centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 498A

Arquitectura multidominio de Puesto de Trabajo (*End Point*) seguro
Caso de Uso: Difusión Limitada – Sin Clasificar

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
2020.06.18 20:17:25 +02'00'

NIPO: 083-20-098-3

Fecha de Edición: junio de 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. OBJETO

1. El objeto de la presente guía es el de presentar una serie de casos de uso frecuentes en los que sería aplicable la arquitectura multidominio de puesto de trabajo (*End Point*) seguro descrita en la guía CCN-STIC-498. Por tanto, el contenido de esta guía no debe considerarse de forma aislada, sino como un complemento de la anterior en el que se refinan las medidas de seguridad de aplicación en base a la aplicación de un contexto determinado.

2. Concretamente, se consideran los escenarios específicos en el que un mismo equipo anfitrión va a manejar información clasificada y está configurado para trabajar con dos dominios de seguridad: DIFUSIÓN LIMITADA y SIN CLASIFICAR.

3. En los casos presentados se hablará, de forma genérica, de DIFUSIÓN LIMITADA, aunque serían aplicables las mismas consideraciones a cualquier otro ámbito equivalente (NATO RESTRICTED, UE RESTRICTED, OCCAR RESTRICTED, etc.).

2. CASOS DE USO

2.1 ORDENADOR PORTÁTIL CON SEPARACIÓN DE INFORMACIÓN DIFUSIÓN LIMITADA Y SIN CLASIFICAR Y ACCESO A INTERNET

2.1.1 DESCRIPCIÓN DEL CASO DE USO

4. En numerosas ocasiones, el personal de la Administración y de las empresas que dan servicio a la Administración necesitan manejar información clasificada desde sus ordenadores portátiles durante viajes u otras actividades que incluyan desplazamientos. Típicamente, necesitarán transportar y manejar información clasificada hasta nivel DIFUSIÓN LIMITADA (DL) o equivalente (NATO RESTRICTED, UE RESTRICTED, OCCAR RESTRICTED, etc.).

5. Además, también se contempla la necesidad de disponer de acceso a internet en condiciones seguras, así como de intercambiar información con la organización a la que pertenece el usuario sin que ello suponga un riesgo de divulgación de información clasificada, para lo que se emplean soluciones de cifra *on line* (p.ej. una VPN) u *off-line*.

6. A continuación, se proponen posibles soluciones para este caso de uso empleando una arquitectura *End Point* Tipo 1 y Tipo 2.

2.1.2 ARQUITECTURA END POINT TIPO 1: CASO 1

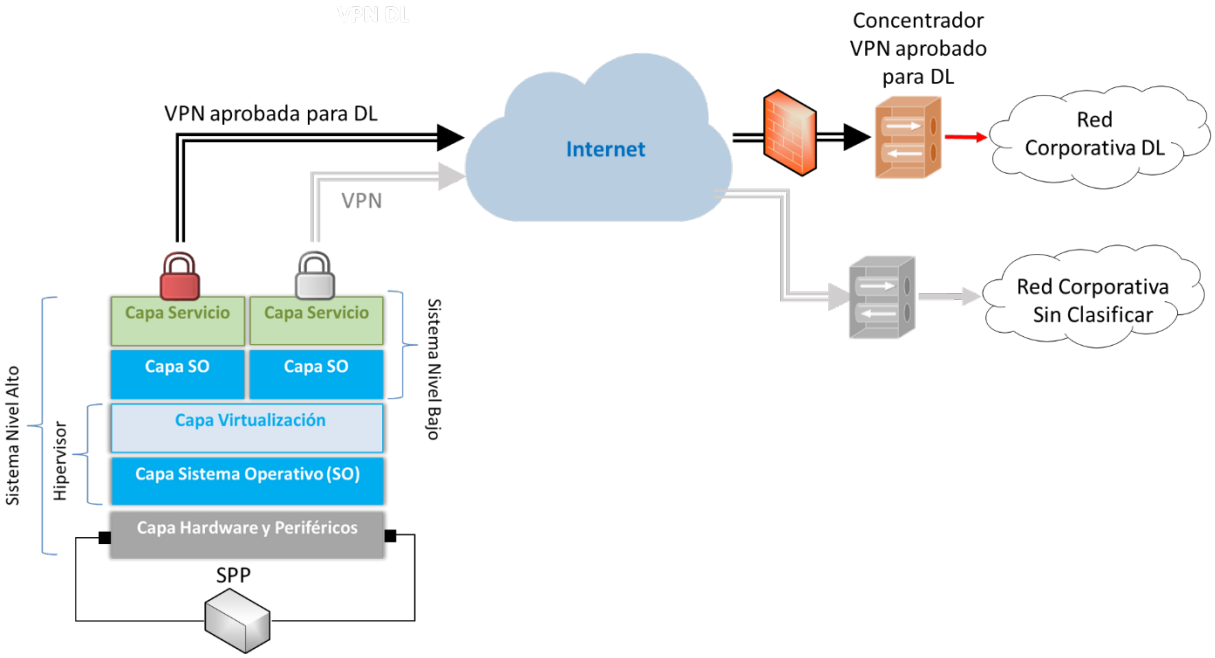

Figura 1. Esquema de arquitectura Tipo1: Caso 1.

