Configuración segura de equipos terminales de usuario en el ámbito del ENS

Abstract: el presente documento recoge una propuesta para garantizar la seguridad de los equipos terminales de usuarios de organismos de pequeño tamaño y recursos limitados, en el ámbito del Esquema Nacional de Seguridad, a través de una configuración segura antes de su instalación en su ubicación definitiva.

Contenido:

1. ANTECEDENTES Y OBJETIVO DEL DOCUMENTO

Durante la realización de los proyectos de adecuación al **Esquema Nacional de Seguridad**, ENS, que el Centro Criptológico Nacional (CCN) ha venido acometiendo en los últimos tiempos y, muy especialmente, cuando se han visto involucrados organismos de pequeño tamaño y recursos limitados (por ejemplo, pequeños ayuntamientos) se ha puesto de manifiesto (y así lo han expresado sus responsables) la necesidad de garantizar la seguridad de los **equipos terminales de los usuarios**.

No solo se precisa garantizar los sistemas de información de nivel superior que pueden dar servicio a tales instituciones, como los servicios prestados a través de diputaciones provinciales u organismos competencialmente equivalentes, sino también la **seguridad de los terminales ubicados en las dependencias municipales.** Garantizar la seguridad, no solo cuando se conectan a los sistemas de información para beneficiarse de servicios compartidos, sino también cuando, de forma independiente, desarrollan actividades propias no soportadas en aquellos servicios.

El presente documento tiene por objeto realizar una propuesta para dar una solución a la problemática señalada en el párrafo anterior, mediante la **creación de Unidades de Bastionado de Equipos de Usuario (UBEU),** que puedan **configurar de manera segura tales equipos, incluso antes de su instalación en sus ubicaciones definitivas**.

2. PROPÓSITO DE LA INICIATIVA

Los equipos de los usuarios de las organizaciones (*end-point*) suelen ser uno de los elementos de mayor riesgo para la seguridad de los sistemas de información de las

entidades del ámbito de aplicación del ENS, especialmente cuando tales equipos pertenecen a organizaciones de pequeño tamaño, que no suelen disponer de los recursos adecuados para la implantación y vigilancia de la seguridad de los sistemas. Ejemplos claros de esta problemática los encontramos en los ayuntamientos más pequeños, con escasa o nula presencia de recursos humanos capaces de abordar dichas competencias.

La iniciativa que se propone pretende dotar a los equipos de usuarios de una **configuración segura antes de su instalación en su ubicación definitiva,** de forma que, llegado el momento de su incorporación a la red de la organización, no sea necesario realizar actividades de bastionado adicionales o se limiten a un conjunto mínimo de operaciones.

La actividad que se propone se enmarca dentro la iniciativa genérica del Centro Criptológico Nacional (CCN) de estandarizar, hasta donde sea posible, los procesos de configuración segura de sistemas, facilitando su despliegue en todos los entornos.

3. BENEFICIOS ESPERADOS DE LA INICIATIVA

3.1 Beneficios operativos

- La entidad destinataria de los equipos no necesita contar de forma permanente con especialistas en el bastionado o configuración segura de los equipos, ni precisará contratar tales actividades a ningún tercero, salvo, quizás, en casos puntuales o cuando las labores de mantenimiento así lo exijan y no estén cubiertas por el servicio de bastionado de las UBEU, que estarán a su vez asesoradas por el CCN y entidades integradoras acreditadas (Guía CCN-STIC 121).
- Optimización de los esfuerzos de configuración segura de los equipos terminales y de los recursos necesarios.
- Integración de los equipos terminales así configurados en la **superficie de equipamiento seguro del CCN**. Esta posibilidad podría permitir a las UBEU otorgar a los equipos de usuario bastionados de un distintivo de **Dispositivo Seguro,** que podría integrarse con las exigencias y requisitos del ENS, facilitando las labores posteriores de inspección y auditoría, y renovándose periódicamente, atendiendo a las estipulaciones que se señalen en los correspondientes acuerdos de mantenimiento que la entidad destinataria pudiera celebrar con dichas UBEU.
- Optimización *just in time* de los equipos, facilitando una rápida entrada en servicio, de forma segura.
- Implementación práctica de la **seguridad desde el diseño y por defecto**, cumpliendo por tanto las exigencias del ENS y de la regulación en materia de Protección de Datos.

- Conformidad con el ENS y homogeneización de las soluciones de seguridad de los equipos terminales de usuario, de todos los sectores del ámbito de aplicación del ENS.

3.2 Beneficios económicos

- Menor coste para la entidad usuaria, si el bastionado se realiza de forma estándar por una unidad especializada. (Economía de escala).

4. DETALLES DEL PROCEDIMIENTO DE BASTIONADO

Seguidamente se recogen algunos detalles en relación con el proceso de bastionado por parte de las UBEU.

