



**POLÍTICAS
IMPLEMENTADAS EN
SISTEMAS OPERATIVOS Y
BASE DE DATOS.
CNCO.IT.C007**

Vigencia: 01/07/2024
Versión: 7.0



	CNCO.IT.C007 - POLÍTICAS IMPLEMENTADAS EN SISTEMAS OPERATIVOS Y BASE DE DATOS	
	Código	
	Tema	Correlativo
	SI-CRP-PR	024
		Página
		2 de 5

Tabla de contenidos

1.	Objetivo	3
2.	Alcance	3
3.	Definiciones y abreviaturas	3
4.	Descripción del procedimiento	3
4.1.	Extracción de información	3
4.2.	Metodología de Análisis	4
4.3.	Consideraciones a tener en cuenta por plataforma	4
4.4.	Armado de Cédula/Documentación	5
4.5.	Remediaciones	5
4.6.	Cierre del Control	5
4.7.	Evidencia.....	5

	CNCO.IT.C007 - POLÍTICAS IMPLEMENTADAS EN SISTEMAS OPERATIVOS Y BASE DE DATOS	
	Código	Página
	Tema	Correlativo
	SI-CRP-PR	024
		3 de 5

1. Objetivo

Definir los pasos necesarios para la efectuar la revisión de estándares técnicos contemplados en el control de Seguridad **CNCO.IT.C007**.

2. Alcance

Se encuentran alcanzadas las plataformas en Scope del Testing Anual del grupo CENCOSUD, según se indica en los listados de Servidores DC (Inventario Servidores DC) y Servidores POS (Inventario Servidores POS) publicados en SharePoint vigente al momento de ejecutar el control.

El listado excluye las aplicaciones que no están asignadas a ningún bloque, las declaradas como EECC y aquellas aplicaciones cuyas soluciones están fuera de Cencosud (SAAS e IAAS).

3. Definiciones y abreviaturas

- EECC: Estado Contable
- SO: Sistema Operativo
- BD: Base de Datos
- DC: Controlador de dominio
- SAAS: Software as a Service – Software como Servicio
- IAAS: Infrastructure as a Service – Infraestructura como Servicio
- SAT: Software de seguridad (Caja de credenciales) que permite realizar la administración de usuarios especiales que por su criticidad deben tener un trato especial en su utilización.
- CyberArk: Software de seguridad (caja de credenciales) que permite realizar la administración de usuarios especiales que por su criticidad deben tener un trato especial en su utilización.

4. Descripción del procedimiento

4.1. Extracción de información


Se realiza la descarga de los Inventarios de Servidores publicados por las áreas de IT Tech y IT País, el cual incluye todas las aplicaciones que son administradas por dichas áreas para analizar. Este documento es el universo del control, el cual incluye la infraestructura a analizar y que conforma el universo del control:

- El universo del control es un consolidado conformado por los servidores DC y los servidores POS de los distintos países.
- Del Universo, se excluyen los servidores de Sistema Operativo 4690, la arquitectura de la APL074 – Active Directory, que son DC y los balanceadores (ej. F5).
- De los Servidores alcanzados, se deben realizar tres universos conformados de la siguiente manera:
 - BD: Se filtran por el campo “Base de Datos” y se excluyen todos los que son “N/A”. Luego se procede a quitar los servidores duplicados.
 - SO: Se filtran por el campo “Base de Datos” y solo se consideran los “N/A”. Luego se procede a quitar los servidores duplicados.
 - SO con BD: El universo es el mismo que describe en BD.

Para cada universo, se realiza una muestra aleatoria según el detalle debajo:

- Universo de BD: la muestra es de 40 casos.
- Universo de SO: la muestra es de 20 casos.
- Universo de SO de BD: la muestra es de 40 casos.

CORPORATIVO	Marco Normativo de Seguridad de la Información	INTERNO
-------------	--	---------

	CNCO.IT.C007 - POLÍTICAS IMPLEMENTADAS EN SISTEMAS OPERATIVOS Y BASE DE DATOS	
	Código	Página
	Tema	Correlativo
	SI-CRP-PR	024
		4 de 5

En ocasión que, alguno de los casos que fueron seleccionados en las muestras, se encuentre fuera de servicio por estar siniestrado, por tienda cerrada, decomisado, o por cualquier otro motivo técnico que impida realizar la revisión, se reemplazará con otro utilizando el universo correspondiente a la muestra del servidor a reemplazar.

Una vez que se tenga el listado consolidado de servidores, se ejecutan los scripts de seguridad y/o comandos solicitados al área de IT Tech o IT País, según corresponda, para cada uno de ellos. En los casos que no exista un script o no sea posible su ejecución por cualquier motivo, la extracción de la información se debe realizar de manera manual según lo determinado en el estándar técnico de seguridad.

