



GUÍA DE SEGURIDAD DE LAS TIC
(CCN-STIC-409 A)

COLOCACIÓN DE ETIQUETAS DE SEGURIDAD

MAYO 2013

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE LA PRESIDENCIA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC,
ou=sello electrónico, serialNumber=S2800155J,
o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2019.02.12 09:18:54 +01'00'

© Editor y Centro Criptológico Nacional, 2013

Fecha de Edición: mayo 2013

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

PRÓLOGO

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

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

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

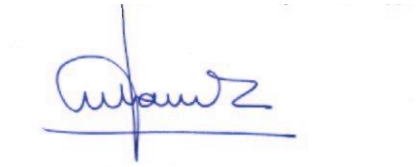
Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIC.

Disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos es, además, uno de los principios que establece la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 sobre el Esquema Nacional de Seguridad (ENS).

Precisamente el Real Decreto 3/2010 de 8 de Enero de desarrollo del Esquema Nacional de Seguridad fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

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

Mayo de 2013



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN 5
2. OBJETO 5
3. COLOCACIÓN DE ETIQUETAS EN EQUIPOS DE USO GENERAL 5
3.1. TECLADO 7
3.2. CPU 8
3.3. MONITOR 9
3.4. TELÉFONO 10
3.5. ROUTER 11
3.6. PORTATIL 12

1. INTRODUCCIÓN

1. El Centro Criptológico Nacional es el responsable de garantizar la seguridad de las tecnologías de la información. Una de las formas de garantizar esta seguridad es la de enseñar el uso de medidas preventivas para detectar posibles manipulaciones del diferente equipamiento desplegado mediante la colocación de etiquetas de seguridad.

2. Estas etiquetas proporcionan unos mecanismos de detección ante manipulaciones que garantizan razonablemente la integridad hardware de los equipos.

3. Las etiquetas que se utilizaran para todos los ejemplos son ADVANTAGE.

2. OBJETO

4. Esta guía tiene por objeto servir como referencia para la colocación de etiquetas de seguridad en dispositivos de uso general en los diferentes organismos de la Administración Pública.

5. La colocación de las etiquetas de seguridad en los cifradores certificados criptológicamente por el Centro Criptológico Nacional se recogen en la guía "CCN-STIC 409 B Colocación de etiquetas de seguridad en equipos de cifra". Dicha guía está clasificada como CONFIDENCIAL, por lo que debe ser solicitada por oficio detallando la marca y el modelo del equipo de cifra del que se desea recibir la información sobre la colocación de etiquetas.

3. COLOCACIÓN DE ETIQUETAS EN EQUIPOS DE USO GENERAL

6. La colocación de etiquetas de seguridad detecta la instalación de hardware no autorizado dentro de un equipo o la modificación de sus elementos.

7. Para una correcta instalación de las mismas debemos asegurar que cualquier apertura del equipo (autorizada o no) implique la rotura de la etiqueta o el levantamiento de la misma. Además, se debe evitar la colocación de etiquetas en superficies con ángulos o superficies con gran curvatura.

8. Las etiquetas de seguridad empleadas (ya sean tipo ADVANTAGE u otro) deben dejar una marca en el equipo del que se han levantado (ver Figura 1) y en la propia etiqueta debe aparecer una leyenda para reconocer que ha sido manipulada (habitualmente VOID o NULO) (ver Figura 2).



