SUPERINTENDENCIA DE SALUD

Unidad de Planificación, Innovación y Control de Gestión

Resolución Exenta SS/N°

MAT: Aprueba Política de Seguridad y Ciberseguridad de la Información para la Superintendencia de Salud y deroga Resolución Exenta SS/N°994 del 9 de diciembre de 2021.

Santiago,

VISTOS:

El DFL N° 1/19.653 de 2000, del Ministerio Secretaría General de la Presidencia, que fija el texto refundido, coordinado y sistematizado de la Ley N°18.575, Orgánica Constitucional de las Bases Generales de la Administración del Estado; el DFL 29, de 2005, del Ministerio de Hacienda, que fijó el texto refundido, coordinado y sistematizado de la Ley N**°**18.834, sobre Estatuto Administrativo; lo establecido en la Resolución N° 7, de 2019, de la Contraloría General de la República; el D.S. N°83 de 2005, del Ministerio Secretaria General de la Presidencia, que aprueba la norma técnica para los órganos de la Administración del Estado, sobre seguridad y confidencialidad de los documentos electrónicos; las actuales normas NCH ISO/IEC 27001: 2013 sobre requisitos de un sistema de gestión de seguridad de la información y NCH ISO/IEC 27002:2013, sobre códigos de buenas prácticas para la gestión de la seguridad de la información; la Resolución Exenta SS N°994 del 9 de diciembre de 2021, que aprobó la anterior Política de Seguridad de la Información de la Superintendencia de Salud; la Resolución Exenta SS N°665 del 5 de septiembre 2019 que nombra a la Oficial de Seguridad de la información; Resolución Exenta N°710 del 11 junio de 22024, que crea el Comité de Tecnologías y Seguridad de la Información; la Ley 21663 del 8 de abril 2024 Ley Marco de Ciberseguridad del Ministerio del Interior Y Seguridad Pública; y la Resolución Exenta N° 1661 de 2023 que aprueba la Política Nacional de Ciberseguridad 2023-2028 y, teniendo presente las facultades que me confiere el artículo 109 del DFL N°1, de 2005, y,

CONSIDERANDO:

1. Que parte de las políticas del Estado están orientadas a la incorporación permanente de tecnologías de información y comunicaciones en los órganos de Administración del Estado, con el fin de mejorar los servicios e información que se entregan a los usuarios, generando una gestión pública eficaz y eficiente que incremente la transparencia del sector público y la participación ciudadana;

2. Que, a través de la Resolución Exenta SS/N°994 del 9 de diciembre de 2021, esta Superintendencia dictó normas tendientes a proteger la seguridad de la información, instituyendo una Política de Seguridad de la Información Institucional;

3. Que, para avanzar en una eficiente gestión en materia de seguridad de la información, y teniendo presente la reciente creación de la Coordinación Nacional de Ciberseguridad, Unidad de la Subsecretaría del Interior que tiene por objeto coordinar la acción de los organismos públicos en materia de ciberseguridad, debemos implementar medidas para proteger la seguridad y ciberseguridad según se establece en los objetivos de esta institución;

TANA RMSC OAVS CSMB JADC RDCL

4. Que dicha política está sujeta a evaluación periódica, con el propósito de incorporar mejoras y actualizaciones provenientes del avance tecnológico y de los desarrollos legislativos en materia de ciberseguridad;

5. Que, precisado lo anterior, procedo a aprobar la Política que se adjunta a este acto administrativo, y que se entiende formar parte integrante del mismo, cumpliendo con los principios de control y eficiencia establecidos en los artículos 3° y 10° de la Ley Orgánica Constitucional de Bases Generales de la Administración del Estado, N°18.575. Dicha política, denominada "Política de Seguridad y Ciberseguridad de la Información", tiene como objetivo "resguardar los activos informáticos de la institución, garantizando un alto nivel de continuidad operativa de sus procesos de negocio, contribuyendo de esta forma al cumplimiento de su misión y objetivos estratégicos", y consta de 8 páginas.

