SUPERINTENDENCIA
DE SALUD

Resolución Exenta SS/N° 994

MAT: Aprueba Política de Seguridad de la Información para la Superintendencia de Salud y deroga Resolución Exenta SS/N°537 del 31 de julio de 2019.

Santiago, 29 DIC 2021

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° 1600, de 2008, 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°537 del 31 de julio de 2019, que aprobó la anterior Política de Seguridad de la Información de la Superintendencia de Salud; la Resolución Exenta N° 613 de mayo de 2016, que crea el Comité de Tecnologías y Seguridad de la Información; la Resolución Exenta N° 1545 de Diciembre de 2015 que nombra a la Oficial o Encargada de Seguridad de la Información de la Superintendencia de Salud 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°537 del 31 de julio de 2019, esta Superintendencia dictó normas tendientes a proteger la seguridad de la información, instituyendo una política de seguridad institucional;

3. Que, para avanzar en una eficiente gestión en materia de seguridad de la información, teniendo presente la existencia del Grupo de Agenda Digital de Gobierno, en su rol de coordinador en estas materias y la necesidad de implementar medidas proteger la seguridad en el ciberespacio según lo establece el Ministerio del Interior y Seguridad Ciudadana.

4. Que, dicha política está sujeta a evaluación periódica, con el propósito de incorporarle mejoras;

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, denominada "Política de Seguridad de la Información", cuyo objetivo es "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", que consta de 71 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 de la Información**", cuyo texto es el siguiente:

SUPERINTENDENCIA
DE SALUD

Unidad de Innovación, Planificación
y Control de Gestión

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Normas y principios generales de seguridad

SUPERINTENDENCIA DE SALUD

CONTROL DOCUMENTAL DE ACTUALIZACIONES

Versión	Fecha	Rol responsable	Nombre	Firma
Novena	29.12.21	Superintendente de Salud	Patricio Fernández Pérez	
	29.12.21	Oficial de Seguridad de la Información	Tamara Núñez Andrewartha	

SUPERINTENDENCIA DE SALUD * SUPERINTENDENTE *

SUPERINTENDENCIA DE SALUD UNIDAD DE PLANIFICACIÓN, INNOVACIÓN Y CONTROL DE GESTIÓN

Versión	Fecha Aprobación	Motivo de actualización	Páginas Modificadas	Autor
1	05/08/2010	Primera Revisión Política General	Todas	Oscar Muñoz
2	19/08/2010	Revisión General Equipo Dpto. Gestión	Todas	Oscar Muñoz
3	22/11/2010	Incorpora el periodo de revisión de la política	6	Oscar Muñoz
4	12/03/2012	Declara no realización de actividades de comercio electrónico	6 y 7	Manuel Pérez
5	31/12/2014	Revisión con referencias a Normas ISO 27001:2013 e ISO 27002:2013	Todas	Manuel Pérez
6	10/12/2015	Define roles y funciones de la estructura de administración de Seguridad	4, 6 a 9	Manuel Pérez
7	23/05/2016	Readecuación y reclasificación de textos y secciones del documento, complementando y mejorando la política con aportes de otros organismos públicos	Todas	Tamara Núñez Manuel Pérez
8	26 /07/2019	Incorporación de políticas de ciberseguridad y simplificación	Cambio completo	Roberto Duarte
9	23/07/2021	Actualización por vencimiento de vigencia	Se incorpora Norma de Transferencia de Archivos	Roberto Duarte

Contenido

Política de Seguridad y Ciberseguridad de la Información

Declaración Institucional

La Superintendencia de Salud, hace suyo e incorpora a su quehacer diario, de políticas, normas y procedimientos que regulen el uso, almacenamiento, acceso y distribución de sus activos informáticos.

Para llevar a cabo esta acción, ha implementado un Sistema de Seguridad y Ciberseguridad de la Información, el cual tiene como finalidad 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.

La información, directrices y alcances definidos en el presente documento, como también aquellos derivados de él, como son los que consignan normas y procedimientos de seguridad informática, son susceptibles de mejorar continuamente y, por tanto, ser modificados para mantenerse vigentes de acuerdo a las condiciones requeridas por la autoridad respecto a la seguridad de sus medios tecnológicos.

Respecto de la Seguridad de la Información de las entidades que la Superintendencia regula, desde el Gobierno Central se definieron las directrices[1] que establecen el control en esta materia como una temática de fiscalización que debe aplicarse, independiente de la forma en que la Institución avanza en su propio proceso de Ciberseguridad.

Introducción

La Superintendencia de Salud es un organismo público, sucesor legal de la Superintendencia de Isapres, que inicia sus operaciones el 1 de enero de 2005, conforme lo establece la Ley de Autoridad Sanitaria (Ley N° 19.937).

La misión de la Superintendencia de Salud es proteger y promover los derechos en salud de las personas, con relación a Fonasa, Isapres y prestadores. Sus funciones están determinadas, tanto como establece la Ley de Autoridad Sanitaria, como también en lo indicado en Libros I y II del DFL 1/2005.

En lo referente a Seguridad de la Información institucional, la Superintendencia de Salud en el marco del cumplimiento de las normativas vigentes, el creciente uso de información y la necesidad de cumplir con altos estándares de integridad, confiabilidad y disponibilidad, requiere la habilitación de mecanismos adecuados de seguridad en la organización, estableciendo para ello políticas y procedimientos de seguridad efectivos que disminuyan los riesgos para garantizar la continuidad de sus servicios.

Es por ello que esta Superintendencia asume la responsabilidad de implantar, mantener y mejorar continuamente un Sistema de Gestión de la Seguridad de la Información (SGSI) que permita lograr niveles adecuados de seguridad y ciberseguridad para todos los activos de información institucional considerados relevantes, de manera de garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos en el entorno y las tecnologías.

Esta Política y las Normas Internas específicas de seguridad asociados utilizarán como marco de referencia los requerimientos del D.S. N° 83/2005, del Ministerio Secretaría General de la Presidencia (Seguridad y Confiabilidad de documentos electrónicos). Adicionalmente serán consideradas las buenas prácticas definidas en las normas NCH ISO/IEC 27001-2013 y NCH ISO/IEC 27002-2013, las cuales constituyen el marco rector de todas las iniciativas de seguridad adoptadas por esta Superintendencia.

[1] Decreto Exento N° 2221, del 11 de noviembre 2019, que aprueba Convenio de Colaboración entre al Ministerio del Interior y Seguridad Públicas, Ministerio de Hacienda y las Superintendencias de Educación; Salud; Seguridad Social; Insolvencia y Reemprendimiento; Servicios Sanitarios; Educación Superior; Electricidad y Combustible; Medio Ambiente; y Casinos y Juegos.

Objetivos

La presente Política provee un conjunto de normas destinadas a implementar y mantener un nivel de seguridad y ciberseguridad de la información acorde a los riesgos que se presentan cubriendo los siguientes objetivos:

a) Establecer las expectativas de la Jefatura del Servicio respecto del correcto uso que el personal haga de los recursos de información de la Superintendencia, así como de las medidas que se deben adoptar para la su protección.
b) Establecer, para todo el personal de la organización, la necesidad de la seguridad de la información y promover la comprensión de sus responsabilidades individuales.
c) Determinar las medidas esenciales de seguridad de la información que esta Superintendencia debe adoptar, para protegerse apropiadamente contra amenazas que podrían afectar la confidencialidad, integridad y disponibilidad de la información, ocasionando alguna de las siguientes consecuencias:
    - Pérdida o mal uso de los activos de información (datos, equipos, documentación impresa, etc.).
    - Pérdida de imagen como organismo regulador y fiscalizador de las entidades que participan en el sistema de salud.
    - Interrupción total o parcial de los procesos que soportan el negocio.
d) Proporcionar a todo el personal de la Superintendencia una herramienta que facilite la toma de decisiones apropiada, en situaciones relacionadas con la preservación de la seguridad de la información.
e) Establecer mecanismos de acción que permitan la protección efectiva de ataques de ciberseguridad.
f) Establecer mecanismos que permitan la recuperación de datos frente a la materialización de una vulnerabilidad que produzca pérdida o daño de información.

La información y los distintos medios que la soportan (procesos, sistemas, medios y/o dispositivos tecnológicos y redes de comunicación) representan para la Superintendencia de Salud, herramientas de primera necesidad para el desarrollo de sus funciones como ente regulador y fiscalizador del sistema de salud chileno, por ello la seguridad de esta información cobra especial relevancia, debiendo mantenerse bajo adecuados niveles de resguardo para protegerla de la pérdida, manipulación y/o divulgación no autorizadas. Así mismo, debe estar disponible para todo el personal de la Superintendencia de Salud, y para terceras partes debidamente autorizadas.

Alcance

Esta política se aplica a:

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.
b) 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.
c) 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.
d) Acciones de seguridad que se realizan en el ciberespacio, sus transacciones, almacenamiento y acceso.

La gestión de la seguridad de la información se realizará mediante un proceso sistemático, documentado y conocido por toda la organización basándose en metodologías de mejoramiento continuo. Este proceso de gestión 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 normará las particularidades de cada dominio.

Cada norma interna de seguridad cuenta mecanismos de control y sanciones asociadas al no cumplimiento.

Vigencia y Periodicidad de Evaluación y Revisión de la Política

a) La revisión y mantención de la presente política será realizada por el Oficial (Encargado) de Seguridad de la Información y sus cambios aprobados por el Comité de Seguridad y el Jefe máximo del Servicio, aprobada formalmente mediante Resolución Exenta.
b) La presente política deberá ser revisada y aprobada por el Comité de Seguridad, de acuerdo a las necesidades de la institución a lo menos cada dos años contados desde su publicación. Sin embargo, ésta política podrá ser revisada y actualizada antes de cumplirse este periodo según requerimiento de alguno de sus miembros o por alguna circunstancia coyuntural que lo requiera, que afecten la adecuada protección de la información, considerando como tales entre otros, cambios en la misión, objetivos estratégicos, productos estratégicos, infraestructura, personal y/o procedimientos relacionados con la protección de la información. Hechos los cambios y aprobación, el Oficial de seguridad deberá difundir la nueva versión.

Definición de Roles Claves, Funciones y Atribuciones

Definiciones necesarias para el cumplimiento de la Política de Seguridad de la Información.

ROL	FUNCIONES	RESPONSABILIDADES ESTABLECIDAS PARA LAS FUNCIONES
1.Jefe de servicio	Sancionar y liderar el proceso de Seguridad de la Información	- Aprobar políticas y validar el proceso de gestión de Seguridad de la Información. - Aprobar estrategias y mecanismos de control para el tratamiento de riesgos que afecten a los activos de información institucional, que se generen como resultado de los reportes o propuestas del Oficial de Seguridad y/o del Comité de Seguridad, así como proveer los recursos necesarios para su ejecución.
2.Comité de Seguridad	Definir y establecer los lineamientos generales de seguridad, publicar y aprobar las políticas y demás definiciones en lo que respecta a seguridad de la información	- Aprobar la política y normas de Seguridad de la Información. - Definir las estrategias de la Entidad y sus unidades dependientes sobre temas específicos de seguridad de la información. - Velar por la vigencia, cumplimiento y actualización de las Políticas de Seguridad de la Información de la Entidad y sus unidades dependientes, a través del mantenimiento y difusión de las medidas de protección de la información que conforman el marco normativo, aplicables a toda la información cualquiera sea su forma y/o medio de conservación.
3.Oficial (Encargado) de Seguridad	Gestionar y coordinar actividades de seguridad y ciberseguridad de la información. Velar por el desarrollo del marco normativo y los requerimientos necesarios para garantizar la protección de la información y los medios donde esta reside, sujeto a las políticas de la Organización.	- Velar por el desarrollo del marco normativo y los requerimientos necesarios para garantizar la protección de la información y los medios donde esta reside, sujeto a las políticas de la Organización. - Tener a su cargo el desarrollo de las políticas de seguridad al interior de la organización, su actualización periódica considerando estándares internacionales y por su correcta implementación y aplicación. - Coordinar, en conjunto con las unidades técnicas, la respuesta a incidentes computacionales. - Establecer puntos de enlace con encargados de seguridad de otros organismos públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes. - Hacer cumplir la "Norma Técnica sobre Seguridad y Confidencialidad del Documento Electrónico", contenida en el Artículo primero del Decreto N°83, del Ministerio Secretaría General de la Presidencia. - Hacer cumplir el Instructivo Presidencial N°8 del 23 de octubre de 2018 sobre ciberseguridad. - Revisar y proponer al Jefe del Servicio y al Comité de Seguridad de la Información, las opciones de mejora en el sistema de gestión de seguridad, así como de los incidentes relevantes y su solución.

ROL	FUNCIONES	RESPONSABILIDADES ESTABLECIDAS PARA LAS FUNCIONES
4. Custodio de Datos	Todas las Jefaturas de cada una de las áreas de la Institución, respecto a la información correspondiente a sus áreas de trabajo. La responsabilidad sobre los datos no se puede delegar, y solamente se puede asignar a un colaborador de su respectiva área las tareas operativas de administración y control de las medidas de seguridad correspondientes a su información.	- Identificar toda la información y procesamiento de la misma que corresponde a su área de responsabilidad cualquiera sea su forma y medio de conservación. - Clasificar todos los datos de su propiedad de acuerdo con el grado de criticidad de los mismos. - Documentar y actualizar periódicamente la clasificación de datos efectuada. - Asegurar que el personal tenga el acceso apropiado a los datos de acuerdo con sus respectivas funciones de trabajo. - Llevar un adecuado registro de los usuarios permitidos a acceder a su información. - Conservar las llaves y/o combinaciones para acceder a las cajas de seguridad propias donde se conserva la información considerada como secreta. - Autorizar cualquier transmisión, envío, impresión y/o destrucción de información considerada secreta. - Autorizar a los usuarios el acceso en los equipos / servicios / aplicaciones sobre la base de apropiados permisos a implementar a través de un software de control de acceso. - Definir los eventos de seguridad adicionales que considere necesario para la protección de su información. - Conservar la información relacionada con la encriptación de los datos considerados secretos.
5. Administrador de Seguridad de la Información	Tiene a su cargo, en conjunto con las personas que designe, la administración de la seguridad de cada uno de los equipos y/o servicios donde se procese información. Esta función corresponde a la Jefatura del Subdpto. de Tecnologías de la Información.	- Aplicar mecanismos tecnológicos y/o de procedimientos para llevar a cabo las políticas de seguridad de la información. - Revisión y actualización permanente de procedimientos y/o protocolos específicos derivados de las políticas y normas internas de seguridad vigentes. - Registrar y gestionar incidentes de seguridad, en el marco de administración y gestión de riesgos de seguridad; proponer y ejecutar acciones específicas para resolver situaciones de riesgo. - Reportar periódicamente al Encargado de Seguridad y al Comité de Seguridad, de los incidentes registrados en el período y su solución aplicada. - Proponer estrategias y soluciones específicas para la implantación de controles necesarios para cumplir con las políticas de seguridad establecidas. - Administrar todas las solicitudes de creación, baja y modificación de permisos relacionados con los accesos de los usuarios a los respectivos equipos y aplicaciones. - Mantener actualizada una lista de todos los usuarios con permisos de acceso en sus equipos. - Asistir a los usuarios en las tareas relacionadas con la protección de los datos. - Confirmar periódicamente que solamente los usuarios autorizados tengan acceso a los equipos. - Implementar todas las medidas de seguridad definidas para su correspondiente equipo. - Mantener un archivo con los documentos de soportes de las tareas relacionadas con la seguridad.
6. Custodio Físico	Se establecen como Custodios Físicos de la información a las respectivas jefaturas o encargados de áreas que son: - Los responsables de los archivos centralizados de la información en soportes escritos; - Los usuarios finales que conserven en su poder los soportes de información; - Los responsables de cada uno de los centros de cómputos o sitios donde se encuentren los equipos de procesamiento centralizado, de	- Implementar las medidas de seguridad física definidas para la protección de la información. - Solicitar la asistencia del Comité de Seguridad en caso de necesitar adaptar las definiciones de la normativa a casos específicos. - Disponer la efectiva custodia de las claves de mayor riesgo de los equipos / servicios / aplicaciones conservadas en sobre cerrado.

