IFCT0109. SEGURIDAD INFORMÁTICA

MF0488_3 GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

UD03

UNIDAD 03. CONTROL DE CÓDIGO MALICIOSO

DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

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

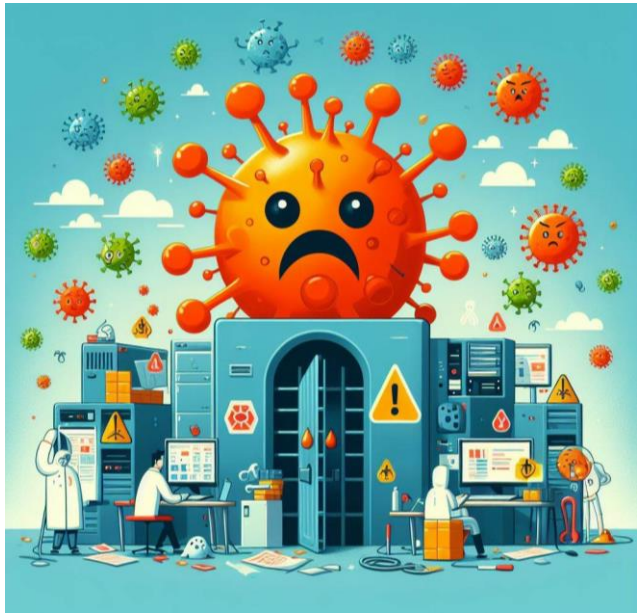
1. INTRODUCCIÓN

LOS ATAQUES E INTRUSIONES QUE PUEDE RECIBIR UN EQUIPO SON DE LO MÁS VARIADOS Y CUANTIOSOS. UNO DE LOS MÁS NOCIVOS Y HABITUALES SON **LOS CÓDIGOS MALICIOSOS**.

EN ESTE CAPÍTULO SE DEFINE EL CONCEPTO DE CÓDIGO MALICIOSO Y SE DESCRIBEN EN PROFUNDIDAD LAS **DISTINTAS FORMAS QUE PUEDEN TOMAR, CÓMO ACTÚAN Y CUÁLES SON LOS SISTEMAS MÁS FRECUENTES PARA SU DETECCIÓN**.

1. INTRODUCCIÓN

CON CONOCER CÓMO FUNCIONAN NO ES SUFICIENTE PARA EVITAR QUE SE PRODUZCAN DAÑOS EN EL EQUIPO, SON NECESARIAS UNA SERIE DE **HERRAMIENTAS ENCARGADAS DE SU CONTROL Y CONTENCIÓN** QUE SE IRÁN DESCRIBIENDO JUNTO CON LAS DISTINTAS OPCIONES QUE SE PUEDEN INSTALAR EN FUNCIÓN DE LAS VÍAS DE INFECCIÓN QUE SE DESEAN CONTROLAR Y DE LA TOPOLOGÍA DE LA INSTALACIÓN DE RED DE CADA ORGANIZACIÓN.



1. INTRODUCCIÓN

ES VITAL **CONFIGURAR ESTAS HERRAMIENTAS SIGUIENDO CRITERIOS** DEFINIDOS QUE SEAN **ACORDES CON LA POLÍTICA DE SEGURIDAD DE LA ORGANIZACIÓN**.

CRITERIOS QUE TENDRÁN QUE VER EN **CÓMO** SE DEBE **ACTUAR ANTE LA DETECCIÓN DE CÓDIGO MALICIOSO** Y EN LA **POLÍTICA DE ACTUALIZACIÓN DE LAS HERRAMIENTAS** DE DETECCIÓN Y CONTENCIÓN PARA NO REBAJAR EL NIVEL DE SEGURIDAD EN TODO LO QUE SEA POSIBLE.

1. INTRODUCCIÓN

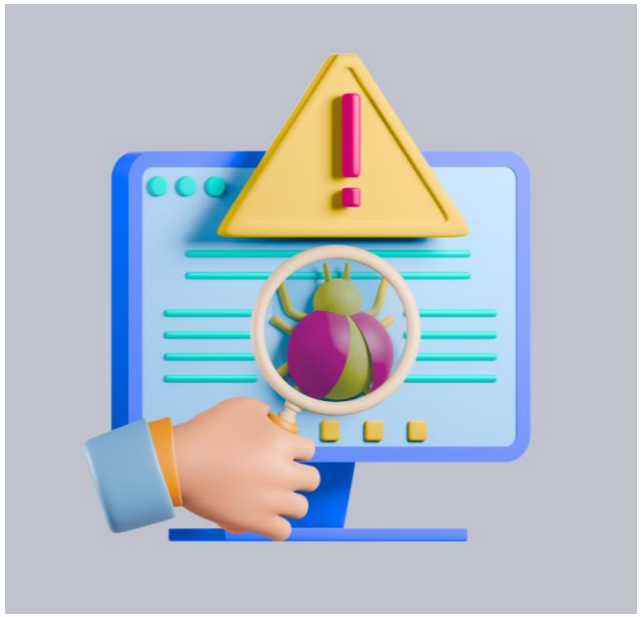
OTRA OPCIÓN PARA DETECTAR Y CONTENER CÓDIGO MALICIOSO O MALWARE SON **SUS REGISTROS DE AUDITORÍA**.

MEDIANTE UNA SERIE DE APLICACIONES **SE PUEDEN CONOCER LOS REGISTROS DE SEGURIDAD Y ESTABLECER PATRONES DE COMPORTAMIENTO Y ESTADÍSTICAS** DE LAS HERRAMIENTAS DE DETECCIÓN QUE PERMITIRÁN CONOCER SU EFECTIVIDAD Y SABER SI ES NECESARIO CAMBIAR SUS CRITERIOS O CONFIGURACIONES PARA OBTENER MEJORAS DE LA SEGURIDAD.

1. INTRODUCCIÓN

PARA TERMINAR EL CAPÍTULO, SE TRATARÁN LOS **ENTORNOS DE EJECUCIÓN CONTROLADA Y LOS DESENSAMBLADORES.**

DOS TIPOS DE **HERRAMIENTAS QUE TRATAN DE IDENTIFICAR LOS CÓDIGOS MALICIOSOS Y CONOCER SU COMPORTAMIENTO** CON EL FIN DE ESTABLECER MEDIDAS DE CONTENCIÓN MÁS ESPECÍFICAS Y EFICACES.



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

2. SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO

PARA ENTENDER ESTOS SISTEMAS Y SU FUNCIONAMIENTO **ES NECESARIO TENER UNOS CONOCIMIENTOS PREVIOS SOBRE LOS DISTINTOS TIPOS DE CÓDIGO MALICIOSO Y SU FUNCIONAMIENTO BÁSICO**.

SE CONCRETA EN ESTOS CONCEPTOS Y SE APORTAN UNOS CONOCIMIENTOS BÁSICOS QUE VAN A PERMITIR COMPRENDER LA FORMA DE ACTUAR QUE TIENEN LOS SISTEMAS DE DETECCIÓN Y CONTENCIÓN PARA COMBATIR ESTOS CÓDIGOS.

2. SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO

CÓDIGOS MALICIOSOS: CONCEPTOS BÁSICOS Y TIPOS

LA EVOLUCIÓN DEL MUNDO ELECTRÓNICO HA PROVOCADO UN **CRECIMIENTO DE LA INSEGURIDAD DEBIDO AL ELEVADO NÚMERO DE INTENTOS Y ATAQUES** QUE SE PRODUCEN DÍA TRAS DÍA.

LA COMUNIDAD DE INTRUSOS CADA VEZ ES MÁS AMPLIA **Y LA DECISIÓN DE A QUIÉN ATACAR** PUEDE TOMAR VARIAS VERTIENTES:

- PUEDEN DECIDIR **ATACAR A OBJETIVOS CLAROS Y ESPECÍFICAMENTE DEFINIDOS** (UN USUARIO U ORGANIZACIÓN DETERMINADA, ETC.).
- PUEDEN DECIDIR **ATACAR A UN PÚBLICO OBJETIVO DEFINIDO ATENDIENDO AL GRUPO DE INTERÉS**.
- PUEDEN **DECIDIR SUS OBJETIVOS ALEATORIAMENTE** SIN NINGÚN RACIONAMIENTO PREVIO.

2. SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO

CÓDIGOS MALICIOSOS: CONCEPTOS BÁSICOS Y TIPOS

DEL MISMO MODO LAS **MOTIVACIONES DE LOS INTRUSOS** TAMBIÉN PUEDEN SER DE LO MÁS DIVERSAS:

- **LUCRATIVAS:** ROBAR Y VENDER POSTERIORMENTE INFORMACIÓN DE VALOR, ENTRAR EN BASES DE DATOS PARA CONSEGUIR DIRECCIONES DE CORREO ELECTRÓNICO AL QUE MANDAR PUBLICIDAD O SPAM, ETC.
- **ENTRETENIMIENTO:** LOS INTRUSOS PUEDEN MOVERSE POR MERA DIVERSIÓN O PARA AUMENTAR SU EGO. TAMBIÉN ES FRECUENTE QUE LOS INTRUSOS UTILICEN CÓDIGOS MALICIOSOS PARA PROPAGAR ELEMENTOS PORNOGRÁFICOS.
- **MOTIVACIONES IDEOLÓGICAS:** LOS INTRUSOS PUEDEN FUNDAMENTAR SUS ATAQUES TAMBIÉN PARA REALIZAR APOLOGÍA DEL TERRORISMO O PARA DIFUNDIR SUS IDEOLOGÍAS POLÍTICAS, ÉTICAS O RELIGIOSAS.

2. SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO

CÓDIGOS MALICIOSOS: CONCEPTOS BÁSICOS Y TIPOS

LOS CÓDIGOS MALICIOSOS O MALWARE SON UNA SERIE DE PROGRAMAS INFORMÁTICOS QUE HAN SIDO DISEÑADOS CON FINES DESTRUCTIVOS PARA CONSEGUIR CIERTOS **OBJETIVOS** COMO:

- **DESTRUIR DATOS**, ELIMINANDO ARCHIVOS O, INCLUSO, FORMATEANDO DISCOS.
- **ROBAR INFORMACIÓN** Y CLAVES.
- **EXTENDERSE A TRAVÉS DE UN EQUIPO** A LOS DEMÁS EQUIPOS QUE FORMAN UNA RED O POR INTERNET.
- **COMPROMETER SISTEMAS** OPERATIVOS.
- **MOSTRAR PUBLICIDAD** INVASIVA.

2. SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO

CÓDIGOS MALICIOSOS: CONCEPTOS BÁSICOS Y TIPOS

LOS CÓDIGOS MALICIOSOS **SON CADA VEZ MÁS SOFISTICADOS**. ES POR ELLO QUÉ **CADA VEZ HAY MÁS VARIEDADES DISTINTAS** DE ESTOS TIPOS DE CÓDIGOS. AUN ASÍ, LOS DISTINTOS TIPOS DE MALWARE TIENEN CIERTOS **ASPECTOS COMUNES**:

- SUELEN SER COMPONENTES DE SOFTWARE **DISEÑADOS CON UN FIN ESPECÍFICO**.
- EN SU FUNCIONAMIENTO **INTERFIEREN CON LA OPERACIÓN NORMAL DEL SISTEMA** AL QUE ATACAN.
- ES MUY HABITUAL QUE SE **INSTALEN Y EJECUTEN SIN QUE HAYA UN CONSENTIMIENTO** EXPRESO DEL USUARIO DEL EQUIPO.
- PARA LOGRAR SUS OBJETIVOS **NECESITAN UN SISTEMA DE CÓMPUTO ANFITRIÓN**, UN EQUIPO EN EL QUE INSTALARSE Y PROPAGARSE.

2. SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO

CÓDIGOS MALICIOSOS: CONCEPTOS BÁSICOS Y TIPOS

A PESAR DE LAS CARACTERÍSTICAS COMUNES DE LOS CÓDIGOS MALICIOSOS HAY QUE REMARCAR QUE SUS DIFERENCIAS SON NUMEROSAS, LO QUE **CLASIFICA LOS DISTINTOS TIPOS ATENDIENDO A CARACTERÍSTICAS** COMO:

- **FORMA**
- **ORIGEN**
- **DAÑOS PROVOCADOS**
- **FINALIDAD PARA LA QUE SE DISEÑAN**

2. SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO

CÓDIGOS MALICIOSOS: CONCEPTOS BÁSICOS Y TIPOS

ATENDIENDO A ESTAS CARACTERÍSTICAS SE DISTINGUE ENTRE VARIOS **TIPOS DE MALWARE**:

- **VIRUS**
- **TROYANOS**
- **COOKIES**
- **KEYLOGGERS**
- **SPYWARE**
- **WORMS O GUSANOS**

2. SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO

CÓDIGOS MALICIOSOS: CONCEPTOS BÁSICOS Y TIPOS

VIRUS

SON PROGRAMAS INFORMÁTICOS DISEÑADOS CON LA FINALIDAD DE PRODUCIR ALGÚN TIPO DE DAÑO EN EL EQUIPO, TRABAJANDO SIN QUE EL USUARIO SE DÉ CUENTA.

PARA FUNCIONAR NECESITAN UN ANFITRIÓN O HUÉSPED EN EL QUE ALOJARSE, QUE PUEDE SER DE LO MÁS VARIADO: DESDE ARCHIVOS EJECUTABLES HASTA DISCOS DE ARRANQUE O UNIDADES DE MEMORIA.

EL DAÑO ES VARIABLE: DESDE EFECTOS MENOS NOCIVOS COMO LA APARICIÓN DE MENSAJES EN PANTALLA HASTA LA ELIMINACIÓN DE ARCHIVOS O LA INHABILITACIÓN DE ACCESO AL SISTEMA OPERATIVO.

2. SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO

CÓDIGOS MALICIOSOS: CONCEPTOS BÁSICOS Y TIPOS

VIRUS

CUANDO SE EJECUTA UN VIRUS SE **PRODUCEN DOS ACCIONES**:

- **EL DAÑO AL DISPOSITIVO.**
- **LA PROPAGACIÓN DEL VIRUS** INFECTANDO OTROS DISPOSITIVOS O ARCHIVOS.

EL **MODO MÁS HABITUAL DE CONTAGIO ES** POR **INTERNET**, **PERO NO EL ÚNICO**: LOS CANALES DE ENTRADA PUEDEN SER CUALQUIER DISPOSITIVO DE ALMACENAMIENTO (DISCOS DUROS, PENDRIVES, DISCOS DUROS EXTERNOS, ETC.) O, INCLUSO, REDES LOCALES (PROPAGACIÓN DEL VIRUS MEDIANTE LA UTILIZACIÓN DE CARPETAS COMPARTIDAS).

2. SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO

CÓDIGOS MALICIOSOS: CONCEPTOS BÁSICOS Y TIPOS

VIRUS

LA VARIEDAD DE VIRUS TAMBIÉN ES BASTANTE AMPLIA, HABIENDO EN LA ACTUALIDAD NUMEROSAS **CLASIFICACIONES** EN FUNCIÓN DE VARIAS CARACTERÍSTICAS O CRITERIOS COMO, POR EJEMPLO:

- *ORIGEN DEL VIRUS*
- *MODO DE INFECCIÓN Y PROPAGACIÓN*
- *DAÑOS OCASIONADOS*
- *LUGARES EN LOS QUE SE ESCONDEN*

2. SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO

CÓDIGOS MALICIOSOS: CONCEPTOS BÁSICOS Y TIPOS

TROYANOS

GENERALMENTE, LOS CÓDIGOS MALICIOSOS DENOMINADOS TROYANOS SON AQUELLOS **PROGRAMAS CON FUNCIONALIDADES OCULTAS** DISEÑADAS PARA FINES MALICIOSOS CONTRA EL USUARIO QUE LOS TIENE INSTALADOS.

A DIFERENCIA DE LOS VIRUS, LOS TROYANOS **NO TIENEN CAPACIDAD DE MULTIPLICARSE.**

ADEMÁS, SUELEN FORMAR PARTE DEL CÓDIGO FUENTE DEL PROGRAMA QUE SE VA A INSTALAR, MIENTRAS QUE EL VIRUS SE LIMITA A SUPLANTAR EL PROGRAMA ORIGINARIO O A AÑADIRSE.

2. SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO

CÓDIGOS MALICIOSOS: CONCEPTOS BÁSICOS Y TIPOS

TROYANOS

TIENEN UNAS **FINALIDADES COMUNES** COMO:

- CAPACIDAD PARA COMPARTIR ARCHIVOS.
- CAPACIDAD PARA APAGAR Y/O REINICIAR EL SISTEMA.
- CAPACIDAD PARA RECUPERAR CONTRASEÑAS ALMACENADAS EN LA MEMORIA CACHÉ.
- CAPTURA DE PANTALLAS DEL EQUIPO INFECTADO.
- MONITORIZACIÓN DEL TRÁFICO DE RED DEL EQUIPO INFECTADO.
- REDIRECCIÓN DE PUERTOS Y APLICACIONES.
- EJECUCIÓN DE APLICACIONES NO CONTROLADAS POR EL USUARIO.
- EMISIÓN DE MENSAJES E IMÁGENES EN PANTALLA.
- FUNCIONES FUN O DIVERTIDAS: FUNCIONES QUE PRETENDEN MOLESTAR AL USUARIO CUANDO UTILIZA EL EQUIPO. POR EJEMPLO, FUNCIONES DE APERTURA O CIERRE DEL LECTOR DE CD O DVD, INTERCAMBIO DE TECLAS DEL TECLADO, EJECUCIÓN DE ARCHIVOS DE SONIDO, ETC.

2. SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO

CÓDIGOS MALICIOSOS: CONCEPTOS BÁSICOS Y TIPOS

TROYANOS

SU **FUNCIONAMIENTO** SE DIVIDE **EN TRES FASES** DIFERENCIADAS:

1. **ENTRADA AL DISPOSITIVO** O SISTEMA A INFECTAR
2. **CONSOLIDACIÓN DE LA POSICIÓN** DEL CÓDIGO MALICIOSO
3. **COMUNICACIÓN** DEL SISTEMA ATACADO **CON EL EQUIPO DEL ATACANTE**

2. SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO

CÓDIGOS MALICIOSOS: CONCEPTOS BÁSICOS Y TIPOS

COOKIES

LAS **COOKIES** SE DISEÑARON CON LA FINALIDAD DE QUE LOS SITIOS WEB PUDIESEN **DETECTAR Y ALMACENAR LAS PREFERENCIAS DEL USUARIO EN SU NAVEGACIÓN** POR DICHA WEB PARA OFRECER SERVICIOS MÁS ACORDES EN SUS PRÓXIMAS VISITAS.

CON LA EXPANSIÓN DE LA UTILIZACIÓN DE INTERNET Y SERVICIOS WEB, LAS COOKIES **SE HAN CONVERTIDO EN HERRAMIENTAS DE MARKETING** QUE PERMITEN A LAS EMPRESAS CONOCER TODO TIPO DE DETALLES DEL USUARIO CUANDO ESTE NAVEGA POR SUS PÁGINAS WEB.

2. SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO

CÓDIGOS MALICIOSOS: CONCEPTOS BÁSICOS Y TIPOS

COOKIES

LAS COOKIES **NO SE CONSIDERAN DIRECTAMENTE UNA AMENAZA** A LOS EQUIPOS O A SUS ARCHIVOS, PERO SÍ **PUEDEN VULNERAR LA CONFIDENCIALIDAD Y PRIVACIDAD DE LOS USUARIOS**, YA QUE PERMITEN A LAS WEBS EL ALMACENAMIENTO DE LOS REGISTROS DE CADA VISITA DE LOS USUARIOS.

SON ARCHIVOS QUE ALMACENAN EN EL DISCO DURO DEL USUARIO DATOS SOBRE LA UTILIZACIÓN DE SU NAVEGADOR.

2. SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO

CÓDIGOS MALICIOSOS: CONCEPTOS BÁSICOS Y TIPOS

COOKIES

LA INTRODUCCIÓN EN EL SISTEMA SE PRODUCE CADA VEZ QUE EL USUARIO VISITA UNA PÁGINA WEB QUE TENGA HABILITADA LA UTILIZACIÓN DE COOKIES Y **SU FUNCIONAMIENTO SE ESTABLECE EN VARIAS FASES**:

1. LAS **COOKIES SE ENVÍAN DESDE EL SERVIDOR AL NAVEGADOR DEL USUARIO Y SE ALMACENAN EN ÉL**.
2. EL NAVEGADOR **ENVÍA LAS COOKIES AL SERVIDOR CON EL FIN DE IDENTIFICAR AL USUARIO/CLIENTE** Y CONOCER SU COMPORTAMIENTO DE NAVEGACIÓN.

2. SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO

CÓDIGOS MALICIOSOS: CONCEPTOS BÁSICOS Y TIPOS

KEYLOGGERS

SON APLICACIONES DISEÑADAS CON EL FIN DE **REGISTRAR EL COMPORTAMIENTO DE UN USUARIO EN UN ORDENADOR DE MODO REMOTO**.

ALMACENA TODO LO QUE SE ESCRIBE CON EL TECLADO PARA ENVIAR LA INFORMACIÓN AL ATACANTE O TAMBIÉN, LA ALMACENA EN EL DISCO DURO PARA QUE EL ATACANTE LA PUEDA RECUPERAR CUANDO LO REQUIERA.

2. SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO

CÓDIGOS MALICIOSOS: CONCEPTOS BÁSICOS Y TIPOS

KEYLOGGERS

EN GENERAL **ESTÁN DISEÑADOS PARA PASAR INADVERTIDOS** POR PARTE DEL USUARIO Y SU **FUNCIONAMIENTO BÁSICO** CONSISTE EN:

1. CONFIGURACIÓN DE LOS DISTINTOS ASPECTOS DEL KEYLOGGER ATENDIENDO A LA INFORMACIÓN QUE SE PRETENDE OBTENER.
2. INSTALACIÓN DEL KEYLOGGER EN EL EQUIPO VÍCTIMA.
3. RECUPERACIÓN DE LA INFORMACIÓN OBTENIDA Y ALMACENADA POR EL KEYLOGGER.

2. SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO

CÓDIGOS MALICIOSOS: CONCEPTOS BÁSICOS Y TIPOS

SPYWARE

APLICACIÓN DISEÑADA PARA **CONTROLAR EL COMPORTAMIENTO DE LOS USUARIOS CON FINALIDADES LUCRATIVAS**. A PESAR DE LA GRAN VARIEDAD DE SPYWARE **SU FUNCIONAMIENTO SIGUE EL SIGUIENTE PROCEDIMIENTO**:

1. **ENTRADA AL SISTEMA** DEL USUARIO.
2. **RECOLECCIÓN DE LA INFORMACIÓN LOCAL** DEL SISTEMA DEL USUARIO VÍCTIMA.
3. **MONITORIZACIÓN DEL SISTEMA** DEL USUARIO VÍCTIMA.
4. **REGISTRO DE LA ACTIVIDAD** DEL USUARIO.
5. **ACTUACIÓN** DE LAS EMPRESAS DE MARKETING Y PUBLICIDAD **ATENDIENDO A LA INFORMACIÓN OBTENIDA** DEL USUARIO.

2. SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO

CÓDIGOS MALICIOSOS: CONCEPTOS BÁSICOS Y TIPOS

SPYWARE

SON VARIAS E IMPORTANTES LAS DIFERENCIAS QUE EXISTEN ENTRE LOS DISTINTOS **TIPOS DE SPYWARE**, DISTINGUIENDO ENTRE:

- **ADWARE:** APLICACIONES QUE INCLUYEN VENTANAS DE PUBLICIDAD EN SUS INTERFACES DE USUARIO.
- **SCUMWARE:** PERSONALIZAN LA PUBLICIDAD QUE SE MUESTRA EN EL NAVEGADOR DEL USUARIO.
- **BROWSER HIJACKERS:** MODIFICAN CARACTERÍSTICAS DEL EXPLORADOR, ACTUANDO SOBRE EL REGISTRO DEL SISTEMA OPERATIVO.
- **SERVER SIDE SPYWARE:** SPYWARE QUE SE IMPLEMENTA EN LOS SERVIDORES DE LOS ATACANTES EN LUGAR DE INSTALARSE EN EL EQUIPO DEL USUARIO VÍCTIMA.

2. SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO

CÓDIGOS MALICIOSOS: CONCEPTOS BÁSICOS Y TIPOS

GUSANOS O WORMS

SON PROGRAMAS AUTOCONTENIDOS **DISEÑADOS CON EL FIN DE PROPAGARSE DE UN SISTEMA A OTRO** PARA DEGRADAR EL RENDIMIENTO DE SUS RECURSOS.

SU MISIÓN ES SIMPLEMENTE AUTOREPLICARSE, NO PRETENDEN CAUSAR DAÑO DIRECTO, AUNQUE SE PUEDEN ADJUNTAR A OTROS TIPOS DE CÓDIGOS MALICIOSOS COMO COMPLEMENTO.

SU PRINCIPAL **VÍA DE INFECCIÓN** ES POR **ARCHIVOS ADJUNTOS EN CORREOS ELECTRÓNICOS,** UTILIZANDO VULNERABILIDADES DE LOS SERVICIOS DE RED Y A TRAVÉS DE REDES P2P.

2. SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO

SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO

A PESAR DE LAS DISTINTAS CARACTERÍSTICAS QUE TIENEN LAS TIPOLOGÍAS DE CÓDIGO MALICIOSO, **LOS SISTEMAS UTILIZADOS PARA SU DETECCIÓN Y CONTENCIÓN** SON COMUNES ENTRE ELLOS:

- **IDS/IPS.**
- **ANTIVIRUS.**
- **FIREWALL O CORTAFUEGOS.**

2. SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO

SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO

IDS/IPS

SIRVEN PARA **DETECTAR E INFORMAR** A LOS ADMINISTRADORES SOBRE LOS **INTENTOS DE INTRUSIÓN** QUE SE PRODUCEN EN UN EQUIPO, RED O DISPOSITIVO.

PARA SU CORRECTA UTILIZACIÓN **ES NECESARIO UN ALTO NIVEL DE EXPERIENCIA Y CONOCIMIENTO DEL SISTEMA**, DE MODO QUE SUS CONFIGURACIONES PERMITAN EL EQUILIBRIO ENTRE LA DETECCIÓN DE FALSOS POSITIVOS Y FALSOS NEGATIVOS DEFINIDO POR LA ORGANIZACIÓN.

SE CONSIDERAN UNAS HERRAMIENTAS MUY EFICACES PARA LA DETECCIÓN Y PREVENCIÓN DE ACCESOS NO AUTORIZADOS.

2. SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO

SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO

ANTIVIRUS

TIENEN COMO FUNCIÓN **DETECTAR Y ELIMINAR CÓDIGO MALICIOSO**. TAMBIÉN TIENEN **OTRAS FUNCIONES**:

- REVISAN EL CORREO ELECTRÓNICO.
- REVISAN EL HISTORIAL DE PÁGINAS WEB VISITADAS PARA DETECTAR CÓDIGO MALICIOSO OCULTO.
- REVISAN LOS SISTEMAS PARA DETECTAR SI HAY ALGÚN TROYANO O GUSANO.
- REALIZAN TAREAS PROPIAS DE LOS SISTEMAS IDS/IPS Y DE LOS CORTAFUEGOS.

LO HABITUAL ES QUE **SE INSTALEN EN EL SISTEMA OPERATIVO DEL EQUIPO**, AUNQUE **TAMBIÉN HAY EN SERVIDORES O EN REDES** QUE ANALIZAN EL SISTEMA DEL USUARIO DE MODO REMOTO.

2. SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO

SISTEMAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO

FIREWALL O CORTAFUEGOS

SON ELEMENTOS TANTO DE SOFTWARE COMO DE HARDWARE QUE SE UTILIZAN EN UN EQUIPO O EN UNA RED DE EQUIPOS COMO MEDIDA DE CONTROL DE LAS COMUNICACIONES ESTABLECIDAS, PERMITIENDO O DENEGANDO EL ACCESO A LOS SISTEMAS SEGÚN LAS POLÍTICAS DE SEGURIDAD DETERMINADAS POR LA ORGANIZACIÓN.

UN CORTAFUEGOS **FUNCIONA EFICAZMENTE COMO BARRERA PARA EVITAR EL ACCESO DE CÓDIGO MALICIOSO A LOS SISTEMAS DE LA ORGANIZACIÓN, AUNQUE POR SÍ SOLO NO ES SUFICIENTE**: ES NECESARIA LA INSTALACIÓN DE MEDIDAS DE PROTECCIÓN ADICIONALES COMO ANTIVIRUS O SISTEMAS IDS/IPS.

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

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

LA GRAN MAYORÍA DE USUARIOS HAN TENIDO ALGUNA VEZ UNA INFECCIÓN CON CÓDIGO MALICIOSO EN SU EQUIPO.

PARA DETECTAR, CONTENER Y ELIMINAR LAS AMENAZAS **HAY MUCHAS HERRAMIENTAS** QUE SE DEDICAN A AUTOMATIZAR ESTOS PROCESOS.

POR ELLO **SE DEBE ELEGIR ENTRE UNAS U OTRAS** DEPENDIENDO DE LA TOPOLOGÍA DE LA INSTALACIÓN Y DE LAS VÍAS DE INFECCIÓN QUE SE PRETENDEN CONTROLAR.

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

VEAMOS LAS CARACTERÍSTICAS GENERALES DE VARIOS ANTIVIRUS, RECOMENDADOS POR LA REVISTA PCWORD PARA EL AÑO 2022:

NORTON 360 DELUXE

MCAFEE TOTAL PROTECTION

BITDEFENDER TOTAL SECURITY

BULLGUARD PREMIUM PROTECTION

ESET SMART SECURITY PREMIUM

KASPERSKY SECURITY CLOUD

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

NORTON 360 DELUXE

RECIBE ESTE NOMBRE PORQUE OFRECE SEGURIDAD COMPLETA PARA PROTEGER TODOS TUS DISPOSITIVOS, ASÍ COMO ALERTARTE EN CASO DE QUE TUS CLAVES DE ACCESO Y CONTRASEÑAS SE ENCUENTREN A LA VENTA EN LA WEB OSCURA.