7. El caso planteado es una arquitectura *End Point* Tipo 1 con dos (2) máquinas virtuales. La información clasificada DL se manejaría en la Capa de Servicio de la

máquina virtual destinada al Nivel Alto, mientras que la no clasificada se manejaría en la Capa de Servicio de la máquina virtual dedicada al Nivel Bajo.

8. Ambas máquinas dispondrán de la posibilidad de conectarse remotamente a redes corporativas en las que se maneje información clasificada del mismo ámbito y nivel haciendo uso de un medio de cifra. La conexión a internet se realizará desde el sistema de la organización utilizando la arquitectura de seguridad de este, nunca directamente.

9. La arquitectura planteada es la descrita en el apartado 8 de la guía CCN-STIC-498, con las especificaciones concretas que se detallan a continuación.

2.1.2.1 CIFRADO DE DATOS (CIF)

10. Se describen los diferentes mecanismos de cifrado de datos:

    a) **Cifrado *on-line***. En este caso, el sistema hará uso de dos redes privadas virtuales (VPN) para proteger las comunicaciones entre las máquinas y la organización. El canal de información aportará también autenticación extremo a extremo basada en la utilización de certificados. En el caso de la VPN para DL, deberán utilizarse medios de cifra aprobados para ese grado de clasificación y ámbito de trabajo[1] (p.ej. cliente VPN *software* aprobado para NATO RESTRICTED).

    b) **Cifrado *off-line***: En este caso, la utilización de cifrado *off-line* no será obligatoria, dado que se cuenta con una VPN aprobada para intercambiar información clasificada DL con la organización. No obstante, esta medida sigue siendo exigible en caso de que exista la necesidad de almacenar, enviar o transportar dicha información de forma no controlada en un medio inseguro (p.ej.: un *pen drive*). En este caso, todos los dispositivos/herramientas de cifrado *off-line* deberán estar aprobados para la protección de información grado DL.

    Como ya se indica en el apartado 8 de la guía CCN-STIC-498, en caso de que la información transportada no esté cifrada 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 para garantizar la confidencialidad e integridad de la información clasificada ya que el dispositivo, al ser un equipo de viaje, sale de una zona controlada.

    Todos los dispositivos/herramientas de cifrado *at-rest* deberán estar aprobados para la protección de información DL. En caso contrario, serán de aplicación al equipo las **medidas de protección en el transporte de Información Clasificada establecidas en las Normas de la Oficina Nacional de Seguridad**.

[1] El medio de cifra aprobado para el ámbito de trabajo puede ser un cliente software VPN, o un teléfono móvil seguro conectado a modo de equipo de cifra externo, un cifrador IP portable, etc.

2.1.2.2 BORRADO SEGURO (BSD)

11. Deberán utilizarse herramientas de borrado seguro, de acuerdo con lo establecido en la guía *CCN-STIC-305 Destrucción y Sanitización de soportes informáticos* para DL, en los siguientes casos:

    a) Cuando el sistema se encuentre en tareas de mantenimiento externo o deje de estar operativo.

    b) Cuando la información haya dejado de ser necesaria.

2.1.2.3 INTERCONEXIÓN DE SISTEMAS

12. Como ya se indicó en el apartado 8 de la guía CCN-STIC-498, las comunicaciones entre máquinas virtuales estarán deshabilitadas, no obstante, en caso de que sea necesario realizar intercambio de información entre ambas, deberá establecerse una interconexión DL<->SIN CLASIFICAR, y por lo tanto, deberán utilizarse los sistemas de protección de perímetro (SPP) para ese escenario establecidos en la guía *CCN-STIC 302 Interconexión de sistemas de las TIC que manejan información clasificada en la Administración* o, en su defecto, un air gap.

2.1.2.4 COMPONENTES APROBADOS

13. Para el sistema clasificado DL, se utilizarán **obligatoriamente** productos que se encuentren en el listado de productos aprobados del CPSTIC para el grado de clasificación DL o superior, para los siguientes casos:

    a) Sistemas operativos.

    b) Dispositivos/herramientas de cifrado empleados para la protección de información DL.

14. Para el sistema DL, 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 DL. En caso de que no existan productos dentro del listado, se utilizarán productos incluidos en el listado de Productos Cualificados del CPSTIC. En caso de que no existan 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).

15. Para el sistema Sin Clasificar, los dispositivos/herramientas de seguridad empleados para proteger a los activos del sistema deberán encontrarse, siempre que sea posible, dentro del listado de Productos Cualificados del CPSTIC. Al igual que en el caso anterior, cuando no existan 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).

