centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 498

Arquitectura multidominio de Puesto de Trabajo (*End Point Seguro*)

Junio 2020

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2020.06.04 16:09:31 +02'00'

NIPO: 083-20-098-3

Fecha de Edición: Junio 2020

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

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 y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del 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, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, 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 la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Junio de 2020

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN

1. El despliegue de Tecnologías de la Información y las Comunicaciones (TIC) basado en redes de comunicación de mayor o menor extensión, se compone de equipos que permiten la transmisión, almacenamiento o procesamiento de la información, junto con terminales en los cuales los usuarios finales pueden manejar esta información. Dichos terminales de usuario, conocidos en el contexto de este documento con el término ***end point (EP)***, abarcan plataformas o sistemas finales, fijos o móviles, que un usuario de una red de comunicaciones utiliza como puesto de trabajo.

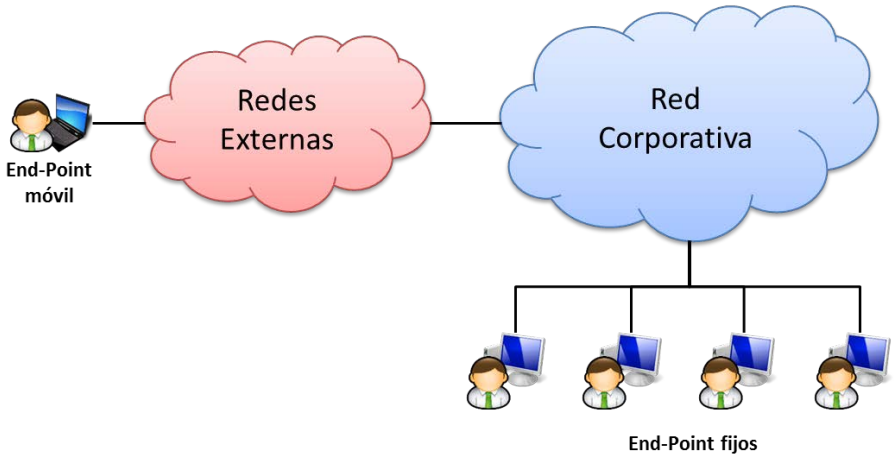

Figura 1. *End points* fijos y móviles

2. En este escenario, es bastante común que surjan necesidades operativas de manejar información que, por su naturaleza, presenta diferentes exigencias en cuanto a confidencialidad, integridad o disponibilidad, o incluso pertenece a ámbitos diferentes (Nacional, OTAN, UE, etc.). Así, podríamos diferenciar entre información sensible, de acuerdo con la categorización del ENS, e información clasificada, que es aquella información cuya divulgación no autorizada puede, además, dañar o poner en riesgo la seguridad y defensa del Estado, y que debe ser protegida de acuerdo con normativa nacional o internacional.

3. En el ámbito normativo, el Esquema Nacional de Seguridad, establece los principios básicos y requisitos mínimos que permiten la protección adecuada de la información sensible (no clasificada) en la Administración Electrónica Española, mientras que los requisitos para la protección de información clasificada, en España, son publicados por la Oficina Nacional de Seguridad (ONS), dependiente del Centro Nacional de Inteligencia (CNI), siguiendo las directrices de la Autoridad Nacional de Seguridad Delegada (ANS-D).

4. En cualquiera de estos ámbitos (información sensible o clasificada), son habituales los escenarios en los que se maneja información que exige diferentes niveles de seguridad (sistemas multidominio), lo que obliga a trabajar en equipos diferenciados, o bien en uno que implemente los requisitos de seguridad para la protección de la información más sensible, pero que podría resultar excesivo en lo que respecta a la información menos sensible y plantear problemas en su operación

5. Por lo tanto, es necesario diseñar una arquitectura que posibilite el manejo de cualquier tipo de información (siempre y cuando la normativa lo permita) en un único equipo *end point* adecuado para tal fin, de modo que las medidas de seguridad aplicadas sean las estrictamente necesarias.

6. La arquitectura propuesta se basa en el empleo de entornos de escritorio remoto o entornos virtualizados que permiten abstraer los recursos *hardware* de la máquina física (*host*) del *firmware* y *software* del sistema, de forma que se pueden dividir los recursos existentes en el host entre los diferentes entornos o dominios de seguridad.

2. OBJETO

7. El presente documento tiene como objetivo establecer una arquitectura de *end point* seguro que permita a un usuario de un sistema TIC manejar información de diferentes niveles de seguridad (desde el mismo terminal con las debidas garantías).

8. Se denomina sistema al conjunto de equipamiento *hardware*, sistema operativo y aplicaciones *software* que manejen un tipo de información en un ámbito determinado.

9. En concreto, para la arquitectura mencionada, se determinarán las medidas de seguridad asociadas a los siguientes ámbitos:

    a) **Esquema Nacional de Seguridad.**

    b) **Información Clasificada nacional o procedente de organizaciones internacionales.**

10. Es importante destacar que las arquitecturas planteadas en el presente documento deben tomarse como un conjunto de soluciones que dan respuesta a la necesidad de manejar en un mismo *end point* información de distintos dominios de seguridad. En ningún momento deben tomarse como un conjunto exclusivo y limitante de soluciones, ya que pueden existir otras alternativas igualmente válidas que cumplan con los requisitos establecidos por la normativa vigente para cada ámbito y que deberán analizarse caso por caso.

3. ESTRUCTURA DEL PRESENTE DOCUMENTO

11. El presente documento se estructura en los siguientes apartados que recogen los diferentes objetivos de seguridad, las condiciones de uso, las posibles arquitecturas y las distintas medidas de seguridad en función del tipo de información a manejar, además de los correspondientes apartados con definiciones, referencias y abreviaturas:

    a) **Apartado 4**. Objetivos de seguridad. En este apartado se presentan los objetivos de seguridad a alto nivel que debe implementar el *end point* con objeto de proteger a sus activos.

    b) **Apartado 5**. Entorno operativo. En este apartado se describen las condiciones de entorno que se han considerado a la hora de definir qué medidas de seguridad debe implementar el *end point*.

    c) **Apartado 6**. Análisis de arquitecturas. En él se describen los diferentes tipos de arquitecturas de *end point* que se van a considerar en este documento, junto con sus principales características técnicas.

    d) **Apartado 7**. Medidas de seguridad. En este apartado se describen, de manera genérica, todas las medidas de seguridad que pueden utilizarse de cara a satisfacer los objetivos de seguridad descritos en el apartado 4.

    e) **Apartado 8**. En él se describe qué medidas de seguridad son de aplicación para un *end point* que maneje información clasificada y se particularizan teniendo en cuenta la normativa existente y atendiendo a los diferentes niveles de clasificación.

    f) **Apartado 9**. En este apartado se describen las medidas de seguridad que son de aplicación para un *end point* en el ámbito del ENS.

    g) **Los casos de uso específicos asociados a las arquitecturas descritas en este documento serán publicados en anexos independientes que se nombrarán de misma forma que la presente guía más un carácter alfabético consecutivo: CCN-STIC-498A[1], CCN-STIC-498B, etc.**

[1] Casos de uso de end point con dominios de seguridad Difusión Limitada de diferentes ámbitos Sin Clasificar con acceso a internet

4. OBJETIVOS DE SEGURIDAD

12. A continuación, se detallan los **objetivos de seguridad** para la arquitectura objeto de diseño:

a) **Protección de la información**. El *end point* deberá tener la capacidad de manejar de manera segura información sensible o clasificada que demande protección en cualquiera de sus tres (3) dimensiones de seguridad (confidencialidad, integridad y disponibilidad), en su almacenamiento, procesamiento y transmisión. Para ello, deberá implementar:

- **Control de los flujos de información:** Los flujos de información estarán restringidos, físicamente o mediante configuración software, a las interfaces habilitadas. Se protegerá la confidencialidad, integridad y autenticidad, lo que impedirá el establecimiento de canales encubiertos que faciliten la transmisión no autorizada de información entre los distintos Sistemas que forman parte del *end point* o entre éstos y el exterior.
- **Aislamiento de los recursos asignados a cada dominio de seguridad**. El *end point* debe garantizar la separación de los distintos dominios de seguridad, de forma que no se produzca trasvase de información entre dichos dominios, salvo los que estén autorizados, que deberán ser debidamente controlados y monitorizados.
- **Acceso autorizado a la información**. El *end point* debe garantizar el acceso a la información de cada dominio de seguridad únicamente al personal que esté debidamente autorizado.

b) **Protección de la funcionalidad principal del *end point***. El *end point* deberá protegerse de ataques (actualizaciones no permitidas, *malware*, etc.) que puedan alterar su correcto funcionamiento y en especial sus funcionalidades de seguridad críticas.

c) **Aislamiento de fallos**: Un fallo en un sistema no deberá transmitirse en cascada al resto, de tal forma que se permita la detección, contención y recuperación de forma local.

5. ENTORNO OPERATIVO

13. El entorno operativo para este tipo de soluciones puede ser muy variable, desde terminales en una red corporativa, que podrían disponer de medidas adecuadas de protección y encontrase en zonas protegidas (como puede ser una Zona de Acceso Restringido o una Zona administrativa de protección), a terminales de usuarios desplegados que deben conectarse a las redes corporativas a través de redes inseguras o que se encuentran completamente aislados y no se conectan a red alguna (pero que están desplegados en entornos inseguros o no controlados).

14. A efectos de seguridad, se asume que el *end point* debe reunir las condiciones de seguridad adecuadas para su autoprotección, independientemente de la arquitectura global de seguridad existente.

15. Asimismo, se supone que los diferentes sistemas operativos empleados en el *end point* están correctamente configurados y pueden ser actualizados de forma periódica, independientemente del entorno operativo del citado terminal.

6. ANÁLISIS DE ARQUITECTURAS

16. Teniendo en cuenta los requisitos y condiciones anteriormente expuestas, en el siguiente análisis se describen tres (3) posibles arquitecturas utilizadas en sistemas multidominio.

17. Para cumplir los requisitos de seguridad indicados, se propone el uso de **entornos virtualizados**, dado que esta tecnología permite introducir mediante *software* una capa de abstracción entre los recursos *hardware* de la máquina física (*host*) y los sistemas ejecutados en una o varias instancias virtuales, de tal forma que se dividen dichos recursos entre los diferentes entornos de ejecución.

18. El **hipervisor, o Monitor de Máquinas Virtuales (VMM)**, es un componente software que permite al equipo físico soportar los distintos entornos virtuales con sus configuraciones. Cada entorno virtual se encapsula en **una máquina virtual (VM)** que tiene asignados unos recursos virtuales, como memoria, procesador, SO invitado y aplicaciones.

19. En las arquitecturas presentadas se contempla el uso de dos (2) tipos de hipervisores:

    a) **Hipervisor tipo 1 o nativo**: Es el *software* que se ejecuta directamente sobre el *hardware* para ofrecer la funcionalidad propia del hipervisor. También denominado *unhosted* o *bare metal* (en terminología anglosajona, sobre metal desnudo), ya que está implementado en la propia máquina.

    b) **Hipervisor tipo 2 o *hosted***: Es un *software* que se ejecuta sobre un sistema operativo instalado en el terminal para ofrecer la funcionalidad de hipervisor.

20. Los ejemplos y gráficos expuestos en el presente documento se plantean para una arquitectura de dos niveles de seguridad (n=2). No obstante, puede generalizarse fácilmente para un número de niveles n=N -aplicando a cada *host* o máquina virtual las medidas de seguridad indicadas para el nivel de seguridad requerido -, o para el caso trivial de n=1 en el que no se contempla el multidominio sino un único *host* o máquina virtual.

6.1 ARQUITECTURA *END POINT* TIPO 1: MÁQUINAS VIRTUALES SOBRE HIPERVISOR NATIVO

21. En este caso, el manejo de la información en el *end point* se habilitará únicamente en máquinas virtuales ejecutadas sobre un hipervisor nativo o tipo 1 instalado en el equipo (*host*), una para el manejo de la información de bajo nivel de seguridad y otra para el manejo de la información de nivel alto de seguridad.

