Departamento de Tecnologías de Información y Comunicaciones
Unidad de Seguridad de Información y Ciberseguridad

Indicador COMGES N° 9.4

Implementación del Plan de Ciberseguridad conforme a Ley 21.663

ORIENTACIONES TECNICAS

Año 2026

I. RESUMEN EJECUTIVO

Durante 2024, en el marco del Indicador COMGES, se avanzó en el fortalecimiento de la seguridad de la información en el sector salud, estableciendo las bases de una gobernanza sólida y alineada con la norma NCh-ISO 27001:2022. Todas las Direcciones de Servicios de Salud y Hospitales de Alta Complejidad designaron encargados de seguridad y adoptaron políticas generales de seguridad y ciberseguridad, lo que representa un avance importante en la formalización de responsabilidades.

El diagnóstico nacional realizado evidenció, un bajo nivel de madurez general en la implementación de controles de seguridad, destacando brechas en gestión de incidentes, continuidad operativa, configuraciones seguras, auditorías y mejora continua. Estas debilidades reflejaron la necesidad urgente de reforzar capacidades técnicas, fortalecer la cultura de seguridad y establecer métricas que permitan evaluar la efectividad de los controles.

De cara al 2025, el foco se centró en la implementación prioritaria de los controles críticos identificados en la brecha y avanzar en la conformación de Sistema de Gestión de Seguridad de la Información (SGSI) para los Servicios de Salud y Hospitales de Alta Complejidad.

Para el año 2026, el principal desafío será cumplir con las nuevas exigencias de la Ley N° 21.663 de Ciberseguridad, que establece obligaciones para los Organismos de Interés Vital (OIV), entre ellos el sector salud. Esto implica que cada institución deberá prepararse mejor, contando con una gobernanza clara, monitoreo permanente, y planes de respuesta ante incidentes que sigan buenas prácticas y estándares reconocidos como ISO 27001 y el Marco Nacional de Ciberseguridad.

El presente COMGES busca ayudar a las instituciones del Sector a avanzar en esa dirección, implementando un Plan de Ciberseguridad propio, que permita cumplir con las exigencias de la ley, proteger sus servicios críticos y fortalecer la capacidad de respuesta ante posibles ataques o fallas tecnológicas.

II. Indicador

Objetivo
Garantizar la implementación del Plan de Ciberseguridad conforme a la Ley N° 21.663 y la línea base del MINSAL, asegurando protección de servicios críticos y continuidad operativa.

Nombre:
Implementación del Plan de Ciberseguridad conforme a Ley 21.663.

Fórmula:
(Medidas implementadas del Plan de Ciberseguridad/ Total de medidas definidas según línea base) *100

III. REQUISITO

- **Frecuencia de medición:** Semestral.
- **Periodo de evaluación del cumplimiento:** Anual.
- **Meta sugerida para 2026:** Alcanzar un 80% de implementación efectiva de las medidas del Plan de Ciberseguridad Institucional, conforme a la línea base definida por el MINSAL.
- **Fuente de verificación:** Informe de avance del Plan de Ciberseguridad, validado por la Unidad de Ciberseguridad y Seguridad de la Información del MINSAL.
- **Fuente de datos:** Políticas y procedimientos formalizados, resoluciones exentas, registros de sistemas de información, informes de proveedores, herramientas de monitoreo de seguridad y reportes complementarios.
- **Criterio por eje estratégico**: Para considerar un eje como cumplido, deberá verificarse el 100% de los medios de verificación asociados.

