05 de Octubre de 2021
Ficha N° 15 A.12.5.1
CSIRT DE GOBIERNO

Ficha de Control Normativo A.12.5.1

Instalación de Software en Sistemas Operacionales

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:

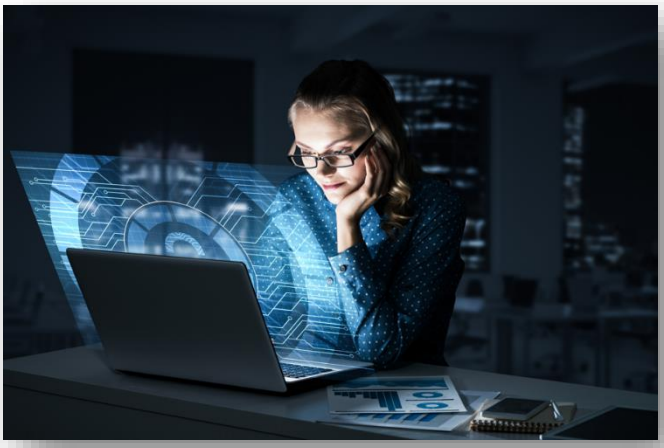
- El Instructivo Presidencial N°8 / 2018[2].
- El Decreto Supremo N°83 / 2005[3].
- El Decreto Supremo N°93 / 2006[4].
- El Decreto Supremo N°14 de 2014[5].
- El Decreto Supremo N°1 de 2015[6].
- La norma Nch-ISO/IEC 27001[7].
- La norma Nch-ISO/IEC 27002.
- La norma Nch-ISO/IEC 27010.
- La norma ISA/IEC-62443[8] (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 Software Operacional

"Un sistema informático podemos considerarlo como un sistema que nos permite almacenar y procesar información mediante una serie de partes interrelacionadas, como el hardware, el software y el personal. De hecho, estos son sus tres componentes fundamentales. En otras palabras, podemos decir que los sistemas informáticos son el conjunto de técnicas que nos permiten procesar y garantizar la seguridad de información mediante sistemas informatizados"[10].

"Del mismo modo un sistema de información es un conjunto de componentes que interactúan entre sí con un fin común. En informática, los sistemas de información ayudan a administrar, recolectar, recuperar, procesar, almacenar y distribuir información relevante para los procesos fundamentales y las particularidades de cada organización"[11].



Con estas orientaciones en mente podemos avanzar en la conceptualización de software operacional, donde en esta categoría consideraremos a todo software ya sea desarrollado, interna o externamente, o sea adquirido bajo cualquier modalidad de licenciamiento comercial o GNU u OpenSource, que esté destinado a prestar servicio en nuestra institución, principalmente a ser instalado en:

- Servidores físicos o virtuales institucionales.
- Servidores en alguna modalidad de nube.
- Equipos de usuarios de los sistemas.
- Dispositivos institucionales (móviles, IoT).
- Appliance institucionales.

Algunos ejemplos de software operacional son:

- Sistemas Operativos (GNU/Linux, Windows, OSX o Chrome OS, entre otros)[12]
- Firmware o Sistemas Operativos de appliance: IOS de Cisco o JunOS de Junipe, entre otros.

[10] https://www.euroinnova.cl/blog/que-es-un-sistema-informatico
[11] https://es.wikipedia.org/wiki/Sistema_de_informaci%C3%B3n
[12] https://www.eaeprogramas.es/blog/negocio/tecnologia/cuatro-sistemas-operativos-que-debes-conocer

- Móviles: Android de Google o iOS de Apple, entre otros.
- Aplicativos Operacionales comerciales u Opensource: Webserver apache, Webserver IIS, Microsoft Office, AntiMalware, Herramientas gráficas, entre otros.
- Sistemas construidos a medida o desarrollados, interna o externamente, para prestar servicios internos o a la ciudadanía: sitios o sistemas web por ejemplo.
- Software virtualizador: VMWare, Oracle VM VirtualBox, entre otros.

Otro antecedente relevante es que en el marco de la ley de transformación digital, N°21.180, se establece que:

> Uso obligatorio de plataformas electrónicas. Los órganos de la Administración estarán obligados a disponer y utilizar adecuadamente plataformas electrónicas para efectos de llevar expedientes electrónicos, las que deberán cumplir con estándares de seguridad, interoperabilidad, interconexión y ciberseguridad.
>
> Los escritos, documentos, actos y actuaciones de toda especie que se presenten o verifiquen en el procedimiento se registrarán en el expediente electrónico correspondiente, siguiendo las nomenclaturas pertinentes, de acuerdo a cada etapa del procedimiento.
>
> La conservación de los expedientes electrónicos estará a cargo del órgano respectivo, el cual será el responsable de su integridad, disponibilidad y autenticidad.
>
> Si fuere necesaria la reconstitución de un expediente o piezas de éste se reemplazará en todo o parte por una copia fiel, que se obtendrá de quien la tuviere, si no se dispusiere de ella directamente.
>
> Si no existiere copia fiel los actos se dictarán nuevamente, para lo cual la Administración reunirá los antecedentes que le permitan fundamentar su preexistencia y contenido, y las actuaciones se repetirán con las formalidades previstas para cada caso.
>
> Las comunicaciones oficiales entre los órganos de la Administración serán registradas en una plataforma electrónica destinada al efecto.
>
> Mediante reglamento, dictado en conjunto por el Ministerio Secretaría General de la Presidencia y el Ministerio de Hacienda, se fijarán los estándares que deberán cumplir dichas plataformas, en los términos previstos en esta ley considerando, además, condiciones de accesibilidad para los interesados, seguridad, funcionamiento, calidad, protección y conservación de los documentos.".