4.2. Metodología de Análisis

El análisis de cada una de las plataformas es realizado en concordancia con los distintos estándares de Seguridad definidos y aprobados por CENCOSUD.

Para cada parámetro analizado se generan los siguientes resultados:

- **NO APLICA:** No aplica la revisión del parámetro ya que se encuentra excluido o justificado (ej. por versión, imposibilidad técnica, etc.). La justificación queda declarada dentro de la cédula.
- **CUMPLE:** El parámetro se encuentra acorde al estándar
- **NO CUMPLE:** El parámetro no se encuentra acorde al estándar, o no se pudo constatar por falta de evidencia.

Dentro del cumplimiento de los parámetros de contraseña asociados a usuarios, se toman las siguientes consideraciones, que son evaluadas durante la ejecución del CNCO.IT.C006 (Procedimiento de Certificación de Usuarios IT.):

- **Validación de usuarios “Nominales”:**
 - Aquellos con permisos de administración deben estar incluidos dentro de las nóminas de CyberSecurity o IT Tech/IT País.
- **Validación de usuarios “No Nominales”:**
 - Aquellos con privilegios de administración deben estar ensobrados (SAT y/o CyberArk) o exceptuados según los anexos correspondientes al momento de la ejecución del control.

Para cada servidor analizado se generan los siguientes resultados:

- **OK:** La totalidad de los parámetros se encuentran en “**CUMPLE**” y/o “**NO APLICA**”.
- **NO OK:** El servidor posee uno o más parámetros con resultado “**NO CUMPLE**”. Por lo tanto, el servidor se enviará a remediar, informando en el campo “Comentario”, los parámetros/usuarios/cuentas que se encuentran incorrectos con la configuración actual.


4.3. Consideraciones a tener en cuenta por plataforma

Existe la posibilidad de que la configuración aplicada sea más restrictiva que la sugerida por los Estándares de Seguridad.

GENERAL:

- Si la duración “**Máxima de la Contraseña**” es menor a lo requerido, el valor configurado es correcto.
- Si la duración “**Mínima de la Contraseña**” es mayor a lo requerido, el valor configurado es correcto.
- Si la longitud “**Mínima de la contraseña**” es mayor a lo requerido, el valor configurado es correcto.
- Si el “**Historial de la contraseña**” es mayor a lo requerido, el valor configurado es correcto.

CORPORATIVO	Marco Normativo de Seguridad de la Información	INTERNO
-------------	--	---------

	CNCO.IT.C007 - POLÍTICAS IMPLEMENTADAS EN SISTEMAS OPERATIVOS Y BASE DE DATOS	
	Código	Página
	Tema	Correlativo
	SI-CRP-PR	024
		5 de 5

Para UNIX se considera lo siguiente:

- En las distribuciones Solaris, AIX y SUSE, si el script “parse_history_all.sh” se encuentra configurado para su ejecución en “crontab”, el punto se considerará como correcto.

Pueden existir otras excepciones, las mismas se encontrarán declaradas dentro de la cédula.

4.4. Armado de Cédula/Documentación

La evaluación de cada parámetro y servidor analizado se vuelca en un documento de análisis, confeccionado por el área de IT Governance & Compliance, llamado cédula.

La confección de la cédula cuenta con 2 instancias:

- Inicial: Resultado de la primera revisión de parámetros realizada por el equipo de IT Governance & Compliance.
- Final: Resultado final de la revisión de parámetros realizada por el equipo de IT Governance & Compliance, considerando las remediaciones realizadas como resultado de la cédula inicial.

4.5. Remediaciones

Realizado el análisis de los parámetros y su alineación con los estándares, en la cédula inicial, se envían los hallazgos a los equipos de IT Tech y/o IT País, según corresponda, para su remediación y/o justificación, para realizar las siguientes tareas:

- Remediación de los puntos observados
- Envío de la evidencia que los puntos remediados. En caso de no poder remediarse por limitaciones técnicas, se envían las justificaciones y evidencias correspondientes.

Si corresponde se actualizan los estándares que apliquen, avalados por CyberSecurity.

4.6. Cierre del Control

El control se cierra con la confección de la cédula final, con el resultado del análisis de todos los parámetros de plataformas y bases de datos alcanzados en la muestra, el correspondiente informe del control y las remediaciones y/o adecuaciones que correspondiere.

4.7. Evidencia

- Listado de Aplicaciones alcanzadas por el Testing Anual.
- Listado de Servidores publicado por IT Tech y Servidores POS publicado por IT País
- Crudos de Relevamiento de Servidores
- Solicitud de remediación aprobada de la herramienta de gestión vigente, en caso de corresponder
- Procedimiento de ejecución del Control
- Reporte de Sobre SAT/CyberArk/FF
- Anexo de cuentas exceptuadas.
- E-mails de Gestión de Ejecución del control y comunicación a los interesados.
- Nóminas de IT correspondientes
- Informe/resultado del control