## 1. OBJETIVO

Asegurar la implementación de buenas prácticas de configuración y aseguramiento sobre la plataforma tecnológica TI (Tecnologías de la Información) y TO (Tecnologías de la Operación) de Ocensa minimizando posibles riesgos sobre la misma.

## 2. PREMISAS

- Las configuraciones de seguridad propuestas en las líneas base de configuración y aseguramiento aplican a nivel de sistema operativo en servidores Linux, Windows y Bases de Datos Oracle, en cualquiera de los ambientes (Productivo, Calidad, Desarrollo, DRP) y , se incluyen las líneas base de configuración para los equipos de control de Nivel 2 de Tecnología de la Operación (TO), las cuales establecen los parámetros mínimos de configuración segura y control de acceso para los sistemas y dispositivos que soportan los procesos operativos.
- Todos los componentes de la plataforma tecnológica y los equipos de control de Nivel 2, deberán están asegurados a nivel de sistema operativo y base de datos acorde a lo descrito en el este documento. Igualmente deberán regirse por lo establecido en el documento de PROCEDIMIENTO DE GESTIÓN DE ACCESOS Y USUARIOS – INFRAESTRUCTURA TECNOLÓGICA Y PROCEDIMIENTO ADMINISTRACIÓN DE ACCESOS Y USUARIOS PLATAFORMA CRÍTICA TO V1, respectivamente.
- Es responsabilidad de los administradores de plataforma y base de datos (DBA), garantizar que todos los CIs se encuentren asegurados acorde a las practicas aquí descritas a lo largo del ciclo de vida del CI.
- Anualmente el Profesional Senior Control y Seguridad de la Información y Profesional de Automatización (o quien este designe para tal fin) llevarán a cabo revisiones mediante muestreo de la configuración de la plataforma y equipos, a fin de garantizar que las prácticas de seguridad y configuración se mantengan. En caso de evidenciarse desviaciones se deberá definir e implementar un plan de acción por parte del administrador de la plataforma o DBA según corresponda.

## 3. ACTIVIDADES

**TI**: Cada vez que se realice la instalación de un nuevo componente (Sistema operativo/Base de datos) se deberán aplicar las prácticas de configuración y aseguramiento aquí descritas previo a su operatividad, dejando registro de su aplicación en el correspondiente formato de Check list.

**TO**: Durante la puesta en servicio de nuevos sistemas o equipos, como parte de las actividades de mantenimiento o por incidentes de seguridad o vulnerabilidad detectadas, se deberán aplicar las prácticas de configuración y aseguramiento aquí descritas, dejando registro de su aplicación en el correspondiente formato de Check list.

## 3.1. ASEGURAMIENTO DE SERVIDORES LINUX

| CATEGORÍA | No. | ITEM | DESCRIPCIÓN | VERIFICACIÓN |
|---|---|---|---|---|
| 1. INSTALACIÓN | 1.1 | Módulos de FS inseguros deshabilitados | Deshabilitar módulos de ficheros inseguros: cramfs, freevxfs, jffs2, hfs, hfsplus, squashfs, udf, vfat | `lsmod |
| | 1.2 | Opciones nodev, nosuid, noexec en /dev/shm | Aumenta seguridad en /dev/shm evitando ejecución de binarios no autorizados | `mount |
| | 1.3 | Sticky bit habilitado solo en directorios elegidos | Evita borrado accidental o malicioso de archivos en directorios compartidos | find / -xdev -type d \( -perm -0002 -a ! -perm -1000 \) |
| | 1.4 | Montado automático deshabilitado | Evita que se monten automáticamente dispositivos externos inseguros | externos inseguros<br>systemctl is-enabled autofs |
| | 1.5 | AIDE instalado y chequeo periódico | Herramienta de integridad del sistema para detectar cambios no autorizados | rpm -q aide y `crontab -u root -l |
| | 1.6 | Prelink deshabilitado | Evita modificaciones que interfieran con ASLR y seguridad de memoria | rpm -q prelink |
| 2. ACTUALIZACIONES | 2.1 | Aplicación de parches y actualizaciones | El aseguramiento de la instalación de parches permite reforzar al sistema en contra de la explotación de vulnerabilidades conocidas en los sistemas Unix | Parches y Actualizaciones según plan de parchado |
| | 2.2 | Configuración de repositorios seguros | Verificar GPG check activado | grep ^gpgcheck /etc/yum.conf |
| | 2.3 | Gestión de actualizaciones de seguridad | Proceso documentado de parches | Verificar historial de actualizaciones |
| | 2.4 | Procedimiento de actualización de software | Uso de repositorios locales y controlados para parches y software | yum repolist / dnf repolist |
| | 2.5 | GPGCheck activado | Validar que gpgcheck está habilitado globalmente para integridad de paquetes | grep ^gpgcheck /etc/yum.conf /etc/dnf/dnf.conf |

| CATEGORÍA | No. | ITEM | DESCRIPCIÓN | VERIFICACIÓN |
|---|---|---|---|---|
| | 2.6 | Llaves GPG configuradas | Garantiza que los paquetes provienen de fuentes confiables | rpm -q gpg-pubkey |
| | 2.7 | Suscripciones de Red Hat configuradas | Asegura acceso a repositorios oficiales y soporte | subscription-manager identity |
| | 2.8 | Actualizaciones y parches instalados | Garantiza que el sistema esté actualizado según plan de parchado | yum check-update |
| 3. SERVICIOS | 3.1 | Remover o deshabilitar los comandos "R" | Muchos servicios poseen vulnerabilidades fácilmente explotables | Los comandos rlogind, rshd, rcmd, rexecd, rbootd, rquotad, rstatd, rusersd, rwalld and rexd, deben ser deshabilitados. Utilice SSH para autenticación. |
| | 3.2 | Remover o deshabilitar fingerd | Muchos servicios poseen vulnerabilidades fácilmente explotables | Deshabilitar fingerd |
| | 3.3 | Remover o deshabilitar tftpd | Muchos servicios poseen vulnerabilidades fácilmente explotables | Deshabilitar tftpd |
| | 3.4 | Deshabilitar el servicio discard | Muchos servicios poseen vulnerabilidades fácilmente explotables | Deshabilitar el servicio discar en el archivo inetd.conf |
| | 3.5 | Deshabilitar el servicio Chargen | Muchos servicios poseen vulnerabilidades fácilmente explotables | Deshabilitar el servicio chargen en el archivo inetd.conf |
| | 3.6 SERVICIOS INETD | | | |
| | 3.6.1 | Servicios innecesarios deshabilitados | Evita servicios vulnerables de Inetd como chargen, daytime, discard, echo, time, tftp | Comando de ejecución: systemctl disable <servicio> según corresponda<br>Comando de comprobación: `systemctl list-unit-files --type=service |
| | 3.6.2 | Sincronización NTP o Chrony habilitada | Garantiza sincronización de tiempo para logs y seguridad | Comando de ejecución: NTP o Chrony según corresponda<br>Comando de comprobación: service ntpd status o chronyc tracking<br>Resultado esperado: Servicio habilitado y funcionando |
| | 3.6.3 | Deshabilitar X-Windows por defecto | Evita ejecución de modo gráfico y reduce superficie de ataque | Comando de ejecución: systemctl set-default multi-user.target<br>Comando de comprobación: systemctl get-default<br>Resultado esperado: multi-user.target |

| CATEGORÍA | No. | ITEM | DESCRIPCIÓN | VERIFICACIÓN |
|---|---|---|---|---|
| | 3.6.4 | Servicios clientes inseguros no instalados | Evita rsh, talk, telnet, ypbind | Comando de ejecución: yum -y remove <paquete><br>Comando de comprobación: rpm -q <paquete><br>Resultado esperado: paquete no instalado |
| **4. SCRIPT** | 4.1 | Deshabilitar los scripts innecesarios durante el arranque del sistema. | La ejecución de script en el arranque del sistema podría levantar servicios vulnerables. | Deshabilite los scripts no requeridos. De lo contrario, documente porque se requiere. |
| **5. MINIMIZAR PROGRAMAS "setUID/setGID"** | 5.1. BASTIONADO DE PROCESOS | | | |
| | 5.1.2 | Volcados de núcleo deshabilitados | Evita que se generen core dumps que puedan exponer información sensible | Comando de ejecución: Añadir a /etc/security/limits.conf->hard core 0 y sysctl -w fs.suid_dumpable=0<br>Comando de comprobación: grep "hard core" /etc/security/limits.conf /etc/security/limits.d/* y sysctl fs.suid_dumpable<br>Resultado esperado: fs.suid_dumpable = 0 |
| | 5.1.3 | ASLR habilitado | Evita que se generen core dumps que puedan exponer información sensible | Comando de ejecución: sysctl -w kernel.randomize_va_space=2<br>Comando de comprobación: sysctl kernel.randomize_va_space<br>Resultado esperado: kernel.randomize_va_space = 2 |
| | 5.1.4 | Soporte XD/NX activado | Protege contra ejecución de código en páginas de memoria no ejecutables | Comando de ejecución: Activar en BIOS si necesario (64 bits)<br>Comando de comprobación: `dmesg |
| **6. USER LOGON** | **6. 1. Administración de cuentas** | | | |
| | 6.1.1 | Creación de cuentas | Las cuentas creadas no autorizadas pueden generar accesos no autorizados al sistema. | Todas las cuentas creadas deben tener un responsable y una autorización evidenciable (formatos, correos) |
| | 6.1.2 | Eliminación de cuentas | Las cuentas de usuarios no utilizados deben ser eliminadas | Se debe eliminar la cuenta, directorios /home y archivos del usuario eliminado.<br>-las cuentas no deben tener cron asociados<br>-Use el comando ps para matar cualquier proceso asociado al UID del usuario eliminado. |
| | **6.2. Cuentas Especiales** | | | |
| | 6.2.1 | No deben existir cuentas compartidas | las cuentas compartidas no permiten trazabilidad | todos los usuarios deben tener un único ID de usuario |

