30 de Septiembre de 2021
Ficha N° 14 A.12.4.4
CSIRT DE GOBIERNO

Ficha de Control Normativo A.12.4.4

Sincronización de Relojes

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

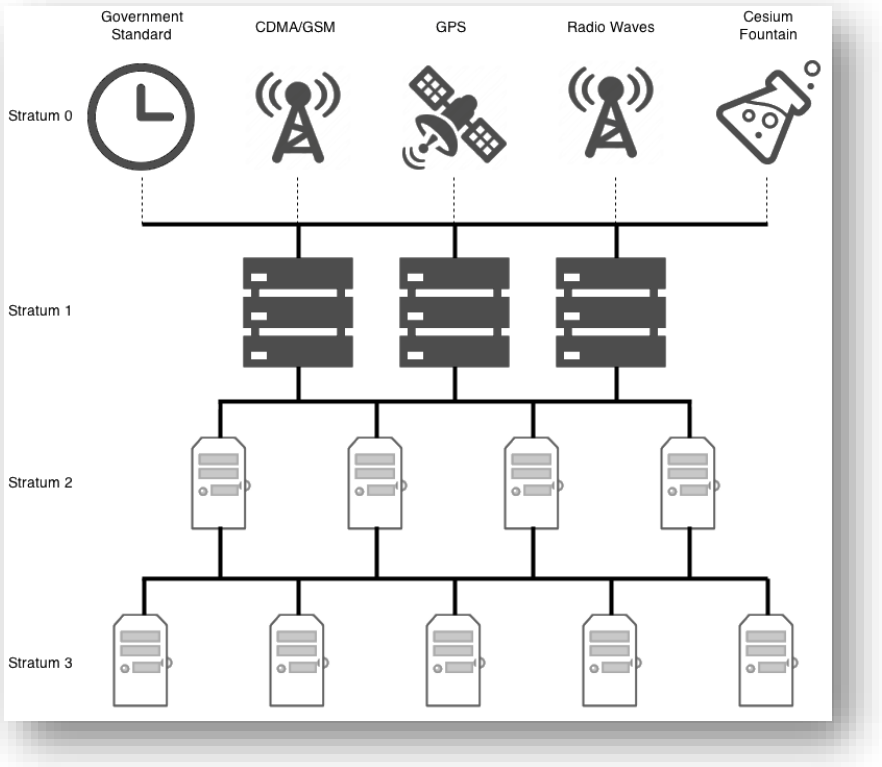
II. El tiempo[10]

Para conseguir una buena eficiencia en los servicios, evitar complicaciones y facilitar los análisis temporales de los diferentes registros que incorporan el sello de tiempo, la sincronización de todos los componentes de la red juega un papel relevante. Existen varios mecanismos de sincronización, siendo los tipos Simple Network Time Protocol (SNTP), Network Time Protocol (NTP) y Precision Time Protocol (PTP) los más comunes. El protocolo PTP es el más preciso, con una exactitud del orden de los nanosegundos, mientras que los protocolos SNTP y NTP tienen una precisión menor, del orden de los microsegundos, siendo suficientes para determinadas necesidades industriales y comerciales.

El error en la medición del tiempo o en los protocolos utilizados, ya sea provocado por un atacante o no, podría suponer:

- Un error en un procedimiento industrial por desorganización mecánica.
- Fallos de la actualización, al retrasar un reloj y nunca llegar a la fecha objetivo.
- La caducidad en ciertos programas al aumentar la fecha del reloj interno.
- Complicaciones en los certificados digitales y sus sellos de tiempo.
- Complejidades en los análisis forenses.

[10] Información extraída de INCIBE.



Descripción de protocolos y últimas versiones

Tanto en el protocolo NTP como en el SNTP la comunicación comienza con un mensaje de petición por parte del cliente. Además, envían y reciben el mismo formato de mensaje con el servidor. La diferencia principal entre ambos es el proceso de sincronización que llevan a cabo. El protocolo NTP puede utilizar varios servidores y tiene en cuenta la velocidad de actuación del componente que solicita la hora. Al usar varios dispositivos el método NTP puede discriminar el tiempo de aquellos que se alejen mucho de los demás. Esto confiere al protocolo NTP más fiabilidad que el SNTP, que utiliza solo un servidor o reloj máster.

Ambos protocolos son interoperables, es decir, un dispositivo que funcione con SNTP puede conectarse a otro que esté utilizando NTP y viceversa. Esto es posible gracias a que, como se ha comentado anteriormente, el formato de mensajes que intercambian ambos algoritmos es el mismo. Otra característica que tienen en común dichos protocolos es la utilización de la hora UTC (Coordinated Universal Time). Esta hora es la misma para todo el mundo y permanece constante a lo largo del año.

NTP

NTP es implementado en la mayoría de los sistemas operativos basados en Linux y Windows, ampliamente utilizados en los sistemas de control.

