1 OBJETO Y ALCANCE

El presente documento propone una lista de verificación de las medidas de seguridad mínimas requeridas por el Esquema Nacional de Seguridad – ENS - en relación al bastionado de equipos. Concretamente, para equipos **servidores**, equipos **de usuario** y **dispositivos de red**.

Trata de una lista no exhaustiva, el adjudicatario deberá cumplir también con todas las normas y leyes que apliquen por ámbito en el momento vigente de su diseño e implementación.

La información se recoge en formato tabla, donde:

- Primera columna: indica si el requisito es obligatorio (O) o recomendable (R)
- Segunda columna: indica el requisito a cumplir.

2 MEDIDAS MÍNIMAS DE BASTIONADO

2.1 Servidores

2.1.1 Cuentas de usuario

O	Renombrar la cuenta de administrador
O	Eliminar la cuenta "root" de los servidores Linux ***[1]***
O	Eliminar la cuenta de invitado
O	Configurar una política de contraseñas robustas

[1] *En caso de que no se pueda poner medidas compensatorias, por ejemplo, que no pueda hacerse login con root.*

2.1.2 Control de acceso a la red

O	Deshabilitar NETBIOS en caso de no ser requerido por ninguna aplicación
O	Activar la firma de paquetes SMB como cliente y como servidor
R	Cifrar las comunicaciones del protocolo RDP ***[2]***
O	Impedir la enumeración de recursos compartidos y cuentas SAM
O	Deshabilitar la opción que permite apagar el sistema sin iniciar sesión
O	Impedir que se guarden las contraseñas en el cliente
O	Impedir la conversión SID a nombre de usuario y viceversa
O	Si no se emplea, desactivar ipv6, así como cualquier otro protocolo de red que no sea utilizado. En caso de que se emplee ipv6, se deben aplicar las mismas medidas de seguridad (filtrado en equipamiento de red, control de acceso, segmentación de red, detección de intrusiones, etc.) en el tráfico ipv6 que las que se aplican al tráfico ipv4.
O	Activar el Firewall o cortafuegos
O	Deshabilitar usuarios anónimos para cualquier servicio
O	Deshabilitar communities públicas y/o predecibles para SNMP

[2] *En la medida de lo posible evitar uso de RDP no controlado.*

2.1.3 Protección de la información

O	Deshabilitar la funcionalidad de compartir unidades de disco con propósitos administrativos en aquellas máquinas que se encuentren en entornos críticos o inseguros (como DMZ)
O	Seguir la política del mínimo privilegio en los permisos del sistema de archivos
O	Activar el filtro de ejecución de aplicaciones maliciosas (Data Execution Prevention, DEP)

2.1.4 Sistema Operativo

O	El Sistema Operativo, así como cualquier aplicación instalada en el dispositivo debe tener su correspondiente licencia de uso de acuerdo al fabricante o propietario del mismo
O	Se eliminará todo software innecesario para la función a desarrollar
O	Se realizará una revisión de los servicios inhabilitando todos aquellos innecesarios
O	Se cerrarán todos los puertos innecesarios
R	Se comprobará la instalación y actualización adecuada de software antivirus ***[3]***
O	Requerir Ctrl+Alt+Del antes de la acreditación del usuario
O	Deshabilitar la caché de Contraseñas y Usuarios
O	Pedir la contraseña cuando se requiera una elevación de privilegios
R	Se activará un protector de pantalla que bloquee el terminal con contraseña al cabo de un tiempo predeterminado según la ***Normativa de seguridad del puesto de trabajo [4]***
O	Se configurará el servicio NTP para que se sincronice con el servidor NTP
O	Desactivar la ejecución automática
O	Impedir la instalación de drivers por parte de los usuarios

[3] *Hay que disponer de un antivirus en todos aquellos equipos en los que se pueda poner si afectar a la funcionalidad del mismo*
[4] *En cualquier caso, hay que bloquear el equipo tras 10 minutos de inactividad*

2.1.5 Auditoría

O	Habilitar el Registro de Auditoria (Quién realiza la acción, cuándo, sobre qué información Registrar tanto éxitos como fracasos)

2.1.6 Actualizaciones y Parches

O	Se comprobará la adecuada configuración de los servicios de actualización automática

2.1.7 Protección del arranque y Firmware

O	Activar Secure Boot en sistemas compatibles
O	Proteger el acceso a BIOS/UEFI mediante contraseña
O	Deshabilitar el arranque desde dispositivos externos no autorizados
O	Mantener actualizado el firmware (BIOS/UEFI)
R	Implementar medición o verificación de integridad del arranque (TPM, Measured Boot)

O	Gestionar de forma controlada las excepciones a Secure Boot, conforme al criterio definido por ciberseguridad OT

2.2 Puesto de trabajo

2.2.1 Cuentas de Usuario

O	Renombrar la cuenta de administrador
O	Eliminar la cuenta de invitado
O	Configurar una política de contraseñas robustas