ESTA APLICACIÓN ESTÁ DISPONIBLE PARA WINDOWS, MAC, IOS Y ANDROID, POR LO QUE ESTE ANTIVIRUS ESTÁ PENSADO PARA CUALQUIER USUARIO. EN LOS ANÁLISIS DE AV-TEST MÁS RECIENTES, CONSIGUIÓ BUENÍSIMOS RESULTADOS EN CUANTO A PROTECCIÓN Y FACILIDAD DE USO.

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

NORTON 360 DELUXE

DESTACA UNA PROTECCIÓN CONTRA LOS VIRUS EXCELENTE, ASÍ COMO PROTECCIÓN PARA NAVEGACIÓN WEB, PROTECCIÓN CONTRA EL PHISHING, UN SERVICIO VPN Y UN GESTOR DE CONTRASEÑAS. TAMBIÉN TIENES 50 GB DE ALMACENAMIENTO EN LA NUBE Y HERRAMIENTAS PARA ACELERAR TU ORDENADOR.

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

NORTON 360 DELUXE

PROS

- EXCELENTE PROTECCIÓN CONTRA MALWARE
- PROTECCIÓN DE IDENTIDAD
- VPN ILIMITADA

CONTRAS

- COPIA DE SEGURIDAD SOLO EN WINDOWS
- FUNCIONES LIMITADAS EN IOS Y MACOS

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

MCAFEE TOTAL PROTECTION

EL MCAFEE TOTAL PROTECTION PROMETE “PROTECCIÓN TOTAL”. LOS USUARIOS DE MCAFEE PUEDEN ESTAR TRANQUILOS, OFRECE PROTECCIÓN EN MUCHOS ASPECTOS.

TE SERÁN ÚTILES SUS MÚLTIPLES FUNCIONES, DESDE LA NUEVA **PROTECCIÓN CRIPTOJACKING** A SU GESTOR DE CONTRASEÑAS, ASÍ COMO LA POSIBILIDAD PARA CREAR UNA CARPETA PROTEGIDA CON CONTRASEÑA.

LA PROTECCIÓN CONTRA MALWARE ES TAMBIÉN EXCELENTE, AUNQUE NO TE RECOMENDAMOS QUE PAGUES DINERO EXTRA PARA OBTENER TAMBIÉN EL VPN DE MCAFEE.

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

MCAFEE TOTAL PROTECTION

PROS

- MUY FÁCIL DE USAR
- VPN ILIMITADA
- PROTECCIÓN DE IDENTIDAD

CONTRAS

- CONTROLES PARENTALES NO EFECTIVOS
- VPN SIN KILL SWITCH

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

BITDEFENDER TOTAL SECURITY

ADEMÁS DE DARTE LA POSIBILIDAD DE ESCANEAR DOCUMENTOS Y SISTEMAS, HAY UN ESCÁNER DEDICADO A ENCONTRAR SOFTWARE QUE NECESITE ACTUALIZARSE, ASÍ COMO CONTRASEÑAS DÉBILES.

TAMBIÉN OFRECE PROTECCIÓN CONTRA NUEVAS Y EMERGENTES AMENAZAS COMO PUEDE SER EL **RANSOMWARE**.

SE TRATA DE LA FUNCIÓN *NETWORK THREAT PREVENTION* QUE ELIMINA AMENAZAS ANTES DE QUE ACTÚEN.

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

BITDEFENDER TOTAL SECURITY

TIENE UN GESTOR DE CONTRASEÑAS, UN CONTROL PARENTAL, HERRAMIENTAS ANTI-TRACKING Y UNA VPN CON 200 MB AL DÍA POR DISPOSITIVO.

EN EL ÚLTIMO INFORME DE AV-TEST, CONSIGUIÓ ELIMINAR TODO EL MALWARE.

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

BITDEFENDER TOTAL SECURITY

PROS	CONTRAS
• EXCELENTE PROTECCIÓN CONTRA MALWARE	• VPN LIMITADA A 200 MB AL DÍA
• PORTAL DE GESTIÓN	• SIN PROTECCIÓN DE IDENTIDAD

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

BULLGUARD PREMIUM PROTECTION

DISEÑADO ESPECIALMENTE PARA HOGARES, TIENE UN ESCÁNER DE REDES QUE PROTEGERÁ CUALQUIER DISPOSITIVO CONECTADO A INTERNET, ADEMÁS OFRECER UNA RÁPIDA DETECCIÓN DE MALWARE.

OTRA DE LAS FUNCIONES DESTACADAS ES UN BUSCADOR QUE RASTREARÁ CUALQUIER FILTRACIÓN QUE SE HAGA EN LA WEB DE TU NOMBRE, CORREO ELECTRÓNICO Y DETALLES BANCARIOS. TAMBIÉN TE OFRECERÁ CONSEJO EN EL CASO DE QUE TUS DATOS PERSONALES HAYAN SIDO VULNERADOS.

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

BULLGUARD PREMIUM PROTECTION

LA OPCIÓN DE CONTROL PARENTAL PUEDE ACTIVARSE EN LOS DISPOSITIVOS MÓVILES DE LOS MÁS PEQUEÑOS, CON LA QUE PODRÁS VER SUS LLAMADAS, MENSAJES Y FOTOS, ASÍ COMO CONTROLAR SU LOCALIZACIÓN.

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

BULLGUARD PREMIUM PROTECTION

PROS	CONTRAS
• PROTECCIÓN DE IDENTIDAD INCLUIDA • EXCELENTE PROTECCIÓN CONTRA MALWARE	• SIN VPN

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

ESET SMART SECURITY PREMIUM

LA INTERFAZ DEL ESET SMART SECURITY ES MUY SIMPLE, SIN FLORITURAS, PERO ESO NO SIGNIFICA QUE NO OFREZCA UNA AMPLIA GAMA DE PRESTACIONES MUY IMPRESIONANTES (AUNQUE TAMBIÉN BASTANTE COMPLEJAS).

ENTRE ELLAS, SOLO LOS CONTROLES PARENTALES Y LA CONFIGURACIÓN DE CORTAFUEGOS NOS DECEPCIONAN UN POCO. TAMBIÉN MERECE LA PENA DECIR QUE NO SE OFRECE NINGUNA VPN NI NADA PARA PROTEGER Y MONITORIZAR TU IDENTIDAD.

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

ESET SMART SECURITY PREMIUM

POR SUERTE, LA PRINCIPAL PROTECCIÓN ANTE MALWARE (TAMBIÉN INCLUYE PROTECCIÓN CONTRA RANSOMWARE) ES TOTALMENTE SÓLIDA.

SÍ QUE IMPACTA NEGATIVAMENTE SOBRE SU RENDIMIENTO UN POCO, ESPECIALMENTE AL INSTALAR APPS, PERO ESO ES ALGO QUE NO HARÁS A MENUDO.

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

ESET SMART SECURITY PREMIUM

PROS

- PROTECCIÓN CONTRA MALWARE SÓLIDA
- MUCHAS PRESTACIONES PARA USUARIOS EXIGENTES

CONTRAS

- SIN PROTECCIÓN DE IDENTIDAD
- SIN VPN

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

KASPERSKY SECURITY CLOUD

A SIMPLE VISTA, NO HAY NADA QUE NOS HAGA DECANTAR POR EL KASPERSKY SECURITY CLOUD O POR EL KASPERSKY TOTAL SECURITY. AMBOS DISPONEN DE LAS HERRAMIENTAS PRINCIPALES DE UN ANTIVIRUS, POR LO QUE APOSTAR POR UNO U OTRO PARECE UNA BUENA IDEA.

LO QUE HACE AL ANTIVIRUS SECURITY CLOUD DIFERENTE ES QUE DISPONE DE UNA TECNOLOGÍA DE SEGURIDAD QUE SE ADAPTA AUTOMÁTICAMENTE A TU USO. ASÍ, TU CONFIGURACIÓN SE AJUSTARÁ SEGÚN QUÉ ACTIVIDADES HAGAS UTILIZANDO INTERNET.

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

KASPERSKY SECURITY CLOUD

ESTE ANTIVIRUS, ADEMÁS, TE AYUDARÁ A DETECTAR DISPOSITIVOS NO AUTORIZADOS O PÁGINAS WEB ALGO DUDOSAS Y A BLOQUEAR ADWARE, ASÍ COMO A CREAR CONTRASEÑAS FUERTES Y SEGURAS Y A GESTIONARLAS DE MANERA EFICAZ.

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

KASPERSKY SECURITY CLOUD

PROS	CONTRAS
• EXCELENTE PROTECCIÓN CONTRA MALWARE • PROTECCIÓN DE IDENTIDAD	• EL HOME NETWORK MONITOR NO ES MUY ÚTIL

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

4. CRITERIOS DE SEGURIDAD PARA LA CONFIGURACIÓN DE LAS HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

PARA DETECTAR ESTOS ATAQUES SE ENUMERAN A CONTINUACIÓN UNA SERIE DE **SÍNTOMAS** QUE PUEDEN SER **INDICIOS DE QUE HAY UNA INFECCIÓN** EN EL EQUIPO O EN EL SISTEMA:

- LAS APLICACIONES CARGAN LENTAMENTE O TARDAN EN CARGAR (BAJO RENDIMIENTO).
- APARECEN ARCHIVOS DESCONOCIDOS EN EL DISCO DURO.
- DESAPARECEN DEL DISCO DURO ARCHIVOS NECESARIOS PARA EJECUTAR ALGUNA APLICACIÓN HABITUAL.
- LA PANTALLA NO SE COMPORTA DE UNA FORMA HABITUAL.
- HAY CAMBIOS REPENTINOS EN EL TAMAÑO DE LOS ARCHIVOS RESPECTO A SU TAMAÑO ORIGINAL.

4. CRITERIOS DE SEGURIDAD PARA LA CONFIGURACIÓN DE LAS HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

SÍNTOMAS

- EL SISTEMA OPERATIVO SE RESETEA INESPERADAMENTE.
- EL SISTEMA OPERATIVO MUESTRA ALGÚN MENSAJE DE ERROR O NO SE INICIA CORRECTAMENTE.
- SE CARGAN APLICACIONES DESCONOCIDAS O EXTRAÑAS AL INICIAR EL SISTEMA OPERATIVO.
- LAS APLICACIONES TIENEN COMPORTAMIENTOS ERRÓNEOS O INESPERADOS.