SNTP

El método SNTP es mucho más sencillo que el NTP, ya que omite varios pasos y solo ajusta el tiempo periódicamente, consiguiendo una precisión menor. El contenido del paquete con el que se comunica con el servidor omite muchas de las funcionalidades del procedimiento NTP. No es recomendable el uso del protocolo SNTP como fuente o reloj principal. La última versión de este protocolo es la SNTPv4. El principal problema de este protocolo es su baja seguridad porque carece de método de cifrado, haciéndolo vulnerable a ataques en los que se puede modificar el tiempo.

El uso del protocolo SNTP es interesante en los siguientes casos:

- Dispositivos simples, como microcontroladores y ordenadores pequeños, con poca memoria.
- Equipos en los que la sincronización del tiempo no sea determinante.
- Dispositivos de control como PLC, remotas y dispositivos embebidos.

PTP

A diferencia de NTP y el SNTP, en el protocolo PTP la conexión empieza con una petición del servidor. La intención de este protocolo es ser utilizado en redes locales y en dispositivos industriales. Otra diferencia con respecto a los otros dos protocolos es que para utilizar este algoritmo se requiere de hardware específico. Además, en este momento no existen servidores PTP gratuitos, por lo que es necesario un pago para poder utilizar esta fuente, o disponer de un servidor principal dentro de la instalación. Utiliza dos puertos UDP: el 319 para mensajes de eventos y el 320 para mensajes generales.

Principalmente el uso de PTP se encuentra en:

- La generación y control de energía.
- El control de sistemas de fabricación de piezas.
- Transacciones bancarias.
- Correlación de valores en el testeo de medidas.
- Control robótico.

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

III. RECOMENDACIONES Y MEJORES PRÁCTICAS ASOCIADAS AL CONTROL

El control: Sincronización de relojes

Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o domino de seguridad deben estar sincronizados a una sola fuente horaria de referencia.

Recomendaciones generales

Asegurar la sincronización de los dispositivos en procedimientos industriales es de vital importancia. La principal amenaza está ligada al uso de servidores de Internet. Las organizaciones deberán utilizar servidores con mecanismo GPS como método de sincronización como estrato cero e implementar cortafuegos que eviten la entrada de comandos que puedan hacer variaciones de tiempo en caso de uso de los métodos NTP y SNTP.

Necesitamos especificar bien cuáles son las necesidades concretas de nuestros equipos para su buen funcionamiento. Cuanto más compleja y exacta tenga que ser la labor de los equipos, mayor precisión en el tiempo será necesaria. En esta situación la implantación del algoritmo PTP será la más adecuada.

Si nuestros dispositivos no tienen unas necesidades que requieran alta precisión, el uso de los protocolos NTP y SNTP es el apropiado. La elección de uno de estos dos métodos dependerá de la posición del dispositivo en la red, la capacidad de memoria y su necesidad de precisión.

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[11].

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

Se deberán documentar los requisitos externos e internos para la representación, la sincronización y la precisión del tiempo. Dichos requisitos pueden ser legales, normativos, contractuales, de cumplimiento con normas o para el monitoreo interno. Se debería definir una hora de referencia estándar para utilizar dentro de la organización.

Se deberá documentar e implementar el enfoque de la organización para obtener una hora de referencia de fuentes externas y la manera de sincronizar los relojes internos de manera confiable.

La institución debe generar los procedimientos para la sincronización de hora de todos los dispositivos conectados a la red y, en la medida que se requiera, deberá realizar las siguientes recomendaciones:

- Se deben aplicar los parches de actualización a los sistemas operativos de los distintos dispositivos conectados a la red de la institución, si hay cambios de hora.
- Se sugiere que la institución cuente con un servidor o equipo interno a los cuales se puedan conectar y sincronizar sus relojes. Este servidor o equipo interno deberá conectarse solo a servidores en internet válidos para estos efectos, por ejemplo, ntp.shoa.cl
- En caso de que no se cuente con una plataforma de actualización centralizada de hora, se recomienda que la institución cuente con los procedimientos específicos para el cambio de

hora, el cual deberá ser ejecutado por un operador o administrador de plataforma, teniendo en consideración que este cambio deberá realizarse en fecha y hora en el cual se produzca el cambio de hora en Chile.

Algunas evidencias que pueden servir para demostrar que su proceso de sincronización de relojes esta implementado y operativo podría ser:

- Protocolo documentado de cambio de hora.
- Evidencia de los cambios de hora de los servidores y dispositivos conectados a la red institucional.
- Publicación de los decretos de cambio de horario a nivel nacional.
- Inclusión de alguna manera del servidor nacional del SHOA: ntp.shoa.cl.

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[12] como en el CSIRT de Gobierno[13] (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.

[12] https://digital.gob.cl/
[13] https://www.csirt.gob.cl/

Anexo I: Ejemplo de estructura de Políticas y Procedimientos