| CATEGORÍA | No. | ITEM | DESCRIPCIÓN | VERIFICACIÓN |
|---|---|---|---|---|
| | 6.2.2 | deshabilitar cuentas por defecto y asignar un password seguro | las cuentas por defecto son una vulnerabilidad que puede ser aprovechada por un atacante | cuantas de invitado o por defecto deshabilitadas |
| | **6.3. Cuentas de Root** | | | |
| | 6.3.1 | El password de root solo puede ser conocido por un mínimo de usuarios | No existe trazabilidad en la ejecución de procesos cuando los passwords son compartidos. | La cuenta de usuario root debe ser usada por un único usuario. De lo contrario, se deben documentar las labores por cada usuario que usa la cuenta y deben existir formatos de autorización |
| | 6.3.2 | No usar la cuenta de root para realizar logon interactivo | Se pierde trazabilidad en los procesos | Para trazabilidad si más de un usuario debe usar la cuenta de root, esta debe ser llamada desde la shell del usuario autorizado para uso de la cuenta. Use el comando su |
| | 6.3.3 | Dependiendo del sabor de Unix, el paquete RBAC o sudo debe estar instalado y configurado. El usuario root no debe ser usado en estos sistemas | El paquete RBAC o sudo, permite asignar controles de acceso de acuerdo con los roles del usuario para los sistemas. Por tal razón no se debe usar el usuario root. | Los usuarios de administración deben tener su propia cuenta. El usuario root no debe ser usado. |
| | **6.4. Path** | | | |
| | 6.4.1 | Verificar que los directorios vacíos como ".", no se encuentren el path. | Es posible la ejecución de código malicioso a través de scripts cuando se encuentran cadenas de path vacías | Verifique que los nombres de path sean absolutos y no contengan cadenas vacías. |
| | **6.5. Controles de Sesión de Usuarios** | | | |
| | **6.5.1** | Tiempo de inactividad de una sesión | Si no hay tiempos de log out por inactividad, se expone al sistema a accesos no permitidos | Configure los tiempos de log out por inactividad en 5 minutos |
| | **6.6 PAM– Contraseñas y autenticación** | | | |
| | **6.6.1** | PAM – Requisitos de contraseña | Validar que las políticas de complejidad y bloqueo de cuenta estén habilitadas. No aplica si se usa LDAP | Comando de ejecución: Editar /etc/pam.d/password-auth y /etc/pam.d/system-auth según control Comando de comprobación: grep pam_pwquality.so ... y otros según control Resultado esperado: Configuración presente |
| | **6.6.2** | PAM – Bloqueo por intentos fallidos | Bloqueo de cuenta tras N intentos fallidos. No aplica si LDAP | Comando de ejecución: Editar /etc/pam.d/password-auth y /etc/pam.d/system-auth con pam_faillock.so |

| CATEGORÍA | No. | ITEM | DESCRIPCIÓN | VERIFICACIÓN |
|---|---|---|---|---|
| | | | | Comando de comprobación: grep pam_faillock.so ...<br>Resultado esperado: Configuración presente |
| | **6.6.3** | PAM – Reuso de contraseñas limitado | Impide reutilizar N contraseñas previas. No aplica si LDAP o CyberArk | Comando de ejecución: Editar /etc/pam.d/password-auth y /etc/pam.d/system-auth con remember=10<br>Comando de comprobación: egrep '^password\s+sufficient\s+pam_unix.so' ...<br>Resultado esperado: Configuración presente |
| | **6.6.4** | PAM – Algoritmo hash SHA-512 | Garantiza que contraseñas se guarden usando SHA-512. No aplica si LDAP | Comando de ejecución: Editar /etc/pam.d/password-auth y /etc/pam.d/system-auth<br>Comando de comprobación: egrep '^password\s+sufficient\s+pam_unix.so' ...<br>Resultado esperado: Configuración SHA-512 presente |
| | **6.5 POLÍTICAS DE CONTRASEÑAS** | | | |
| | **6.5.1** | Contraseña caduca en 90 días | Garantiza que usuarios cambien contraseñas periódicamente | Comando de ejecución: Editar /etc/login.defs -> PASS_MAX_DAYS 90<br>Comando de comprobación: grep PASS_MAX_DAYS /etc/login.defs<br>Resultado esperado: PASS_MAX_DAYS 90 |
| | **6.5.2** | Mínimo días entre cambios | Mínimo de 1 día entre cambios. No aplica si CyberArk | Comando de ejecución: Editar /etc/login.defs -> PASS_MIN_DAYS 1<br>Comando de comprobación: grep PASS_MIN_DAYS /etc/login.defs<br>Resultado esperado: PASS_MIN_DAYS 1 |
| | **6.5.3** | Advertencia de caducidad | 30 días antes | Comando de ejecución: Editar /etc/login.defs -> PASS_WARN_AGE 30<br>Comando de comprobación: grep PASS_WARN_AGE /etc/login.defs<br>Resultado esperado: PASS_WARN_AGE 30 |
| | **6.5.4** | Cuentas inactivas | Desactivar tras 120 días. No aplica LDAP/CyberArk | Comando de ejecución: useradd -D -f 120<br>Comando de comprobación: `useradd -D |
| | **6.5.5** | Banners de login local (MOTD) | Mensaje del día (MOTD) visible al iniciar sesión local. Permite informar al usuario sobre políticas de uso, advertencias legales o información corporativa. Ayuda a disuadir accesos no autorizados. | Comando de ejecución: Editar /etc/motd y que contenga Banner Telefónica<br>Comando de comprobación: cat /etc/motd<br>Resultado esperado: Contenido del banner presente |

| CATEGORÍA | No. | ITEM | DESCRIPCIÓN | VERIFICACIÓN |
|---|---|---|---|---|
| | **6.5.6** | Banner de advertencia login local (/etc/issue) | Banner que se muestra antes de la autenticación local. Sirve para advertir sobre el uso autorizado del sistema y las implicaciones legales de accesos no permitidos. | Comando de ejecución: Editar /etc/issue y que contenga Banner Telefónica<br>Comando de comprobación: cat /etc/issue<br>Resultado esperado: Contenido del banner presente |
| | **6.5.7** | Banner de advertencia login remoto (/etc/issue.net) | Banner mostrado en accesos remotos (SSH). Informa y advierte sobre el uso autorizado, reforzando la política de seguridad y registro de accesos remotos. | Comando de ejecución: Editar /etc/issue.net y que contenga Banner Telefónica<br>Comando de comprobación: cat /etc/issue.net<br>Resultado esperado: Contenido del banner presente |
| | **6.5.8** | Permisos en archivos de banners | Asegura que los archivos de banners no puedan ser modificados por usuarios no autorizados. Propietario root y permisos 644 garantizan integridad y confidencialidad de los mensajes de advertencia. | Comando de ejecución: chown root:root /etc/motd /etc/issue /etc/issue.net<br>chmod 644 /etc/motd /etc/issue /etc/issue.net<br>Comando de comprobación: stat /etc/motd, stat /etc/issue, stat /etc/issue.net<br>Resultado esperado: Propietario root y permisos 644 |
| **7. CONTROL DE ACCESO** | **7.1. Protección de archivos** | | | |
| | 7.1.1 | Permisos para archivos claves y directorios | Se debe asegurar la protección de los archivos del sistema para que no sean ejecutados por usuarios diferentes al root | Los siguientes archivos deben ser propiedad del root<br>- Archivos de configuración del sistema<br>- archivos runtime<br>- Archivos de log<br>- Archivos holding del kernel y módulos del kernel<br>- Haga una lista de los directorios que no son propiedad del root que se encuentran fuera del home de cada usuario y verifique sus permisos. (Auditar) |
| | **7.2 permisos del directorio home** | | | |
| | 7.2.1 | Los permisos de los directorios home son exclusivos para cada usuario | Los usuarios con acceso a otros directorios home podrían tener acceso a información relevante | Asegúrese que cada usuario solo puede tener permisos de escritura en su directorio home y no en otros directorios de otros usuarios.<br>Los directorios home podrían tener permisos con un valor de 700. |
| | **7.3. Cron** | | | |

| CATEGORÍA | No. | ITEM | DESCRIPCIÓN | VERIFICACIÓN |
|---|---|---|---|---|
| | 7.3.1 | Permisos y propiedad de crontab | Asegurar crontab para que sea propiedad del root y que solo sea usado con sus privilegios. | Se podría colocar el valor de los permisos de crontab para el usuario root en 600<br>El propietario del crontab podría ser el root |
| | 7.3.2 | Restricciones en crontab y permisos | Evita ejecución no autorizada de tareas programadas | Comando de ejecución: chown root:root y chmod og-rwx /etc/crontab /etc/cron.* /etc/at.* según corresponda<br>Comando de comprobación: stat /etc/crontab y directorios<br>Resultado esperado: permisos correctos, propietario root |
| | **7.4. TCP** | | | |
| | 7.4.1 | Habilite el uso de SSH v2 | El uso de SSH no garantiza la seguridad completamente en la comunicación cliente servidor. | Tenga en cuenta las siguientes consideraciones en el uso de SSH<br>Utilice SSH v2<br>Deshabilite otras opciones de autenticacion<br><br>En el archivo /etc/ssh/sshd_config, (o similar dependiendo del sistema operativo) se debe quitar el comentario a la línea Protocol 2. La línea Protocol 2,1 y la línea Protocol 1, deben quedar con comentarios |
| | 7.4.2 | Habilite la autenticación segura para el uso de samba. | El uso de samba para compartir archivos con sistemas Microsoft, puede ser inseguro. | Verifique que la versión de samba sea la 3.0.2 o superior<br><br>Si existe un dominio Microsoft, configure samba para que la autenticacion sea a través del directorio activo<br><br>So se encuentra en un dominio de micdrosoft, habilite los niveles de seguridad de usuario. |
| | 7.4.4 | No ejecute servicios FTP | Los servicios FTP son vulnerables a diferentes ataques. | Deshabilite el uso de FTP, se debe validar si el servidor lo requiere. |
| | 7.4.5 | Habilite el uso de logs del sistema para registrar los accesos | Al habilitar los syslog, se tiene trazabilidad de los eventos de seguridad en una estación Unix | Habilite el uso de los syslog del sistema operativo |

