19 de Octubre de 2021
Ficha N° 17 A.12.6.2
CSIRT DE GOBIERNO

Ficha de Control Normativo A.12.6.2

Restricciones sobre la instalación de software

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. ¿Por qué podrían ser importante las restricciones en la instalación de software?

En general las organizaciones deben definir y poner en vigencia una política estricta sobre qué tipos de software pueden instalar los usuarios en los equipos y dispositivos institucionales.

Al respecto cabe tener presente que las instalaciones de software puede ser realizadas por el usuario de manera intencional o no intencional. La instalación puede ser también maliciosa o benigna, lo que determinará los impactos positivos o negativos en la organización y sus controles. También es necesario entender que la instalación de software puede ser realizada por terceras partes (soporte u otras personas). Finalmente es necesario señalar que el software puede ser instalado por otras piezas de software (malware por ejemplo) que se propagan lateralmente dentro de una organización desde una máquina contaminada a otra máquina vulnerable.

En este contexto es necesario establecer controles que ayuden a mitigar los impactos negativos de instalaciones de software malicioso o, desde otra óptica, software no licenciado (con impacto en el cumplimiento legal de la institución exponiéndola a multas e infracciones por uso ilegal de software con propiedad intelectual).

La buena práctica en este sentido conduce a que la instalación de software en la institución debe ser controlada y centraliza por un equipo que vele por el cumplimiento de los estándares de seguridad, funcionalidad y legalidad del software institucional.

Este control requiere manejar algunos términos relevantes, cuyo conocimiento es crucial para poder articular las actividades relativas a la implementación de este control y de sus interrelaciones con otros controles.

Basándonos en el glosario de términos que disponibiliza INCIBE[10] se pueden entender los términos más utilizados en este contexto:

Activo de información

Es cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.

Actualización de seguridad

Modificaciones que se aplican, de forma automática o manual, en el software de los sistemas operativos o aplicaciones instalado en los dispositivos electrónicos, con el objetivo de corregir fallos

[10] https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

de seguridad, errores de funcionamiento o bien para dotar a los dispositivos de nuevas funcionabilidades, así como incorporar mejoras de rendimiento.

Sinónimo: Parches de seguridad.

Acuerdo de licencia

Es una cesión de derechos entre un titular de derechos de propiedad intelectual (licenciante) y otra persona que recibe la autorización de utilizar dichos derechos (licenciatario) a cambio de un pago convenido de antemano (tasa o regalía) o de unas condiciones determinadas. Existen distintos tipos de acuerdos de licencias que pueden clasificarse en las siguientes categorías:

- acuerdos de licencia tecnológica
- acuerdos de licencia y acuerdos de franquicia sobre marcas
- acuerdos de licencia sobre derecho de autor

Amenaza

Circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. Una amenaza puede tener causas naturales, ser accidental o intencionada. Si esta circunstancia desfavorable acontece a la vez que existe una vulnerabilidad o debilidad de los sistemas o aprovechando su existencia, puede derivar en un incidente de seguridad.

Brecha de seguridad

Violaciones de la seguridad que ocasionan la destrucción, pérdida o alteración accidental o deliberada de datos personales cuando están siendo transmitidos, están almacenados o son objeto de otros tratamientos. Las brechas de seguridad también afectan a la comunicación o acceso no autorizados a dichos datos.

Ciberataque

Intento deliberado de un ciberdelincuente de obtener acceso a un sistema informático sin autorización sirviéndose de diferentes técnicas y vulnerabilidades para la realización de actividades con fines maliciosos, como el robo de información, extorsión del propietario o simplemente daños al sistema.

Ciberdelincuente

Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información, deterioro de software o hardware, fraude y extorsión. Casi siempre están orientados a la obtención de fines económicos.

Firmware

Tipo de software que permite proporcionar un control a bajo nivel de un dispositivo o componente electrónico, siendo capaz de proveer un entorno de operación para las funciones más complejas del componente o comportándose como sistema operativo interno en armonía con otros dispositivos o componentes.

