GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA

CCN
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 834

Protección ante código dañino en el ENS

Septiembre 2018

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2018.09.17 18:32:17 +02'00'

NIPO: 083-19-022-8

Fecha de Edición: septiembre de 2018

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

PRÓLOGO

El uso masivo de las tecnologías de la información y la comunicación (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de enero, modificado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y la comunicación (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Septiembre de 2018

Félix Sanz Roldán

Secretario de Estado

Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

1. La correcta implantación del Esquema Nacional de Seguridad (Real Decreto 3/2010 de 8 de enero) requiere en ocasiones la utilización de herramientas y soluciones adecuadas. Así sucede, por ejemplo, cuando se persigue la satisfacción de lo dispuesto en sus artículos 7 (Prevención, reacción y recuperación), 8 (Líneas de defensa), 18 (adquisición de productos de seguridad y contratación de servicios de seguridad), 20 (Integridad y actualización del sistema), 21 (Protección de información almacenada y en tránsito), 23 (Registro de actividad) y 24 (Incidentes de seguridad), entre otros.
2. Los puestos de usuario (los denominados *Endpoint*) son probablemente los elementos más numerosos, heterogéneos y potencialmente más peligrosos de los Sistemas de Tecnologías de la Información y Comunicaciones en las Administraciones Públicas. Una vez comprometidos por código dañino, es posible utilizarlos como herramienta pivote para atacar infraestructuras de orden superior, tales como servidores, dispositivos de red, recursos en la nube (*cloud*) y otros servicios que puedan contener información sensible o confidencial, o que se utilicen para prestar servicios comprendidos en las competencias de la Organización.
3. Además de lo anterior, los puestos de usuario son utilizados generalmente por personal no experto en seguridad, infravalorando la importancia de los incidentes de seguridad producidos en tales equipos, que no suelen estar catalogados como equipamiento crítico y, por tanto, la estimación del impacto de los incidentes que los afectan puede resultar inferior a la real.
4. Por todo ello, los puestos de usuario se erigen en uno de los principales vectores de ataque de las organizaciones.
5. Podemos clasificar las herramientas de protección del Endpoint en dos grandes grupos: EPP (*Endpoint Protection Platform*) y EDR (*Endpoint Defense and Response*). Ambas constituyen la panoplia de herramientas que, conjunta o separadamente, pueden utilizarse para la mejor protección de los equipos de usuario.
6. Las soluciones EPP (*Endpoint Protection Platform*) (más conocidas con el nombre de “antivirus”), han sido durante décadas la solución más utilizada para proteger los puestos de usuario. Estas herramientas se apoyan en un conjunto de tecnologías que se empezaron a desarrollar en la década de los 80. Su estrategia principal se basa en buscar patrones dañinos dentro de los ficheros manejados por los puestos de usuario mediante un archivo de identificadores. Este recurso es publicado por el proveedor regularmente, y contiene una descripción codificada que facilita la búsqueda de patrones para identificar las amenazas conocidas en el momento de su generación y despliegue.
7. Publicar periódicamente un archivo de identificadores comporta ir necesariamente un paso por detrás de la creación del código dañino, ya que, en general, es necesario esperar a la aparición de nuevas amenazas para poder analizarlas e incorporarlas a los ficheros de firmas. Los recientes cambios en el

volumen, objetivos, modo de operación y sofisticación del código dañino hacen que esta solución no sea suficiente en todos los casos, demandando estrategias complementarias para proteger de forma efectiva los puestos de usuario y servidores.

8. Por su parte, los productos EDR (*Endpoint Defense and Response*) complementan la funcionalidad de las soluciones EPP, incorporando nuevas tecnologías que permiten reaccionar ante incidentes de seguridad provocados por código dañino todavía desconocido para el proveedor. Además, añaden herramientas de resolución y respuesta, que ayudan a determinar el impacto de la infección, minimizando los daños y revertiendo los equipos afectados a su estado original.

2. OBJETO

9. El objeto de la presente guía es ayudar a los Responsables de Seguridad de las entidades del ámbito de aplicación del ENS a adoptar una estrategia coherente de herramientas de protección de los puestos de usuario (EPP y EDR), atendiendo a la categoría de seguridad del sistema de información concernido, determinada en base al procedimiento descrito en el Anexo I del ENS.

3. HERRAMIENTAS DE SEGURIDAD EPP

10. Las soluciones EPP han estado presentes en puestos de usuario y servidores desde la década de los 80, y básicamente funcionan bloqueando la ejecución del código dañino detectado a través del fichero de firmas. Utilizando este mecanismo, las EPP son capaces de cubrir una amplia variedad de amenazas, tales como virus, troyanos, gusanos y otros, así como desinfectar o borrar los elementos infectados.
11. El incremento en la complejidad y sofisticación del código dañino ha provocado el desarrollo de una nueva generación de herramientas de protección que, concurrentemente con las anteriores, completan la seguridad ofrecida por el fichero de firmas. Estas tecnologías desarrollan dos líneas de acción: extendiendo la funcionalidad del archivo de identificadores con el objetivo de detectar amenazas desconocidas y reduciendo la superficie de ataque o la exposición de los puestos de usuario.
12. Las tecnologías que amplían la capacidad de detección del fichero de firmas son:
    - Análisis heurísticos y de código decompilado.
    - Sistemas anti-*exploit* y *anti-fileless*.
    - Análisis por emulación.
    - Análisis, entre otras, de aplicaciones web, correo y mensajería.
13. Por su parte, las tecnologías que reducen la superficie de ataque son:
    - Cortafuegos.
    - HIPS (*Host Intrusion Protection System*).
    - Filtrado de direcciones URLs.

- Control de dispositivos.
- Control de aplicaciones / listas blancas.

14. Aunque estas tecnologías han permitido la evolución de las soluciones EPP, poseen ciertas limitaciones estructurales que podrían traducirse en una menor efectividad frente a ataques por APTs (*Advanced Persistent Threats* - Amenazas Persistentes Avanzadas) requiriendo una atención constante por parte de los administradores de la seguridad del sistema, como es el caso del control de aplicaciones / listas blancas de aplicaciones.
15. Como quiera que el software EPP únicamente bloquea el código dañino en las etapas de explotación y distribución, una vez que el código dañino hubiere sorteado ambas podría permanecer indetectable por tiempo indefinido, generalmente hasta que sus efectos sean observados y los administradores de seguridad del sistema envíen una muestra al proveedor para su estudio y generación del identificador de detección correspondiente.
16. Una vez detectada la amenaza, los responsables de la seguridad del sistema tienen la garantía de que ese código dañino en concreto no volverá a infectar los puestos de usuario y servidores del sistema de información, pero no obtendrá información sobre las circunstancias particulares que propiciaron la infección, cuánto duró, cual fue el primer equipo infectado de la Organización, hasta qué punto el sistema y la Organización han sido comprometidos y qué daños ha ocasionado. Tampoco podrá determinar con precisión si la amenaza se ha neutralizado completamente o, por el contrario, sobrevive en alguno de los equipos afectados.

3.1. CARACTERÍSTICAS DEL FICHERO DE FIRMAS

3.1.1. DEPENDENCIA DE LA FIRMA DEL CÓDIGO DAÑINO

17. Las soluciones EPP convencionales reúnen en el fichero de firmas la inteligencia de seguridad que generan, volcando en él los identificadores de las muestras junto a otros mecanismos que desarrollan para generalizar las detecciones. Este fichero es descargado de forma regular por los puestos de usuario protegidos, bloqueando la ejecución del código dañino conocido y borrándolo del disco duro o enviándolo a una zona de cuarentena para su revisión posterior. Esta estrategia implica conocer "**ex ante**" el código dañino desarrollado dado que el fichero de firmas no podrá detectarlo hasta que un usuario perciba actividad sospechosa y envíe al proveedor una muestra del fichero para su estudio.

3.1.2. TIEMPO DE EXPOSICIÓN Y VENTANA DE SEGURIDAD

18. El tiempo que transcurre desde la aparición de una nueva amenaza hasta que es incorporada al fichero de firmas se conoce como "Ventana de oportunidad". Durante este intervalo, el código dañino no será detectado y podrá infectar todos los puestos cuyo sistema de seguridad se base únicamente en búsqueda de patrones por ficheros de firmas.

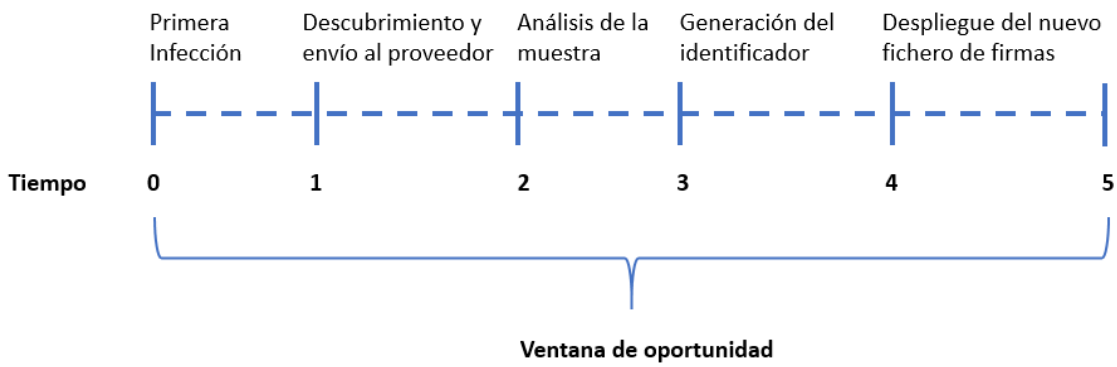

Ilustración 11: Estadios de la Ventana de oportunidad

19. La Ventana de oportunidad es la suma de las siguientes etapas :
    - Tiempo 1: intervalo que transcurre entre la puesta en marcha del código dañino con la primera infección y su detección visual por parte del usuario.
    - Tiempo 2: envío de la muestra automática o manualmente a los laboratorios del proveedor de seguridad.
    - Tiempo 3: análisis del comportamiento y la morfología, clasificación de la muestra y extracción del identificador o firma que representa al código dañino encontrado.
    - Tiempo 4: modificación del fichero de firmas y despliegue en todos los clientes del proveedor.
    - Tiempo 5: todos los clientes del proveedor se encuentran actualizados.
20. En el diagrama, el Tiempo 1 presenta la mayor variación comparándola con el resto, ya que depende de las técnicas de ocultación del código dañino, así como de sus efectos, si son claramente visibles o no por el usuario. En el Tiempo 5 la amenaza tal y como fue formulada originalmente pierde efectividad ya que es detenida por los antivirus con el fichero de firmas actualizado.
21. El Tiempo 2, que comprende el análisis de la muestra, es prácticamente el único punto donde un proveedor de seguridad tradicional puede acortar los plazos para conseguir una mejora importante en los tiempos de respuesta. Sin embargo, es posible que reduciendo este intervalo se ponga en peligro la fiabilidad de la clasificación que se menciona en el Tiempo 3 generando falsos positivos.
22. Una estrategia para reducir el Tiempo 4, y seguida en la actualidad por un grupo de proveedores cada vez más numeroso, consiste en mover la inteligencia de seguridad a la nube: al residir en un servidor remoto, los puestos de usuario se conectarán a un servicio publicado en Internet para comprobar si el fichero que están analizando es o no código dañino. Aunque no resuelve el problema de la Ventana de oportunidad por completo, los tiempos se reducen ya que el proveedor no necesita desplegar el fichero de firmas en cada cliente. Otra variante mixta consiste en utilizar un archivo de identificadores local como caché, que contiene los patrones de las amenazas más frecuentes, y mantener las más esporádicas en la nube para su consulta en tiempo real.