| CATEGORÍA | No. | ITEM | DESCRIPCIÓN | VERIFICACIÓN |
|---|---|---|---|---|
| | 7.4.6 | Telnet | Los servicios Telnet son vulnerables a diferentes ataques. | Deshabilite el uso de Telnet |
| | 7.4.7 | Configuración segura de SSH | Limita acceso y asegura trazabilidad de sesiones | Comando de ejecución: Ediciones en /etc/ssh/sshd_config según control (Protocol 2, MaxAuthTries, X11Forwarding no, etc.)<br>Comando de comprobación: grep de cada parámetro<br>Resultado esperado: Valores configurados según control |
| | **7.7 CONTROL DE ACCESO OBLIGATORIO** | | | |
| | 7.7.1 | SELinux activado y funcionando | SELinux implementa un control de acceso obligatorio que limita lo que los usuarios y procesos pueden hacer. Nota: Este control no es necesario si se usa PIM | Comando de ejecución: En /etc/selinux/config establecer SELINUX=enforcing<br>Comando de comprobación: sestatus<br>Resultado esperado: SELinux status: enabled … Current mode: enforcing |
| | 7.7.2 | Política SELinux configurada | Verificar que la política SELinux está configurada correctamente. Nota: No necesario si se usa PIM | Comando de ejecución: Editar /etc/selinux/config: SELINUXTYPE=targeted<br>Comando de comprobación: grep SELINUXTYPE=targeted /etc/selinux/config<br>Resultado esperado: SELINUXTYPE=targeted |
| | 7.7.3 | SETroubleshoot no instalado | SETroubleshoot puede exponer vulnerabilidades | Comando de ejecución: yum -y remove setroubleshoot<br>Comando de comprobación: rpm -q setroubleshoot<br>Resultado esperado: package setroubleshoot is not installed |
| | 7.7.4 | mcstrans no instalado | El servicio MCS (mcstrans) no es necesario y podría representar riesgo | Comando de ejecución: yum -y remove mcstrans<br>Comando de comprobación: rpm -q mcstrans<br>Resultado esperado: package mcstrans is not installed |
| | 7.7.5 | Número de demonios limitados | No debe existir un número ilimitado de demonios corriendo | Comando de ejecución: Investigue cualquier daemon no configurado encontrado durante la acción de auditoría.<br>Comando de comprobación: `ps -eZ |

| CATEGORÍA | No. | ITEM | DESCRIPCIÓN | VERIFICACIÓN |
|---|---|---|---|---|
| **8. CONTROL DE SOFTWARE** | 8.1 | Integración de IdM | Integración de la autenticación con LDAP, Kerberos u otros servicios de directorio | Comprobar que cada servicio use la integración de IdM según corresponda |
| **9. CONFIGURACIÓN RED** | **9.1 CONFIGURACIÓN RED** | | | |
| | 9.1.1 | Reenvío IP deshabilitado | Impide que el sistema funcione como router no autorizado, evitando que paquetes IP sean reenviados a otras redes. Reduce riesgo de sniffing o ataques de enrutamiento internos. | Comando de ejecución: sysctl -w net.ipv4.ip_forward=0; sysctl -w net.ipv4.route.flush=1<br>Comando de comprobación: sysctl net.ipv4.ip_forward<br>Resultado esperado: net.ipv4.ip_forward = 0 |
| | 9.1.2 | Redirección de paquetes deshabilitada | Evita que el host envíe redirecciones de paquetes a otros sistemas. Protege contra ataques de MITM (Man-in-the-Middle) y redirecciones maliciosas dentro de la red. | Comando de ejecución: sysctl -w net.ipv4.conf.all.send_redirects=0; sysctl -w net.ipv4.conf.default.send_redirects=0; sysctl -w net.ipv4.route.flush=1<br>Comando de comprobación: sysctl net.ipv4.conf.all.send_redirects; sysctl net.ipv4.conf.default.send_redirects<br>Resultado esperado: 0 |
| | 9.1.3 | Paquetes de origen enrutados no aceptados | Deshabilitar rutas de origen previene que se acepten paquetes con rutas maliciosas. Esto protege contra intentos de manipulación de tráfico y ataques de spoofing de red. | Comando de ejecución: sysctl -w net.ipv4.conf.all.accept_source_route=0; sysctl -w net.ipv4.conf.default.accept_source_route=0; sysctl -w net.ipv4.route.flush=1<br>Comando de comprobación: sysctl net.ipv4.conf.all.accept_source_route; sysctl net.ipv4.conf.default.accept_source_route<br>Resultado esperado: 0 |
| **10. INICIO SEGURO** | 10.1 | Permisos en bootloader | Asegura que los archivos de configuración del bootloader sean propiedad de root y no sean modificables por otros usuarios. | Comando de ejecución: chown root:root /boot/grub2/grub.cfg /boot/grub2/user.cfg && chmod og-rwx /boot/grub2/grub.cfg /boot/grub2/user.cfg<br>Comando de comprobación: stat /boot/grub2/grub.cfg /boot/grub2/user.cfg<br>Resultado esperado: Propietario root, permisos 600 o similares. |
| | 10.2 | Contraseña de bootloader | Protege el arranque del sistema mediante contraseña en GRUB. | Comando de ejecución: grub2-setpassword<br>Comando de comprobación: grep "^GRUB2_PASSWORD" /boot/grub2/user.cfg |

| CATEGORÍA | No. | ITEM | DESCRIPCIÓN | VERIFICACIÓN |
|---|---|---|---|---|
| | | | | Resultado esperado: Contraseña configurada. |
| | 10.3 | Autenticación para modo usuario único | Garantiza que solo usuarios autorizados puedan acceder al modo de usuario único. | Comando de ejecución: Editar /usr/lib/systemd/system/rescue.service y /usr/lib/systemd/system/emergency.service fijando ExecStart=-/bin/sh -c "/sbin/sulogin; /usr/bin/systemctl --fail --no-block default" Comando de comprobación: grep /sbin/sulogin /usr/lib/systemd/system/rescue.service /usr/lib/systemd/system/emergency.service Resultado esperado: ExecStart configurado correctamente. |
| | 10.4 | SELinux habilitado en bootloader | Evita deshabilitar SELinux durante el arranque. | Comando de ejecución: Eliminar parámetros selinux=0 y enforcing=0 en /etc/default/grub y ejecutar grub2-mkconfig -o /boot/grub2/grub.cfg Comando de comprobación: grep "^\s*linux" /boot/grub2/grub.cfg Resultado esperado: SELinux habilitado (no aparece selinux=0 o enforcing=0). |
| **11. AUDITORIA** | 11.1 | Tamaño log de auditoría | Configura tamaño máximo de logs de auditoría. | Comando de ejecución: Editar /etc/audit/auditd.conf -> max_log_file=<MB> Comando de comprobación: grep max_log_file /etc/audit/auditd.conf |
| | 11.2 | Servicio auditd habilitado | Garantiza que el servicio de auditoría esté activo. | Comando de ejecución: systemctl enable auditd Comando de comprobación: systemctl is-enabled auditd |
| | 11.3 | Auditoría de procesos previos a auditd | Asegura que procesos críticos sean auditados desde el arranque. | Comando de ejecución: Añadir audit=1 en GRUB_CMDLINE_LINUX y ejecutar grub2-mkconfig -o /boot/grub2/grub.cfg Comando de comprobación: grep "^\s*linux" /boot/grub2/grub.cfg |
| | 11.4 | Eventos que modifican fecha y hora | Registra cambios de tiempo del sistema. | Comando de ejecución: Añadir reglas audit a /etc/audit/rules.d/audit.rules para adjtimex, settimeofday, clock_settime, /etc/localtime y reiniciar auditd Comando de comprobación: `auditctl -l |

| CATEGORÍA | No. | ITEM | DESCRIPCIÓN | VERIFICACIÓN |
|---|---|---|---|---|
| | 11.5 | Eventos que modifican /user/group | Registra cambios en archivos críticos de usuarios y grupos. | Comando de ejecución: Añadir reglas audit para /etc/passwd, /etc/shadow, /etc/group, /etc/gshadow, /etc/security/opasswd y reiniciar auditd<br>Comando de comprobación: `auditctl -l |
| | 11.6 | Eventos que modifican entorno de red | Registra cambios en configuración de red y hosts. | Comando de ejecución: Añadir reglas audit para /etc/hosts, /etc/issue*, /etc/sysconfig/network* y reiniciar auditd<br>Comando de comprobación: `auditctl -l |
| | 11.7 | Eventos que modifican MAC | Auditoría de cambios en SELinux y control de acceso obligatorio. | Comando de ejecución: Añadir reglas audit para /etc/selinux/ y /usr/share/selinux/<br>Comando de comprobación: `auditctl -l |
| | 11.8 | Configuración de syslog | Comprueba que rsyslog esté funcionando y configurado correctamente, garantizando que los logs del sistema se generen, roten y almacenen de forma centralizada o local según la política. | systemctl status rsyslog |

