



CHILQUINTA SERVICIOS S.A.
GERENCIA DE TECNOLOGIA

Identificación:
CS GT SGTI I 04

Fecha Creación:
06/06/2025

Fecha Revisión/Modificación:
NA

Versión:
0

INSTRUCTIVO

HARDENING DE SERVIDORES SERVER HARDENING

Revisado por:
JESUS AYALA
Fecha: 17.06.2025

Aprobado por:
ALFREDO MARTINEZ
Fecha: 17.06.2025

1. OBJETIVO

El propósito de este documento es definir los niveles de aplicabilidad para cada servidor y sistema operativo, estableciendo las opciones de seguridad que se implementarán, con el fin de obtener criterios heterogéneos para cada servidor.

2. ALCANCE

Instructivo aplicable a las áreas de la Subgerencia de Telecomunicaciones y TI administradoras de los dispositivos de red y de seguridad perimetral, que controlan la navegación web y uso de la red corporativa por parte de los colaboradores del Grupo Empresas Chilquinta.

3. DEFINICIONES Y ABREVIACIONES

ESXi: Es un hipervisor desarrollado por VMware para la virtualización de servidores. Permite la creación y gestión de máquinas virtuales en un entorno de servidor físico.

GLPI: Herramienta utilizada para la gestión de cambios, requerimientos, incidencias y problemas

IDRAC: Interfaz de administración remota.

iLO: Interfaz de administración remota.

LVM: Gestor de volúmenes lógicos.

MFA: Autenticación multifactor.

NTP: Protocolo de tiempo de red.

SNMP: Protocolo simple de administración de red.

TLS: Seguridad de la capa de transporte.

4. RESPONSABILIDAD Y AUTORIDAD

CARGO	DESCRIPCIÓN
Jefe de Sistemas e Infraestructura.	(Ejecución de labores/Revisiones y/o aprobaciones) Supervisar cumplimiento.
Ingenieros de Sistemas	Ejecutar tareas asignadas.

5. CONTENIDO

El instructivo de hardening de seguridad establece niveles de seguridad para servidores y sistemas operativos, asegurando homogeneidad en los criterios aplicados. Incluye la instalación de parches y antivirus, desactivación de actualizaciones automáticas, integración al dominio, y deshabilitación de servicios innecesarios. A continuación, se detallan las medidas específicas para servidores **Linux/Unix, Windows y ESXi**.

5.1. Servidores Linux/Unix

ID	Control
1	Acceso a BIOS protegido por contraseña (maq física)
2	Sistema operativo Base con todos los parches de seguridad al día de la instalación
3	Actualización automática deshabilitada
4	Agente GLPI instalado
5	Agente Monitoreo Pandora instalado
6	Inclusión en plataforma de respaldo (si aplica)
7	Habilitación SNMP para acceso desde Monitoreo SNMP v3.
8	Usuario de respaldo "admveeam" creado y con privilegios necesarios para respaldar
9	Archivo de passwords encriptado
10	login directo a root bloqueado
11	Firewall local habilitado. Default Deny policy
12	Cambio de passwords de root por defecto
13	NTP configurado para sincronismo de hora
14	Banner de advertencia configurado
15	Usuario Admchil creado
16	Rotación de logs configurado
17	Configuración de políticas de password de acuerdo con la definición corporativa "ESPECIFICACIÓN TÉCNICA ADMINISTRACIÓN DE CONTRASEÑAS"
18	Interfaz gráfica deshabilitado
19	Particiones independientes al menos para / /PRODUCCION /home /var /tmp /boot /boot/efi swap Siempre sobre LVM
20	ssh escuchando en puerto 2222
21	Auditoría habilitada para: -elevación de privilegios -login fallidos -reboots -Instalación de paquetes o software
22	MFA habilitado (a la puesta en producción)
23	IP v6 deshabilitado
24	Interfaces de red no usadas en estado deshabilitada
25	Interfaz de administración remota (iLO, IDRAC, Xclarity, etc) en red diferente a la productiva (servidores físicos)