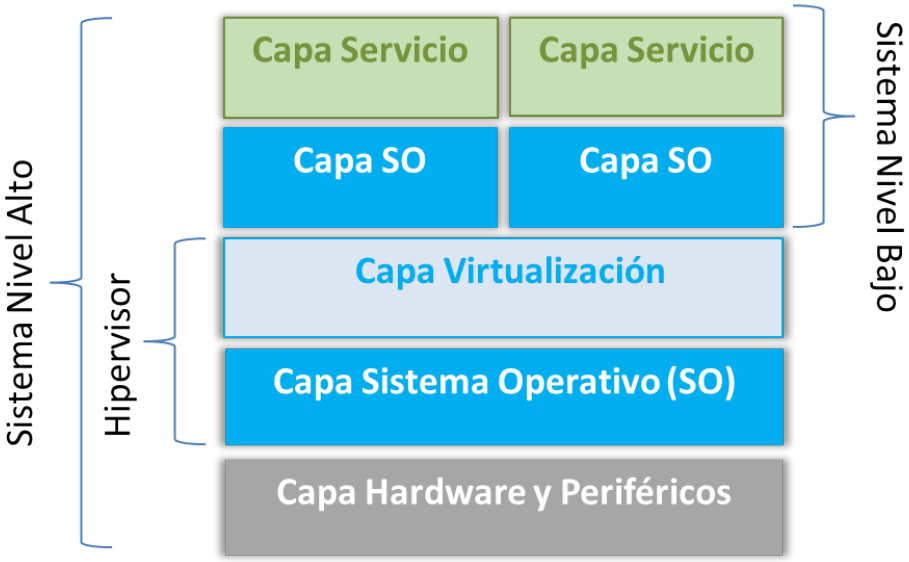

Figura 2. Arquitectura *end point* tipo 1

22. La capa de virtualización permitirá proteger los recursos de la máquina virtual de nivel alto para que no sean accesibles desde la otra máquina de nivel bajo, y se impedirán los flujos de información en todas las capas OSI (p.ej.: a través de recursos compartidos, interfaces de red, etc.) a excepción de la interfaz USB limitada a los dispositivos *hardware* específicamente autorizados en las máquinas virtuales. Del mismo modo, en la capa de virtualización se configurarán las interfaces necesarias para que la máquina virtual de nivel bajo tenga acceso a red y a cualquier dispositivo USB autorizado.

23. Aunque el Sistema Nivel Bajo hace uso de todas las capas inferiores (Virtualización, Sistema Operativo, Hardware y Periféricos), éstas se consideran parte del Sistema Nivel Alto, dado que deben implementar las medidas de protección asociadas al Nivel Alto.

24. La adecuada configuración del *host* deberá restringir su uso al despliegue de las correspondientes máquinas virtuales por parte de los usuarios y a tareas de mantenimiento por parte de los administradores.

6.2 ARQUITECTURA *END POINT* TIPO 2: *HOST* Y MÁQUINA VIRTUAL SOBRE HIPERVISOR TIPO 2

25. En esta arquitectura, en el *end point* se habilita el manejo de la información de nivel alto de seguridad directamente soportado en el sistema operativo del equipo (*host*). Mientras que el Sistema que maneja información de nivel bajo de seguridad se implementaría en una máquina virtual.

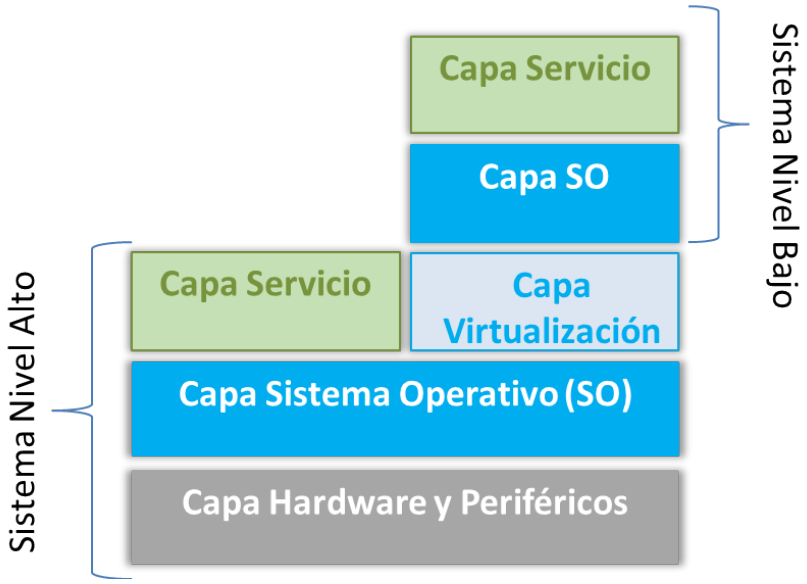

Figura 3. Arquitectura *end point* Tipo 2

26. Una capa de virtualización permitiría ejecutar en el *host* una máquina virtual (MV) para el manejo de la información de nivel bajo. La capa de virtualización actuaría como un contenedor que **impediría:**

    a) El acceso desde la máquina virtual al resto de recursos del *host*.
    b) Los flujos no autorizados de información entre el *host* y la máquina virtual en todas las capas OSI (p.ej.: a través de recursos compartidos, interfaces de red, etc.),

27. Al igual que en el caso de la Arquitectura Tipo 1, las capas de Virtualización, Sistema Operativo, Hardware y Periféricos se consideran parte del Sistema Nivel Alto, dado que deben implementar las medidas de protección asociadas al Nivel Alto.

28. En cuanto a las interfaces USB, estas estarán limitadas a los dispositivos *hardware* específicamente autorizados en la máquina virtual.

6.3 ARQUITECTURA *END POINT* TIPO 3: *THIN-CLIENT* CON VDI

29. La tecnología VDI (*Virtual Desktop Infrastructure*) provee y permite gestionar escritorios virtuales mediante una arquitectura cliente-servidor en la que el *end point* (actuando como cliente) cuenta con una configuración mínima (*thin client*) y delega la mayor parte del procesamiento en los servidores centralizados en los que residen los escritorios virtualizados. De esta forma, el usuario puede interactuar a través del *end point* con las aplicaciones/escritorios virtualizados ejecutados en el servidor.

30. Los dispositivos *thin client* pueden concebirse para ejecutar únicamente determinadas aplicaciones o programas de escritorio remoto soportados sobre un sistema operativo con funcionalidades muy reducidas que podría quedar embebido en una memoria de solo lectura.

31. En este tipo de arquitectura, el procesamiento y almacenamiento de la información se realiza en sendas infraestructuras de red, una de menor nivel de seguridad y otra de mayor nivel de seguridad, lo que permite el aislamiento de los datos y recursos utilizados en cada caso mientras el usuario interactúa alternativamente con ellos desde el *thin client* a través de escritorios virtualizados en un servidor remoto.

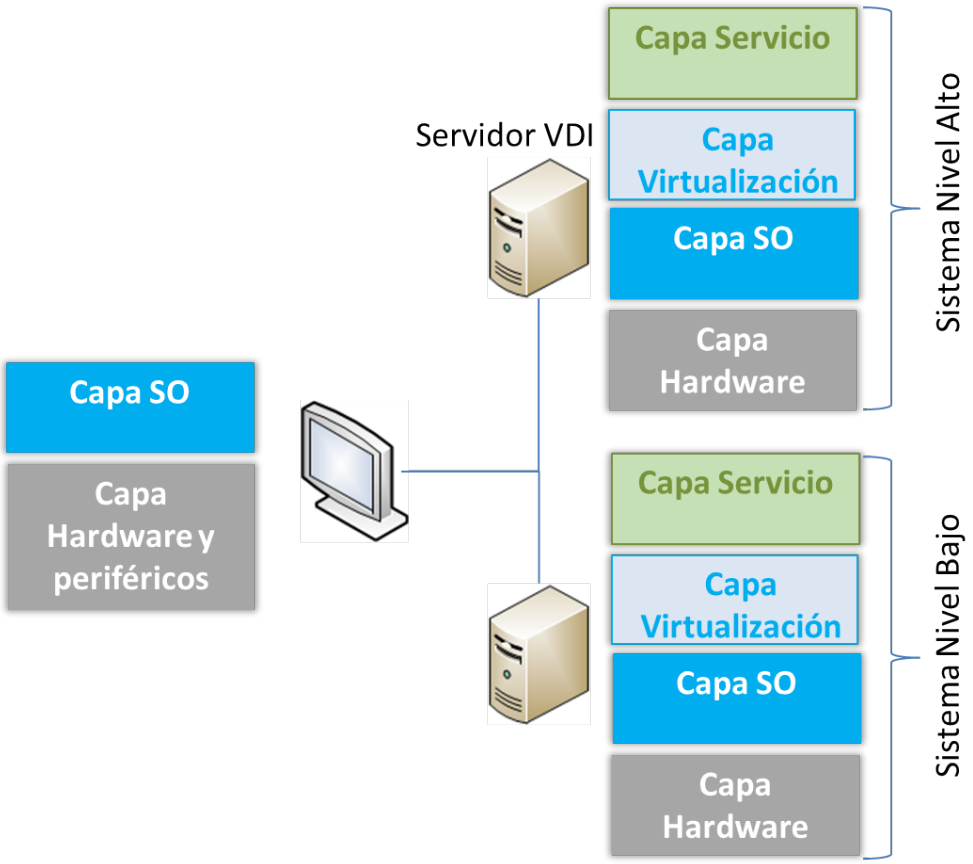

Figura 4. Arquitectura para *end point* con *Thin-Client*

32. La configuración segura en este escenario debe extenderse conforme a la normativa aplicable a las redes y a las conexiones con estas desde el *end point,* ya que por ellas fluirá la información, incluyendo la de nivel alto entre su respectiva red y el correspondiente escritorio virtualizado en el *thin client*. De este modo, varios de los requisitos impuestos a la arquitectura para *end point* deberían ser directamente delegados en la infraestructura que soporta los servicios remotos.

33. Uno de los factores determinantes para la adopción de esta solución es la necesidad de disponer de conectividad de red entre el extremo servidor y el *end point* para el acceso remoto al escritorio virtual, en particular, el proporcionado para el Sistema de Nivel Alto con los requisitos de protección de comunicaciones requerido (como es el caso de los cifradores a emplear para acceder a información de nivel alto).

6.4 CARACTERÍSTICAS DE USO Y MANTENIMIENTO DE LAS SOLUCIONES PLANTEADAS

34. La Tabla 1 recoge las características de uso y mantenimiento inherentes a cada una de las arquitecturas planteadas en los apartados anteriores:

	USABILIDAD	MANTENIMIENTO
ARQUITECTURA 1 (MÁQUINAS VIRTUALES SOBRE HIPERVISOR TIPO 1)	• Necesidad de arrancar el entorno virtual para el manejo de información de ambos niveles.	• Gestión simplificada mediante distribución de imágenes virtuales estandarizadas para ambos niveles.
ARQUITECTURA 2 (HOST Y MÁQUINA VIRTUAL SOBRE HIPERVISOR TIPO2)	• Necesidad de arrancar el entorno virtual para el manejo de información en el Sistema de Nivel Bajo.	• Gestión simplificada mediante distribución de imágenes virtuales estandarizadas para el nivel bajo.
ARQUITECTURA 3 (THIN-CLIENT CON ESCRITORIOS VIRTUALES REMOTOS E INDEPENDIENTES)	• Condicionado a la conectividad con la infraestructura de virtualización. Imposibilidad de almacenar información en el *thin client*.	• Fundamentalmente centrado en la infraestructura VDI. • Enfocado a un volumen relevante de *end points* estandarizados y no a soluciones individualizadas. • Requiere administración de las comunicaciones cliente-servidor. • Proporciona centralización de la gestión de copias y eventos de seguridad.

Tabla 1.- Características de uso y mantenimiento de las arquitecturas planteadas

7. MEDIDAS DE SEGURIDAD

35. Partiendo de las arquitecturas definidas en la sección anterior para la implementación del *end point,* a continuación, se detallan cada uno de los componentes y las medidas de seguridad que deberían implementarse para cumplir con los objetivos de seguridad referidos en la sección 3, sin perjuicio de otras medidas de seguridad aplicables por requisitos normativos y/o funcionales adicionales que existan en el contexto de cada organización.

36. Dependiendo de la arquitectura seleccionada, estos mecanismos serán implementados en una única máquina, cuando se trata de un end *point* tipo host con capacidades de virtualización (arquitecturas tipos 1 y 2) o aplicables a toda una infraestructura distribuida como en el caso de la arquitectura tipo 3, en el que el *end point* está compuesto por un *thin client* y uno o varios servidores de virtualización VDI pertenecientes a una o distintas redes.