## 3.2. ASEGURAMIENTO DE SERVIDORES WINDOWS

| CATEGORÍA | No. | ITEM | DESCRIPCIÓN | VERIFICACIÓN |
|---|---|---|---|---|
| 1 ACTUALIZACIONES | 1.1 | Aplicación de parches y actualizaciones | El aseguramiento de la instalación de parches permite reforzar al sistema en contra de la explotación de vulnerabilidades conocidas en los sistemas Windows | Instalación de parches y actualizaciones del sistema con fecha no anterior a 6 meses desde la fecha actual. |
| | 1.2 | Validación automática de actualizaciones críticas | Garantiza que el servidor tenga habilitado Windows Update para recibir parches críticos y de seguridad automáticamente. | Revisar Settings → Windows Update y política de grupo. |
| | 1.3 | Configuración de repositorio de actualizaciones corporativo (WSUS / SCCM) | El sistema operativo debe obtener actualizaciones desde un repositorio corporativo controlado (ej. WSUS), garantizando consistencia en la distribución de parches y evitando que el equipo consulte directamente servidores externos de Microsoft. | Verificar que la configuración de Windows Update apunte al repositorio autorizado mediante GPO o parámetros locales. |
| | 1.4 | Habilitar Windows NTP Client | Garantiza que el sistema sincronice la hora mediante el cliente NTP corporativo, | gpedit.msc → Computer Configuration → Administrative |

| CATEGORÍA | No. | ITEM | DESCRIPCIÓN | VERIFICACIÓN |
|---|---|---|---|---|
| | | | minimizando problemas de autenticación, Kerberos y registros. Control CIS 5.3.12.1.1 | Templates → System → Windows Time Service → Time Providers → Enable Windows NTP Client = Enabled |
| **2. ACCOUNTS** | 2.1 | Configurar: Renombrar la cuenta de administrador local | La cuenta de administrador local integrada es un nombre de cuenta conocido al que se dirigirán los atacantes. Se recomienda elegir otro nombre para esta cuenta y evitar nombres que denoten cuentas de acceso elevado o administrativas. Asegúrese de cambiar también la descripción predeterminada para el administrador local (a través de la consola de Administración de equipos). | Se renombra la cuenta |
| | 2.2 | Configurar: Renombrar la cuenta de invitado (Guest) y deshabilitar | La cuenta de invitado local incorporada es otro nombre muy conocido para los atacantes. Se recomienda cambiar el nombre de esta cuenta a algo que no indique su propósito. | Se renombra la cuenta |
| | 2.3 | limitar el uso de la cuenta local de contraseñas en blanco al inicio de sesión de la consola solamente' a 'Activado' | Esta configuración de directiva determina si las cuentas locales que no están protegidas con contraseña se pueden usar para iniciar sesión desde ubicaciones que no sean la consola física de la computadora. Si habilita esta configuración de directiva, las cuentas locales que tengan contraseñas en blanco no podrán iniciar sesión en la red desde computadoras cliente remotas. Tales cuentas solo podrán iniciar sesión en el teclado de la computadora. | Habilitado |
| | 2.4 | Revisión de cuentas con rol SYSADMIN | Solo administradores autorizados deben tener el rol SYSADMIN. | SELECT name FROM sys.server_principals WHERE is_sysadmin = 1; |
| | 2.5 | Deshabilitar el inicio automático del último usuario | Impide que Windows inicie sesión automáticamente después de reinicios, evitando accesos no autorizados. | GPO → Sign-in last interactive user automatically after system restart = Disabled. |
| | 2.6 | Bloquear el uso de cuentas Microsoft | Evita que usuarios agreguen cuentas Microsoft personales en dispositivos corporativos. | GPO → Accounts: Block Microsoft Accounts = Enabled |
| | 2.7 | Permitir solo administradores para formatear medios extraíbles | Reduce fuga accidental de datos y uso indebido de USB. | GPO → Devices: Allowed to format and eject removable media = Administrators |
| | 2.8 | Bloquear instalación de drivers de impresoras | Evita instalación de drivers no autorizados que puedan incluir vulnerabilidades. | GPO → Devices: Prevent users from installing printer drivers = Enabled |

| CATEGORÍA | No. | ITEM | DESCRIPCIÓN | VERIFICACIÓN |
|---|---|---|---|---|
| | 2.9 | Deshabilitar Offer Remote Assistance | Reduce riesgo de acceso remoto no controlado. | Validar que Remote Assistance está deshabilitado |
| | 2.10 | Permitir que cuentas Microsoft sean opcionales. | Evita que Windows obligue a usar cuentas Microsoft para ciertas funciones o apps. CIS 5.4.1.1 | gpedit.msc → Computer Configuration → Administrative Templates → Windows Components → App Runtime → Allow Microsoft accounts to be optional = Enabled |
| **3. MICROSOFT NETWORK SERVER** | 3.1 | Establecer 'Servidor de red Microsoft: cantidad de tiempo inactivo requerido antes de suspender la sesión' a '15 minutos o menos | Esta configuración de directiva le permite especificar la cantidad de tiempo de inactividad continuo que debe pasar en una sesión de SMB antes de que la sesión se suspenda debido a la inactividad. Los administradores pueden usar esta configuración de directiva para controlar cuándo una computadora suspende una sesión de SMB inactiva. Si la actividad del cliente se reanuda, la sesión se restablece automáticamente. Un valor de 0 desconectará una sesión inactiva lo más rápido posible. El valor máximo es 99999, que es 208 días; en efecto, este valor desactiva la configuración. | Habilitado |
| | 3.2 | Establecer 'Servidor de red Microsoft: firmar digitalmente las comunicaciones (siempre)' a 'Habilitado' | Esta configuración de directiva determina si se requiere el servicio SMB del lado del servidor para realizar la firma de paquetes SMB. Habilite esta configuración de directiva en un entorno mixto para evitar que los clientes indirectos utilicen la estación de trabajo como servidor de red. | Habilitado |
| | 3.3 | Establecer 'Servidor de red Microsoft: firmar digitalmente las comunicaciones (si el cliente está de acuerdo)' a 'Habilitado' | Esta configuración de directiva determina si el servicio SMB del lado del servidor puede firmar paquetes SMB si un cliente que intenta establecer una conexión así lo solicita. Si el cliente no envía una solicitud de firma, se permitirá una conexión sin una firma si el servidor de red de Microsoft: la configuración de las comunicaciones de firma digital (siempre) no está habilitada. Nota Habilite esta configuración de directiva en clientes SMB en su red para que sean completamente efectivos para la firma de paquetes con todos los clientes y servidores de su entorno. | Habilitado |

| CATEGORÍA | No. | ITEM | DESCRIPCIÓN | VERIFICACIÓN |
|---|---|---|---|---|
| 4. REGLAS DE ENTRADA | 4.1 | Se debe configurar registro (SNMP) (Simple Network Management Protocol ) Tipo de protocolo UDP | Con esta configuración garantizamos configurar los servidores en la plataforma de monitoreo SolarWinds | Configurado |
| | 4.2 | Se debe configurar registro (WMI) (Windows Management Instrumentation) Tipo de protocolo TCP puerto ALL | Con esta configuración garantizamos configurar los servidores en la plataforma de monitoreo SolarWinds | Configurado |
| | 4.3 | Restricción de IPs con acceso al SQL | Solo IPs autorizadas deben tener acceso al motor de SQL. | Revisión de reglas del firewall. |
| 5. SOFTWARE | **5.1 SOFTWARE REQUERIDOS** | | | |
| | 5.2 | Instalación de Antivirus | Confirma que el antivirus corporativo está presente y operativo, garantizando protección básica contra malware según las políticas de seguridad. | Instalado |
| | 5.3 | Instalación de Vulnerability Protection * Esto aplica si Ocensa cuenta con el servicio activo de TrendMicro | Valida que el módulo esté instalado para asegurar detección y mitigación de vulnerabilidades en tiempo real. TrendMicro | Instalado |
| | 5.4 | Deshabilitar de la tarjeta de red el protocolo IPV6 | Al deshabilitar IPv6 el equipo buscará direcciones IPv4 inmediatamente, eliminando la búsqueda de direcciones IPv6 que generan pequeños retrasos en la red. | Deshabilitado |
| | 5.5 | Servicios configurados para reinicio automático | Los servicios de SQL Server deben reiniciarse automáticamente ante fallos. | sc qc MSSQLSERVER. |
| | 5.6 | Configuración restrictiva de Windows Installer (basado en CIS 5.4.11.1) | Restringe el uso de Windows Installer para impedir la instalación no autorizada de paquetes MSI por parte de usuarios estándar. Reduce riesgo de ejecución de software malicioso o no aprobado y garantiza que solo administradores puedan realizar instalaciones mediante políticas. | Validar GPO: Computer Configuration → Administrative Templates → Windows Components → Windows Installer. Confirmar que “Windows Installer: Disable MSI” o “Prohibit user installs” esté configurado según política corporativa (Recommended: Enabled / Always). |
| 6. SQL SERVER | 6.1 | Políticas de contraseñas SQL habilitadas | Todas las cuentas SQL deben cumplir políticas de complejidad, longitud y expiración. | SELECT name, is_policy_checked, is_expiration_checked FROM sys.sql_logins; |
| | 6.2 | Cifrado SSL/TLS para conexiones | Las conexiones cliente-servidor deben emplear cifrado TLS. | SELECT encrypt_option FROM sys.dm_exec_connections; |