23. El Tiempo de exposición es un concepto equivalente a la "Ventana de oportunidad", pero referido a un puesto en particular: es el intervalo que transcurre desde que un equipo de usuario recibe una muestra de código dañino no identificada, hasta que es detectada y bloqueada. Durante ese período, el puesto afectado se considera comprometido. El "Tiempo de exposición" es siempre menor que la "Ventana de oportunidad" si se trata de código dañino ya en circulación, o igual a la ella si estamos ante la primera infección conocida.
24. Debido a que el envío del código dañino al proveedor depende de la velocidad de detección manual por parte del usuario y del tiempo dedicado al análisis de la muestra, el "Tiempo de exposición" y la "Ventana de oportunidad" suelen ser amplios.

3.1.3. LA CLASIFICACIÓN DE FICHEROS DESCONOCIDOS O GOODWARE

25. Para minimizar fallos al clasificar ficheros, es deseable que la herramienta de seguridad sea capaz de catalogar todos los archivos en circulación para generar tanto listas negras de software (el propio fichero de firmas) como blancas con los programas permitidos, por tratarse de *goodware*, o programas no dañinos.
26. Debido a que el proveedor de seguridad necesita acceder físicamente a cada uno de los archivos y procesos que analiza, es muy complicado clasificar todos los ficheros en circulación.
27. Existen algunas estrategias para autogenerar listas blancas sin necesidad de analizar los ficheros, como por ejemplo comprobar si el software está firmado por una entidad de confianza, si el origen del archivo es una fuente o repositorio fiable, o si pertenece a la distribución básica del sistema operativo. No obstante, el ingente volumen de software generado en todo el mundo hace que esta labor de clasificación esté fuera del alcance de la mayoría de los agentes interesados.

3.1.4. IMPACTO EN EL RENDIMIENTO DEL EQUIPO

28. El análisis mediante ficheros de firmas compara cada archivo almacenado en el equipo con los identificadores que contiene. Esto es una operación costosa en recursos (memoria, ciclos de CPU y espacio en el disco duro), proporcional al número de muestras representadas en el fichero de firmas. Con el incremento de la cantidad de amenazas únicas en circulación, el tamaño de los ficheros de firmas ha crecido de forma pareja impactando notablemente en el rendimiento del puesto del usuario.

3.2. CARACTERÍSTICAS DEL ANÁLISIS HEURÍSTICO Y TÉCNICAS DE INGENIERÍA INVERSA / DECOMPILACIÓN

29. El análisis heurístico y del código decompilado son dos estrategias de tipo estático que completan la protección ofrecida por el fichero de firmas.
30. En el análisis heurístico se examinan las cabeceras de los ejecutables buscando marcas o patrones concretos, llamados "*features*", que sean sospechosos de producir código dañino en ejecución. Los proveedores actualizan estos patrones

de búsqueda mediante reglas, que introducen en los ficheros de firmas para detectar nuevas amenazas.

31. En el análisis por decompilación, se obtiene el código fuente a partir del fichero binario de la amenaza, y se examina buscando operaciones sospechosas o maliciosas.

32. En ambos casos, al tratarse de análisis estáticos no se requiere ejecutar el código dañino y por lo tanto son más rápidos que otros tipos de técnicas que monitorizan el comportamiento. Tampoco revelan el método de detección exacto utilizado por el proveedor de seguridad, ya que no es necesario generar una firma para identificarlo. De esta forma, es más difícil para los creadores de código dañino evitar ser detectados modificando ligeramente la estructura de la amenaza, una estrategia muy común para sortear el fichero de firmas tradicional.

33. Debido a que el análisis se ejecuta de forma estática, la detección es bastante limitada e imprecisa. Si el proveedor de seguridad no ha incorporado la inspección de una determinada "*feature*", ésta no será reconocida, o si la amenaza ha sido ofuscada utilizando técnicas de cifrado, empaquetamiento o compresión desconocidas, el análisis estático será incapaz de acceder al contenido del fichero completo y terminará sin resultados concluyentes.

34. El análisis heurístico es propenso a generar falsos positivos y falsos negativos. Por esta razón el análisis heurístico no identifica de forma estricta el riesgo de un fichero, sino que genera un índice de probabilidad de peligro (*score*) que es utilizado como complemento de otras técnicas.

3.3. CARACTERÍSTICAS DE LOS SISTEMAS ANTI EXPLOIT / FILELESS

35. Muchas amenazas y ataques dirigidos no residen en archivos con código dañino que pueden ser detectados mediante un identificador almacenado en el fichero de firmas, como es el caso de los "*exploits*" y las amenazas "*fileless*".

36. Pese a que las amenazas "*fileless*" son conocidas desde hace tiempo, recientemente han ganado en popularidad al implementar estrategias de infección que no requieren depositar ficheros en el disco duro del equipo, con lo que los antivirus basados en archivos de identificadores son incapaces de detectarlos.

37. Muchas amenazas "*fileless*" en sistemas Windows utilizan intérpretes instalados en el equipo, tales como WSH (Windows Scripting Host), Powershell y APIs tales como WMI (Windows Management Instrumentation), para comprometer sistemas sin depositar un solo binario en el disco duro.

38. Otras amenazas "*fileless*" en sistemas basados en Unix, utilizan llamadas a funciones propias del sistema como "ptrace" con el fin modificar el comportamiento o estado de los procesos.

39. Existen tres tipos de amenazas "*fileless*":

    - Residentes en memoria: utilizan el espacio de memoria asignado a un proceso legítimo y permanecen en segundo plano e inactivos hasta que se produce un evento determinado que los activa.

- Rootkits: sustituyen ciertas librerías y herramientas del sistema operativo para ocultar su presencia.
- Registro: escriben el *payload* cifrado en ramas ocultas del registro de sistemas operativos Windows o en los ficheros de miniaturas (*thumbnails*) creados por el sistema operativo en las carpetas que contienen fotografías o en archivos *thumbs.db*.

40. Un *exploit* es una secuencia de datos recibida por un proceso vulnerable, y especialmente diseñada para provocar un fallo controlado. El programa comprometido interpretará parte de la secuencia de datos dañinos como código ejecutable, desencadenando acciones peligrosas para la seguridad del puesto o servidor.
41. El fallo más usual en un programa vulnerable se da en la gestión de los buffers de entrada del proceso. Si el volumen de datos recibido es mayor que el tamaño del buffer reservado y su gestión es defectuosa, los datos sobrantes no se descartarán, sino que se escribirán en zonas de memoria adyacentes que podrán ser interpretadas como código ejecutable. En la actualidad los sistemas operativos cuentan con tecnologías DEP (*Data Execution Prevention*) que impiden la ejecución de páginas de memoria destinadas a datos y marcadas como no ejecutables, invalidando la explotación de fallos por desbordamiento de buffer.
42. Para contrarrestar la tecnología DEP, las amenazas avanzadas sobrescriben otras secciones de la memoria. La técnica ROP modifica la pila de llamadas (*call stack*) de un proceso vulnerable para ejecutar zonas de código del propio proceso, conocidas como "*gadgets*". Así, el atacante puede "armar" flujos de ejecución alternativos al original, formado por partes de código del proceso atacado.
43. Una vez aprovechada la vulnerabilidad, el *exploit* descarga código, herramientas y otros datos de la red, conocidos como el "payload" del exploit, que le permitan ejecutarlos en el contexto del programa vulnerable.
44. Las protecciones anti exploit implementadas por las soluciones EPP protegen a los equipos bloqueando la ejecución de pares CVE-*payload* concretos. Cualquier variación en el par implicará la no detección del ataque hasta que sea reconocido por el proveedor de seguridad.

3.4. CARACTERÍSTICAS DEL ANÁLISIS POR EMULACIÓN

45. El análisis por emulación monitoriza parcialmente la ejecución de los programas sospechosos de contener código dañino, y analiza las acciones localmente para evaluar si son peligrosas o no.
46. Existen varios tipos de análisis por emulación, el más conocido consiste en "pre ejecutar" el inicio de cada programa lanzado en un área estanca dentro del puesto de usuario, y monitorizar su actividad. Comprobado que el inicio de la ejecución no contiene código dañino, se vuelve a ejecutar, pero esta vez sobre los recursos físicos reales del equipo.
47. El problema de esta estrategia es que impone un cierto retraso en la ejecución del programa sospechoso, que impacta directamente en el usuario. Por esta razón es

labor del proveedor balancear los inconvenientes de retrasar el inicio del programa con la conveniencia de ejecutar el programa en el entorno emulado durante un tiempo mínimo suficiente para poder detectar conductas extrañas. Debido a esta situación, el código dañino puede anticipar la existencia de la preejecución de prueba y simplemente retrasar su ejecución durante un tiempo prudencial.

48. Otros enfoques más complejos implican la instalación de un entorno *sandbox* que ejecuta la amenaza en un equipo físico o virtual aislado e independiente del puesto del usuario, para analizar las acciones desencadenadas y emitir una clasificación. En este esquema, cuando un usuario ejecuta un programa sospechoso evaluado por otras técnicas (como análisis heurístico, por ejemplo), el archivo es bloqueado automáticamente y enviado a la maquina *sandbox* donde será ejecutado por completo y analizada su respuesta.

49. Los entornos *sandbox* presentan algunos de los siguientes problemas:

    - Manejar correctamente este tipo de entorno requiere personal técnico cualificado que no siempre pertenece a la plantilla de la Organización. Algunos proveedores ofrecen ese servicio, alojando en la nube entornos *sandbox* bajo demanda para analizar las amenazas enviadas por sus clientes.
    - El código dañino puede pasar inadvertido si detecta que está siendo ejecutado en un hardware virtual, reteniendo por tiempo indefinido su línea de ejecución dañina, o presentando un juego de acciones alternativo que enmascare el código dañino. Por lo tanto, un entorno *sandbox* efectivo se debería diseñar incorporando el uso de máquinas reales para evitar estas técnicas de ocultación.
    - El análisis puramente automático en un entorno *sandbox* es una tarea muy imprecisa. Frecuentemente, el código dañino no llega a desplegar todo su recorrido por no encontrar determinados programas instalados y necesarios para ejecutar un *exploit*, o requerir algún tipo de acción por parte del usuario que en un entorno automatizado no se va a producir. Aun con todo, aunque el código dañino se haya podido ejecutar en su totalidad en el entorno *sandbox*, puede ser muy complicado clasificarlo como amenaza con los datos generados de una única ejecución automatizada.

3.5. CARACTERÍSTICAS DE LAS TECNOLOGÍAS QUE REDUCEN LA SUPERFICIE DE EXPOSICIÓN

50. Cada tecnología que reduce la superficie de exposición en los puestos de usuario y servidores bloquea un tipo de distribución del código dañino:

    - Distribución por descarga web: el filtrado URL limita la navegación del usuario evitando páginas que contienen código dañino.
    - Distribución por dispositivos USB: el control de dispositivos limita o impide el uso de dispositivos de almacenamiento extraíbles o módems/wifis que sorteen las protecciones perimetrales instaladas en la organización.