4. CRITERIOS DE SEGURIDAD PARA LA CONFIGURACIÓN DE LAS HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

PARA EVITAR ESTAS INFECCIONES E INTRUSIONES SE RECOMIENDA QUE **LAS HERRAMIENTAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO Y QUE LOS SISTEMAS OPERATIVOS Y APLICACIONES DE UN EQUIPO SE CONFIGUREN SIGUIENDO UNOS CRITERIOS DE SEGURIDAD PREVENTIVOS**:

- MANTENER LOS SISTEMAS OPERATIVOS, LAS HERRAMIENTAS Y LAS APLICACIONES ACTUALIZADAS.
- IMPLEMENTAR SOFTWARE ANTIVIRUS EN EQUIPOS, ARCHIVOS Y SERVIDORES DE CORREO.
- IMPLEMENTAR SOFTWARE DE ADMINISTRACIÓN DE CONTENIDOS.
- CONFIGURAR LAS HERRAMIENTAS DE CONTENCIÓN DE CÓDIGO MALICIOSO ATENDIENDO A LAS POLÍTICAS DE FILTRADO DE CONTENIDOS DEFINIDA EN LA ORGANIZACIÓN.

4. CRITERIOS DE SEGURIDAD PARA LA CONFIGURACIÓN DE LAS HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

- IMPLEMENTAR HERRAMIENTAS DE BÚSQUEDA Y ACTUALIZACIÓN DE VULNERABILIDADES.
- IMPLEMENTAR UN SISTEMA DE ALARMAS EN LA HERRAMIENTA DE CONTENCIÓN DE CÓDIGO MALICIOSO.
- UTILIZAR CLAVES Y CONTRASEÑAS DE ALTA SEGURIDAD.
- REALIZACIÓN PERIÓDICA DE COPIAS DE SEGURIDAD DEL SISTEMA OPERATIVO.
- NAVEGAR POR PÁGINAS WEB SEGURAS Y DE CONFIANZA, CONFIGURANDO LAS HERRAMIENTAS Y NAVEGADORES PARA QUE BLOQUEEN TEMPORALMENTE LAS WEBS POTENCIALMENTE PELIGROSAS.
- IMPLEMENTAR UN CORTAFUEGOS.
- CONFIGURAR EL NAVEGADOR PARA QUE RECHACEN LOS DIFERENTES TIPOS DE COOKIES.

4. CRITERIOS DE SEGURIDAD PARA LA CONFIGURACIÓN DE LAS HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

LA **CONFIGURACIÓN DE LAS HERRAMIENTAS DE CONTENCIÓN Y DETECCIÓN DE CÓDIGO MALICIOSO ES FUNDAMENTAL** PARA UNA PROTECCIÓN ADECUADA DE LOS EQUIPOS.

SE RECOMIENDA QUE **ADEMÁS** DE LAS HERRAMIENTAS ANTI-MALWARE **SE CONFIGUREN LOS DISTINTOS ELEMENTOS QUE FORMAN PARTE DEL SISTEMA OPERATIVO Y DE LAS APLICACIONES** PARA QUE, ANTE FALLOS DE LAS HERRAMIENTAS, EL EQUIPO NO QUEDE COMPLETAMENTE DESPROTEGIDO Y HAYA UNA BARRERA MÁS DE PROTECCIÓN.

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

5. DETERMINACIÓN DE LOS REQUERIMIENTOS Y TÉCNICAS DE ACTUALIZACIÓN DE LAS HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

ATENDIENDO A LA NORMA **ISO 27001**, **EL RESPONSABLE DE SEGURIDAD DEBE DEFINIR LOS CONTROLES DE DETECCIÓN Y PREVENCIÓN PARA LA PROTECCIÓN CONTRA EL SOFTWARE MALICIOSO**.

ADEMÁS, DEBE DESARROLLAR **PROCEDIMIENTOS ADECUADOS DE CONCIENCIACIÓN** DE USUARIOS EN CUANTO A SEGURIDAD, CONTROLES DE ACCESO AL SISTEMA Y ADMINISTRACIÓN DE CAMBIOS.

5. DETERMINACIÓN DE LOS REQUERIMIENTOS Y TÉCNICAS DE ACTUALIZACIÓN DE LAS HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

ACCIONES Y REQUERIMIENTOS PARA UN CORRECTO CONTROL DE ACCESOS

LOS CONTROLES DEBEN COMPRENDER UNA SERIE DE ACCIONES COMO:

- **PROHIBIR LA INSTALACIÓN Y USO DE SOFTWARE NO AUTORIZADO** POR LA ORGANIZACIÓN.
- **REDACTAR PROCEDIMIENTOS PARA EVITAR RIESGOS RELACIONADOS CON OBTENCIÓN DE ARCHIVOS Y SOFTWARE EXTERNOS** A TRAVÉS DE REDES, O POR CUALQUIER OTRO MEDIO, SEÑALANDO LAS MEDIDAS DE PROTECCIÓN A TOMAR.
- **INSTALAR Y ACTUALIZAR PERIÓDICAMENTE EL SOFTWARE DE DETECCIÓN Y REPARACIÓN** DE VIRUS, EXAMINANDO LOS EQUIPOS Y MEDIOS INFORMÁTICOS.
- **REVISAR PERIÓDICAMENTE EL CONTENIDO DEL SOFTWARE Y LOS DATOS DE LOS EQUIPOS** QUE SUSTENTAN PROCESOS CRÍTICOS DE LA ORGANIZACIÓN.
- **CONCIENCIAR AL PERSONAL** SOBRE EL PROBLEMA DE LOS FALSOS ANTIVIRUS, DE LAS CADENAS FALSAS Y DE CÓMO PROCEDER FRENTE A LOS MISMOS.

5. DETERMINACIÓN DE LOS REQUERIMIENTOS Y TÉCNICAS DE ACTUALIZACIÓN DE LAS HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

ACCIONES Y REQUERIMIENTOS PARA UN CORRECTO CONTROL DE ACCESOS

- **MANTENER LOS SISTEMAS AL DÍA** CON LAS ÚLTIMAS ACTUALIZACIONES DE SEGURIDAD DISPONIBLES. SE RECOMIENDA REALIZAR PREVIAMENTE PRUEBAS Y COMPROBACIONES EN UN ENTORNO DE PRUEBA SI LAS ACTUALIZACIONES PROVOCAN CAMBIOS CRÍTICOS EN EL SISTEMA.
- **VERIFICAR PREVIAMENTE LA PRESENCIA DE VIRUS** EN ARCHIVOS DE MEDIOS ELECTRÓNICOS DE ORIGEN INCIERTO O EN ARCHIVOS RECIBIDOS A TRAVÉS DE REDES POCO CONFIABLES.
- **REDACTAR PROCEDIMIENTOS** PARA VERIFICAR LA INFORMACIÓN RELATIVA A SOFTWARE MALICIOSO, GARANTIZANDO QUE LOS MENSAJES DE ALERTA SEAN EXACTOS E INFORMATIVOS.
- **REDACTAR NORMAS DE PROTECCIÓN** Y HABILITACIÓN DE PUERTOS DE CONEXIÓN DE DISPOSITIVOS MÓVILES Y SUS DERECHOS DE ACCESO.

5. DETERMINACIÓN DE LOS REQUERIMIENTOS Y TÉCNICAS DE ACTUALIZACIÓN DE LAS HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

ACCIONES Y REQUERIMIENTOS PARA UN CORRECTO CONTROL DE ACCESOS

LA **ISO 27001** SE ESTABLECE UNA SERIE DE **REQUERIMIENTOS Y TÉCNICAS DE ACTUALIZACIÓN** PARA LAS HERRAMIENTAS DE CONTROL Y CONTENCIÓN DE CÓDIGO MALICIOSO:

- **PROTECCIÓN ANTIVIRUS CONTINUA**, 24 HORAS AL DÍA LOS 7 DÍAS DE LA SEMANA.
- **HERRAMIENTAS DE ACTUALIZACIÓN AUTOMÁTICA Y CONTINUA**, QUE NO PROVOQUEN INTERRUPCIONES EN EL TRABAJO.
- **GENERACIÓN PERIÓDICA DE INFORMES Y ESTADÍSTICAS**. GESTIÓN AVANZADA DE INFORMES.
- **PROTECCIÓN PARA TODO TIPO DE SERVIDORES** (LINUX, WINDOWS, ETC.).
- **DETECCIÓN DE VIRUS EN TIEMPO REAL**.
- REALIZACIÓN DE **COPIAS DE SEGURIDAD Y DISCOS DE ARRANQUE** PERIÓDICOS.

5. DETERMINACIÓN DE LOS REQUERIMIENTOS Y TÉCNICAS DE ACTUALIZACIÓN DE LAS HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

ACCIONES Y REQUERIMIENTOS PARA UN CORRECTO CONTROL DE ACCESOS

- **MÉTODOS DE ESCANEO Y ANÁLISIS DE POSIBLES CÓDIGOS MALICIOSOS** QUE PERMITAN LA DETECCIÓN DE VIRUS ANÓMALOS Y DESCONOCIDOS.
- **COMPROBACIÓN Y SEGURIDAD REMOTA** DEL ESTADO DE LOS EQUIPOS Y DISPOSITIVOS.
- **UTILIZACIÓN DE DISTINTOS MÉTODOS** DE ESCANEO, DETECCIÓN Y ELIMINACIÓN DE CÓDIGOS MALICIOSOS PARA INCREMENTAR EL GRADO DE PROTECCIÓN DE LOS EQUIPOS.
- **FACILIDAD DE MANEJO Y GESTIÓN** DE LAS HERRAMIENTAS DE PROTECCIÓN Y CONTENCIÓN.
- **ADMINISTRACIÓN CENTRALIZADA** EN LA QUE SE PUEDAN RECIBIR REPORTES DE VIRUS, ACTUALIZACIONES Y PERSONALIZAR CONFIGURACIONES SEGÚN EL TIPO DE USUARIO.