| CATEGORÍA | No. | ITEM | DESCRIPCIÓN | VERIFICACIÓN |
|---|---|---|---|---|
| | 6.3 | Auditoría de intentos fallidos | Deben registrarse intentos fallidos de login. | SELECT login_name, COUNT(*) FROM sys.dm_exec_sessions WHERE status='failed'; |
| | 6.4 | Revisión de roles asignados | Validar que los roles de base de datos sean correctos y mínimos. | Consulta JOIN de roles y miembros. |
| | 6.5 | Copias de seguridad cifradas | Las copias deben contar con cifrado activo. | SELECT name, is_encrypted FROM msdb.backupset; |
| | 6.6 | Revisión de parches de SQL Server | Además del sistema operativo, SQL Server debe contar con parches críticos de seguridad actualizados. | Validación vía SSMS → Installed Updates. |
| | 6.7 | Bloqueo de cuentas SQL por defecto no requeridas | Las cuentas internas y por defecto de SQL deben estar bloqueadas o deshabilitadas para reducir superficie de ataque. | SELECT name, is_disabled FROM sys.sql_logins; verificar que cuentas sin uso = is_disabled = 1. |
| **7. POLÍTICAS DE CONTRASEÑAS** | 7.1 | Longitud mínima | La política OCENSA establece que las contraseñas deben tener mínimo 12 caracteres. | Configurado: 12 → OK |
| | 7.2 | Complejidad habilitada | La contraseña debe incluir como mínimo un dígito, una mayúscula, una minúscula y un carácter especial. No deben usarse nombres comunes o relacionados a la organización. | Parámetro definido → OK |
| | 7.3 | Carácter especial obligatorio | Debe existir al menos un carácter especial dentro de la contraseña. | Configurado → OK |
| | 7.4 | Historial de contraseñas | Deben recordarse 24 contraseñas previas para evitar reutilización. | Configurado: 24 → OK |
| | 7.5 | Frecuencia de cambio (Lifetime) | OCENSA exige cambio cada 60 días. | Configurado: 180 días → KO |
| | 7.6 | Umbral de bloqueo | La cuenta debe bloquearse después de 4 intentos fallidos. | Configurado: 4 → OK |
| | 7.7 | Tiempo de bloqueo | OCENSA exige 5 días, equivalente a 432.000 segundos. | Configurado: 432.000 segundos → OK |
| | 7.8 | Días mínimos entre cambios | Establecido en 0 días, permitiendo cambio inmediato cuando sea necesario. | Configurado → OK |
| | 7.9 | Advertencia de expiración | Se debe advertir al usuario 7 días antes de la expiración. | Configurado: 7 días → OK |
| **8. ANTIVIRUS** | 8.1 | Instalación de solución antivirus corporativa | Garantiza la detección y mitigación de malware conocido y comportamientos maliciosos. | Verificar que el antivirus esté instalado y activo: systemctl status <servicio> o interfaz del agente. |
| | 8.2 | Motor de antivirus actualizado | Reduce el riesgo de infecciones al asegurar firmas y motores actualizados. | Validar fecha de la última actualización de firmas. No debe superar 24 horas. |

| CATEGORÍA | No. | ITEM | DESCRIPCIÓN | VERIFICACIÓN |
|---|---|---|---|---|
| | 8.3 | Análisis programados (Full Scan / Quick Scan) | Permite detectar amenazas latentes o no identificadas en tiempo real. | Revisar políticas del antivirus: evidencia de escaneos semanales completos y diarios rápidos. Validar módulo de Real-Time Protection activo desde consola local o consola central. |
| 9. CONTROL PANEL | 9.1 | Prevent enabling lock screen slide show | Restringe que los usuarios habiliten presentación de imágenes en la pantalla de bloqueo, reduciendo exposición visual innecesaria según lineamiento CIS. | gpedit.msc → Computer Configuration → Administrative Templates → Control Panel → Personalization → Prevent enabling lock screen slide show = Enabled. |
| | 9.2 | Turn off toast notifications on the lock screen | Evita que se muestren notificaciones en la pantalla de bloqueo, mitigando fuga accidental de información sensible. | gpedit.msc → User Configuration → Administrative Templates → Start Menu and Taskbar → Notifications → Turn off toast notifications on the lock screen = Enabled. |
| | 9.3 | Turn off Help Experience Improvement Program | Bloquea el envío de telemetría del sistema hacia Microsoft relacionada con la experiencia del usuario, reduciendo la divulgación de información no controlada. | gpedit.msc → User Configuration → Administrative Templates → System → Internet Communication Management → Internet Communication Settings → Turn off Help Experience Improvement Program = Enabled. |
| | 9.4 | Allow users to enable online speech recognition services | Deshabilita que usuarios activen el reconocimiento de voz en línea, evitando captación remota de audio o envío a servicios externos. | gpedit.msc → Computer Configuration → Administrative Templates → Control Panel → Regional and Language Options → Allow users to enable online speech recognition services = Disabled. |
| | 9.5 | Allow Online Tips | Evita que Windows descargue y muestre tips o recomendaciones desde Internet, reduciendo telemetría no necesaria. | gpedit.msc → Computer Configuration → Administrative Templates → Control Panel → Allow Online Tips = Disabled. |
| | 9.6 | Disable Control Panel and PC Settings | Restringe el acceso al Panel de Control y Configuración para usuarios no administrativos, reduciendo cambios no autorizados en el sistema. | gpedit.msc → User Configuration → Administrative Templates → Control Panel → Prohibit access to Control Panel and PC settings = Enabled. |

| CATEGORÍA | No. | ITEM | DESCRIPCIÓN | VERIFICACIÓN |
|---|---|---|---|---|
| | 9.7 | Hide specified Control Panel ítems | Permite ocultar secciones críticas del Panel de Control, evitando modificaciones de red, sistema o cuentas por usuarios estándar. | gpedit.msc → User Configuration → Administrative Templates → Control Panel → Hide specified Control Panel items = Enabled. Configurar lista de elementos. |
| | 9.8 | Show only specified Control Panel ítems | Limita estrictamente qué elementos del Panel de Control pueden visualizarse, endureciendo la superficie de configuración. | gpedit.msc → User Configuration → Administrative Templates → Control Panel → Show only specified Control Panel items = Enabled. Configurar lista de elementos permitidos. |
| | 9.9 | Disable access to Control Panel personalization settings | Evita que usuarios modifiquen temas, fondos, colores y configuraciones visuales que puedan revelar información o generar inconsistencias corporativas. | gpedit.msc → User Configuration → Administrative Templates → Control Panel → Personalization → Prevent changing theme = Enabled; Prevent changing lock screen or login image = Enabled. |
| | 9.10 | Prevent changing advanced power settings | Restringe a los usuarios modificar configuraciones de energía que puedan impactar disponibilidad, suspensión o reinicio no autorizado. | gpedit.msc → User Configuration → Administrative Templates → Control Panel → Power Options → Prohibit access to advanced power settings = Enabled |
| | 9.11 | Disable language installation by users | Impide que usuarios agreguen nuevos paquetes de idioma, lo cual también detiene la descarga de contenido desde internet. | gpedit.msc → Computer Configuration → Administrative Templates → Control Panel → Regional and Language Options → Restrict language features = Enabled |
| | 9.12 | Disable location settings modification | Evita que usuarios alteren configuraciones de ubicación, reduciendo fuga de metadatos a servicios geográficos. | gpedit.msc → Computer Configuration → Administrative Templates → Control Panel → Regional and Language Options → Allow users to change location = Disabled |
| | 9.13 | Prevent enabling suggested content | Evita que Windows descargue contenido sugerido desde Microsoft (tips, apps sugeridas, contenido online). | gpedit.msc → Computer Configuration → Administrative Templates → Windows Components → Cloud Content → Turn off Microsoft consumer features = Enabled |
| | 9.14 | Disable Sync Settings | Evita que usuarios sin control repliquen configuraciones a la nube Microsoft, | gpedit.msc → Computer Configuration → Administrative |

| CATEGORÍA | No. | ITEM | DESCRIPCIÓN | VERIFICACIÓN |
|---|---|---|---|---|
| | | | reduciendo fuga de telemetría y metadatos personales/corporativos. | Templates → Windows Components → Sync your settings → Do not sync = Enabled |
| | 9.15 | Deshabilitar comunicación interactiva con Microsoft Support Diagnostic Tool (MSDT) | Evita que MSDT envíe información interactiva o telemetría sensible a Microsoft durante diagnósticos. Recomendación CIS 5.3.10.1.1 | gpedit.msc → Computer Configuration → Administrative Templates → System → Troubleshooting and Diagnostics → Microsoft Support Diagnostic Tool → Turn on MSDT interactive communication with support provider = Disabled |
| | 9.16 | Deshabilitar Windows PerfTrack | Evita que Windows recopile y envíe datos de rendimiento hacia Microsoft (telemetría). Recomendación CIS 5.3.10.2.1. | gpedit.msc → Computer Configuration → Administrative Templates → System → Troubleshooting and Diagnostics → Windows Performance PerfTrack → Enable/Disable PerfTrack = Disabled |
| | 9.17 | Deshabilitar Advertising ID | Bloquea el uso de Advertising ID para personalización y telemetría, reduciendo exposición de datos del usuario. CIS 5.3.11.1 | gpedit.msc → Computer Configuration → Administrative Templates → System → User Profiles → Turn off the advertising ID = Enabled |
| **10. AUDITORÍA DE SEGURIDAD** | 10.1 | Política de Auditoría – Validación de Credenciales | Registra cada intento de validación de credenciales, permitiendo detectar accesos fallidos o intentos sospechosos de autenticación. | Verificar que Audit Credential Validation esté configurado en Success y Failure. |
| | 10.2 | Auditoría de Administración de Cuentas | Permite rastrear cualquier creación, eliminación o modificación de cuentas o grupos, facilitando la trazabilidad de cambios administrativos. | Verificar que Account Management esté habilitado en Success y Failure. |
| | 10.3 | Auditoría de Eventos de Inicio de Sesión | Registra cada intento de inicio y cierre de sesión, incluyendo eventos especiales, para identificar accesos no autorizados o anómalos. | Verificar que Audit Logon, Audit Logoff y Audit Special Logon estén habilitados. |
| | 10.4 | Auditoría de Cambios de Políticas | Detecta cuando se modifica una política de seguridad o configuración crítica del sistema. | Verificar que Policy Change esté configurado en Success. |
| | 10.5 | Auditoría de Uso de Privilegios Sensibles | Registra cuando un usuario utiliza privilegios avanzados (ej. SeDebugPrivilege), permitiendo identificar usos indebidos de privilegios. | Verificar que Audit Sensitive Privilege Use esté habilitado en Success y Failure. |