37. La Figura 5 muestra un esquema de las medidas de seguridad consideradas para cada una de las capas o niveles del sistema:

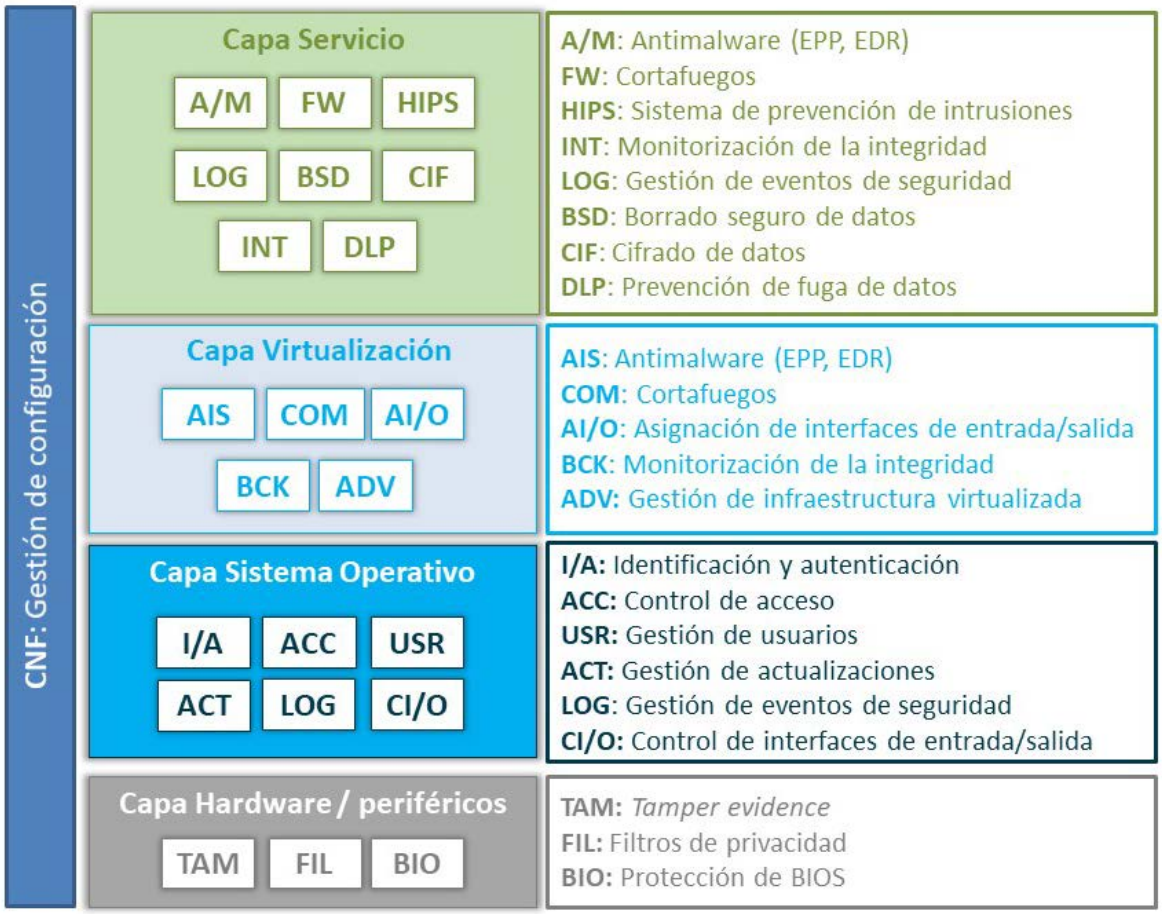

Figura 5. Medidas de seguridad por capas

38. La configuración de estas medidas de seguridad deberá ser realizada siempre por administradores y, por defecto, se limitará el acceso a funciones de configuración al resto de usuarios.

7.1 DESCRIPCIÓN DE MEDIDAS DE SEGURIDAD APLICABLES A TODAS LAS CAPAS (HARDWARE, SISTEMA OPERATIVO, VIRTUALIZACIÓN Y SERVICIO)

7.1.1 GESTIÓN DE CONFIGURACIÓN (CNF)

39. Abarca el proceso de provisión, configuración inicial y gestión continua de la configuración de los dispositivos y sistemas operativos. Para ello, se recomienda la utilización de productos tipo UEM (*Unified EndPoint Management*) en las redes de la organización. De esta forma, se controlará y administrará de manera centralizada la configuración de los *End Point*.

7.2 DESCRIPCIÓN DE MEDIDAS DE SEGURIDAD *HARDWARE*

7.2.1 *ANTI-TAMPERING* (TAM)

40. Esta tecnología consiste en utilizar diferentes mecanismos para prevenir, detectar o responder ante la manipulación no autorizada de los elementos *hardware* de un dispositivo.

41. Existen diversos mecanismos *anti-tampering* que se clasifican dependiendo de la función que realicen, ya sea dejando un rastro del proceso de manipulación del dispositivo, detectándolo, resistiéndose o incluso ofreciendo una respuesta:

    a) ***Tamper Evidence*:** Indicadores de manipulación que proporcionan evidencias visuales de un intento de acceso físico no autorizado al dispositivo. (Ej.: pegatina, encapsulados, etc.)

    b) ***Tamper Detection*:** Mecanismos que permiten detectar los intentos de acceso físico no autorizados al dispositivo. (Ej.: sistema de alarmas)

    c) ***Tamper Response*:** Mecanismos orientados a realizar una acción de respuesta ante una manipulación física no autorizada de un dispositivo de cara a mitigar los riesgos. (Ej: Reseteo de parámetros críticos (*Zeroización*)).

7.2.2 FILTROS DE PRIVACIDAD (FIL)

42. Los filtros de privacidad son paneles que se colocan sobre la pantalla complicando la visión de aquellas personas que no se encuentren directamente frente a esta. Así se evitará que las personas que no están utilizando el equipo puedan visualizar su contenido.

7.2.3 PROTECCIÓN DE ACCESO A BIOS (BIO)

43. La BIOS (*Basic Input Output System*) es un sistema de la placa base de cualquier equipo encargado, entre otras cosas, del arranque, los chequeos de componentes *hardware* del equipo y la carga del sistema operativo.

44. Deben protegerse adecuadamente a través de una contraseña robusta dado que, de lo contrario, un usuario malicioso podría configurar el equipo para arrancar desde un dispositivo removible y obtener acceso privilegiado a los recursos de este.

7.3 DESCRIPCIÓN DE MEDIDAS DE SEGURIDAD DEL SISTEMA OPERATIVO

7.3.1 GESTIÓN DE USUARIOS (USR)

45. Un sistema operativo permite definir múltiples usuarios con diferentes privilegios de acceso en función de rol que posean.

46. Una correcta gestión de usuarios deberá basarse en la segregación de funciones que permita establecer cuentas de administrador (de sistema y/o de seguridad), desde las que llevar a cabo únicamente tareas de administración y de usuarios genéricos desde las que no sea posible administrar el equipo.

7.3.2 CONTROL DE ACCESOS (ACC)

47. El control de acceso de los usuarios a los recursos y datos del sistema se basará en la existencia de diferentes perfiles de usuario, contando al menos con usuario(s) no privilegiado(s) y con administrador(es) privilegiado(s).

48. El control de accesos debe permitir aplicar los siguientes criterios:
    a) Todo acceso debe estar prohibido, salvo concesión expresa.
    b) Cada entidad quedará identificada singularmente.
    c) La utilización de los recursos debe estar protegida.
    d) La identidad de la entidad deberá quedar previamente autenticada.
    e) La información de seguridad será restringida a usuarios administradores.

49. La gestión del control de accesos es aplicable tanto a las MVs como a la infraestructura que las despliega (hipervisor o sistema operativo).

7.3.3 IDENTIFICACIÓN Y AUTENTICACIÓN (I/A)

50. El proceso de identificación y autenticación de los usuarios se basa en el empleo de uno o varios de los siguientes factores, en función del nivel de seguridad requerido:

a) **Algo que se sabe**: Contraseñas o claves concertadas. Dependiendo del nivel de seguridad, se aplicarán ciertas exigencias de complejidad/calidad y renovación.

b) **Algo que se tiene**: Componentes lógicos, tales como certificados *software* o dispositivos físicos (*tokens*). Se requerirá el empleo de elementos criptográficos *hardware* usando algoritmos y parámetros autorizados por el Centro Criptológico Nacional (CCN)

c) **Algo que se es**: elementos biométricos (lector de huella, iris, etc.).

51. Además, para el proceso de identificación y autenticación suele establecerse un número máximo de intentos de autenticación, de cara a evitar ataques de autenticación por fuerza bruta.

7.3.4 GESTIÓN DE ACTUALIZACIONES (ACT)

52. Abarca el proceso de gestión de las actualizaciones publicadas por los fabricantes, principalmente de aquellas relacionadas con la seguridad y la remediación de vulnerabilidades en los sistemas.

53. La distribución de las actualizaciones podrá realizarse *online* y de una manera automatizada en los sistemas que cuenten con conectividad y cuando el contexto operacional y normativo lo permita u *off-line*, en cuyo caso serán instaladas por personal autorizado utilizando dispositivos de almacenamiento externo siguiendo los procedimientos establecidos.

7.3.5 CONTROL DE INTERFACES DE ENTRADA/SALIDA (CI/O)

54. Son mecanismos de control que permiten restringir, habilitar y configurar capilarmente los interfaces de entrada/salida, hacia o desde los sistemas operativos. En el caso de que el dispositivo esté gestionado por un UEM de la organización, este control podría ser realizado de forma centralizada desde el propio UEM.

7.3.6 GESTIÓN DE EVENTOS DE SEGURIDAD (LOG)

55. Son mecanismos que permiten el almacenamiento y retención de *logs* y eventos de seguridad generados por el sistema y/o los usuarios durante un periodo de tiempo determinado, conforme a la política aplicable la organización.

56. Además, pueden implementarse mecanismos de correlación de eventos que los complementen y que facilitan la búsqueda de anomalías o posibles amenazas para la seguridad del sistema.

7.4 DESCRIPCIÓN DE MEDIDAS DE SEGURIDAD DE LA CAPA DE VIRTUALIZACIÓN

7.4.1 GESTIÓN DE INFRAESTRUCTURA VIRTUALIZADA (ADV)

57. La gestión de la infraestructura virtualizada comprende actividades y permisos de creación, configuración, mantenimiento y destrucción de máquinas virtuales.

7.4.2 AISLAMIENTO DE DATOS Y RECURSOS (AIS)

58. Son medidas orientadas a asegurar un completo aislamiento de los datos, tanto en reposo como en uso entre los diferentes sistemas VMs/*host*, incluyendo sus respectivos procesos y recursos tales como memorias o medios de almacenamiento.

59. En particular, están enfocadas a limitar las funcionalidades que permiten la transferencia de datos entre máquinas virtuales o con el *host*.

7.4.3 COPIAS DE SEGURIDAD (BCK)

60. Las copias de seguridad consistirán en imágenes (*snapshots*) y/o copias de archivos que permitan recuperar datos de una antigüedad determinada conforme a la normativa aplicable. Estas copias abarcarán la información de la organización, aplicaciones, sistema operativo, datos de servicios y equipos, claves, etc., y tendrán el mismo nivel de seguridad que los datos originales.

61. Deben emplearse canales seguros, que garanticen la confidencialidad y la integridad de la información y la autenticación extremo a extremo, cuando las copias puedan ser ejecutadas y transferidas remotamente.

7.4.4 CONTROL DE INTERFACES DE COMUNICACIONES (COM)

62. Son mecanismos implementados para restringir las interfaces de comunicaciones desde los sistemas virtualizados.

63. En el caso de la arquitectura tipo 3 *Thin Client*, este debe permitir la conectividad con el servicio de VDI que le proporciona el escritorio y cumplir con los requisitos de protección de comunicaciones requerido.

64. Todas las comunicaciones deben estar protegidas, para lo que se utilizan canales seguros que garantizan la confidencialidad e integridad de la información, así como la autenticación extremo a extremo.

7.4.5 ASIGNACIÓN DE INTERFACES DE ENTRADA/SALIDA (AI/O)

65. Son mecanismos de control que permiten asignar los interfaces de entrada/salida a cada uno de los sistemas virtualizados, así como restringirlos a los estrictamente necesarios.

7.5 DESCRIPCIÓN DE MEDIDAS DE SEGURIDAD DE LA CAPA DE SERVICIO

7.5.1 *ANTI-MALWARE* (A/M)

66. Cuando hablamos de herramientas *Anti-Malware* para *end point* nos referimos, básicamente, a dos (2) tipos de herramientas:

    a) EPP (*End Point Protection Platform*). Las soluciones EPP 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.

    b) EDR (*End Point Detection and Reaction*). El incremento en la complejidad y sofisticación del código dañino ha provocado el desarrollo de una nueva generación de herramientas de protección que complementan a los EPP, que añaden características de seguridad enfocadas a la detección y bloqueo de código dañino desconocido mediante análisis de comportamiento.

67. Este *software* ofrece protección en tiempo real y análisis al arrancar el sistema o al conectar un dispositivo removible. Las firmas utilizadas para la detección se deberán actualizar de forma periódica conforme a las políticas de la organización.

7.5.2 BORRADO SEGURO (BSD)

68. Los mecanismos de borrado seguro permiten al usuario eliminar la información de manera que no sea recuperable.

7.5.3 CIFRADO DE DATOS (CIF)

69. El cifrado de datos permite proteger la confidencialidad e integridad de la información tanto en el almacenamiento como en la transmisión. En particular, estos mecanismos tendrán que ser empleados en los dispositivos removibles que manejen información que requiera protección.

70. Además, el sistema no debe almacenar de manera insegura las claves criptográficas que se encuentren en uso.

7.5.4 PREVENCIÓN DE FUGA DE DATOS (DLP)

71. Una solución DLP (*Data Loss Prevention*) está diseñada para detectar y prevenir brechas en la seguridad de la información sensible, monitorizando, detectando y bloqueando su utilización no autorizada, mientras se encuentra "en uso" (*end points*), "en movimiento" (tráfico de red) o "en reposo" (almacenamiento de datos), por medio de inspecciones profundas de contenido, análisis de la seguridad contextual de una transacción (atributos del originador, objetos de datos, medio, tiempos, destinos, etc...).

7.5.5 CORTAFUEGOS (FW)

72. Un cortafuegos personal constituye una primera barrera de protección frente a posibles ataques al *host* procedentes de la red a la que esté conectado. Este mecanismo de seguridad proporciona un amplio rango de protección incluyendo restricciones en puertos y servicios, control de dispositivos removibles, control de posibles programas maliciosos que se ejecuten en el *host*, y capacidad de reportar *logs*.

