8 de Julio de 2021
Ficha N° 2 A.6.1.1
CSIRT DE GOBIERNO

Ficha de Control Normativo A.6.1.1

Organización de la Seguridad de la Información

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].

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].

[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

II. ORGANIZACIÓN DE LA SEGURIDAD DE LA 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.

La asignación de las responsabilidades de seguridad de la información se debería hacer de acuerdo con las políticas de seguridad de la información (ver A.5.1.1). Se deberían identificar las responsabilidades para la protección de activos individuales y para realizar procesos de seguridad de la información. Se deberían definir las responsabilidades para las actividades de administración de riesgos de seguridad de la información y en particular para la aceptación de riesgos residuales. Estas responsabilidades se deberían complementar, donde sea necesario, con orientación más detallada para los sitios específicos y las instalaciones de procesamiento de información. Se deberían definir las responsabilidades para la protección de activos para realizar procesos de seguridad de la información.

Las personas asignadas con responsabilidades de seguridad de la información pueden delegar las tareas de seguridad a otros. Sin embargo, siguen siendo responsables y deberían determinar que cualquier tarea delegada se haya realizado correctamente.

Se deberían indicar las áreas por las que las personas son responsables. En particular, debería ocurrir lo siguiente:

a) se deberían definir e identificar los actives y los procesos de seguridad de la información;
b) se debería asignar a la entidad responsable de cada activo o proceso de seguridad de la información y se deberían documentar los detalles de la responsabilidad (ver cláusula 8.1.2 de la Nch-ISO/IEC 27002:2013);
c) se deberían definir y documentar los niveles de autorización;
d) para poder cumplir con las responsabilidades en el área de seguridad de la información, las personas asignadas deberían ser competentes en el área y deberían contar con oportunidades para mantenerse al día en los desarrollos;
e) se debería identificar y documentar la coordinación y la supervisión de los aspectos de seguridad de la información de las relaciones con los proveedores.

Muchas organizaciones asignan a un rol estratégico a la dirección de seguridad de la información para tomar la responsabilidad general del desarrollo y la implementación de la seguridad de la información

y para apoyar la identificación de controles. En el caso de las instituciones públicas deben encausar este requisito bajo las directivas del Decreto Supremo N°83, artículo 12, y el Instructivo presidencial N°8 de 2018.

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 establecer un marco de administración para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.

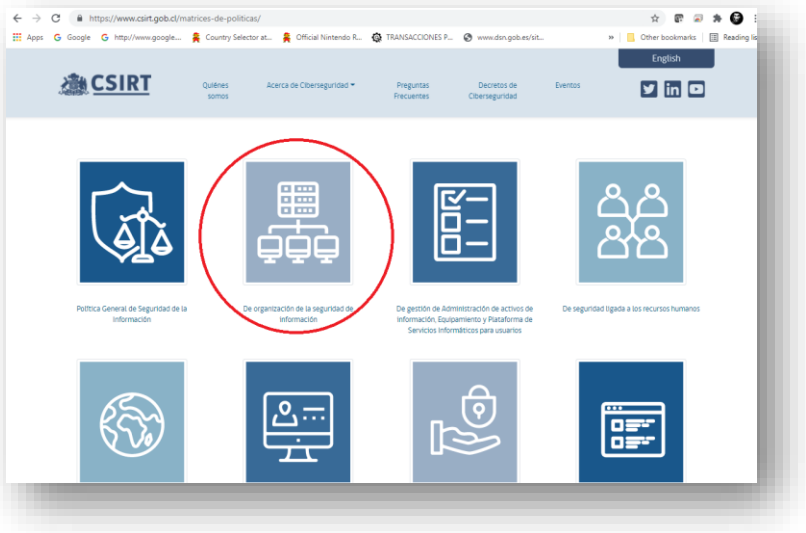
Recomendaciones generales

De acuerdo con los requisitos de cumplimiento de la norma NCH-ISO/IEC 27001, los cuales serán declarados en la Política General de Seguridad de la Información Institucional, se deberán establecer los deberes y derechos de todos los que trabajarán en forma directa por el cumplimiento de estas políticas y la protección adecuada de los activos de información. Además, se deberá implementar en los descriptores de cargo de todo el personal institucional, sus propios listados de deberes y derechos respecto a la Seguridad de la Información, utilizando para ello, el criterio de "Necesidad de Conocer".