| CATEGORÍA | No. | ITEM | DESCRIPCIÓN | VERIFICACIÓN |
|---|---|---|---|---|
| | 10.6 | Auditoría de Integridad del Sistema | Supervisa componentes clave del sistema operativo para detectar alteraciones, fallos o manipulación de archivos críticos y servicios. | Verificar que Audit System Integrity esté habilitado en Success y Failure. |
| | 10.7 | Auditoría de Creación de Procesos | Registra cada proceso iniciado por el sistema o usuarios, mejorando la trazabilidad para análisis forense y detección de actividad maliciosa. | Verificar que Audit Process Creation esté habilitado en Success. |
| **11. SEGURIDAD DE RED (MSS – Legacy)** | 11.1 | Deshabilitar IP Source Routing | Evita que un atacante manipule rutas IP para desviar tráfico o realizar suplantación. | GPO → MSS: DisableIPSourceRouting = Enabled (Highest Protection) |
| | 11.2 | Bloquear ICMP Redirects | Impide que se modifiquen rutas mediante mensajes ICMP, reduciendo el riesgo de ataques de 'hombre en el medio' (MITM). | GPO → MSS: EnableICMPRedirect = Disabled |
| | 11.3 | Bloquear solicitudes de liberación de nombre NetBIOS | Mitiga intentos de spoofing del servicio de nombres NetBIOS. | GPO → MSS: NoNameReleaseOnDemand = Enabled |
| | 11.4 | Deshabilitar LLMNR / Multicast Name Resolution | Reduce riesgo de ataques de suplantación o envenenamiento en la red. | Validar política en GPO para LLMNR = Deshabilitado |
| | 11.5 | Deshabilitar servicios de descubrimiento de red (LLTDIO) | Evita la exposición innecesaria de información sobre la topología de red. | Revisar GPO → Servicios de descubrimiento = Off |
| | 11.6 | Deshabilitar servicios Peer-to-Peer | Reduce servicios no necesarios que abren puertos adicionales. | Validar servicios P2P deshabilitados |
| | 11.7 | Prohibir creación de puentes de red (Network Bridge) | Evita configuraciones no autorizadas que afecten segmentación. | Revisar GPO → Bridge = Prohibido |
| | 11.8 | Requerir privilegios para cambiar perfil de red | Evita modificar perfiles de red sin autorización. | Validar GPO → Network Location |
| | 11.9 | Deshabilitar Windows Connect Now | Evita asistentes de conexión inalámbrica no corporativos. | Evita asistentes de conexión inalámbrica no corporativos. |
| | 11.10 | Autenticación en RPC Endpoint Mapper | Mejora la seguridad en conexiones remotas RPC. | Validar autenticación RPC habilitada |
| **12. REMOTE DESKTOP** | 12.1 | Allow log on through Remote Desktop Services | Define qué usuarios están autorizados a iniciar sesión vía RDP. Según CIS, solo deben permitirse Administrators y Remote Desktop Users. | GPO → Computer Configuration → Windows Settings → Security Settings → Local Policies → User Rights Assignment → Allow log on through Remote Desktop Services |
| | 12.2 | Deny log on through Remote Desktop Services | Impide que ciertos grupos (ej. Guests) puedan iniciar sesión por RDP. | GPO → Computer Configuration → Windows Settings → Security Settings → Local Policies → User Rights Assignment → Deny log on through Remote Desktop Services |

| CATEGORÍA | No. | ITEM | DESCRIPCIÓN | VERIFICACIÓN |
|---|---|---|---|---|
| | 12.3 | Do not allow passwords to be saved | Evita guardar contraseñas de RDP en el cliente, mitigando robo de credenciales. | GPO → Computer Configuration → Administrative Templates → Windows Components → Remote Desktop Services → Remote Desktop Connection Client → Do not allow passwords to be saved = Enabled |
| **13. POWERSHELL & EXECUTION CONTROL (OBLIGATORIO GLOBAL)** | 13.1 | Deshabilitar PowerShell Script Block Logging | CIS exige que, si Script Block Logging no es requerido por el SOC, se mantenga deshabilitado para reducir telemetría y evitar exposición de comandos internos. | gpedit.msc → Computer Configuration → Administrative Templates → Windows Components → Windows PowerShell → Turn on PowerShell Script Block Logging = Disabled |
| | 13.2 | Deshabilitar PowerShell Transcription | Evita que PowerShell registre transcripciones completas de sesiones, lo cual expone información sensible si no se usa un repositorio seguro centralizado. Debe estar deshabilitado si no es obligatorio por políticas SOC. | gpedit.msc → Computer Configuration → Administrative Templates → Windows Components → Windows PowerShell → Turn on PowerShell Transcription = Disabled |
| **ONEDRIVE** | 14.1 | Deshabilitar OneDrive para almacenamiento de archivos | CIS recomienda impedir el uso de OneDrive cuando la organización no utiliza este servicio, evitando sincronización no autorizada, fuga de datos o almacenamiento externo no controlado. Basado en CIS 5.4.7.1. | gpedit.msc → Computer Configuration → Administrative Templates → Windows Components → OneDrive → Prevent the usage of OneDrive for file storage = Enabled |

## 3.3. ASEGURAMIENTO DE BASE DE DATOS ORACLE

| CATEGORÍA | No. | ITEM | DESCRIPCIÓN | VERIFICACION |
|---|---|---|---|---|
| **1. CONFIGURACIÓN ESPECIFICA DEL SISTEMA OPERATIVO Y MOTOR DE BASE DE DATOS** | 1.1 | Agrupación de usuarios | A nivel de sistema operativo (archivo /etc/groups), todos los usuarios de la base de datos deben tener asociado un mismo grupo. | En Linux (cat /etc/groups) y en Windows (en la consola) verificar que todos los usuarios de la base de datos estén incluidos dentro de un grupo.<br><br>Documentar la evidencia que verifique el procedimiento realizado. |

| CATEGORÍA | No. | ITEM | DESCRIPCIÓN | VERIFICACION |
|---|---|---|---|---|
| | 1.2 | Perfiles del sistema operativo | Los perfiles de usuario a nivel de sistema operativo deben asegurar que únicamente personal autorizado pueda ejecutar las herramientas de la base de datos. | En Unix (ls-la>permisos.txt) evaluar los usuarios dueños de la base de datos y las restricciones de acceso.<br><br>Documentar la evidencia que verifique el procedimiento realizado. |
| | 1.3 | Versión y Parches | Asegurar que la más reciente versión de Oracle es la utilizada y que los más recientes parches de Oracle Metalink han sido aplicados.<br><br>Utilizar software desactualizado o sin parches adecuados pondrá a la base de datos Oracle y al sistema host en un riesgo innecesario y atenta a las mejores prácticas de seguridad. | Revisar el sitio web oficial de Oracle para asegurar que el uso de las versiones más recientes: http://www.oracle.com/technology/software/index.html y de los parches de seguridad más recientes: http://metalink.oracle.com/metalink/plsql/ml2_gui.startup<br><br>Verificar opatch lsinventory -detail y documentar la evidencia que verifique el procedimiento realizado. |
| | 1.4 | tkprof | Restricción de permisos del sistema. La utilidad tkprof debe ser restringida en los ambientes de producción; es una herramienta productiva para un atacante para encontrar vulnerabilidades en la base de datos que se ejecuta. Si tkprof se mantiene en el sistema de producción, debe protegerse con permisos apropiados. | Establezca permisos de archivo de 0750 o menos en sistemas Linux. En sistemas Windows, restrinja el acceso a esos usuarios que lo requieren y verifique que "Everyone" no tiene acceso.<br><br>Documentar la evidencia que verifique que en el directorio $ORACLE_HOME/bin se ha removido o cambiado los permisos para la utilidad tkprof. |
| | 1.5 | Cuentas por defecto de las aplicaciones y base de datos Oracle | Las contraseñas por defecto de todas las cuentas estándar de las aplicaciones y la base de datos Oracle deben ser cambiadas y todas las cuentas que no se utilizan deben ser deshabilitadas. | Documentar la evidencia que verifique que se han cambiado las contraseñas por defecto. En la tabla DBA_users se compara el campo "password" contra el campo "password" de la tabla usuarios por defecto en papel (campo Hash). Se evalúa la posesión de estas claves (si aplica) y se modifican las contraseñas encontradas. |