- Distribución por correo: el sistema antispam y los complementos (*plugins*) de clientes de mensajería impiden la recepción del correo no solicitado y mensajes mal formados que contienen adjuntos peligrosos o enlaces que redirigen al usuario a páginas web dañinas.

51. Aunque este enfoque hace menos probable la infección a costa de limitar el uso del equipo informático, las tecnologías que reducen la superficie de exposición solo actúan previniendo la infección. Una vez sorteadas, no influyen en la ejecución del código dañino.

4. EL CICLO DE PROTECCIÓN COMPLETA

52. Las estrategias de seguridad de nueva generación asumen que es imposible desarrollar una barrera de protección impenetrable en torno a los sistemas de las Tecnologías de la Información y Comunicaciones que evite la entrada del 100% del código dañino en circulación. Por esta razón se ha producido una evolución hacia una estrategia de seguridad más completa, dividida en cuatro etapas:

    - Protección / Prevención
    - Detección
    - Resolución / Respuesta
    - Adaptación.

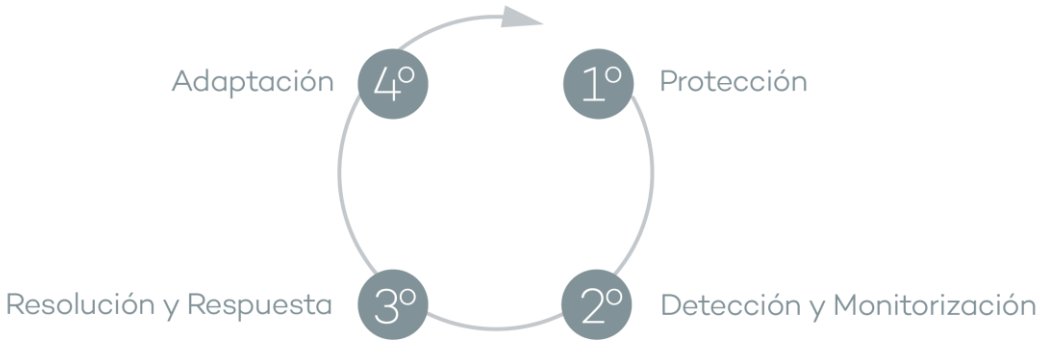

Ilustración 2: Estrategia de seguridad Ciclo de protección completa

53. Esta estrategia se representa como un proceso circular llamado Ciclo de protección completa, formada por etapas que se repiten de forma indefinida y que a su vez impulsan el concepto de Modelo de Madurez de Seguridad (*Security Maturity Model*) en las organizaciones.

4.1. FASE 1: PROTECCIÓN / PREVENCIÓN

54. El Ciclo de protección completa asimila en su primera etapa de Protección/Prevención las funcionalidades propias de una solución EPP. En esta fase, la estrategia de seguridad se centra únicamente en prevenir la infección de puestos de usuario y servidores mediante tecnologías que reducen la superficie de ataque. Para ello se utilizan funcionalidades tradicionalmente implementadas por el software EPP como:

- Fichero de firmas.
- Cortafuegos.
- HIPS (Host Intrusion Protection System).
- Filtrado de URLs.
- Control de dispositivos.
- Control de aplicaciones.

55. La protección frente a amenazas se implementa mediante tecnologías de detección basada en ficheros de firmas principalmente, y otras formas complementarias como análisis heurístico, contextual, protección anti-exploit etc. La generación de la inteligencia de seguridad que reciben estas tecnologías se automatiza en el proveedor en mayor o menor medida.

56. La fase de Protección / Prevención es la primera línea de defensa y está diseñada para aportar una protección básica y suficiente en entornos de riesgo bajo, bloqueando buena parte del código dañino conocido en circulación. Este código dañino tiene las características siguientes:

    - Emplea técnicas de infección poco sofisticadas o bien conocidas.
    - Previamente al intento de infección ha permanecido un tiempo mínimo en circulación, infectando equipos y revelando sus efectos.
    - La ventana de oportunidad se ha cerrado para el grueso de proveedores, que han incorporado el identificador al fichero de firmas / inteligencia de seguridad.

4.2. FASE 2: DETECCIÓN

57. Con el transcurso del tiempo los agentes de las amenazas descubren debilidades en la Política de Seguridad de la Información de las Organizaciones que pueden aprovechar para introducirse en los Sistemas de información. Una vez infectado un puesto de usuario, la fase de Protección ya no tiene efecto hasta que la amenaza ejecute acciones dañinas observables por el usuario y se pueda iniciar el reporte de la muestra. Por esta razón, son necesarias nuevas características en las herramientas de seguridad para detectar código dañino desconocido de forma automática sin pasar por este proceso, que puede llegar a ser bastante dilatado en el tiempo:

    - Detección basada en técnicas de monitorización que no requieran archivo de identificadores.
    - Clasificación de amenazas desconocidas de forma temprana. No es un requisito imprescindible que el usuario o el Responsable del Sistema sospechen de la existencia de código dañino en los sistemas de información de la Organización.
    - Clasificación de amenazas desconocidas de forma fiable, sin falsos positivos ni falsos negativos.

- Generación de información detallada y centralizada sobre el comportamiento de los procesos.

58. Además, la monitorización de los procesos genera información sobre su actividad, que será aprovechada en la fase Adaptación, y aportará datos para la modificación de la Política de Seguridad de la Información, y a la vez permitirá detectar procesos con comportamientos anómalos, evaluar su peligrosidad e iniciar acciones de Resolución y Respuesta en la fase 3 del Ciclo de protección completa.

4.3. FASE 3: RESOLUCIÓN Y RESPUESTA

59. Si en la etapa Detección se han descubierto equipos comprometidos y la amenaza ha sido detectada, el Ciclo de protección completa requiere herramientas que permitan:

    - Resolver el incidente bloqueando el código dañino encontrado, interrumpiendo su propagación y proporcionando los mecanismos necesarios para facilitar su reparación.
    - Recopilar toda la información necesaria y presentarla de forma ordenada para poder determinar el alcance del incidente y los daños producidos.
    - Recopilar todos los indicios observados previos a la declaración del incidente que sirvan de base en la fase Adaptación.

4.4. FASE 4: ADAPTACIÓN

60. Una vez resuelto el incidente, en la fase Adaptación se reúne la información generada por todas las herramientas involucradas en las fases anteriores, con el objetivo de impulsar la modificación de la Política de Seguridad de la Información.

61. El objetivo de esta fase es mejorar la Política de Seguridad de la Información de la Organización, atendiendo a lo dispuesto en el artículo 26 (mejora continua del proceso de seguridad) del ENS, para que en el futuro el código dañino sea detenido en una fase más temprana del Ciclo de protección completa, generalmente en la etapa Protección. Adicionalmente, el Administrador de la seguridad del sistema podrá detectar y bloquear amenazas similares que actúen de forma equivalente o que empleen técnicas parecidas.

62. Los cambios en la Política de Seguridad de la Información pueden involucrar variaciones en la configuración de las herramientas utilizadas en las fases Protección, Detección y Respuesta (Gestión de incidentes [op.exp.7]) o la incorporación de otras nuevas, iniciativas de formación (Formación [mp.per.4]) para empleados y equipo técnico, por mencionar algunas medidas típicas. También se producirá una actualización automática de la inteligencia de seguridad con el identificador que describe al nuevo código dañino detectado.

5. LAS HERRAMIENTAS EDR Y EL CICLO DE PROTECCIÓN COMPLETA

63. Debido a que las herramientas EPP no cubren todas las fases del Ciclo de protección completa, ha surgido una nueva categoría de aplicaciones llamadas

EDR (*Endpoint Detection and Response*) que añaden características de seguridad enfocadas a detectar y bloquear el código dañino desconocido.

64. La noción de EDR ha evolucionado a lo largo del tiempo. En su concepto original se trataba de herramientas para monitorizar y observar la ejecución de procesos. Al no incorporar tecnologías de Prevención ni Resolución, no se las consideraba soluciones sustitutivas de herramientas EPP. Ante la reticencia generalizada de los Administradores de la seguridad a instalar más programas que los estrictamente necesarios en un mismo puesto de usuario o servidor, las herramientas EDR han evolucionado abarcando parte de las características EPP e incorporando funcionalidades IR (*Incident Response*), hacia una nueva categoría llamada *Next Generation Endpoint Protection Platform* (NGEPP).

65. En la actualidad, aunque las soluciones EDR incorporan funcionalidad EPP e IR, también permiten su despliegue y utilización simultánea junto con otras herramientas de seguridad tradicionales, del mismo o de distinto fabricante.

66. Instalar una única solución EDR -con funcionalidades EPP e IR- del mismo fabricante, pese a que puede tener el inconveniente de estar diseñada bajo una única filosofía operativa, puede tener las siguientes ventajas:

    - Un único proveedor para todas las herramientas: mayor facilidad de mantenimiento y gestión de incidencias.
    - Una única consola de administración para todas las herramientas: menor tiempo de adaptación, mayor facilidad de uso, gestión centralizada.
    - Menor coste medio frente a adquirir varias soluciones independientes.
    - Menor consumo de recursos, al integrar toda la funcionalidad en un único software.
    - Generación de información consolidada y centralizada en todas las fases del Ciclo de protección completa.
    - Mejor coordinación, y por lo tanto mayor sinergia y efectividad, entre los diferentes módulos que componen la protección.

67. Por otro lado, utilizar una herramienta EDR de un proveedor distinto al contratado para la protección EPP o IR tiene las siguientes ventajas:

    - Las herramientas estrictamente EDR o EPP implementan más funcionalidades y las desarrollan de forma más completa acorde a su mayor focalización.
    - Acceso a una mayor Inteligencia de seguridad al ser proporcionada por dos o más proveedores independientes, que se puede traducir en menos incidentes de seguridad.
    - Aumento del grado de seguridad al disminuir los posibles riesgos de explotación de vulnerabilidades de varias herramientas distintas en el mismo tiempo.

68. A diferencia del software EPP enfocado en la protección / prevención de los puestos de los usuarios impidiendo su infección, las soluciones EDR asumen que ya han sido infectados y dispone de herramientas orientadas a:

    - Detección temprana de actividades sospechosas indicativas de un ataque en curso.
    - Validación de la actividad sospechosa y clasificación como perteneciente a un ataque.
    - Interrupción de la actividad sospechosa detectada.
    - Explotación de los datos recogidos.

5.1. ENFOQUES PARA CLASIFICAR ACTIVIDADES SOSPECHOSAS

69. Satisfaciendo de este modo la medida [op.mon.1] "Detección de intrusión", todas las herramientas EDR detectan y clasifican las amenazas monitorizando la actividad de los programas ejecutados en el propio puesto de usuario o servidor. Sin embargo, la forma de procesar e interpretar la información y los recursos dedicados a esta tarea varían notablemente entre proveedores. Dependiendo del lugar físico donde se evalúen los datos monitorizados. Existen tres enfoques:

    - Clasificación local: la propia herramienta EDR instalada en el puesto del usuario incorpora algoritmos que evalúan los datos monitorizados.
    - Clasificación en los sistemas de información de la Organización: el software EDR instalado en el puesto del usuario se integra con otras herramientas desplegadas en la Organización, que facilitan a los administradores de seguridad del sistema la evaluación de los datos recogidos.
    - Clasificación en los Sistemas del proveedor: la herramienta EDR instalada en el puesto del usuario envía los datos monitorizados a la nube del proveedor donde se analizan en entornos automatizados con la ayuda de expertos en código dañino.

