20 de Julio de 2021
Ficha N° 4 A.8.1.1
CSIRT DE GOBIERNO

Ficha de Control Normativo A.8.1.1

Inventarios de Activos

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 presente relativo al Instructivo Presidencial N°8 / 2018[2], el Decreto Supremo N°83 / 2005[3], el Decreto Supremo N°93 / 2006[4], el Decreto Supremo N°1 de 2015[5] y a la Nch-ISO IEC 27001[6].

[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=1078308
[6] https://ecommerce.inn.cl/nch-iso-iec-27001202078002

II. ACTIVOS DE INFORMACIÓN

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 de Administración de Activos, que permita a los funcionarios acercarse e internalizar los conceptos para aplicarlos de manera transversal en su quehacer diario.

Una organización debería identificar los activos pertinentes en el ciclo de vida de la información y documentar su importancia. El ciclo de vida de la información debería incluir su creación, procesamiento, almacenamiento, transmisión, eliminación y destrucción. Se debería mantener la documentación en inventarios dedicados o existentes según corresponda.

El inventario de activos debería ser preciso, actualizado, coherente y acorde a otros inventarios. Para cada uno de los activos identificados, se debería asignar su propiedad (ver A.8.1.2 Nch-ISO/IEC 27002:2013) y clasificación. (Ver A.8.2 Nch-ISO/IEC 27002:2013).

La información que se produce, procesa, transmite, almacena y los medios físicos utilizados por la Institución y sus funcionarios, es de propiedad de la Institución y su custodia y protección será de responsabilidad del dueño del proceso que se vincule con dicha información. Con relación a los datos contenidos en medios administrados por la unidad TIC o equivalente, esta unidad estará a su cargo y resguardo. Sin embargo, los accesos y usabilidad de la información, en las Unidades usuarias, son de responsabilidad de los dueños de los procesos y trabajadores que la acceden, los que deberán quedar formalmente establecidos en documentos de control de proyectos.

Los activos asociados a la información y a las instalaciones de procesamiento de la información deben ser identificados por cada Unidad a cargo y se debe mantener un inventario de dichos activos.

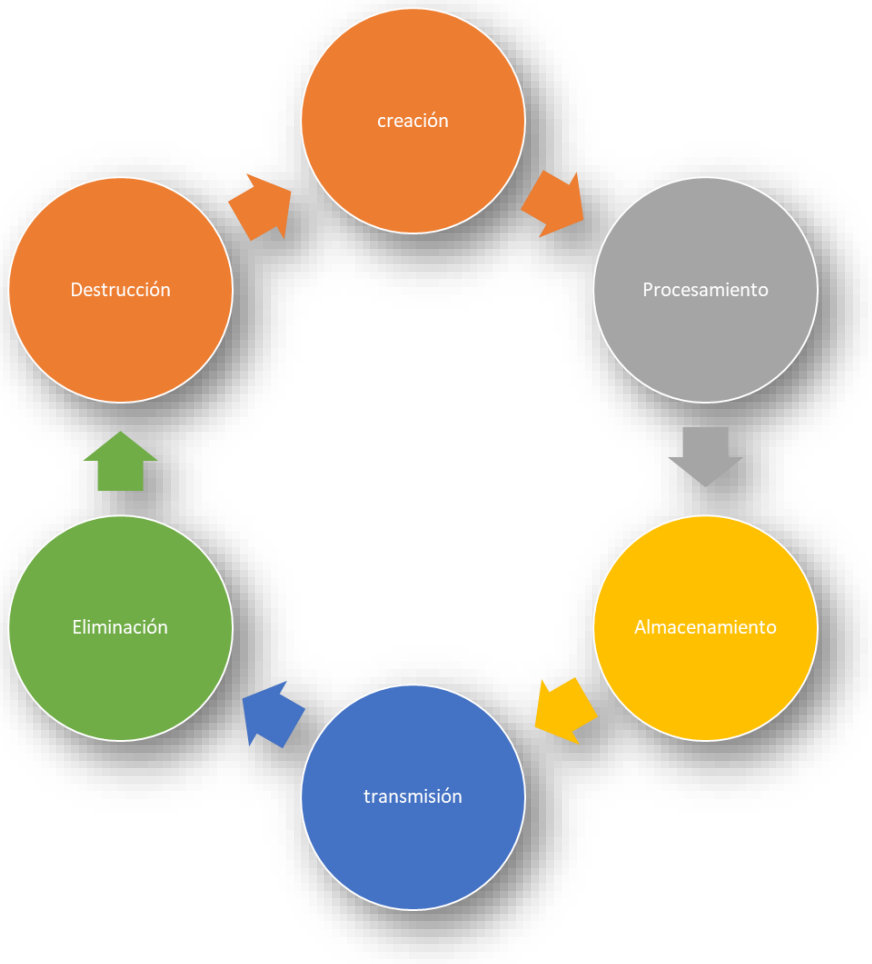
La información y campos que debe contener este inventario son:

- Código (Id) del activo: en el caso de ser un activo inventariable, identificar el código asignado por el departamento de Administración.
- Nombre del activo: Nombre operativo o comercial del activo.
- Tipo de activo: clasificación del activo, los utilizados son: software, sistema, equipos, documento, infraestructura, formulario, base de datos, y otros.