En los contratos con proveedores, también deberán ser agregados los requisitos de cumplimiento de los aspectos de seguridad de la información, a nivel del contrato institución-empresa, y con el personal externo permanente o transitorio.

Además, se hace necesario el establecimiento de acuerdos de confidencialidad para el personal interno y de proveedores.

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

- Listados de deberes y derechos relacionados con la seguridad de la información para el personal interno de la institución.

- Declaración de obligaciones del rol de Encargado de Ciberseguridad y/o Seguridad de la Información, del subrogante y de los miembros del Comité de Seguridad de la Información.

Responsable del Control

Recursos Humanos. Encargado de Ciberseguridad y/o Seguridad de la Información.

Recomendaciones específicas

Se sugiere que se evalúen caso a caso al menos los siguientes roles y responsabilidades:

Alta Dirección Institucional:

Rol:

- Supervisión General.

Responsabilidad:

- Aprobar y comunicar la Política de Seguridad de la Información.
- Supervigilar que las estrategias definidas por el Comité, para el control asociado a los activos de información, estén en concordancia con las políticas institucionales de seguridad de la información y los objetivos del negocio.

Comité de Riesgos y Seguridad de la Información:

Rol:

- Supervisión y Coordinación de Decisiones.

Responsabilidad:

- Proponer las definiciones estratégicas, lineamientos y prioridades, así como también los recursos e insumos, que permitan orientar y focalizar las políticas, planes, programas e iniciativas en materias de Seguridad de la Información.
- Definir roles y las responsabilidades de todo el personal involucrado, incluyendo además colaboradores y terceras personas en materia de Seguridad de la información.
- Evaluar y seleccionar materias a incorporar en la Política de Seguridad de la Información.

- Impulsar y proponer al Jefe de Servicio las políticas y directrices definidas en materia de seguridad de la información.
- Apoyar y promover la seguridad de la información dentro de la empresa, mediante la difusión, educación y concientización sobre las Políticas y otras medidas de seguridad.
- Coordinar, supervisar y monitorear la implementación de las Políticas y procedimientos de la seguridad de la información.
- Coordinar los esfuerzos con las diferentes Divisiones, Departamentos, Servicios y todos los grupos interés de la empresa que tengan responsabilidades sobre la seguridad de la información.
- Analizar, evaluar y priorizar las estrategias de tratamiento de riegos en la Seguridad de la Información.
- Asegurar la protección de los activos de información en la empresa.
- Reportar al [Directorio], el resultado de la implementación de la Política, de los Riesgos, y de las medidas de administración de la Seguridad de la Información.
- Aprobar los aspectos operativos de la implementación del Sistema de Gestión de Seguridad de la Información.
- Definir los mecanismos a través de los cuales se implementará el alcance de la Política General de Seguridad.
- Delimitar las responsabilidades de todo el personal involucrado, incluyendo además colaboradores y terceras partes.
- Sesionar periódicamente, o cuando fuese necesario, conforme a la planificación anual definida por el Comité de Riesgo y comunicada según las instancias establecidas.
- Gestionar la actualización de las Políticas tanto General como Específicas.
- Gestionar la actualización de los Procedimientos, Guías, Protocolos y todos los documentos auxiliares que fueren necesarios para el mejor despliegue, comprensión y aplicabilidad de las directrices superiores.

<u>Encargado de Ciberseguridad de Alto Nivel (Titular y Subrogante):</u>

Rol:

- Supervisión de alto nivel.

Responsabilidad:

- Ser el responsable de la seguridad informática en el servicio.
- Proponer al Comité de Riesgos y Seguridad de la Información las debidas respuestas y posible priorización de medidas de tratamiento de incidentes y riesgos vinculados a los activos de información de los procesos institucionales y sus objetivos de negocio.