IV. NIVEL DE APLICACIÓN

- Servicios de Salud y Hospitales de Alta Complejidad

V. MARCO DE DEFINICIONES

Para los efectos de la aplicación de este documento, los términos que a continuación se señalan tendrán el significado que se indica:

- **Activos de información**: toda información o recurso relacionado para la creación, almacenamiento, gestión o transmisión de dicha información. Podrán ser activos materiales (RRHH especializados, aparatos, equipos, redes, instalaciones, soportes y sistemas de almacenamiento) o intangibles (datos, aplicaciones, sistemas operativos, bases de datos, imagen, reputación, marcas de la organización)

- **Activo informático**: toda información almacenada en una red y sistema informático que tenga valor para una persona u organización.
- **Autenticación**: propiedad de la información que da cuenta de su origen legítimo.
- Agencia: la Agencia Nacional de Ciberseguridad, que se conocerá en forma abreviada como ANCI.
- **Auditorías de seguridad:** procesos de control destinados a revisar el cumplimiento de las políticas y procedimientos que se derivan del Sistema de Gestión de la Seguridad de la Información.
- **Ciberataque:** intento de destruir, exponer, alterar, deshabilitar, o exfiltrar u obtener acceso o hacer uso no autorizado de un activo informático.
- **Incidente de ciberseguridad**: Todo evento que perjudique o comprometa la confidencialidad o integridad de la información, la disponibilidad o resiliencia de las redes y sistemas informáticos, o la autenticación de los procesos ejecutados o implementados en las redes y sistemas informáticos.
- **Ciberseguridad:** Preservación de la confidencialidad e integridad de la información y de la disponibilidad y resiliencia de las redes y sistemas informáticos, con el objetivo de proteger a las personas, la sociedad, las organizaciones o las naciones de incidentes de ciberseguridad.
- **Confidencialidad:** Propiedad que consiste en que la información no es accedida o entregada a individuos, entidades o procesos no autorizados.
- **Continuidad de servicios:** Adoptar las medidas que permitan proveer un nivel mínimo de servicio, entendiendo por esto las prestaciones propias del sistema, reduciendo el riesgo de eventos que puedan dar lugar a una interrupción o inestabilidad en las operaciones de la entidad, manteniendo niveles aceptables y propiciando la recuperación de los servicios de las tecnologías de la información (TI) en el menor tiempo posible.
- **Concienciación, Educación y Capacitación en Seguridad de la Información**: Es el proceso de sensibilización y formación continua del personal sobre riesgos de ciberseguridad, buenas prácticas y cumplimiento normativo. Se deben realizar programas de capacitación periódicos, simulacros de incidentes y campañas de concienciación para fortalecer la cultura de seguridad en la organización.
- **Derechos de Acceso:** Privilegios y permisos asignados a usuarios, sistemas y aplicaciones para acceder a recursos de información dentro de una organización. Su objetivo es garantizar que solo las personas o sistemas autorizados puedan visualizar, modificar o administrar información y activos tecnológicos, minimizando el riesgo de accesos no autorizados o uso indebido de los datos.
- **Disponibilidad:** Propiedad que consiste en que la información está disponible y es utilizable cuando es requerida por un individuo, entidad o proceso autorizado.