2.1.2.5 PROTECCIÓN DE EMISIONES ELECTROMAGNÉTICAS

16. Al tratarse de un sistema DL, no existen requisitos de emanaciones aplicables al sistema.

2.1.3 ARQUITECTURA END POINT TIPO 1: CASO 2

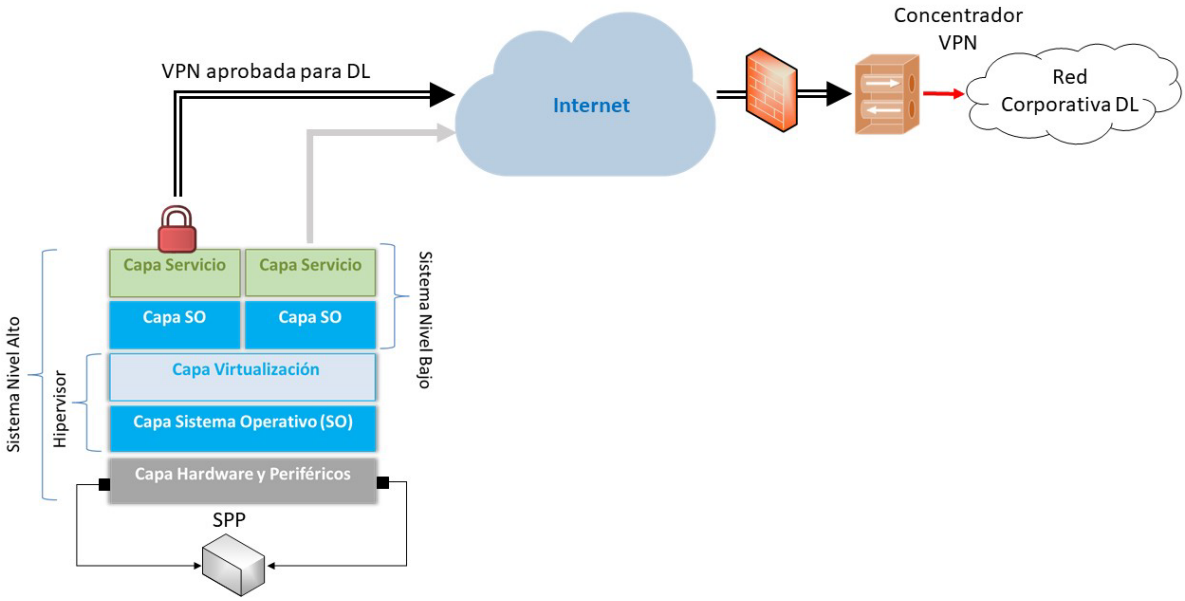

Figura 2. Esquema de arquitectura Tipo1: Caso 2.

17. Al igual que en el Caso 1, se trata de una arquitectura *End Point* Tipo 1 con dos (2) máquinas virtuales. La información clasificada DL se manejaría en la Capa de Servicio de la máquina virtual destinada al Nivel Alto, mientras que la no clasificada se manejaría en la Capa de Servicio de la máquina virtual dedicada al Nivel Bajo.

18. Existirá la posibilidad de conexión remota a una red corporativa del mismo ámbito y grado de clasificación que el de la MV haciendo uso de un medio de cifra *on-line*. La conexión a internet se realizará desde la máquina sin clasificar.

19. La arquitectura planteada es la descrita en el apartado 8 de la guía CCN-STIC-498, con las especificaciones concretas que se detallan a continuación.

2.1.3.1 CIFRADO DE DATOS (CIF)

20. Se describen los diferentes mecanismos de cifrado de datos:

    a) **Cifrado *on-line***. En este caso, el sistema hará uso de una red privada virtual (VPN) DL para proteger las comunicaciones entre la máquina virtual y la organización. El canal de información aportará también autenticación extremo a extremo basada en la utilización de certificados. Esta VPN deberá proteger la información DIFUSIÓN LIMITADA y, por lo tanto, deberán

utilizarse medios de cifra aprobados para ese grado de clasificación y ámbito de trabajo[2] (p.ej. cliente VPN *software* aprobado para NATO RESTRICTED).

b) **Cifrado *off-line***: En este caso, la utilización de cifrado *off-line* no será obligatoria, dado que se cuenta con una VPN aprobada para intercambiar información clasificada con la organización. No obstante, esta medida sigue siendo exigible en caso de que exista la necesidad de almacenar, enviar o transportar dicha información de forma no controlada en un medio inseguro (p.ej.: un *pen drive*). En este caso, todos los dispositivos/herramientas de cifrado *off-line* deberán estar aprobados para la protección de información grado DL.

   Como ya indicamos en el apartado 8 de la guía CCN-STIC-498, en caso de que la información transportada no esté cifrada 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 para garantizar la confidencialidad e integridad de la información clasificada cuando el dispositivo salga de la zona controlada.