2.2.2 Control de acceso a la red

O	Deshabilitar NETBIOS en caso de no ser requerido por ninguna aplicación
O	Activar la firma de paquetes SMB como cliente y como servidor
R	Cifrar las comunicaciones del protocolo RDP ***[5]***
O	Impedir la enumeración de recursos compartidos y cuentas SAM
O	Deshabilitar la opción que permite apagar el sistema sin iniciar sesión
O	Impedir que se guarden las contraseñas en el cliente
O	Impedir la conversión SID a nombre de usuario y viceversa
O	Si no se emplea, desactivar ipv6, así como cualquier otro protocolo de red que no sea utilizado. En caso de que se emplee ipv6, se deben aplicar las mismas medidas de seguridad (filtrado en equipamiento de red, control de acceso, segmentación de red, detección de intrusiones, etc.) en el tráfico ipv6 que las que se aplican al tráfico ipv4.
O	Activar el Firewall o cortafuegos
O	Deshabilitar usuarios anónimos para cualquier servicio
O	Deshabilitar communities públicas y/o predecibles para SNMP

[5] *En la medida de lo posible evitar uso de RDP no controlado.*

2.2.3 Protección de la información

O	Deshabilitar la funcionalidad de compartir unidades de disco con propósitos administrativos en aquellas máquinas que se encuentren en entornos críticos o inseguros (como DMZ) ***[6]***
O	Seguir la política del mínimo privilegio en los permisos del sistema de archivos
O	Activar el filtro de ejecución de aplicaciones maliciosas (Data Execution Prevention, DEP)

[6] *En general, no compartir unidades de disco en la medida de lo posible.*

2.2.4 Sistema Operativo

O	El Sistema Operativo, así como cualquier aplicación instalada en el dispositivo debe tener su correspondiente licencia de uso de acuerdo al fabricante o propietario del mismo
O	Eliminar todo software innecesario para la función a desarrollar
O	Realizar una revisión de los servicios inhabilitando todos aquellos innecesarios

O	Cerrar todos los puertos innecesarios
R	Comprobar la instalación y actualización adecuada de software antivirus ***[7]***
O	Requerir Ctrl+Alt+Del antes de la acreditación del usuario
O	Deshabilitar la caché de Contraseñas y Usuarios
O	Pedir la contraseña cuando se requiera una elevación de privilegios
R	Se activará un protector de pantalla que bloquee el terminal con contraseña al cabo de un tiempo predeterminado según la ***Normativa de seguridad del puesto de trabajo. [8]***
O	Desactivar la ejecución automática
O	Impedir la instalación de drivers por parte de los usuarios

[7] *Hay que disponer de un antivirus en todos aquellos equipos en los que se pueda poner si afectar a la funcionalidad del mismo.*
[8] *En cualquier caso, hay que bloquear el equipo tras 10 minutos de inactividad.*

2.2.5 Actualizaciones y Parches

O	Se comprobará la adecuada configuración de los servicios de actualización automática ***[9]***

[9] *En cualquier caso, se debe disponer de una planificación de actualización y aplicación de parches de sistemas y aplicaciones*

2.2.6 Protección del arranque y Firmware

O	Activar Secure Boot en sistemas compatibles
O	Proteger el acceso a BIOS/UEFI mediante contraseña
O	Deshabilitar el arranque desde dispositivos externos no autorizados
O	Mantener actualizado el firmware (BIOS/UEFI)
R	Implementar medición o verificación de integridad del arranque (TPM, Measured Boot)
O	Gestionar de forma controlada las excepciones a Secure Boot, conforme al criterio definido por ciberseguridad OT

2.3 Electrónica de red

2.3.1 Cuentas de Usuario

O	Eliminar las cuentas y contraseñas por defecto y/o predecibles
O	Cambiar las contraseñas por defecto y/o predecibles
O	Configurar una política de contraseñas robustas

2.3.2 Control de acceso a la red

O	Deshabilitar “communities” públicas y/o predecibles para SNMP

2.3.3 Sistema Operativo

O	El Sistema Operativo, así como cualquier aplicación instalada en el dispositivo debe tener su correspondiente licencia de uso de acuerdo al fabricante o propietario del mismo
O	Realizar una revisión de los servicios inhabilitando todos aquellos innecesarios
O	Cerrar todos los puertos innecesarios
O	Deshabilitar la caché de Contraseñas y Usuarios

2.3.4 Actualizaciones y Parches

O	Comprobar y actualizar el firmware del dispositivo en caso necesario

ANEXO

Se indica el cuadro de decisión por tipo de activo para la activación del Secure Boot:

Tipo de activo	Exigencia	Criterio	Comentarios prácticos
Puestos de operación (thin clients / HMIs)	Obligatorio	Alta exposición física y riesgo de manipulación	Prioritario reactivar tras incidencias o gestión de vulnerabilidades
Servidores físicos (Windows / Linux)	Obligatorio (si es compatible)	Activos críticos con riesgo de persistencia de malware y afectación a servicios esenciales	Asegurar compatibilidad con BIOS y SO
Servidores virtuales (VM)	Recomendado	Depende del hipervisor y configuración UEFI	Implementar progresivamente
Hipervisores (ESXi, etc.)	Recomendado	Dependencia de versión y arquitectura	Definir roadmap de adopción
Sistemas SCADA / legacy	Excepción justificada	Frecuente incompatibilidad	Documentar excepción y medidas compensatorias
Equipos de comunicaciones (switches, routers)	No aplica	No usan Secure Boot estándar UEFI	Aplicar controles equivalentes de firmware
Cabinas de almacenamiento	No aplica	Arquitectura propietaria	Relevante solo autenticación y firmware
Equipos de campo OT (PLC, RTU, etc.)	No aplica (en general)	No soportan Secure Boot	Aplicar control de firmware y acceso
Equipos portables de mantenimiento	Obligatorio	Alta exposición (USB, movilidad)	Clave para evitar vectores de entrada