5 de Julio de 2021
Ficha N° 1 A.5.1.1
CSIRT DE GOBIERNO

Ficha de Control Normativo A.5.1.1

Políticas para la seguridad de la información

I. CONTEXTO

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].

Por tanto estas directrices no reemplazan el análisis de riesgo institucional, pero 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].

II. INTRODUCCIÓN

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

[1] https://www.auditoriainternadegobierno.gob.cl/wp-content/upLoads/2018/10/DOCUMENTO-TECNICO-N-107-MODELO-DE-MADUREZ.pdf
[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

administrar sus objetivos de seguridad de la información. Las políticas de seguridad de la información deberían abordar al menos las siguientes fuentes de requisitos:

- estrategia de negocio;
- normativas, legislación y contratos;
- el entorno de amenazas a la seguridad actual y proyectada.

La política de seguridad de la información debería, en consecuencia, tener planteamientos respecto a lo siguiente:

- definición de la seguridad de la información, los objetivos y principios para guiar a todas las actividades relacionadas con la seguridad de la información;
- asignación de responsabilidades generales y específicas para la administración de la seguridad de la información de acuerdo a los roles definidos;
- procesos para manejar desviaciones y excepciones.

A un nivel inferior o un poco más operativo, la política de seguridad de la información se debería respaldar por políticas específicas de un tema, dominio, ámbito o grupo de problemáticas agrupables, que estipule la implementación de controles de seguridad de la información y que típicamente se estructuran para abordar las necesidades de ciertos grupos objetivo dentro de una organización.

Algunos ejemplos de temas de políticas específicas:

a) control de accesos (ver cláusula 9 – Nch-ISO IEC 27002);
b) clasificación de la información (y manejo) (ver 8.2 - Nch-ISO IEC 27002);
c) seguridad física y ambiental (ver cláusula 11 - Nch-ISO IEC 27002);
d) temas orientados al usuario final como:
    - uso aceptable de activos (ver 8.1.3 - Nch-ISO IEC 27002);
    - escritorio despejado y pantalla despejada (ver 11.2.9 - Nch-ISO IEC 27002);
    - transferencia de información (ver 13.2.1 - Nch-ISO IEC 27002);
    - dispositivos móviles y teletrabajo (ver 6.2 - Nch-ISO IEC 27002);
    - restricciones sobre las instalaciones y el uso de software (ver 12.6.2 - Nch-ISO IEC 27002);
e) respaldo (ver 12.3 - Nch-ISO IEC 27002);
f) transferencia de información (ver 13.2 - Nch-ISO IEC 27002);
g) protección contra malware (ver 12.2 - Nch-ISO IEC 27002);
h) administración de vulnerabilidades técnicas (ver 12.6.1 - Nch-ISO IEC 27002);
i) controles criptográficos (ver cláusula 10 - Nch-ISO IEC 27002);
j) seguridad en las comunicaciones (ver cláusula 13 - Nch-ISO IEC 27002);

k) privacidad y protección de información personal identificable (ver18.1.4 - Nch-ISO IEC 27002);
l) relaciones con los proveedores (ver cláusula 15 - Nch-ISO IEC 27002).

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

III. RECOMENDACIONES Y MEJORES PRÁCTICAS ASOCIADAS AL CONTROL

El control:

Las instituciones deben definir un conjunto de políticas para la seguridad de la información y las debe aprobar la dirección para publicarla y comunicarla a los empleados y a todas las partes externas pertinentes.

Recomendaciones generales

Las instituciones, en el proceso de implementación de los requisitos de la norma NCH-ISO IEC 27001:2013 y NCH-ISO IEC 27002:2013, deben identificar sus requisitos de seguridad.

Existen tres fuentes principales de requisitos de seguridad:

- La evaluación de los riesgos para la organización, considerando la estrategia y los objetivos generales de la organización. Las amenazas a los activos se identifican a través de una evaluación de riesgos, se evalúa además la vulnerabilidad y la probabilidad de ocurrencia y se estima su posible impacto;
- Los requisitos legales, estatutarios, normativos y contractuales que una organización, sus socios comerciales, contratistas y proveedores de servicio deberían satisfacer y su entorno sociocultural;
- El conjunto de principios, objetivos y requisitos comerciales para el manejo, el procesamiento, el almacenamiento, la comunicación y el archivado de la información que ha desarrollado una empresa para apoyar a sus operaciones.

Además, debe identificar y seleccionar aquellos controles de la norma NCH-ISO 27001:2013, que pueden ser aplicables en la institución, descartando aquellos que, por razones estratégicas, legales, operacionales o tecnológicas, no puedan ser implementados.

Los controles se pueden seleccionar a partir de esta norma o de otros conjuntos de controles[7][8][9][10], o bien se pueden diseñar nuevos controles para cumplir con las necesidades específicas según sea necesario.

La selección de los controles depende de las decisiones organizacionales en base a los criterios para la aceptación de riesgos, las opciones de tratamiento de riesgos y el enfoque de administración general de riesgos que se aplica a la organización y también estará sujeta a toda la legislación y normativas nacionales e internacionales pertinentes. La selección del control también depende de la forma en que interactúan los controles para brindar protección en profundidad.

Una vez seleccionados los controles, se debe crear un Documento de Aplicabilidad (SoA por su sigla en inglés), en el cual se detalle qué controles serán aplicados en la organización y aquellos que serán descartados, agregando para estos últimos, las justificaciones que sean requeridas.

El Documento de Aplicabilidad, en conjunto con la Política de Seguridad de la Información, deberán ser revisadas al menos una vez al año, para verificar su validez y que contenga todos aquellos aspectos de tratamiento y protección de los Activos de Información de la Institución.

Se recomienda en forma adicional, la incorporación de un Procedimiento de Gestión de la Seguridad de la Información, el cual apoye la gobernabilidad del Sistema de Gestión de Seguridad de la Información, establezca la composición y funcionamiento del Comité de Seguridad de la Información, métricas de gestión, evaluaciones de terceros, entre otros aspectos.

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].

Algunas evidencias requeridas para validar cumplimiento:

Primera fase: Implementación.

- Oficio o resolución o documento equivalente que declare la aprobación de Política de Seguridad y del Documento de Aplicabilidad (SoA).
- Notificación oficial al personal institucional y a terceras partes interesadas (proveedores, otras instituciones, entre otros).

[7] https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
[8] https://cloudsecurityalliance.org/research/cloud-controls-matrix/
[9] https://www.nist.gov/cyberframework
[10] https://www.inn.cl/
[11] https://www.csirt.gob.cl/matrices-de-politicas/

- Oficio que nombre al Encargado de Ciberseguridad, incluyendo a su subrogante, en modalidad de atención 7x24, y la constancia de notificación al CSIRT de Gobierno.

Segunda fase en adelante: Operación.

- Validación de la vigencia de la Política de Seguridad de la Información y del Documento de Aplicabilidad.
- Revisión y modificaciones hechas a la política (si aplica).
- Actas de sesiones de Comité de Seguridad de la Información.

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[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 no dude en consultarnos a 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