14 de Septiembre de 2021
Ficha N° 12 A.12.4.1
CSIRT DE GOBIERNO

Ficha de Control Normativo A.12.4.1

Registro de Eventos

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 CAIGG[1].

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 / 2018[2].
- El Decreto Supremo N°83 / 2005[3].
- El Decreto Supremo N°93 / 2006[4].
- El Decreto Supremo N°14 de 2014[5].
- El Decreto Supremo N°1 de 2015[6].
- La norma Nch-ISO/IEC 27001[7].
- La norma Nch-ISO/IEC 27002.
- La norma Nch-ISO/IEC 27010.
- La norma ISA/IEC-62443[8] (estándar global de ciberseguridad para la automatización industrial).
- Ley N°21.180 sobre Transformación digital del Estado[9].

[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. Eventos

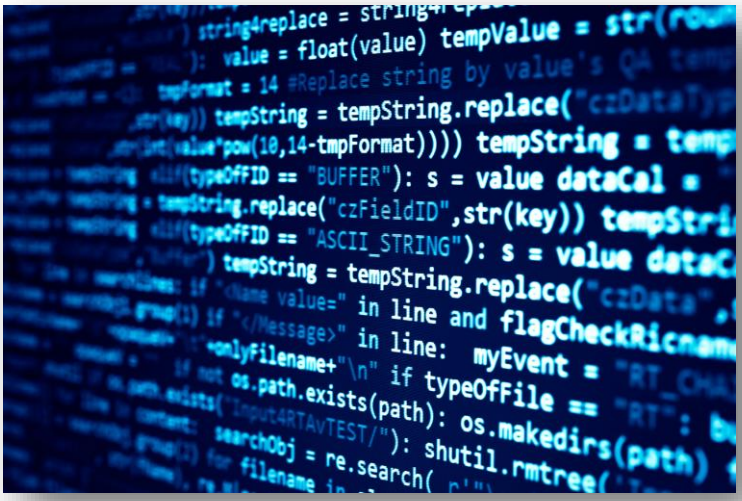
En el nivel más alto, las organizaciones deberían definir una “política general de seguridad de la información" debidamente aprobada por la dirección y que establezca el enfoque de la organización para administrar sus objetivos de seguridad de la información.

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.

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.

Por tanto estos registros deben estar protegidos para evitar su pérdida por fallas del almacenamiento o modificaciones maliciosas o por terceras parte son autorizadas.

En general estos registros pueden llamarse eventos.

Complementariamente podemos entender el concepto de Evento de Seguridad de la Información como la “ocurrencia identificada de un sistema, servicio o estado de la red que indica una posible

violación de la política de seguridad de la información o una falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad".

Con estos eventos de seguridad de la información podemos identificar el accionar de un incidente de seguridad de la información, al que entenderemos como "uno o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información".

Entonces los eventos en general y en especial los eventos de seguridad de la información son muy relevantes para los analistas de ciberseguridad y serán cruciales a la hora de detectar lo más temprano posible un incidente de ciberseguridad o entender desde la mirada forense que sucedió con nuestros sistemas que permitieron un ciberataque o la acción maliciosa de un ciberdelincuente.

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

Integridad:

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

Confidencialidad:

Los eventos 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 eventos 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.

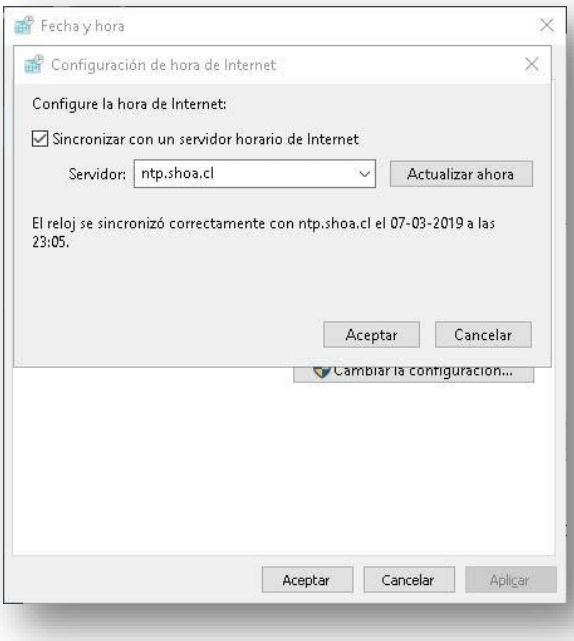
¿Cuáles son los aspectos clave a tener en consideración para el registro de eventos?:

Todos los dispositivos y aplicativos deben generar eventos.