26	Interfaz exclusiva para respaldo configurada (solo aplica a servidores físicos)
----	---

5.2. Servidores Windows

ID	Control
1	Acceso a BIOS protegido por contraseña
2	Sistema operativo Base con todos los parches de seguridad a la fecha de instalación
3	Actualización automática deshabilitada
4	Agente antivirus instalado
5	Agente GLPI instalado
6	Agente Monitoreo Pandora instalado
7	Inclusión en plataforma de respaldo (si aplica)
8	Servidor ingresado al dominio
9	Disco exclusivo para Sistema Operativo
10	Disco independiente para aplicativos
11	Firewall habilitado (Default Deny policy)
12	Cambio de password de Administrador local
13	Usuario Administrador local deshabilitado
14	Servicios no necesarios deshabilitados
15	SNMP habilitado para monitoreo por PRTG
16	TLS 1.3
17	IP v6 deshabilitado
18	Interfaces de red no usadas en estado deshabilitada
19	Interfaz de administración remota (iLO, IDRAC, Xclarity, etc) en red diferente a la productiva
20	Interfaz exclusiva para respaldo configurada (solo aplica a servidores físicos)
21	Auditoría habilitada para: -elevación de privilegios -login fallidos -reboots -Instalación de paquetes o software

5.3. Servidores ESXi

ID	Control
1	Acceso a BIOS protegido por contraseña
2	Sistema operativo Base con todos los parches de seguridad a la fecha de instalación
3	Actualización automática deshabilitada
4	Acceso ssh bloqueado
5	Cambio de passwords de root por defecto
6	NTP configurado para sincronismo de hora
7	Servicios no necesarios deshabilitados
8	Incorporación a Vcenter

9	Interfaz de administración remota (iLO, IDRAC, Xclarity, etc) en red diferente a la productiva
10	Interfaz exclusiva para respaldo configurada (solo aplica a servidores físicos)
11	Interfaces de red no usadas en estado deshabilitada
12	IP v6 deshabilitado

6. NORMATIVA VIGENTE

- ISO/IEC 27001: Gestión de Seguridad de la información.
- ISO/IEC 27002: Controles de Seguridad de la información.

7. REFERENCIAS

- CS GT SGTI PO 32 Control de Cambios al Ambiente Operativo

8. ASUNTOS ÉTICOS

Consultas o inquietudes relacionadas con temas éticos pueden ser realizadas al Oficial de cumplimiento (Gerente Legal) al fono: 322452429.

9. HISTORIAL DE REVISIONES Y MODIFICACIONES

Nº Versión	Fecha Vigencia	Comentario	Elaborado por	Revisado por	Aprobado por
0	17.06.2025	Creación documento	del OHS	JAD	AMB



CHILQUINTA SERVICIOS SA.
TECHNOLOGY MANAGEMENT

Identification:
CS GT SGTI I 04

Creation Date:
6/6/2025

Date Reviewed/Modified:
NA

Version:
0

INSTRUCTIVE

SERVER HARDENING
HARDENING DE SERVIDORES

Reviewed by:
JESUS AYALA
Date: 17.06.2025

Approved by:
ALFREDO MARTINEZ
Date: 17.06.2025

1. OBJECTIVE

The purpose of this document is to define the levels of applicability for each server and operating system, establishing the security options to be implemented, in order to obtain heterogeneous criteria for each server.

2. SCOPE

Instructive applicable to the areas of the Subgerencia de Telecomunicaciones y TI that administer network devices and perimeter security, which control web browsing and use of the corporate network by the collaborators of Grupo Empresas Chilquinta.

3. DEFINITIONS AND ABBREVIATIONS

ESXi: A hypervisor developed by VMware for server virtualization. It enables the creation and management of virtual machines within a physical server environment.

GLPI: A tool used for managing changes, requests, incidents, and problems.

IDRAC: Remote administration interface.

iLO: Remote administration interface.

LVM: Logical Volume Manager.

MFA: Multi-factor authentication.

NTP: Network Time Protocol.