| CATEGORÍA | No. | ITEM | DESCRIPCIÓN | VERIFICACION |
|---|---|---|---|---|
| | 1.6 | Archivos en $ORACLE_HOME/bin | Verificar y establecer la propiedad. Los archivos oracle y lsnrctl en $ORACLE_HOME/bin deben tener permisos RWX para el dueño, R-X para el grupo y ninguno para otros. Para conexiones locales modificar el TNSNAME ORA o hacer el usuario parte del grupo DBA y/o OINSTALL. | Cambie la propiedad de los binarios a la cuenta apropiada. Documente la evidencia que soporte el procedimiento de revisión de este cambio con |
| | 1.7 | init.ora | Configuración de los parámetros de control de archivos. Los permisos deben ser restringidos solo al propietario de la base de datos Oracle y al grupo dba. | Verificación:<br>chmod 640 control_file chown oracleuser.oraclegroup control_file<br>grep -i control_files init.ora<br>ls -al <result> select name from V$controlfile;<br><br>Documentar la evidencia que verifique el procedimiento realizado. |
| | 1.8 | Archivos en el directorio $ORACLE_HOME/ network/admin | Verificar y establecer permisos. Los permisos para todos los archivos deben ser restringido al propietario de la base de datos Oracle y al grupo dba. Si una aplicación que requiere acceso a la base de datos también se instala en el servidor de la base de datos, el usuario con el que la aplicación se ejecuta debe tener acceso de lectura a los archivos tnsnames.ora y sqlnet.ora. | Verificación:<br>chmod 644 $ORACLE/network/admin/* chown oracleuser.oraclegroup \<br>$ORACLE_HOME/network/admin/*<br>ls -al $ORACLE_HOME/network/admin/*<br><br>Documentar la evidencia que verifique el procedimiento realizado. |
| | 1.9 | sqlnet.ora | Verificar y establecer permisos de lectura para todos los usuarios.<br>El sqlnet.ora contiene los archivos de configuración para la comunicación entre el usuario y el servidor incluyendo el nivel de encripción requerida. Si se utiliza encripción la llave se almacena en el parámetro | Evaluación:<br>chmod 644 sqlnet.ora chown oracleuser.oraclegroup sqlnet.ora<br><br>Documentar la evidencia que verifique la configuración con:<br>ls –al sqlnet.ora |

| CATEGORÍA | No. | ITEM | DESCRIPCIÓN | VERIFICACION |
|---|---|---|---|---|
| | | | SQLNET.CRYPTO_SEED en el archivo sqlnet.ora. En estos escenarios, el acceso a este archivo debe ser limitado. | |
| | 1.10 | Auditoría habilitada | Verificar que Oracle tenga la auditoría habilitada a nivel de la instancia. La auditoría permite registrar eventos críticos, accesos y acciones administrativas que afectan la seguridad de la base de datos. | SHOW PARAMETER audit_trail;<br>Resultado esperado: DB, EXTENDED o XML. |
| | 1.11 | Cuentas por defecto bloqueadas | Todas las cuentas estándar de Oracle como SCOTT, HR, OUTLN, OLBM, etc., deben estar bloqueadas o vencer sus contraseñas. Estas cuentas son ampliamente conocidas y representan un riesgo de acceso no autorizado. | SELECT USERNAME, ACCOUNT_STATUS FROM DBA_USERS;<br>Validar que cuentas por defecto estén en LOCKED. |
| | 1.12 | Políticas de contraseñas seguras | Se debe configurar un perfil de contraseñas que incluya tiempos de vida, complejidad, historial, intentos fallidos y bloqueo. Esto protege contra ataques de fuerza bruta y uso de claves débiles. | SELECT * FROM DBA_PROFILES WHERE RESOURCE_NAME = 'PASSWORD_LIFE_TIME';<br>Resultado recomendado: 45 - 90 días. |
| | 1.13 | Cifrado TDE | Verificar que Oracle Transparent Data Encryption (TDE) esté habilitado para datos sensibles. Protege información almacenada en disco ante accesos no autorizados o pérdida del medio. | SELECT * FROM V$ENCRYPTION_WALLET;<br>Resultado esperado: OPEN |

| CATEGORÍA | No. | ITEM | DESCRIPCIÓN | VERIFICACION |
|---|---|---|---|---|
| | 1.2. UNIX | | | COMANDO / CONSULTA |
| | 1.2.1 | Uso de sudo para administración Oracle | Validar que solo usuarios autorizados (root/oracle) pueden ejecutar sudo para tareas administrativas. Reduce riesgo de escalación indebida. | cat /etc/sudoers \| grep oracle |
| | 1.2.2 | Permisos del archivo passwd | Validar permisos del archivo /etc/passwd aseguran integridad de usuarios Oracle. | ls -l /etc/passwd \| grep oracle |
| | 1.2.3 | Permisos del archivo shadow | Validar seguridad del archivo /etc/shadow evitando lectura no autorizada de hashes de contraseñas. | ls -l /etc/shadow \| grep oracle |
| | 1.2.4 | Servicios activos Oracle | Verificar que solo servicios Oracle necesarios estén activos; evitar procesos maliciosos o innecesarios. | systemctl list-units --type=service --state=running \| grep oracle |
| | 1.2.5 | Auditoría de archivos Oracle | Validar reglas de auditoría activas relacionadas con Oracle. | auditctl -l \| grep oracle |
| | 1.2.6 | Firewall para conexiones Oracle | Validar que el firewall solo permite conexiones a Oracle desde hosts autorizados. | iptables -L \| grep 1521 |
| | 1.2.7 | Seguridad SSH | Validar que root no pueda autenticarse por SSH. Reduce riesgo de acceso directo privilegiado. | cat /etc/ssh/sshd_config \| grep 'PermitRootLogin' |
| | 1.2.8 | Revisión de parches del servidor Oracle | Validar que no existan actualizaciones críticas pendientes y revisar actividad en directorios Oracle. | ./OPatch/opatch lsinventory |
| | 1.2.9 | Permisos en ORACLE_HOME | Validar permisos correctos para protección de binarios y archivos fundamentales. | ls -ld $ORACLE_HOME |
| | 1.2.10 | Límites de recursos (ulimit) | Validar parámetros para estabilidad del motor Oracle (nofile, nproc). | ulimit -a \| grep oracle |
| | 1.2.11 | Revisión de logs del sistema | Validar que no existan errores críticos relacionados con Oracle en logs del sistema. | cat /var/log/syslog \| grep oracle |

| CATEGORÍA | No. | ITEM | DESCRIPCIÓN | VERIFICACION |
|---|---|---|---|---|
| | 1.2.12 | Montajes seguros (nosuid/nodev/noexec) | Validar que sistemas de archivos Oracle usen parámetros seguros para evitar ejecución o escalación no autorizada. | mount \| grep 'nosuid' \| grep oracle |
| **2. CONFIGURACIÓN DE PARAMETROS ORACLE** | 2.1 | DICTIONARY_ACCESSIBITY | Esta implementado el acceso protegido al diccionario de datos y solamente por el personal adecuado y autorizado | Documentar la evidencia donde el parámetro se 07_DICTIONARY_ACCESSIBITY se encuentre en FALSE. Si este parámetro está en falso y se tiene que tener acceso a objetos en el esquema SYS, entonces deben concederle privilegios de objeto explícitos:<br><br>• SELECT_CATALOG_ROLE,<br>• EXECUTE_CATALOG_ROLE y<br>• DELETE_CATALOG_ROLE |
| | 2.2 | remote_os_roles | remote_os_roles= FALSE<br><br>Se debe prevenir el spoofing de conexión. | Documentar la evidencia que verifique el parámetro en FALSE. |
| | 2.3 | Registro de intentos de inicio fallidos | Validar que Oracle registre intentos fallidos de autenticación para detectar ataques de fuerza bruta, accesos indebidos o errores de autenticación. | SELECT * FROM DBA_AUDIT_SESSION WHERE RETURN_CODE != 0; |
| | 2.4 | Tiempo de inactividad (IDLE_TIME) | Establecer límites de tiempo para desconectar sesiones inactivas y evitar abuso de sesiones abandonadas. | SELECT * FROM DBA_PROFILES WHERE RESOURCE_NAME = 'IDLE_TIME';<br>Recomendado: 5 - 30 min |
| | 2.5 | Seguridad en conexiones externas | Validar que el parámetro para uso de passwordfile esté configurado como EXCLUSIVE o NONE. | SHOW PARAMETER remote_login_passwordfile; |
| **3. TABLAS, VISTAS, PROXY** | 3.1 | Tablas | Prevenir el acceso a PERFSTAT.STATS$SQLTEXT<br><br>Revocar el acceso a todos los usuarios, hasta donde sea posible. SQLTEXT almacena los textos completos de sentencias SQL que se han ejecutado y pueden contener información | Documentar la evidencia que verifique la configuración:<br>SELECT GRANTEE, PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME=" STATS$SQLTEXT"; |

| CATEGORÍA | No. | ITEM | DESCRIPCIÓN | VERIFICACION |
|---|---|---|---|---|
| | | | sensible.<br><br>REVOKE ALL ON PERFSTAT.STATS$SQLTEXT | |
| | 3.2 | Vistas | Prevenir el acceso a cualquier vista DBA.<br><br>Las vistas DBS generan información sobre todos los objetos de sistema y deben ser accesibles solamente para los administradores.<br><br>REVOKE ALL ON DBA_<TABLENAME> FROM <USER> | Documentar la evidencia que verifique la configuración:<br>SELECT GRANTEE, PRIVILEGE, TABLE_NAME FROM DBA_TAB_PRIVS WHERE TABLE_NAME LIKE(„DBA_$%"); |
| | 3.3 | Autenticación Proxy | Limitar el esquema de privilegios de usuario solo a CREATE SESSION.<br><br>La cuenta proxy solo debe tener la habilidad de conectarse a la base de datos. No se debe otorgar ningún otro privilegio a esta cuenta.<br><br>REVOKE ALL ON <USER>;<br>GRANT CREATE SESSION TO <USER> | Documentar la evidencia que verifique la configuración:<br>SELECT * FROM DBA_ROLE_PRIVS WHERE GRANTEE="<PROXY ACCOUNT>";<br>SELECT * FROM DBA_TAB_PRIVS WHERE GRANTEE="<PROXY ACCOUNT>";<br>SELECT * FROM DBA_SYS_PRIVS WHERE GRANTEE="<PROXY ACCOUNT>"; |
| | 3.4 | Revisión de permisos SYSDBA/SYSOPER | Validar que únicamente personal autorizado tenga privilegios SYSDBA o SYSOPER, evitando abuso de control total del motor. | SELECT * FROM V$PWFILE_USERS; |
| | 3.5 | Revisión de permisos innecesarios | Revisar que no existan cuentas con privilegios excesivos o no requeridos que permitan elevación de privilegios. | SELECT * FROM DBA_SYS_PRIVS WHERE GRANTEE NOT IN ('SYS','SYSTEM'); |
| | 3.6 | Reglas de acceso basadas en roles (RBAC) | Verificar asignación apropiada de roles seguros y minimizar acceso innecesario. | SELECT * FROM DBA_ROLE_PRIVS WHERE GRANTED_ROLE = 'SECURE_ROLE'; |