   Todos los dispositivos/herramientas de cifrado *at-rest* deberán estar aprobados para la protección de información DL. En caso contrario, serán de aplicación al equipo las **medidas de protección en el transporte de Información Clasificada establecidas en las Normas de la Oficina Nacional de Seguridad**.

2.1.3.2 BORRADO SEGURO (BSD)

21. Son aplicables las mismas medidas que para el Caso 1 de la presente Guía.

2.1.3.3 INTERCONEXIÓN DE SISTEMAS

22. Son aplicables las mismas medidas que para el Caso 1 de la presente Guía.

2.1.3.4 COMPONENTES APROBADOS

23. Son aplicables las mismas medidas que para el Caso 1 de la presente Guía.

2.1.3.5 PROTECCIÓN DE EMISIONES ELECTROMAGNÉTICAS

24. Al tratarse de un sistema DL, no existen requisitos de emanaciones aplicables al sistema.

[2] El medio de cifra aprobado para el ámbito de trabajo puede ser un cliente software VPN, o un teléfono móvil seguro conectado a modo de equipo de cifra externo, un cifrador IP portable, etc.

2.1.3.6 MECANISMOS DE PROTECCIÓN ADICIONALES

25. Dado que en este caso uno de los sistemas se conecta directamente a internet sin utilizar la arquitectura de seguridad de la organización a la que pertenece, deberá implementar mecanismos de protección de la navegación, como pueden ser herramientas de filtrado de navegación y proxy.

2.1.4 ARQUITECTURA END POINT TIPO 1: CASO 3

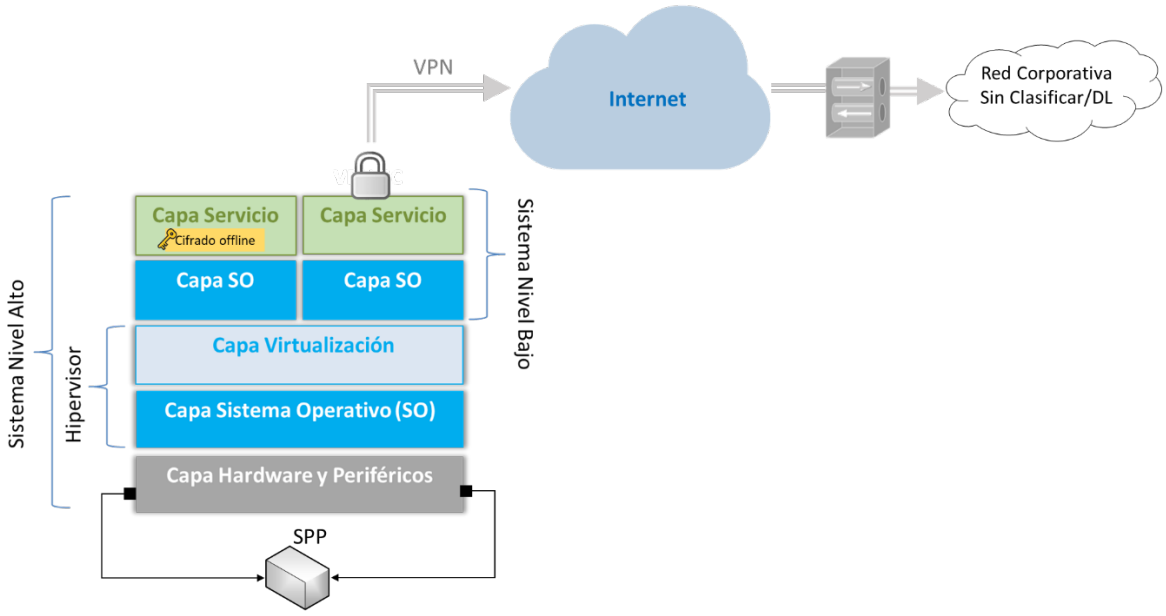

Figura 3. Esquema de arquitectura Tipo1: Caso 3.

26. Al igual que en los casos anteriores, se trata de una arquitectura *End Point* Tipo 1 con dos (2) máquinas virtuales. La información clasificada DL se manejaría en la Capa de Servicio de la máquina virtual destinada al Nivel Alto, mientras que la no clasificada se manejaría en la Capa de Servicio de la máquina virtual dedicada al Nivel Bajo.

27. Existirá la posibilidad de conexión remota a través de VPN a una red corporativa SIN CLASIFICAR o DIFUSIÓN LIMITADA desde la máquina sin clasificar. En caso de que se desee enviar información clasificada a la organización se enviará cifrada a través de ese canal. La conexión a internet se realizará desde la red de la organización.

28. La arquitectura planteada es la descrita en el apartado 8 de la guía CCN-STIC-498, con las especificaciones concretas que se detallan a continuación.