- La entidad final (por ejemplo, el pequeño Ayuntamiento) adquirirá los equipos terminales de usuario conforme a los procedimientos habituales derivados de la Ley de Contratos del Sector Público[1], con el asesoramiento del CCN, que podrá ayudar a la entidad a determinar la tipología y características de equipamiento más adecuado en cada caso y los requisitos de hardware y software que se consideren[2].
- La entidad final, en el caso de ya disponer de los equipos terminales, podrá cumplimentar un formulario de autoevaluación que identifique las medidas técnicas y organizativas existentes para su posterior envío a las **Unidades de Bastionado de Equipos de Usuario (UBEU),** a elección de la entidad final, que realizará la evaluación segura del estado de aplicación de medidas requeridas. Con ello se determinará si es requerido el envío del equipo evaluado a la UBEU.
- En el caso de tener que adquirir los equipos terminales, el fabricante o proveedor de los mismos, a requerimiento de la entidad final, entregará los equipos en una de las **UBEU que realizará la configuración segura de los mismos**.
- Las Unidades de Bastionado de Equipos de Usuario (UBEU) pertenecerán a empresas u organizaciones que hayan sido previamente habilitadas por el Centro Criptológico Nacional para tales propósitos y que deberían poseer unas capacidades mínimas que garanticen la calidad de los servicios. Estas UBEU podrían ser parte de las **Entidades Implementadoras de Guías CCN-STIC**, recogidas en la Guía CCN-STIC 121.
- Las UBEU, en sus propias instalaciones, configurarán el sistema operativo del equipo, conforme a las Guías CCN-STIC, a los documentos de Buenas Prácticas y

[1] En el caso de que los equipos terminales de usuario se encuentren ya instalados en las dependencias de la entidad final, el bastionado se realizaría en dichas dependencias, con un coste suplementario, por desplazamiento de los técnicos necesarios.

[2] A estos efectos, podría pensarse en la definición de unos pocos "módulos", que tipificarán las características técnicas que deben poseer los equipos terminales de usuario más habituales.

resto de documentos emanados del CCN, atendiendo también a las recomendaciones del fabricante y a las exigencias que la normativa o procedimientos internos de la entidad final hubiera podido disponer al efecto.

- Los informes de validación de la configuración de seguridad de los equipos generados por las UBEU serán **integrados en soluciones centralizadas propias de la entidad final o las soluciones puestas a su disposición por el CCN** para su correcto seguimiento y gestión en el tiempo (mejora continua).
- Con la periodicidad que sea establecida, la entidad final realizará la ejecución de los procesos establecidos por la UBEU para la revisión de configuración de seguridad de sus equipos, cuyo resultado, será enviado a la UBEU quien verificará el correcto mantenimiento y cumplimiento de los requisitos exigidos por la normativa aplicable.
- Será la UBEU quien determinará la necesidad de intervención en cualquiera de los equipos informados para restablecer su configuración de seguridad.
- Las UBEU podrán establecer acuerdos de asesoramiento y apoyo por parte del CCN o entidades integradoras acreditadas, como soporte ante cualquier resolución de incidencia para la validación de las configuraciones de seguridad.
- El soporte recibido por las UBEU por parte del CCN o entidades integradoras acreditadas, para la subsanación de incidencias de equipos de las entidades finales, permitirá su participación mediante acceso remoto, cumpliéndose en todo momento las condiciones de configuración segura del acceso, transmisión y tratamiento para el manejo de información sensible.
- Además de ello, la UBEU, de conformidad con la Política de Seguridad de la Información de la entidad, los niveles de seguridad y la categoría de seguridad determinada para el sistema de información al que se incorporarán los equipos terminales de usuario, realizará las siguientes actividades, en el marco del ENS.

Actividad	Medida del ENS
Documentará un análisis de riesgo del equipo terminal, en la configuración de seguridad que finalmente se adopte.	Medida [op.pl.2]
Documentará la arquitectura de seguridad del equipo terminal bastionado.	Medida [op.pl.2]
Instalará y documentará, en su caso, los componentes de seguridad que precisen estar certificados en materia de seguridad, atendiendo a la categoría de seguridad del sistema de información.	Medida [op.pl.5]
Instalará y documentará los controles de acceso básico implementados en el bastionado.	Medida [op.acc.2]
En su caso, instalará y documentará las instancias software precisas para implementar los mecanismos de autenticación requeridos.	Medida [op.acc.5]