- **Datos Personales o datos de carácter personal:** los datos relativos a cualquier información concerniente a personas naturales, identificadas o identificables, con independencia de su soporte.
- **Datos Sensibles:** Datos personales que se refieren a características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual.
- **Equipo de Respuesta a Incidentes de Seguridad Informática o CSIRT:** Centros multidisciplinarios que tienen por objeto prevenir, detectar, gestionar y responder a incidentes de ciberseguridad o ciberataques, en forma rápida y efectiva, y que actúan conforme a procedimientos y políticas predefinidas, ayudando a mitigar sus efectos.
- **Gestión de incidentes:** Procedimientos para la detección, análisis, manejo, contención y resolución de un incidente de ciberseguridad y responder ante ésta.
- **Gestión de Cambios:** Comprende la planificación, control y auditoría de modificaciones en sistemas, aplicaciones o infraestructura tecnológica, con el objetivo de minimizar riesgos de seguridad. Debe incluir la evaluación de impactos, pruebas previas, aprobación formal y documentación de cada cambio implementado.
- **Incidente:** Evento inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes, equipos y sistemas de información (véase también ciberincidente).
- **Interrupción:** Se refiere a cualquier evento que afecte la continuidad operativa de los servicios de información, pudiendo ser causado por incidentes de seguridad, fallos técnicos o desastres naturales. Se deben implementar planes de continuidad del negocio (BCP) y recuperación ante desastres (DRP) para mitigar el impacto de interrupciones y asegurar la resiliencia de los sistemas.
- **Infraestructura crítica:** las instalaciones, sistemas físicos o servicios esenciales y de utilidad pública, redes, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, denegación, interrupción o destrucción cause un grave daño a la salud o al abastecimiento de la población, a la actividad económica esencial, al medioambiente o a la seguridad del país. Se entiende por este concepto la infraestructura indispensable para la generación, transmisión, transporte, producción, almacenamiento y distribución de los servicios e insumos básicos para la población, tales como energía, gas, agua o telecomunicaciones; la relativa a la conexión vial, aérea, terrestre, marítima, portuaria o ferroviaria, y la correspondiente a servicios de utilidad pública, como los sistemas de asistencia sanitaria o de salud.
- **Integridad:** Propiedad que consiste en que la información no ha sido modificada o destruida sin autorización.
- **Nube privada:** La infraestructura de la nube se aprovisiona para uso exclusivo de una única organización aun cuando comprenda múltiples unidades de dicha organización. Puede ser

propiedad, administrado y operado por la organización, un tercero o una combinación de ellos, y puede existir dentro o fuera de las instalaciones de la organización.

- **Nube pública:** La infraestructura y los recursos lógicos que forman parte del entorno se encuentran disponibles para el público en general a través de Internet. Suele ser propiedad de un Prestador de Servicios que gestiona la infraestructura y el servicio o servicios que se ofrecen.
- **Protección de los activos de información:** Adoptar las medidas que resguarden la seguridad física de los dispositivos, así como los accesos a éstos.
- **Red y sistema informático:** conjunto de dispositivos, cables, enlaces, enrutadores u otros equipos de comunicaciones o sistemas que almacenen, procesen o transmitan datos digitales.
- **Resiliencia:** Capacidad de las redes y sistemas informáticos para seguir operando luego de un incidente de ciberseguridad, aunque sea en un estado degradado, debilitado o segmentado, y la capacidad de las redes y sistemas informáticos para recuperar sus funciones después de un incidente de ciberseguridad.
- **Respaldo:** La información de respaldo (backup) se refiere al proceso de copiar y almacenar datos críticos para garantizar su disponibilidad en caso de pérdida, corrupción, o incidentes de seguridad como ataques cibernéticos, fallas de hardware o desastres naturales.
- **Riesgo de Ciberseguridad:** Toda circunstancia o hecho razonablemente identificable que tenga un posible efecto adverso en la seguridad de las redes, equipos y sistemas de información. Se puede cuantificar como la probabilidad de materialización de una de las amenazas antes mencionadas que produzca un impacto en términos de operatividad, o de integridad, confidencialidad o disponibilidad de datos.
- **Seguridad de la información**: Conjunto de medidas preventivas y reactivas de los organismos administradores y sus respectivos sistemas tecnológicos, que tienen por objeto resguardar y proteger la información, asegurando la confidencialidad, integridad, autenticidad y disponibilidad de los datos, continuidad de servicios y protección de activos de información.
- **Seguridad de la Información en la Relación con Proveedores:** Define la importancia de establecer requisitos de seguridad en los contratos con proveedores de tecnología y servicios, asegurando que cumplan con normativas y estándares de seguridad. Deben incluirse cláusulas sobre confidencialidad, gestión de accesos, protección de datos y cumplimiento de auditorías de seguridad.
- **Tratamiento de datos:** Cualquier operación o complejo de operaciones o procedimientos técnicos de carácter automatizado o no, que permitan recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, disociar, comunicar,

ceder, transferir, transmitir o cancelar datos de carácter personal, o utilizarlos en cualquier otra forma.

- **Vulnerabilidad**: Debilidad de un activo o control que puede ser explotado por una o más amenazas informáticas.