2.1.4.1 CIFRADO DE DATOS (CIF)

29. Se describen los diferentes mecanismos de cifrado de datos:

a) **Cifrado *on-line***. En este caso, el sistema hará uso de una red privada virtual (VPN) para proteger las comunicaciones entre la máquina virtual y la organización. El canal de información aportará también autenticación extremo a extremo basada en la utilización de certificados.

b) **Cifrado *off-line***: En este caso, la utilización de cifrado *off-line* será obligatoria siempre que sea necesario enviar información clasificada a la organización a través de la VPN, dado que se utiliza un sistema sin clasificar para ello. Además, esta medida también se exigirá en caso de que exista la necesidad de almacenar, enviar o transportar información DL de forma no controlada en un medio inseguro (p.ej.: un *pen drive*). En este caso, todos los dispositivos/herramientas de cifrado *off-line* deberán estar aprobados para la protección de información grado DL.

   Como ya indicamos en el apartado 8 de la guía CCN-STIC-498, en caso de que la información transportada no esté cifrada 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 para garantizar la confidencialidad e integridad de la información clasificada cuando el dispositivo salga de la zona controlada.

   Todos los dispositivos/herramientas de cifrado *at-rest* deberán estar aprobados para la protección de información DL. En caso contrario, serán de aplicación al equipo las **medidas de protección en el transporte de Información Clasificada establecidas en las Normas de la Oficina Nacional de Seguridad**.

2.1.4.2 BORRADO SEGURO (BSD)

30. Son aplicables las mismas medidas que para el Caso 1 de la presente Guía.

2.1.4.3 INTERCONEXIÓN DE SISTEMAS

31. El SPP entre las MV dependerá de si es necesario realizar intercambio de información entre ellas o se puede considerar que la MV no clasificada actúa como "*relé*" de información clasificada cifrada *off-line*, desde la MV DL a la Red Corporativa DL. En este caso, el SPP entre MV podría estar constituido por un único cortafuegos.

32. En caso de que sea necesario realizar intercambio de información entre ambas, deberá establecerse una interconexión DL<->SIN CLASIFICAR y, por lo tanto, deberán utilizarse los sistemas de protección de perímetro (SPP) para ese escenario establecidos en la guía *CCN-STIC 302 Interconexión de sistemas de las TIC que manejan información clasificada en la Administración* o, en su defecto, un *air gap*.

2.1.4.4 COMPONENTES APROBADOS

33. Son aplicables las mismas medidas que para el Caso 1 de la presente Guía.

2.1.4.5 PROTECCIÓN DE EMISIONES ELECTROMAGNÉTICAS

34. Al tratarse de un sistema DL, no existen requisitos de emanaciones aplicables al sistema.

2.1.5 ARQUITECTURA END POINT TIPO 1: CASO 4

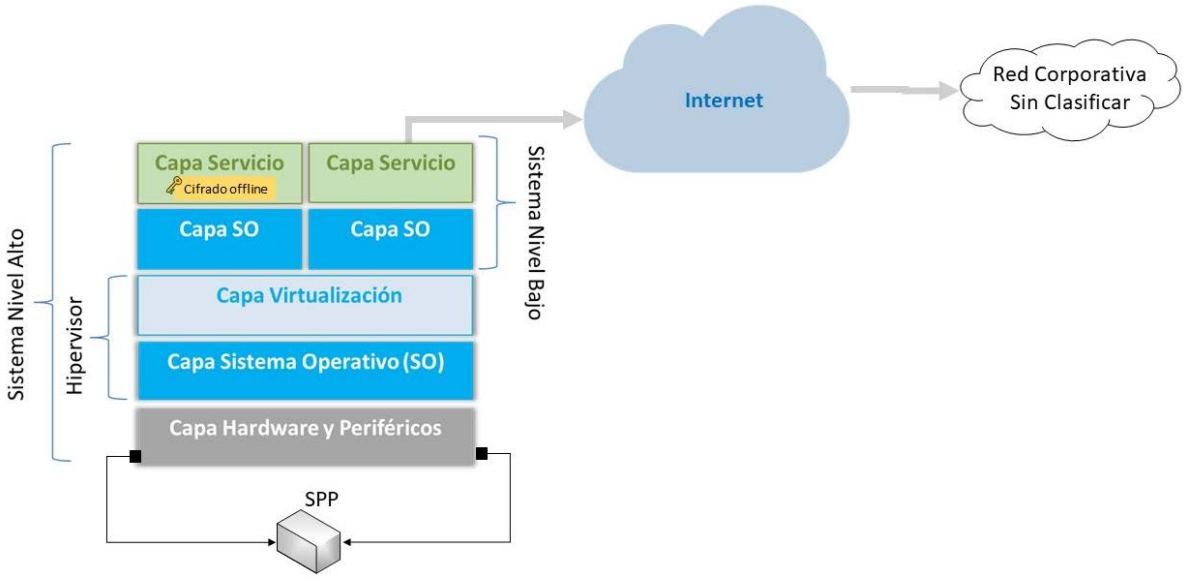

Figura 4. Esquema de arquitectura Tipo1: Caso 4.