Existen diferentes niveles de detalle con los que se reportan y para diferentes niveles de severidad; tenga presente que a mayor detalle de los eventos es posible mejorar el análisis, pero también los hace más complejo pues el volumen de registros aumenta de manera muy significativa.

Se debe tener en consideración las limitaciones de almacenamiento interno de cada dispositivo o servidor, de manera que es muy recomendable considera un concentrador de eventos con alta capacidad de almacenamiento y altos estándares de protección y resiliencia.

El sello de tiempo de los registros es fundamental y deben estar sincronizados contra una fuente de tiempo central, y coordinados con la referencia nacional de tiempo ntp.shoa.cl.



Debe existir capacidad para transformar los eventos a un formato que permita su procesamiento posterior por sistemas de inteligencia y correlación.

Establecer tiempos de retención de registros suficientemente largos como para contar con una historia que permita análisis retrospectivos y no tan largos para no sobre exigir los requerimientos de almacenamiento. Se sugiere al menos 1 año de historia.

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

III. RECOMENDACIONES Y MEJORES PRÁCTICAS ASOCIADAS AL CONTROL

El control: Respaldo de Información

Se deben generar, mantener y revisar con regularidad los registros de eventos de las actividades del usuario, excepciones, fallas y eventos de seguridad de la información.

Recomendaciones generales

Los registros de eventos deberían incluir, cuando corresponda:

a) IDs de usuarios;

b) Actividades del sistema;

c) Fechas, horas y detalles de los eventos clave, es decir el inicio y la finalización de la sesión;

d) La identidad del dispositivo y su ubicación si es posible, junto con el identificador del sistema;

e) Los registros de los intentos de acceso al sistema exitosos y rechazados;

f) Los registros de los datos exitosos y rechazados y otros intentos de acceso a los recursos;

g) Los cambios a la configuración del sistema;

h) El uso de privilegios;

i) El uso de utilidades y aplicaciones del sistema;

j) Los archivos y el tipo de acceso;

k) Las direcciones y protocolos de redes;

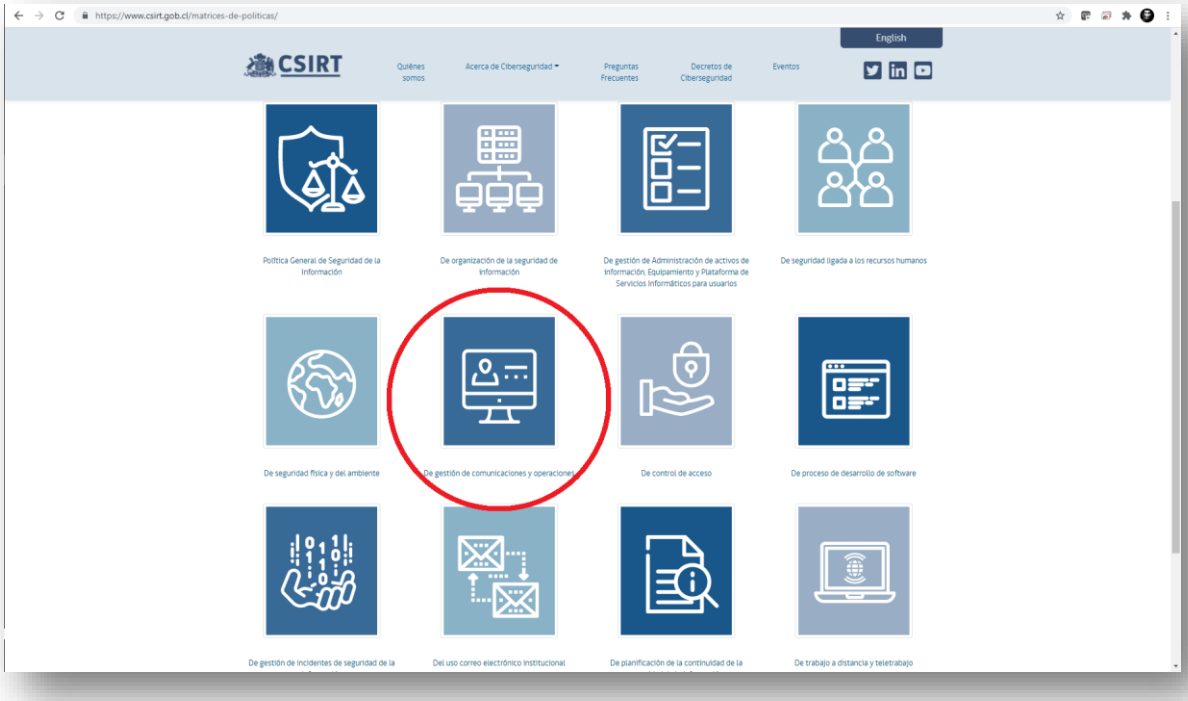
l) Las alarmas que se activaron con el sistema de control de acceso;