ROL	FUNCIONES	RESPONSABILIDADES ESTABLECIDAS PARA LAS FUNCIONES
	comunicación y/o de almacenamiento.	
7. Personal y Usuarios de los recursos en general	Corresponde al personal de planta, contrata, honorarios y personal externo que preste servicios a la institución. Se incluye a los prestadores de servicios, proveedores y cualquier entidad externa que pueda hacer uso autorizado de la información de la Superintendencia.	- Operar los procesos institucionales, cumpliendo con las políticas y normativas de seguridad correspondientes. - Hacer uso de activos de información institucionales, cuidando que se cumplan a cabalidad todas las normas que permitan garantizar su integridad, disponibilidad y confidencialidad. - Cumplir con las Políticas de Seguridad de la Información, Normas y Procedimientos específicos de seguridad. - Usar los activos tecnológicos y de información de la Institución o Servicio solamente para fines propios de ellas. - Poner en conocimiento de la Administración cualquier situación detectada, que pueda poner en peligros la seguridad de la información.

Disposiciones Generales

Las siguientes disposiciones generales aplicarán para el cumplimiento de la Política de Seguridad de la Información:

De la Información Interna

a) La información es un activo vital y todos sus accesos, usos y procesamiento, deberán ser consistentes con las políticas y estándares emitidos por esta Superintendencia.
b) La información debe ser protegida, por sus custodios, de una manera consistente con su importancia, valor y criticidad, siguiendo las reglas establecidas en las políticas específicas de seguridad de la información, sus procedimientos asociados y las recomendaciones dadas por el responsable designado de dicha información. Para ello la Superintendencia proveerá los recursos que permitan implementar controles para otorgar el nivel de protección correspondiente al valor de los activos.
c) Toda la información creada o procesada por la organización debe ser considerada como "Pública", a menos que se determine otro nivel de clasificación, pudiendo ser "Reservada" o "Secreta" de acuerdo a lo establecido en el ordenamiento jurídico vigente. Periódicamente se deberá revisar la clasificación, con el propósito de mantenerla o modificarla según se estime apropiado.
d) La Superintendencia de Salud proveerá los mecanismos para que la información sea accedida y utilizada por el personal que acuerdo a sus perfiles y funciones asignadas. La institución se reserva el derecho de revocar privilegios de acceso a la información y tecnologías que la soportan, si la situación y las condiciones lo ameritan.
e) La Superintendencia de Salud, en relación a los activos de información, declara que no realiza comercio electrónico a través de las redes públicas ni de otra índole. Se agrega que toda relación contractual con proveedores externos, se circunscribe a procedimientos y canales de comunicación establecidos en la normativa vigente para las instituciones públicas, enmarcada en la Ley N° 19.886 (Ley de Compras) y su Reglamento.
f) Todo incidente que afecte a la información institucional en lo relativo a su seguridad, deberá ser tratado con la mayor discreción, buscando en todo momento preservar la confidencialidad de la información. Se deberán tener procedimientos actualizados que especifiquen cuando y a qué autoridades (regulatorias, de supervisión, contraloras), se debería contactar y cómo se deben informar los incidentes de seguridad identificados de manera oportuna.
g) Todos los funcionarios deberán firmar un documento llamado *"Acuerdo de Confidencialidad y Aceptación de Políticas de Seguridad de la Información de la Superintendencia de Salud"*, cuyo objetivo es establecer con claridad a cada funcionario, sus deberes respecto de la forma de proteger la información que tendrán a disposición, dadas las funciones que desarrollan en el ejercicio de su trabajo, aun cuando haya cesado su vínculo contractual con la institución.

De la Información de Usuarios Externos

a) Si la institución procesa y mantiene información de usuarios externos que sean datos personales y/o sensibles de acuerdo a la normativa vigente, la Superintendencia se

compromete a asegurar que esta información no será divulgada sin previa autorización y estará protegida de igual manera que la información interna.

b) Si se requiere compartir información de usuarios externos con instituciones externas, a éstas se le exigirá la firma de un contrato y/o convenio de confidencialidad y no divulgación previa a la entrega de la información.

De la Supervisión y Evaluación de Seguridad

Con objeto de verificar la efectividad de las normas, estándares y procedimientos establecidos en materia de seguridad y derivados de esta política, se establecen las siguientes directivas:

a) 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) Cada área o unidad de la institución debe dar cumplimiento a las indicaciones que la institución dispone establecidas en la Política de Seguridad de la Información y las respectivas normas vigentes derivadas de esta política. Se realizarán verificaciones mediante los mecanismos que establece Gobierno Digital ajustándose al calendario que se establezca oportunamente con el área seleccionada.

c) Con objeto de respetar el carácter confidencial de la información, se requiere que todo el personal de la Superintendencia se conduzca conforme a esta política, normas, estándares y procedimientos establecidos.

Del compromiso de la Alta Dirección Institucional

a) Para los efectos de organización interna de las coordinaciones y directrices sobre seguridad de la información, y para el control de implementación del proceso del sistema de seguridad, en la institución funcionará un Comité de Seguridad, además deberá existir un(a) Oficial o Encargado(a) de Seguridad y Ciberseguridad de la Información (en adelante Oficial de Seguridad), que actuará como asesor del Jefe de Servicio, en las materias relativas a seguridad.

b) La institución deberá abordar el tema de seguridad de la información en toda administración de proyectos, sin importar su tipo.

c) La Dirección del Servicio propiciará la existencia de mecanismos o procedimientos formales que permitan asegurar la continuidad del negocio ante situaciones que impidan el acceso a la información imprescindible para el funcionamiento de la organización.

Deberes del Personal

a) La información y las tecnologías de información deben ser usadas sólo para propósitos relacionados con el servicio, debiéndose aplicar criterios de buen uso en su utilización.

b) Las claves de acceso a la información y a las tecnologías de información son individuales, intransferibles y de responsabilidad única de su propietario.

c) El personal está en la obligación de alertar, de manera oportuna y adecuada, cualquier incidente que atente contra lo establecido en esta política según procedimientos establecido en el manejo de incidentes.

d) Está absolutamente prohibido al personal de la organización divulgar cualquier información que según el ordenamiento jurídico esté catalogada como "Reservada", "Secreta" o "Sensible".

e) Todo el personal deberá respetar las normas, estándares, y procedimientos de seguridad de la información derivados de la presente política.

f) El personal será responsable de proteger la información y recursos bajo su uso, custodia o que sean puestos a su disposición para la realización de sus labores, siguiendo las normas, estándares, y procedimientos definidos para tales efectos por la Superintendencia de Salud.

g) Las distintas áreas deberán cumplir los controles de seguridad de la información necesarios para proteger los activos informáticos de la organización.

Difusión de la Política y Normas Internas de Seguridad de la Información

a) Para que la presente política se integre a la cultura organizacional, debe existir un plan formal y periódico de difusión, capacitación y sensibilización en torno a la seguridad de la información. El responsable de la definición y ejecución de este Plan será el Oficial de Seguridad.
b) La presente política y las normas de seguridad de la información que emanen de ella, será difundida ocupando el medio de difusión que sea el más adecuado para alcanzar a la totalidad de los funcionarios, indicando el sitio en donde quedará disponible (publicada) de forma permanente para las consultas de toda la organización. Esta misma indicación se hará a terceras partes que puedan hacer uso de la información de la Superintendencia y que hayan sido debidamente autorizadas para ello (prestadores de servicios, proveedores y cualquier persona o entidad externa).
c) La Dirección del Servicio, mediante la estructura definida en la sección "Definición de Roles Claves, Funciones y Atribuciones", procurará que todo el personal reciba un entrenamiento suficiente y coherente con sus necesidades y el rol que tenga dentro de la Superintendencia.

Evaluación de Cumplimiento y Sanciones

a) La presente Política General de Seguridad de la Información entra en vigencia una vez oficializada por el Superintendente de Salud mediante Resolución Exenta. Las jefaturas de las distintas áreas y unidades de la institución serán responsables de ponerlas en conocimiento de su personal subordinado.
b) La presente política está alineada con las directrices de las leyes y regulaciones existentes.
c) Cualquier conflicto con estas regulaciones debe ser informado inmediatamente al Oficial o Encargada(o) de Seguridad, responsable de este documento.
d) Se aplicarán las sanciones correspondientes al incumplimiento de las normas, estándares, guías de mejores prácticas y procedimientos derivados de la presente política.
e) Toda violación o incumplimiento de las políticas de seguridad y su cuerpo de normas será sancionada de acuerdo a las indicaciones establecidas en la Ley N° 18.834 sobre Estatuto Administrativo, evaluando la gravedad e intencionalidad manifiestas.

Marco legal

- Ley 18.834, del Ministerio de Hacienda, sobre Estatuto Administrativo
- Ley 19.628, Protección de la vida privada
- Ley 19.799, Documentación Electrónica, Firma Electrónica y servicios de certificación de dicha firma
- Ley 20.285, Acceso a Información Pública
- Ley 19.880, Procedimientos Administrativos que rigen los actos de los órganos de la administración del estado
- Ley 19.223, Delitos Informáticos
- Ley 17.336, Propiedad Intelectual
- Ley 19.927, Que modifica Código Penal, Código de Procedimiento Penal y Código de Procesal Penal en materias de delitos de Pornografía Infantil
- 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 de 2004, Seguridad y Confidencialidad de documentos electrónicos
- Decreto 77 de 2004, Eficiencia de las comunicaciones electrónicas
- 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
- Decreto 93 de 2006, Minimizar efectos perjudiciales de los mensajes electrónicos masivos
- Decreto 100 de 2006, Desarrollo de sitios Web

- Decreto 158 de 2007, Modifica Decreto 81 sobre Interoperabilidad de documentos electrónicos
- Instructivo Presidencial N° 5 de 2001, Desarrollo de Gobierno Electrónico
- Instructivo Presidencial N° 6 de 2005, Implementación y uso de firma electrónica
- Instructivo Presidencial N° 8 de 2006, Transparencia activa y publicidad de la Información
- Instructivo Presidencial 008 del 23 de octubre de2018 sobre Ciberseguridad
- Decreto Exento N° 2221, del 11 de noviembre 2019.

Normas – Políticas Internas

Adicionalmente, esta política de seguridad contiene un cuerpo de normas que son la base para la aplicación de las políticas:

Norma N° 1: Tratamiento de la información

Objetivo

Identificar y clasificar la información disponible en la institución en todas sus formas y medios, de acuerdo con su criticidad, con la finalidad de establecer un tratamiento y manejo que asegure su confiabilidad, integridad y disponibilidad.

Responsables del cumplimiento

Todo el personal de la institución y los terceros, que interactúan de manera habitual u ocasional, que accedan a la información y/o a los recursos informáticos para el desarrollo de sus tareas habituales.

Incumplimientos

Las medidas disciplinarias están descritas en el Anexo de Sanciones por incumplimientos que forma parte del conjunto de medidas disciplinarias de la Superintendencia.

Responsables

Todos los usuarios, Administradores de Seguridad, Custodio de las Datos, las Unidades de Informática, Jefe de Servicio, Directores, Jefaturas de Intendencias, Jefaturas de Departamento y Subdepartamentos y la Unidad de Gestión de Personas son responsables del cumplimiento de este procedimiento.

Disposiciones de la norma

Es norma en la institución, respecto de:

Definición de información[2]

Se considera **información** a todo dato, cualquiera sea su formato y medio de comunicación y/o conservación:

- Formularios en papel y/o comprobantes propios, y/o de terceros
- Información en los sistemas y/o informes, documentos y reportes impresos
- Contenidos en soportes magnéticos móviles y/o fijos institucionales
- Contenidos en video y/o audio y datos almacenados en el ciberespacio

Definición de Encargado Administrativo de los Datos (según NCH-ISO 27002)

Se considera como **"Encargado Administrativo de los Datos"**, al usuario(a) o funcionario(a) con las habilidades y responsabilidades asignadas y suficientes para gestionar el "control, producción, desarrollo, mantenimiento, uso y seguridad de un activo de información". También se utiliza la denominación "Dueño de los Datos" de la unidad de negocio, estableciendo que el término "dueño" no significa que la persona tiene derechos de propiedad sobre el activo.

Riesgos de la Información

El Encargado Administrativo de los Datos, en conjunto con el Área de Informática, deben identificar los riesgos a los que está expuesta su información a cargo, considerando la posibilidad de que personal interno y/o externo realice una divulgación no autorizada, modificación indebida, pérdida o destrucción de los soportes que la contienen.

Para disminuir y/o eliminar los riesgos en el manejo de información, se deberán segregar los deberes y áreas de responsabilidad para reducir las oportunidades de modificación o uso indebido no autorizado o no intencional de los activos de información institucionales[3].

El Encargado de Seguridad, en conjunto con el Área de Informática y Recursos Humanos, deberá desarrollar y mantener actualizado un documento de *"Acuerdo de Confidencialidad y no Divulgación"* que refleje la protección de la información involucrada de la institución en. Este documento deberá servir para el compromiso con los

[2] ISO 27002:2013 A.8.1.2 b
[3] ISO 27002:2013 A.6.1.2

funcionarios(s) internos como también de terceros externos que interactúen en tareas de la Superintendencia de Salud[4].

Criterios básicos para clasificar la información

El Encargado Administrativo de los Datos, el Oficial de Seguridad, en conjunto con el Área de Informática, debe analizar su información para proceder a su clasificación, basándose principalmente en los perjuicios que pudiera ocasionarle a la institución, y/o al personal, el incumplimiento de las definiciones y normas de seguridad de la información definidas en la Política General[5]. Complementariamente se deben considerar las definiciones involucradas en leyes y/o reglamentaciones vigentes.

Se deberá explicitar aspectos relacionados con la rotulación para activos de información, teniendo a su vez en consideración el etiquetado de la documentación de salida que es considerada como sensible[6].

Tipos de información

El Encargado Administrativo de los Datos en conjunto con el Área de Informática, deben clasificar toda su información teniendo en cuenta la criticidad[7], en cuanto a:

Información de acceso público

Es toda aquella información que no representa riesgo significativo para la institución y para la cual no es necesario establecer restricciones especiales, más allá de las recomendaciones sobre su buen uso y conservación.