5. DETERMINACIÓN DE LOS REQUERIMIENTOS Y TÉCNICAS DE ACTUALIZACIÓN DE LAS HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

ADEMÁS, NO HAY QUE OLVIDAR QUE **LAS HERRAMIENTAS DEBEN CONTROLAR Y PROTEGER LAS DISTINTAS VÍAS DE ACCESO** DE UN MODO PERSONALIZADO PARA CADA UNA DE ELLAS:

- **SISTEMAS DE FICHERO**
- **RED LOCAL**
- **CORREO ELECTRÓNICO**
- **NAVEGADORES**

5. DETERMINACIÓN DE LOS REQUERIMIENTOS Y TÉCNICAS DE ACTUALIZACIÓN DE LAS HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

SISTEMAS DE FICHERO

PUEDE SER CUALQUIER DISPOSITIVO QUE SOPORTE SISTEMAS DE ARCHIVO. **LAS HERRAMIENTAS PARA PROTEGERLOS DEBEN CUMPLIR UNA SERIE DE REQUERIMIENTOS**:

- LOS PROGRAMAS ANTIVIRUS DEBEN ESTAR INSTALADOS TANTO EN CLIENTES COMO EN SERVIDORES.
- DEBEN REALIZAR UNA GESTIÓN EFICIENTE DEL ESCRITORIO, CONTROLANDO Y REALIZANDO UN INVENTARIO DEL SOFTWARE INSTALADO EN EL DISPOSITIVO.
- DEBE GESTIONAR LAS VULNERABILIDADES DEL SISTEMA, DEBIENDO IDENTIFICARLAS Y PARCHEARLAS DE MODO AUTOMÁTICO.
- DEBEN OFRECER UNA PROTECCIÓN ESPECIAL A CÓDIGOS MALICIOSOS ADWARE Y SPYWARE.

5. DETERMINACIÓN DE LOS REQUERIMIENTOS Y TÉCNICAS DE ACTUALIZACIÓN DE LAS HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

RED LOCAL

EN UNA GRAN MAYORÍA DE VECES LA TRANSMISIÓN DE CÓDIGOS MALICIOSOS SE PRODUCE A TRAVÉS DE LA RED LOCAL. POR ELLO, LAS HERRAMIENTAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGOS MALICIOSOS **DEBEN PRESTAR UNA PROTECCIÓN ESPECIAL A LA RED LOCAL** PARA IMPEDIR SU PROPAGACIÓN.

SE RECOMIENDA **REALIZAR UNA CONFIGURACIÓN CENTRALIZADA DE LOS CORTAFUEGOS** DE LOS DISPOSITIVOS QUE FORMAN PARTE DE LA RED LOCAL, ADEMÁS DEL **ESTABLECIMIENTO DE POLÍTICAS CENTRALIZADAS DE SEGURIDAD Y RESPUESTA** ANTE DETECCIÓN DE INTRUSIONES.

5. DETERMINACIÓN DE LOS REQUERIMIENTOS Y TÉCNICAS DE ACTUALIZACIÓN DE LAS HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

CORREO ELECTRÓNICO

LAS HERRAMIENTAS DEBEN CONTENER **PROGRAMAS ANTIVIRUS ESPECIALIZADOS PARA CONTROLAR Y DETECTAR CÓDIGOS MALICIOSOS EN LOS CORREOS ELECTRÓNICOS** QUE CIRCULAN POR LOS EQUIPOS Y DISPOSITIVOS DE LA ORGANIZACIÓN.

ESTOS PROGRAMAS **DEBEN CONTROLAR Y VERIFICAR LA INEXISTENCIA DE CÓDIGO MALICIOSO EN LA ENTRADA DE CORREOS ELECTRÓNICOS Y**, ADEMÁS, TAMBIÉN **DEBEN REALIZAR COMPROBACIONES CONSTANTES EN AQUELLOS SERVIDORES QUE ALMACENEN BUZONES DE CORREO ELECTRÓNICO.**

5. DETERMINACIÓN DE LOS REQUERIMIENTOS Y TÉCNICAS DE ACTUALIZACIÓN DE LAS HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

CORREO ELECTRÓNICO

TODO ELLO DEBE COMPLEMENTARSE CON LA IMPLEMENTACIÓN DE **POLÍTICAS DE SEGURIDAD ESPECÍFICAS PARA CORREO ELECTRÓNICO** EN LA GESTIÓN DE LA SEGURIDAD DE UNA ORGANIZACIÓN.

5. DETERMINACIÓN DE LOS REQUERIMIENTOS Y TÉCNICAS DE ACTUALIZACIÓN DE LAS HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

NAVEGADORES

LAS HERRAMIENTAS DE PROTECCIÓN ANTE CÓDIGOS MALICIOSOS **DEBEN PROTEGER LA ACTIVIDAD Y ACCIONES DE LOS NAVEGADORES** INSTALADOS TANTO EN LOS SERVIDORES COMO EN LOS EQUIPOS CLIENTE DE LA RED DE LA ORGANIZACIÓN.

PARA UNA PROTECCIÓN ADECUADA NAVEGADORES CORRECTAMENTE Y DE UN MODO ACORDE A LAS POLÍTICAS DE SEGURIDAD ESTABLECIDAS PREVIAMENTE Y HAY QUE **INSTALAR PROGRAMAS ANTIVIRUS QUE REALICEN ANÁLISIS PERIÓDICOS Y SEAN CAPACES DE DETECTAR CÓDIGOS MALICIOSOS EN** LOS DISTINTOS **NAVEGADORES** DE LOS EQUIPOS.

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

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

NO ES SUFICIENTE CON IMPLEMENTAR HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO.

LAS HERRAMIENTAS DE PROTECCIÓN EN LAS ORGANIZACIONES YA FORMAN UNA INFRAESTRUCTURA TAN COMPLEJA QUE **CUESTA LLEVAR A CABO UN CONTROL** PORMENORIZADO Y MANUAL DE TODAS ELLAS.

UNA SOLUCIÓN ÚTIL ES EL ANÁLISIS DE EVENTOS DE SEGURIDAD CENTRALIZADO A TRAVÉS DE **AUDITORÍAS DE SEGURIDAD INFORMÁTICA.**

SE CONCIBEN PARA ANALIZAR Y MEDIANTE UNA SERIE DE PRUEBAS REALIZADAS POR PERSONAL INDEPENDIENTE.

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

ESTAS AUDITORÍAS **RESPONDEN A PREGUNTAS COMO**:

- *¿ES ADECUADA LA SEGURIDAD DE LOS EQUIPOS Y DISPOSITIVOS?*
- *¿LA INFORMACIÓN ESTÁ ALMACENADA EN MEDIOS FIABLES? ¿EXISTE LA POSIBILIDAD DE QUE HAYA PÉRDIDAS DE INFORMACIÓN IRREVERSIBLES?*
- *¿LA SEGURIDAD DE LOS SISTEMAS PERMITE LA CONSECUCIÓN DE LOS OBJETIVOS Y LAS METAS DE LA ORGANIZACIÓN?*
- *¿LA INFRAESTRUCTURA DE SEGURIDAD ES EFICIENTE? ¿SE APROVECHAN LOS RECURSOS DE UN MODO ADECUADO?*

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

REQUISITOS Y FUNCIONALIDADES DE LAS AUDITORÍAS DE SEGURIDAD

CON LAS AUDITORÍAS DE SEGURIDAD EN LAS ORGANIZACIONES SE CONSIGUE INFORMACIÓN MUY VALIOSA QUE PUEDE DETERMINAR SI LAS POLÍTICAS Y MEDIDAS DE SEGURIDAD APLICADAS SON CORRECTAS, SUFICIENTES Y ADECUADAS.

PARA ELLO, UNA AUDITORÍA DE SEGURIDAD ADECUADA DEBE RESPONDER A **FUNCIONALIDADES** COMO:

- ANÁLISIS DE LOS COSTES QUE SUPONDRÍA UNA RUPTURA DE LA SEGURIDAD DE LA INFORMACIÓN.
- INFORME DE LA SITUACIÓN ACTUAL DE LOS EQUIPOS Y DISPOSITIVOS Y EL NIVEL DE SEGURIDAD ESTABLECIDO EN CADA UNO DE ELLOS.

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

REQUISITOS Y FUNCIONALIDADES DE LAS AUDITORÍAS DE SEGURIDAD

- AUDITORÍAS DE SEGURIDAD DE LOS DISTINTOS SISTEMAS DE INFORMACIÓN DE LA ORGANIZACIÓN.
- PRUEBAS Y TEST DE INTRUSIONES.
- BÚSQUEDA DE VULNERABILIDADES EN LOS SISTEMAS.
- PREVENCIÓN DE ATAQUES MEDIANTE ANTIVIRUS Y ANTISPYWARE, ENTRE OTRAS HERRAMIENTAS DE PREVENCIÓN.
- CONTROL DE ACCESO A LOS SISTEMAS Y A LAS APLICACIONES INSTALADAS EN ELLOS.
- ANÁLISIS DE REGISTROS DE SEGURIDAD (O LOGS) PARA DETECTAR LOS ATAQUES PRODUCIDOS.

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

LOS ARCHIVOS DE REGISTRO O ARCHIVOS DE LOG

LOS ARCHIVOS DE REGISTRO O ARCHIVOS DE LOG SON **UNA FUENTE IMPORTANTE DE SEGURIDAD Y DE SOLUCIÓN DE PROBLEMAS**: SON ARCHIVOS EN LOS QUE SE ENCUENTRA INFORMACIÓN DIVERSA DE UN SISTEMA.

A TRAVÉS DE ELLOS **SE PUEDE ANALIZAR INFORMACIÓN** Y CONOCER EL TRÁFICO DE LA RED, LAS APLICACIONES UTILIZADAS Y LOS USUARIOS QUE HAN ACCEDIDO A CADA APLICACIÓN Y QUÉ HAN HECHO CON ESTAS.

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

LOS ARCHIVOS DE REGISTRO O ARCHIVOS DE LOG

PERMITEN DESCUBRIR POSIBLES ATAQUES A LOS SISTEMAS, DETECTANDO INFORMACIÓN SOBRE PROBLEMAS O INCIDENCIAS DE SEGURIDAD PRODUCIDAS EN ELLOS.

SE GENERA **INFORMACIÓN SOBRE LAS ACTIVIDADES DE LOS ADMINISTRADORES Y USUARIOS** Y SI SE EMPLEAN LAS HERRAMIENTAS Y PROCEDIMIENTOS ADECUADOS **SE PUEDE CONSEGUIR INFORMACIÓN SOBRE VIOLACIONES DE LA SEGURIDAD DEL SISTEMA** Y OTROS DATOS PARA **COMPROBAR EL GRADO DE CUMPLIMIENTO** DE LAS POLÍTICAS DE SEGURIDAD DEFINIDAS EN UNA ORGANIZACIÓN.