- Identificar las amenazas o riesgos en la seguridad de la información o de sus instalaciones.
- Coordinar las actividades relativas a la seguridad de la información con el Comité de Riesgos y Seguridad de la Información.
- Coordinar con las distintas unidades del Servicio las acciones tendientes a cumplir y apoyar los objetivos de seguridad de la información.
- Mantener historial de versiones de las Políticas institucionales en la materia.
- Desarrollar políticas, estándares, procesos y directrices para asegurar la seguridad física y electrónica de sistemas automatizados. Asegurar que la política y los estándares de administración de seguridad son adecuados para el propósito, están actualizados y están implementados correctamente. Revisar nuevas propuestas de negocio y proveer asesoramiento especializado en temas e implicaciones de seguridad.
- Monitorear la aplicación y el cumplimiento de procedimientos de administración de seguridad y revisar sistemas de información para detectar infracciones reales o potenciales en la seguridad. Asegurar que todas las infracciones de seguridad identificadas se investigan rápidamente y en profundidad y que cualquier cambio al sistema requerido para mantener la seguridad sea implementado. Asegurar que los registros de seguridad son precisos y están completos y que las solicitudes de soporte se abordan de conformidad con los estándares y procedimientos establecidos. Contribuir a la creación y el mantenimiento de políticas, estándares, procedimientos y documentación de seguridad.
- Mantener los procesos de administración de la seguridad y comprobar que todas las solicitudes de soporte sean tratadas conforme a procedimientos acordados. Proveer orientación para definir derechos y privilegios de acceso. Investigar las infracciones de seguridad de conformidad con procedimientos establecidos, recomendar acciones requeridas y soportar/hacer seguimiento para asegurar que sean implementadas.
- Investigar infracciones de seguridad menores conforme a los procedimientos establecidos. Asistir a los usuarios en la definición de sus derechos y privilegios de acceso. Ejecutar tareas de administración de seguridad no estándares y resolver asuntos relacionados con la administración de la seguridad.
- Recibir y responder a solicitudes rutinarias de soporte en materia de seguridad. Mantener registros y asesorar a las personas relevantes sobre las acciones tomadas. Asistir con la investigación y resolución de asuntos relacionados con los controles de acceso y los sistemas de seguridad.
- Ejecutar tareas simples de administración de seguridad. Mantener documentación y registros relevantes.

Jefes de División:

Rol:

- Implementación de las medidas de la seguridad de la información.

Responsabilidad:

- Apoyar y promover la Política de Seguridad de la información dentro de la empresa, mediante la difusión, educación y concientización sobre la Políticas y otras medidas de seguridad.
- Cumplir con los requerimientos que el Comité de Riesgos y Seguridad de la Información efectúe a las unidades.
- Construir las directrices de mapas de procesos a implementar en los Servicios de la Institución.

Jefe de Departamento de Estrategia Planificación y Control de Gestión:

Rol:

- Monitorear el avance de las medidas de seguridad.

Responsabilidad:

- Realizar seguimiento al avance general y los resultados de la implementación de las estrategias de tratamiento y control de los riesgos de la seguridad de la información.
- Reportar al Comité de Riesgos y Seguridad de la Información los resultados del control efectuado sobre las medidas de tratamiento y los riesgos de la seguridad de la información.
- Recopilar la información de los Servicios y Unidades de la empresa.
- Controlar el inventario o registro de activos de información debidamente coordinado con los responsables: división, departamento, unidad y programa.

Jefe de Auditoría Interna:

Rol:

- Evaluar y mejorar la eficiencia de los procesos de gestión de riesgos, control y gobierno.

Responsabilidad:

- Asegurar la implementación de la Política de Seguridad de la Información en la Empresa.
- Verificar y evaluar el cumplimiento de las medidas de tratamiento de Riesgos en la Seguridad de la Información comprometidas con el Comité de Riesgos y Seguridad de la Información.
- Reportar el resultado de las evaluaciones al [Directorio] y al Comité de Riesgos y Seguridad de la Información.
- Evaluar el cumplimiento el avance de cada una de las etapas de la implementación del Sistema de Seguridad de la Información (SSI).