35. Al igual que en el Caso 1, se trata de una arquitectura *End Point* Tipo 1 con dos máquinas virtuales. La información clasificada DL se manejaría en la Capa de Servicio de la máquina virtual destinada al Nivel Alto, mientras que la no clasificada se manejaría en la Capa de Servicio de la máquina virtual dedicada al Nivel Bajo.

36. Existirá la posibilidad de conexión a través de internet a una red corporativa sin clasificar desde la máquina sin clasificar. La conexión a internet se realizará directamente desde el *end point*.

37. La arquitectura planteada es la descrita en el 8 de la guía CCN-STIC-498, con las especificaciones concretas que se detallan a continuación.

2.1.5.1 CIFRADO DE DATOS (CIF)

38. Se describen los diferentes mecanismos de cifrado de datos:

    a) **Cifrado *on-line***. En este caso, no se utilizarán mecanismos de cifrado *on-line*.

    b) **Cifrado *off-line***: En este caso, la utilización de cifrado *off-line* será obligatoria siempre que sea necesario enviar información clasificada a la organización

través de canales inseguros que no implementan cifrado. Además, esta medida también se exigirá en caso de que exista la necesidad de almacenar, enviar o transportar información DL de forma no controlada en un medio inseguro (p.ej.: un *pen drive*). En este caso, todos los dispositivos/herramientas de cifrado *off-line* deberán estar aprobados para la protección de información grado DL.

Como ya indicamos en el apartado 8 de la guía CCN-STIC-498, en caso de que la información transportada no esté cifrada 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 para garantizar la confidencialidad e integridad de la información clasificada cuando el dispositivo salga de la zona controlada.

Todos los dispositivos/herramientas de cifrado *at-rest* deberán estar aprobados para la protección de información DL. En caso contrario, serán de aplicación al equipo las **medidas de protección en el transporte de Información Clasificada establecidas en las Normas de la Oficina Nacional de Seguridad**.

2.1.5.2 BORRADO SEGURO (BSD)

39. Son aplicables las mismas medidas que para el Caso 1 de la presente Guía.

2.1.5.3 INTERCONEXIÓN DE SISTEMAS

40. Son aplicables las mismas medidas que para el Caso 1 de la presente Guía.

2.1.5.4 COMPONENTES APROBADOS

41. Son aplicables las mismas medidas que para el Caso 1 de la presente Guía.

2.1.5.5 PROTECCIÓN DE EMISIONES ELECTROMAGNÉTICAS

42. Al tratarse de un sistema DL, no existen requisitos de emanaciones aplicables al sistema.

2.1.5.6 MECANISMOS DE PROTECCIÓN ADICIONALES

43. Dado que en este caso, uno de los sistemas se conecta directamente a internet, sin utilizar la arquitectura de seguridad de la organización a la que pertenece, deberá implementar mecanismos de protección de la navegación, como pueden ser herramientas de filtrado de navegación y proxy.

2.1.6 ARQUITECTURA END POINT TIPO 2

44. Los casos de uso planteados para la arquitectura de virtualización Tipo 1 son aplicables para una arquitectura de Tipo 2. En esta arquitectura la información clasificada DL se manejaría en la Capa de Servicio del host destinada al Nivel Alto, mientras que la no clasificada se manejaría en la Capa de Servicio de la máquina virtual dedicada al Nivel Bajo.