m) La activación y la desactivación de los sistemas de protección, como los sistemas de antivirus y los sistemas de detección de intrusos;

n) Los registros de las transacciones ejecutadas por los usuarios en las aplicaciones.

El registro de eventos establece las bases para los sistemas de monitoreo automatizado que son capaces de generar informes y alertas consolidadas sobre la seguridad del sistema.

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 enlace[10].



Las Instituciones del Estado, deberán implementar logs de auditoria en los diversos sistemas tecnológicos que se encuentren conectados a su red. Estos registros o logs deberán ser obtenidos y almacenados en forma segura para evitar su alteración o modificación no autorizada. En caso de que los logs o registros de eventos puedan contener datos sensibles o información de identificación personal, se deberán tomar medidas adicionales de protección de esta información.

En todos los sistemas, en los cuales se active los registros de eventos o logs de auditoría, se deberá deshabilitar los permisos a las cuentas privilegiadas para el borrado, modificación o desactivación de estos registros.

Se deberá implementar una política de retención de estos registros, por un tiempo que defina la institución en función a sus requerimientos de negocio. Por tanto, la institución deberá asegurar la capacidad tecnológica para mantener estos registros por el tiempo definido.

[10] https://www.csirt.gob.cl/matrices-de-politicas/

Si la institución implementa soluciones de correlación de eventos a través de un Sistema de Información y Gestión de Eventos (SIEM), entonces los registros de eventos o logs de auditoria podrán ser enviados al sistema de correlación, asegurando además el almacenamiento de una copia de cada registro en el formato original en la plataforma de almacenamiento de Logs, ya que pueden requerirse como evidencia ante situaciones de carácter legal por mal uso de infraestructura tecnológica, fraude, robos, entre otros aspectos.

Algunas evidencias que pueden servir para acreditar que está operando este control pueden ser:

- Estructura de registros de eventos o logs de auditoria.
- Lista de servidores, equipos de seguridad y otros dispositivos conectados a la red institucional, a los cuales se almacenarán los registros de eventos o logs de auditoría.
- Evidencia (cuando ocurra) de logs extraídos por temas legales.
- Evidencia de restricciones de permisos a cuentas de administradores y operadores para que no puedan modificar o eliminar registros de eventos sobre los sistemas tecnológicos de la institución.
- Evidencia de permisos de acceso de personal autorizado a acceder a servidor o plataforma concentrador de logs.

En las políticas que contemplen estos conceptos al menos debieran considerar los siguientes aspectos:

Registro de auditorias

Los sistemas de información, así como los servidores, dispositivos de red y demás servicios tecnológicos, deberán guardar registros de auditoría y logs, los cuales contemplarán, siempre y cuando sea posible:

- Id del usuario.
- Fecha y hora de la transacción.
- Dirección IP y nombre del dispositivo desde el cual se realizó la transacción.
- Tipo de transacción.
- Intentos fallidos de conexión.
- Cambios en la configuración del sistema.
- Cambio o revocación de privilegios.
- Alarmas originadas por los sistemas de monitoreo.
- Desactivación de los mecanismos de protección.
- acceso, creación, borrado y actualización de información confidencial;
- inicio y fin de conexión en la red corporativa;
- inicio y fin de ejecución de aplicaciones y sistemas;

- inicio y fin de sesión de usuario en aplicaciones y sistemas; intentos de inicio de sesión fallidos;
- cambios en las configuraciones de los sistemas y aplicativos más importantes;
- modificaciones en los permisos de acceso;
- funcionamiento o finalización anómalos de aplicativos;
- aproximación a los límites de uso de ciertos recursos físicos:
    - capacidad de disco;
    - memoria;
    - ancho de banda de red;
    - uso de CPU;
- indicios de actividad sospechosa detectada por antivirus, Sistemas de Detección de Intrusos (IDS), etc.;
- transacciones relevantes dentro de los aplicativos.

