OBJECTE

El present document proposa una llista de verificació de les mesures de seguretat mínimes que demana l'ENS en relació amb la fortificació.
És una llista no exhaustiva; l'adjudicatari haurà de complir també totes les normes i lleis que s'hi apliquin per àmbit en el moment vigent del seu disseny i implementació.

MESURES MÍNIMES DE FORTIFICACIÓ PER A SERVIDORS EQUIPS D'USUARI I DISPOSITIUS DE XARXA

Les taules tenen 2 columnes:

- Primera columna: indica si el requisit d'aquesta fila és obligatori (O) o recomanable (R).
- Segona columna: indica el requisit que cal complir.

SERVIDORS

1. COMPTES D'USUARI

O	Canviar el nom del compte d'administrador
O	Eliminar el compte "root" dels servidors Linux ***[1]***
O	Eliminar el compte de convidat
O	Configurar una política de contrasenyes robustes

[1] *En cas que no es puguin posar mesures compensatòries, per exemple, que no pugui fer-se inici de sessió amb root.*

2. CONTROL D'ACCÉS A LA XARXA

O	Deshabilitar NETBIOS en cas que no el requereixi cap aplicació
O	Activar la signatura de paquets SMB com a client i com a servidor
R	Xifrar les comunicacions del protocol RDP ***[2]***
O	Impedir l'enumeració de recursos compartits i comptes SAM
O	Deshabilitar l'opció que permet apagar el sistema sense iniciar sessió
O	Impedir que es guardin les contrasenyes en el client
O	Impedir la conversió SID a nom d'usuari i viceversa
O	Si no s'utilitza, desactivar ipv6, així com qualsevol altre protocol de xarxa que no sigui utilitzat. En cas que s'utilitzi ipv6, s'han d'aplicar les mateixes mesures de seguretat (filtratge en equipament de xarxa, control d'accés, segmentació de xarxa, detecció d'intrusions, etc.) en el trànsit ipv6 que les que s'apliquen al trànsit ipv4.
O	Activar el Firewall o tallafocs
O	Deshabilitar usuaris anònims per a qualsevol servei
O	Deshabilitar comunitats públiques i/o predictibles per SNMP

[2] *En la mesura que sigui possible, evitar l'ús d'RDP no controlat.*

3. PROTECCIÓ DE LA INFORMACIÓ

O	Deshabilitar la funcionalitat de compartir unitats de disc amb propòsits administratius en aquelles màquines que es trobin en entorns crítics o insegurs (com DMZ)
O	Seguir la política del mínim privilegi en els permisos del sistema d'arxius
O	Activar el filtre d'execució d'aplicacions malicioses (Data Execution Prevention, DEP)

4. SISTEMA OPERATIU

O	El sistema operatiu, així com qualsevol aplicació instal·lada en el dispositiu, ha de tenir la corresponent llicència d'ús d'acord amb el fabricant o propietari d'aquest
O	S'ha d'eliminar tot programari innecessari per a la funció que cal desenvolupar
O	Revisar els serveis i inhabilitar tots aquells innecessaris
O	Cal tancar tots els ports innecessaris
R	S'ha de comprovar la instal·lació i actualització adequada de programari antivirus [3]
O	Requerir Ctrl+Alt+Del abans de l'acreditació de l'usuari
O	Deshabilitar la memòria cau de contrasenyes i usuaris
O	Demanar la contrasenya quan es requereixi una elevació de privilegis
R	S'ha d'activar un protector de pantalla que bloquegi el terminal amb contrasenya al cap d'un temps predeterminat segons la ***Normativa de seguretat del lloc de treball [4]***
O	Cal configurar el servei NTP perquè se sincronitzi amb el servidor NTP
O	Desactivar l'execució automàtica
O	Impedir la instal·lació de controladors per part dels usuaris

[3] *Cal disposar d'un antivirus en tots aquells equips en els quals es pugui posar si n'afecta la funcionalitat*
[4] *En qualsevol cas, cal bloquejar l'equip després de 10 minuts d'inactivitat*

5. AUDITORIA

O	Habilitar el registre d'auditoria (Qui fa l'acció, quan, sobre quina informació. Registrar tant èxits com fracassos)

6. ACTUALITZACIONS I PEDAÇOS

O	Cal comprovar l'adequada configuració dels serveis d'actualització automàtica

LLOC DE TREBALL

1. COMPTES D'USUARI

O	Canviar el nom del compte d'administrador
O	Eliminar el compte de convidat
O	Configurar una política de contrasenyes robustes