| CATEGORÍA | No. | ITEM | DESCRIPCIÓN | VERIFICACION |
|---|---|---|---|---|
| **4. LOGS DE AUDITORIA Y REGISTRO DE EVENTOS** | 4.1 | Logs de auditoria | Verificar que la base de datos debe tiene habilitada la auditoria. | Documentar la evidencia donde se verifica que se encuentra habilitada la auditoria (show parameter audit_trail. El resultado debe ser DB o OS o XML) |
| | 4.2 | Eventos de auditoria | Eventos de auditoria (alter database, alter table, alter user, update table, delete table, drop table, truncate table, insert table, grant any privilege, db_links, drop user,execute) | Documentar la evidencia donde verifique los eventos de auditoria (select substr(user_name,1,12) usuario, privilege, success,failure from dba_priv_audit_opts order by user_name, privilege; ) |
| | 4.3 | audit sys | AUDIT_SYS_OPERATIONS =TRUE<br><br>La auditoría de los usuarios autenticados como SYSDBA o SYSOPER provee un vistazo de los usuarios más privilegiados. Es importante que el usuario de la base de datos no tenga acceso a los directorios del sistema donde se graban los registros de auditoría. Se asegura esto al establecer este parámetro en TRUE. | Documentar la evidencia que verifique el parámetro AUDIT_SYS_OPERATIONS=TRUE y el parámetro AUDIT_FILE_DEST hacia el directorio de registro designado.<br>Windows: El valor por defecto es el archivo de registro del Event Viewer<br>Unix: El valor por defecto es $ORACLE_HOME/rdbms/audit |
| | 4.4 | Auditoría de cambios de objetos sensibles | Verificar auditoría en tablas críticas como salarios, empleados o información financiera. | SELECT * FROM DBA_OBJ_AUDIT_OPTS WHERE OBJECT_NAME IN ('EMPLOYEES','SALARY'); |
| | 4.5 | Auditoría personalizada | Validar políticas de auditoría definidas por el cliente. | SELECT * FROM DBA_AUDIT_POLICIES; |
| | 4.6 | Auditoría estructural avanzada | Auditoría activa para cambios de sistema, creación/eliminación de objetos, privilegios, políticas y autenticación. | SELECT * FROM DBA_AUDIT_TRAIL WHERE ACTION_NAME IN (...); |
| **5. RESPALDOS Y DIRECTORIOS** | 5.1 | Validación de rutas de control files y respaldos | Verificar que las rutas de respaldo estén correctamente definidas y distribuidas para alta disponibilidad. | SHOW PARAMETER control_files; |

| CATEGORÍA | No. | ITEM | DESCRIPCIÓN | VERIFICACION |
|---|---|---|---|---|
| | 5.2 | Permisos en directorios críticos | Validación de permisos en directorios como DATA_PUMP_DIR, ORACLE_HOME, ORACLE_BASE y OPATCH. | SELECT DIRECTORY_NAME, DIRECTORY_PATH FROM DBA_DIRECTORIES;<br><br>SELECT GRANTEE, PRIVILEGE FROM ALL_TAB_PRIVS WHERE TABLE_NAME = '<DIRECTORIO>'; |
| | 5.3 | Estado de tablespaces | Verificar que todos los tablespaces se encuentren en estado ONLINE. | SELECT TABLESPACE_NAME, STATUS FROM DBA_TABLESPACES; |

## 3.4. ASEGURAMIENTO EQUIPOS NIVEL 2 – TO

Cada área debe asegurar el hardening teniendo en cuenta línea base de equipos de control en nivel 2 para ser aplicados en los equipos bajo su custodia

| TIPO DE ACTIVO | MARCA | ESTACION |
|---|---|---|
| **PLC** | Allan Bradley/Modicom | CUS, POR, MR, VS, CC, CV |
| **HMI** | Allan Bradley | POR,MR,VS,CC,CV |
| **RTU** | Stardom | Todas las estaciones y válvulas |
| **COMPUTADOR DE FLUJO** | OMNI | CUS, POR, VAS, CV |
| **DCS** | Foxboro FCP/ABB | Todas las estaciones |
| **MASTER STATION** | RotorK | CUS, POR, MR, LB, VS, CC, CV |

| Nº | Categoría | Actividad / Paso | Descripción | Aplicabilidad | Verificación |
|---|---|---|---|---|---|
| **1** | Control de Acceso | Deshabilitar autologin | Evita el ingreso automático sin autenticación | PLC/HMI/RTU/CF/DCS/MS | El equipo no permite el inicio de sesión automático (autologin), solicita usuario y contraseña |
| **2** | Control de Acceso | Deshabilitar funciones de acceso | Evita que accedan al programa o recursos | PLC/HMI/RTU/CF/DCS/MS | Las funciones o servicios de acceso no requeridos se encuentran deshabilitados |
| **3** | Control de Acceso | Usuario y contraseña nombrados | Protege el acceso a los sistemas de control y garantizar la trazabilidad de las acciones realizadas | PLC/HMI/RTU/CF/DCS/MS | Cada usuario que accede cuenta con credenciales únicas. |
| **4** | Gestión de Cuentas y Autenticación | Desactivar cuentas por defecto o innecesarias | Elimina accesos inseguros por cuentas predefinidas | PLC/HMI/RTU/CF/DCS/MS | - Confirmar que todas las cuentas están asociadas a un responsable.<br>- No se utilizan cuentas genéricas o por defecto |
| **5** | Gestión de Cuentas y Autenticación | Aplicar principio de mínimo privilegio | Limita permisos al mínimo necesario para cada usuario | PLC/HMI/RTU/CF/DCS/MS | Los usuarios y servicios cuentan únicamente con los privilegios mínimos necesarios Administrador, Operador, Visualización |
| **6** | Monitoreo y Registro | Activar registros y logs operativos | Permite trazabilidad y diagnóstico ante incidentes | PLC/HMI/RTU/CF/DCS/MS | Verificar que se tiene habilitada la función de registro o logging para eventos como conexiones, cambios de configuración, accesos de usuario |
| **7** | Seguridad de red | Deshabilitar puertos y servicios no utilizados | Cerrar o inhabilitar todos los puertos de red, interfaces físicas y servicios de software que no sean necesarios | PLC/HMI/RTU/CF/DCS/MS | -Verificar que todos los puertos de comunicación y servicios que no sean estrictamente necesarios para su operación y mantenimiento se encuentren deshabilitados o bloqueados |

| Nº | Categoría | Actividad / Paso | Descripción | Aplicabilidad | Verificación |
|---|---|---|---|---|---|
| **8** | Seguridad de red | Segmentación de red | Dividir la red en subredes o zonas lógicas para controlar, aislar y proteger el tráfico entre diferentes dispositivos | PLC/HMI/RTU/CF/DCS/MS | Verificar configuraciones o reglas de firewall local, listas de control de acceso (ACL) o segmentación de red para restringir el tráfico solo a las direcciones o puertos permitidos |
| **9** | Protección del Software | Control de cambios sobre el software de gestión | Registrar cualquier modificación al código de control o configuración | PLC/DCS | Todo cambio realizado en la lógica, configuración o firmware se encuentra documentado y aprobado |
| **10** | Backup y Recuperación | Backups automáticos | Proteger las copias de respaldo de datos, configuraciones y programas | PLC/DCS | Validar existencia de respaldos actualizados y política de restauración. |
| **11** | Control Físico de Acceso | Gabinetes con cerradura o candado | Impedir que personal no autorizado (como visitantes, operadores sin entrenamiento, técnicos externos) toque, desconecte o modifique equipos sensibles. | PLC/RTU/CF/DCS/MS | Los gabinetes, racks o tableros se encuentran físicamente protegidos mediante cerradura, candado o sistema de control de acceso. |

Se anexa documento Check list de Hardening Nivel 2 - Controladores_OCSA

## 4. CONTROL DE ACTUALIZACIONES

| VERSIÓN | FECHA | DESCRIPCIÓN |
|---|---|---|
| 0 | 31/12/2019 | Emisión del documento |
| 1 | 26/12/2025 | Modificación numeral 1. Objetivo Adición Línea Base TO<br>Modificación numeral 2. Premisas. Se incluye alcances y responsables de TI y TO.<br>Adición y modificación a los aspectos de a las líneas base de configuración TI:<br>Inclusión numeral 3.4 ASEGURAMIENTO EQUIPOS NIVEL 2 – TO<br>Cambio de código, anterior GSE-PRD-005 |

EVELIN JIMENEZ MONROY
Profesional Senior Control y Seguridad de la Información
**Revisó**

OLFER ALEXIS LEON BARBOSA
Jefe Ciberseguridad y Ciberdefensa
**Revisó**

VICTOR ALEJANDRO PAYARES MARZOLA
Jefe Infraestructura Y Servicios Digitales
**Aprobó**