Información Reservada (o de acceso autorizado)

Es toda información cuyo acceso indebido podría presentar riesgos para la institución, y cuyo acceso debe ser expresamente autorizado por el encargado administrativo de los datos y/o Jefe de Proyecto usuario, y restringida a un grupo reducido de usuarios que la necesite para el desarrollo de sus tareas habituales, quienes deben cumplir con las siguientes consideraciones:

- **Autorización.** Su acceso y disponibilidad debe estar expresamente autorizado, el acceso a los sistemas debe establecerse a través de un adecuado control. El usuario administrador de sistemas debe definir los tipos de permisos que dará a los usuarios, ya sea como lectores o con privilegios para copiar, modificar y/o eliminar información.
- **Conservación**. Se conservará exclusivamente en los equipos de procesamiento centralizados, asegurando su inclusión en los procesos de respaldo y planes de recuperación del procesamiento. En caso que un funcionario requiera utilizar información de carácter reservada como una forma de apoyar un proceso de trabajo almacenándola en un PC, deberá tomar los resguardos para su eliminación luego de utilizarla. Para todo tipo de información, deben implementarse políticas de "escritorios vacíos" conservando todo documento impreso en forma segura; el concepto de escritorio vacío se extiende a las pantallas de los puestos de trabajo, los que deben considerar un mecanismo de bloqueo automático cuando el equipo queda desatendido[8].
- **Envíos.** El Área de Informática debe proveer herramientas que controlen la integridad, exactitud, confidencialidad e inviolabilidad de los datos transmitidos electrónicamente, asegurando la correcta recepción del envío por parte del destinatario. Los envíos y/o transmisión de los datos deberán considerar todos los resguardos que indiquen las políticas, procedimientos y controles formales de transferencia de información mediante el uso de las instalaciones de comunicación existentes[9]. Otra consideración especial respecto de envíos de información, corresponde a **acuerdos para la transferencia de información entre la institución y partes externas**. El Subdepartamento Informática debe mantener actualizado un procedimiento que considere:
  - Administración de responsabilidades para notificar y controlar la transmisión el despacho y recepción de información

[4] ISO 27002:2013 A.13.2.4
[5] ISO 27002:2013 A.8.2.1
[6] ISO 27002:2013 A.8.2.2
[7] ISO 27002:2013 A.8.2.1
[8] ISO 27002:2013 A.11.2.9
[9] ISO 27002:2013 A.13.2.1

- Normas técnicas de la transmisión
- Responsabilidades en caso de incidentes de seguridad
- Mantención de cadena de custodia durante el tránsito de información.
- Niveles aceptables de control de acceso[10].

- **Impresión.** Se debe evitar la impresión de documentos más allá de lo necesario para efectuar las tareas diarias.
- **Divulgación a terceros.** Se deben instrumentar convenios de confidencialidad con terceros que necesariamente deban y/o puedan acceder a información institucional para desarrollar sus actividades (por ejemplo, personal de mantenimiento de equipos, y/o de limpieza, etc.). No se debe transmitir información en forma verbal y/o escrita a personas externas sin la autorización expresa del encargado administrativo de los datos y/o Directivos superiores. En los contratos con terceros, que involucren información institucional, se debe indicar en forma expresa la ley que regula la temática de seguridad de la información (Ley N° 19.628 sobre datos personales y DS N° 83 sobre documento electrónico y seguridad de la información).
  Todos los funcionarios, personal a honorarios y terceros, deben conocer las restricciones al tratamiento de datos y de la información a la cual tengan conocimiento por motivo del ejercicio de sus funciones. La toma de conocimiento se realiza según el tipo de contrato, es decir:
  - Funcionarios, según lo establecido en la Ley 18.834 sobre Estatuto Administrativo.
  - Honorarios, a través de cláusula de confidencialidad que debe contener obligatoriamente el contrato de honorarios.
  - Terceros, según lo establezca el Acuerdo de Confidencialidad específico que debe obligatoriamente contener el contrato con terceros

  Mediante esos instrumentos, los funcionarios, personal a honorarios y terceros, se comprometen a utilizar la información solamente para el uso específico de sus labores y a no comunicar, diseminar, o hacer pública la información a ninguna otra persona, firma, compañía, o terceros, salvo previa autorización escrita de sus Jefaturas y/o Supervisores directos.
  El ejercicio de funciones y conocimiento de información, se realizará en el contexto de las siguientes leyes: Ley 19.628, sobre protección a la vida privada, Ley 20.285 sobre acceso a la información pública, Ley 18.834 sobre Estatuto Administrativo.
- **Destrucción.** Para la destrucción de información y sus correspondientes soportes lógicos y/o físicos, se requiere la autorización del Encargado de Seguridad y de Auditoría Interna, basada en el informe de riesgos que deberá entregar el usuario encargado administrativo de los datos. Para el caso de documentos en papel, se debe seguir el procedimiento del Sistema Documental de Oficina de Partes[11].
  Adicionalmente se necesita la aprobación de expurgo de la Dirección Regional del Ministerio de Bienes Nacionales para la eliminación de medios físicos de almacenamiento, como es el caso de cintas magnéticas de respaldo de datos.
- **Información sensible.** Es toda aquella información de acceso autorizado, según indicaciones de Ley N° 19.628 (Habeas Data), que puede presentar riesgos importantes para la institución, y que debe cumplir con medidas adicionales de seguridad para limitar y proteger su uso:

  El Área Operaciones y Redes del Área de Informática hará monitoreo de archivos con información sensible en cualquiera de las siguientes situaciones:
  - Generación de copias de respaldo.
  - Conservación de accesos en LOG de eventos.
  - En caso de encriptación y desencriptación de información sensible, el Área de Informática debe conservar toda información clave para la ejecución de tales procesos.
  - Para reportes conteniendo información sensible, solo deben tener acceso los usuarios autorizados por el encargado administrativo de los datos.

[10] ISO 27002:2013 A.13.2.2
[11] ISO 27002:2013 A.8.1.2 d

- Para la destrucción de soportes impresos con información sensible, se deben utilizar trituradoras de papel.
- El uso de información sensible No está permitido para propósitos de prueba en los desarrollos y/o implementación de sistemas, salvo expresa autorización del Encargado Administrativo de los Datos y Encargado de Seguridad institucional.

Información propia de los usuarios en los sistemas
Toda información que es generada y tratada por los usuarios en los equipos que le ha asignado la institución, debe ser almacenada en un directorio o carpeta LABORAL que está incluida en los procesos de respaldo periódico. En todos los casos se seguirán las pautas y normativa definida en la Política de Seguridad de la Información institucional.
Información involucrada en aplicaciones que pasen a través de redes públicas
Esta información deberá ser protegida de actividad fraudulenta, acceso y/o modificación no autorizada mediante autenticación, requisitos de protección de información confidencial y protección que evite pérdida o duplicación de la información transaccional. También se deberá proteger evitando la transmisión incompleta, enrutamiento incorrecto mediante técnicas tales como firma electrónica, autenticación punto a punto, protocolos de comunicación protegidos y/o certificados digitales de confianza[12].

Obligaciones especiales según la Ley N° 19.628 de Habeas Data
Para cumplir con los requerimientos particulares de la Ley N° 19.628 sobre PROTECCION DE LOS DATOS PERSONALES, la institución debe definir en conjunto con el área legal, si algunas o todas sus bases de datos se encuentra dentro de las definiciones de la ley de Protección de Datos Personales[13].
En caso de que así lo estuvieran, deberá cumplir con:

- **Inscripción.** Toda Base de Datos con alcance en la Ley N° 19.628, debe ser inscrita en el Registro de Bases de Datos que se administra en el Servicio de Registro Civil, de acuerdo a lo instruido en la ley.
- **Responsabilidades sobre los datos.** Se considera a la persona cuyos datos figuren en los archivos como Titular de los datos, mientras que a la institución se la considera responsable y/o usuaria de los datos.
- **Utilización de datos personales.** No pueden ser utilizados los datos personales para fines distintos a los que motivaron su obtención, uso para el cual el titular de los datos debió consentir expresamente. Cuando dichos datos no sean necesarios para los fines para los que se recolectaron, deben ser destruidos. No es necesario el consentimiento cuando los datos deriven de una relación contractual, científica o profesional del titular de los datos y resulten necesarios para su desarrollo o cumplimiento.
- **Derecho de acceso, rectificación, actualización y supresión de datos por parte del titular de ellos.** Toda persona cuyos datos personales estén contenidos en bases de datos institucionales, tiene el derecho de ser informado en cuáles bases de datos está, y adicionalmente cual es el contenido de dichos datos, tanto en los sistemas como en los reportes impresos, y puede solicitar a la institución que proceda a la rectificación, actualización, supresión y/o sometimiento a confidencialidad, en caso de que se observen errores.
- **Implementar medidas de seguridad en los sistemas.** La institución, como responsable o usuaria del archivo de datos, debe adoptar todas las medidas técnicas y organizativas necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado y que permitan detectar los riesgos que provengan de la acción humana o del medio técnico utilizado.
- **Personal que accede a datos personales.** Todo el personal que acceda a bases de datos institucionales que contengan datos personales, debe cumplir con los requerimientos de secreto profesional.

[12] ISO 27002:2013 A.14.1.2 / A.14.1.3
[13] ISO 27002:2013 A.18.1.4

- **Datos personales.** Se consideran datos de carácter personal o datos personales, los relativos a cualquier información concerniente a personas naturales, identificadas o identificables.
- **Datos sensibles.** Se deben considerar como datos sensibles, a todos los datos personales que revelen origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual. Estos datos no pueden ser transmitidos a ningún tercero.
- **Transmisión de datos.** Solicitar la autorización expresa a la persona cuando sea necesaria la transmisión de sus datos personales a un tercero.
- **NOTA**

Implementación de medidas adicionales de seguridad

Para el tratamiento de datos acorde con las obligaciones que impone la ley n° 19.628 de protección a los datos personales, considerando las definiciones contenidas en la ley:
Para el tratamiento de la información en funciones específicas, tales como consulta de BD en el trabajo diario y/o transmisión de datos entre unidades o hacia el exterior de la institución, se debe hacer uso de controles criptográficos y/o metodologías de encriptación de datos para los nuevos desarrollos, que garanticen su uso adecuado, protegiendo la confidencialidad, la autenticidad y/o la integridad de la información[14].
Para ello se debe implementar una política sobre el uso y administración de controles criptográficos o metodologías de encriptación, considerando:

- Un enfoque de administración hacia el uso de controles criptográficos en toda la institución
- Uso de métodos de encriptación para proteger la información que se transporte en medios móviles o extraíbles o a través de líneas de comunicación
- Enfoque de administración de claves
- Definición de responsabilidades de implementación de la política y la administración de claves, incluida la tarea de generación de ellas.
- Aplicar cifrado o encriptación para la protección de información sensible o crítica, almacenada o transmitida
- Uso de firmas digitales que verifiquen la autenticidad de los mensajes y/o la integridad de la información almacenada o transmitida, sensible o crítica
- Uso de técnicas criptográficas para brindar evidencia de la ocurrencia o no de un evento o acción.
- Uso de técnicas criptográficas para autenticar a los usuarios u otras entidades que soliciten acceso o realicen transacciones con usuarios, entidades y/o recursos de la plataforma institucional.
- La administración de claves debería considerar[15]:
  - Generación de claves con emisión y obtención de claves públicas
  - Distribución de claves incluyendo el procedimiento de activación luego de la entrega
  - Almacenamiento incluyendo método de acceso de los usuarios
  - Procedimiento de cambio o actualización de claves
  - Procedimiento para eliminar claves, incluido la forma de retirar y desactivar claves por desvinculación de usuarios
  - Recuperación de claves corruptas o perdidas.
  - Destrucción de claves
  - Registro y auditoría de las actividades de administración de clave

[14] ISO 27002:2013 A.10.1.1
[15] ISO 27002:2013 A.10.1.2

Norma N° 2: Gestión de Identidad

Objetivo

Asegurar la oportuna creación, actualización y eliminación de privilegios de acceso de usuarios, considerando su perfil de cargo y las necesidades de acceso a los diversos sistemas de información, asegurando un adecuado y oportuno ejercicio de sus funciones.

Alcances

Esta norma es aplicable al ingreso, cambio de cargo y desvinculación de un empleado de la institución y al personal externo que realiza trabajos en las instalaciones de la institución y, en general, a toda persona que requiera o cuente con accesos a:

- Datos
- Sistemas Operativos
- Sistemas de Aplicación
- Bases de Datos
- Otros Recursos Informáticos

Responsables del cumplimiento

Todos los usuarios, Encargado de Seguridad, Administradores de Seguridad, Custodio de las Datos, las Unidades de Informática, Jefe de Servicio, Directores, Jefaturas de Intendencias, Jefaturas de Departamento y Subdepartamentos y Gestión de Personas son responsables del cumplimiento de esta norma.

Incumplimientos

Las medidas disciplinarias están descritas en el Anexo Sanciones por incumplimientos que forma parte del conjunto de medidas disciplinarias de la institución.

Registros de Control

La Unidad de Tecnologías de Información a través del área de Operaciones y Redes y Soporte a Usuarios en conjunto con la Unidad de Gestión de Personas son responsables de construir los procedimientos de gestión de identidad.

Disposiciones de la norma

Es norma de la institución:

Generalidades

- Toda persona que tenga acceso al equipamiento (hardware), información y/o aplicaciones (software), redes y servicios asociados de propiedad de la Superintendencia, debe ser autorizada e individualizada mediante una identificación, y una contraseña, lo que constituye una "cuenta de acceso", asignada y administrada por el Área de Informática[16].
- Los accesos de los usuarios a sistemas (o aplicaciones) y/o información clasificada, serán otorgados cuando éstos tengan alguna relación laboral con la institución y de acuerdo al perfil del cargo que ejercerán o sólo cuando sean solicitados por un responsable de su supervisión.
- Los procesos de vinculación, cambios de puestos de trabajo y desvinculación de funcionarios, deberán considerar las coordinaciones y comunicaciones necesarias y oportunas para la creación, modificación y/o eliminación de cuentas y los correspondientes privilegios de acceso[17] a redes y servicios de red. La responsabilidad de las coordinaciones adecuadas a la gestión de privilegios y permisos de acceso, corresponderá a las jefaturas directas, el área de Recursos Humanos y el área de Informática.
- El Área de Informática es la encargada de administrar la plataforma tecnológica de la Superintendencia y para ello debe contar con los procedimientos y herramientas de administración suficientes para el desarrollo de las tareas de monitoreo.

Cuentas de usuario

Manejo de Cuentas

- Los tipos de cuenta son:
  - **Cuentas de acceso interno**, permiten acceso a red interna, sistemas de información, áreas de uso compartido, correo electrónico y equipamiento computacional.
  - **Cuentas de acceso remoto**, permiten acceso desde el exterior a zonas

[16] ISO 27002:2013 A.9.2.2
[17] ISO 27002:2013 A.7.3.1

delimitadas definidas según la función que se requiera desarrollar.

- La solicitud de acceso de usuarios nuevos de cuentas se realizará a través de la Unidad de Gestión de Personas, que por su parte tiene la responsabilidad de establecer el perfil de los usuarios con las correspondientes jefaturas de los funcionarios de cada unidad.
- La solicitud de bajas de usuarios se realizará a través de la Unidad de Gestión de Personas, que comunicará las acciones a seguir, a través del Sistema de Mesa de Ayuda a la Unidad de Soporte a Usuarios de la Unidad de Tecnologías de Información.
- La solicitud de modificaciones de usuarios lo realizarán las correspondientes jefaturas a través del Sistema de Mesa de Ayuda a la Unidad de Soporte a Usuarios de la Unidad de Tecnologías de Información.
- Las unidades de Área Operaciones y Redes y Soporte a Usuarios del Área de Informática son las unidades encargadas de crear y administrar las cuentas de usuarios según los perfiles de cargo ya señalados[18].
- Las cuentas de usuario dan acceso a utilizar un computador personal, redes, servicios de red e información clasificada de propiedad institucional, elementos que pueden ser utilizados sólo para las funciones asignadas.
- Toda cuenta de acceso a la red institucional tiene también privilegios de acceso a las áreas comunes de almacenamiento de archivos.
- Las cuentas especiales con altos privilegios deberán ser solicitadas por las correspondientes jefaturas a través del Sistema de Mesa de Ayuda a la Unidad de Soporte a Usuarios de la Unidad de Tecnologías de Información y autorizadas por la jefatura de la Unidad de tecnologías de Información.