- Ubicación: identificación del lugar físico que aloja al activo o lógico, en caso de ser un software, sistema y/o base de datos.
- Fecha de creación: Fecha con el cual el activo fue creado o recibido.
- Definición de propietario.

El inventario debe estar automatizado y disponible en tiempo real para ser auditado por terceras partes interna o externas debidamente autorizadas.

Deberán emitirse informes mensuales que den cuenta del estado de los inventarios de los activos tecnológicos, que den cuenta de las existencias, corroborar sus parámetros certificando su asignación y su efectiva existencia en bodega.



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

III. RECOMENDACIONES Y MEJORES PRÁCTICAS ASOCIADAS AL CONTROL

El control:

Los activos asociados a la información y las instalaciones de procesamiento de la información deben ser identificados y se deben mantener y realizar un inventario de dichos activos.

Recomendaciones generales

Se recomienda hacer un levantamiento de todos los activos de información institucionales y luego clasificarlos en diversas categorías, por ejemplo: Documentos físicos, Activos Electrónicos (archivos digitales, bases de datos, códigos fuente, entre otros), Plataforma Base (PC, Servidores, Sistema Operativo, Ofimática, Motores de Bases de Datos, Software Antimalware, entre otros), Infraestructura de Soporte al Giro (equipos de comunicaciones, impresoras, Datacenter, Aire Acondicionado, Edificio o Instalaciones, entre otros), y en particular, las personas que integran la institución.

Sobre este listado, se deben realizar los análisis respectivos de riesgos y tomar las medidas adecuadas de protección.

En el caso de que la institución cuente con activos de información de terceros (personas, equipamiento en arriendo, bases de datos de terceros, etc.), deberá mantener este catastro en otra lista, la cual debe considerar datos adicionales tales como a quien pertenece, contrato de arriendo, ubicación, fecha de término de contrato, etc. El tratamiento de los riesgos para estos activos de terceros, corresponde al dueño del activo en cuestión.

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[7].

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

Algunas evidencias requeridas para validar cumplimiento

- Inventario de activos de Información Institucionales.
- Inventario de activos de terceros, utilizados por la institución.
- Análisis de riesgos sobre los activos de información institucionales.
- Declaración de cobertura del inventario de activos de la información (listado de áreas o procesos que se consideran en el inventario de activos en el período en análisis y de otros que se abordarán en otros períodos).

Responsable del Control

Encargados departamentales/división, en conjunto con el Encargado de Ciberseguridad y/o Seguridad de la Información.

Recomendaciones específicas

Se sugiere que al menos considere estos ámbitos de acción que inciden directamente en una buena administración de los activos de información institucional:

- Inventario de la información
    - Elaborar un inventario detallado de los activos de información de su empresa.
- Criterios de clasificación de la información

- Determinar claramente los criterios de seguridad con los que clasificará los activos de información de su empresa.

- Clasificación de la información
  - Etiquetar los activos de información según los criterios de seguridad establecidos.
- Tratamientos de seguridad disponibles
  - Establecer una lista con todos los tratamientos de seguridad de la información disponibles en su empresa.
- Establecer y aplicar los tratamientos que corresponden a cada tipo de información
  - Aplicar correctamente los tratamientos de seguridad que corresponden a cada activo información.
- Auditorías
  - Realizar auditorías de comprobación cada cierto tiempo de manera regular y eventualmente en modalidad aleatoria.

Si tiene alguna necesidad específica no dude en contactar al Equipo de Comunicaciones del CSIRT para averiguar si existe materia sobre algún tema específico de ciberseguridad, si existe lo guiarán para que pueda acceder a él y distribuirlo en su institución o bien si existe la disponibilidad de recursos se podría desarrollar y disponibilizar para la comunidad.

Estudie las múltiples opciones y recomendaciones para avanzar en la implementación de este control y 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[8] como en el CSIRT de Gobierno[9] (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.

[8] https://digital.gob.cl/
[9] https://www.csirt.gob.cl/

Anexo I: Ejemplo de estructura de Políticas y Procedimientos