6. Que, atendido lo expuesto y, con la recomendación de la Oficial de Seguridad de la Información Institucional, procedo a dictar la siguiente

RESOLUCIÓN:

1. **APRUÉBASE** la presente "**Política de Seguridad y Ciberseguridad de la Información**", cuyo texto es el siguiente:

SUPERINTENDENCIA DE SALUD

Unidad de Planificación, Innovación y Control de Gestión

Junio 2024

POLÍTICA SEGURIDAD Y CIBERSEGURIDAD DE LA INFORMACIÓN

Unidad de Planificación, innovación y Control de Gestión

Tabla de contenido

SUPERINTENDENCIA DE SALUD

Unidad de Planificación, Innovación y Control de Gestión

POLÍTICA DE SEGURIDAD Y CIBERSEGURIDAD

Propósito

La política de Seguridad y Ciberseguridad de la Información define la forma de garantizar la confidencialidad, integridad y disponibilidad de la información, particularmente los datos sensibles y críticos de la institución, mediante la implementación de medidas de seguridad robustas, la concientización del personal y la respuesta eficaz a amenazas cibernéticas, con el fin de proteger los activos digitales y mantener la confianza de los usuarios y de entidades públicas y privadas.

Aplica a todas las áreas, sistemas, activos y funcionariado de la institución. Incluye, datos sensibles, sistemas y redes, todo el personal, interno y externo, empresas contratistas y de prestación de servicios, procesos y procedimientos, dispositivos móviles y remotos y proveedores externos.

Debemos considerar que la información y sus medios de soporte son cruciales para las funciones regulatorias y fiscalizadoras de la Superintendencia en el Sistema de Salud Chileno. Esto implica que la seguridad y ciberseguridad es primordial para protegerla de pérdidas, manipulación y divulgación no autorizada, y garantizar su disponibilidad para el personal y terceros autorizados.

Por ello es fundamental promover una cultura de seguridad y ciberseguridad de la información, centrando los objetivos en implementar medidas de protección adecuadas y en la preparación para hacer frente a posibles incidentes de seguridad de manera eficaz, bajo las siguientes directrices:

- Fomentar una cultura organizacional orientada hacia la seguridad de la información, donde todo el personal comprenda la importancia de proteger los datos confidenciales y cumpla con las mejores prácticas de seguridad.
- Establecer un marco claro de responsabilidades individuales y colectivas en relación con la seguridad de la información, asegurando que cada funcionario/a entienda su papel en la protección de los activos de información.
- Implementar medidas técnicas y procedimientos operativos que salvaguarden la confidencialidad, integridad y disponibilidad de los datos de la Superintendencia de Salud, mitigando los riesgos de pérdida, manipulación y divulgación no autorizada.
- Proporcionar a los funcionarios/as herramientas y recursos necesarios para tomar decisiones informadas y adecuadas en situaciones que afecten la seguridad de la información.
- Establecer mecanismos proactivos para detectar y responder a posibles amenazas cibernéticas, garantizando la protección continua de los sistemas de información.
- Desarrollar planes de contingencia efectivos que permitan la rápida recuperación de datos en caso de incidentes de seguridad, minimizando el impacto en las operaciones de la Superintendencia y sus partes interesadas.

Alcance

Esta política se aplica a:

- Todo el personal de la Superintendencia, planta, contrata y honorarios, y también al personal externo que preste o prestare servicios a la institución, sean o no remunerados. Se incluye también a los prestadores de servicios, proveedores y cualquier persona o entidad externa que pueda hacer uso de la información de la Superintendencia y que haya sido debidamente autorizado para ello.
- Todos los sistemas de información, redes de comunicación, dispositivos tecnológicos y medios de almacenamiento que se utilicen para almacenar, procesar o transmitir información relacionada con las funciones de la Superintendencia.
- Todo activo de información que la organización posea en la actualidad o en el futuro, de manera que la no inclusión explícita en el presente documento, no constituye argumento para no proteger estos activos de información.
- Toda la información, entre otras, la impresa o escrita en papel, almacenada electrónicamente, trasmitida por correo o usando medios electrónicos, mostrada en películas o hablada en una conversación.
- Todas las acciones de seguridad que se realizan en el ciberespacio, sus transacciones, almacenamiento y acceso.

