



22 de Septiembre de 2021

Ficha N° 13 A.12.4.3

CSIRT DE GOBIERNO

Ficha de Control Normativo A.12.4.3

Registros del Administrador y el Operador

I. INTRODUCCIÓN

Este documento, denominado “Ficha de Control Normativo”, tiene como objetivo ilustrar sobre los diferentes controles normativos que se estima son prioritarios para todo Sistema de Gestión de Seguridad de la Información. Ciertamente cada control debe ser evaluado y aplicado según su mérito e impacto en los procesos de cada institución según el respectivo proceso de gestión del riesgo.

La experiencia nos ha permitido identificar algunos controles que tienen propiedades basales y que en la práctica se considera que debieran estar presentes en toda institución con grados de implementación “verificado” según la escala de madurez que ha promovido el CAIGG¹.

Nivel	Aspecto	% de cumplimiento	Descripción
1	Inicial	20%	No existe este elemento clave o no está aprobado formalmente y no se ejecuta como parte del Sistema de Prevención
2	Planificado	40%	Se planifica y se aprueba formalmente. Se programa la realización de actividades
3	Ejecutado	60%	Se ejecuta e implementa de acuerdo con lo aprobado y planificado
4	Verificado	80%	Se realiza seguimiento y medición de las acciones asociadas a la ejecución
5	Retroalimentado	100%	Se retroalimenta y se toman medidas para mejorar el desempeño

¹ <https://www.auditoriainternadegobierno.gob.cl/wp-content/uploads/2018/10/DOCUMENTO-TECNICO-N-107-MODELO-DE-MADUREZ.pdf>



Por tanto estas directrices si bien no reemplazan el análisis de riesgo institucional, si permiten identificar instrumentos, herramientas y desarrollos que pueden conducir a la implementación del control aludido e ir mejorando la postura global de ciberseguridad institucional.

Todo esto bajo el marco referencial vigente:

- El Instructivo Presidencial N°8 / 2018².
- El Decreto Supremo N°83 / 2005³.
- El Decreto Supremo N°93 / 2006⁴.
- El Decreto Supremo N°14 de 2014⁵.
- El Decreto Supremo N°1 de 2015⁶.
- La norma Nch-ISO/IEC 27001⁷.
- La norma Nch-ISO/IEC 27002.
- La norma Nch-ISO/IEC 27010.
- La norma ISA/IEC-62443⁸ (estándar global de ciberseguridad para la automatización industrial).
- Ley N°21.180 sobre Transformación digital del Estado⁹.

² <https://transparenciaactiva.presidencia.cl/instructivos/Instructivo-2018-008.pdf>