SNMP: Simple Network Management Protocol.

TLS: Transport Layer Security.

4. RESPONSIBILITY AND AUTHORITY

POSITION	DESCRIPTION (Execution of tasks/reviews and/or approvals)
Head of Systems and Infrastructure.	Monitor compliance.
Systems Engineers	Run assigned tasks.

5. CONTENT

The security hardening instruction establishes security levels for servers and operating systems, ensuring homogeneity in the criteria applied. Includes installation of patches and anti-virus software, disabling automatic updates, domain integration, and disabling unnecessary services. Specific measures for **Linux/Unix**, **Windows**, and **ESXi** servers are detailed below.

5.1. Linux/Unix Servers

ID	Control

1	Password Protected BIOS Access (physical mag)
2	Base operating system with all security patches on installation day
3	Auto Update Disabled
4	GLPI Agent Installed
5	Pandora Monitoring Agent installed
6	Inclusion in backup platform (if applicable)
7	Enabling SNMP for access from SNMP Monitoring v3.
8	Backup user "admveeam" created and with necessary privileges to back up
9	Encrypted passwords file
10	Direct login to blocked root
11	Local firewall enabled. Default Deny policy
12	Changing default root passwords
13	NTP configured for time synchronization
14	Warning banner configured
15	Admchil User Created
16	Log rotation configured
17	Configuring password policies according to the corporate definition "TECHNICAL SPECIFICATION PASSWORD MANAGEMENT"
18	Graphical interface disabled
19	Separate partitions at least for / /PRODUCTION /home /var /tmp /boot /boot/efi swap Always over LVM
20	ssh listening on port 2222
21	Audit enabled for: - elevation of privileges -login failed -reboots - Package or software installation
22	MFA enabled (on production)
23	IP v6 Disabled
24	Unused network interfaces in disabled state
25	Remote management interface (iLO, IDRAC, Xclarity, etc) on a different network than the productive one (physical servers)
26	Exclusive backup interface configured (applies to physical servers only)

5.2. Windows Servers

ID	Control
1	Password Protected BIOS Access
2.	Base operating system with all security patches as of installation date
3	Auto Update Disabled
4	Anti-virus agent installed
5	GLPI Agent Installed
6	Pandora Monitoring Agent installed
7.	Inclusion in backup platform (if applicable)
8	Server entered into domain
9	Operating System Only Disk
10	Application Stand-alone Disk
11	Firewall Enabled (Default Deny policy)
12	Local Administrator Password Change
13	Local Administrator user disabled
14	Unneeded services disabled
15	SNMP enabled for PRTG monitoring
16	TLS 1.3
17	IP v6 Disabled
18	Unused network interfaces in disabled state
19	Remote management interface (iLO, IDRAC, Xclarity, etc) on a different network than the productive one
20	Exclusive backup interface configured (applies to physical servers only)
21	Audit enabled for: - elevation of privileges -login failed -reboots - Package or software installation

5.3. ESXi Servers

ID	Control
1	Password Protected BIOS Access
2.	Base operating system with all security patches as of installation date
3	Auto Update Disabled
4	Ssh Access Blocked
5	Changing default root passwords
6	NTP configured for time synchronization
7.	Services not required disabled
8	Joining Vcenter
9	Remote management interface (iLO, IDRAC, Xclarity, etc) on a different network than the productive one

10	Exclusive backup interface configured (applies to physical servers only)
11	Unused network interfaces in disabled state
12	IP v6 Disabled

6. EXISTING LEGISLATION

- ISO/IEC 27001: Information Security Management.
- ISO/IEC 27002: Information Security Controls.

7. REFERENCES

- CS GT SGTI PO 32 Control of Changes to the Operating Environment

8. ETHICAL ISSUES

Inquiries or concerns related to ethical issues can be made to the Compliance Officer (Legal Manager) at phone: 322452429.

9. REVISION AND MODIFICATION HISTORY

Version No	Effective Date	Comment	Prepared by	Reviewed By	Approved By
0	17.6.2025	Document Creation	OHS	JAD	WBA