Actividad	Medida del ENS
Instalará y documentará la configuración de seguridad realizada.	Medida [op.exp.2]
Instalará y documentará las medidas protección frente a código dañino.	Medida [op.exp.6]
En su caso, instalará y documentará las herramientas para la gestión de incidentes.	Medidas [op.exp.7] y [op.exp.9]
En su caso, instalará y documentará las medidas de protección de las claves criptográficas.	Medida [op.exp.11]
En su caso, documentará las medidas a adoptar para la realización de las pruebas periódicas, de conformidad con la normativa de la entidad destinataria de los equipos.	Medida [op.cont.3]
En su caso, documentará las medidas a adoptar para la caracterización del puesto de trabajo, de conformidad con la normativa de la entidad destinataria de los equipos.	Medida [mp.per.1]
Configurará y documentará las medidas relativas al bloqueo del puesto de trabajo.	Medida [mp.eq.2]
En su caso, configurará y documentará las medidas relativas a la protección de portátiles.	Medida [mp.eq.3]
Etiquetará y documentará el etiquetado de los equipos, atendiendo a la normativa suministrada por la entidad destinataria.	Medida [mp.si.1]
Configurará y documentará los mecanismos criptográficos aplicables a los equipos de usuario, atendiendo a la normativa suministrada por la entidad destinataria.	Medida [mp.si.3]
Cumplimentará los registros de entrada/salidas de equipamiento, atendiendo a la normativa de la entidad destinataria.	Medida [mp.si.4]
En su caso, instalará y documentará las herramientas para borrado seguro.	Medida [mp.si.5]
En su caso, implantará y documentará las medidas para el cifrado de la información en el equipo de usuario.	Medida [mp.info.3]
En su caso, instalará y documentará las herramientas y/o certificados digitales para la firma electrónica y el sellado de tiempo, de conformidad con la Política de Firma, Sello y Certificados de la entidad destinataria de los equipos.	Medidas [mp.info.4] y [mp.info.5)
Instalará y documentará las herramientas para limpieza de documentos.	Medida [mp.info.6]
En su caso, instalará y documentará las herramientas para la realización de copias de seguridad del equipo.	Medida [mp.info.9]
Realizará la configuración segura y documentará, atendiendo a la normativa de la entidad destinataria, de las herramientas para la protección del correo electrónico.	Medida [mp.s.1]
En su caso, instalará, configurará y documentará las herramientas para la protección de aplicaciones web.	Medida [mp.s.2]
En su caso, instalará, configurará y documentará las herramientas para la protección frente a la denegación de servicio o incluirá el equipo en el catálogo de equipos a proteger, si el servicio anti-DDoS fuera prestado por un tercero.	Medida [mp.s.8]

- Además de lo anterior, las UBEU:
  - Instalarán las instancias individuales de las **herramientas del CCN** que se consideren necesarias para cada caso.

  - Instalarán cualquier otro software que se requiera en cada caso.
  - A petición de la entidad final, podrá instalar **aplicativos específicos** usados por la entidad final para el desarrollo de sus competencias, incluyendo suites de ofimática, software cliente de aplicaciones propietarias, etc., todo ello con el propósito de entregar un equipo totalmente configurado y listo para el trabajo, una vez incorporado, física y lógicamente, a la red de la entidad final.

- Antes de la prestación de los servicios, la UBEU redactará un borrador de **Contrato y Acuerdo de Nivel de Servicio** con la entidad destinataria, así como los procedimientos para la gestión diaria de los servicios (medidas [op.ext.1] y [op.ext.2] del ENS).
- Con anterioridad a la entrega a la entidad final de los equipos configurados, la UBEU planificará las **sesiones de formación/concienciación** que se consideren necesarias, si ello fuere preciso, siguiendo las indicaciones del CCN.
- Para cada equipo terminal así bastionado, la UBEU redactará y entregará a la entidad final y al CCN un documento que recoja:
  - Las medidas de seguridad/bastionado implantadas en cada equipo.
  - Las medidas que resten por implantar para asegurar la conformidad del equipo con el ENS, atendiendo a los niveles y categoría de seguridad del sistema de información en cuestión.
- Una vez bastionados todos los equipos, la UBEU redactará y entregará a la entidad final y al CCN un documento, para lectura humana y procesable automáticamente, con el **inventario de los equipos bastionados, sus características de configuración y la fecha de su realización**, para su incorporación al inventario general del sistema de información de la entidad final (medida [op.exp.1]).
- Cada UBEU recibirá una **contraprestación económica por cada equipo bastionado**, que será satisfecha por la entidad destinataria de los servicios, en base a unos **módulos que se publicarán** en la página web del CCN (https://www.ccn.cni.es/index.php/es/menu-guias-ccn-stic-es/menu-guias-ccn-stic-121).
- Cada UBEU podrá suscribir con las entidades destinatarias un servicio de **mantenimiento y gestión de las configuraciones realizadas** (medidas [op.exp.3], [op.exp.4], [op.exp.5], [op.exp.6], etc.), que comprenderá la renovación de los Distintivos de Dispositivo Seguro.
- El CCN, en el ejercicio de sus competencias, velará por la adecuada y permanente adecuación de los procedimientos de bastionado a cada caso, y supervisará las actuaciones realizadas por las UBEU.