Donde estas exigencias en buena parte se han de implementar con sistemas y hardware, y se han de disponer para sus usuarios, funcionarios y ciudadanos mediante alguna interfaz que facilite su utilización.

Esta ley de transformación digital implica que la ciberseguridad una de la diferentes características que deben tenerse en cuenta a la hora de su implementación, es decir, no se puede avanzar en transformación digital sin considera sistemas que sean seguros para su operación y para el resguardo de la integridad, confidencialidad y disponibilidad de los procesos e información que gestionarán.

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

III. RECOMENDACIONES Y MEJORES PRÁCTICAS ASOCIADAS AL CONTROL

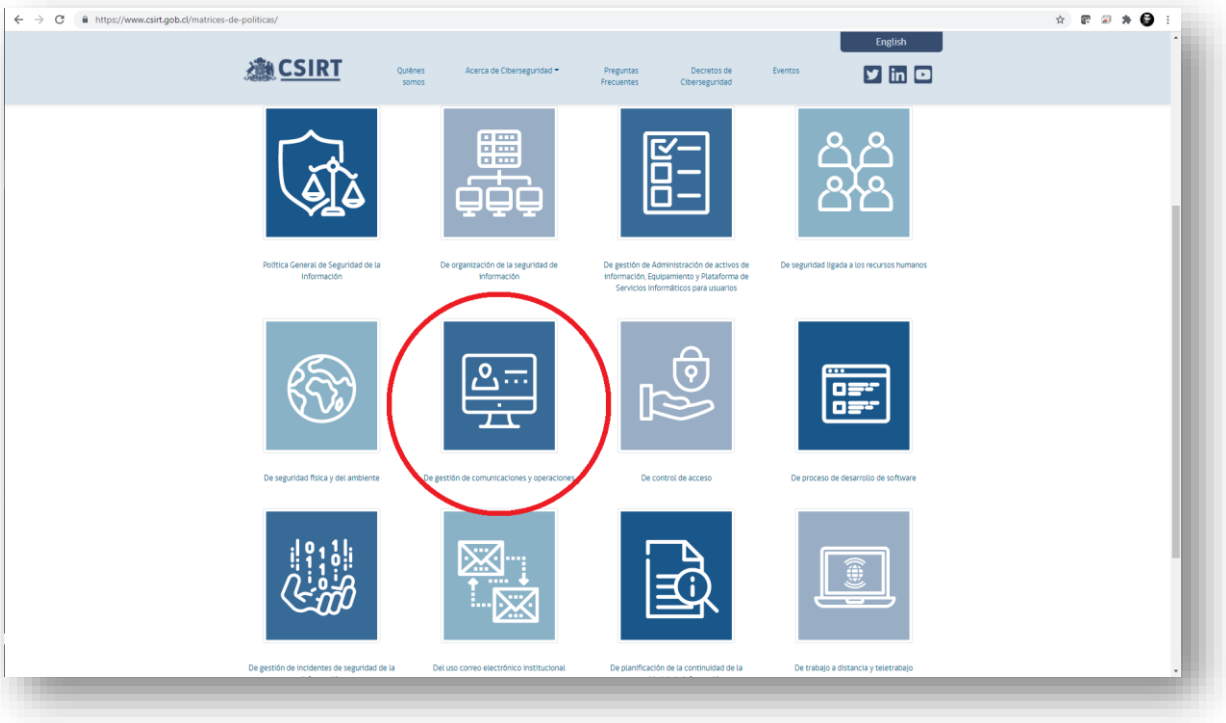
El control: Instalación de Software en Sistemas Operacionales

Se deben implementar los procedimientos para controlar la instalación de software en los sistemas operacionales.

Recomendaciones generales

Se deebn 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[13].