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

LOS ARCHIVOS DE REGISTRO O ARCHIVOS DE LOG

LOS LOGS, COMO MÍNIMO, DEBEN REGISTRAR INFORMACIÓN SOBRE:

- **INTENTOS DE ACCESO AL SISTEMA** O A ALGUNA APLICACIÓN, TANTO EXITOSOS COMO FALLIDOS.
- **IDENTIDAD DEL USUARIO**.
- **FECHA** DEL INTENTO DE ACCESO.
- **TIEMPO** DE CADA **INTENTO DE ENTRADA**.
- **FECHA Y TIEMPO DE SALIDA** DEL SISTEMA O DE LA APLICACIÓN.
- **DISPOSITIVOS UTILIZADOS** EN LA CONEXIÓN.
- **LAS ACTIVIDADES Y FUNCIONES EJECUTADAS** POR EL USUARIO QUE HA ACCEDIDO.

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

LOS ARCHIVOS DE REGISTRO O ARCHIVOS DE LOG

CON ESTA INFORMACIÓN FACILITADA LOS REGISTROS DE AUDITORÍA SIRVEN PARA AYUDAR A LOS RESPONSABLES DE SEGURIDAD A TENER CONTROLADA UNA SERIE DE ASPECTOS:

- **RECONSTRUCCIÓN DE EVENTOS:** CON UNA REVISIÓN DE LOS LOGS SE PUEDE REALIZAR UN SEGUIMIENTO DE LAS ÚLTIMAS OPERACIONES LLEVADAS A CABO EN EL SISTEMA Y DETECTAR CÓMO, CUÁNDO Y POR QUÉ SE HA GENERADO CUALQUIER INCIDENCIA DE SEGURIDAD. CON EL ANÁLISIS DE LOS LOGS TAMBIÉN SE PUEDE DETECTAR CÓMO SE ORIGINÓ LA INCIDENCIA, SI FUE POR ALGÚN ERROR DEL SOFTWARE O SI, POR EL CONTRARIO, LA GENERÓ ALGÚN USUARIO. ADEMÁS, SI HAY ALGUNA PÉRDIDA DE DATOS EL ANÁLISIS DE LOGS PUEDE AYUDAR EN SU PROCESO DE RECUPERACIÓN.

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

LOS ARCHIVOS DE REGISTRO O ARCHIVOS DE LOG

- **CONTROL DE ACCESO:** A TRAVÉS DE LOS LOGS SE PUEDEN CONOCER LAS ACCIONES QUE LOS USUARIOS AUTORIZADOS REALIZAN Y ASÍ PODER EVALUAR Y TOMAR DECISIONES SOBRE LA ASIGNACIÓN DE AUTORIZACIONES Y PERMISOS DE USUARIO.
- **DETECCIÓN DE INTRUSOS:** LOS REGISTROS DE AUDITORÍA SE PUEDEN DISEÑAR E IMPLEMENTAR DE MODO QUE SEAN UN APOYO A LA DETECCIÓN DE INTRUSIONES. CONFIGURADOS CORRECTAMENTE PUEDEN LLEGAR A DETECTAR INTRUSIONES A TIEMPO REAL O DESPUÉS DE HABERSE PRODUCIDO EL INCIDENTE DE SEGURIDAD. PARA ELLO ES BÁSICA LA MONITORIZACIÓN DE ESTOS REGISTROS PARA QUE GENEREN MENSAJES DE ADVERTENCIA Y ALARMAS EN CUANTO SE PRODUZCA ALGÚN INTENTO DE INTRUSIÓN.

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

LOS ARCHIVOS DE REGISTRO O ARCHIVOS DE LOG

OTRO ASPECTO IMPORTANTE DE LOS FICHEROS DE REGISTRO ES LA NECESIDAD DE **REALIZAR REVISIONES PERIÓDICAS PARA DETECTAR LAS ALARMAS Y LOS MENSAJES DE ADVERTENCIA** GENERADOS.

ESTOS MENSAJES PUEDEN APORTAR INFORMACIÓN SOBRE LOS INTENTOS DE CONEXIONES SIN ÉXITO, PERO TAMBIÉN PUEDEN DAR UNA ABUNDANTE INFORMACIÓN QUE NO TIENE NADA QUE VER CON LA SEGURIDAD DEL SISTEMA.

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

LOS ARCHIVOS DE REGISTRO O ARCHIVOS DE LOG

LA REVISIÓN DE ESTOS MENSAJES PUEDE SER UNA TAREA BASTANTE TEDIOSA DEBIDO A LA GRAN CANTIDAD DE INFORMACIÓN IRRELEVANTE Y LO MÁS HABITUAL ES LA **UTILIZACIÓN DE HERRAMIENTAS ESPECIALIZADAS EN ANÁLISIS DE FICHEROS DE REGISTRO QUE PROPORCIONAN SOLO LA INFORMACIÓN RELEVANTE.**

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

LOS ARCHIVOS DE REGISTRO O ARCHIVOS DE LOG

LAS HERRAMIENTAS PUEDEN EJECUTAR LOS ANÁLISIS DE DOS MODOS:

- **REALIZANDO COMPROBACIONES PERIÓDICAS.** TIENEN COMO VENTAJA QUE SOLO SE EJECUTAN UNA VEZ CADA CIERTO TIEMPO, LO QUE IMPLICA QUE LA UTILIZACIÓN DE RECURSOS ES ESCASA Y POR CORTOS PERIODOS DE TIEMPO. ES NECESARIO CONFIGURAR LAS HERRAMIENTAS PARA QUE ANALICEN SOLO LOS REGISTROS NUEVOS PARA EVITAR PÉRDIDAS DE EFICIENCIA.
- **REALIZANDO COMPROBACIONES CONSTANTES** MEDIANTE LA LECTURA CONTINUA DE LOS ARCHIVOS DE LOG. EN ESTE CASO LOS ARCHIVOS DE LOG SE VAN ANALIZANDO CONFORME SE VAN GENERANDO: CONSUME MÁS RECURSOS, PERO LA INFORMACIÓN SE OBTIENE DE UN MODO INMEDIATO HABIENDO MÁS POSIBILIDADES DE EVITAR ATAQUES.

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

7. ESTABLECIMIENTO DE LA MONITORIZACIÓN Y PRUEBAS DE LAS HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

LA MONITORIZACIÓN DE LAS HERRAMIENTAS Y LAS PRUEBAS QUE DEBEN REALIZARSE **SE DEFINEN EN EL PROCEDIMIENTO ESTABLECIDO** ANTE LA APARICIÓN DE ALGÚN CÓDIGO MALICIOSO.

ESTE PROCEDIMIENTO ESTÁ FORMADO POR UNA SERIE DE **PASOS**:

1. **CONTENCIÓN DE LOS DAÑOS PROVOCADOS POR EL MALWARE**
2. **DETECCIÓN DE LAS ACTIVIDADES QUE HA LLEVADO A CABO EL CÓDIGO MALICIOSO**
3. **EVALUACIÓN DE LOS DAÑOS PRODUCIDOS POR EL CÓDIGO MALICIOSO**
4. **REPARACIÓN Y REVISIÓN DE LA INFECCIÓN**

7. ESTABLECIMIENTO DE LA MONITORIZACIÓN Y PRUEBAS DE LAS HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

1. **CONTENCIÓN DE LOS DAÑOS PROVOCADOS POR EL MALWARE**. SI NO HUBIESE SOLUCIONES CONOCIDAS DE CONTENCIÓN SE RECOMIENDA:
    - IDENTIFICAR EL SOFTWARE MALICIOSO Y EXTRAER UNA MUESTRA.
    - MONITORIZAR LAS COMUNICACIONES Y LOS CAMBIOS QUE PUEDA OCASIONAR EL CÓDIGO MALICIOSO.
    - REALIZAR PRUEBAS PARA COMPARAR LOS DISTINTOS COMPORTAMIENTOS EN UN ENTORNO CONTROLADO ANTES Y DESPUÉS DE LA EJECUCIÓN DEL SOFTWARE MALICIOSO OBSERVANDO Y ANALIZANDO LO SIGUIENTE:
        A. LA ACTIVIDAD DE RED PARA CONOCER LAS COMUNICACIONES QUE HA REALIZADO EL SOFTWARE.
        B. LOS PROCESOS DEL SISTEMA QUE HA INICIADO EL SOFTWARE.
        C. LOS CAMBIOS QUE SE HAN PRODUCIDO EN LA ESTRUCTURA DE FICHEROS DEL SISTEMA.
        D. LOS CAMBIOS PRODUCIDOS EN LOS REGISTROS DE LOS EVENTOS.

7. ESTABLECIMIENTO DE LA MONITORIZACIÓN Y PRUEBAS DE LAS HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

- REALIZAR PRUEBAS QUE VERIFIQUEN EL GRADO DE CONFIABILIDAD, INTEGRIDAD Y VALIDEZ DE LA INFORMACIÓN FACILITADA POR LA HERRAMIENTA DE PROTECCIÓN.
- REALIZAR PRUEBAS QUE VERIFIQUEN EL GRADO DE EFECTIVIDAD DE LAS HERRAMIENTAS DE PROTECCIÓN Y CONTENCIÓN DE CÓDIGO MALICIOSO UTILIZADO: PRUEBAS EN ENTORNOS CONTROLADOS QUE PERMITAN COMPARAR LO QUE HUBIERA OCURRIDO ANTE INTRUSIONES SI NO ESTUVIERA INSTALADA LA HERRAMIENTA DE PROTECCIÓN EN EL EQUIPO.

7. ESTABLECIMIENTO DE LA MONITORIZACIÓN Y PRUEBAS DE LAS HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

2. GRACIAS ESTOS ANÁLISIS SE PUEDEN **DETECTAR LAS ACTIVIDADES QUE HA LLEVADO A CABO EL CÓDIGO MALICIOSO** Y DEFINIR CON MAYOR RAPIDEZ LAS MEDIDAS QUE HAY QUE TOMAR PARA GESTIONAR EL INCIDENTE Y CONTENER LOS DAÑOS OCASIONADOS.
3. **EVALUACIÓN DE LOS DAÑOS PRODUCIDOS POR EL CÓDIGO MALICIOSO**. UNA VEZ CONTENIDOS LOS DAÑOS HAY QUE ANALIZARLOS Y EVALUARLOS EN VARIOS ASPECTOS COMO: EL COSTE DE LA PÉRDIDA DE LOS DATOS ELIMINADOS, LA PÉRDIDA DE PRODUCTIVIDAD CAUSADA, EL GRADO DE PROPAGACIÓN DEL CÓDIGO MALICIOSO TANTO A NIVEL INTERNO COMO A NIVEL EXTERNO, ETC.