VI. CONSIDERACIONES TECNICAS: PLAN DE CIBERSEGURIDAD INSTITUCIONAL (LÍNEA BASE)

Eje Estratégico	Pond. Obj.	Objetivo Asociado	Pond Act.	Actividades Claves	Verificación/ Evidencia
1. Gobernanza y Cumplimiento	**20%**	Fortalecer la estructura institucional de seguridad	33%	Designar Delegado o Encargado y al Comité de Seguridad de la Información y Ciberseguridad de acuerdo con Ley 21.663 e I.G./2025 N°3.	1. Resolución de designación de Delegado. 2. Resolución de Comité de Seguridad de la Información y Ciberseguridad.
			33%	Mantener trazabilidad de las acciones y coordinaciones del Comité de Seguridad, sesionando al menos dos veces durante el periodo 2026.	1. Minutas y actas firmadas de cada sesión, con registro de asistentes, temas tratados, acuerdos adoptados y seguimiento de compromisos (con un mínimo dos sesiones durante el año 2026).
			34%	Implementar el modelo base de SGSI alineado a ISO 27001:2022 en la Institución.	1. Clasificación de criticidad de Activos (archivo Excel). 2. Matriz de Riesgo actualizada (archivo Excel). 3. Plan de tratamiento (archivo Excel). 4. Reporte / presentación a Comité y Dirección del Plan (documento o ppt).
2. Protección de Infraestructura Crítica	**20%**	Proteger los sistemas críticos y reducir superficie de ataque.	25%	Mantener un inventario actualizado de servidores y sistemas, asegurando la aplicación oportuna de parches críticos y la gestión del estado de soporte.	1. Inventario consolidado que incluya el estado de los sistemas y dispositivos Institucionales, considerando: -Estado de actualización (vigente, desactualizado o sin soporte). - En red segmentada (Si/No). -Estado de respaldo (Respaldado / No Respaldado).
			25%	Implementar segmentación de red por funciones, actualización de firewalls y revisión periódica de logs.	1. Diagrama de segmentación de red. 2. Configuraciones vigentes de firewalls y actualización de firmware según recomendación del fabricante, fecha de últimas actualizaciones.
			25%	Desplegar y gestionar soluciones Antivirus/EDR, asegurando cobertura, actualización y monitoreo en endpoints.	1. Informe de estado de las herramientas implementadas: - Número de agentes instalados, versiones vigentes de AV/EDR (equipos sin agente o desactualizados) - Plan de regularización.

Eje Estratégico	Pond. Obj.	Objetivo Asociado	Pond Act.	Actividades Claves	Verificación/ Evidencia
			25%	Realizar escaneos periódicos de vulnerabilidades sobre sistemas críticos, priorizando aquellos expuestos o que procesen información sensible.	1. Informes de escaneo realizados durante el año, con identificación de hallazgos clasificados por criticidad (con un mínimo de 3 escaneos de sistemas o portales críticos de la Institución). Se aceptan informes emitidos por ANCI, MINSAL o proveedores Externos. 2. Planes de mitigación.
3. Identidad y Acceso Seguro	**20%**	Fortalecer el control de acceso y prevenir accesos indebidos	50%	Implementar autenticación multifactor (MFA) en accesos críticos y servicios en nube.	1. Listado de sistemas críticos expuestos a internet con MFA habilitado y no habilitado. - Nombre del Sistema (Si/No). - Correo (Si/No). - VPN (Si/No). - Otros 2. Informe de implementación de MFA en los sistemas que dispongan de esta funcionalidad, priorizando sistemas críticos, cuentas privilegiadas, servicios en la nube.
			50%	Revisar y eliminar cuentas inactivas o sin uso (usuarios internos y proveedores).	1. Registro bimensual de revisión de usuarios, perfiles administrativos y accesos privilegiados, evidenciando cumplimiento de la política o procedimiento de gestión de cuentas y accesos (revocación y accesos). - Listado de usuarios activos. - Listado de usuarios activos con privilegios elevados. - Detalle de altas, bajas y modificaciones realizadas en el período. - Revocaciones ejecutadas (con fecha y responsable) 2. Registro bimensual de revisión de accesos otorgados a proveedores sobre activos institucionales, asegurando vigencia contractual y eliminación de accesos cuando corresponda.
4. Detección y Respuesta ante Incidentes	**20%**	Detectar y responder oportunamente a ciberamenazas.	33%	Definir e implementar un Procedimiento de Respuesta ante Incidentes de Seguridad de la Información.	1. Procedimiento formalmente documentado y aprobado, con definición de roles, etapas de gestión y canales de comunicación.