Malware

Es un tipo de software que tiene como objetivo dañar o infiltrarse sin el consentimiento de su propietario en un sistema de información. Palabra que nace de la unión de los términos en inglés de software malintencionado: malicious software. Dentro de esta definición tiene cabida un amplio elenco de programas maliciosos: virus, gusanos, troyanos, backdoors, spyware, etc. La nota común a todos estos programas es su carácter dañino o lesivo. Sinónimo: Software malicioso

Software

Definimos software del inglés como un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en un dispositivo. El software conforma todas aquellas acciones que se pueden realizar gracias a las instrucciones previamente contempladas y programadas e incluidas dentro de un programa que permite al usuario interactuar con el sistema de forma fácil e intuitiva.

Riesgo

Es la posibilidad de que una amenaza o vulnerabilidad se convierta en un daño real para la empresa, que resulte en una pérdida o robo de información o en una detención de su actividad como consecuencia del daño ocasionado. El riesgo puede ser mitigado mediante políticas de seguridad y continuidad del negocio que suelen prever posibles ataques y proponen soluciones de actuación ante situaciones cuyo riesgo pueda ser elevado.

Virus

Malware que tiene como característica principal que infecta ficheros ejecutables o sectores de arranque de dispositivos de almacenamiento.

Vulnerabilidad

Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos (normalmente mediante un programa que se denomina exploit). Cuando se descubre el desarrollador del software o hardware lo solucionará publicando una actualización de seguridad del producto.

Sinónimo: Agujero de seguridad

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

III. RECOMENDACIONES Y MEJORES PRÁCTICAS ASOCIADAS AL CONTROL

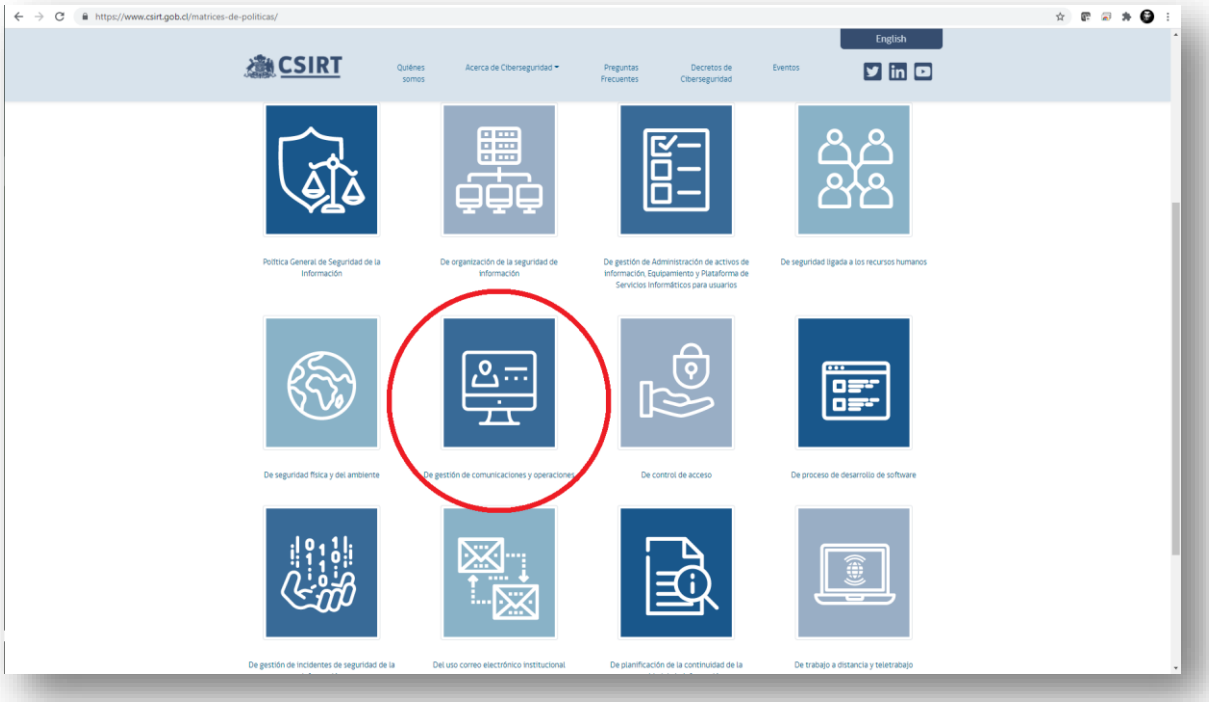
El control: Restricciones sobre la instalación de software

Se deben establecer e implementar las reglas que rigen la instalación de software por de parte de los usuarios.

