7 de Diciembre de 2021
Ficha N° 19 A.13.1.2
CSIRT DE GOBIERNO

Ficha de Control Normativo A.13.1.2

Seguridad de los servicios de red

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 Nch-ISO/IEC 27032.
- 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. La importancia de la red y la ciberseguridad

En general, las normas sobre privacidad y comunicaciones electrónicas tienen por objeto garantizar la privacidad, la confidencialidad y la protección de los datos personales de estas comunicaciones, en amparo de los derechos y libertades fundamentales de las personas físicas y jurídicas.

En este contexto, es importante incorporar el concepto de acuerdos de nivel de servicio ("Service Level Agreement", SLA). Un SLA es un contrato que describe el nivel de servicio que un cliente espera de su proveedor.

Existen diferentes tipos de SLA, según ITIL:

SLA de servicio:

Aplica un SLA estándar a todos los clientes que contratan un mismo servicio. Es útil cuando la institución ofrece varios servicios con tiempos de resolución y respuesta diferentes.

Por ejemplo, los servicios Premium y los servicios Estándar, los servicios tipo incidencias y los tipo consulta o cualquier distinción propia entre servicios.

SLA basado en el cliente:

Aplica a todos los servicios contratados por un mismo cliente, un grupo de clientes o una misma área de negocio.

Por ejemplo, puede determinar un tiempo límite de resolución de incidencias tipo "petición de presupuesto", y a la vez priorizar las que vengan del "departamento de finanzas" o de un cliente externo.

SLA multinivel:

Combina el SLA de servicio, tanto a nivel cliente como a nivel corporativo, para todos los usuarios de una institución. Los SLA multinivel evitan duplicaciones e incompetencias entre varios acuerdos, haciendo posible integrar en un mismo sistema varias condiciones.

Por ejemplo, la persona que dirige el área comercial puede abrir peticiones creando tickets que apliquen el SLA estándar para el departamento, o un SLA más restrictivo para "dirección de negocio", o un SLA de un servicio específico dentro de su departamento, como "proveedores".

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

III. RECOMENDACIONES Y MEJORES PRÁCTICAS ASOCIADAS AL CONTROL

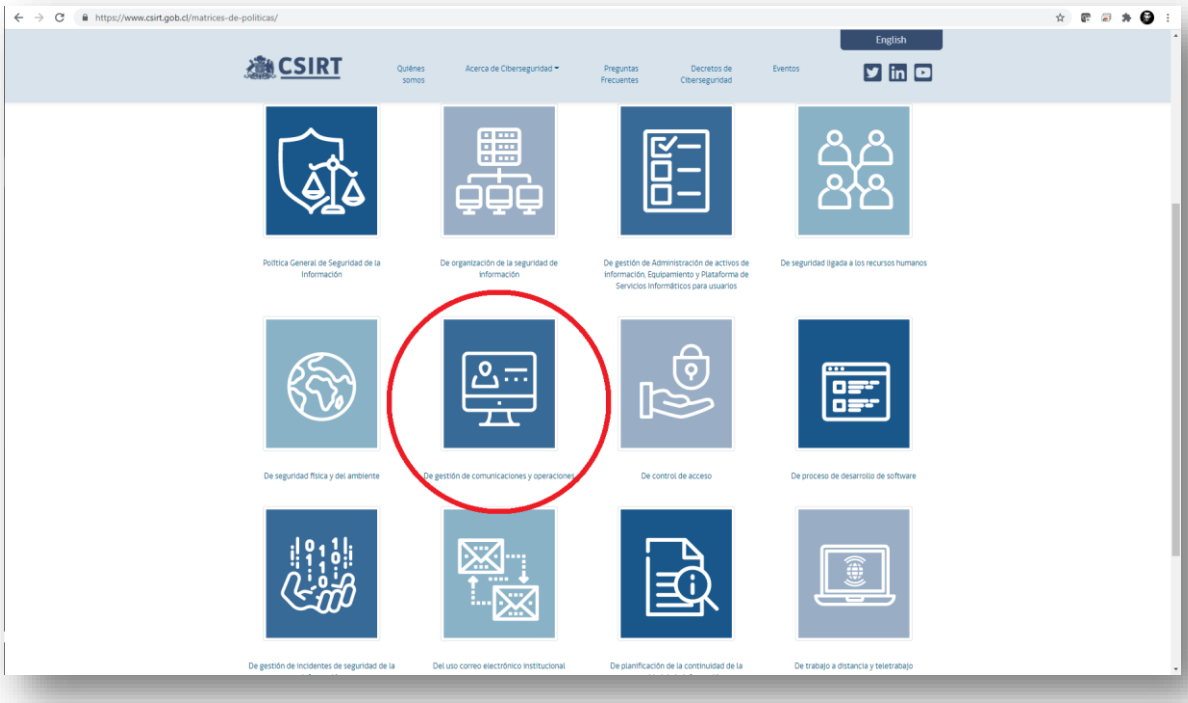
El control: Controles de red

Los mecanismos de seguridad, los niveles del servicio y los requisitos de la gestión de todos los servicios de red se deben identificar e incluir en los acuerdos de servicios de red, ya sea que estos servicios sean prestados dentro de la organización o por terceros.

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 mantener seguras las redes y la información que fluye por ellas.

El CSIRT de Gobierno 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[10].



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

La organización debe determinar y monitorear de manera regular la capacidad del proveedor de servicios de red para administrar los servicios de manera segura y, se debe acordar el derecho a la auditoría.

Se debe identificar las disposiciones de seguridad necesarias para ciertos servicios, como las funciones de seguridad, los niveles de servicio y los requisitos de administración. La organización debe garantizar que los proveedores de servicios de red implementen estas medidas.

La Institución deberá acordar durante el proceso de contratación de servicios de conectividad, ya sea entre sus oficinas o instalaciones, con otras instituciones, o directamente a Internet, requisitos de seguridad para resguardar la confidencialidad, integridad y disponibilidad de la información que se transmitirá por dichas conexiones, sin que estas sean interferidas o manipuladas de forma indebida.

Adicionalmente, deberá acordar con el proveedor el aseguramiento de los niveles de uptime (disponibilidad) de las conexiones, con un nivel que permita a la institución no verse afectada.

También deberá acordar con el proveedor, sobre todo si este administra los enlaces y equipos de red de la institución, cláusulas de revisión de auditoria, con el objeto de asegurar un nivel óptimo de cumplimiento de servicio, sino asegurar que la conectividad del proveedor hacia la red institucional se realice con equipos computacionales autorizados y que no permita la conectividad con otras instituciones u organismos de forma no autorizada.

Respecto a aquellos contratos de servicios de conectividad vigentes a la fecha de lectura del presente documento, la institución deberá negociar con su actual proveedor, cláusulas similares a las anteriormente descritas.

En términos generales los SLA deberán cubrir la seguridad de la red en sus tres principales pilares: Confidencialidad, Integridad y Disponibilidad.

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[11] como en el CSIRT de Gobierno[12] (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.

[11] https://digital.gob.cl/
[12] https://www.csirt.gob.cl/

Anexo I: Ejemplo de estructura de Políticas y Procedimientos