Gestión

La gestión de la seguridad de la información se realiza mediante un proceso sistemático, documentado y conocido por toda la organización basándose en metodologías de mejoramiento continuo. Este proceso deberá ser aplicado prioritariamente a todos los procesos de negocio de la organización, luego a los procesos estratégicos y finalmente a los procesos de apoyo o soporte.

Respecto a definiciones y modo de operación, así también, como apoyo a esta política general, cada dominio especificado por el estándar ISO 27001, tiene una política o norma interna específica, que complementa la presente y que regula las particularidades de cada dominio.

Vigencia y Periodicidad de Evaluación y Revisión de la Política

La revisión y mantención de la presente Política será realizada por el/la Oficial de Seguridad de la Información y sus cambios aprobados por el Comité de Seguridad y el Superintendente de Salud, aprobada formalmente mediante Resolución Exenta.

El Comité de Seguridad de la Información está encargado de revisar y aprobar la Política de Seguridad y Ciberseguridad de la Información, asegurándose de que se ajuste a las necesidades de la institución al menos cada dos años desde su publicación inicial. No obstante, esta política podrá ser sometida a revisión y actualización anticipada si así lo requiere algún miembro del comité o en caso de circunstancias coyunturales que puedan afectar la protección adecuada de la información. Dichas circunstancias incluyen, entre otras, cambios en la misión, objetivos estratégicos, productos, infraestructura, personal o procedimientos relacionados con la protección de la información.

Una vez realizados los cambios y aprobada la nueva versión, el/la Oficial de Seguridad de la Información deberá encargarse de difundirla.

Responsabilidades

La tabla que se despliega a continuación define la funciones y responsabilidades de todos los funcionarios/as, respecto del rol que cada uno debe cumplir en el contexto de Seguridad y Ciberseguridad de la Información.

ROL	FUNCIONES	RESPONSABILIDADES
Superintendente	Establecer expectativas claras sobre el uso seguro de los recursos de información de acuerdo con las regulaciones y políticas establecidas	- Asignar recursos adecuados para la seguridad de la información. - Fomentar una cultura de seguridad de la información en toda la organización.
Comité de Seguridad - **Miembros del Comité**	Revisar, aprobar y actualizar políticas, estándares y procedimientos de seguridad de la información de acuerdo con las regulaciones y políticas vigentes.	- Supervisar la implementación y cumplimiento de controles de seguridad. - Evaluar y mitigar riesgos de seguridad de la información.
Oficial de Seguridad - **Jefatura Unidad de Planificación, Innovación y Control de Gestión**	Desarrollar, implementar y mantener políticas y procedimientos de seguridad de la información de acuerdo con las regulaciones y estándares pertinentes.	- Coordinar la respuesta a incidentes de seguridad. - Proporcionar formación y concienciación sobre seguridad de la información conforme a los requisitos establecidos. - Realizar campañas permanentes de seguridad con la finalidad de mantener estable una cultura en esta materia.
Custodio de Datos - **Todas las jefaturas de cada área o unidad**	Almacenar y gestionar datos de manera segura, asegurando la confidencialidad, integridad y disponibilidad de acuerdo con las regulaciones y políticas aplicables.	- Implementar y mantener medidas de seguridad física y lógica para proteger los datos de acuerdo con las normativas vigentes.
Administrador de Seguridad - **Jefatura del Subdpto de Tecnologías**	Implementar y administrar controles de seguridad de TI, como firewalls, sistemas de detección de intrusiones, etc., en conformidad con las regulaciones y políticas establecidas.	- Supervisar la actividad de red para detectar y responder a posibles amenazas de acuerdo con los protocolos establecidos. - Mantener actualizados y seguros los sistemas y herramientas de seguridad según las normativas vigentes.
Custodio Físico Funcionarios/as que utilizan sistemas e información para su trabajo	Proteger la información en soportes físicos, como documentos impresos y dispositivos de almacenamiento, en cumplimiento con las regulaciones y políticas de seguridad establecidas	- Controlar el acceso físico a áreas de almacenamiento de datos de acuerdo con los protocolos de seguridad establecidos.
Funcionarios/as de la Institución	Seguir las políticas y procedimientos de seguridad de la información establecidos por la institución.	- Participar en actividades de formación y concienciación sobre seguridad de la información. - Reportar cualquier incidente o violación de seguridad de la información a las autoridades correspondientes.