7.5.6 HOST IPS (HIPS)

73. Un HIPS es una herramienta que monitoriza la actividad de un *host* para detectar actividades sospechosas y analizar los eventos generados. En otras palabras, el objeto de un HIPS es detectar y detener la ejecución de *malware* mediante la monitorización del comportamiento del sistema.

7.5.7 MONITORIZACIÓN DE LA INTEGRIDAD (INT)

74. Son mecanismos que permiten comprobar, de forma periódica, la integridad del *firmware* empleado en los dispositivos *hardware* del sistema (BIOS, infraestructura de red, etc.) así como de los ficheros más críticos incluyendo los de configuración del sistema. Además, tras una caída, discontinuidad del sistema o comportamiento anómalo, se deberán llevar a cabo verificaciones de integridad.

7.5.8 GESTIÓN DE EVENTOS DE SEGURIDAD (LOG)

75. Son mecanismos que permiten el almacenamiento y retención de *logs* y eventos de seguridad generados por el sistema y/o los usuarios durante un periodo de tiempo determinado, conforme a la política aplicable la organización.

76. Además, pueden implementarse mecanismos de correlación de eventos que los complementen y que facilitan la búsqueda de anomalías o posibles amenazas para la seguridad del sistema.

8. ARQUITECTURA DE END POINT SEGURO PARA MANEJO DE INFORMACIÓN CLASIFICADA

77. Todos los sistemas que manejen información clasificada, con independencia del ámbito al que pertenezcan o de su grado de clasificación, deberán estar acreditados por la Autoridad de Acreditación Nacional de acuerdo con la guía *CCN-STIC-001 Política de Seguridad de las TIC.*

78. Partiendo de los modelos de arquitectura de *end point* descritos en la Sección 6 y de las medidas de seguridad descritas en la Sección 7, se incluye cada uno de los elementos que deben considerarse para implementar una arquitectura segura para el escenario en el que el/los sistemas manejen información clasificada.

79. Es importante destacar que el listado de medidas de seguridad establecido en el presente documento cumple con la guía *CCN-STIC-301 Medidas de Seguridad TIC a implementar en sistemas clasificados* y **parte de un escenario de uso genérico, que podrá ser modificado o refinado por los resultados del preceptivo análisis de riesgos para cada escenario de uso concreto**.

8.1 GESTIÓN DE CONFIGURACIÓN (CNF)

80. Debe permitir, al menos, la configuración de los interfaces de entrada/salida de datos y/o emisiones electromagnéticas, así como la gestión de las medidas de seguridad propias del EP o de los usuarios que lo utilicen.

81. Los Sistemas y elementos del Sistema deberán provisionarse con una configuración conocida y aprobada. Dicha configuración podrá ser modificada por el responsable del Sistema en todo momento. **Medida "Gestión de la configuración" [op.exp.3] CCN-STIC-301.**

8.2 CAPA *HARDWARE* Y PERIFÉRICOS

82. El *end point* contará con una capa *hardware* que dé soporte a los distintos sistemas en un mismo equipo físico y que dispondrá de las medidas de seguridad descritas en la presente sección.

83. Además, todos aquellos sistemas con un grado de clasificación CONFIDENCIAL o superior no deberán compartir tarjetas de red con otros de menor clasificación, salvo en los casos en los que los flujos de información procedentes de los diferentes sistemas se encuentren cifrados **desde la máquina origen,** utilizando productos aprobados para la protección de la información del grado de clasificación requerido.

8.2.1 *ANTI-TAMPERING* (TAM)

84. Deberán utilizarse, al menos, dispositivos indicadores de manipulación (*Tamper Evidence*), u otros mecanismos más avanzados.

8.2.2 PROTECCIÓN DE LA BIOS (BIO)

85. Se protegerá mediante contraseña el acceso a la BIOS. Esta contraseña deberá cumplir con unos requisitos mínimos de fortaleza y vigencia que serán establecidos por la política de seguridad del sistema. Además, deberá configurarse atendiendo al principio de mínima funcionalidad.

86. Siempre que sea posible, deberá configurarse arranque seguro de la UEFI. **Medida "Configuración de seguridad" [op.exp.2] CCN-STIC-301.**

8.2.3 FILTROS DE PRIVACIDAD (FIL)

87. En el caso de que el grado de clasificación del sistema permita la consulta de información fuera de una Zona de Acceso Restringido (ZAR), se recomienda la utilización de **Filtros de Privacidad (FIL)** como mecanismo de refuerzo en la protección de la confidencialidad.

8.3 CAPA DE SISTEMAS OPERATIVOS

88. La arquitectura implementada podrá disponer de diferentes capas de sistemas operativos (SO) sobre instancias físicas y/o virtualizadas dentro del *end point*. En cualquiera de los casos estos sistemas operativos proporcionarán el *software* de base y darán soporte a muchas de las medidas de seguridad implementadas por las otras capas que se ejecutarán sobre ellos, tales como la identificación y autenticación de los usuarios o el control de accesos a los sistemas de ficheros.

89. **En ningún caso se podrán utilizar sistemas operativos que no dispongan de soporte de seguridad del fabricante o que no estén aceptados por la Autoridad de Acreditación. Medida "Mantenimiento" [op.exp.4] de la STIC-301.**

90. Es fundamental que la capa del SO implemente las siguientes medidas de seguridad:

8.3.1 GESTIÓN DE USUARIOS (USR)

91. **Medida "Identificación" [op.acc.1] CCN-STIC-301.** Para un mismo sistema, deberán establecerse diferentes usuarios con diferentes niveles de privilegios, de forma que:

    a) Únicamente se podrá administrar el sistema desde un perfil de administrador.

    b) Las sesiones de administración únicamente se emplearán para administrar el sistema.

    c) Se implementará una configuración que limite y controle la ejecución de *software* de acuerdo con los principios de mínima funcionalidad y mínimo privilegio.

8.3.2 CONTROL DE ACCESOS (ACC)

92. **Medida "Control de acceso" [op.acc] CCN-STIC-301.** El control de acceso de los usuarios a los recursos y datos del sistema se hará en base a la existencia de diferentes perfiles de usuario. Como mínimo, se definirán dos (2) tipos de perfiles: usuario(s) no privilegiado(s) y administrador(es) privilegiado(s).

93. El control de accesos deberá permitir aplicar los siguientes criterios:

    a) Todo acceso debe estar prohibido, salvo concesión expresa.

    b) Los privilegios de cada entidad, usuario o proceso se reducirán al mínimo para cumplir con sus obligaciones (principio de mínimo privilegio).

    c) Cada entidad quedará identificada singularmente.

    d) La utilización de los recursos debe estar protegida.

    e) La identidad de la entidad deberá quedar previamente autenticada.

    f) Exclusivamente el personal con competencia para ello podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos.

    g) La gestión del control de accesos es aplicable tanto a las MVs como a la infraestructura que la controla (hipervisor).

8.3.3 IDENTIFICACIÓN Y AUTENTICACIÓN (I/A)

94. Se requerirá que el usuario haya superado un proceso de identificación positiva antes de realizar cualquier acción sobre el sistema:

    a) Para sistemas sin clasificar, la identificación y autenticación de los usuarios se basará en el empleo de un usuario y contraseña. A la hora de seleccionar contraseñas para las cuentas de administrador autorizadas, deberán seguirse las siguientes directrices y opciones de configuración:

        - Deberán ser fáciles de recordar, de modo que los usuarios no se sientan tentados a escribirlas. En caso de que sea necesario guardar una copia física de la contraseña, se hará en un contenedor seguro.
        - Deberán ser privadas y no compartirse con nadie.
        - Deberán cambiarse periódicamente, con un período establecido en los procedimientos operativos de seguridad del sistema que dependerá del grado de clasificación/sensibilidad de la información que se va a manejar.
        - Se recomienda no permitir la repetición de al menos las 10 últimas contraseñas utilizadas.
        - No deberá utilizarse la misma contraseña para acceder a distintos sistemas.

- No deberá realizarse un nuevo cambio de contraseña en los 4 días posteriores al último cambio.
- Deberán ser de 12 caracteres como mínimo.
- Deberán incluir caracteres alfanuméricos y caracteres especiales como "!", "@", "#", "$", "%", "^", "&", "*", "(" y ")", al menos una letra en mayúscula y otra en minúscula, un número o más, y un signo de puntuación o más.
- Deberán contener un al menos 3 juegos de caracteres o de cambios en el juego de caracteres.
- Son contraseñas poco seguras palabras comúnmente utilizadas o cadenas de caracteres consecutivos (Ej.: "1234"). A continuación, se establecen una serie de contraseñas prohibidas:
  - Palabras de diccionario.
  - Caracteres repetitivos o secuenciales (Ej.: "aaaaaaa" o "1234abcd").
  - Patrones de teclado (Ej.: 'zaq12wsx' or 'qwertyuiop').
  - Nombres propios específicos de contexto, nombres de usuario, nombre del host del sistema, etc.
- Las contraseñas establecidas por defecto deberán ser modificadas la primera vez que se inicie la sesión.

b) Para sistemas clasificados, se llevará a cabo una autenticación de **doble factor** (la utilización de autenticación biométrica deberá ser aprobada por la Autoridad de Acreditación), siguiendo los criterios establecidos en la guía CCN-STIC-301. Esta medida podría relajarse y sustituirse por un único factor siempre que sea el entorno operacional2 el que establezca mecanismos de autenticación fuerte. El uso de pines de acceso, OTP o factores de autenticación biométrica deberá ser aprobado por la Autoridad de Acreditación. **Medida "Mecanismo de autenticación" [op.acc.5] Refuerzo R1 CCN-STIC-301.**

95. Se fijará un tiempo máximo de validez de contraseñas, no superior a 6 meses, que será acordado entre el AOSTIC del sistema, y la Autoridad de Acreditación.

96. Se forzará una renovación de todas las credenciales cuando estas hayan sido comprometidas.

97. El núcleo de seguridad del sistema bloqueará el acceso al *end point* y requerirá un nuevo proceso de identificación y autenticación en los siguientes casos:

a) Después de un determinado período de inactividad o cuando el propio usuario bloquee la sesión. En este caso, se bloqueará la sesión activa y se

[2] Por entorno operacional podría entenderse el mecanismo de control de acceso aportado por una Zona de Acceso Restringido (ZAR).

impedirá cualquier acción sobre el sistema a menos que un usuario la desbloquee.

b) Después de varios intentos fallidos de acceso. En este caso, se impedirá cualquier acción sobre el sistema hasta que un administrador autorizado la desbloquee.

8.3.4 GESTIÓN DE ACTUALIZACIONES (ACT)

98. Los sistemas deberán mantenerse convenientemente actualizados para protegerse frente a las nuevas amenazas o vulnerabilidades conocidas. Para los niveles de clasificación para los cuales no sea viable instalar de forma automática actualizaciones de software o descarga de firmas, será necesario contemplar mecanismos manuales para la actualización local**. Medida "Mantenimiento" [op.exp.4] CCN-STIC-301.**

8.3.5 CONTROL DE INTERFACES DE ENTRADA/SALIDA (CI/O)

99. Deberán controlarse los interfaces de entrada/salida de datos y/o emisiones electromagnéticas, de tal forma que se encuentren habilitados únicamente los necesarios.

100. Se recomienda deshabilitar por defecto el uso de medios externos (CD, DVD o USBs) y habilitarlos únicamente cuando sea necesario, en cuyo caso solamente podrán conectarse medios externos autorizados.

101. La función de habilitar y deshabilitar el uso de medios externos debe ser realizada por un usuario administrador, autorizado por el Responsable de Seguridad del organismo.

102. En caso de extracción de información del sistema, se deberá tener en cuenta el Procedimiento de Entrada y Salida de Información Clasificada, incluido en los Procedimientos Operativos de Seguridad.

8.3.6 GESTIÓN DE EVENTOS DE SEGURIDAD (LOG)

103. **Medida "Registro de la actividad" [op.exp.8] CCN-STIC-301**. El sistema deberá disponer de una referencia de tiempo (*timestamp*) confiable para garantizar las funciones de registro de eventos y auditoría. La modificación de la referencia de tiempo del sistema será una función de administración y, en caso de realizarse su sincronización con otros dispositivos, deberán utilizarse mecanismos de autenticación e integridad.

104. Se utilizarán mecanismos para el registro de *logs* y eventos de seguridad generados por el sistema y/o los usuarios, que permitan almacenar y retener los registros durante el periodo que aplique conforme a la política establecida en la organización.

105. Los *logs* de sistemas operativos e hipervisores deberán contener, al menos:

a) Eventos de autenticación de usuarios y administradores.

b) Eventos de acciones realizadas sobre ficheros y objetos.

c) Eventos de exportación (*upload*) e importación (*download*).

d) Eventos de acciones sobre cuentas de usuarios.

e) Eventos de acciones realizadas por usuarios privilegiados.

f) Todos aquellos eventos adicionales reflejados en las diferentes políticas de seguridad de los sistemas.