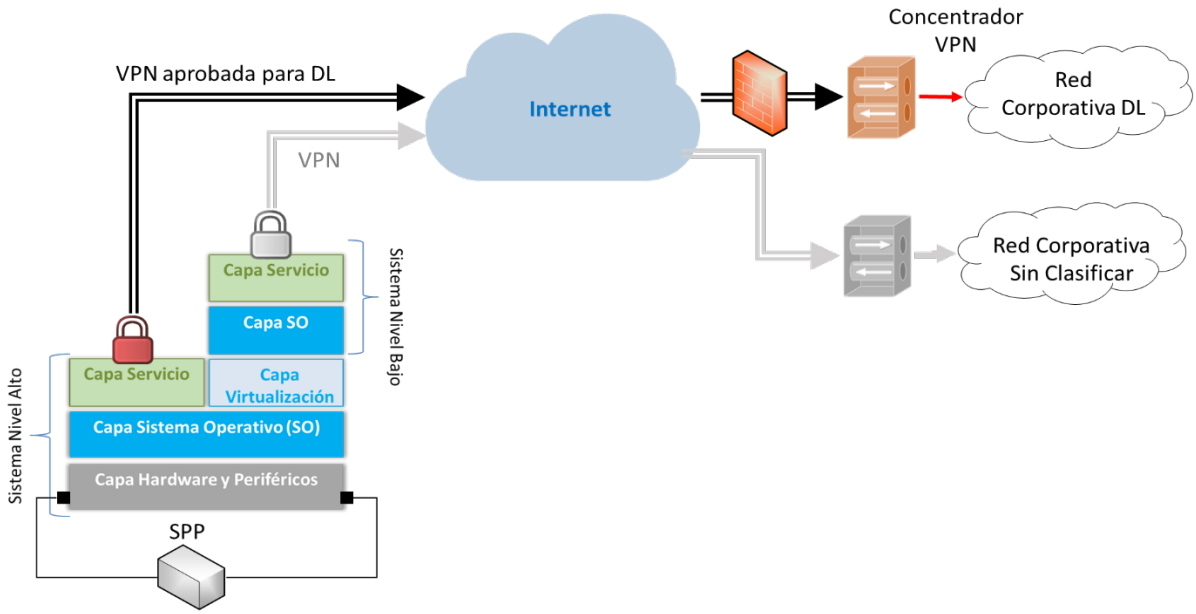

Figura 10. Ejemplo de esquema de arquitectura Tipo 2

2.2 ORDENADOR PORTÁTIL CON SEPARACIÓN DE INFORMACIÓN DIFUSIÓN LIMITADA DE DIFERENTES ÁMBITOS Y SIN CLASIFICAR Y ACCESO A INTERNET

2.2.1 DESCRIPCIÓN DEL CASO DE USO

45. Cuando se trabaja con información clasificada, es frecuente tener la necesidad de acceder a información de diferentes ámbitos de clasificación (OTAN, UE, Nacional…) y de diferentes niveles. Por ello, es necesario contemplar esta casuística a la hora de definir la arquitectura de *End Point* multidominio.

46. Además, también se contempla la necesidad de disponer de acceso a internet en condiciones seguras, así como de intercambiar información con la organización a la que pertenece el usuario sin que ello suponga un riesgo de divulgación de información clasificada, para lo que se emplean soluciones de cifra *on line* (p.ej. una VPN) u *off-line*.

2.2.2 ARQUITECTURAS END POINT TIPO 1 Y 2

47. Al igual que en los casos anteriores, se proponen Arquitecturas *End Point* Tipo 1 y Tipo 2, ya que son las más comunes en estos casos de uso.

48. A fin de no multiplicar el número de máquinas virtuales, se recomienda optar por una arquitectura en la que se agrupen en una misma máquina virtual aquellos ámbitos cuya coexistencia está admitida (posibilidad de doble acreditación), siempre y cuando se utilicen medios de cifra aprobados que admitan doble uso (p.ej. nacional y OTAN) y que se interconecten con sistemas acreditados a los mismos ámbitos de clasificación.

49. Por ejemplo, un ordenador portátil aislado puede acreditarse para DIFUSIÓN LIMITADA NACIONAL y a la vez para UE RESTRICTED y NATO RESTRICTED (bajo las condiciones más restrictivas de los tres ámbitos); sin embargo, un medio de cifra aprobado para DIFUSIÓN LIMITADA y NATO RESTRICTED, no podrá emplearse para UE RESTRICTED (se requieren diferencias significativas respecto a la versión OTAN).

50. Así, se plantea una Arquitectura *End Point* Tipo 1, con una máquina virtual destinada a DIFUSIÓN LIMITADA nacional y NATO RESTRICTED, otra máquina virtual destinada a UE RESTRICTED y, finalmente, una máquina virtual para información sin clasificar y acceso a internet. Es necesario precisar que esta distribución de máquinas virtuales y ámbitos de información podría ser diferente; dependerá de los ámbitos de clasificación de la información a los que se necesita acceder y la disponibilidad de soluciones de cifra con doble aprobación.