2. CONTROL D'ACCÉS A LA XARXA

O	Deshabilitar NETBIOS en cas que no el requereixi cap aplicació
O	Activar la signatura de paquets SMB com a client i com a servidor
R	Xifrar les comunicacions del protocol RDP ***[5]***
O	Impedir l'enumeració de recursos compartits i comptes SAM
O	Deshabilitar l'opció que permet apagar el sistema sense iniciar sessió
O	Impedir que es guardin les contrasenyes en el client
O	Impedir la conversió SID a nom d'usuari i viceversa
O	Si no s'utilitza, desactivar ipv6, així com qualsevol altre protocol de xarxa que no sigui utilitzat. En cas que s'utilitzi ipv6, s'han d'aplicar les mateixes mesures de seguretat (filtratge en equipament de xarxa, control d'accés, segmentació de xarxa, detecció d'intrusions, etc.) en el trànsit ipv6 que les que s'apliquen al trànsit ipv4.
O	Activar el Firewall o tallafocs
O	Deshabilitar usuaris anònims per a qualsevol servei
O	Deshabilitar comunitats públiques i/o predictibles per SNMP

[5] *En la mesura que sigui possible, evitar ús d'RDP no controlat.*

3. PROTECCIÓ DE LA INFORMACIÓ

O	Deshabilitar la funcionalitat de compartir les unitats de disc amb propòsits administratius en aquelles màquines que es trobin en entorns crítics o insegurs (com DMZ) ***[6]***
O	Seguir la política del mínim privilegi en els permisos del sistema d'arxius
O	Activar el filtre d'execució d'aplicacions malicioses (Data Execution Prevention, DEP)

[6] *En general, no compartir unitats de disc en la mesura que sigui possible.*

4. SISTEMA OPERATIU

O	El sistema operatiu, així com qualsevol aplicació instal·lada en el dispositiu, ha de tenir la corresponent llicència d'ús d'acord amb el fabricant o propietari d'aquest.
O	Eliminar tot programari innecessari per a la funció que cal desenvolupar
O	Revisar els serveis i inhabilitar tots aquells innecessaris
O	Tancar tots els ports innecessaris
R	Comprovar la instal·lació i actualització adequada de programari antivirus ***[7]***
O	Requerir Ctrl+Alt+Del abans de l'acreditació de l'usuari
O	Deshabilitar la memòria cau de contrasenyes i usuaris
O	Demanar la contrasenya quan es requereixi una elevació de privilegis
R	S'ha d'activar un protector de pantalla que bloquegi el terminal amb contrasenya al cap d'un temps predeterminat segons la **Normativa de seguretat del lloc de treball.** ***[8]***
O	Desactivar l'execució automàtica
O	Impedir la instal·lació de controladors per part dels usuaris

[7] *Cal disposar d'un antivirus en tots aquells equips en els quals es pugui posar si n'afecta la funcionalitat.*
[8] *En qualsevol cas, cal bloquejar l'equip després de 10 minuts d'inactivitat.*

6. ACTUALITZACIONS I PEDAÇOS

O	Cal comprovar l'adequada configuració dels serveis d'actualització automàtica ***[9]***

[9] *En qualsevol cas, s'ha de disposar d'una planificació d'actualització i aplicació de pedaços de sistemes i aplicacions*

ELECTRÒNICA DE XARXA

1. COMPTES D'USUARI

O	Eliminar els comptes i contrasenyes per defecte i/o predictibles
O	Canviar les contrasenyes per defecte i/o predictibles
O	Configurar una política de contrasenyes robustes

2. CONTROL D'ACCÉS A LA XARXA

O	Deshabilitar comunitats públiques i/o predictibles per SNMP

3. SISTEMA OPERATIU

O	El sistema operatiu, així com qualsevol aplicació instal·lada en el dispositiu, ha de tenir la corresponent llicència d'ús d'acord amb el fabricant o propietari d'aquest
O	Revisar els serveis i inhabilitar tots aquells innecessaris
O	Tancar tots els ports innecessaris
O	Deshabilitar la memòria cau de contrasenyes i usuaris

4. ACTUALITZACIONS I PEDAÇOS

O	Comprovar i actualitzar el microprogramari del dispositiu en cas necessari