8.4 CAPA DE VIRTUALIZACIÓN

106. A la hora de configurar sistemas que manejen información clasificada en un entorno virtualizado, deberán tenerse en cuenta las restricciones establecidas en la guía *CCN-STIC-301,* según la cual, podrán convivir en una misma arquitectura virtualizada:

Caso A. Sistemas que manejen información del mismo nivel, pero de diferentes ámbitos de clasificación de la información (RESERVADO, NATO SECRET, UE SECRET) entre los que existan acuerdos de equiparación.

Caso B. Sistemas que manejen información del mismo ámbito y diferente grado de clasificación de la información (SECRETO, RESERVADO, CONFIDENCIAL).

Caso C. Sistemas que manejen información de diferentes ámbitos y grados de clasificación de la información (SECRETO, NATO SECRET, EU CONFIDENTIAL).

107. En la siguiente tabla se muestra los tipos de arquitecturas permitidas en función de las opciones descritas:

CASOS	ARQUITECTURA TIPO 1	ARQUITECTURA TIPO 2	ARQUITECTURA TIPO 3
CASO A. Sistemas del mismo nivel, pero diferente ámbito de clasificación	Permitido	La utilización de este tipo de arquitectura deberá ser específicamente aprobada por la Autoridad de Acreditación. Será permitida normalmente sobre equipos especializados y en sistemas con un propósito específico. En caso de que uno de los sistemas tenga clasificación nacional, será el que corra directamente sobre el *host*.	Permitido

CASOS	ARQUITECTURA TIPO 1	ARQUITECTURA TIPO 2	ARQUITECTURA TIPO 3
CASO B. Sistemas del mismo ámbito de clasificación y diferente nivel	Permitido	La utilización de este tipo de arquitectura deberá ser específicamente aprobada por la Autoridad de Acreditación. Será permitida normalmente sobre equipos especializados y en sistemas con un propósito específico. Se deberá tener en cuenta que siempre el nivel de mayor clasificación será el que corra directamente sobre el *host*..	Permitido
CASO C. Sistemas de distinto nivel y ámbito de clasificación	Permitido	No permitido	Permitido

108. Los sistemas que manejen información clasificada CONFIDENCIAL o superior no podrán compartir, en ningún caso, arquitectura de virtualización con sistemas que no manejen información clasificada. La inclusión, en una arquitectura de virtualización, de sistemas con grado de clasificación DIFUSIÓN LIMITADA o equivalente deberá ser estudiada, caso por caso, por la Autoridad de Acreditación.

109. Además, deberán implementarse las medidas de seguridad que se detallan a continuación.

8.4.1 GESTIÓN DE INFRAESTRUCTURA VIRTUALIZADA (ADV)

110. La funcionalidad de creación de máquinas virtuales deberá configurarse y controlarse adecuadamente. Esta funcionalidad estará restringida a usuarios privilegiados (administradores). Al finalizar su uso, las máquinas virtuales deberán tratarse del mismo modo que las físicas.

111. Toda la administración relacionada con la arquitectura de virtualización deberá realizarse de manera independiente para cada uno de los sistemas que residan en ella. El personal administrador de virtualización deberá realizar una administración aislada y específica para cada uno de ellos.

112. En el caso de máquinas virtuales que manejen información no clasificada, estas deberán permitir reiniciar su configuración cada vez que se produzca un arranque y mantener intactos los registros de auditoría generados.

8.4.2 AISLAMIENTO DE DATOS Y RECURSOS (AIS)

113. Consistirá en un conjunto de medidas/opciones de configuración implementadas entre los diferentes sistemas VMs/*host*, destinadas a impedir que se produzca una transferencia no controlada de datos entre ambos dominios de seguridad.

114. En este sentido, se exigirá:

a) Compartimentación de las máquinas virtuales, de tal forma que no esté permitida la compartición lógica de recursos incluida la posibilidad de copiar, cortar, pegar y crear carpetas compartidas entre máquinas.

b) Asignación estática de los recursos de memoria y almacenamiento. En caso de que sea necesario reasignar recursos de una máquina a otra de menor grado de clasificación, deberán utilizarse los mecanismos de sanitización descritos en la guía CCN-STIC-305 *Destrucción y Sanitización de soportes informáticos* para el grado de clasificación del sistema que se desee sanitizar.

8.4.3 CONTROL DE INTERFACES DE COMUNICACIONES (COM)

115. Consistirá en un conjunto de medidas/opciones de configuración, destinadas proteger y controlar las comunicaciones de las distintas máquinas virtuales/hosts. Este control será especialmente crítico para los sistemas que manejen información clasificada.

116. La conmutación entre segmentos de red en una máquina virtual deberá ser específicamente autorizada por la Autoridad de Acreditación.

117. La conmutación virtual que permite el hipervisor para establecer comunicaciones entre máquinas deberá estar deshabilitada.

8.4.4 ASIGNACIÓN DE INTERFACES DE ENTRADA/SALIDA (AI/O)

118. Consistirá en un conjunto de medidas/opciones de configuración, destinadas proteger y controlar los interfaces de entrada/salida permitidas para cada uno de los sistemas. Este control será especialmente crítico para sistemas que manejen información clasificada.

8.4.5 COPIAS DE SEGURIDAD (BCK)

119. Con carácter general, se recomienda realizar regularmente copias de seguridad mediante imágenes (*snapshots*) o copias de archivos que permitan recuperar datos de una antigüedad determinada conforme a la normativa aplicable. Estas copias abarcarán la información de la organización, logs del sistema, aplicaciones, sistema operativo, datos de servicios y equipos, claves, etc., y exigirán el mismo nivel de seguridad que los datos originales.

120. Cuando las copias puedan ser ejecutadas y transferidas remotamente, se establecerán canales seguros, para los que se utilizarán herramientas o dispositivos aprobados para la protección de la información clasificada del grado correspondiente.

121. El proceso de restauración de dichas copias debe estar sujeto a un programa de pruebas periódicas que verifiquen su correcto funcionamiento. **Medida "Copias de seguridad (*backup*)" [mp.info.9] CCN-STIC-301.**

122.

8.5 CAPA DE SERVICIOS

123. Dentro de cada uno de los sistemas deberán implementarse las siguientes medidas:

8.5.1 HERRAMIENTA *ANTI-MALWARE* (A/M)

124. **Medida "Protección frente a código dañino" [op.exp.6]. CCN-STIC-301.** El *software* de detección de código dañino deberá configurarse para:

    a) Analizar todo fichero procedente de fuentes externas antes de trabajar con él.

    b) Actualizar sus bases de datos cada 24 horas. Mayores períodos de tiempo serán aprobados previamente por la Autoridad de Acreditación o por el Supervisor de Seguridad TIC (SSTIC).

    c) Revisar el sistema cada vez que arranque.

    d) Implementar protección en tiempo real de acuerdo con las recomendaciones del fabricante.

    e) Realizar escaneos regulares para detectar *software* malicioso.

125. Por regla general, salvo que se justifique debidamente en el proceso de acreditación de los sistemas, deberán utilizarse, independientemente de si el sistema maneja información clasificada o no:

    a) **Herramientas EPP**.

    b) **Herramientas EDR.** Es una práctica recomendable seleccionar un EPP que no sea del mismo fabricante que el EDR.

126. En el caso de sistemas clasificados sin conexión a internet, deberán establecerse los mecanismos adecuados para la actualización periódica de firmas.

8.5.2 CORTAFUEGOS (FW)

127. Deberá utilizarse un cortafuegos personal que permita únicamente los flujos de comunicación autorizados conforme a las políticas de la organización. Un

principio clave cuando se define una política de cortafuegos es seguir una aproximación basada en denegación por defecto, en la que selectivamente se permite solo lo estrictamente necesario. Por el contrario, una aproximación de denegación selectiva se fundamenta en denegar todo aquello que no está permitido, práctica muy poco recomendable por su difícil gestión y porque deja una superficie de ataque mucho mayor.

128. **Por lo tanto, los cortafuegos deberán configurarse siguiendo el principio de denegación por defecto, es decir, se habilitará lo permitido y se bloqueará todo lo demás mediante reglas de rechazo y denegación total.**

8.5.3 SISTEMA DE PREVENCIÓN DE INTRUSIÓN EN HOST (HIPS)

129. Se empleará un sistema para la prevención de intrusiones en el sistema (HIPS) con el fin de detectar y bloquear en tiempo real cualquier intento de intrusión. El conjunto de reglas predefinidas y patrones de firmas utilizados para detectar posibles ataques serán personalizados y actualizados periódicamente conforme a las políticas de la organización.

130. Para algunos sistemas, en función de sus requisitos operacionales, puede no ser recomendable el uso de un HIPS. Un ejemplo sería el de aquellos sistemas en los que exista un riesgo de que falsos positivos causen falta de disponibilidad de un servicio crítico. En estos casos se recomienda la utilización de un HIDS.

131. En el caso de sistemas clasificados sin conexión directa a internet, deberán establecerse los mecanismos adecuados para la actualización periódica de firmas.

8.5.4 MONITORIZACIÓN DE LA INTEGRIDAD (INT)

132. Se emplearán mecanismos para comprobar de forma periódica la integridad del sistema (BIOS, infraestructura de red, etc.) así como de los ficheros más críticos incluyendo los de configuración del sistema. Además, tras una caída, discontinuidad del sistema o comportamiento anómalo, se deberán llevar a cabo verificaciones de la integridad.

8.5.5 GESTIÓN DE EVENTOS DE SEGURIDAD (LOG)

133. Ver Apartado 7.3.6

8.5.6 CIFRADO DE DATOS (CIF)

134. Deberán aplicarse mecanismos criptográficos para la protección de la confidencialidad e integridad de la información de los sistemas que manejen información clasificada (recomendable para sistemas sin clasificar). Concretamente, estos mecanismos serán:

a) **Cifrado *on-line***. Para la protección de información en tránsito. Típicamente implementado mediante la utilización de redes privadas virtuales (VPN) o cifradores *hardware*. En este caso, el canal de información aportará también autenticación extremo a extremo. La utilización de cifrado *on line* será obligatoria siempre que se envíe información clasificada por un canal inseguro.

   Todos los dispositivos/herramientas de cifrado *on-line* deberán estar aprobados para la protección de la información del máximo grado de clasificación que maneje el sistema

b) **Cifrado *off-line***: Para la protección de la información que vaya a ser enviada por/almacenada en un medio inseguro. La utilización de cifrado *off-line* es obligatoria cuando se desee convertir información roja en información negra para, posteriormente, enviarla por correo electrónico fuera de los sistemas clasificados o transportarla en un dispositivo removible. En este caso, todos los dispositivos/herramientas de cifrado *off-line* deberán estar aprobados para la protección de información del grado de clasificación que se desee transportar.

   Podría prescindirse de la utilización de cifrado *off-line* o del uso de productos aprobados para el grado de clasificación requerido. No obstante, en estos casos la información transportada será considerada clasificada y, por tanto, serán de aplicación las **medidas de protección en el transporte de Información Clasificada establecidas en las Normas de la Oficina Nacional de Seguridad**.

c) **Cifrado *at-rest*** o cifrado de la información almacenada. Deberá utilizarse siempre que la solución de *end point* sea móvil o portátil, para garantizar la confidencialidad e integridad de la información clasificada cuando el dispositivo salga de la zona controlada.

   En los casos en los que sea requerido el cifrado *at rest*, todos los dispositivos/herramientas de cifrado deberán estar aprobados para la protección de información del máximo grado de clasificación que maneje el sistema. En caso contrario, la información transportada en el dispositivo será considerada clasificada y, por tanto, serán de aplicación las **medidas de protección en el transporte de Información Clasificada establecidas en las Normas de la Oficina Nacional de Seguridad**.

135. Sin perjuicio de lo anteriormente indicado, cualquier sistema, independientemente de que maneje o no información clasificada, utilizará canales de comunicación cifrados (IPSec, TLS 1.2 o superior, https/TLS) que proporcionen protección de confidencialidad, de integridad y autenticación extremo a extremo para el establecimiento de comunicaciones con entidades autorizadas (servidores de autenticación, auditoría, administración remota, etc…) o cuando se establezcan conexiones a través del navegador Web (https/TLS).

136. Todas las claves criptográficas que se encuentren en uso deberán almacenarse de manera segura, utilizando mecanismos que presenten, al menos, la misma fortaleza que la de las claves.

8.5.7 PREVENCIÓN DE FUGA DE DATOS (DLP)

137. Para los sistemas que manejen información clasificada, deberán utilizarse mecanismos que permitan controlar la información exportada desde el sistema y habilitar únicamente los medios externos autorizados. Aunque el control de dicha información puede realizarse mediante medidas no técnicas, la utilización de dispositivos DLP está recomendada.

8.5.8 BORRADO SEGURO (BSD)

138. Se implementarán mecanismos de borrado seguro que permitan al usuario eliminar la información sensible de manera que no sea recuperable. **Medida "Borrado y destrucción" [mp.si.5] CCN-STIC-301.**

139. Para la sanitización de soportes que manejan información clasificada deberá cumplirse con lo establecido en la guía *CCN-STIC-305 Destrucción y Sanitización de soportes informáticos* para el grado de clasificación del sistema que se desee sanitizar.