5.1.1. CLASIFICACIÓN LOCAL

70. Los datos monitorizados se analizan en el puesto del usuario mediante algoritmos más o menos sofisticados, y en muchos casos con recursos equivalentes al fichero de firmas que incorporan una parte de la lógica de clasificación.

71. Su principal ventaja es una mayor confidencialidad de los datos monitorizados ya que no salen de los Sistemas de información de la Organización.

72. Sus principales desventajas son las siguientes:

    - Al evaluar únicamente los datos monitorizados del puesto de usuario, la clasificación es imprecisa ya que son necesarias múltiples ejecuciones en distintos puestos y servidores de un mismo programa sospechoso para poder emitir una clasificación fiable.
    - Al ejecutar el proceso de evaluación con recursos limitados los algoritmos de clasificación tienen que ser simplificados ya que implican técnicas muy

intensivas de computación. Para aliviar esta carga, el análisis en local suele utilizar el equivalente a los ficheros de firmas en herramientas EPP. Esta dependencia limita la detección de las amenazas desconocidas a variaciones de muestras ya estudiadas por el proveedor, con lo que se incurre en el mismo problema que aparece al utilizar únicamente herramientas EPP.

- No es posible analizar de forma continua todos los procesos ejecutados en el puesto de usuario sin impactar en el rendimiento. Por esta razón se tiende a no analizar el software clasificado previamente como *goodware* (código, supuestamente, NO dañino), perdiéndose la posibilidad de detectar comportamientos anómalos de software legítimo, pero vulnerables a la explotación de fallos.

5.1.2. CLASIFICACIÓN EN LOS SISTEMAS DE LA ORGANIZACIÓN

73. La clasificación en los Sistemas de la Organización se utiliza para paliar las deficiencias encontradas en el modo de clasificación local. Estos sistemas añaden una etapa adicional que deriva en esquemas más complejos de valoración de amenazas.
74. Los ficheros sospechosos encontrados en los puestos de usuarios son enviados a un entorno *sandbox* donde se monitoriza su ejecución completa y se evalúan los resultados. La clasificación puede ser automática, aunque en una gran parte de los casos requiere la intervención del Administrador de Sistemas para asistir en el procedimiento.
75. También es posible visualizar los eventos monitorizados en paneles de control o herramientas SIEM equivalentes que faciliten al Administrador de Sistemas la valoración del comportamiento del programa sospechoso.
76. Las principales ventajas de este método de clasificación son:
    - Razonable confidencialidad de los datos, ya que éstos no abandonan el ámbito de control de los Sistemas de información de la Organización.
    - Para casos corrientes, la entidad no necesita un departamento formado por técnicos especialistas en detectar patrones sospechosos, aunque sigue siendo muy recomendable su existencia.
    - El proveedor puede completar el proceso de clasificación en la Organización emitiendo una segunda opinión, generalmente imprecisa pero que puede valer para confirmar o reforzar las conclusiones obtenidas por el Administrador de la seguridad del sistema.
    - Mejoran la precisión de la valoración del sospechoso con respecto al modelo de clasificación local.
77. Sus principales desventajas son:
    - El proceso completo es más complejo ya que involucra un mayor número de capas: (clasificación local + *sandbox* + valoración del proveedor)

- En ocasiones la clasificación pierde fiabilidad debido a las limitaciones de los entornos *sandbox* indicados anteriormente.
- El análisis en *sandbox* o mediante otras herramientas de terceros que requieran la asistencia de los responsables de la administración de la seguridad del sistema tiende a ser lento y por lo tanto el trastorno provocado al usuario es mayor.
- Para una parte considerable de amenazas desconocidas sí se requiere un departamento de técnicos expertos que sepan interpretar patrones sospechosos.
- La valoración emitida por el proveedor sobre el fichero o proceso sospechoso es un número (*score*) que da una idea de la confianza o peligrosidad del archivo analizado. Queda en manos del Administrador de la seguridad del sistema la tarea de juzgar y decidir si es realmente peligroso o no, estableciendo un umbral o punto de corte por debajo del cual todos los valores (*scores*) serán considerados malware. Si se trata de una amenaza compleja probablemente no será detectada por el sistema de clasificación del proveedor o emitirá una valoración muy ambigua.

5.1.3. CLASIFICACIÓN EN LOS SISTEMAS DEL PROVEEDOR

78. Todos los datos monitorizados se envían en tiempo real a la infraestructura del proveedor y se analizan mediante algoritmos sofisticados de *Machine Learning*. Al trabajar sobre múltiples ejecuciones de un mismo programa sospechoso y contar con recursos hardware correctamente dimensionados, producen las clasificaciones más precisas y rápidas, sin la intervención del Administrador del sistema de la Organización.
79. La mayoría de procesos se clasifican automáticamente, los que formen patrones de ejecución y comportamientos muy complicados pueden dificultar la clasificación en tiempo real y con la debida certeza, requiriendo la intervención de expertos en código dañino. Así, es posible detectar amenazas avanzadas (APTs) o ataques ejecutados manualmente por hackers (*Managed attacks*).
80. Las ventajas de este modelo son:
    - No se requiere un equipo técnico en la Organización entrenado en la detección de patrones de ejecución sospechosos.
    - El proceso completo es mucho más rápido, habilitando la posibilidad de una detección temprana, el trastorno provocado al usuario es menor.
    - No requiere que el Administrador de la seguridad del sistema de la Organización tome ninguna decisión sobre la peligrosidad de la muestra.
    - Para el código dañino tradicional las técnicas de autoaprendizaje clasifican de forma automática las aplicaciones y procesos. La valoración se produce en tiempo real.
    - Si las técnicas de autoaprendizaje identifican elementos complejos en el fichero sospechoso y el modelo no tiene suficiente confianza matemática

como para emitir un diagnóstico sin error sobre la peligrosidad de la muestra, el proveedor cuenta con un equipo de expertos en seguridad que la examinan de forma manual. Al implicar pruebas en laboratorio, este escenario puede penalizar el tiempo de respuesta, aunque garantiza la fiabilidad de la clasificación.

81. Aunque no es necesario un departamento en la Organización formado por técnicos expertos en la detección de patrones de ejecución, si es recomendable contar con un equipo o servicio especializado en análisis forense, que sepa interpretar los datos de la monitorización para determinar el alcance de los incidentes.

5.2. CONTENCIÓN DEL INCIDENTE

82. Si existen puestos de usuario o servidores en los Sistemas de información de la Organización afectados por código dañino y la amenaza ha sido detectada en la etapa Detección, el Ciclo de protección completa puede requerir herramientas IR (*Incident Response*) que permitan resolver esta situación.

83. Las herramientas EDR de resolución (IR) tienen las siguientes características:

- Son capaces de bloquear procesos dañinos.
- Aíslan de la red a los puestos afectados.
- Permiten el acceso remoto controlado a los puestos afectados.
- Facilitan la restauración de los puestos afectados al estado previo al incidente.

5.2.1. BLOQUEO DE PROCESOS DAÑINOS

84. La herramienta EDR evita la ejecución de los procesos dañinos o los detiene si ya estaban en ejecución. Dependiendo del tipo de amenaza y vector de ataque, el usuario puede perder los datos que maneja el proceso (por ejemplo, un documento abierto con los programas de Microsoft Office, que se encontraba comprometido por haber ejecutado un virus de macro). La herramienta avisará de esta posibilidad antes de aplicar el proceso de resolución.

5.2.2. AISLAMIENTO DE LOS EQUIPOS

85. Al aislar un puesto de usuario o servidor se interrumpen todas sus comunicaciones para impedir que el código dañino se propague y envíe datos e información sensible o confidencial hacia el exterior. Esta situación no afecta a las herramientas de gestión remota de la solución EDR.

86. Las herramientas EDR emplean varias técnicas para aislar puestos y servidores:

- Cambio de la configuración de red del puesto para moverlo a una subred de cuarentena.
- Configuración de reglas en el cortafuegos que filtren paquetes e impidan el tráfico hacia el exterior.

- Apagado completo del equipo, reinicio remoto o bloqueo para que el usuario no pueda seguir operando hasta que el problema haya sido solucionado.

87. Una vez resuelto el incidente, la herramienta EDR permite reincorporar el puesto del usuario o servidor a la red de la Organización.

5.2.3. ACCESO REMOTO A LOS EQUIPOS AFECTADOS

88. Mediante herramientas de acceso remoto los técnicos acceden sin desplazarse físicamente a los puestos de usuario afectados para efectuar pruebas y comprobaciones, así como para restaurarlo a su estado original.
89. Las herramientas de acceso remoto permiten acceder en segundo plano a los recursos del puesto sin interrumpir el trabajo del usuario para efectuar un diagnostico o reparación. Los recursos accesibles de forma remota y no intrusiva son:

    - Gestor de procesos.
    - Línea de comandos remota.
    - Acceso al registro remoto en el caso de sistemas Windows.
    - Carga y descarga de ficheros.
    - Instalación y desinstalación de programas remota.
    - Ejecución de archivos de comandos remotos (scripts).
    - Gestión de los servicios o demonios (Unix) instalados.
    - Acceso al visor de sucesos en el caso de sistemas Windows.

90. Por el contrario, el acceso al escritorio remoto permite un control completo del puesto de usuario, aunque implica la interrupción de su trabajo hasta que se solucione el incidente.
91. Todos los recursos de acceso remoto son plenamente funcionales en los puestos de usuario aislados por la herramienta EDR como resultado de una infección.

5.2.4. RESTAURACIÓN DE LOS EQUIPOS AFECTADOS

92. Las herramientas de resolución detienen los procesos comprometidos o dañinos y los borran del equipo o los mueven a la zona de cuarentena, a la espera de un examen posterior. Si hay archivos infectados y el proveedor desarrolla la rutina de desinfección, se aplicará sobre el fichero automáticamente y se restaurará de la cuarentena a su localización original.
93. En el caso de *rootkits* y otras amenazas avanzadas es necesario realizar un análisis del puesto de usuario en profundidad. Para ello, la herramienta EDR reinicia el equipo en modo seguro (sistemas Windows) o en modo recuperación (sistemas Linux) y analiza los cambios efectuados en el sistema operativo cuando el código dañino todavía no se ha cargado en memoria, para revertirlos.

5.2.5. SISTEMAS DE RECUPERACIÓN DE DATOS PERDIDOS

94. Las amenazas por secuestro de archivos (*ransomware*) están cobrando importancia y los proveedores de seguridad han desarrollado herramientas específicas para evitar este tipo de ataques o recuperar los datos si ya se han producido.

95. Los ataques por secuestro de archivos (*ransomware*) cifran los ficheros de datos que pueden ser esenciales para la Organización. En principio, el ataque está diseñado para que solo se pueda revertir previo pago de una cantidad de dinero, generalmente en criptomonedas como *bitcoins* para impedir la localización del atacante. Los archivos secuestrados/cifrados, en muchos casos, no es posible su descifrado sin la clave privada y por esta razón los proveedores pueden implementar soluciones basadas en copias de seguridad automáticas.

