CERTIFICACION DE USUARIOS IT. CNCO.IT.C006

Vigencia: 01/07/2024
Versión: 7.0

Caratula

Historial de versiones		
Versión	**Fecha**	**Comentario**
1.0	01/10/2018	Versión Inicial
2.0	01/10/2019	Revisión Anual
3.0	01/10/2020	Revisión Anual
4.0	04/08/2021	Revisión Anual
5.0	21/07/2022	Revisión Anual
6.0	01/04/2023	Revisión Anual
7.0	01/07/2024	Revisión Anual

Tabla de contenidos

1. Objetivo

Definir los pasos necesarios para efectuar la Certificación de Usuarios IT contemplado en el control de Seguridad **CNCO.IT.C006**.

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

- AGP: Se entiende como el sistema de Auto Gestión de Permisos, la cual se encuentra ubicada en la Intranet Corporativa que se utiliza para canalizar y solicitar accesos a los sistemas dentro de CENCOSUD (AGP, AGP Brasil, AGP Colombia).
- 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.
- EECC: Estados Contables.
- 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.

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, los balanceadores F5 y la arquitectura de la APL074 – Active Directory, que son DC.
- 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 se describe en BD.

La cantidad de servidores, los cuales son seleccionados aleatoriamente para cada universo, es la siguiente:

- 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.

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

4.2. Generación de documentación.

Sobre los casos que salieron en las muestras, se solicita al área de IT Tech o IT País la ejecución de los scripts de forma manual, según corresponda.

Se analiza de cada servidor de la muestra, los usuarios y grupos correspondientes contra las nóminas de IT Tech / IT País y CyberSecurity, y los listados de ensobrados o exceptuados.

Se excluyen del análisis los usuarios bloqueados, expirados e inhabilitados.

En el caso de las Bases de Datos, se analizan todas las instancias del servidor correspondientes a las aplicaciones alcanzadas en el Scope del Testing Anual.

4.2.1. Consideraciones

Dentro de la salida de scripts, para las BD Oracle, solo se consideran aquellos usuarios declarados en el punto n°13 (Listado de usuarios) ya que los otros registros de usuarios (en otros puntos) son exclusivamente históricos y ya no existen en el servidor.

Si hay grupos de usuarios con permisos de escritura/administración sobre el servidor (SO/BD) se envían a certificar de la misma manera que los usuarios nominales.

4.3. Envío de documentación

Se confeccionan el/los archivo/s con los usuarios/grupos IT a certificar, y se envía el correo a las áreas de CyberSecurity, IT Tech y IT País para que realicen la validación.

4.4. Certificación

Las áreas de CyberSecurity, IT Tech y IT País deberán validar durante la ejecución del control el correspondiente permiso para cada usuario/grupo dentro de cada servidor de la muestra.

En caso de corresponder el ajuste o baja de un usuario/grupo, se deberán generar las solicitudes de ajustes mediante la herramienta de gestión vigente.

Para aquellos usuarios/grupos notificados, los cuales CyberSecurity, IT Tech o IT País declaran que no le corresponde su certificación, (ej. al momento de validar no tienen permisos, están justificados, ya no se encuentran en el servidor al momento de su revisión, etc.) deberán enviar la debida evidencia o justificación para respaldar el caso.

Todos aquellos casos que no posean justificación de parte de CyberSecurity IT Tech o IT País, se les gestionará la baja por medio de la herramienta de gestión vigente.

El área de IT Governance & Compliance puede extender el plazo de revisión y remediación mientras el mismo esté dentro del margen definido para la realización del control.

4.5. Cierre del control

El equipo de IT Governance & Compliance podrá cerrar el control con la certificación de todos los usuarios/grupos realizados o en su defecto su justificación, y con sus correspondientes solicitudes de remediación aprobadas.

Queda en total potestad de CyberSecurity, aplicar remediaciones solicitadas en la segunda quincena del mes de diciembre.

La implementación de las remediaciones se podrá posponer a enero del siguiente año si dicha remediación de los usuarios propone una afectación de la continuidad operativa y tomando en consideración que debemos salvaguardar la integridad de las operaciones de la compañía durante el período festivo de Fin de Año.

4.6. Evidencia

- Listado de usuarios de SO/BD a certificar con la documentación de la muestra realizada
- 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