Manejo de contraseñas

- La contraseña debe ser conocida únicamente por el usuario propietario de la cuenta, que la puede modificar a su arbitrio para una mayor protección.
- Cada usuario será responsable de la confidencialidad y uso de su contraseña de red y para cada sistema que tenga acceso. Si un usuario entrega su cuenta y contraseña a un tercero, será igualmente responsable de las acciones que se realicen bajo su perfil computacional.
- Diariamente se verifica la debilidad de las contraseñas. Si no cumple con los estándares mínimos de seguridad, se envía un mensaje al usuario para que cambie su clave e incorpore otra de mayor nivel.
- Las contraseñas serán proporcionadas de manera segura y se deben entregar por escrito.
- Las contraseñas de acceso creadas por los funcionarios deben ser difíciles de descubrir por terceros, se sugiere mezclar caracteres alfanúmeros y numéricos.
- Los sistemas de información deben validar la robustez de las contraseñas.
- No se permitirá reutilizar una clave utilizada en período reciente.
- Las contraseñas deben ser únicas para cada funcionario y deben cumplir a lo menos con los siguientes requisitos:
  - Deben contener caracteres alfanuméricos y numéricos
  - No deben contener nombres o apellidos del usuario(a)
  - No debe contener palabras completas
- La contraseña temporal de una cuenta de usuario se creará con fecha de expiración, de modo de obligar su cambio durante el primer acceso.
- Las contraseñas de cuentas de administrador deben ser generadas por el Administrador de Windows del Área de Informática.
- Para los dispositivos de red (routers, firewalls, switches), no se permitirá la administración remota, y su acceso se permitirá solo a personal autorizado y en forma directa.

Acceso a sistemas de información

- Toda aplicación se debe acceder mediante su identificación y contraseña y permitir al usuario usar sus funcionalidades de acuerdo a su perfil de acceso.
- Los cambios en los perfiles de acceso de los usuarios a los sistemas serán determinados por las jefaturas directas y administrados por el usuario administrador del mismo. En caso de no contar con las herramientas para hacerlo, estos cambios deben ser solicitados al Área de Informática, según el procedimiento definido para ello.

[18] ISO 27002:2013 A.9.2.5

- Los sistemas de información deben poseer las herramientas necesarias para administrar los perfiles de los distintos usuarios que accederán a ellas. Adicionalmente se deberá tener en consideración:
  - Denunciar toda irregularidad que el funcionario(a) observe o tome conocimiento respecto al resguardo y seguridad de la información.
  - Las referencias anteriores deben ser de cumplimiento permanente en cualquier cargo y/o puesto de trabajo que el funcionario este sirviendo en la institución.
  - Ante una situación de cese de funciones, la institución seguirá el procedimiento correspondiente para la recepción de todos los activos asignados y/o de responsabilidad del funcionario que se desvincula[19].

Registros de Control

Los registros de control serán almacenados en el Sistema de Mesa de Ayuda que administra la Unidad de Soporte de la Unidad de Tecnologías de Información.

[19] ISO 27002:2013 A.7.1.2

Norma N° 3: Respaldo y Recuperación de la Información

Objetivo

Definir reglas que aseguren una adecuada generación, resguardo, mantenimiento y recuperación de la información de la Institución, almacenada en unidades de respaldo para para resguardar la continuidad operativa necesaria para el funcionamiento Institucional[20].

Responsables del cumplimiento

Todos los usuarios, Administradores de Seguridad, Custodio de las Datos, las Unidades de Informática, Jefe de Servicio, Directores, Jefaturas de Intendencias, Jefatura de Departamento y Gestión de Personas son responsables del cumplimiento de este procedimiento.

Incumplimientos

Las medidas disciplinarias están descritas en el Anexo Sanciones por incumplimiento, que forma parte del conjunto de medidas disciplinarias de la Superintendencia de Salud.

Registros de Control

La Unidad de Tecnologías de Información a través del área de Operaciones y Redes y Soporte a Usuarios son responsables de construir los procedimientos de respaldo y restauración de la información.

Disposiciones de la norma

Contenidos que se respaldan

- Casillas de Correos electrónico
- Bases de Datos
- Archivos en áreas compartidas
- Computadores personales
- Servidores
- Aplicaciones

Tipo de respaldo o copias de Seguridad

- **Respaldo Completo (o Full),** considera la totalidad de la información contenida en un equipo o dispositivo computacional.
- **Respaldo diferencial,** se construye inicialmente con un respaldo completo de la información, incorporándose posteriormente solo los archivos modificados en forma completa o los archivos nuevos (diferencias).
- **Respaldo Incremental**, solamente se almacenan las modificaciones realizadas desde el último respaldo, esto obliga a mantener la información de contenidos del respaldo anterior, sobre la que se continua el respaldo de los "incrementos". Utilizan un mínimo espacio de almacenamiento a costa de una recuperación o restauración más compleja.

Periodicidad de las copias de seguridad

Se efectuará el respaldo de toda la información contenida en los servidores, más toda la información laboral contenida en los equipos computacionales asignados a los funcionarios, utilizando para ello respaldos de periodicidad Inmediata (en línea) Diaria, Semanal, Mensual, Anual o como se estime conveniente. La periodicidad de los respaldos se realizará bajo la siguiente forma:

- **Inmediato (en línea)**, son respaldos que se realizan en forma inmediata a la creación de los archivos en un equipo o dispositivo computacional.
- **Diarios,** están enfocados a todo equipo computacional que sufre modificaciones diariamente.
- **Semanales,** es la suma de los respaldos diarios acumulados en una semana o un respaldo que se realiza generalmente el último día de la semana
- **Mensuales,** es la suma de los respaldos semanales o diarios, acumulados en un mes, o un respaldo que se realiza generalmente el último día del mes.
- **Anuales,** es la suma de los respaldos mensuales, o un respaldo que se realiza generalmente último día del año.

Soporte físico

El Área Operaciones y Redes del Área de Informática definirá los soportes físicos más

[20] ISO 27002:2013 A.12.3.1 / A.18.1.3

adecuados para recibir las copias de respaldo, como por ejemplo unidades ópticas, discos ópticos, cintas y/o similares.

Rotación de Medios Físicos

Se conservarán los respaldos en medios magnéticos por un período determinado por el Encargado de Seguridad de la Información de acuerdo a recomendaciones del Área de Informática, luego se pondrán a disposición para ser reutilizados.

Copia histórica

Corresponde a la información que se almacena en forma indefinida o por un periodo definido por la autoridad, habitualmente en un lugar externo.

Generalidades

- Se considerará como práctica permanente, la migración de información histórica a medios que puedan ser recuperados por los nuevos equipos en funcionamiento, dado el continuo avance tecnológico que periódicamente deja obsoletos a los medios de respaldo.
- Las copias de respaldo deben conservarse considerando las pautas básicas específicamente definidas en la norma de Protección Física.
- Se llevará en forma permanente un inventario de los soportes de respaldo existentes, su contenido y el lugar donde están almacenados.
- Las copias de respaldo deberán almacenarse en una ubicación remota, junto con registros exactos y completos de su contenido y los procedimientos documentados de restablecimiento. Esta instalación deberá estar emplazada a una distancia tal que escape de cualquier daño producto de un desastre en el sitio principal.
- Los respaldos de sistemas y configuraciones deberán ser probadas con regularidad, a lo menos cada 18 meses, asegurando que tales respaldos satisfacen los requisitos estipulados en los planes de continuidad institucionales.
- Las áreas de Operaciones y Redes y de Mesa de Ayuda TIC serán las encargadas de mantener procedimientos actualizados para la administración de medios extraíbles y llevar en forma permanente un registro e inventario de los soportes de respaldo existentes, su contenido y el lugar donde están almacenados. La administración debe considerar los criterios de acceso para quienes deban operar en la reutilización, eliminación y transporte (servicio de courier) a otras instalaciones de forma segura[21].

Se respaldará la siguiente información, garantizando posteriormente la integridad de la restauración de información contenida en los medios físicos**:**

- Casillas de Correos electrónicos de todos los funcionarios.
- Bases de Datos de todas las aplicaciones y contenedores de información.
- Archivos en áreas compartidas.
- Carpeta LABORAL contenida en los computadores personales asignados a los funcionarios.
- Servidores para asegurar la continuidad operacional de la institución.

Obligaciones y Responsabilidades

- Es responsabilidad de cada funcionario mantener la información de carácter laboral en las carpetas definidas e informadas por el Área de Informática. No se podrá exigir restauración de información que no se encuentre en dichas carpetas.
- La solicitud de restauración de la información, debe ser canalizada a través del soporte del Área de Informática.
- Todo funcionario que solicite restauración de información de otro usuario o de alguna base de datos, deberá contar con la debida autorización de su supervisor directo.
- Será responsabilidad del Área Operaciones y Redes y del área de Mesa de Ayuda del Área de Informática velar por la disponibilidad, seguridad, y condiciones de almacenamiento adecuadas, garantizando la confiabilidad de la información contenida en los medios físicos.

Respaldo Institucional según contenido

La tabla que se presenta a continuación indica las exigencias básicas de periodicidad, tipos de respaldos a aplicar y su tiempo de retención, con la finalidad de mantener operativos correos electrónicos, Bases de Datos, Archivos en áreas compartidas, Computadores personales, Servidores y Aplicaciones (programas fuentes).

[21] ISO 27002:2013 A.8.3.1 / A.8.3.2 / A.8.3.3

Contenido	Periodicidad	Tipo de Respaldos	Retención
Correos electrónico	Respaldo Diario	Completo (o Full)	Indefinido
Bases de Datos	Respaldo Diario	Completo (o Full)	Indefinido
Archivos en áreas compartidas	Respaldo Diario	Completo (o Full)	Indefinido
Computadores personales	Respaldo Diario	Completo (o Full)	Indefinido
Servidores	Respaldo Diario	Completo (o Full)	Indefinido
Aplicaciones (programas fuentes)	Mensual	Completo (o Full)	Indefinido

Pruebas de Realización y Restauración de Copias de Respaldo

La Restauración corresponde a la recuperación de información desde los soportes físicos hacia un equipamiento de destino requerido, dejándola disponible para los usuarios.

La realización de las pruebas de restauración de las copias de respaldo confirmará el funcionamiento correcto del proceso de recuperación de copias de datos y garantizará la integridad de los datos que contienen. Por ello que se deberán realizar pruebas respecto a la restauración de las copias de respaldo, de forma rotativa y con una periodicidad de a lo menos cada un año.

Las pruebas y los resultados de restauración deberán ser registrados por el Área Operaciones y Redes y como consecuencia de las mismas, documentar las incidencias que se hayan puesto de manifiesto durante su desarrollo.

Comprobación periódica de los procedimientos de restauración

Para garantizar la eficacia de los procedimientos de restauración y la capacidad para recuperar activos desde las copias de respaldo, se establecerá el procedimiento de comprobación periódica que se detalla a continuación:

- Seleccionar al azar un activo de información (Servidor, Base de Datos Aplicativos, Estaciones de trabajo, Equipos comunicacionales y otros que se definan) almacenado en la copia de respaldo.
- Ejecutar una restauración del activo sobre una ubicación temporal, comprobando la restauración del activo y que se eliminará posteriormente.
- Almacenar el log de la herramienta de generación de copias con el resultado de la operación de restauración en el registro de operaciones de comprobación periódica.

Norma N° 4: Prevención de programa malicioso informático

Objetivo

Proteger a los activos de información institucional contra todo software malicioso que pueda dañar su consistencia, confiabilidad, disponibilidad e integridad[22].

Responsables del cumplimiento

Todo el personal de la institución y terceros que interactúan de manera habitual u ocasional, accediendo a información institucional y/o a los recursos informáticos en el desarrollo de sus tareas habituales.

Incumplimientos

Las medidas disciplinarias están descritas en el Anexo Sanciones por incumplimiento que forma parte del conjunto de medidas disciplinarias de la institución.

Definiciones

Se define como **Malware** (del inglés malicious software), también llamado badware, código maligno, software malicioso o malintencionado, a un tipo de software que tiene como objetivo infiltrarse y dañar los contenidos en una computadora sin el consentimiento de su propietario. El término malware incluye virus, gusanos, troyanos, la mayoría de los rootkits, spyware, adware intrusivo, crimeware y otros softwares maliciosos.

Disposiciones de la norma

Servicio

- El Área Operaciones y Redes del Área de Informática implementará un sistema automático de vigilancia y supervisión para la detección y el control antimalware, que permita prevenir y minimizar las consecuencias de su actividad cuando son ejecutados.
- El sistema de vigilancia y supervisión debe verificar la presencia de virus o malware en archivos de medios electrónicos de origen incierto o no autorizado, recibidos desde redes no confiables, archivos adjuntos en correo electrónico o descargado desde Internet.
- Los programas antimalware deben ser instalados por el Área de Informática, en los equipos centralizados de procesamiento, y en las estaciones de trabajo de los funcionarios y equipos móviles para que estén activados durante su uso.
- Se debe establecer en los contratos con el proveedor de esta tecnología su actualización periódica, así como también los servicios de reparación y de apoyo frente a alguna situación de ataque o infección reportada por el Área de Informática.
- El sistema de control, monitoreo y supervisión antimalware, debe permitir su actualización en forma periódica, automática y centralizada, en equipos centralizados de procesamiento y en las estaciones de trabajo y equipos móviles[23].
- Cuando el sistema automático de control no puede eliminar la aplicación malware, el Área Operaciones y Redes del Área de Informática debe escalar el problema al proveedor de la herramienta para resolver las situaciones particulares que se presenten.
- El Área de Soporte de la Unidad de Tecnologías de Información tiene la responsabilidad de recuperar los datos de los computadores personales que pudiera haberse dañado producto de la acción de algún programa malicioso. Para ello cuenta con un respaldo en línea de la información que los usuarios tienen la obligación de almacenar dentro del directorio "Laboral" que pueden organizar en subcarpetas en su interior. Los usuarios deben hacer uso del Sistema de Mesa de Ayuda para solicitar la atención que permita resolver cualquier inconveniente con sus datos.

Responsabilidades y recomendaciones

- Todos los funcionarios de la Superintendencia de Salud, son responsables de notificar al Área de Informática, utilizando el Soporte y procedimientos de Mesa de Ayuda, ante cualquier situación anómala que detecten (en el equipamiento, dispositivos externos o correo electrónico), con el fin de prevenir contagios o fallas en el equipamiento.
- Los funcionarios no deben abrir correos de remitentes desconocidos y tampoco intentar abrir archivos ejecutables que vengan anexos a correos.
- El Área Operaciones y Redes del Área de Informática deberá realizar escaneos de

[22] ISO 27002:2013 A.12.2.1
[23] ISO 27002:2013 A.12.2.1

malware en los PC por lo menos una vez por semana. Además, deberá realizar una verificación, de los PC de los usuarios, por lo menos una vez cada 6 meses,

- El Área Operaciones y Redes del Área de Informática deberá incorporar medidas complementarias de administración de mensajería, como la posibilidad de incorporar procedimientos de cuarentena utilizando el software entregado por el proveedor, de manera de aislar los virus y establecer la forma de su tratamiento posterior.

Norma N° 5: Ambientes de Procesamiento

Objetivo

Maximizar la efectividad de las operaciones y asegurar una adecuada separación de los distintos ambientes lógicos de procesamiento, permitiendo proteger la integridad, disponibilidad y confidencialidad de los activos digitales de información.

Definir las directrices y requisitos para establecer y controlar de procedimientos de operaciones, de paso a producción y mantenimiento de documentación actualizada y la gestión de seguridad de las operaciones tecnológicas.

Responsables del Cumplimiento

Todo el personal de la institución y personal externo autorizado, que interactúa de manera habitual u ocasional, que accedan a información y/o recursos informáticos en el desarrollo de aplicaciones y/o ejecución de sistemas.