96. Esta estrategia consiste en interceptar las escrituras a ficheros de ofimática y bases de datos del usuario, almacenando una copia de seguridad automática y oculta. Si un *ransomware* cifra un fichero, el software EDR podría recuperarlo a su estado original.

97. Este enfoque tiene como desventaja el consumo de espacio en el área de almacenaje de la Organización, por lo que se mantienen un número limitado de copias de seguridad y se evita la copia de ficheros modificados por aplicaciones legítimas. Conocido este hecho, el *ransomware* puede implementar varias estrategias:

    - Escribir varias veces en cada fichero con el objetivo de agotar el número de copias que mantiene el software EDR.
    - Ocultarse para impedir que el software EDR pueda distinguir una modificación legítima de otra provocada por una amenaza. Por ejemplo, mediante exploits o virus de macro, un atacante puede cifrar ficheros a través de herramientas legítimas.

5.3. EXPLOTACIÓN DE LOS DATOS GENERADOS

98. Para cubrir la medida [op.exp.7] “Gestión de incidentes”, las herramientas EDR pueden recopilar los datos monitorizados de las aplicaciones que se han ejecutado en los Sistemas de información, para, posteriormente filtrarlos con el fin de su interpretación. Se utilizan listados, diagramas y otros recursos gráficos que permiten al Administrador de la seguridad del sistema valorar los eventos generados por las aplicaciones dañinas, y así determinar el alcance del incidente y diseñar una respuesta. Las herramientas de explotación de datos tienen las siguientes características:

    - Generación de alertas en tiempo real e integración con sistemas SIEM.
    - Acceso a la actividad de los puestos de usuario y servidores en cualquier momento del tiempo pasado.
    - Acceso a la actividad del código dañino desde el inicio del incidente.
    - Centralización de la información generada por el incidente.

- Trazabilidad del código dañino en la red.
- Información y características del proceso dañino.
- Actividad del código dañino dentro de los equipos.
- Información ampliada del código dañino.

5.3.1. GENERACIÓN DE ALERTAS EN TIEMPO REAL E INTEGRACIÓN CON SISTEMAS SIEM

99. El proveedor gestiona automáticamente el envío de alertas a los responsables de la seguridad del sistema con cada patrón de ejecución sospechoso detectado, o con cada clasificación o reclasificación confirmada de un programa con comportamiento dañino. Estas alertas pueden ser enviadas directamente al sistema SIEM de la Organización.

100. El Administrador de la seguridad del sistema visualiza toda la información suministrada por la solución EDR desde los paneles de control (*dashboards*) de la plataforma SIEM implantada. Las herramientas de *ticketing* como LUCIA se integran con la plataforma SIEM, generando automáticamente tickets para los técnicos, que alertan de situaciones anómalas para programar una intervención manual.

101. Las soluciones EDR que detectan la ejecución o llegada de programas desconocidos (sin clasificar) a los sistemas de información de la Organización, y que requieren una clasificación no automatizada, también generan avisos en estas circunstancias. Así, los responsables de la seguridad del sistema podrá realizar el seguimiento de estos procesos hasta su clasificación final.

5.3.2. ACCESO A LA CRONOLOGÍA DE LA ACTIVIDAD DEL CÓDIGO DAÑINO DESDE EL INICIO DEL INCIDENTE

102. La monitorización de los procesos recoge toda la cronología de acciones ejecutadas (*timeline*) por el software dañino desde su aparición. Las herramientas EDR de análisis forense utilizan este registro para mostrar visualmente los datos clave y construir el ciclo de vida del código dañino. Con esta información, el Administrador de la seguridad del sistema puede evaluar el alcance del incidente, diseñar los planes de resolución y ajustar la Política de Seguridad de la Información para evitar ataques similares en el futuro.

103. Al monitorizar desde el inicio la actividad del código dañino, la herramienta de análisis forense podrá retrotraerse en la cronología (*timeline*) del Ciclo de vida del código dañino hasta su comienzo para acceder a información relacionada con la trazabilidad del software dañino, acceso a datos sensibles o confidenciales y fuga de información, o el vector de infección utilizado, entre otros.

104. Las herramientas de análisis forense muestran la información siguiente sobre las acciones ejecutadas por el código dañino:

- Conexiones remotas establecidas por el software dañino para enviar la información recogida o descargar nuevos elementos utilizados en el ataque.
- Destino de las conexiones remotas, identificando el país y la región.
- Lecturas y escrituras en ficheros y bases de datos donde se almacena la información sensible o confidencial de la entidad.
- En el caso de sistemas Windows, accesos a las ramas del registro en el puesto usuario o servidor para ganar persistencia y sobrevivir a reinicios del hardware.
- En el caso de sistemas Unix/Linux, accesos a los distintos archivos de arranque o configuración modificados para ganar persistencia y sobrevivir a reinicios de hardware.
- Instalación de controladores (drivers) y servicios que enmascaren o dificulten la detección del código dañino.
- Ejecución de aplicaciones y carga de módulos de código.

5.3.3. ACCESO A LA CRONOLOGÍA DE LA ACTIVIDAD DE TODOS LOS PROCESOS EN EL PUESTO DE USUARIO

105. La capacidad para analizar la cronología (*timeline*) de acciones de cualquier proceso (sea o no código dañino) ejecutado en el puesto, permite identificar patrones de comportamiento anómalos también en aplicaciones confiables, provocados por la explotación de vulnerabilidades.

5.3.4. CRONOLOGÍA CENTRALIZADA DE LA INFORMACIÓN GENERADA POR EL INCIDENTE

106. Para facilitar el análisis forense, la información recogida se consolida de forma centralizada en un único repositorio que representa la cronología completa del incidente, compuesta por todos los datos suministrados por cada uno de los puestos de usuario y servidores afectados. Las herramientas EDR pueden integrarse con plataformas SIEM, de forma que en un mismo panel de control se pueda mostrar toda la información generada por los Sistemas de la Organización.

5.3.5. TRAZABILIDAD DEL CÓDIGO DAÑINO EN LOS SISTEMAS DE INFORMACION

107. Las herramientas EDR de análisis forense extraen la siguiente información de los datos generados en el proceso de monitorización:

- El momento exacto en el que comenzó la infección.
- El primer equipo afectado en la Organización, conocido como el “Paciente cero”.

- Los movimientos del código dañino ejecutado tanto en el quipo Paciente cero como dentro de los sistemas de información de la Organización.

108. El momento de la infección determina el "Tiempo de exposición". Cuanto mayor sea éste, mayor será el número de equipos potencialmente afectados y más complicado será el proceso de análisis forense para determinar el alcance exacto del incidente.

109. El Paciente cero indica el primer equipo de la red infectado por el código dañino. Junto con el vector de ataque o vector de infección utilizado, establece la vulnerabilidad aprovechada por el atacante en la fase Protección. Dentro del flujo de datos generado, la herramienta de análisis forense localiza los atributos del Paciente cero: nombre, dirección IP, usuario que utilizaba el puesto, procesos en ejecución, rol del usuario y otra información relevante.

110. Finalmente, la herramienta EDR de análisis forense detecta los patrones de infección en los puestos de usuario, llamados Movimientos laterales. En APTs y otros ataques avanzados se utiliza para ganar persistencia dentro de los sistemas de información, y buscar servicios clave que permitan alcanzar los objetivos del atacante. Los movimientos laterales se mantienen en la sombra al producirse dentro del perímetro de la red y tratarse de código dañino desconocido o de software que utiliza herramientas administrativas comunes, invisibles para la capa de Protección.

5.3.6. INFORMACIÓN Y CARACTERÍSTICAS DEL PROCESO DAÑINO

111. La herramienta EDR de análisis forense podrá recuperar del flujo de acciones monitorizadas la siguiente información del proceso dañino:

- Programa del usuario o mecanismo utilizado para la descarga del código dañino.
- Información de contexto del programa utilizado para la obtención del código dañino.
- Línea de comandos utilizada en la invocación de la aplicación dañina.
- Usuario que había iniciado sesión en el equipo en el momento de la infección.
- Cuenta de usuario utilizada para ejecutar el código dañino.

112. El programa de usuario o mecanismo que descargó la amenaza permite determinar el vector de ataque utilizado para la infección: correo, web, dispositivos de almacenamiento removible, programas de mensajería, red local, entre otros.

113. La información de contexto del programa utilizado para la infección mostrará la dirección URL de la página visitada en el caso de que la amenaza haya llegado por web, las cabeceras del correo si se recibió en forma de fichero adjunto, e información similar dependiente del método utilizado para obtención del código dañino en el sistema.

114. La línea de comandos introducidos permite ver los parámetros de ejecución del código dañino y de los programas lanzados por éste. Esta información es útil en labores de análisis forense para aquellas amenazas que utilizan herramientas propias del sistema operativo.

115. La cuenta que ha iniciado sesión en el puesto permite localizar al usuario de la Organización que lo estaba utilizando en el momento de la infección. Con este dato se puede evaluar el nivel técnico del usuario para organizar iniciativas de formación (Formación [mp.per.4]) que eviten futuras infecciones por desconocer los recursos comunes de ingeniería social empleados por los atacantes (ataques de *phishing* y otros).

116. La cuenta de usuario utilizada para lanzar el código dañino permite determinar los privilegios mínimos que tenía la amenaza en el momento de su ejecución. Esta información puede servir para acotar el alcance del incidente de seguridad y determinar si se ha utilizado posteriormente otro conjunto de herramientas para obtener un privilegio superior en el sistema.

5.3.7. HERRAMIENTAS PARA EL ESTUDIO DEL CÓDIGO DAÑINO

117. Para las organizaciones que cuentan con recursos propios dedicados a investigar y clasificar o validar el código dañino, los proveedores pueden ofrecer entornos *sandbox* en los sistemas de información de la Organización, o estar alojados en la nube, así como un servicio de entrega de especímenes de código dañino para su estudio. De esta manera, es posible preparar una ejecución monitorizada de la amenaza controlada por el cliente, y obtener todo su Ciclo de vida sin peligro. A su término, el Administrador de la seguridad del sistema recibirá un informe completo con las acciones del código dañino, así como un análisis estático del fichero, indicando las librerías cargadas y otros datos relevantes. Los entornos de *sandbox* no garantizan la correcta ejecución del código dañino debido a que algunas amenazas avanzadas incorporan mecanismos para evitar ser monitorizadas en equipos virtuales.

5.4. RESPUESTA Y ADAPTACIÓN

118. La fase Adaptación reúne la información obtenida en los pasos anteriores del Ciclo de protección completo para modificar la Política de Seguridad de la Información de la Organización, y así poder bloquear nuevos ataques en la etapa Protección.

119. Las soluciones EDR ofrecerán mecanismos e información para adaptar la Política de Seguridad de la Información, aunque no todas las medidas a tomar entran dentro del ámbito de las herramientas de protección instaladas. Por ejemplo, tras un ataque donde el vector de infección fue un correo no solicitado, está indicado instruir a los usuarios en el uso del correo electrónico según las medidas de seguridad [mp.per.3] “Concienciación” y [mp.per.4] “Formación”; en cambio, si el vector de infección fue una configuración de permisos en los puestos, es conveniente organizar una auditoria de red completa a un proveedor externo que cumpla el articulo 34 (Auditoria de la seguridad) y el Anexo III del ENS para

localizar problemas adicionales que hayan permanecido ocultos a los responsables de seguridad del sistema.