³ <https://www.bcn.cl/leychile/navegar?idNorma=234598>

⁴ <https://www.bcn.cl/leychile/navegar?idNorma=251713>

⁵ <https://www.bcn.cl/leychile/navegar?idNorma=1059778&idParte=9409404>

⁶ <https://www.bcn.cl/leychile/navegar?idNorma=1078308>

⁷ <https://ecommerce.inn.cl/nch-iso-iec-27001202078002>

⁸ <https://www.isa.org/>

⁹ <https://www.bcn.cl/leychile/navegar?idNorma=1138479>



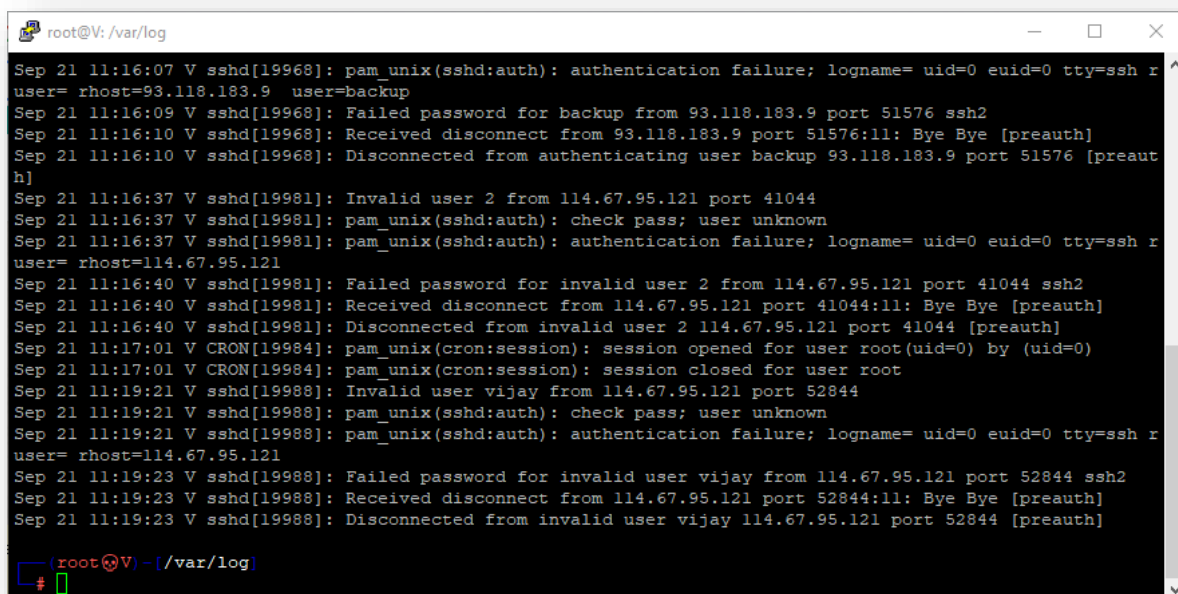
II. Registros

En el nivel más alto, las organizaciones deberían definir una “política general de seguridad de la información” debidamente aprobada por la dirección y que establezca el enfoque de la organización para administrar sus objetivos de seguridad de la información.

Debajo de la política general debiera estructurarse una política específica que regule y entregue las directrices sobre la organización de la ciberseguridad dentro de la institución.

Todo esto debidamente armonizado con una adecuada política específica de Seguridad de las Operaciones, que permita a los funcionarios acercarse e internalizar los conceptos para aplicarlos de manera transversal en su quehacer diario.

Esta directiva de debiera incorporar instrucciones, medidas y controles para integrar uno de los controles importantes: el registro de eventos.



```
root@V: /var/log
Sep 21 11:16:07 V sshd[19968]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh r
user= rhost=93.118.183.9 user=backup
Sep 21 11:16:09 V sshd[19968]: Failed password for backup from 93.118.183.9 port 51576 ssh2
Sep 21 11:16:10 V sshd[19968]: Received disconnect from 93.118.183.9 port 51576:11: Bye Bye [preauth]
Sep 21 11:16:10 V sshd[19968]: Disconnected from authenticating user backup 93.118.183.9 port 51576 [preaut
h]
Sep 21 11:16:37 V sshd[19981]: Invalid user 2 from 114.67.95.121 port 41044
Sep 21 11:16:37 V sshd[19981]: pam_unix(sshd:auth): check pass; user unknown
Sep 21 11:16:37 V sshd[19981]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh r
user= rhost=114.67.95.121
Sep 21 11:16:40 V sshd[19981]: Failed password for invalid user 2 from 114.67.95.121 port 41044 ssh2
Sep 21 11:16:40 V sshd[19981]: Received disconnect from 114.67.95.121 port 41044:11: Bye Bye [preauth]
Sep 21 11:16:40 V sshd[19981]: Disconnected from invalid user 2 114.67.95.121 port 41044 [preauth]
Sep 21 11:17:01 V CRON[19984]: pam_unix(cron:session): session opened for user root(uid=0) by (uid=0)
Sep 21 11:17:01 V CRON[19984]: pam_unix(cron:session): session closed for user root
Sep 21 11:19:21 V sshd[19988]: Invalid user vijay from 114.67.95.121 port 52844
Sep 21 11:19:21 V sshd[19988]: pam_unix(sshd:auth): check pass; user unknown
Sep 21 11:19:21 V sshd[19988]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh r
user= rhost=114.67.95.121
Sep 21 11:19:23 V sshd[19988]: Failed password for invalid user vijay from 114.67.95.121 port 52844 ssh2
Sep 21 11:19:23 V sshd[19988]: Received disconnect from 114.67.95.121 port 52844:11: Bye Bye [preauth]
Sep 21 11:19:23 V sshd[19988]: Disconnected from invalid user vijay 114.67.95.121 port 52844 [preauth]

(root@V) - [/var/log]
#
```

En este contexto, todos los equipos y sistemas bien diseñados contemplan funciones de auditoría, trazas de error y mensajería en general sobre estatus del procesamiento y funcionamiento.

Estos registros hablan de los que está sucediendo con ellos, los problemas, y general todo tipo de señales que nos ayudan a diagnosticar situaciones cuando hay problemas.