Incumplimientos

Las medidas disciplinarias están descritas en el Anexo Sanciones por incumplimientos, que forma parte del conjunto de medidas disciplinarias de la institución.

Disposiciones de la norma

Implementar en distintas áreas el procesamiento para desarrollo de sistemas de información, prueba y producción, tal como se detalla en las siguientes secciones[24]:

Ambiente de Desarrollo de Sistemas

Ambiente en donde se realizan tareas de análisis y programación de aplicaciones en sus etapas de desarrollo, mantenimiento, y aprobación por el personal TIC, y en donde se encuentran:

- Herramientas para el desarrollo (diseñadores, utilitarios, compiladores y/o similares).
- Programas fuentes y objetos y parametrizaciones que están siendo modificados
- Información para desarrollo.
- Bases de datos para desarrollo.

A este ambiente solo podrán acceder:

- Personal del área de Desarrollo de Sistemas.
- Personal externo contratado para desarrollar sistemas para la Superintendencia
- Encargado de Seguridad institucional
- Responsable definido para el paso al ambiente de producción.
- Personal del Área Operaciones y Redes del Área de Informática para efectuar tareas de administración de servidores.

Cuando por necesidades del proceso de desarrollo se requiera copia de archivos de datos en ambiente de producción hacia el ambiente de desarrollo, el coordinador del área de desarrollo deberá solicitar la copia al coordinador del Área Operaciones y Redes, informando también al Encargado de Seguridad institucional. Una vez utilizados los datos, el coordinador del área de desarrollo deberá eliminarlos.

Seguridad de los sistemas de información en desarrollo

En la etapa de análisis del desarrollo de nuevas aplicaciones, el encargado del área de Desarrollo, en conjunto con el encargado del Área Operaciones y Redes, serán responsables de identificar cuáles de las funcionalidades del nuevo sistema (o aplicación), pudieran comprometer la seguridad de los datos existentes, definiendo medidas de seguridad estándares y adicionales si fuesen necesarias, tales como:

Medidas estándares:

- Sistema de control de acceso a los sistemas por parte de los funcionarios, que permita:
  - Identificar a los usuarios que tendrán privilegios de acceso a la aplicación
  - Segregación de funciones (roles, perfiles)
  - Asignación de permisos a través de grupos/perfiles modelos
- Todo sistema debe contar con la correspondiente ayuda en línea y manuales de uso, de operaciones y de mantenimiento.

Medidas adicionales:

[24] ISO 27002:2013 A.12.1.4

- Reportes y registros de auditoría automáticos sobre transacciones y actividad de los usuarios que han accedido a la aplicación
- Alertas en línea de accesos o intentos de accesos no autorizados a información de carácter sensible

Ambiente de Pruebas

Ambiente donde operan las versiones fuentes de sistemas de información, que están siendo probadas por el área de Desarrollo y personal de Control de Calidad (QA), para el posterior paso a producción, en este ambiente se encuentran:

- Programas fuentes, objetos y parametrizaciones que están siendo probados
- Información para pruebas
- Bases de datos para pruebas

A este ambiente solo podrán acceder:

- Usuarios responsables del área de Desarrollo, usuario líder del sistema en prueba y personal de QA
- Encargado de Seguridad institucional
- Responsable definido para el paso a Producción
- Personal del Área Operaciones y Redes para efectuar tareas de administración de servidores

El responsable definido para el paso a producción, debe asegurar la uniformidad de todas las versiones habilitadas en el ambiente de pruebas.

En caso que se requiera utilizar datos o bases de datos del área de producción para apoyar el proceso de prueba de aplicaciones, se deberá contemplar su eliminación al final del proceso mencionado.

Ambiente de Producción

Es el ambiente donde operan los sistemas de información (ejecutables) y los datos reales, para ser utilizados por los funcionarios(as) de la institución y usuarios externos. Aquí se encuentran:

- Programas o aplicaciones ejecutables, objetos y parametrizaciones de ejecución
- Información real de producción
- Bases de datos de producción

A este ambiente solo podrán acceder:

- Funcionarios de la institución y usuarios externos autorizados
- Encargado de Seguridad de la Información institucional
- Personal del Área Operaciones y Redes para efectuar tareas de administración de servidores, que incluyen la configuración, instalación, mantención y monitoreo de servidores y sus contenidos[25].

El Área Operaciones y Redes será la encargada de controlar los cambios en el entorno operacional y de las instalaciones de procesamiento, mediante la asignación de responsabilidades y procedimientos formales para garantizar el control satisfactorio de los cambios, y evaluar el posible impacto al entorno operacional[26].

También deberá mantener un procedimiento de monitoreo y ajuste de la capacidad del entorno operacional para garantizar el rendimiento que los sistemas requieren[27].

Periódicamente el Área Operaciones y Redes deberá realizar una evaluación de las vulnerabilidades técnicas existentes en las plataformas operativas, identificándolas y estableciendo procesos de administración eficaz de los riesgos asociados[28]. Además, si fuera necesario deberá solicitar al área de Desarrollo la aplicación de medidas que permitan eliminar brechas de seguridad que pudieran surgir en el transcurso de la operación de los sistemas de información.

Accesos de emergencia al ambiente de Producción

Ante situaciones de emergencia operativa, cuando el personal del área de Desarrollo requiera programas y datos reales en producción para soporte de

[25] ISO 27002:2013 A.12.5.1
[26] ISO 27002:2013 A.12.1.2
[27] ISO 27002:2013 A.12.1.3
[28] ISO 27002:2013 A.12.6.1

emergencia, deberá solicitarlos al Encargado del Área Operaciones y Redes e informar al Encargado de Seguridad. Una vez concluida la situación de emergencia, se deberá contemplar la eliminación de los datos reales utilizados.

Inventario de sistemas de información desarrollados

- El área de Desarrollo es responsable de llevar un registro de todas las aplicaciones desarrolladas y sus versiones, y el Área Operaciones y Redes será la encargada de mantener el control de las versiones ejecutables que operen en el ambiente de producción.

Este inventario deberá mantenerse actualizado y deberá ser reportado por el encargado del área de Desarrollo a la jefatura del Área de Informática al menos una vez al año.

Protección en redes e instalaciones

El Área Operaciones y Redes, será la encargada de la protección de la información en las redes y sus instalaciones, en particular:

- Implementación de la seguridad de las comunicaciones, garantizando la protección de la información en las redes e instalaciones de procesamiento.
- Establecer responsabilidades y procedimientos para la administración y monitoreo del equipamiento sobre sus correspondientes redes, controles para resguardar la confidencialidad e integridad de datos que pasan por redes públicas o inalámbricas y la aplicación de autenticación de los sistemas conectados a las redes[29].
- Establecer y monitorear la capacidad de los proveedores de servicios de red para administrar los servicios de manera segura[30].
- Establecer una segregación de redes que permita una adecuada administración de la seguridad de las plataformas operativas y de los distintos ambientes de procesamiento[31].
- Manejo del personal informático asignado de acuerdo a la disposición que la Institución determine.
  - ✓ Denunciar toda irregularidad que el funcionario(a) observe o tome conocimiento respecto al resguardo y seguridad de la información.
  - ✓ Las referencias anteriores deben ser de cumplimiento permanente en cualquier cargo y/o puesto de trabajo que el funcionario esté sirviendo en la institución.
  - ✓ Ante una situación de cese de funciones, la institución seguirá el procedimiento correspondiente para la recepción de todos los activos asignados y/o de responsabilidad del funcionario que se desvincula[32].

[29] ISO 27002:2013 A.13.1.1
[30] ISO 27002:2013 A.13.1.2
[31] ISO 27002:2013 A.13.1.3
[32] ISO 27002:2013 A.7.1.2

Norma N° 6: Gestión de la Continuidad Operacional

Objetivo

Contribuir en el aseguramiento de la continuidad de operación de los procesos, ante eventos que interrumpan el normal desarrollo de sus funciones, a través de una metodología de manejo de información, sistemas y servicios tecnológicos que permitan recuperar el normal procesamiento de los recursos críticos.

Por otra parte, y dado el avance tecnológico que permite el resguardo y manipulación de información en la nube (pública o privada), el objetivo también comprende acciones de protección de datos presentes en el ciberespacio y la infraestructura que se utiliza de soporte, para evitar efectos adversos, minimizar riesgos y amenazas propias de la continuidad del negocio.

Responsables del cumplimiento

Todo el personal de la institución y personal externo autorizado, que interactúa de manera habitual u ocasional, que accedan a información y/o recursos informáticos en el desarrollo de aplicaciones y/o ejecución de sistemas.

Incumplimientos

Las medidas disciplinarias están descritas en el Anexo Sanciones por incumplimientos que forma parte del conjunto de medidas disciplinarias de la institución.

Conceptos preliminares

Plan de Continuidad Operacional

Es el conjunto de actividades a ejecutar ante distintos escenarios de desastres que pudieran afectar la operación de funciones críticas institucionales.

Plan de Continuidad del Procesamiento

También conocido como Plan de Contingencia Tecnológica. Es el subconjunto de actividades del Plan de Continuidad Operacional, orientadas a:

- Definir riesgos ante eventos de interrupción no prevista del procesamiento de la información.
- Definir planes de recuperación de la capacidad de proceso, incluyendo tareas para:
  - Minimizar y/o eliminar impactos de la interrupción.
  - Focalizando las actividades en recuperar las funciones y sistemas críticos del negocio.
- El Área de Informática es la encargada de desarrollar y mantener el Plan de Contingencia Tecnológica, de modo de contribuir con el Plan de Continuidad Operacional, minimizando con ello el impacto en la detención de las funciones críticas institucionales, para ello y en particular en los conceptos y contenidos del Plan, puede ser apoyada por el Área de Informática u otros profesionales de otras áreas que convengan al propósito del Plan.
- En el ámbito de la Ciberseguridad, el Área de Informática debe gestionar la seguridad de sus activos de información expuestos a riesgos en el ciberespacio, entendido este como el entorno que permite la interacción lógica, es decir no física, mediante la conexión de redes tecnológicas.

Disposiciones de la norma

En prevención de eventos que interrumpan los servicios, es norma institucional

Servicios y continuidad de procesamiento institucional

- El Área Operaciones y Redes debe garantizar la continuidad de soporte de todas las funciones institucionales en un esquema de servicio que asegure una disponibilidad de 99% (up-time o tiempo de actividad sin interrupciones).
- Las funcionalidades críticas deberán estar activas en un esquema de servicio 24/7, es decir, las 24 horas, todos los días del año y deberán estar disponibles en instalaciones con altos estándares de seguridad y niveles de servicios que aseguren la continuidad de procesamiento de a lo menos un 99,9%[33].
- Los respaldos de información, junto con registros exactos y completos de las copias de respaldo de sistemas y los procedimientos documentados de restablecimiento, deberán almacenarse y recuperarse desde una ubicación remota, la cual deberá estar emplazada a una distancia tal que escape de cualquier daño producto de un desastre en el sitio principal.

[33] ISO 27002:2013 A.17.2.1

- El Área Operaciones y Redes debe cooperar en el desarrollo de un plan de continuidad operacional que indique la forma de poner en práctica acciones de recuperación ante eventos de interrupción de servicios, plan que debe ser liderado en su generación y posteriormente aprobado por el Comité de Seguridad[34].
- El Plan de Continuidad debe ser revisado y/o actualizado cada dos años como mínimo o frente a un cambio significativo de las condiciones tecnológicas y legales que lo sustentan.

Prevención para una continuidad operacional efectiva

Como actividad de prevención y para garantizar un enfoque coherente y eficaz en la administración de incidentes incluyendo aquellos de seguridad de la información, el Área Operaciones y Redes, es la encargada de desarrollar, mantener y actualizar un procedimiento que permita el registro, análisis y gestión de incidentes (Mesa de Ayuda), posibilitando:

- Establecer responsabilidades y directrices orientadas a garantizar una rápida, eficaz y ordenada resolución de incidentes[35].
- Establecer canales de recepción de información de incidentes que permitan la priorización y asignación de recursos para resolverlos[36].
- Permitir el análisis y evaluación de vulnerabilidades de las plataformas operativas y/o manejo de información involucrada[37].
- Posibilitar la evaluación de los incidentes, su clasificación y generación de respuesta con fines de referencia futura[38].
- Mantener procedimientos documentados para el tratamiento y respuesta ante incidentes, especialmente de aquellos clasificados como seguridad de la información[39].
- Permitir la utilización del conocimiento, análisis y resolución de incidentes para reducir la probabilidad o impacto de incidentes futuros[40].
- Permitir y aplicar procedimientos orientados a la identificación, recopilación, adquisición y preservación de información que pueda servir de evidencia[41].

El Área Operaciones y Redes, deberá desarrollar y mantener actualizado, un procedimiento para la mantención y revisión periódica de los registros de eventos de usuario, excepciones, fallos y eventos de seguridad de la información. También se deben establecer controles de protección de tales registros, contra la adulteración y acceso no autorizado. Por último, se deberá agregar protección y revisión periódica de los registros de actividades de administradores y operadores de sistemas, dados sus privilegios para la manipulación de registros en las plataformas operativas bajo su control[42].

Plan de Continuidad[43]

El Área de Informática debe evaluar posibles escenarios de eventos de interrupción del servicio y su impacto en el negocio, además considerar el desarrollo e implementación de una estrategia de recuperación de los procesos críticos, asegurando una documentación suficiente para resolver toda la gama de situaciones evaluadas con las correspondientes pruebas de validación.

Deberá considerar una etapa de evaluación previa, que consigne, además de los posibles escenarios de interrupción, sus riesgos y la ponderación de su posible ocurrencia, fijando un alcance específico a los eventos de mayor probabilidad e impacto, sus condiciones de activación y la responsabilidad de los equipos humanos en la ejecución de los componentes del plan.

Deberá contener la definición de los procedimientos de emergencia y a los encargados de ejecutarlos, además de considerar los aspectos comunicacionales al momento de activar el plan, comunicación que debe abarcar como mínimo, la efectiva gestión de las relaciones públicas, una eficiente coordinación con autoridades

[34] ISO 27002:2013 A.17.1.1
[35] ISO 27002:2013 A.16.1.1
[36] ISO 27002:2013 A.16.1.2
[37] ISO 27002:2013 A.16.1.3
[38] ISO 27002:2013 A.16.1.4
[39] ISO 27002:2013 A.16.1.5
[40] ISO 27002:2013 A.16.1.6
[41] ISO 27002:2013 A.16.1.7
[42] ISO 27002:2013 A.12.4.1 / A.12.4.2 / A.12.4.3
[43] ISO 27002:2013 A.17.1.2

externas (como policía, bomberos, autoridades directivas, etc.), y mecanismos eficaces para convocar a los responsables de los procesos de negocio y sistemas informáticos afectados. A lo anterior, se deberá agregar una evaluación de los posibles perjuicios y los costos asociados.

Por otra parte, y considerando la evolución tecnológica hacia el almacenamiento y transacciones de información en la nube (pública o privada), debe habilitar funciones dedicadas a la *Ciberseguridad* que resguarden su confidencialidad, integridad y disponibilidad.

Además, deberá establecer una estrategia de recuperación de procesos, en función de lo siguiente:

- Trabajar y capacitar a los usuarios claves de las distintas áreas institucionales, evaluando el impacto de los eventos de interrupciones de servicio, definiendo posibles alternativas de recuperación de procesos y funciones críticas, determinando costos y el tiempo máximo de espera de reinicio de procesos antes de que el negocio sea impactado.
- Declarar los eventos de interrupción (comunicación institucional) y las tareas necesarias para volver a la situación normal.
- Documentar las actividades a implementar y asegurar mediante procesos de prueba periódicos y establecidos formalmente, el correcto funcionamiento del plan.