8.6 INTERCONEXIÓN DE SISTEMAS

140. Cuando un sistema que maneje información clasificada establezca una interconexión con otro sistema, aunque este se encuentre en la misma arquitectura de virtualización, deberá cumplir lo establecido en la guía *CCN-STIC 302 Interconexión de sistemas de las TIC que manejan información clasificada en la Administración.*

141. En este sentido, la compartimentación de las máquinas virtuales, incluida la posibilidad de copiar, cortar y pegar entre máquinas virtuales, estará estrictamente controlada, dado que el intercambio de información entre ambos sistemas, se considera una interconexión y, por lo tanto, deberá contemplar el uso de los dispositivos de protección de perímetro establecidos en la normativa.

8.7 COMPONENTES APROBADOS

142. El Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC) publicado por el CCN como guía CCN-STIC-105, presenta un listado de **Productos Aprobados** para el manejo de información clasificada hasta un determinado grado de clasificación.

143. Deberán encontrarse **obligatoriamente** dentro de dicho listado, como Productos Aprobados para el grado de clasificación de sistema correspondiente, los siguientes productos:

a) Todos los sistemas operativos.

b) Todos los dispositivos/herramientas de cifrado empleados para la protección de información clasificada. Para este tipo de productos será necesario aplicar aquellas medidas que resulten de aplicación de la guía CCN-STIC 003 *Instrucción de uso de cifradores certificados para protección de información clasificada*. Además, cumplirán con lo establecido en la guía CCN-STIC-970 *Uso de cifradores IP en Redes Públicas*.

c) Todos los dispositivos/herramientas de protección de perímetro para un nivel alto de seguridad (pasarelas, diodos).

144. Los dispositivos/herramientas de seguridad empleados para proteger a los activos del sistema que no se encuentren incluidos en los anteriormente citados, deberán encontrarse, siempre que sea posible, dentro de los Productos Aprobados para el manejo de información clasificada para ese nivel de seguridad.

145. En caso de que no existan productos dentro del listado, se utilizarán productos incluidos en el listado de Productos Cualificados del CPSTIC. Si tampoco existiesen productos en el listado de Cualificados se utilizarán, preferiblemente, productos que cuenten con una certificación de seguridad reconocida por el Organismo de Certificación del ENECSTI (*Common Criteria*, LINCE).

146. Solo en caso de que no existan productos certificados y/o esté debidamente justificado podrán utilizarse productos sin certificación alguna.

147. En cualquier caso, será obligatorio que se encuentren configurados de acuerdo con las guías de configuración segura CCN-STIC en vigor. En su defecto, se aceptará una guía de configuración segura elaborada por el fabricante del producto o una guía elaborada por el organismo propietario del sistema.

8.8 CONTROL DE SESIÓN

148. Antes del establecimiento de una sesión en el sistema deberá aparecer un mensaje advirtiendo de que solo los usuarios autorizados pueden acceder al Sistema y que la actividad será supervisada para asegurar el cumplimiento de la política de seguridad. En dicho mensaje no se facilitará información del Sistema que pueda identificarlo o caracterizarlo ante un atacante.

149. Se informará al usuario del último acceso efectuado con su identidad.

150. En los procedimientos de seguridad del sistema se establecerá un tiempo máximo de inactividad de sesión, a partir del cual, esta se cerrará.

8.9 ADMINISTRACIÓN REMOTA

151. El acceso remoto para la administración del sistema únicamente estará habilitado y activo cuando vaya a ser utilizado. Para ello, se utilizará un protocolo de comunicaciones seguro que aporte protección de confidencialidad, integridad y autenticación extremo a extremo.

152. Deberán recogerse registros de auditoría de este tipo de conexiones. **Medida "Mecanismo de autenticación" [op.acc.5] - Control de Sesión CCN-STIC-301.**

153.

8.10 Utilización De WIFI

154. La Autoridad de Acreditación de Seguridad deberá autorizar la utilización de WIFI en sistemas clasificados.

155. En el caso de que el *end point* establezca conexiones inalámbricas basadas en el estándar WIFI (802.11), deberán seguirse las indicaciones establecidas en la guía *CCN-STIC- 497 Uso de tecnologías inalámbricas WIFI (802.11) en redes clasificadas.*

156. A continuación, se resumen los aspectos más importantes considerados en la citada guía:

    a) Se recomienda utilizar el protocolo WPA3 (estándares 802.1X) como método de protección de acceso a la red inalámbrica. En caso de que el *end point* no implemente esta tecnología podrá utilizarse WPA2. En ambos casos, se recomienda emplear su variante *Enterprise* con autenticación mutua EAP-TLS mediante certificados entre cliente y servidor.

    b) Para asegurar un cifrado extremo a extremo se debe complementar el cifrado inalámbrico con el uso de soluciones de VPN aprobadas por el CCN para el manejo de Información Clasificada del grado correspondiente.

157. Además, se establecen los siguientes requisitos de configuración y operación:

    a) No se permitirá el uso simultáneo de LAN y WLAN en el mismo entorno virtual.

    b) No se deberán establecer comunicaciones *ad-hoc* con otro dispositivo cliente.

    c) Se utilizarán SSID que no revelen la identidad del usuario o información sobre el equipo o la configuración de este.

    d) Cuando el *end point* no vaya a establecer conexiones inalámbricas, se deberá retirar y/o deshabilitar dichas interfaces.

8.11 PROTECCIÓN DE EMISIONES ELECTROMAGNÉTICAS

158. Todos los sistemas clasificados como CONFIDENCIAL o SUPERIOR deberán cumplir con los requisitos de emanaciones exigidos en función del local en que vaya a instalarse, de acuerdo con lo recogido en la SDIP-29.

8.12 POLÍTICA DE CONFIGURACIÓN Y USO

159. Las arquitecturas presentadas requieren de una apropiada configuración, operación y mantenimiento, que permita el manejo de diferentes niveles de información en el *end point* sin poner en riesgo la confidencialidad, integridad y disponibilidad de esta.

160. Deberán tenerse en cuenta los siguientes aspectos:

a) El sistema y cada una de las partes que lo componen, deben diseñarse y configurarse siguiendo el **principio de mínima funcionalidad**, por lo que se restringirán los servicios habilitados, en base a las necesidades operativas. Esta restricción y/o habilitación debe poder gestionarse dinámicamente y debe poder conocerse en todo momento la situación/configuración de los elementos (EP) del sistema.

b) Debe aplicarse el **principio de mínimo privilegio**, de modo que los usuarios inicien sesión con cuentas de usuario limitadas. Las modificaciones a la configuración, del host o de los entornos virtualizados, estarán restringidas a personal administrador con credenciales solo para tareas administrativas.

c) Se recurrirá a **los procedimientos de empleo seguro** del CCN o, en su defecto, a las guías publicadas por el fabricante o elaboradas por el organismo, para los entornos virtualizados implantados y todas aquellas herramientas de seguridad instaladas en *el end point*.

d) En la siguiente tabla se muestra un resumen de los principios generales establecidos que deberán tenerse en cuenta en las políticas de configuración y uso, algunos de ellos ya comentados en apartados anteriores:

ASPECTO	SISTEMA SIN CLASIFICAR	SISTEMA CLASIFICADO
Reinicio de configuración cada vez que se produzca un arranque	Recomendable	No aplicable
Configuración de "mínima funcionalidad"	Recomendable	Obligatorio
Gestión de Infraestructura de virtualización	Administrador (solo se permite al usuario la ejecución de MVs)	Administrador (solo se permite al usuario la ejecución de MVs)

ASPECTO	SISTEMA SIN CLASIFICAR	SISTEMA CLASIFICADO
Autenticación de doble factor	Recomendable	Obligatorio (podrá considerarse el control de acceso del local)
Complejidad de contraseñas[3]	Obligatorio	Obligatorio
Auto bloqueo de sesión tras cierto tiempo de inactividad	Obligatorio	Obligatorio
Bloqueo de usuario tras ciertos intentos fallidos de autenticación	Obligatorio	Obligatorio
Almacenamiento cifrado de datos	Recomendable si *end point* fuera de perímetro controlado	Obligatorio si e*nd Point* fuera de perímetro controlado
Almacenamiento cifrado de claves	Obligatorio	Obligatorio
Uso de canales cifrados para envío de información	Recomendable	Obligatorio
Uso de canales cifrados para comunicación con entidades autorizadas	Obligatorio	Obligatorio
Autenticación extremo a extremo con certificados digitales	Recomendable	Obligatorio
Instalación de actualizaciones del Sistema Operativo	Obligatorio	Obligatorio
Instalación/ actualización de software	Por Administrador	Por Administrador, siguiendo el Procedimiento de Seguridad aprobado
Centralización de monitorización de logs y alertas de seguridad	Recomendable	Recomendable
Control de la configuración	Obligatorio	Obligatorio
Copias de seguridad	Recomendable	Recomendable

[3] Véase Anexo C

ASPECTO	SISTEMA SIN CLASIFICAR	SISTEMA CLASIFICADO
Uso de interfaz USB como dispositivo de almacenamiento	Permitido	Solo dispositivos controlados y autorizados
Mecanismos de borrado seguro	Recomendable	Obligatorio
Retención de registros de auditoría	Recomendable. Conforme a política de la organización	Obligatorio

Tabla 2. Política de configuración del *End Point*

161. Como se ha indicado anteriormente, el listado de medidas de seguridad recomendadas y obligatorias incluido en la Tabla 2 podrán ser **modificado o refinado en base a los resultados del preceptivo análisis de riesgos para cada escenario de uso concreto.**

162. En cualquier caso, el sistema host sobre el *end point* deberá cumplir con la política de configuración establecida para el sistema de más alto grado de clasificación que contenga.

163. Los procesos de supervisión de la gestión/monitorización de la seguridad en los diferentes sistemas deberán ser ejecutados por procedimiento y de manera periódica por parte de los administradores.

164. La gestión y monitorización de la seguridad en los *end point,* cuando se realice de manera remota, se hará por canales de comunicación seguros.

9. ARQUITECTURA DE *END POINT* SEGURO PARA MANEJO DE INFORMACIÓN ENS

165. Partiendo de los modelos de arquitectura de *end point* descritos en la Sección 6 y de las medidas de seguridad descritas en la Sección 7, se detallan cada uno de los elementos que debe implementar una arquitectura segura para el caso concreto en el que los sistemas estén bajo el alcance del Esquema Nacional de Seguridad (ENS).

166. Es importante destacar que el listado de medidas de seguridad establecido en el presente documento parte de un escenario de uso genérico y podrán ser **modificado o refinado por los resultados del preceptivo análisis de riesgos para cada escenario de uso concreto.**

9.1 GESTIÓN DE CONFIGURACIÓN (CNF)

167. Los sistemas y elementos del sistema deberán provisionarse con una configuración conocida y aprobada. Dicha configuración podrá ser modificada por el responsable del sistema en todo momento.

168. El responsable del sistema debe poder realizar una recuperación y monitorización de las configuraciones de los elementos del sistema en todo momento mediante las herramientas de gestión de la configuración incluidas en el mismo.

9.2 CAPA *HARDWARE* Y PERIFÉRICOS

169. El *end point* contará con una capa *hardware* que dé soporte a ambos sistemas en un mismo equipo físico y que dispondrá de las siguientes medidas de seguridad:

9.2.1 TAMPER EVIDENCE (TAM)

170. Se recomienda utilizar equipos que dispongan de, al menos, dispositivos indicadores de manipulación (*Tamper Evidence*), especialmente en el caso de dispositivos móviles o portátiles que son utilizados en entornos no controlados.

9.2.2 PROTECCIÓN DE LA BIOS (BIO)

171. Se protegerá mediante contraseña el acceso a la BIOS. Esta contraseña deberá cumplir con unos requisitos mínimos de fortaleza y vigencia que serán establecidos por la política de seguridad del sistema. Además, deberá configurarse atendiendo al principio de mínima funcionalidad.

172. Siempre que sea posible, deberá configurarse arranque seguro de la UEFI.

9.2.3 FILTROS DE PRIVACIDAD (FIL)

173. Se recomienda dotar al *end point* de filtros de privacidad para ayudar a proteger los datos confidenciales, sensibles y personales.

9.3 CAPA DE SISTEMAS OPERATIVOS

174. La arquitectura implementada podrá disponer de diferentes capas de sistemas operativos (SO) sobre instancias físicas y/o virtualizadas dentro del *end point*. En cualquiera de los casos, estos sistemas operativos proporcionarán el *software* de base y darán soporte a muchos de las medidas de seguridad implementadas por las otras capas que se ejecutarán sobre ellos, tales como la identificación y autenticación de los usuarios o el control de accesos a los sistemas de ficheros.

175. **En ningún caso se podrán utilizar sistemas operativos que no dispongan de soporte de seguridad del fabricante.**

176. Es fundamental que la capa del SO implemente las siguientes medidas de seguridad:

9.3.1 GESTIÓN DE USUARIOS (USR)

177. Para un mismo sistema, deberán establecerse diferentes usuarios con diferentes niveles de privilegios, de tal forma que:

    a) Únicamente se podrá administrar el sistema desde un perfil de administrador.

    b) Las sesiones de administración únicamente se emplearán para administrar el sistema.

    c) Se implementará una configuración que restrinja y controle la ejecución de software de acuerdo con mínima funcionalidad y mínimo privilegio.