- Evaluar en forma permanente los controles internos establecidos por la Administración y recomendar medidas que signifiquen una mejora.
- Cooperar en la adopción de mecanismos de autocontrol en las Unidades operativas del Servicio.
- Verificar que los sistemas de información aplicados en la empresa generen productos confiables, oportunos y veraces.
- Velar por que las políticas y actividades de la Unidad de Auditoría Interna sean coherentes con aquellas emanadas de la autoridad.
- Remitir los informes de auditoría al [Directorio], advirtiendo sobre eventuales riesgos detectados, que requieran acciones correctivas o rectificaciones por parte del Servicio.
- Efectuar seguimientos de las medidas preventivas y correctivas emanadas de los informes de auditoría aprobados por la Autoridad.
- Participar en el Comité de Auditoría Ministerial.
- Apoyar la operación del Proceso de Gestión de Riesgos en el Servicio y cumplir con las responsabilidades establecidas para la Unidad.

Jefe División Jurídica:

Rol:

- Asesoría jurídica.

Responsabilidad:

- Asesorar al Comité de Riesgos y Seguridad de la Información en materias jurídicas relacionadas con la implementación de la Política de Seguridad de la Información y evaluar la legalidad de los actos que de ésta demande.
- Asegurar la incorporación de los requisitos del Sistema de Seguridad de la información, en las diferentes celebraciones de contratos y servicios.
- Efectuar el control jurídico de los actos administrativos que realizan las unidades organizacionales dependientes de la empresa.
- Revisar e informar las investigaciones internas que se instruyan por orden de las autoridades.

Jefe [Unidad responsable de Ciberseguridad]:

Rol:

- Coordinación y rol operativo.

Responsabilidad:

- Asesorar el diseño, elaboración, desarrollo, implementación, mantenimiento y actualización de planes estratégicos y acciones tendientes a otorgar seguridad a los activos de información.
- Implementar la Política General de Seguridad de la Información.
- Implementar las Políticas específicas de Seguridad de la Información.
- Implementar políticas, procedimientos, guías, protocolos, estándares, procesos y directrices para asegurar la seguridad física y lógica de sistemas automatizados. Asegurar que la política y los estándares de administración de seguridad son adecuados para el propósito, están actualizados y están implementados correctamente. Revisar nuevas propuestas de negocio y proveer asesoramiento especializado en temas e implicaciones de seguridad.
- Coadyuvar al Encargado de Ciberseguridad al monitoreo del cumplimiento de las Políticas y Procedimientos de seguridad de la Información.
- Coadyuvar a las instancias de auditoría para que puedan materializarse con las condiciones óptimas que permitan obtener conclusiones relevantes para la empresa en materia de cumplimiento de políticas y normas, así como en el cumplimiento de las metas establecidas por la gestión del riesgo institucional.
- Liderar el desarrollo técnico de los Planes de Continuidad Operacional Institucional (BCP por sus siglas en inglés) y los planes de recuperación ante desastres (DRP por sus siglas en inglés).
- Establecer una coordinación con el Encargado de Ciberseguridad para que el desarrollo de las políticas y su implementación converjan en soluciones viables, sustentables, eficaces y eficientes tanto técnica como económicamente.
- Impulsar la implementación de sistemas de monitorear del cumplimiento de procedimientos de administración de seguridad y revisión de sistemas de información para detectar infracciones reales o potenciales en la seguridad.
- Aportar toda la evidencia que permita que todas las infracciones de seguridad identificadas sean investigan rápidamente y en profundidad y que cualquier cambio al sistema requerido por la empresa para mantener la seguridad sea implementado.
- Proveer sistemas que permitan asegurar que los registros de seguridad son precisos y están completos y que las solicitudes de soporte se abordan de conformidad con los estándares y procedimientos establecidos.
- Contribuir a la creación y el mantenimiento de políticas, estándares, procedimientos y documentación de seguridad.
- Implementar procesos de administración de la seguridad y comprobar que todas las solicitudes de soporte sean tratadas conforme a procedimientos acordados.
- Implementar las directrices sobre derechos y privilegios de acceso.
- Colaborar en la Investigación de las infracciones de seguridad de conformidad con procedimientos establecidos, adoptar las recomendaciones sugeridas, manteniendo el debido seguimiento para asegurar que sean implementadas.