Norma N° 7: Licencias Legales de Software

Objetivo

Asegurar que todo software, instalado en los servidores institucionales y en el equipamiento entregado y utilizado por el personal de la Superintendencia de Salud, tenga licencias de uso legales[44].

Responsables del cumplimiento

Todo el personal de la Superintendencia de Salud y terceros que interactúen en labores de desarrollo de software de manera habitual u ocasional, y que accedan a los recursos informáticos en el desarrollo de sus tareas habituales.

Incumplimientos

Las medidas disciplinarias por el incumplimiento a estas normas, están descritas en el Anexo Sanciones por Incumplimiento, que forma parte del conjunto de medidas disciplinarias de la Superintendencia de Salud.

Disposiciones de la norma

Adquisición de software

Todo software que se utiliza en los equipos informáticos, es adquirido a nombre de la Superintendencia de Salud y cuenta con una licencia legal para su utilización, excepto aquellos que son de uso libre.

La adquisición de software se realizará previo estudio de las necesidades institucionales, impacto, compatibilidad con la tecnología existente, niveles de uso, integración a los sistemas existentes y toda información que permita una compra adecuada. Las bases técnicas o argumentos de compra de tecnología informática deberán quedar documentados en informe visado por la jefatura del Área de Informática.

Software recibido para su prueba

Cuando se reciba software de terceros en forma de préstamo para su prueba y evaluación, se debe generar un documento formal que así lo indique, conformando una constancia legal que considere todos los detalles relevantes. También debe quedar formalmente establecido quienes implementarán, evaluarán y aprobarán tales aplicaciones.

Instalación de software

El área operaciones y redes, es responsable de la homologación inicial, instalación y/o eliminación, de cualquier tipo de software en todo el equipamiento tecnológico institucional.

El perfil de usuarios es restringido, el cual no permite instalar ningún tipo de software en los equipos informáticos de la institución, bajo ningún concepto, sin la autorización del Área de Informática, aun cuando el software sea de uso libre o haya sido adquirido a favor del funcionario(a)[45].

Desarrollo interno de software

Todo software desarrollado para su utilización por parte de los funcionarios(as), es propiedad de la Superintendencia de Salud y sus modos de operación, diseño, estructura de datos a manejar y administración, estarán descritos en la respectiva documentación que tendrá a su cargo y disponibilidad, el área de Desarrollo de Sistemas de Información, que forma parte del Área de Informática.

Transferencia a Terceros

- Toda transferencia a terceros, de software desarrollado internamente, debe estar autorizada por el Comité de Seguridad y debe contar con el correspondiente respaldo legal.
- No se permitirá la transferencia de software adquirido a nombre de la Superintendencia, cuyas licencias no estén amparadas en el contrato respectivo.
- En las donaciones de equipos informáticos, éstos no llevarán cargados ni les serán instalados ningún recurso de software.

[44] ISO 27002:2013 A.18.1.2
[45] ISO 27002:2013 A.12.6.2

Contratos con terceros

El Área de Informática es el área encargada de generar las bases técnicas para el desarrollo de software específico en contratos de adquisición a terceros, debiendo contemplar los resguardos suficientes para que ante cualquier situación que impida al proveedor seguir prestando sus servicios, asegure a la Superintendencia de Salud, la obtención de los programas fuentes, manuales y toda la documentación asociada, permitiendo dar continuidad al proceso de desarrollo.

Este tipo de desarrollos será supervisado por el área de Desarrollo TI, desde su inicio, hasta la disposición final, considerando todas las formalizaciones necesarias para establecer la propiedad por parte de la Superintendencia de Salud.

Control de Licencias

Debe existir un inventario actualizado permanente de las licencias de software adquiridas e instaladas en todos los equipos informáticos de la institución, implementando controles para asegurar que el número máximo de licencias en uso no exceda lo definido.

El área de Desarrollo de Sistemas de Información del Área de Informática, deberá mantener un inventario actualizado de todos los sistemas desarrollados, reportando un informe periódico y actualizado a la Jefatura del Subdepartamento. Debe cumplir con las siguientes directrices:

- Disponer (programas, hardware, software), como también aquellos de su entorno (impresoras, escáner, CD, DVDs, pendrives, etc.)[46].
- Resguardar y proteger la información que por las condiciones y atribuciones de su cargo tiene acceso, correspondiente al manejo de datos, sistemas y procesos informáticos.
- Resguardar las claves de acceso atendiendo su carácter de personal e intransferible debiendo actuando conforme a las instrucciones emanadas de la Política de Seguridad de la Información
- Administrar los equipos informáticos asignados de acuerdo a la disposición que la Institución determine.
- Denunciar toda irregularidad que el funcionario(a) observe o tome conocimiento respecto al resguardo y seguridad de la información.

Las referencias anteriores deben ser de cumplimiento permanente en cualquier cargo y/o puesto de trabajo que el funcionario este sirviendo en la institución.

Ante una situación de cese o inminente término de funciones, la institución seguirá el procedimiento correspondiente para la recepción de todos los activos asignados y/o de responsabilidad del funcionario que se desvincula[47].

[46] ISO 27002:2013 A.7.1.2
[47] ISO 27002:2013 A.7.1.2

Norma N° 8: Uso de Recursos Tecnológicos

Objetivo

Garantizar la adecuada utilización de los recursos tecnológicos provistos por la institución, por parte de los funcionarios de la Superintendencia de Salud.

Responsables del cumplimiento

Todos los funcionarios de la Superintendencia de Salud y terceros que, interactuando en forma permanente u ocasional, hagan uso de cualquier recurso tecnológico institucional asignado por esta Superintendencia.

Incumplimientos

Las medidas disciplinarias están descriptas en el Anexo Sanciones por Incumplimiento que forma parte del conjunto de medidas disciplinarias de la institución.

Disposiciones de la norma

Para los efectos de esta normativa, se entenderá como recurso tecnológico a:

- Computadores de escritorio
- Impresoras de escritorio
- Impresoras de red
- Scanner
- Servidores computacionales
- Teléfonos IP
- Proyectores Multimedia
- Equipamiento tecnológico de Sala Auditórium
- Notebooks y Netbooks
- Software Base
- Sistemas de información
- Equipos móviles de comunicación (Smartphone)

Respecto de medios removibles, al final de esta norma se especifica la seguridad que se debe aplicar en su manejo.

Administración de los recursos

- Los funcionarios del Área Operaciones y Redes, serán responsables de los procedimientos para el uso correcto de los recursos tecnológicos de esta Superintendencia.
- El Área Operaciones y Redes deberá mantener procedimientos en donde se adopten políticas y medidas de seguridad y apoyo para administrar los riesgos asociados al uso de equipamiento móvil. También se deberá tener procedimientos que definan las condiciones y restricciones para el desarrollo de teletrabajo[48].
- El personal de Soporte (Mesa de Ayuda) será responsable de efectuar, los procesos de habilitación y mantención de los equipos tecnológicos, en los puestos de trabajo de los funcionarios de la Superintendencia.
- En caso de fallas en los equipos tecnológicos, en particular de aquellas que no tengan una solución con recursos internos, el área de Soporte del Área de Informática será la única responsable de solicitar soporte externo, considerando las indicaciones habidas en el contrato que se suscriba con la empresa externa. Respecto del área de servidores y/o de equipamiento tecnológico crítico, el Área Operaciones y Redes será la encargada de los procesos de mantención, para garantizar su continuidad, disponibilidad e integridad, considerando:
    - Que el equipamiento sea mantenido de acuerdo a la periodicidad y especificaciones de servicio recomendados por el proveedor y/o fabricante.
    - Solo el personal de mantenimiento autorizado deberá realizar las operaciones de reparación y/o servicio a los equipos.
- Para conformar los puestos de trabajo institucionales, a cada funcionario(a) se le asignará un equipo computacional incluyendo el software necesario para la realización de sus tareas, y los accesos a las redes, servicios de red e información clasificada. El uso de estos recursos será de exclusiva responsabilidad de cada funcionario(a)[49].
- El área de Soporte (Mesa de Ayuda) es la encargada de mantener procedimientos

[48] ISO 27002:2013 A.6.2.1 / A.6.2.2
[49] ISO 27002:2013 A.9.3.1

actualizados, tanto para la entrega de equipamiento tecnológico a cargo y de responsabilidad de los funcionarios, como también para la devolución de ese equipamiento cuando un funcionario se desvincula de la institución. La entrega y devolución de equipamiento de funcionarios y/o con proveedores tecnológicos serán registradas y los inventarios mantenidos y actualizados periódicamente[50]. La entrega de equipamiento en devolución y/o mantención a los proveedores tecnológicos se hará siguiendo procedimientos de seguridad respecto de los contenidos almacenados, los que se deberán controlar y eliminar[51].

- El Área Operaciones y Redes deberá desarrollar, documentar y mantener actualizados sus procedimientos operativos para garantizar las operaciones correctas y seguras en las instalaciones de procesamiento. En lo específico, estos procedimientos deben considerar la instalación y configuración de sistemas[52], mantención de equipamiento y software, manipulación de información, instrucciones para el manejo de errores, contactos de apoyo, escalamiento en actividades de soporte, procedimientos de recuperación y monitoreo[53-54].
- Periódicamente el Área Operaciones y Redes deberá realizar una evaluación de las vulnerabilidades técnicas existentes en las plataformas operativas, identificándolas y estableciendo procesos de administración eficaz de los riesgos asociados.
- El Área Operaciones y Redes deberá mantener actualizado un procedimiento para sincronizar los relojes de todos los sistemas de procesamiento con una fuente de tiempo de referencia única. Se deberá documentar e implementar el enfoque institucional para obtener una hora de referencia y su manera de sincronización de los relojes internos de manera confiable[55].
- El área de Soporte, deberá desarrollar y mantener actualizado un procedimiento para aplicar seguridad a los equipos y/o medios que eventualmente deban operar fuera de las dependencias de la institución. El procedimiento debe considerar al menos las siguientes pautas:
    - Los equipos y medios que se saquen fuera de las dependencias deben estar supervisados en forma permanente en lugares públicos;
    - Se deberán evaluar los riesgos de operar en distintas ubicaciones (hogar, teletrabajo, sitios temporales) y aplicar controles según corresponda;
    - Se deberá mantener un registro de la entrega y devolución del equipamiento y/o medio que se autoriza en salida[56].
- Respecto del Área Operaciones y Redes debe mantener actualizados los procedimientos que permitan mantener activos los servicios básicos de apoyo (es decir: la electricidad, las telecomunicaciones, suministro de agua, climatización), permitiendo que:
    - Cumpla especificaciones técnicas asociadas a los fabricantes y/o requisitos legales y/o técnicos asociados
    - Se someta a evaluaciones periódicas de desempeño y asegure el crecimiento planificado de los servicios que presta
    - Se someta a inspecciones y pruebas periódicas para garantizar su correcto funcionamiento
    - Contar con alarmas para detección de fallas, y en el caso de la electricidad, contar con servicios de respaldo eléctrico o de alimentación desde distintos enrutamientos físicos[57].

El equipamiento computacional de usuarios perteneciente a la Superintendencia, estará bajo la exclusiva administración del área de Soporte, y por tanto queda prohibido al usuario:

- Manipulación no autorizada
- Ingerir alimentos y/o bebidas en el módulo o mueble en el que se encuentre instalado el equipo y/o dispositivos, así como colocar o manipular líquidos en su cercanía.
- Hacer uso irracional y desconsiderado del espacio disponible en el disco duro de los equipos, acumulando material no relacionado con el aspecto laboral, como

[50] ISO 27002:2013 A.11.2.5
[51] ISO 27002:2013 A.11.2.7
[52] ISO 27002:2013 A.12.5.1
[53] ISO 27002:2013 A.12.1.1
[54] ISO 27002:2013 A.11.2.5
[55] ISO 27002:2013 A.12.4.4
[56] ISO 27002:2013 A.11.2.6
[57] ISO 27002:2013 A.11.2.2 / A.11.2.4

software sin licencia o no autorizado, archivos con música, videos, fotos y otros similares, provenientes de internet u otros medios que no estén relacionado con sus funciones.

- Abrir equipos, reemplazar y/o desconectar componentes.
- Reasignaciones permanentes o temporales sin autorización.
- Instalación de programas, sistemas, módulos y/o archivos externos.
- Empleo de juegos y/o programas con fines no laborales.
- Modificación de la configuración de sistemas, programas o dispositivos.
- Desinstalar sistemas, programas, módulos habilitados por el Área Operaciones y Redes.
- Conexión a redes de datos o eléctricas no certificadas y/o autorizadas, las que serán expresamente indicadas por el área de Soporte.
- Trasladar equipamiento computacional dentro de la institución sin la debida autorización.
- Sacar equipamiento computacional fuera de la institución sin autorización del área de Soporte.
- Instalar equipamiento propio con conexión a redes institucionales sin autorización del área de Soporte[58].

Inventario de los Equipos Tecnológicos

El Área de Informática será la encargada de mantener en forma permanente un inventario del equipamiento tecnológico y software habilitados en la Superintendencia de Salud, su contenido y el lugar donde están instalados[59].

Situaciones de emergencia

- Ante incidentes de cualquier tipo que afecten al equipamiento computacional asignado a los usuarios o al equipamiento de red que esté utilizando, el usuario debe informar de inmediato al área de Soporte (Mesa de Ayuda).
- El área de Soporte es responsable de las acciones a ejecutar cuando ocurran incidentes que puedan afectar el normal funcionamiento de los equipos tecnológicos en cualquier locación de la Superintendencia de Salud.

Privacidad y Seguridad[60]

- Los funcionarios de la Superintendencia deben utilizar las tecnologías dispuestas para el desarrollo de sus labores habituales, de manera responsable y segura, bajo la supervisión y apoyo del Área de Informática y el Área Operaciones y Redes.
- Las estaciones de trabajo y equipamiento portátil, cuando corresponda, deben tener aplicado el estándar relativo a protector de pantalla definido por el Área Operaciones y Redes, de manera que se active ante un tiempo definido sin uso (equipo desatendido).
- La pantalla de autenticación en la red institucional, debe requerir solamente la identificación de la cuenta y una clave, y no entregar ni solicitar otra información.
- La autenticación de los usuarios, debe ser requerida toda vez que el equipamiento se encienda, reinicie, bloquee o después de aparecer el protector de pantalla si existe.
- Los funcionarios no deben intercambiar con otros usuarios sus nombres de acceso, contraseñas y/o información de acceso a las aplicaciones que pueda utilizar.
- Los funcionarios, cuando se ausenten de sus escritorios, deben bloquear su equipamiento de trabajo y desconectarse de sistemas y de Internet, además de programas o aplicaciones en ejecución, protegiéndose de un acceso no autorizado o acceso a la integridad de sus diversas credenciales de seguridad[61].
- Los funcionarios deben localizar su equipamiento en ubicaciones que no queden expuestas al acceso de terceros no autorizados.
- Los equipos que queden cerca de zonas de atención de público o tránsito de público, deben situarse de modo que los contenidos en las pantallas no puedan ser visualizadas por personas no autorizadas.
- Cuando sea aplicable en los lugares donde se un equipo que almacene información sensible, se deben implementar condiciones mínimas para un

[58] ISO 27002:2013 A.8.1.2 c
[59] ISO 27002:2013 A.8.1.1
[60] ISO 27002:2013 A.8.1.3
[61] ISO 27002:2013 A.11.2.8 / A.11.2.9

funcionamiento estable en condiciones de temperatura y humedad adecuadas.