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

Se deberá considerar las siguientes pautas para controlar los cambios de software en los sistemas operacionales:

a) la actualización del software operacional, las aplicaciones y las bibliotecas de programas solo la deberán realizar administradores capacitados luego de obtener la autorización correspondiente de la dirección (ver directiva 9.4.5 Nch-ISO-27002);

b) los sistemas operacionales solo deberán tener un código ejecutable aprobado y no un código de desarrollo o compiladores;

c) las aplicaciones y el software de sistema operativo solo se deberán implementar después de realizar pruebas exhaustivas y exitosas; las pruebas deberán cubrir la capacidad de uso, la seguridad, los efectos en otros sistemas y la facilidad de uso para los usuarios en sistemas independientes (ver directiva 12.1.4 Nch-ISO-27002); es necesario asegurarse de que todas las bibliotecas de fuentes de programas correspondientes se han actualizado;

d) se deberá utilizar un sistema de control de configuración para mantener el control de todo el software implementado, así como también la documentación del sistema;

e) deberá existir una estrategia de reversión antes de que se implementen los cambios;

f) se deberá mantener un registro de auditoría de todas las actualizaciones a las bibliotecas de programas operacionales;

g) se deberá retener las versiones anteriores del software de aplicación como medida de contingencia;

h) se deberá archivar las versiones antiguas de software, junto con toda la información, los parámetros, los procedimientos y los detalles de configuración necesarios que soportan al software mientras que se mantienen los datos en el archivo.

Se deberá mantener el software suministrado por proveedores que se utiliza en los sistemas operacionales a un nivel al que preste soporte el operador. Con el tiempo, los proveedores de software dejarán de prestar soporte a las versiones anteriores de software. La organización deberá considerar los riesgos de utilizar software sin soporte.

Cualquier decisión de actualizar a una nueva versión deberá considerar los requisitos del negocio para el cambio y la seguridad de la versión, es decir, la introducción de nuevas funcionalidades de seguridad de la información o la cantidad y la gravedad de los problemas de seguridad de la versión que afectan a esta nueva versión. Se deberá aplicar parches de software cuando pueden ayudar a eliminar o reducir las debilidades de la seguridad de información (ver directiva 12.6 Nch-ISO-27002).

Solo se deberá dar acceso físico o lógico a los proveedores para fines de soporte cuando sea necesario y con la aprobación de la dirección. Se deberán monitorear las actividades del proveedor (ver directiva 15.2.1 Nch-ISO-27002).

El software informático puede utilizar software y módulos suministrados de manera externa, los que se deberán monitorear y controlar para evitar cambios no autorizados y que pueden introducir falencias en la seguridad.

La institución debe restringir los privilegios de instalación de cualquier aplicativo en los servidores, equipos de comunicaciones, equipos de seguridad u otro dispositivo conectado a la red, permitiendo que solo personal especializado, por ejemplo: los administradores o personal de implantación, en caso de servidores, equipos de seguridad y comunicaciones; y de soporte técnico, sea este interno o externo, en caso de estaciones de trabajo.

- Si la instalación que se requiere hacer en servidores productivos, es de algún aplicativo o sistema desarrollado, debe contar con un procedimiento adecuado de implantación. Las buenas prácticas de desarrollo seguro y de administración de plataforma indican que quien actualiza, implementa un aplicativo o sistema debe tener un rol distinto al de administrador (cumpliendo el control de segregación funcional), Para esto, si la estructura funcional lo permite, la implementación de software la desarrolla un rol de implantador, el cual se dedica exclusivamente a instalar software, actualizaciones u otros en producción, siguiendo además las reglas relacionadas con control de cambios y velando que la tarea a realizar cuente con todas las pruebas (seguridad, funcionalidad) y las autorizaciones respectivas. Siguiendo con esta práctica, el administrador supervisa que las tareas realizadas por el implantador sean hechas en forma adecuada, siguiendo los pasos de la guía o procedimiento de implantación.

- Por el contrario, si la instalación se requiere hacer a nivel de estaciones de trabajo, solo personal de soporte técnico podrá realizar esta labor.

Todas las acciones asociadas a la instalación de un producto, sistema, aplicativo, parche de actualización, etc., debe quedar registrada a través de los logs de auditoria y registros de eventos de sistema. Estos registros deben ser almacenados en forma segura y centralizada.

Se recomienda que la Institución tenga registro de todos los sistemas operativos, aplicaciones o sistemas instalados tanto en la plataforma de servidores, equipos de comunicaciones y seguridad, como también en estaciones de trabajo, formulando listas blancas (software autorizado) y listas negras (software no permitido en la institución). Estas listas deberán incluir que versiones se encuentran instaladas, esto con el objeto de vigilar el riesgo de obsolescencia del software instalado.

Además, se recomienda que la Institución tenga un repositorio con todos los sistemas operativos, software de base de datos, aplicativos específicos, códigos fuentes, etc., en forma centralizada.

Si existieran aplicativos que deban ser implementados por proveedores, se debe establecer protocolos de trabajo para tales efectos, tomando todos los resguardos necesarios para evitar problemas en la plataforma tecnológica y registrando todas las acciones a través de logs de auditoria y registros de eventos.

Algunas evidencias requeridas para validar cumplimiento:

- Lista de aplicativos permitidos en la institución y de aquellos que no están autorizados. Este listado debe incluir versiones.
- Evidencia de implantación de aplicaciones.
- Evidencia de actualizaciones.
- Evidencia (en caso de ocurrir) de protocolo de trabajo establecido con proveedores.

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[14] como en el CSIRT de Gobierno[15] (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.

[14] https://digital.gob.cl/
[15] https://www.csirt.gob.cl/

Anexo I: Ejemplo de estructura de Políticas y Procedimientos