También ayudan estos registros a tener trazabilidad de las acciones ejecutadas por los usuarios de los sistemas, siendo una herramienta importante para auditorías.

Un grupo especial de estos registros son aquellos que dicen relación con los que cuentan las acciones de los administradores y de los operadores. Por ejemplo, las conexiones del usuario “root” fallidas y exitosas en un sistema Linux:

```
root@V: /var/log
Sep 21 11:31:25 V sshd[20336]: Disconnected from authenticating user root 221.181.185.135 port 61677 [preauth]
Sep 21 11:31:25 V sshd[20336]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= root st=221.181.185.135 user=root
Sep 21 11:31:27 V sshd[20338]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=221.181.185.135 user=root
Sep 21 11:31:29 V sshd[20338]: Failed password for root from 221.181.185.135 port 30213 ssh2
Sep 21 11:31:32 V sshd[20338]: Failed password for root from 221.181.185.135 port 30213 ssh2
Sep 21 11:31:34 V sshd[20338]: Failed password for root from 221.181.185.135 port 30213 ssh2
Sep 21 11:31:36 V sshd[20338]: Disconnected from authenticating user root 221.181.185.135 port 30213 [preauth]
Sep 21 11:31:36 V sshd[20338]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= root st=221.181.185.135 user=root
Sep 21 11:33:33 V sshd[20345]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=222.186.42.213 user=root
Sep 21 11:33:35 V sshd[20345]: Failed password for root from 222.186.42.213 port 27806 ssh2
Sep 21 11:33:38 V sshd[20345]: Failed password for root from 222.186.42.213 port 27806 ssh2
Sep 21 11:33:42 V sshd[20345]: Failed password for root from 222.186.42.213 port 27806 ssh2
Sep 21 11:33:43 V sshd[20345]: Disconnected from authenticating user root 222.186.42.213 port 27806 [preauth]
Sep 21 11:33:43 V sshd[20345]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= root st=222.186.42.213 user=root
(root@V) - [/var/log]
#
```

Estos registros son especiales, pues como su nombre lo dice, narran las actividades realizadas por el administrador y los operadores de los sistemas, y deben resguardarse de posibles manipulaciones por parte de los mismos administradores.

Se debe resguardar su integridad y disponibilidad, para que terceras partes puedan cumplir a cabalidad el rol de auditoría sobre estas actividades.

¿Que puede llegar a afectar la integridad, confidencialidad o disponibilidad de los registros?

Integridad:

Los registros pueden ser modificados por diferentes actores ya sea maliciosamente o por simple error humano.



Confidencialidad:

Los registros pueden mostrar información sensible y si sus repositorios o las formas de comunicación que utilizan los sistemas para enviarlos a repositorios externos al dispositivo mismo son inseguros, puede quedar expuestos a que terceras partes no autorizadas accedan a estos datos, violando con esto la confidencialidad que debe estar asignada a estos activos en la institución.

Disponibilidad:

La disponibilidad de los registros se ve afectada principalmente por un agestión inadecuada de los espacio de almacenamiento. En general los dispositivos propiamente tales no cuentan con almacenamiento muy grande para estos fines, razón por la cual almacena una historia corta de estos registros, perdiéndose todos aquellos que excedan el tamaño establecido de almacenamiento.

Ver anexo I con un ejemplo de estructura de políticas y procedimientos.