Disposiciones

Las siguientes disposiciones generales son aplicables para el cumplimiento de la Política de Seguridad de la Información de la Superintendencia de Salud:

Información Interna

Activos de información: La información es un activo vital. Todos los accesos, usos y procesos relacionados con ella deben alinearse con las políticas y estándares de la Superintendencia.

a) *Protección:* La información debe ser protegida de acuerdo con su importancia, valor y criticidad. Los custodios de la información deben seguir las políticas específicas de seguridad de la información, los procedimientos asociados y las recomendaciones del responsable designado. La Superintendencia proporcionará los recursos necesarios para implementar controles adecuados para proteger los activos.
b) *Clasificación:* Toda la información creada o procesada por la institución será considerada "Pública" a menos que se clasifique como "Reservada" o "Secreta" según el ordenamiento jurídico vigente. Esta clasificación será revisada periódicamente para asegurar su vigencia.
c) *Acceso:* La Superintendencia proporcionará mecanismos para que el personal acceda y utilice la información según sus perfiles y funciones asignadas. La institución se reserva el derecho de revocar privilegios de acceso a la información y tecnologías según lo ameriten las circunstancias.
d) *Comercio Electrónico:* La Superintendencia no realiza comercio electrónico a través de redes públicas ni de otra índole. Las relaciones contractuales con proveedores externos seguirán los procedimientos y canales establecidos por la Ley N° 19.886 (Ley de Compras) y su reglamento.
e) *Incidentes:* Los incidentes que afecten la seguridad de la información institucional deben tratarse con discreción, preservando la confidencialidad de la información. Se deben tener procedimientos actualizados que especifiquen cuándo y a qué autoridades contactar y cómo informar los incidentes de seguridad de manera oportuna.
f) *Acuerdo de Confidencialidad:* Todos los funcionarios y trabajadores de empresas externas deben firmar un "Acuerdo de Confidencialidad y Aceptación de Políticas de Seguridad de la Información de la Superintendencia de Salud", que establece sus deberes en la protección de la información, incluso después de cesar su vínculo con la institución.

Información de Usuarios Externos

a) *Protección de Datos Personales: La Superintendencia asegurará que la* información de usuarios externos, considerada como datos personales y/o sensibles, no será divulgada sin autorización previa y estará protegida de igual manera que la información interna.
b) *Compartir Información:* Si se requiere compartir información de usuarios externos con otras instituciones, se exigirá la firma de un contrato o convenio de confidencialidad y no divulgación antes de la entrega de la información.

Supervisión y Evaluación de Seguridad

a) *Responsabilidad de las Áreas:* Todas las áreas de la Superintendencia son responsables de promover, mejorar, difundir y controlar el uso de las normas, estándares y procedimientos derivados de esta política.
b) *Cumplimiento de la Política:* Cada área o unidad debe cumplir con las indicaciones establecidas en la Política de Seguridad de la Información y las normas vigentes. Se realizarán verificaciones según el calendario de Gobierno Digital.

c) *Conducta del Personal:* Todo el personal debe conducirse conforme a esta política, normas, estándares y procedimientos establecidos, respetando la confidencialidad de la información.