Eje Estratégico	Pond. Obj.	Objetivo Asociado	Pond Act.	Actividades Claves	Verificación/ Evidencia
			33%	Habilitar y operar monitoreo de seguridad en endpoints, servidores y FW, asegurando cobertura y supervisión continua de eventos relevantes.	1. Plan de implementación de sistemas monitoreo, en caso de mantener vigente, generar informe de estado de estas herramientas. - Registros de monitoreo de eventos (accesos administrativos al FW y alertas críticas con acciones ejecutadas). - Servidores críticos integrados al monitoreo. - Reporte consolidado de eventos de seguridad monitoreado en endpooints - Eventos detectados. - Clasificación de severidad (Crítico, Alto, Medio, Bajo) - Tipología de eventos (malware, intentos de intrusión, accesos no autorizados, phishing, explotación de vulnerabilidades). - Listado de equipos con políticas de contraseña y cifrado habilitado Listado de software autorizados
			34%	Asegurar el cumplimiento del deber de reporte de incidentes de ciberseguridad a la autoridad competente (ANCI) y su notificación interna al Minsal, conforme a la normativa vigente.	1. Registro de incidentes reportados, que incluya: - Fecha de detección, fecha de notificación a ANCI y el código ID del reporte del incidente emitido por ANCI. - Constancia de comunicación a Minsal por parte del Delegado de la Institución (registro de correo).
5. Continuidad Operacional y Ciberresiliencia	**10%**	Asegurar la continuidad de servicios críticos ante incidentes.	50%	Ejecutar al menos una prueba o simulacro anual de continuidad de servicios, en el marco de los planes DRP vigentes.	1. Plan DRP formalmente documentado, aprobado y actualizado. 2. Acta o informe de ejecución del simulacro realizado, incluyendo resultados, brechas detectadas y firma del Delegado.
			50%	Implementar respaldos priorizando sistemas críticos, asegurando segmentación y protección de los respaldos, y realizando pruebas periódicas de restauración.	1. Registros de respaldos de sistemas críticos. - Servidores, bases de datos, aplicaciones core - Fecha y hora, estado de la tarea (exitosa/fallida) - Repositorio segregado, lógicamente distinto del entorno productivo (Si/No). - Sitio alterno, nube o externo a infraestructura local. 2. Logs de respaldos 3. Registro de pruebas de restauración ejecutadas.

Eje Estratégico	Pond. Obj.	Objetivo Asociado	Pond Act.	Actividades Claves	Verificación/ Evidencia
6. Cultura y Capacitación	**10%**	Fortalecer la conciencia y el comportamiento seguro del personal.	50%	Ejecutar programa anual de capacitación en ciberseguridad	1. Convocatorias, registros de asistencia y material presentado. 2. Realización de charlas de capacitación semestralmente para los funcionarios, que considere: - Políticas de Seguridad Institucional, Protección de Datos, y responsabilidad de funcionario en estas materias. - Riesgos existentes en internet, phishing, fraudes, exposición de información sensible e incidentes. - Documentación de campañas de phishing realizadas y reporte de resultados obtenidos.
			50%	Realizar campañas periódicas de phishing para funcionarios.	1. Informes de campañas de phishing realizadas y métricas de resultados (mínimo dos campañas en el año)