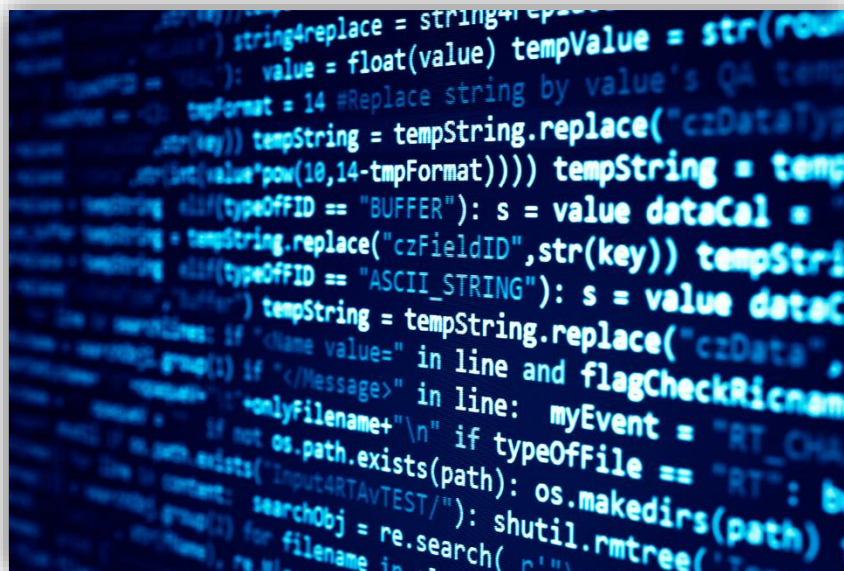
III. RECOMENDACIONES Y MEJORES PRÁCTICAS ASOCIADAS AL CONTROL

El control: Registros del Administrador y el Operador

Se deben registrar las actividades del operador y del administrador del sistema, los registros se deben proteger y revisar con regularidad.

Recomendaciones generales

Los propietarios de cuentas de usuario con privilegios pueden manipular los registros en las instalaciones de procesamiento de información bajo su control directo y, por lo tanto, puede ser necesario proteger y revisar los registros para mantener la responsabilidad de los usuarios con privilegios.



El CSIRT ha preparado algunas políticas que pueden servir de punto de partida para aquellas instituciones que aún no tengan dichos documentos armados y aprobados por sus autoridades. Revíselas en el siguiente enlace¹⁰.

¹⁰ <https://www.csirt.gob.cl/matrices-de-politicas/>



La Institución debe limitar los privilegios de los administradores, operadores y otros usuarios con altos privilegios, ya sea en servidores, bases de datos, equipos de comunicaciones, equipos de seguridad y cualquier otro dispositivo conectado a la red y que requiere supervisión. Para lograr esto se recomienda la siguiente pauta:

Todo usuario de sistema con cuenta privilegiada debe tener un “User ID” personalizado (asociado a su nombre). Esto facilitará el tracking de las acciones sobre los diversos dispositivos a los que tiene acceso.

Toda cuenta de administración genérica no debe ser usada a menos que haya un motivo específico y debidamente autorizado por el Encargado de Ciberseguridad o de Seguridad de la Información. Las claves de estas cuentas deben encontrarse bajo un protocolo de sobre cerrado y bajo resguardo.

Se debe limitar los privilegios para modificar o eliminar registros de eventos o logs de auditoria de las cuentas personalizadas de los administradores de plataforma, operadores, explotadores de sistemas y otros que necesitan contar con un nivel avanzado de privilegios.

Se debe limitar el acceso de usuarios administradores de plataforma, operadores, explotadores y otros que requieran contar con un nivel avanzado de privilegios sobre el servidor o concentrador de registros de eventos.



Se debe monitorear las acciones de usuarios administradores de plataforma, operadores, explotadores y otros que requieran contar con un nivel avanzado de privilegios, ya sea a través de plataformas de monitoreo específicas o de correlación de eventos, a los cuales solo el Encargado de Ciberseguridad o de Seguridad de la Información, o quien este designe pueda tener acceso.

Listado de cuentas con privilegios sobre los sistemas y plataforma tecnológica de la institución, incluyendo evidencia de que estas cuentas no tienen privilegios para modificar o eliminar registros de eventos.

Revisión del Encargado de Ciberseguridad respecto a las actividades de Administradores de Plataforma, Operadores, Explotadores de Sistemas y otros que requieran privilegios.

Evidencia de apertura de sobres con claves de cuentas genéricas de administrador.



Protección de los registros de auditoría

El acceso a los registros de auditoría deberá ser salvaguardado de acceso o modificaciones, que alteren su integridad, para lo cual su acceso es restringido al encargado de seguridad y de sistemas.



Estos registros deberán poseer copias de respaldo, en la medida que se disponga de recursos, procurando mantener una historia de al menos 1 año de eventos y LOGS.

Estudie las múltiples opciones y recomendaciones para avanzar en la implementación de este control y así obtener resultados específicos y concretos que puedan mostrarse al Comité de Seguridad de la Información (o equivalentes). Procure buscar apoyo tanto en el entorno de Gobierno Digital¹¹ como en el CSIRT de Gobierno¹² (Ministerio del Interior y Seguridad Pública) si siente que está detenido en algún punto de la implementación de este control.

En caso de cualquier inquietud o sugerencia no dude en contactarnos en soc-csirt@interior.gob.cl.

¹¹ <https://digital.gob.cl/>

¹² <https://www.csirt.gob.cl/>



Anexo I: Ejemplo de estructura de Políticas y Procedimientos