Equipamiento desatendido por funcionarios, escritorio y pantalla limpios

- Toda vez que los funcionarios(as) se ausenten de su lugar de trabajo, deben bloquear su equipamiento y guardar en lugar seguro todo documento o dispositivo tecnológico que contenga información institucional.
- Al finalizar su jornada de trabajo, los funcionarios (as) deben guardar en lugar seguro toda la documentación de trabajo y dispositivos tecnológicos que contengan información, además de desconectarse de todas las aplicaciones y finalizar todas las sesiones de trabajo que los mantenga conectados a la red institucional.
- Los equipos de reproducción de información como impresoras, escáneres, fotocopiadoras, deben estar ubicados en zonas con acceso controlado y toda la documentación de trabajo, pública, reservada y/o sensible, debe ser retirada inmediatamente del equipamiento luego de su uso.

Seguridad de equipamiento fuera de las instalaciones de la institución

- La asignación de equipamiento para uso exterior, debe ser realizada y autorizada por la jefatura directa, la asignación debe quedar documentada, indicando usuario asignado, equipo y tiempo de uso del equipo.
- Periódicamente el área de Soporte debe revisar el inventario de equipamiento destinado para su uso fuera de institución.
- Cuando un equipamiento sea definido como crítico, se debe registrar su salida y su retorno.
- El equipamiento que es retirado de la institución, no debe ser desatendido en áreas de acceso público.
- Cuando el funcionario(a) viaje con un computador portátil, éste debe ser transportado como equipamiento de mano y de forma disimulada.
- Se deben observar siempre las instrucciones del fabricante para proteger los equipos, por ejemplo, contra la exposición a campos electromagnéticos intensos.
- Para cualquier trabajo fuera de las dependencias de la institución, se deben seguir las directrices de las normas de pantalla y escritorio limpios.
- Cuando los equipos de responsabilidad de un usuario(a) sufran deterioro o daño por mal uso o uso irresponsable, el funcionario(a), será sometido a las medidas administrativas estipuladas en el estatuto administrativo.

Seguridad de la Información en la gestión de medios removibles

- Los medios de almacenamiento removibles como CD, DVD, pendrive, discos duros externos, etc., no son alternativa de respaldo de información en la Superintendencia, siendo responsabilidad de los usuarios mantener la información en los servidores destinados para ello.
- Los medios de almacenamiento removibles indicados solo se pueden utilizar en transporte de información y deben ser escaneados mediante antivirus cada vez que sean conectados a equipamiento de la red de la institución.
- La información transportada en estos medios debe ser encriptada. Cuando la información pierda vigencia, el medio se debe destruir o formatear siguiendo un protocolo de tratamiento seguro.
- Es responsabilidad del área de Soporte, definir el estándar y protocolos de manejo a utilizar en los distintos medios removibles.
- La utilización de un medio removible requiere previamente de una revisión del estándar asignado a ese medio, tarea de responsabilidad del área de Soporte que también debe hacer la revisión inicial del medio.
- Es de responsabilidad exclusiva del funcionario(a), tomar las medidas adecuadas para el almacenamiento y resguardo de los medios removibles para evitar accesos no autorizados, daños o pérdida de información. Si ocurre alguno de estos eventos, el funcionario(a), debe informar de inmediato al área de Soporte, siguiendo el protocolo de gestión de incidentes (Mesa de Ayuda).
- Cuando la información pierda vigencia, el medio removible debe ser formateado, y si esto no es posible, debe ser destruido.
- El deshecho, borrado, limpieza o destrucción de medios removibles, debe ser realizado de acuerdo al procedimiento para la eliminación segura o reutilización de equipos y dispositivos.

Eliminación de medios removibles de almacenamiento

Se deben eliminar los medios de forma segura y sin peligro cuando no se necesiten. Para esto es necesario establecer procedimientos formales de eliminación segura de los medios, a fin de minimizar el riesgo de filtración de información confidencial a personas no autorizadas. Se deberían considerar los siguientes aspectos:

(a) Los medios que contienen información confidencial se deberían almacenar y eliminar de manera segura, es decir, mediante la incineración, o la destrucción o bien a través del borrado de datos para el uso por parte de otra aplicación dentro de la organización;
(b) Deberían existir procedimientos en vigencia para identificar los artículos que pueden requerir de una eliminación segura especial;
(c) Es posible que sea más fácil realizar las disposiciones necesarias para que se recopilen todos los artículos de medios y que se eliminen de manera segura en vez de intentar separar los artículos o dispositivos sensibles;
(d) La eliminación de los artículos o dispositivos sensibles se debería registrar para mantener un seguimiento de auditoría.

Los medios de almacenamiento removibles son entregados por la institución, quedando establecido que no está autorizado el uso de elementos removibles personales o externos no autorizados; específicamente corresponden a:

- Pendrive
- Discos duros portátiles
- Teléfono móvil
- Tablets
- Cámara fotográfica
- Grabadora de audio
- Cámara de video

Es responsabilidad del Área de Informática el desarrollo de protocolos de eliminación de medios, manteniendo los resguardos necesarios para conservar la información antes de proceder al borrado de datos. Estos protocolos deben ser validados por el Oficial de Seguridad.

Norma N° 9: Seguridad Física y Ambiental

Objetivo

Asegura una adecuada seguridad física de los equipos y soportes de procesamiento, transmisión y conservación de la información institucional, contenida en el Área Operaciones y Redes y en las distintas unidades institucionales.

Define directrices para los perímetros de seguridad, controles de ingreso y protección física de las áreas que contienen información.

Responsables del cumplimiento

Todo el personal de la Superintendencia de Salud que tenga acceso autorizado a las dependencias donde se encuentre: equipamiento de puestos de trabajo, de procesamiento centralizado, de comunicación y/o de almacenamiento, y/o información archivada en distintos tipos de soporte que sea de propiedad de la Superintendencia de Salud.

Incumplimientos

Las medidas disciplinarias están descritas en el Anexo Sanciones por incumplimientos que forma parte del conjunto de medidas disciplinarias de la institución.

Disposiciones de la norma

Aspectos Generales de Seguridad Física

- El acceso físico a las dependencias de la institución será restringido solo a personal autorizado mediante la implementación de mecanismos de autenticación como tarjeta magnética u otro similar.
- Existirá un área de recepción atendida por personal de la Superintendencia y los accesos físicos al área o edificio será restringidos solo a personal autorizado.
- El acceso físico a áreas de acceso restringido será controlado mediante registro y autorización de los encargados del área y será limitado a personal autorizado.
- Corresponderá a los niveles de jefatura o directivos que tengan dependencias a cargo, la definición de áreas críticas que ameriten control de acceso, en particular de las áreas donde se encuentren activos definidos como críticos.
- Cualquier área que sea definida como crítica, deberá ser protegida bajo las directrices definidas en esta norma.
- El ingreso de usuarios que no realicen tareas operativas habituales tales como terceros externos, se registrará en forma específica en una nómina, la que será revisada en forma periódica[62].
- Se priorizará el monitoreo mediante el uso de cámaras de video.
- El trabajo en áreas seguras y/o de acceso restringido será registrado y supervisado por personal del área.
- Las áreas de entrega y carga estarán[63] controladas por las áreas de Logística y Servicios Generales y estas últimas coordinadas con la Administración de Edificios Santiago DownTown cuando corresponda y no deben estar en comunicación física con las instalaciones de procesamiento de información. Los materiales u objetos ingresados por estas áreas deberán ser inspeccionados antes de su ingreso a su lugar de utilización.
- Cada vez que se definida un área de trabajo como crítica, el responsable de la dependencia debe informar al Encargado de Seguridad de la Información.

Aspectos Generales de Seguridad Ambiental[64]

- Se instalarán sistemas automáticos de detección y respuesta automática ante condiciones ambientales que puedan afectar el procesamiento de los equipos y/o información contenida en cualquier soporte.
- Cuando no se pueda disponer de un sistema de extinción automática de incendios, se contará con extinguidores habilitados de uso específico.

Seguridad Física y Ambiental asociados al Área Operaciones y Redes

Servicios del Área Operaciones y Redes

Se garantizará la continuidad operativa en un 99% en horario hábil de los servicios del Área Operaciones y Redes considerando los siguientes elementos de seguridad:

Perímetro de seguridad

[62] 27002:2013 A.11.1.2 / A.11.1.3 / A.11.1.5
[63] ISO 27002:2013 A.11.1.6
[64] ISO 27002:2013 A.11.1.4

El perímetro de seguridad estará claramente definido y la resistencia de tal perímetro dependerá de los requisitos de seguridad de los activos dentro del perímetro.
El perímetro deberá tener solidez física en sus muros y todas las puertas exteriores deberán contar con mecanismos de control para el acceso físico del personal autorizado.
Los activos de información que requieran protección especial, se deberán aislar de accesos no autorizados.
El área de trabajos deberá ser localizado en ubicaciones que no queden expuestas al acceso de externo o personal no autorizado, protegiendo tanto el equipamiento tecnológico como la documentación asociada.

Control de acceso

- El acceso físico al ambiente donde se encuentren los equipos será limitado sólo al personal autorizado[65].
- Para acceder al área de acceso restringida, se utilizarán dispositivos automáticos con claves de acceso, combinaciones de cerraduras, tarjetas magnéticas, y/o similares[66].
- El ingreso de usuarios que no realicen tareas operativas habituales tales como terceros externos, se registrará en forma específica en una nómina, la que será revisada en forma periódica. En la nómina se especificará el nombre, empresa, motivo de ingreso y fecha y hora de ingreso y egreso. Durante su permanencia deberá estar siempre acompañado por personal autorizado, a menos que su ingreso se haya aprobado previamente.
- Se utilizarán sistemas de monitoreo a través de cámaras de video.
- No habrá dentro del Área Operaciones y Redes, recursos de uso habitual por parte del personal (impresoras, suministros informáticos o similares).
- Ante situaciones de cambio de área o cargo de algún funcionario, las jefaturas directas deberán revisar sus permisos de acceso físico asignados y verificar el reasignamiento de aquellos permisos de accesos válidos de acuerdo a su nueva función.
- Se debe impedir el ingreso de equipos de computación móvil, fotográficos, de video, audio o cualquier tipo de equipamiento que permita registrar información, a menos que haya sido debidamente autorizado.

Factores ambientales

- Se mantendrán condiciones ambientales básicas de temperatura, climatización, higiene, aislamiento eléctrico y sonoro, y otras medidas similares de acuerdo a los requerimientos específicos del equipamiento informático y a sus protocolos de monitoreo.
- Se instalarán sistemas automáticos de detección y respuesta automática ante condiciones ambientales que puedan afectar el procesamiento de los equipos. También aplicará la instalación de sistemas automáticos de detección de intrusos y alarmas, cubriendo las áreas de acceso.
- Cuando no se pueda disponer de un sistema de extinción automática de incendios, se contará con extinguidores habilitados de uso específico.
- No se deben ingerir alimentos ni líquidos en los módulos o muebles que soporten equipamiento y/o dispositivos tecnológicos, como tampoco manipular y/o dejar líquidos en su cercanía.

Inventario

Se mantendrá un inventario detallado de los recursos de hardware y software instalados dentro de las áreas de Operaciones y Redes y de Soporte de Usuarios.

Seguros de los equipos computacionales

En caso de compra el equipamiento, incluido el Área Operaciones y Redes, deberá estar asegurado. La Jefatura el Subdpto TIC es responsable de gestionar la contratación de seguros de los recursos informáticos indicados, en tanto exista asignación presupuestaria por parte de la jefatura del Depto. de Administración y Finanzas.

[65] ISO 27002:2013 A.11.1.1
[66] ISO 27002:2013 A.11.1.2

Soportes físicos de las copias de respaldo

- Las copias de respaldo se conservarán en dependencias separadas del Área Operaciones y Redes, almacenadas en armarios incombustibles y de acceso restringido y con la respectiva identificación de contenido.
- Para el transporte de los soportes físicos a un sitio externo se utilizarán mecanismos de inviolabilidad y en caso de que sea un proveedor quien lo efectúe, se firmará el respectivo compromiso de confidencialidad.

Instalaciones eléctricas y servicios básicos de apoyo[67]

- Frente a cortes de energía eléctrica que afecten las dependencias del Área Operaciones y Redes, se garantizará un lapso de tiempo que permita: el cierre de las aplicaciones y las bases de datos, para la posterior bajada programada y automática de los servidores de modo de no dañar la información contenida.
- Para el cumplimiento del punto anterior se contará con unidades de suministro continuo de energía (UPS), estabilizadores de tensión y, de ser posible, grupos electrógenos fijos y/o móviles.
- Igualmente, la instalación eléctrica de los equipos será independiente de las instalaciones de consumo general y su instalación será realizada por empresas y/o personal certificados SEC, bajo norma chilena y garantizando máximo rendimiento de operación.
- El Área Operaciones y Redes garantizará que todo equipamiento tecnológico y/o área crítica, esté protegida contras cortes de energía y otras interrupciones provocadas por falla en los servicios básicos, para ello los servicios básicos de apoyo, tales como energía, telecomunicaciones, suministro de agua, ventilación y/o aire acondicionado, deberán cumplir con:
    - Poner en práctica las especificaciones de los fabricantes y/o proveedores del servicio
    - Revisiones regulares para garantizar su funcionamiento correcto
    - Contar con monitoreo y alarmas para la detección de fallas
    - En la conectividad de redes, se debe contar con una redundancia adicional mediante el servicio de conectividad por varias rutas distintas
- El cableado de electricidad y telecomunicaciones para el trasporte de datos o que apoyen los servicios de red interna, deberán estar protegidos para eliminar la posibilidad de intercepción, interferencia o daños, para ello:
    - El cableado de datos estará apartado del cableado de energía para evitar interferencias.
    - Uso de blindaje bajo norma para protección del cableado de datos.
    - Cajas de seguridad en los puntos de distribución de energía y datos
    - Acceso controlado a los paneles de cableado distribuido y/o salas de cableado

[67] ISO 27001:2013 A.11.2.2 / A.11.2.2

Norma N° 10: Uso de Correo electrónico, Internet y Redes Sociales

Objetivo

Proteger la información institucional enviada y recibida a través de servicios de correo electrónico, asegurar el buen uso e internet y de las redes sociales, fomentando el uso correcto y eficaz de los recursos de la Superintendencia de Salud.

Responsables del cumplimiento

Todo el personal de la institución y los terceros que interactúan de manera habitual u ocasional que accedan a información y/o a los recursos informáticos en el desarrollo de sus tareas habituales.

Incumplimientos

Las medidas disciplinarias están descritas en el Anexo – Sanciones por incumplimiento que forma parte del conjunto de medidas disciplinarias de la institución.

Disposiciones de la norma

Es norma de la institución, respecto de:

Correo electrónico

Casillas de Correo

- Las casillas de correo son de propiedad de la institución y asignadas a cada funcionario para el desempeño de sus labores. Su acceso está limitado al uso exclusivo del funcionario al cual fue asignada y solamente debe ser utilizada para las tareas propias de la función desarrollada por el funcionario en la institución.
- Será responsabilidad del funcionario usuario de la cuenta de correo electrónico modificar su clave de acceso periódicamente y en caso de considerar que ha sido vulnerada.
- El espacio asignado a las casillas de correo, será definido e informado de acuerdo a la disponibilidad de recursos institucionales por el Área Operaciones y Redes.
- El servicio no será entregado cuando la capacidad haya sido excedida. Los usuarios deben mantener y limpiar su casilla de correo electrónico. En caso que el usuario requiera conservar mensajería, deberá solicitar al Área Operaciones y Redes la posibilidad de realización de respaldos que fracciones su almacenamiento.
- Las casillas de correo serán respaldadas de forma centralizada y de acuerdo a la Norma de Respaldo institucional.
- La creación de casillas de carácter grupal deberá ser justificada y solicitada formalmente por la jefatura del grupo de trabajo. Su pertinencia y uso será evaluado el Encargado de Seguridad de la Información.
- Cuando el usuario se desvincule de la Institución, su casilla de correo será respaldada y posteriormente eliminada.

