOOFING
- ATAQUE DE PHISHING
- ESCANER DE VULNERABILIDADES OPENVAS
- USO DE SURICATA
- ATAQUE DE DENEGACIÓN DE SERVICIO
- GUIA CIBERSEGURIDAD GESTION FUGA INFORMACIÓN
- INCIDENTES DE CIBERSEGURIDAD

# ANEXOS

- GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD
- CCN-STIC-1453 PROCEDIMIENTO DE EMPLEO SEGURO OPNSENSE
- DESCARGA E INSTALACIÓN DE ANTIVIRUS
- EJEMPLOS PRÁCTICOS DE GESTIÓN DE INCIDENTES
- HERRAMIENTAS DE INVESTIGACIÓN FORENSE

# ESTO ES TODO