Teniendo en cuenta las múltiples fuentes de datos de registros de logs y auditorías, éstos se almacenarán en repositorio digital concentrador de eventos (un servidor de *syslog* como implementación mínima), cuya capacidad estará sujeta a la disponibilidad de recursos, procurando mantener una historia de al menos 1 año de eventos y LOGS.
Para cumplir con el adecuado aseguramiento de estos importantes datos se deben chequear los siguientes temas:

- Qué actividad debe ser registrada
- Información relevante incluida en el registro
- Formato de la información registrada
- Elección del mecanismo de registro
- Protección y almacenamiento
- Sincronización del reloj
- Sistemas de monitorización y alerta

Información relevante incluida en el registro. Los más habituales son:

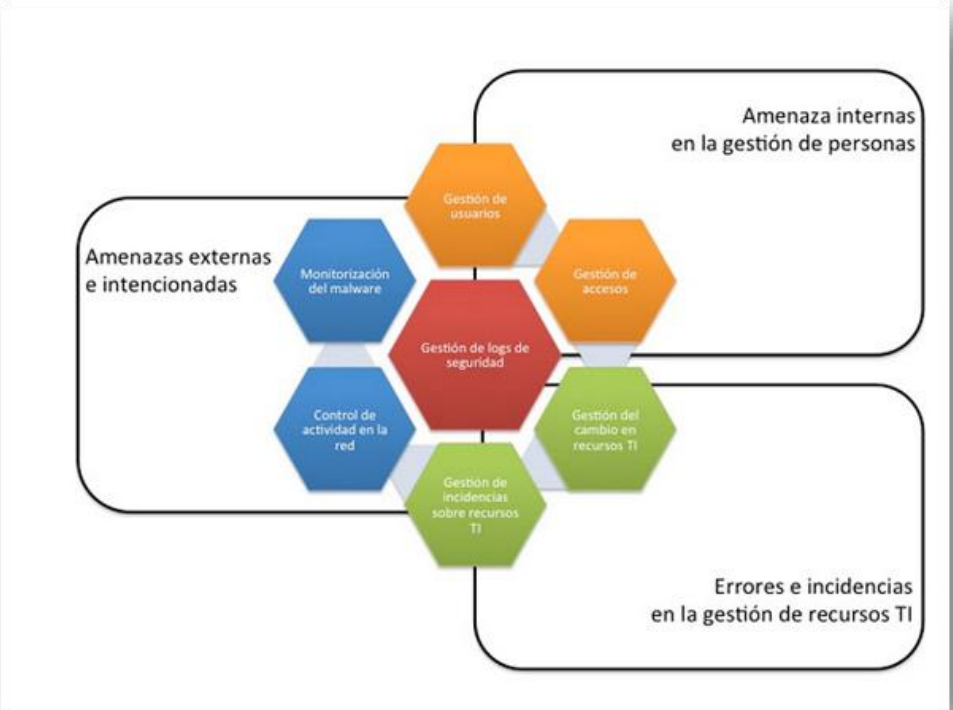
- identificador del usuario que realiza la acción;
- identificación del elemento sobre el que se realiza la acción (archivos, documentos, bases de datos, equipos, etc.);
- identificación de dispositivos, ya sea a través de sus direcciones IP, direcciones MAC, etc.;
- identificación de protocolos;
- fecha y hora de ocurrencia del evento;
- tipología del evento.

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.

Sincronización de relojes

Para garantizar la exactitud de los registros de auditoría, la [Unidad TIC], dispondrá de un servicio de protocolo de tiempo de red NTP que estará sincronizado a su vez con la hora oficial de Chile Continental; servicio que en la actualidad provee el Servicio Hidrográfico y Oceanográfico de la Armada de Chile (SHOA).



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 Digital[11] como en el CSIRT de Gobierno[12] (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