Figura 1 Restos de etiqueta levantada



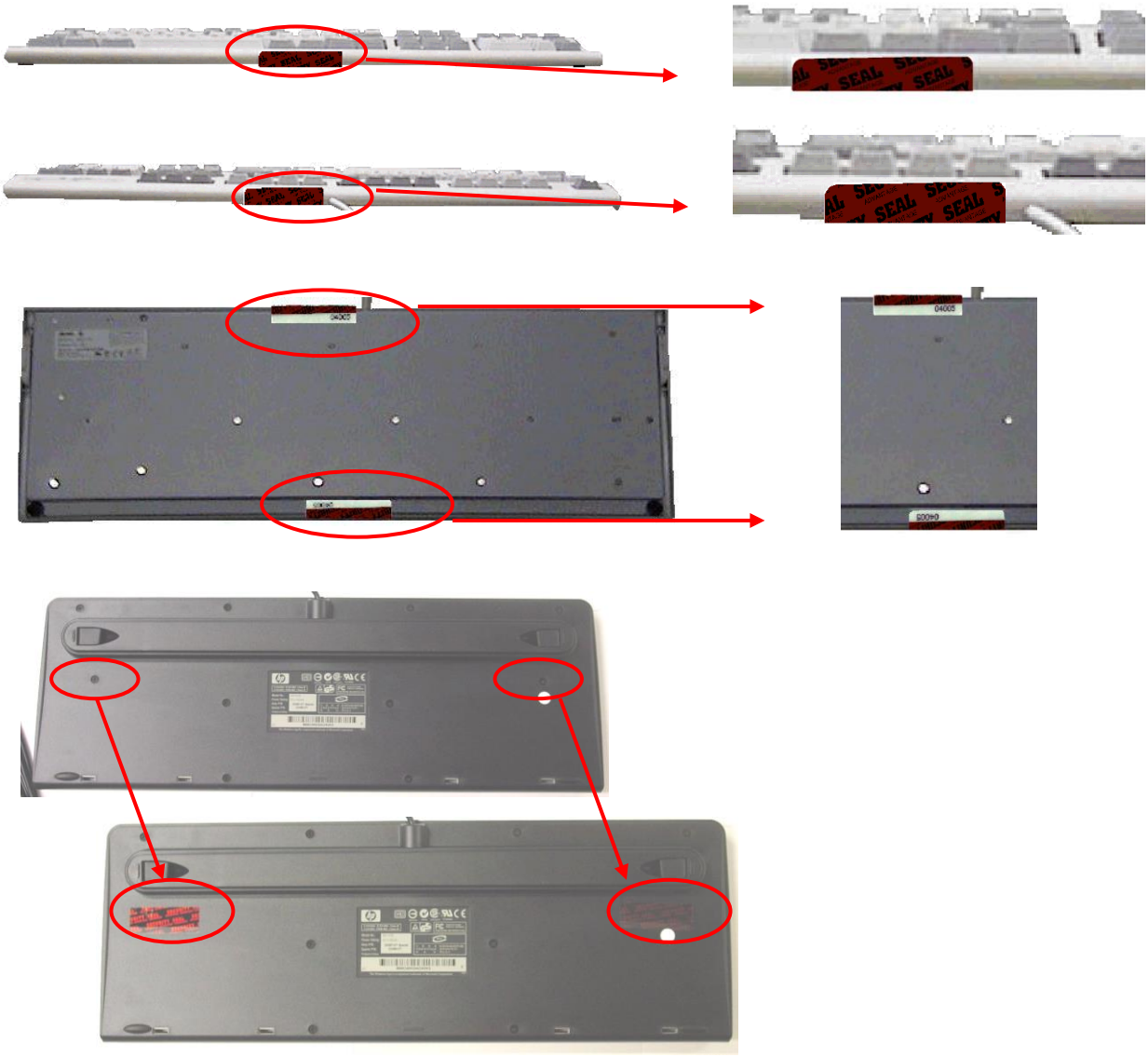
Figura 2 Etiqueta levantada

9. Las etiquetas de seguridad vienen identificadas con un número de serie único. Se debe guardar un registro de los números de serie de las etiquetas utilizadas en cada dispositivo con el fin de detectar la reposición de la etiqueta con un número de serie diferente.

10. En los siguientes apartados se muestran ejemplos de los lugares donde deben colocarse las etiquetas de seguridad en los dispositivos más habituales.