120. Las medidas de adaptación directamente aplicables al software de seguridad son:

- Actualización del comportamiento del código dañino en la capa de protección y detección.
- Actualización del fichero de firmas con la nueva inteligencia de seguridad.
- Actualización de la inteligencia de seguridad almacenada en los puestos y servidores.
- Compartición de la información con herramientas SIEM.
- Reducción de la superficie de ataque.
- Revisión de las excepciones de análisis.
- Inventariado de aplicaciones vulnerables y su actualización.

5.4.1. CORRELACIÓN DEL COMPORTAMIENTO DEL CÓDIGO DAÑINO EN LA CAPA DE PROTECCIÓN Y DETECCIÓN

121. El software EDR puede mostrar mediante un panel de control (*dashboard*) los intentos de intrusión detectados en la capa de Protección y las actividades sospechosas producidas en la capa de Detección, distribuidos por vector de infección y por puesto.

122. La actividad del código dañino, en la mayor parte de los sistemas de información, se concentra en ciertos puestos de usuario. El Administrador de la seguridad del sistema tomará esta información para determinar las causas subyacentes que expliquen los patrones de ataques y bloqueos.

5.4.2. ACTUALIZACIÓN DEL FICHERO DE FIRMAS CON NUEVA INTELIGENCIA DE SEGURIDAD

123. El proveedor de seguridad extrae un identificador de la amenaza hasta ahora desconocida y detectada mediante la monitorización de su actividad, que será incorporado al fichero de firmas automáticamente y descargado por todos los clientes del proveedor. Así, la capa de Protección en todos los puestos de usuario se actualizará con el nuevo identificador y bloqueará inmediatamente cualquier intento de infección posterior.

5.4.3. ACTUALIZACIÓN DE LA INTELIGENCIA DE OTROS DISPOSITIVOS (IOC)

124. El software de seguridad EDR genera un fichero IoC (Indicadores de Compromiso, véase la guía CCN-STIC-423) con los identificadores de los archivos involucrados y las acciones características de la amenaza descubierta.

125. El fichero IoC es enviado al resto de dispositivos del Sistema de información compatibles con el estándar, como por ejemplo UTMs (*Unified Threat Management*, véase Seguridad perimetral y detección de intrusos, CCN-STIC-

432) o proxys con capacidades de protección contra el código dañino, para actualizar su base de conocimiento y reconocer inmediatamente la nueva amenaza, entre otros.

5.4.4. AMPLIACIÓN DE LAS FUENTES DE INTELIGENCIA DE SEGURIDAD

126. El software EDR puede ampliar su número de fuentes de seguridad accesibles y no quedar limitado a la generada por el propio proveedor. En la actualidad, uno de los protocolos de entrega más aceptado en la industria es el intercambio de archivos "IoC", aunque existen otros específicos de fabricantes (Intercambio de información de ciberamenazas. STIX-TAXII. Empleo en REYES, véase Guía CCN-STIC-424).

5.4.5. COMPARTICIÓN DE LA INFORMACIÓN CON HERRAMIENTAS SIEM

127. El software EDR recoge la actividad de los procesos ejecutados en los puestos de usuario y la envía al proveedor, donde se completa con inteligencia de seguridad antes de ser devuelta al servidor SIEM de la Organización. Esta información adicional cubre la peligrosidad de cada acción individual ejecutada por cada uno de los procesos.

128. Con toda la información centralizada en el servidor SIEM de la Organización el administrador puede:

- Relacionar patrones de ejecución y funcionamiento legítimos.
- Identificar secuencias de acciones anteriormente detectadas para penetrar los Sistemas de la Organización, así como anomalías en el comportamiento de las herramientas de seguridad.
- Descubrir el uso de procesos con vulnerabilidades conocidas que todavía no han sido parcheados por los proveedores del software, verificando su ejecución en busca de patrones sospechosos hasta el momento de su parcheo.
- Detectar tráfico de red con destino a direcciones IPs nuevas o situadas en países sin relación con la actividad de la Organización.
- Detectar la aparición de nuevos programas en la red sin clasificar por el proveedor de seguridad. Verificar su ejecución en busca de patrones sospechosos hasta su clasificación.

5.4.6. REDUCCIÓN DE LA SUPERFICIE DE ATAQUE

129. En función del vector de infección empleado por el atacante y del contexto del programa cuando el incidente fue detectado, el software EDR permitirá un refuerzo de la seguridad:

- Evitando la ejecución de las aplicaciones involucradas en el incidente o limitando su comunicación por red.

- Impidiendo el acceso web a las direcciones URLs involucradas en la descarga del código dañino o utilizadas por éste para obtener ficheros o enviar la información recogida o recibir nuevas órdenes de ejecución.
- Incrementando el grado de sensibilidad de la herramienta antispam de la Organización para abarcar valoraciones (*scores*) inferiores.
- Limitando el acceso a dispositivos de almacenamiento removibles, módems y dispositivos externos diversos en los puestos de usuario.
- Impidiendo la ejecución de aplicaciones P2P, mensajería y en general programas que permitan la descarga de ejecutables.
- Limitar el acceso a los Sistemas de Tecnologías de Comunicaciones, configurando reglas más restrictivas en el cortafuegos de los puestos de usuario y servidores.
- Prohibir el acceso a los repositorios de datos remotos mantenidos por los atacantes y descubiertos con las herramientas EDR de análisis forense, así como a los servidores C2 (*Command & Control*) utilizados (véase guía CCN-STIC-425 Ciclo de inteligencia y análisis de intrusiones).
- Limitar la exposición a ataques de red configurando reglas en el cortafuegos y en el módulo HIPS para impedir tráfico mal formado entrante a los puestos de usuario.

5.4.7. LIMITACIÓN DE LA EJECUCIÓN DE APLICACIONES

130. Para limitar la ejecución de aplicaciones, el software EDR implementa listas blancas, listas negras y/o listas dinámicas gestionadas.

131. El enfoque tradicional implica preparar una instalación base en un puesto de usuario donde todos los programas sean legítimos, incluirlos en una lista blanca y denegar la ejecución del software que se encuentre fuera de ella. La desventaja de este enfoque es su mantenimiento, ya que cada vez que un usuario necesita actualizar un programa existente o instalar uno nuevo, es necesario comprobar su seguridad para incluirlo en la lista blanca. Aunque existen algunos métodos que agilizan este proceso añadiendo automáticamente las aplicaciones que vienen de determinados repositorios o los programas que están firmados con certificados emitidos por entidades conocidas, sigue siendo una labor que exige un mantenimiento permanente.

132. El enfoque de listas negras es el que siguen las soluciones EPP mediante el fichero de firmas. Este modelo de seguridad permite la ejecución de todos los programas excepto aquellos que están incluidos en la lista negra. Por esta razón, el software permitido puede ser tanto aplicaciones que el proveedor clasificó anteriormente y comprobó su legitimidad, como programas todavía desconocidos o en proceso de valoración. Este enfoque lleva a permitir la ejecución del software sin clasificar para minimizar los falsos positivos, poniendo en peligro la seguridad de la Organización.

133. El enfoque más avanzado consiste en la generación de listas dinámicas gestionadas, delegando en el proveedor la responsabilidad de determinar qué es

seguro y qué no lo es según sus procesos de monitorización y clasificación continua. De esta manera, el Administrador de la seguridad del sistema no necesita determinar si una aplicación es legítima o dañina, ni mantener las listas blancas o negras a lo largo del tiempo. El bloqueo o ejecución se calcula en función de la clasificación del proceso: el código dañino formará parte de la lista negra y quedará bloqueado, mientras que el código NO dañino (*goodware*) pasará a la lista blanca y se permitirá su ejecución, aunque seguirá siendo monitorizado para descubrir anomalías futuras. Los programas desconocidos por el proveedor son bloqueados temporalmente hasta emitir una valoración definitiva: si son clasificados como código NO dañino (*goodware*) se permitirá su ejecución automáticamente, si resultan ser código dañino, será denegada. Este enfoque solo es viable cuando el proveedor tiene una infraestructura de clasificación desarrollada, que le permita valoraciones rápidas para evitar la inconveniencia de los bloqueos por programas desconocidos que resultaron ser código NO dañino (goodware) una vez completada su clasificación.

134. El enfoque estricto de listas dinámicas según la clasificación del proceso se puede relajar de varias formas:

a) Moviendo elementos de la lista negra o en bloqueo temporal a la lista blanca a petición del Administrador de la seguridad del sistema, añadiendo excepciones que permitan la ejecución de malware conocido (PUPs o programas no deseados) que son considerados dañinos pero que pueden tener alguna funcionalidad valiosa para la Organización.

b) Impidiendo la entrada de elementos desconocidos en la lista negra: éstos pertenecerán a la lista blanca hasta que su clasificación se haya completado, momento en el cual se decide si permanecen allí (*goodware*) o se mueven a la lista negra (código dañino).

c) Aplicando otros criterios adicionales sobre los ficheros desconocidos que aprovechen el contexto para balancear seguridad y conveniencia: bloquear únicamente los programas no vistos anteriormente cuando vienen de una fuente no fiable (como puede ser Internet), derivar la responsabilidad de su ejecución en el propio usuario y otros.

5.4.8. LIMITACIÓN DE ACCESO A LOS FICHEROS CON INFORMACIÓN SENSIBLE O CONFIDENCIAL

135. Para evitar que el *ransomware* y otros tipos de código dañino accedan a ficheros sensibles o confidenciales, se puede limitar el acceso de éstos a ciertos programas determinados, a elección de los responsables de la seguridad del sistema. Así, por ejemplo, si un programa que no sea Microsoft Word intenta abrir un archivo con extensión “.doc / .docx” vería denegado el acceso al fichero. Este tipo de estrategia no evita que un exploit provoque un mal funcionamiento en un programa vulnerable pero legítimo y que acceda a ficheros protegidos indebidamente. Tampoco evita que virus de tipo macro o amenazas que están especialmente diseñadas para valerse de las propias herramientas del sistema operativo accedan a esos ficheros.

5.4.9. BÚSQUEDA DE EQUIPOS EN LA RED CON SOFTWARE VULNERABLE Y FORTIFICACIÓN

136. El software EDR puede realizar un inventario de los programas encontrados en cada puesto de usuario y mostrar aquellos que contengan vulnerabilidades conocidas (véase guía CCN-STIC-431 Herramientas de análisis de vulnerabilidades). El administrador actualizará la configuración de seguridad mediante las acciones siguientes:

- Actualización de la aplicación si existe una versión superior, o parcheo si el proveedor del software ha publicado una solución mediante herramientas de gestión de parches (*Patch Management*) para cumplir con las recomendaciones de seguridad de Gestión de la configuración [op.exp.3] y Mantenimiento [op.exp.4].
- Desinstalación o denegación de ejecución mediante herramientas de tipo Control de aplicaciones.
- Uso de tecnologías antiexploit que impidan la explotación de vulnerabilidades en los programas seleccionados.
- Vigilancia permanente hasta la resolución del problema.