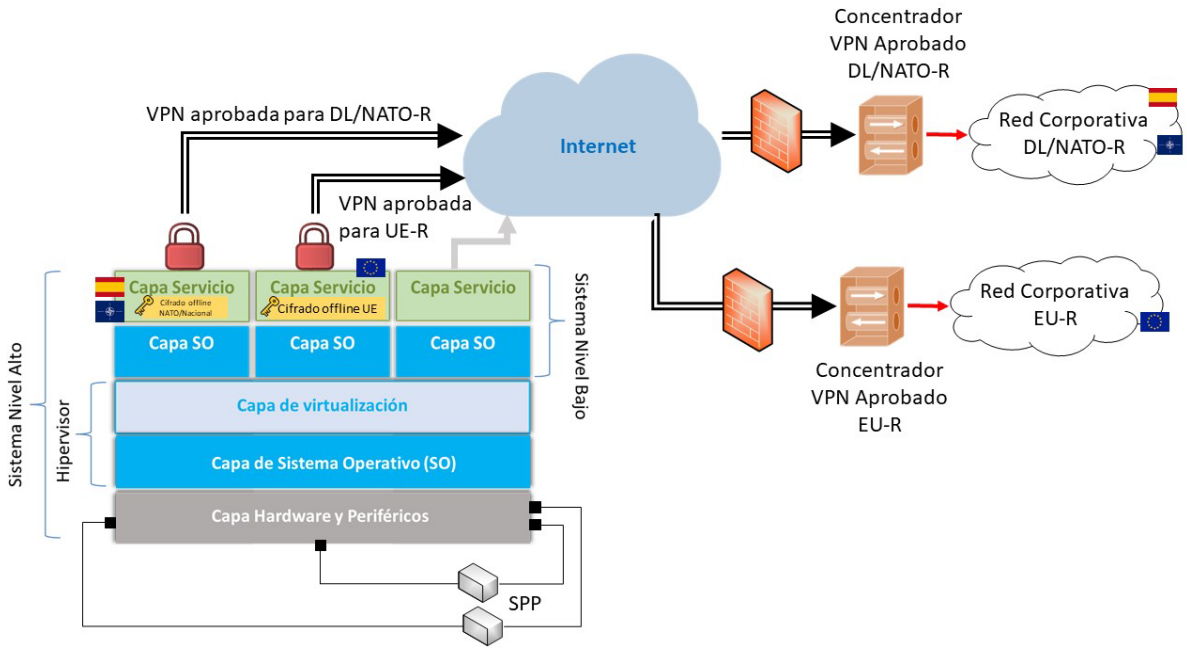

Figura 11. Esquema de arquitectura Tipo2 con diferentes ámbitos de clasificación

51. Desde la Capa de Servicio de la máquina virtual destinada al ámbito nacional y OTAN, existirá la posibilidad de conexión remota a una red corporativa donde se maneje información clasificada de esos dos ámbitos, haciendo uso de un medio de cifra con una aprobación nacional DIFUSIÓN LIMITADA y también NATO RESTRICTED[3]. Por su parte, desde la Capa de Servicio de la máquina virtual destinada al ámbito UE, será posible la conexión remota a una red corporativa donde se maneje información de ese mismo ámbito, para lo que será necesario un medio de cifra con una aprobación UE RESTRICTED[4].

52. Otra posibilidad para el envío y recepción de información clasificada nacional y OTAN será el empleo de una solución de cifrado *off-line* aprobada para DIFUSIÓN LIMITADA y NATO RESTRICTED (también sería factible usar una solución para el ámbito nacional y otra para el ámbito OTAN). Dicha solución deberá ser usada desde la Capa de Servicio de la máquina virtual destinada al ámbito nacional y OTAN, mientras que el envío y recepción de esos archivos cifrados se harán desde la Capa de Servicio de la máquina virtual para la información sin clasificar (con acceso a Internet). Para ello deberá ser posible transferir estos archivos cifrados entre las Capas de Servicio de esas dos máquinas virtuales.

53. De forma equivalente, también existirá la posibilidad de envío y recepción de información clasificada UE RESTRICTED mediante una solución de cifrado *off-line* aprobada para ese ámbito. Dicha solución deberá ser usada desde la Capa de Servicio de la máquina virtual destinada al ámbito UE, mientras que el envío y recepción de esos archivos cifrados se harán desde la Capa de Servicio de la máquina virtual para la información sin clasificar (con acceso a Internet). Para ello deberá ser posible transferir estos archivos cifrados entre las Capas de Servicio de esas dos máquinas virtuales.

54. En el caso de utilizar una Arquitectura Tipo 2, la solución sería la misma, y se utilizará el host **preferiblemente para la máquina con clasificación nacional** (en caso de que la haya). Cuando no se trabaje con información clasificada nacional, no existirán preferencias de configuración.

[3] El medio de cifra aprobado para el ámbito nacional y OTAN puede ser un cliente software VPN, o un teléfono móvil seguro conectado a modo de equipo de cifra externo, un cifrador IP portable, etc.
[4] El medio de cifra aprobado para el ámbito UE puede ser un cliente software VPN, o un teléfono móvil seguro conectado a modo de equipo de cifra externo, un cifrador IP portable, etc.

3. REFERENCIAS

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

STIC.2 CCN-STIC-301 Medidas de Seguridad TIC a implementar en sistemas clasificados

STIC.3 CCN-STIC 302 Interconexión de sistemas de las TIC que manejan información clasificada en la Administración

STIC.4 CCN-STIC-305 Destrucción y Sanitización de soportes informáticos

STIC.5 CCN-STIC- 498 Arquitectura multidominio de Puesto de Trabajo (End Point) Seguro

4. ABREVIATURAS

BSD	Borrado Seguro de Datos
CCN	Centro Criptológico Nacional
CIF	Cifrado de Datos
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación
DL	Difusión Limitada
ENECSTI	Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información
MV	Máquina Virtual
ONS	Oficina Nacional de Seguridad
SPP	Sistema de Protección de Perímetro
STIC	Seguridad de las Tecnologías de la Información y la Comunicación
TIC	Tecnologías de la Información y la Comunicación
VM	*Virtual Machine*
VPN	*Virtual Private Network*