9.3.2 CONTROL DE ACCESOS (ACC)

178. El control de acceso de los usuarios a los recursos y datos del sistema se hará en base a la existencia de diferentes perfiles de usuario. Como mínimo, se definirán dos (2) tipos de perfiles: usuario(s) no privilegiado(s) y administrador(es) privilegiado(s).

179. El control de accesos deberá permitir aplicar los siguientes criterios:

    a) Todo acceso debe estar prohibido, salvo concesión expresa.

    b) Los privilegios de cada entidad, usuario o proceso se reducirán al mínimo para cumplir con sus obligaciones (principio de mínimo privilegio).

    c) Cada entidad quedará identificada singularmente.

    d) La utilización de los recursos debe estar protegida.

e) La identidad de la entidad deberá quedar previamente autenticada.

f) Exclusivamente el personal con competencia para ello podrá conceder, alterar o anular la autorización de acceso a los recursos, conforme a los criterios establecidos.

g) La información de seguridad será restringida a usuarios administradores.

h) La gestión del control de accesos es aplicable tanto a las MVs como a la infraestructura que la controla (hipervisor).

9.3.3 IDENTIFICACIÓN Y AUTENTICACIÓN (I/A)

180. Se requerirá que el usuario haya superado un proceso de identificación positiva antes de realizar cualquier acción sobre el sistema:

a) Para sistemas de categoría BÁSICA, la identificación y autenticación de los usuarios se basará, como mínimo, en el empleo de un usuario y contraseña. A la hora de seleccionar contraseñas para las cuentas de administrador autorizadas, deberán seguirse las siguientes directrices y opciones de configuración:

- Deberán ser fáciles de recordar, de modo que los usuarios no se sientan tentados a escribirlas. En caso de que sea necesario guardar una copia física de la contraseña, se hará en un contenedor seguro.
- Deberán ser privadas y no compartirse con nadie.
- Deberán cambiarse periódicamente, con un período establecido en los procedimientos operativos de seguridad del sistema que dependerá del grado de clasificación/sensibilidad de la información que se va a manejar.
- Se recomienda no permitir la repetición de al menos las 10 últimas contraseñas utilizadas.
- No deberá utilizarse la misma contraseña para acceder a distintos sistemas.
- No deberá realizarse un nuevo cambio de contraseña en los 4 días posteriores al último cambio.
- Deberán ser de 12 caracteres como mínimo.
- Deberán incluir caracteres alfanuméricos y caracteres especiales como “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“y “)”, al menos una letra en mayúscula y otra en minúscula, un número o más, y un signo de puntuación o más.
- Deberán contener un al menos 3 juegos de caracteres o de cambios en el juego de caracteres.

- Son contraseñas poco seguras palabras comúnmente utilizadas o cadenas de caracteres consecutivos (Ej.: "1234"). A continuación, se establecen una serie de contraseñas prohibidas:
  - Palabras de diccionario.
  - Caracteres repetitivos o secuenciales (Ej.: "aaaaaaa" o "1234abcd").
  - Patrones de teclado (Ej.: 'zaq12wsx' or 'qwertyuiop').
  - Nombres propios específicos de contexto, nombres de usuario, nombre del host del sistema, etc.
- Las contraseñas establecidas por defecto deberán ser modificadas la primera vez que se inicie la sesión.

b) Para categoría MEDIA se utilizará doble factor cuando el equipo se encuentre fuera de una zona de acceso controlado.

c) Para categoría ALTA se utilizará doble factor. Esta medida podría relajarse y sustituirse por un único factor siempre que sea el entorno operacional el que establezca mecanismos de autenticación fuerte.

181. Se fijará un tiempo máximo de validez de contraseñas, nunca superior a 6 meses, que será establecido por la Política de Seguridad del organismo, y se forzará a una renovación de contraseñas cuando estas hayan sido comprometidas.

182. Además, el núcleo de seguridad del Sistema bloqueará el acceso al *end point* y requerirá un nuevo proceso de identificación y autenticación positivo en los siguientes casos:

a) Para categoría MEDIA y ALTA, después de un determinado **período de inactividad**, se bloqueará la sesión activa y se impedirá cualquier acción sobre el sistema a menos que un usuario la desbloquee.

b) Después de varios **intentos fallidos**. En este caso se impedirá cualquier acción sobre el sistema hasta que un administrador autorizado la desbloquee.

9.3.4 GESTIÓN DE ACTUALIZACIONES (ACT)

183. Los sistemas deberán mantenerse convenientemente actualizados para protegerse frente a las nuevas amenazas o vulnerabilidades conocidas.

9.3.5 CONTROL DE INTERFACES DE ENTRADA/SALIDA (CI/O)

184. Deberán controlarse los interfaces de entrada/salida de datos y/o emisiones electromagnéticas, de tal forma que se encuentren habilitados únicamente los necesarios, atendiendo a los principios de mínimo privilegio y mínima funcionalidad.

9.3.6 GESTIÓN DE EVENTOS DE SEGURIDAD (LOG)

185. Se utilizarán mecanismos para el registro de *logs* y eventos de seguridad generados por el sistema y/o los usuarios, que permitan almacenar y retener los registros durante el periodo que establezca la Política de Seguridad establecida en el organismo.

186. Para sistemas categoría MEDIA y ALTA, estos registros deben retenerse durante, al menos, **dos (2) años** y solamente podrán ser eliminados por personal autorizado.

187. Para sistemas categoría MEDIA y ALTA, el *end point* deberá poder utilizar una referencia de tiempo para facilitar las funciones de registro de eventos y auditoría. En caso de sincronizarse con otros dispositivos externos, se utilizarán mecanismos de autenticación e integridad. La modificación de la referencia de tiempo será una función del administrador.

188. Para sistemas de categoría ALTA, estos registros deben ser enviados por los *end point* recogidos por un elemento central del sistema que permita su tratamiento. La frecuencia de envío/recogida de registros debe ser configurada por el responsable del sistema.

189. Los *logs* de sistemas operativos e hipervisores deberán contener, al menos:

    a) Eventos de autenticación de usuarios y administradores, con éxito o fallidos.

    b) Eventos relativos a las actividades de administración. En concreto, el acceso y modificación de ficheros o registros de configuración.

    c) Eventos de exportación (*upload*) e importación (*download*).

9.4 CAPA DE VIRTUALIZACIÓN

190. Deberán implementarse las medidas de seguridad que se detallan a continuación.

9.4.1 GESTIÓN DE INFRAESTRUCTURA VIRTUALIZADA (ADV)

191. La funcionalidad de creación de máquinas virtuales deberá configurarse y controlarse adecuadamente. Esta funcionalidad estará restringida a usuarios privilegiados (administradores). Al finalizar su uso, las máquinas virtuales deberán tratarse del mismo modo que las físicas.

9.4.2 AISLAMIENTO DE DATOS Y RECURSOS (AIS)

192. Consistirá en un conjunto de medidas/opciones de configuración implementadas entre los diferentes sistemas VMs/host, destinadas a impedir que se produzca una transferencia no controlada de datos entre ambos sistemas. Por ejemplo, la

compartimentación de las máquinas incluida la posibilidad de copiar, cortar y pegar entre máquinas virtuales estará estrictamente controlada.

9.4.3 CONTROL DE INTERFACES DE COMUNICACIONES (COM)

193. Consistirá en un conjunto de medidas/opciones de configuración, destinadas proteger y controlar las comunicaciones de las distintas máquinas virtuales/*hosts*. Este control será especialmente crítico para los sistemas que manejen información del ENS Categoría ALTA.

9.4.4 ASIGNACIÓN DE INTERFACES DE ENTRADA/SALIDA (AI/O)

194. Consistirá en un conjunto de medidas/opciones de configuración, destinadas controlar los interfaces de entrada salida permitidos para cada uno de los sistemas. Este control será especialmente crítico para los sistemas que manejen información del ENS Categoría ALTA.

9.4.5 COPIAS DE SEGURIDAD (BCK)

195. Con carácter general, se recomienda realizar regularmente copias de seguridad mediante imágenes (*snapshots*) o copias de archivos que permitan recuperar datos de una antigüedad determinada conforme a la normativa aplicable. Estas copias abarcarán la información del organismo, *logs* del sistema, aplicaciones, sistema operativo, datos de servicios y equipos, claves, etc., y exigirán el mismo nivel de seguridad que los datos originales.

196. Cuando las copias puedan ser ejecutadas y transferidas remotamente, se establecerán canales seguros, para lo que se utilizarán herramientas o dispositivos cualificados para los sistemas de la Categoría correspondiente del ENS.

197. El proceso de restauración de dichas copias debe estar sujeto a un programa de pruebas periódicas que verifiquen su correcto funcionamiento.

9.5 CAPA DE SERVICIOS

198. Dentro de cada uno de los sistemas deberán implementarse las siguientes medidas:

9.5.1 HERRAMIENTA ANTI-MALWARE (A/M)

199. El software de detección de código dañino deberá configurarse para:

    a) Analizar todo fichero procedente de fuentes externas antes de trabajar con él.

    b) Actualizar sus bases de datos periódicamente.

    c) Revisar el sistema cada vez que arranque.

d) Implementar protección en tiempo real de acuerdo con las recomendaciones del fabricante.

e) Realizar escaneos regulares para detectar *software* malicioso.

200. Por regla general, salvo causa justificada, deberán utilizarse:

a) **Herramientas EPP:** en cualquier tipo de sistema, en cualquiera de las categorías del ENS.

b) **Herramientas EDR**: Se recomienda para los sistemas que manejen información de categoría MEDIA y ALTA. Para categoría ALTA se recomienda que el EPP no sea del mismo fabricante que el EDR.

201. En el caso de sistemas sin conexión directa a internet, deberán establecerse los mecanismos adecuados para la actualización periódica de firmas.

9.5.2 CORTAFUEGOS (FW)

202. Deberá utilizarse un cortafuegos personal que permita únicamente los flujos de comunicación autorizados conforme a las políticas del organismo. Un principio clave cuando se define una política de cortafuegos es seguir una aproximación basada en denegación por defecto, en la que selectivamente se permite solo lo estrictamente necesario. Por el contrario, una aproximación de denegación selectiva se fundamenta en denegar todo aquello que no está permitido, práctica muy poco recomendable por su difícil gestión y porque deja una superficie de ataque mucho mayor.

203. Por lo tanto, los cortafuegos deberán configurarse siguiendo el principio de denegación por defecto, es decir, se habilitará lo permitido y se bloqueará todo lo demás mediante reglas de rechazo y denegación total.

9.5.3 SISTEMA DE PREVENCIÓN DE INTRUSIÓN EN HOST (HIPS)

204. Para categoría MEDIA y ALTA, se empleará un sistema para la prevención de intrusiones en el sistema (HIPS) con el fin de detectar y bloquear en tiempo real cualquier intento de intrusión en éste. El conjunto de reglas predefinidas y patrones de firma utilizados para detectar posibles ataques deberán ser personalizados y actualizados periódicamente conforme a la Política de Seguridad del organismo.

205. En el caso de sistemas sin conexión directa a internet, deberán establecerse los mecanismos adecuados para la actualización periódica de firmas.

9.5.4 MONITORIZACIÓN DE LA INTEGRIDAD (INT)

206. Se emplearán mecanismos para comprobar de forma periódica la integridad del *firmware* empleado en los dispositivos *hardware* del sistema (BIOS, infraestructura de red, etc.), así como de los ficheros más críticos, incluyendo los

de configuración. Además, tras una caída, discontinuidad del sistema o comportamiento anómalo, deberá llevar a cabo verificaciones de la integridad.

9.5.5 GESTIÓN DE EVENTOS DE SEGURIDAD (LOG)

207. Ver Apartado 8.3.6.

9.5.6 CIFRADO DE DATOS (CIF)

208. Se deberán aplicar mecanismos criptográficos para la protección de la confidencialidad e integridad de la información de los sistemas que manejen información en el ENS. Concretamente, estos mecanismos serán:

    a) **Cifrado *on line***. Para la protección de información en tránsito. Típicamente mediante la utilización de redes privadas virtuales (VPN) que hagan uso de protocolos seguros que proporcionen cifrado, autenticación y protección de la integridad, como TLS o IPsec. El cifrado *on line* será obligatorio siempre que la información se envíe por un canal inseguro. Para todas las categorías del ENS, el canal de información aportará autenticación extremo a extremo y control de integridad, y en el caso de categoría MEDIA y ALTA deberá aportar también confidencialidad. Las características y requisitos de las redes privadas virtuales se tratan en detalle en la guía CCN-STIC 836 *Seguridad en VPN en el marco del ENS*.

    b) **Cifrado *off line***: Para la protección de la información que vaya a ser enviada por/almacenada en un medio inseguro. Se utilizará para proteger información de categoría MEDIA y ALTA cuando esta vaya a ser guardada en un dispositivo removible o enviada por correo electrónico.

    c) **Cifrado *at rest*** o cifrado de la información almacenada. Deberá utilizarse siempre que la solución de *end point* sea móvil o portátil para sistemas ENS categoría ALTA.