Compromiso de la Alta Dirección Institucional

a) *Comité de Seguridad:* Funcionará un Comité de Seguridad y deberá existir un Oficial de Seguridad, quien actuará como asesor del Jefe de Servicio en materias relativas a la seguridad.
b) *Proyectos y Seguridad:* La seguridad de la información debe abordarse en toda administración de proyectos, sin importar su tipo.
c) *Continuidad del Negocio:* La Dirección del Servicio propiciará mecanismos y procedimientos formales que aseguren la continuidad del negocio ante situaciones que impidan el acceso a la información esencial.

Deberes del Personal

a) *Uso Apropiado:* La información y las tecnologías de información deben ser usadas solo para propósitos relacionados con el servicio, aplicando criterios de buen uso.
b) *Responsabilidad de Claves:* Las claves de acceso son individuales, intransferibles y de responsabilidad única de su propietario.
c) *Alerta de Incidentes:* El personal debe alertar oportunamente sobre cualquier incidente que atente contra lo establecido en esta política.
d) *Prohibición de Divulgación:* Está prohibido divulgar información clasificada como "Reservada", "Secreta" o "Sensible".
e) *Respeto a Normas:* Todo el personal debe respetar las normas, estándares y procedimientos de seguridad de la información.
f) *Protección de Recursos:* El personal es responsable de proteger la información y recursos bajo su uso y custodia, siguiendo las normas establecidas.
g) *Controles de Seguridad:* Las áreas deben cumplir con los controles de seguridad necesarios para proteger los activos informáticos de la organización.

Difusión de la Política

a) *Plan de Difusión:* Debe existir un plan formal y periódico de difusión, capacitación y sensibilización sobre la seguridad de la información. El Oficial de Seguridad será el responsable de este plan.
b) *Medios de Difusión:* La política y las normas de seguridad serán difundidas mediante el medio más adecuado para alcanzar a todos los funcionarios. Se indicará dónde estarán disponibles permanentemente para consultas.
c) *Entrenamiento del Personal:* La Dirección del Servicio asegurará que todo el personal reciba entrenamiento suficiente y coherente con sus necesidades y roles.

Evaluación de Cumplimiento y Sanciones

a) *Vigencia de la Política*: La Política General de Seguridad de la Información entra en vigencia una vez oficializada por el Superintendente de Salud mediante Resolución Exenta. Las jefaturas son responsables de informarla a su personal subordinado.
b) *Alineación Legal:* La política está alineada con las leyes y regulaciones existentes. Cualquier conflicto con estas regulaciones debe ser informado inmediatamente al Oficial de Seguridad.
c) *Sanciones:* Se aplicarán sanciones correspondientes al incumplimiento de las normas y procedimientos derivados de esta política, de acuerdo a la Ley N° 18.834 sobre Estatuto Administrativo, evaluando la gravedad e intencionalidad del incumplimiento.