5.4.10. CIFRADO DE FICHEROS SENSIBLES

137. Para evitar que un supuesto atacante obtenga ficheros que contienen información sensible o confidencial, las herramientas EDR facilitarán el uso de los recursos de cifrado del sistema operativo, tales como Bitlocker en el caso de sistemas operativos Windows, o pueden implementar los suyos propios. En cualquier caso, los algoritmos de cifrado implementados por dichas herramientas deberán tener la fortaleza mínima requerida para cada categoría del ENS (véase Guía CCN-STIC-807 Criptología de empleo en el ENS).

5.5. ASPECTOS DE SEGURIDAD EN HERRAMIENTAS EDR

138. Los sistemas de información de las entidades del Sector Público gestionan datos sensibles y confidenciales. Aunque las herramientas EDR no examinan directamente la información almacenada en el sistema de la Organización para detectar amenazas desconocidas, las acciones de monitorización generadas por los procesos suele ser motivo de preocupación para el Administrador de la seguridad del sistema.

139. Por esta razón conviene tener en cuenta una serie de características que minimicen los fallos o el mal uso del software EDR y que puedan provocar filtraciones de datos. Estas funcionalidades se resumen a continuación:

- Entorno de ejecución en nube privada / nube hibrida.
- Control de acceso.
- Comunicaciones cifradas.
- Auditorias de código fuente.

- Registro de actividad.

5.5.1. ENTORNO DE EJECUCIÓN EN NUBE PRIVADA / NUBE HÍBRIDA

140. El esquema de funcionamiento más utilizado por las herramientas EDR consiste en enviar a la infraestructura del proveedor toda la evidencia encontrada en los puestos de los usuarios (acciones monitorizadas y archivos binarios de los programas). De esta manera el análisis de todos los ficheros ejecutables encontrados se centraliza en un único punto y se desarrolla en entornos muy especializados y accesibles para los expertos en código dañino del proveedor.

141. En los casos donde no sea posible enviar la evidencia recogida a la infraestructura del proveedor, se pueden desplegar los recursos necesarios en los sistemas de la Organización para poder clasificar los procesos ejecutados.

142. Este esquema favorece la confidencialidad de los datos ya que todo el proceso se resuelve dentro de la Organización; sin embargo, tiene algunas desventajas:

    - Mayores requisitos de infraestructura en la Organización para alojar los servidores: hardware donde instalar los procesos de clasificación y la consola de administración, licencias de sistemas operativos y bases de datos utilizadas, mayor consumo eléctrico y necesidades de refrigeración, gestión de los servidores / procesos en redundancia, entre otros.
    - Requiere el mantenimiento de los Sistemas instalados: gestión de las garantías del hardware y de las copias de seguridad y restauración, entre otros.
    - Dificultad de acceso a los recursos de la Organización: el proceso de clasificación es en gran medida automático, pero puntualmente se requiere la intervención de personal técnico especializado. Al no disponer de los datos necesarios, esta labor se dificulta. Una solución a este problema consiste es desplazar permanentemente a la Organización un equipo de expertos en clasificación de código dañino.
    - Gestión de la seguridad de la infraestructura de clasificación: configuración de cortafuegos, políticas de seguridad local y otros recursos que impidan la entrada de ataques *Managed*.

5.5.2. CONTROL DE ACCESO

143. Atendiendo a la medida [op.acc], la herramienta EDR limita el acceso a la información al mínimo estrictamente necesario, incorporando las siguientes características:

    - Identificación: se establece el acceso a la herramienta EDR mediante el procedimiento de autenticación en dos fases -según [op.acc.5]- utilizando combinaciones de 2 elementos entre los métodos de autenticación implementados (palabras clave, dispositivos externos, elementos biométricos).

- Separación de tareas: se implementa un sistema de roles para cumplir con las medidas de seguridad [op.acc.3] y [op.acc.4] y limitar los derechos de acceso a la herramienta EDR.

5.5.3. COMUNICACIONES CIFRADAS

144. Las comunicaciones entre todos los elementos que forman parte de la solución EDR deberán establecerse utilizando un canal seguro (TLS 1.2 o superior, HTTPS/TLS, IPSec) en el que se empleen algoritmos criptográficos con la fortaleza mínima requerida, atendiendo a la categoría del sistema (véase Guía CCN-STIC-807 Criptología de empleo en el ENS). Estas comunicaciones serán:

    - La comunicación entre la consola de administración de la herramienta EDR y los recursos alojados en el proveedor (nube pública) o en los sistemas de la organización (nube privada).
    - La comunicación entre el software instalado en los puestos de los usuarios y la infraestructura de clasificación, tanto el envío de monitorizaciones como la recepción de comandos.

5.5.4. CERTIFICACIÓN FUNCIONAL (CRITERIOS COMUNES)

145. La medida de seguridad [op.pl.5] recomienda la utilización de productos cuyas funcionalidades de seguridad hayan sido evaluadas y certificadas conforme a normas europeas o internacionales cuyos certificados estén reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ISO/IEC 15408, Criterios Comunes - Common Criteria - CC) u otras de naturaleza y calidad análogas.

146. El Catálogo de productos de seguridad TIC (CPSTIC) (véase Guia CCN-STIC-105 Catálogo de Productos de Seguridad TIC), ofrece un listado de referencia de productos cuyas funcionalidades de seguridad han sido evaluadas y certificadas de acuerdo a la metodología *Common Criteria* y que han superado con éxito proceso de cualificación diseñado por el CCN para ser utilizados en sistemas del ENS.

5.5.5. REGISTRO DE ACTIVIDAD

147. Según la medida de seguridad [op.exp.8], se recomienda que la herramienta EDR registre la actividad de los usuarios de la consola, indicando quién realiza la actividad, cuándo la ejecuta, de qué tipo de actividad se trata y sobre qué grupo de datos aplica. El registro afecta tanto a las acciones permitidas como a las denegadas según el rol asignado y sus derechos de acceso asociados.

148. Así mismo, se guardarán todos los intentos de acceso al sistema, tanto los concedidos como los denegados.

6. CRITERIOS PARA EL EMPLEO DE HERRAMIENTAS DE SEGURIDAD EN FUNCIÓN DE LA CATEGORÍA DEL SISTEMA DE INFORMACIÓN

149. El cuadro siguiente, en virtud de lo dispuesto en la medida de seguridad [op.exp.6], muestra la utilización deseable de las citadas herramientas de seguridad atendiendo a la categoría del sistema de información de que se trate.

	Categoría del sistema de información		
Tipo de herramienta	**Básica**	**Media**	**Alta**
EPP	Aplica	No aplica	No aplica
EPP + EDR (del mismo fabricante)	Opcional	Aplica	No aplica
EPP + EDR (de distinto fabricante)	Opcional	Opcional	Recomendado

ANEXO A: GLOSARIO DE TÉRMINOS Y ABREVIATURAS

Adaptación	Fase 4 del Ciclo de protección completa donde se reúne la información generada en las fases anteriores para modificar la Política de Seguridad TI.
Amenaza avanzada	Código dañino que hace uso de múltiples técnicas sofisticadas y en su gran parte desconocidas para conseguir principalmente objetivos económicos.
Análisis heurístico	Análisis estático formado por un conjunto de técnicas que inspeccionan el programa sospechoso en base a cientos de características (features) del archivo para determinar la probabilidad de que pueda llevar a cabo acciones dañinas cuando se ejecute en el puesto del usuario.
Análisis forense	Conjunto de técnicas y procesos utilizados por el administrador de seguridad del sistema con herramientas especializadas para seguir la ejecución de programas dañinos y determinar su origen y las consecuencias del incidente.
Análisis por código decompilado	Análisis estático que consiste en obtener el código fuente a partir del binario del programa sospechoso y así determinar la probabilidad de que pueda llevar a cabo acciones maliciosas o dañinas cuando se ejecute en el puesto del usuario.
Análisis por emulación de código	Análisis dinámico que ejecuta durante un tiempo limitado el programa sospechoso en un entorno virtual dentro del puesto del usuario para comprobar si lleva a cabo acciones maliciosas o dañinas.
Anti Spam	Tecnología que busca correos no deseados en función de su contenido.
API	(Application Program Interface) conjunto de funciones y procedimientos que ofrece una biblioteca para ser utilizados por otro software como una capa de abstracción.
APT	(Advanced Persistent Threat) Conjunto de estrategias emprendidas por hackers/atacantes orientadas a infectar la red del cliente, utilizando múltiples vectores de infección simultáneamente para pasar inadvertidos a los antivirus tradicionales durante largos periodos de tiempo. Su objetivo principal es económico (robo de información confidencial y propiedad intelectual de la empresa).
Archivo de Identificadores	(fichero de firmas) Fichero que contiene los patrones que el antivirus utiliza para detectar las amenazas.

Bitlocker	(BitLocker Drive Encryption) Programa que permite cifrar discos en las versiones Ultimate y Enterprise de Windows Vista y Windows 7 así como en las versiones para empresas de Windows Server 2008.
BOTNet	Red de ordenadores infectados y controlados por una misma persona u organización para minar bitcoins, enviar correos no deseados o atacar por denegación de servicio a empresas y organismos públicos.
C2	(Command & Control) Infraestructura que consta de un servidor centralizado o distribuido para el control del comportamiento del código dañino desplegado, que generalmente toma la forma de una BOTNet.
CC	(Criterios Comunes - Common Criteria) Conjunto de estándares sobre seguridad de productos software aplicados en diferentes países con el fin de que establecer un marco evaluación comparable.
Ciclo de protección Completa	Nuevo paradigma de seguridad que admite la imposibilidad de desarrollar una barrera infranqueable ante el 100% de las amenazas en circulación. Dispone de recursos para detectar código dañino desconocido y herramientas que resuelven el incidente y aportan toda la información necesaria para modificar la Política de seguridad TIC.
Ciclo de vida del Malware	Detalle de todas las acciones desencadenadas por un programa dañino, desde que fue visto por primera vez en un equipo del cliente hasta su clasificación como dañino y posterior desinfección.
Clasificación	Conjunto de procesos semiautomáticos que permiten determinar si un programa es seguro o contiene código dañino.
Control de aplicaciones	Módulo que define el comportamiento de las aplicaciones ejecutadas en el puesto del usuario, permitiendo su bloqueo o impidiendo el acceso a determinados recursos del sistema operativo.
Control de dispositivos	Módulo que permite definir el comportamiento del equipo protegido al conectar dispositivos extraíbles o de almacenamiento masivo, para minimizar su superficie de exposición.
Cortafuegos	(Firewall) Tecnología que bloquea el tráfico de red que coincide con patrones definidos por el Administrador de la seguridad del sistema mediante reglas, limitando o impidiendo completamente la comunicación de ciertas aplicaciones que se

	ejecutan en los puestos y restringiendo su superficie de exposición.
CVE	(Common Vulnerabilities and Exposures) lista de información definida y mantenida por The MITRE Corporation sobre vulnerabilidades conocidas de seguridad. Cada referencia tiene un número único que la identifica, ofreciendo una nomenclatura común para el conocimiento público de este tipo de problemas y así facilitar la compartición de datos sobre dichas vulnerabilidades.
CKC (Cyber Kill Chain)	Concepto acuñado por analistas de Lockheed Martin Corporation que representa un ataque informático avanzado mediante una cadena o secuencia de 7 pasos que un atacante tiene que recorrer para introducirse en un sistema y conseguir sus objetivos.
Cuarentena	Área de almacenamiento de ficheros dañinos no desinfectables.
Dashboard	Panel de control formado por elementos gráficos (*widgets)* que permiten valorar rápidamente el estado de la seguridad de los Sistemas de información.
Desbordamiento de buffer	Fallo en la gestión de los buffers en la entrada de un proceso. Si el volumen de datos recibido es mayor que el tamaño de memoria reservado, los datos sobrantes no se descartan, sino que se escriben en zonas adyacentes al buffer, que pueden ser interpretadas como código ejecutable en sistemas anteriores a la aparición de la tecnología DEP.
Detección	Fase 2 del Ciclo de protección completa donde se monitorizan los procesos ejecutados en el puesto del usuario y se envía la información en bruto generada a la infraestructura del proveedor de seguridad para su análisis.
DEP	Característica de los sistemas operativos y plataformas hardware que impide la ejecución de páginas de memoria destinadas a datos y marcadas como no ejecutables. Esta característica se diseñó para prevenir la explotación de fallos por desbordamiento de buffer.
EDR	(Endpoint Defense and Response) Nueva categoría de herramientas de seguridad orientada a detectar investigar y resolver actividades sospechosas en puestos de usuario y servidores.
EPP	(Endpoint Protection Platform, antivirus) Categoría de herramientas de seguridad orientadas a proteger los puestos de usuario y servidores del código dañino conocido.