209. Todos los dispositivos/herramientas de cifrado deberán presentar la fortaleza de mecanismos criptográficos exigida, para la categoría correspondiente de sistema, según se define en la *CCN-STIC-807 Criptología de Empleo en el ENS.*

210. Sin perjuicio de lo anteriormente indicado, cualquier sistema, independientemente de su categoría, utilizará canales de comunicación cifrados (IPSec, TLS 1.2 o superior, https/TLS) para el establecimiento de comunicaciones con entidades autorizadas (servidores de autenticación, auditoría, administración remota, etc) o cuando se establezcan conexiones a través del navegador web (https/TLS).

211. Todas las claves criptográficas que se encuentren en uso deberán almacenarse de manera segura, utilizando mecanismos que presenten, al menos, la misma fortaleza que la de las claves.

9.5.7 PREVENCIÓN DE FUGA DE DATOS (DLP)

212. Para sistemas que manejen información del ENS categoría ALTA, se aplicarán mecanismos que permitan controlar la salida de información desde el sistema de mayor categoría de seguridad. Se deberán utilizar únicamente los medios externos autorizados.

9.5.8 BORRADO SEGURO

213. Todos aquellos archivos que contengan información sensible deberán ser borrados de manera segura cuando finalice su uso utilizando una herramienta cualificada de borrado seguro para el tipo de soporte en donde se encuentre almacenada.

214. El mecanismo de borrado seguro utilizado podrá consistir en una o varias pasadas de sobre escritura o el cifrado de la información.

215. No se considera mecanismo de borrado seguro el formateo de unidades de disco o el borrado estándar ofrecido por los diferentes sistemas operativos.

9.6 UTILIZACIÓN DE WIFI EN SISTEMAS DEL ENS

216. En el caso de que el *end point* establezca conexiones inalámbricas basadas en el estándar WIFI (802.11), deberán seguirse las indicaciones establecidas en la guía *CCN-STIC-816 Seguridad en Redes Inalámbricas en el ENS.*

217. A continuación, se resumen los aspectos más importantes considerados en la citada guía:

    a) Se recomienda utilizar el protocolo *WPA3* como método de protección de acceso a la red inalámbrica. En caso de que el *end point* no implemente esta tecnología, podrá utilizarse *WPA2*.

    Para sistemas de categoría MEDIA y ALTA: se recomienda emplear su variante *Enterprise* con autenticación mutua (802.1X) *EAP-TLS* con doble factor de autenticación. En el caso de contraseñas o claves compartidas, deberá presentar el grado de fortaleza requerido para la categoría del sistema (112 bits para categoría MEDIA y 128 bits para categoría ALTA). Además, para categoría ALTA, en el caso de uso de "algo que se tiene" deberán usarse elementos criptográficos *hardware* que utilicen algoritmos autorizados por el CCN.

    Para sistemas de categoría BÁSICA: además de los permitido para las categorías superiores, se podrá trabajar en modo Personal con utilización de claves precompartidas (PSK) para la autenticación. Estas claves deberán tener la fortaleza exigida para sistemas de categoría BÁSICA (112 bits).

b) Para asegurar un cifrado extremo a extremo se debe complementar el cifrado inalámbrico con el uso de soluciones de VPN cualificadas por el CCN para la categoría de sistema que corresponda.

218. Además, se establecen los siguientes requisitos de configuración y operación:

a) No se permitirá el uso simultáneo de LAN y WLAN en el mismo entorno virtual.

b) No se deberán establecer comunicaciones *ad-hoc* con otro dispositivo cliente.

c) Se utilizarán SSID que no revelen la identidad del usuario o información sobre el equipo o la configuración de este.

d) Cuando el *end point* no vaya a establecer conexiones inalámbricas, se deberá retirar y/o inhabilitar dichas interfaces.

9.7 INTERCONEXIÓN

219. Cuando un sistema bajo el alcance del ENS establezca una interconexión con otro sistema, aunque este se encuentre en la misma arquitectura de virtualización, deberá cumplir lo establecido en la guía *CCN-STIC 811 Interconexión en el ENS.*

220. En este sentido, la compartimentación de las máquinas virtuales, incluida la posibilidad de copiar, cortar y pegar entre máquinas virtuales, estará estrictamente controlada, dado que el intercambio de información entre ambos sistemas, teniendo en cuenta que exigen distintos niveles de seguridad, se considera una interconexión y, por lo tanto, deberá contemplar el uso de los dispositivos de protección de perímetro establecidos en la normativa.

9.8 COMPONENTES CUALIFICADOS

221. Todos los dispositivos/herramientas de seguridad empleados para proteger a los activos del sistema deberán encontrarse, siempre que sea posible, dentro de los productos cualificados para la categoría del ENS requerida.

222. En el caso de que no existan productos cualificados en la familia de productos que se trate, deberá exigirse que posean una certificación de seguridad bajo alguna de las metodologías reconocidas por el Organismo de Certificación (OC) del ENECSTI (Common Criteria / LINCE).

223. Solo en caso de que no existan productos certificados y/o esté debidamente justificado podrán utilizarse productos sin certificación alguna.

224. En cualquier caso, será obligatorio que se encuentren configurados de acuerdo con las guías de configuración segura CCN-STIC en vigor o, en su defecto, a las aportadas por el fabricante.

225. Todos los mecanismos y algoritmos criptográficos utilizados deberán estar entre los autorizados por el CCN en la guía *CCN-STIC-807 Criptología de empleo en el ENS.*

9.9 POLÍTICA DE CONFIGURACIÓN Y USO

226. La arquitectura presentada requiere de una apropiada configuración y mantenimiento en el tiempo, así como un conveniente uso, que permita que el manejo de diferentes categorías de información en el *end point* no ponga en riesgo su protección, especialmente de aquella considerada más sensible.

227. Deberán tenerse en cuenta los siguientes aspectos:

- Debe configurarse la **mínima funcionalidad** necesaria en el dispositivo restringiendo al mínimo los servicios habilitados en base a las necesidades operativas.
- Debe aplicarse el principio de **mínimo privilegio**, de modo que los usuarios inicien sesión con cuentas de usuario limitadas. Las modificaciones a la configuración, ya sea a nivel de *host* como de entornos virtualizados, estarán restringidas a personal administrador con credenciales solo para tareas administrativas.
- Se recurrirá, cuando existan, a guías de configuración segura del CCN también para los entornos virtualizados implantados o, en su defecto, a las publicadas por el fabricante.
- Se tendrán en consideración, en cada uno de los sistemas, al menos los principios generales establecidos para los siguientes aspectos de seguridad:

ASPECTO	SISTEMA ENS BÁSICO	SISTEMA ENS MEDIO Y ALTO
Configuración de "mínima funcionalidad"	Obligatorio	Obligatorio
Gestión de Capa/Infraestructura de virtualización	Administrador (solo se permite al usuario la ejecución de MVs)	Administrador (solo se permite al usuario la ejecución de MVs)
Autenticación de doble factor	No requerido	Obligatorio para categoría MEDIA cuando está fuera de una zona controlada y para categoría ALTA (podría considerarse el control de acceso del local)

ASPECTO	SISTEMA ENS BÁSICO	SISTEMA ENS MEDIO Y ALTO
Complejidad de contraseñas	Obligatorio	Obligatorio
Auto bloqueo de sesión tras cierto tiempo de inactividad	Recomendable	Obligatorio
Bloqueo de usuario tras ciertos intentos fallidos de autenticación	Obligatorio	Obligatorio
Cifrado de soportes de información	No requerido	Obligatorio (para soportes removibles)
Cifrado de disco	No requerido	Obligatorio para ENS categoría ALTA en dispositivos portátiles
Almacenamiento cifrado de claves	Obligatorio	Obligatorio
Uso de VPN para comunicación con el organismo (y gestión remota)	Obligatorio (para la protección de la autenticidad, integridad y confidencialidad)	Obligatorio (para la protección de la autenticidad, integridad y confidencialidad)
Instalación de actualizaciones del Sistema Operativo	Obligatorio	Obligatorio
Instalación/ actualización de *software*	Obligatorio (realizado por administrador)	Obligatorio (realizado por administrador)
Centralización y monitorización de logs y alertas de seguridad	Obligatorio	Obligatorio
Control de la configuración	Obligatorio	Obligatorio

ASPECTO	SISTEMA ENS BÁSICO	SISTEMA ENS MEDIO Y ALTO
Copias de seguridad	Obligatorio	Obligatorio
Mecanismos de borrado en caso de reutilización del dispositivo por otro usuario	Obligatorio	Obligatorio
Retención de registros de auditoría	De acuerdo a la política de la organización	Obligatorio (2 años)

Tabla 3. Política de configuración del *End Point*

228. En cualquier caso, el sistema host sobre el *end point* deberá cumplir con la política de configuración establecida para el sistema de mayor categoría del ENS.

229. Los procesos de supervisión de la gestión/monitorización de la seguridad deberán ser ejecutados de manera periódica y descritos en los Procedimientos de Seguridad del organismo.

10.DEFINICIONES

End point	Plataforma o dispositivo, fijo o móvil, que un usuario de una red de comunicaciones utiliza como puesto de trabajo.
Hipervisor tipo 1 o nativo	También denominado *unhosted* o *bare metal* (sobre metal desnudo) es software que se ejecuta directamente sobre el hardware para ofrecer la funcionalidad propia del hipervisor.
Hipervisor tipo 2 o *hosted*	Es un software que se ejecuta sobre un sistema operativo para ofrecer la funcionalidad de hipervisor.
Información Roja	Información clasificada y que, por lo tanto, requiere protección de acuerdo a la Normativa Protección de Información Clasificada generada por la Oficina Nacional de Seguridad.
Información Negra	Información no clasificada o información clasificada que ha sido cifrada con mecanismos de cifra aprobados por la autoridad competente y que, por lo tanto, puede protegerse con los mismos medios que la información no clasificada.
Información sensible	Información que demanda un alto nivel de seguridad en alguna de sus dimensiones.
Información clasificada	Asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas puedan dañar o poner en riesgo la seguridad y defensa del Estado.
Ámbito de seguridad	Ámbito de origen al que pertenece la información, es decir, la organización o nación propietaria de la información clasificada a la que puede tener acceso, si es necesario. Por ejemplo: OTAN, UE o NACIONAL.
Nivel de seguridad	Máxima clasificación de la información clasificada dentro de un mismo ámbito de seguridad.
Dominio de seguridad	Ámbito de seguridad o nivel de seguridad dentro de un mismo ámbito.
Sistema Multidominio	Escenario en el que se maneja información de diferentes dominios de seguridad.
sistema	Se denomina sistema al conjunto de equipamiento *hardware*, sistema operativo y aplicaciones software que manejen un tipo de información en un ámbito determinado.
Sistema	Se denomina Sistema a cada uno de los entornos que manejan un tipo de información correspondiente a un ámbito y un nivel de seguridad, y que se ejecutan simultáneamente y de forma aislada en el *endpoint.*

11.REFERENCIAS

STIC.1 CCN-STIC-001 Política de Seguridad de las TIC

STIC.2 CCN-STIC 003 Instrucción de uso de cifradores certificados para protección de información clasificada

STIC.3 CCN-STIC-105 Catálogo de Productos de Seguridad TIC (CPSTIC)

STIC.4 CCN-STIC-301 Medidas de Seguridad TIC a implementar en sistemas clasificados

STIC.5 CCN-STIC 302 Interconexión de sistemas de las TIC que manejan información clasificada en la Administración

STIC.6 CCN-STIC-305 Destrucción y Sanitización de soportes informáticos

STIC.7 CCN-STIC- 497 Uso de tecnologías inalámbricas WIFI (802.11) en redes clasificadas

STIC.8 CCN-STIC-807 Criptología de Empleo en el ENS

STIC.9 CCN-STIC-811 Interconexión en el ENS

STIC.10 CCN-STIC-816 Seguridad en redes inalámbricas en el ENS

STIC.11 STIC-836 Seguridad en VPN en el marco del ENS

STIC.12 STIC-970 Uso de cifradores IP En Redes Públicas

12.ABREVIATURAS

AOSTIC	Autoridad Operativa del Sistema de las Tecnologías de la Información y las Comunicaciones (AOSTIC)
BIOS	*Basic Input Output System*
CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación
DLP	*Data Loss Prevention*
EDR	*End Point Detection and Reaction*
ENECSTI	Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información
ENS	Esquema Nacional de Seguridad
EPP	*End Point Protection Platform*
HIPS	*Host Intrusion Prevention System*
HTTPS	*Hypertext Transfer Protocol Secure*
MV	Máquina Virtual
ONS	Oficina Nacional de Seguridad
OSI	*Open System Interconnection*
OTP	*One Time Password*
SO	Sistema Operativo
STIC	Seguridad de las Tecnologías de la Información y la Comunicación
TLS	*Transport Layer Security*
VM	*Virtual Machine*
VPN	*Virtual Private Network*
UEFI	*Unified Extensible Firmware Interface*
UEM	*Unified Endpoint Management*
USB	*Universal Serial Bus*
ZAR	Zona de Acceso Restringido