7. ESTABLECIMIENTO DE LA MONITORIZACIÓN Y PRUEBAS DE LAS HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

4. **REPARACIÓN Y REVISIÓN DE LA INFECCIÓN**. EN EL MOMENTO DE LA EVALUACIÓN DE LOS DAÑOS CAUSADOS POR EL CÓDIGO MALICIOSO DEBE ADOPTARSE UNA SERIE DE MEDIDAS CON EL FIN DE RESTAURAR EL SISTEMA Y VOLVER AL ESTADO ANTERIOR EN EL MENOR TIEMPO POSIBLE. ESTAS MEDIDAS CONSISTEN EN LA REVERSIÓN DE LAS ALTERACIONES PRODUCIDAS POR EL CÓDIGO MALICIOSO EN LOS ARCHIVOS Y SISTEMAS DE LOS EQUIPOS AFECTADOS. PARA ELLO SE UTILIZAN HERRAMIENTAS DE ANÁLISIS FORENSE.

7. ESTABLECIMIENTO DE LA MONITORIZACIÓN Y PRUEBAS DE LAS HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

ESTAS FASES DE CONTENCIÓN, EVALUACIÓN Y REPARACIÓN DE LOS DAÑOS CAUSADOS POR LOS CÓDIGOS MALICIOSOS **PUEDEN SER MONITORIZADAS A TRAVÉS DE HERRAMIENTAS DE PROTECCIÓN**. CON ESTAS SE PUEDEN **MONITORIZAR FUNCIONALIDADES** COMO:

- CREACIÓN DE BITÁCORAS DE HERRAMIENTAS HABILITADAS EN LOS CLIENTES CON ACCESO CENTRALIZADO.
- CREACIÓN DEL INVENTARIO DE SOFTWARE: CONJUNTO DE APLICACIONES INSTALADAS EN LOS SISTEMAS DE CADA EQUIPO.
- SISTEMAS DE DETECCIÓN DE INTRUSOS.
- CREACIÓN Y GESTIÓN DE REGISTROS DE CORREO ELECTRÓNICO.
- CREACIÓN Y GESTIÓN DE REGISTROS DE USO DE PROTOCOLOS DE INTERNET COMO HTTP Y FTP.

7. ESTABLECIMIENTO DE LA MONITORIZACIÓN Y PRUEBAS DE LAS HERRAMIENTAS DE PROTECCIÓN FRENTE A CÓDIGO MALICIOSO

- GESTIÓN CENTRALIZADA DE LAS BITÁCORAS DEL SISTEMA.
- GESTIÓN DE ACCIONES Y MEDIDAS A TOMAR EN CASO DE DETECCIÓN DE INTRUSIONES.
- ACTUALIZACIONES PERIÓDICAS DE LA BASE DE DATOS DE CÓDIGOS MALICIOSOS Y DE LA HERRAMIENTA DE PROTECCIÓN UTILIZADA.

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**

8. ANÁLISIS DE LOS PROGRAMAS MALICIOSOS MEDIANTE DESENSAMBLADORES Y ENTORNOS DE EJECUCIÓN CONTROLADA

LAS TÉCNICAS Y HERRAMIENTAS DE DETECCIÓN Y CONTENCIÓN DE CÓDIGOS MALICIOSOS DESCRITAS SE REFIEREN A UN **ANÁLISIS DINÁMICO DE UNA AMENAZA.**

CON ESTAS SE PRETENDE **MONITORIZAR EL COMPORTAMIENTO DE LOS CÓDIGOS MALICIOSOS PARA OBTENER INFORMACIÓN VALIOSA** Y PODER REACCIONAR AL RESPECTO.

EN ALGUNOS CASOS CONVIENE **EVITAR LA CONEXIÓN REAL DEL USUARIO CON EL SERVIDOR DEL CÓDIGO MALICIOSO**, YA QUE **SE ALERTA A LOS INTRUSOS DE LA PRESENCIA DEL USUARIO.**

8. ANÁLISIS DE LOS PROGRAMAS MALICIOSOS MEDIANTE DESENSAMBLADORES Y ENTORNOS DE EJECUCIÓN CONTROLADA

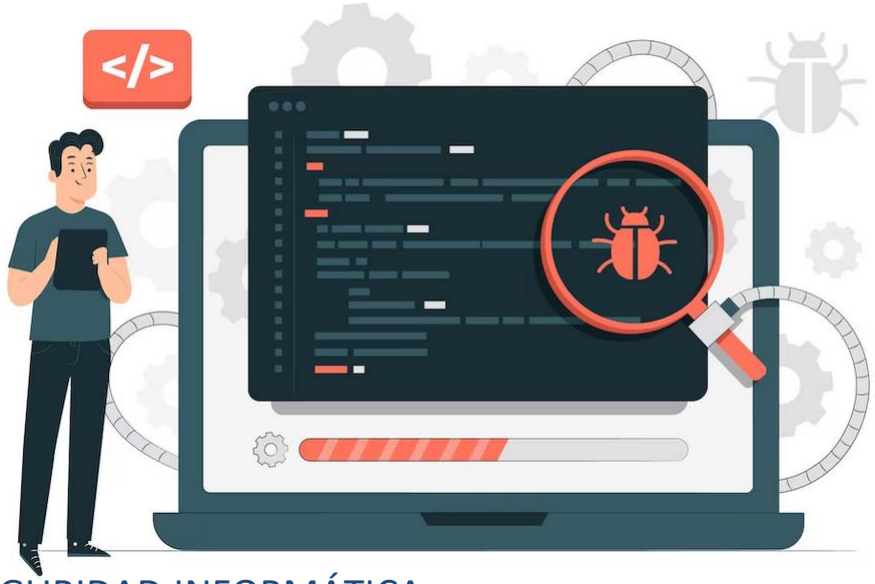
UNA ALTERNATIVA A CONSIDERAR **SERÍA LA SIMULACIÓN DE CIERTAS SITUACIONES**. SE PUEDE **HACER CREER AL CÓDIGO MALICIOSO QUE SE ESTÁ COMUNICANDO CON LOS SERVIDORES MALICIOSOS** CUANDO, EN REALIDAD, SE ESTÁ COMUNICANDO CON UNA MÁQUINA CONTROLADA POR EL USUARIO O ADMINISTRADOR.

ESTA TÉCNICA SE REFIERE A LA **CREACIÓN DE ENTORNOS SIMULADOS DE EJECUCIÓN CONTROLADA**.

RECIBEN LOS PAQUETES QUE VAN LLEGANDO DEL MALWARE Y VAN GENERANDO RESPUESTAS FALSAS ACORDES CON LO ESPERADO POR EL CÓDIGO MALICIOSO.

8. ANÁLISIS DE LOS PROGRAMAS MALICIOSOS MEDIANTE DESENSAMBLADORES Y ENTORNOS DE EJECUCIÓN CONTROLADA

CON ESTO **SE CONSIGUE UN CONOCIMIENTO MÁS PROFUNDO Y EXACTO DEL COMPORTAMIENTO DEL CÓDIGO MALICIOSO** QUE INTENTA ACCEDER AL EQUIPO EVITANDO QUE HAYA UNA CONEXIÓN DIRECTA ENTRE EL EQUIPO Y EL SERVIDOR MALICIOSO.



8. ANÁLISIS DE LOS PROGRAMAS MALICIOSOS MEDIANTE DESENSAMBLADORES Y ENTORNOS DE EJECUCIÓN CONTROLADA

LAS HERRAMIENTAS CON FUNCIONALIDADES DE SIMULAR ENTORNOS DE EJECUCIÓN CONTROLADA SON NUMEROSAS, PERO MERECE LA PENA DESTACAR DOS DE ELLAS:

- **FAKENET:** HERRAMIENTA QUE SE PUEDE EJECUTAR DESDE LA LÍNEA DE COMANDO DE WINDOWS Y PERMITE OBTENER INFORMACIÓN SOBRE LOS SITIOS WEB VISITADOS POR EL MALWARE. NO DISPONE DE INTERFAZ GRÁFICA.
- **INETSIM:** HERRAMIENTA QUE GENERA UN ENTORNO VIRTUAL ENCARGADO DE RECIBIR EL TRÁFICO DE RED DE LA MÁQUINA INFECTADA, REGISTRAR LAS PETICIONES QUE RECIBE Y ENVIAR RESPUESTAS SIMULADAS DE PROTOCOLOS DE RED.

8. ANÁLISIS DE LOS PROGRAMAS MALICIOSOS MEDIANTE DESENSAMBLADORES Y ENTORNOS DE EJECUCIÓN CONTROLADA

DESENSAMBLADORES

SE ENCARGAN DE **DESENSAMBLAR ARCHIVOS DE CÓDIGOS MALICIOSOS PARA IDENTIFICARLOS Y ENTENDER SUS ACTUACIONES**.

LOS USUARIOS ESTÁN UTILIZANDO **TÉCNICAS DE INGENIERÍA INVERSA**:

PRETENDEN OBTENER INFORMACIÓN DEL CÓDIGO MALICIOSO QUE HA INTENTADO ACCEDER AL SISTEMA PARA CONOCER CÓMO ESTÁ DISEÑADO, CÓMO FUNCIONA Y CÓMO ACTÚA PARA CREAR HERRAMIENTAS QUE PUEDAN DETECTARLOS Y CONTENERLOS CON MÁS FACILIDAD.

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**.

RESUMEN

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, EXISTIENDO INCLUSO HERRAMIENTAS DE DETECCIÓN ONLINE QUE NO CONSUMEN RECURSOS DE MEMORIA DE LOS EQUIPOS Y DISPONEN DE BASES DE DATOS DE MALWARE ACTUALIZADAS EN TODO MOMENTO.

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.


ESTO ES
TODO