Recomendaciones generales

Se deben construir políticas y procedimientos que ayuden a establecer las directrices de ciberseguridad y guías operacionales que permitan a todos los intervinientes implementar y utilizar los software operacionales de manera segura.

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/

La organización debe definir y poner en vigencia una política estricta sobre qué tipo de software pueden instalar los usuarios.

Se debe aplicar el principio de los menores privilegios. Si se les otorgan ciertos privilegios, es posible que los usuarios tengan la capacidad de instalar software. La organización debe definir qué tipos de instalaciones de software se permiten (es decir, actualizaciones y parches de seguridad al software existente) y qué tipos de instalaciones se prohíben (es decir, software que es solo para el uso personal y software cuya categoría en cuanto a su posible característica maliciosa es desconocida o sospechosa). Estos privilegios se deben otorgar considerando los roles de los usuarios involucrados.

La institución debe limitar los privilegios de los usuarios de los sistemas informáticos, a un nivel que le permita realizar las labores que le han encomendado, para ello, a nivel de las estaciones de trabajo, se debe configurar su cuenta a un nivel usuario, quitando la opción de quedar como administrador del equipo.

A nivel de Servidores, solo los Administradores de esta plataforma, podrán contar con altos privilegios asociados a sus cuentas.

Si la institución tuviera algún sistema informático antiguo o legacy, en el cual requiera que sus usuarios cuenten con privilegios de administrador sobre sus equipos, esta excepción, de carácter transitorio deberá ser autorizada por el Encargado de Ciberseguridad o de Seguridad de la Información, en conjunto con el Jefe de Servicio, ya que es una situación que puede elevar los niveles de exposición a riesgos. Igualmente, la institución debe hacer los esfuerzos necesarios para contemplar actualizaciones a estos aplicativos legacy, eliminando el requerimiento de contar con privilegios de administrador en la plataforma. Los logs de auditoria o registros de eventos para las cuentas con privilegios, deberá ser resguardado y se deberá verificar periódicamente con el objeto de determinar si los privilegios otorgados se utilizan para fines distintos al asignado.

Algunas evidencias que pueden ayudar a verificar y validar el cumplimiento de este control son:

- Evidencia de configuración de cuentas de usuarios en el dominio y en estaciones de trabajo.
- Listado de usuarios (cuando ocurra) con autorización a tener cuentas privilegiadas.
- Revisión de cuentas de dominio y locales, con el objeto de eliminar o deshabilitar aquellas cuentas que no se han utilizado en más de 90 días, en cumplimiento con la política de control de acceso institucional.
- Evidencia de revisión de logs de auditoria o de Registro de Eventos.

Complementariamente la Unidad TIC, implementará controles para prevenir y detectar código malicioso, lo cual se basa en software, concientización de usuarios y gestión del cambio. Los controles contemplan las siguientes directrices:

- Impedir el uso de software no autorizado.
- Impedir el compartir carpetas en los computadores y/o dispositivos personales.
- Implementar acciones y procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio, señalando las medidas de protección a tomar en procedimientos de soporte a usuarios.
- Instalar y actualizar software de detección y reparación de virus, IPS de host, anti- spyware examinado computadores y medios informáticos, como medida preventiva y rutinaria.
- Mantener los sistemas con las últimas actualizaciones de seguridad disponibles, previa realización de pruebas en un ambiente dispuesto para tal fin.
- Chequear periódicamente el contenido de software y datos de los equipos de procesamiento, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
- Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.
- Informar al personal acerca del problema de los falsos virus y de cómo proceder frente a los mismos.

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.

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