- Investigar desde la dimensión operativa y técnica, infracciones a la seguridad menores conforme a los procedimientos establecidos. Apoyar a los usuarios en la configuración de sus derechos y privilegios de acceso.
- Recibir y responder a solicitudes rutinarias de soporte técnico en materia de seguridad. Mantener registros y asesorar técnicamente a las personas relevantes sobre las acciones tomadas. Asistir con la investigación y resolución de asuntos relacionados con los controles de acceso y los sistemas de seguridad.

Jefe Departamento de Desarrollo y Gestión de Personas:

Rol:

- Coordinación y operativo.

Responsabilidad:

- Informar y notificar al personal que ingrese a la empresa sobre sus obligaciones respecto del cumplimiento de la Política General de Seguridad de la Información y de todas las normas, procedimientos y prácticas aplicadas en la [Empresa XXX]. Informar a la [Unidad responsable de Ciberseguridad] sobre el personal contratado, a efecto de protocolizar, identificar o designar el perfil de usuario del personal ingresado. Se deberá procurar que la entrega de esta información sea automatizada y en tiempo real con el objetivo de disminuir los riesgos de ciberseguridad vinculados a estos casos.
- Informar oportunamente a la [Unidad responsable de Ciberseguridad] acerca de los movimientos del personal para la creación, cambios de estado o eliminación de cuentas de correo institucionales. Se deberá procurar que la entrega de esta información sea automatizada y en tiempo real con el objetivo de disminuir los riesgos de ciberseguridad vinculados a estos casos.
- Avisar oportunamente a la [Unidad responsable de Ciberseguridad] en el caso de modificación de las funciones de un funcionario o empleado de planta, contrata u honorarios, para realizar un análisis de los derechos de accesos a la información actual que posee el usuario en cuestión y se retiran permisos de acceso a la información o se otorgarán nuevos derechos propios de la función asumida, según requiera su Jefatura. Se deberá procurar que la entrega de esta información sea automatizada y en tiempo real con el objetivo de disminuir los riesgos de ciberseguridad vinculados a estos casos.
- Coordinar con la [Unidad responsable de Ciberseguridad] y el Departamento de Administración el ingreso, desvinculación o cambios del personal, para resguardar o recuperar la información de bienes que se encuentran a su cargo y los privilegios de acceso de información.

- Incorporación de la normativa vigente, que se refiera al Sistema de Seguridad de la información, en los actos administrativos y contratos. Las normas y política expresadas en esta resolución, se considerarán parte integrante y se adjuntarán a los decretos o resoluciones de nombramiento o contrataciones de personal, de planta, a contrata o sobre la base de honorarios.

Unidad de Coordinación de Ciberseguridad:

Rol:

- Coordinación de alto nivel

Responsabilidad:

- Materializar los aspectos encomendados por el Directorio en materia de Ciberseguridad.
- Recomendar políticas y normas.
- Promover e impulsar la Protección de las Infraestructuras Críticas.
- Favorecer el uso de protocolos y estándares de ciberseguridad en la empresa.
- Promover buenas prácticas en el funcionamiento del Equipo de Respuesta frente a Incidentes Informáticos de la empresa (CSIRT).
- Promover planes de capacitación, entrenamiento, difusión y educación en el marco de los objetivos planteados por el Directorio.

Responsable de la Información e Instalaciones de Procesos Institucionales:

Rol:

- Operativa Específica.

Responsabilidad:

- Custodiar, proteger o almacenar la información y activos, vinculados a determinado proceso Institucional.
- Definir el acceso a los activos de información y velar por su cumplimiento.

Trabajadores:

Rol:

- Obligación de conocimiento y cumplimiento.

Responsabilidad:

- Conocer y cumplir la Política de Seguridad de la Información vigente, entendiendo en ésta la General y Específicas.
- Utilizar adecuadamente los activos de información a su cargo.
- Utilizar adecuadamente la plataforma tecnológica, servicios informáticos, equipamiento y dispositivos institucionales.

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 no dude en consultarnos a 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