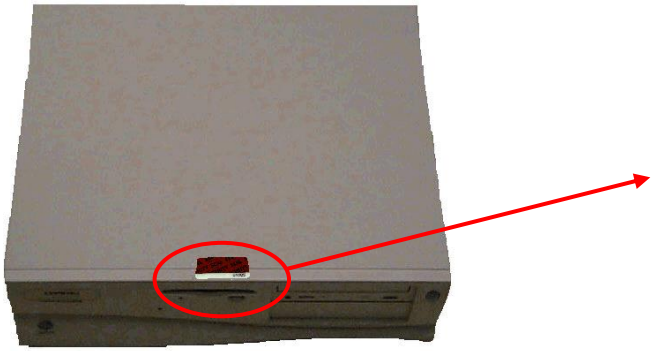
3.1. TECLADO

11. A continuación se muestran ejemplos de colocación de etiquetas de seguridad en teclados.

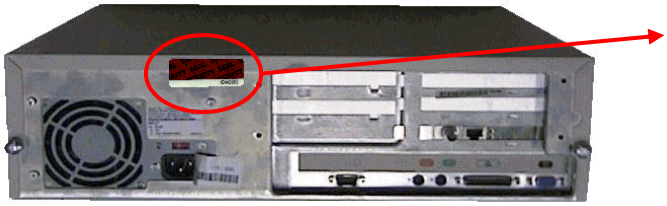


3.2. CPU

12. A continuación se muestran ejemplos de colocación de etiquetas de seguridad en CPU.



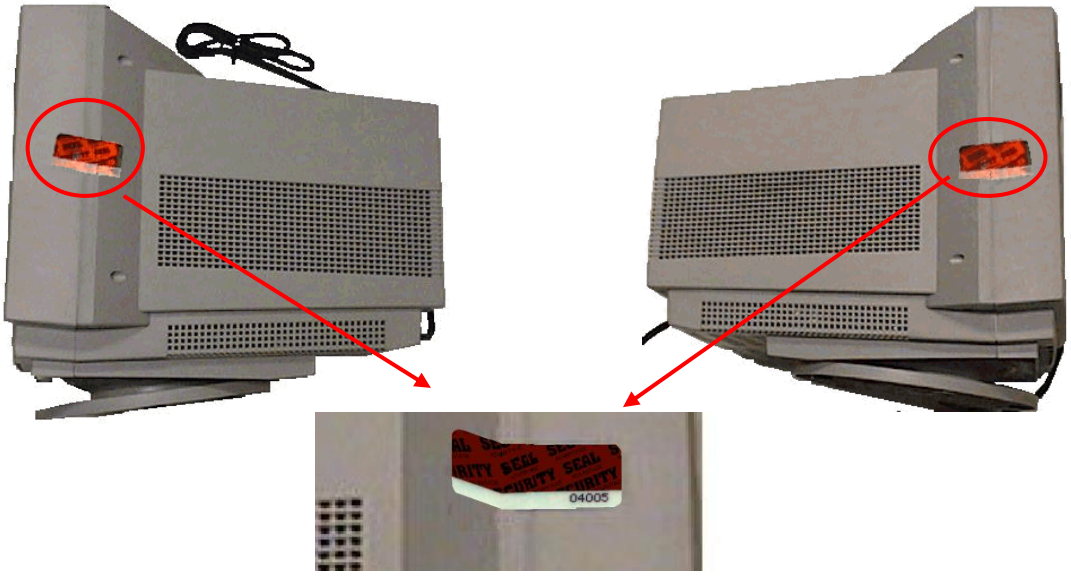






3.3. MONITOR

13. A continuación se muestran ejemplos de colocación de etiquetas de seguridad en monitores.





3.4. TELÉFONO

14. A continuación se muestra un ejemplo de colocación de etiquetas de seguridad en un teléfono.



3.5. ROUTER

15. A continuación se muestra un ejemplo de colocación de etiquetas de seguridad en un router.



3.6. PORTATIL

16. A continuación se muestran ejemplos de colocación de etiquetas de seguridad en un ordenador portátil.



Etiquetas colocadas en la parte superior, protegen el teclado y la apertura de la pantalla.



Etiquetas en la parte inferior que protegen las tapas que dan acceso al interior del equipo, el símbolo ⟶ indica que bajo la etiqueta está un tornillo de fijación de las tapas o de la carcasa