Exploit	Secuencia de datos especialmente diseñada para provocar un fallo controlado en la ejecución de un programa vulnerable. Después de ejecutarse el exploit, el proceso comprometido interpretará por error parte de la secuencia de datos como código ejecutable, desencadenando acciones peligrosas para la seguridad del puesto
Features	Características presentes en las cabeceras de los ficheros binarios y analizados por los algoritmos heurísticos para determinar su peligrosidad.
Fichero de firmas	Ver **Archivo de identificadores**.
Fileless	Amenazas que no depositan ficheros en el disco duro del puesto del usuario, con lo cual dificultan su detección por los antivirus tradicionales EPP.
Filtrado de URLs	Módulo que impide la navegación de los puestos y servidores por determinadas categorías de webs.
Firma	(Identificadores) Mezcla de patrones y código que representan un malware o familia, incluida en el fichero de firmas.
Gadgets	Secciones de código legítimo de los procesos vulnerables, ejecutados por las amenazas que intentan explotarlos para provocar su malfuncionamiento.
Goodware	Fichero clasificado como legítimo y seguro tras su estudio.
Gusanos	Código dañino con la propiedad de duplicarse a sí mismo sin la intervención del usuario.
HIPS	(Host Intrusion Protecionт System) Módulo que detecta y rechaza el tráfico mal formado y especialmente preparado para impactar en el rendimiento o la seguridad del puesto de usuario o servidor protegido.
IR	(Incident Response) Categoría de herramientas diseñadas para gestionar y minimizar los daños provocados por un incidente de seguridad.
IoC	Conjunto de estándares tecnológicos centrados en describir las características técnicas de las amenazas para poder comunicarlas a personas o a productos y dispositivos de seguridad dentro de los Sistemas de información.
IoT	(Internet of Things, Internet de las cosas) Concepto que se refiere a la interconexión digital de objetos cotidianos con Internet.

Insiders	Usuarios de la organización.
Lista blanca	Listado de ficheros o programas mantenido de forma manual cuya ejecución está permitida por considerarse segura.
Lista dinámica	Listado de ficheros o programas mantenido de forma automática que indica si un programa puede ser ejecutado o no por considerarse peligroso.
Lista negra	Listado de ficheros o programas mantenido de forma manual cuya ejecución está prohibida por considerarse peligrosa.
Machine learning	(Algoritmos de autoaprendizaje) Rama de la inteligencia artificial cuyo objetivo es desarrollar técnicas capaces de generalizar comportamientos a partir de información no estructurada suministrada en forma de ejemplos.
Malware	Término general utilizado para referirse a programas que contienen código dañino (MALicious softWARE), ya sean virus, troyanos, gusanos o cualquier otra amenaza que afecta a la seguridad, disponibilidad e integridad de los sistemas informáticos. El código dañino se infiltra y daña un ordenador sin el conocimiento de su dueño, con finalidades muy diversas.
Managed attacks	En contraposición a las amenazas de tipo dañino, que automatizan mediante programas informáticos un conjunto de procesos orientados a obtener un beneficio para el atacante, los Managed Attacks son ataques a los sistemas de información de las Organizaciones asistidos directamente por personal humano.
Modelo de Madurez de Seguridad	(CMM - Capacity Maturity Model) Modelo de evaluación de los procesos relativos a la seguridad en las Organizaciones para medir su grado de madurez. Se definen 5 niveles de clasificación de Sistemas de la información.
Movimiento	Movimiento del código dañino de un equipo a otro dentro de un sistema de información, evitando la protección perimetral de la organización.
Nube	(Cloud Computing) Tecnología que permite ofrecer servicios a través de Internet. En este sentido, la nube es un término que se suele utilizar como una metáfora de Internet en ámbitos informáticos.
Paciente cero	Primer puesto de usuario o servidor infectado en la red.
Patch	Herramienta que automatiza el descubrimiento y aplicación de los nuevos parches que publican los proveedores de software.

Payload	En ciertos tipos de código dañino, las tareas de penetración en los sistemas de información están separadas de las acciones dañinas ejecutadas una vez sorteada la capa de Protección. Este código "útil" (carga útil – Payload) es descargado desde fuentes externas (Internet) una vez que se han sorteado las defensas.
Pirámide de	Estructura gráfica que representa el volumen de los diferentes tipos de activos informáticos en las organizaciones.
Powershell	Intérprete de línea de comandos avanzada para Windows, sucesora de Command.com.
Proceso comprometido	Procesos vulnerables que han sido afectados por un exploit y pueden comprometer la seguridad del equipo de usuario.
Proceso vulnerable	Programas que, debido a fallos en su desarrollo, no son capaces de interpretar correctamente los datos que reciben. Al recoger una secuencia de datos especialmente diseñada (exploit), los atacantes pueden provocar el mal funcionamiento del proceso, induciendo la ejecución de código que compromete la seguridad del puesto del usuario.
Protección anti-exploit	Técnicas que detectan la inyección de código dañino en el espacio de memoria de procesos vulnerables, bloqueándolos o cerrando el proceso comprometido.
Protección y Prevención	Fase 1 del Ciclo de protección completa, equivalente a la funcionalidad encontrada en herramientas de seguridad EPP. Consiste en una capa de protección que impide la infección de los puestos y servidores por código dañino conocido.
PUPs	(Programas potencialmente no deseados, Grayware) Son programas que se introducen de forma invisible o poco clara en el equipo aprovechando la instalación de otro programa que es el que realmente el usuario desea instalar.
Ransomware	(Ransom) Tipo de código dañino especialmente peligroso que impide el acceso a los ficheros de datos del usuario, cifrándolos y pidiendo un rescate a cambio de una contraseña de recuperación.
Resolución y Respuesta	Fase 3 del Ciclo de protección Completo donde se emprenden acciones para mitigar el incidente.
Rol	Configuración específica de permisos y privilegios que se aplica a una o más cuentas de usuario y autoriza a ver o modificar determinados recursos de la consola de administración.
Rootkits	Programa diseñado para ocultar objetos como procesos,

	archivos o entradas del Registro de Windows (incluyendo los suyos propios). Este tipo de software es utilizado para esconder evidencias y utilidades en sistemas previamente comprometidos.
ROP	Técnica utiliza por exploits que permite a un atacante ejecutar código arbitrario en presencia de defensas como DEP o ASLR, sobrescribiendo la pila de llamadas (call stack) en los procesos para ejecutar zonas de código del propio proceso, conocidas como “gadgets”. El atacante puede "armar" un flujo de ejecución alternativo al del programa original, formado por partes de código del proceso atacado.
Sample	Código dañino normalizado para empresas con laboratorio propio de estudio de amenazas.
Sandbox	Entorno de ejecución aislado donde es posible ejecutar los programas sospechosos de contener código dañino para monitorizar su comportamiento. Los entornos de *sandbox* se despliegan en su mayoría sobre máquinas virtuales, dificultando la detección de determinados tipos de amenazas sofisticadas.
Score	Cifra que indica la probabilidad de que el fichero sospechoso será realmente código dañino**.**
SIEM	(Security Information and Event Management) Software que ofrece almacenamiento y análisis en tiempo real de las alertas generadas por los Sistemas de Tecnologías de la Información y Comunicaciones.
Sospechoso	Ver **grayware**.
STIX	Lenguaje estandarizado y estructurado para describir la información sobre amenazas con el objetivo de compartirla**.**
Targeted attacks	Ataques muy específicos a blancos concretos que se apartan del ámbito generalista.
TAXII	Conjunto de servicios y formatos que permiten el intercambio de información sobre amenazas entre organizaciones, automáticamente y en tiempo real.
Tiempo de Exposición	Tiempo que una amenaza ha permanecido sin ser detectada en un equipo de la red.
Timeline	Cronología de acciones ejecutadas por el código dañino.
Troyano	Programa que llega al ordenador de manera encubierta, aparentando ser inofensivo, se instala y realiza determinadas

	acciones que afectan a la confidencialidad del usuario.
UTMs	(Unified Threat Management) dispositivo de red con múltiples funciones de seguridad como cortafuegos, antivirus, sistema de prevención de intrusos y otros.
Vector de infección	Puerta de entrada o procedimiento utilizado por el código dañino para infectar el equipo del usuario. Los vectores de infección más conocidos son la navegación web, el correo electrónico y los dispositivos de almacenamiento removible (USB).
Ventana de Oportunidad	Tiempo que transcurre desde que el primer equipo fue infectado a nivel mundial por una muestra de código dañino hasta su estudio e incorporación a los ficheros de firmas. Durante este periodo de tiempo la amenaza puede infectar equipos sin que los antivirus tradicionales sean conscientes de su existencia.
Virus	Programa que se introduce en los ordenadores y sistemas informáticos de formas muy diversas, produciendo efectos molestos, nocivos e incluso destructivos e irreparables.
Vulnerabilidad	Fallo en el diseño de un programa que permite a los atacantes provocar un funcionamiento erróneo que compromete la seguridad de los Sistema de información y las comunicaciones.
WSH	(Windows Scripting Host) Motor de ejecución de scripts en sistemas operativos Windows, equivalente a los archivos de procesamiento por lotes.
WMI	(Windows Management Instrumentation) Conjunto de extensiones que ofrecen una interface homologada a los recursos de notificación de los sistemas operativos Windows.

ANEXO B: REFERENCIAS

CCN-STIC-818	Herramientas de seguridad en el ENS.
CCN-STIC-808	Verificación del cumplimiento del ENS.
CCN-STIC 911A	Ciclo de una APT.
CCN-STIC-425	Ciclo de inteligencia y análisis de intrusiones.
CCN-STIC-423	Indicadores de compromiso (IoC).
CCN-STIC-432	Seguridad perimetral (detección de intrusos).
CCN-STIC-424	Intercambio de información de ciberamenazas STIX-TAXII. Empleo en Reyes.
CCN-STIC-431	Herramientas de análisis de vulnerabilidades.
CCN-STIC-807	Criptología de empleo en el ENS.
CCN-STIC-105	Catálogo de Productos de Seguridad TIC