Marco legal

- DFL 29 fija texto refundido, coordinado y sistematizado de la Ley nº 18.834, sobre estatuto administrativo; 16 marzo 2005
- Ley 19.628, Protección de la vida privada; 28 agosto 1999
- Ley 19.799, Documentación Electrónica, Firma Electrónica y servicios de certificación de dicha firma; 12 abril 2002
- Ley 20.285, Acceso a la Información Pública; 20 agosto 2008
- Ley 19.880, Establece bases de los procedimientos administrativos que rigen los actos de los Órganos de la Administración del Estado; Modificada 9 febrero 2024, Ley 21658.
- LEY 21459, Establece normas sobre delitos informáticos, Deroga la Ley n° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al Convenio de Budapest; 20 junio 2022
- Ley 17.336, Propiedad Intelectual; 2 octubre 1970
- Ley 19.927, Modifica Código Penal, Código de Procedimiento Penal y Código de Procesal Penal en materias de delitos de Pornografía Infantil; 14 enero 2004
- Norma Chilena Nch ISO 27001:2013
- Norma Chilena Nch ISO 27002:2013
- Documentación, Normativa Legal, instrumentos y Guía Metodológica PMG Sistema de Seguridad de la Información Subsecretaría del Interior
- Ord. A22/N° 665 (marzo 2016) del Ministerio de Salud, sobre instrucciones de seguridad de la información en el uso de carpetas compartidas
- Decreto 83, Aprueba norma técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos; 12 enero 2005
- Resolución 2308 exenta, Fija Normas sobre Comunicaciones Electrónicas e Interoperabilidad con la Subsecretaría de Telecomunicaciones de Trámites que indica; 18 mayo 2011
- Decreto 81 de 2004, Interoperabilidad de documentos electrónicos
- Decreto Supremo 83 de 2005 del Ministerio Secretaría General de la Presidencia, sobre Seguridad y Confidencialidad de los Documentos Electrónicos; 18 mayo 2011
- Decreto 93, Aprueba Norma Técnica para la adopción de medidas destinadas a minimizar los efectos perjudiciales de los mensajes electrónicos masivos no solicitados recibidos en las casillas electrónicas de los Órganos de la Administración del Estado y de sus funcionarios
- Decreto 158, Modifica Decreto supremo Nº 81, de 2004, que aprueba Norma Técnica para los Órganos de la Administración del Estado sobre interoperabilidad de documentos electrónicos; 18 mayo 2007
- Instructivo Presidencial N° 5 de 2001, Desarrollo de Gobierno Electrónico
- Instructivo Presidencial N° 6 de 2005, Implementación y uso de firma electrónica; 11 mayo 2001
- Instructivo Presidencial N° 8 de 2006, Transparencia activa y publicidad de la Información
- Instructivo Presidencial 008, sobre Ciberseguridad; 23 de octubre 2018
- Decreto Exento N° 2221, del 11 de noviembre 2019.
- Resolución Exenta N° 1661, que aprueba la Política Nacional de Ciberseguridad 2023-2028; año 2023.

Normas Internas Complementarias
Es importante destacar que este documento se complementa con un conjunto de Normas de Seguridad y Ciberseguridad de la Información que señalan aspectos específicos y detallados y proporcionan directrices adicionales para garantizar la seguridad de la información en todos los ámbitos de nuestra organización.

Estas normas detalladas están diseñadas para guiar a los funcionarios/as en la implementación efectiva de las políticas y prácticas de seguridad de la información en sus respectivas áreas de trabajo.

2. **Difúndanse** los contenidos de la Política de Seguridad y Ciberseguridad de la Información a todos los funcionarios y funcionarias de la institución, por los medios internos que se consideren adecuados para su efectividad.

3. **Deróguese** la Resolución Exenta SS/N°994 del 9 de diciembre de 2021, que aprobó la anterior Política de Seguridad Institucional de la Información.

ANÓTESE, COMUNÍQUESE Y PUBLÍQUESE EN EL PORTAL WEB

_____

DR. VÍCTOR TORRES JELDES
SUPERINTENDENTE DE SALUD

TANA RMSC OAVS CSMB JADC RDCL

Distribución

- Superintendente de Salud
- Fiscalía
- Intendencia de Fondos y Seguros
- Intendencia de Prestadores de Salud
- Gestión Corporativa y Participación Ciudadana
- Departamento de Administración y Finanzas
- Departamento de Estudios y Desarrollo
- Unidad de Planificación y Control de Gestión
- Unidad de Comunicaciones
- Subdpto de Tecnologías de la Información
- Unidad de Datos y Estadísticas
- Jefaturas de Subdepartamentos
- Jefaturas de Unidades
- Oficina de Partes

  JIRA: RI-999