Mensajes

- Los contenidos de los mensajes enviados, es de absoluta responsabilidad del funcionario(a) a quien haya sido asignada la casilla.
- El tamaño de los mensajes está limitado de acuerdo a la disponibilidad de recursos tecnológicos institucionales.
- Está prohibido el envío de información sensible y datos, ya sea en archivos adjuntos o como parte del texto del correo, a terceros no autorizados que no tengan una relación formal con la Superintendencia y cuyo vínculo no esté relacionado con la información enviada.
- El envío de correos masivos de carácter institucional hacia el exterior, desde el servidor de correos institucional, será realizado exclusivamente por personal del Área Operaciones y Redes. Los requerimientos de correo masivo deben estar autorizados y justificados por los jefes directos de los solicitantes.
- Podrán ser restringidos algunos tipos de archivos que se consideren peligrosos para el normal funcionamiento de la institución, los cuales serán informados por el Área Operaciones y Redes mediante comunicación formal.
- Todo mensaje enviado debe contener una notificación, que indica que su contenido es de carácter privado y confidencial, esto es, un texto estándar incorporado en forma automática, indicando la privacidad y confidencialidad del mensaje que se remite.

Servicio

- La plataforma de correo será la que la institución determine y provea.

- El servicio de correo electrónico debe estar protegido con dispositivos de seguridad lógicos, tales como firewall, antispam, antivirus y los que sean necesarios en tanto evolucione la tecnología.
- El servicio será prestado de manera exclusiva al personal de la institución y, cuando se estime necesario, a terceros externos que mantengan una relación de trabajo con ella.
- El servicio de correo electrónico podrá ser accedido desde dispositivos móviles compatibles, internet y de forma interna en los puestos de trabajo.
- El Área Operaciones y Redes será la encargada de proteger adecuadamente la información de mensajería electrónica, considerando: protección de acceso no autorizado, negación de servicio, garantizar dirección y transporte del mensaje, confiabilidad y disponibilidad del servicio, respaldo y restauración[68].

Consideraciones adicionales.

La institución imparte las siguientes instrucciones respecto al uso seguro del correo electrónico:

- Se advierte sobre accesos no autorizados que puedan vulnerar el correo electrónico institucional;
- Los usuarios serán responsables de la apertura de archivos adjuntos y/o ejecución de programas que se reciban vía correo electrónico, en particular de fuentes desconocidas, que eventualmente puedan vulnerar el correo institucional;
- Se prohíbe divulgar contraseñas de acceso y/o almacenar contraseñas de acceso en el mismo computador desde el cual se accede el correo electrónico;
- Se recomienda el uso de aplicaciones de correo libre o privado para los usuarios que requieran tener cuentas de correo electrónico distintas para uso personal.
- Se recomienda la necesidad de comprobar el origen, despacho, entrega y aceptación de correo electrónico de entrada y salida.
- Se advierte de las responsabilidades que corresponden a los usuarios en caso de comprometer a la institución, por ejemplo, con el envío de correos electrónicos difamatorios, uso para hostigamiento o acoso, compras no autorizadas, cadenas, etc.
- Se prohíbe el uso de cuentas de correos de otros usuarios, siendo responsable el funcionario que facilitó su cuenta y clave de acceso, de alguna situación no deseada que se produzca con su cuenta. En caso que la cuenta y clave de acceso no hayan sido obtenidas del funcionario dueño de ella, se le exime de la responsabilidad, no obstante, se seguirán las acciones administrativas correspondientes a las acciones realizadas.
- Todo correo electrónico enviado desde una cuenta de la Superintendencia de Salud debe incluir, en su pie de página, una advertencia de uso y autorizaciones, quedando bajo responsabilidad del receptor el cuidado y resguardo de la información. El formato a utilizar es el siguiente:
  "Este mensaje y sus adjuntos pueden contener información confidencial y es de uso exclusivo de la persona o entidad de destino. Si no es usted el destinatario indicado, queda notificado que la lectura, utilización, divulgación, reenvío o copia sin autorización no está autorizada por el firmante y se encuentra estrictamente prohibido en virtud de la legislación vigente. Si ha recibido este mensaje por error, le rogamos que nos lo comunique, inmediatamente por esta misma vía y proceda de inmediato a su destrucción"

Uso de redes Sociales

Responsabilidades

Todos los funcionarios

- Es responsabilidad de los funcionarios evitar la publicación en redes sociales, de cualquier información que pueda afectarlos de manera personal o que implique divulgar alguna materia o temática que se relacione con el trabajo institucional. Por ningún motivo se debe utilizar información privilegiada, de manera directa o indirecta, en estos medios sociales.
- Es recomendable utilizar las herramientas que protegen la privacidad de los sitios de redes sociales, tales como Facebook, Instagram u otros. También es

[68] ISO 27002:2013 A.13.2.3

recomendable proteger los datos personales utilizando los sistemas operativos de los teléfonos móviles y de los computadores personales.
- Evitar la descarga de archivos de origen desconocido, que podría tratarse de algún tipo de malware. Si es necesaria su descarga, debería solicitar ayuda al Área de Soporte de la Unidad de Tecnologías de Información.

Uso de internet

Responsabilidades

Al Área Operaciones y Redes le corresponde:
- Revisar las categorías de navegación y las excepciones de las mismas
- Auditar la integridad de las categorías de permiso de navegación.
- Controlar la navegación de Internet.
- Informar al Oficial de Seguridad las situaciones anómalas acontecidas.
- Enviar avisos de violación a las normas, políticas, procedimientos y estándares.

A los funcionarios de la Superintendencia les corresponde:
- Informar a sus Jefaturas Directas de cualquier actividad que contravenga las normas de usos de Internet.
- Ser responsables del acceso permitido al uso de Internet.

Utilización
- Este servicio debe utilizarse exclusivamente para las tareas propias de la institución y no debe usarse para ningún otro fin.
- Los computadores asignados a los funcionarios son configurados con restricciones para la descarga de archivos desde internet, cualquier cambio no autorizado a esta configuración mediante violación de los medios de protección, será sancionada de acuerdo a la gravedad y consecuencias del hecho.
- Cualquier requerimiento para descargar archivos que sean necesarios para la operación o desarrollo de la actividad laboral, debe ser solicitado al Área Operaciones y Redes con conocimiento y autorización de la Jefatura directa.
- En caso de navegar en internet con equipamiento institucional usando un formato de conexión no vinculado a los formatos de protección de la Superintendencia Por ejemplo banda ancha móvil), el funcionario deberá informar oportunamente cualquier situación anómala detectada al Área Operaciones y Redes.
- Está prohibido visitar sitios que inciten a cometer actos ilícitos, que promuevan conductas riesgosas para la institución o que puedan dañar la reputación institucional.

Servicio

Se proveerá el servicio a todo funcionario de la Superintendencia que tenga computador institucional asignado.
- Se bloqueará el acceso a sitios que pudieran perjudicar los intereses y la reputación de la Superintendencia.
- Para limitar el acceso a sitios catalogados como peligrosos, la institución bloqueará la navegación para la protección y seguridad de la información institucional. Para ello se utilizará tecnología vigente (que actualmente es del tipo Proxy y Firewall).
- El Área Operaciones y Redes podrá limitar el acceso a sitios que capturen y consuman el ancho de banda que la institución requiere para su normal operación, esto es entre otros, sitios de distribución de audio (música, radios, sitios de concentración y distribución de links de audio), también se limitará el acceso a contenidos de multimedia (streaming, video directo, televisión abierta, etc.).
- En casos justificados y autorizados se proveerá de conexión tipo VPN a aquellos funcionarios que requieran trabajar a distancia. Conexión que debe contar con todos los niveles de seguridad necesarios para establecer una comunicación que no ponga en riesgo la integridad ni la confidencialidad de los datos transferidos.
- Las conexiones inalámbricas serán provistas por el Área Operaciones y Redes y se vincularán a la red de protección computacional.

Restricciones de Uso de Internet
- No está permitido descargar desde Internet material que infrinja el Ordenamiento Jurídico Nacional y/o las disposiciones contenidas en el Reglamento Interno, en el Código de Ética o en la normativa establecida por la institución.

- El uso de las redes sociales como streaming de información, chats, foros, blogs y sitios de entretenimiento. Su acceso, sólo serán permitido con la autorización formal del Jefe de Servicio.
- Está prohibido el ingreso a páginas web con contenido pornográfico, discriminadores, con violencia explícita, grupos extremistas, abuso de alcohol y drogas y sitios similares.
- Acceso a sitios de "hacking" o sitios reconocidos como inseguros, los cuales pueden poner en riesgo la integridad y confidencialidad de la información de la Institución.
- Instalación o distribución de software que no se encuentre licenciado para el uso por parte de la Superintendencia.
- Cualquier excepción deberá ser estudiada por el Oficial de Seguridad y el Comité de Seguridad de la Información.

Norma N° 11: Comunicaciones

Objetivo

Asegurar la protección de la información en los procesos de transmisión y recepción de datos en las redes internas y externas de la institución.

Responsables del cumplimiento

Todo el personal del Área Operaciones y Redes, funcionarios de la Superintendencia y terceros que estén vinculados a los procesos de transmisión de datos en el desarrollo de sus tareas habituales.

Incumplimientos

Las medidas disciplinarias están descritas en el Anexo Sanciones por incumplimientos que forma parte del conjunto de medidas disciplinarias de la institución.

Disposiciones de la norma

El Área Operaciones y Redes pondrá a disposición una red de datos, para la comunicación interna y externa de los funcionarios utilizando los siguientes componentes y consideraciones:

Conexiones internas

- Dispositivos automáticos de comunicación, para conectar los distintos segmentos de la red interna y también para conectar las distintas estaciones de trabajo y servidores entre sí.
- Mecanismos de encriptación para la información sensible propia de los sistemas (contraseñas, bases de datos de seguridad o similares).
- Esquema de direccionamiento IP teniendo en cuenta las direcciones privadas definidas en la normativa internacional respectiva, para evitar que éstas sean accedidas desde el exterior (protección contra intrusión indebida).
- Puntos de red internos de los usuarios y dispositivos computacionales debidamente rotulados de modo que frente a una falla se pueda dar continuidad operativa a las labores.
- Existencia de un mapa de conexiones entre equipos de comunicación y puntos de red internos, que permita el análisis previo de posibles fallas y la asistencia adecuada cuando los eventos de falla se presenten.

Conexiones externas

- El origen de todas las conexiones remotas será autenticado utilizando un nivel aceptado de autenticación (por ejemplo: autentificación de sistemas, clave VPN, etc.)
- Todo acceso desde el exterior a la red interna de la institución será canalizado a través de una red segmentada y protegida (DMZ - zona desmilitarizada).
- Las conexiones externas podrán acceder solamente a los servicios, sistemas y/o aplicaciones a los que están autorizados.
- Los accesos externos serán registrados y controlados para determinar posibles intentos de accesos no autorizados.
- Los contratos con los proveedores, incluirán, si es pertinente, la utilización de vías alternativas de comunicación para cuando se presenten interrupciones del servicio.
- Las conexiones externas con la red interna de la institución se realizarán a través de tecnologías adecuadamente controladas.
- Se utilizarán sistemas de monitoreo de accesos que permitan la detección de posibles ataques con acciones automáticas para prevenirlos.
- El servicio de Acceso Remoto será utilizado solamente para conexiones entrantes y en función al perfil del usuario que se conecta y su autenticación, se establecerán los servicios y direcciones habilitadas para dicho usuario.
- No se permitirán accesos directos entre dominios no confiables hacia el ambiente de producción. Las excepciones deben ser autorizadas por la Oficial de Seguridad y la jefatura del Área de Informática que debe establecer el control y revisión permanente.
- Todos los dispositivos de red deben tener contraseñas únicas y deben utilizar encriptaciones WPA2 o WPA/SDK o superior, además de no permitir su administración remota.

Aspectos particulares de accesos externos a través de Internet

- Los contratos con proveedores de servicios de Internet, considerarán la descripción de todos los servicios provistos y en lo posible, de todos aquellos que en un futuro pudiera requerir la institución.
- Todas las conexiones se habilitarán a través de un Firewall o equipamiento de control y filtro de comunicaciones de entrada y salida.
- En el caso de las conexiones entrantes, se llevará registro de los intentos fallidos, con registro de la dirección IP de origen, el servicio requerido, el motivo del rechazo, la fecha y hora de acceso.
- En el caso particular de las conexiones salientes, éstas serán validadas a través de un servidor que verifique autenticidad, autorización y monitoreo de la cuenta de usuario, registrando los servicios utilizados, las direcciones IP accedidas, fecha y hora de acceso.

Norma N° 12: Desarrollo y Mantenimiento de Sistemas Informáticos

Objetivo

Asegurar la consistencia, disponibilidad y tratamiento de datos según los requerimientos institucionales, mediante la aplicación de normas en el proceso de mantención y desarrollo de sistemas. Asegurar la inviolabilidad de los códigos fuentes desarrollados.

Alcance de esta norma interna

Se aplica a todos los sistemas de información desarrollados internamente o por terceros externos.

Esta política se aplica a todos los usuarios de la Superintendencia de Salud, ya sean funcionarios de planta, contrata, honorarios, asesores, consultores, practicantes y otros trabajadores, incluyendo aquellas empresas que presten servicios a la Superintendencia.

Responsables del cumplimiento

Todo el personal del área de Desarrollo de Tecnologías de Información y el Área Operaciones y Redes, además de personal externo autorizado que interactúe de manera habitual u ocasional con sistemas de información y/o recursos informáticos institucionales, en labores de planificación, análisis, diseño, desarrollo, mantención e implementación de soluciones informáticas.

Incumplimientos

Las medidas disciplinarias están descritas en el Anexo Sanciones por incumplimiento, que forma parte del conjunto de medidas disciplinarias de la institución. En el caso del personal externo contratado para esta actividad, deberán consignarse en los contratos con las empresas que proveen el servicio, cláusulas que especifiquen las correspondientes sanciones en caso de incumplimiento.

Disposiciones de la norma

Aspectos generales

- En los procesos de desarrollo y mantención de sistemas se deberán considerar aspectos de seguridad en tres ámbitos: programas fuentes, datos y acceso de usuarios. Para ello se deberá aplicar una metodología de desarrollo que involucre los datos, la información que aportará el sistema y los accesos, elementos todos que eventualmente podrían poner en riesgo la seguridad de la información institucional.
- El Encargado del Área Operaciones y Redes designará a las personas de su área que cumplirán las funciones para garantizar el cumplimiento de requerimientos de seguridad referidos al resguardo de programas fuentes, datos y accesos[69].
- Se debe evaluar que los requerimientos de seguridad y los controles requeridos, sean proporcionales en costo y esfuerzo al valor del bien que se quiere proteger y al daño potencial que se pudiera ocasionar a las actividades realizadas. En todo caso es fundamental la protección de los datos sensibles y los datos reservados, de modo de garantizar el cumplimiento legal y la debida reserva de la información de los usuarios, contenida en las bases de datos.
- Cualquier cambio en las plataformas operacionales, debe ser probado previamente en el área de pruebas (ambiente segregado específico)[70].
- Ante posibles vulnerabilidades de los sistemas, se debe establecer, en conjunto con el Área Operaciones y Redes, las acciones que permitan determinar si se precisa de una mejora en los programas fuentes de las aplicaciones en uso.
- Sobre los paquetes de software desarrollados externamente. El Área de Informática y el Área Operaciones y Redes son las áreas encargadas de apoyar la implementación de paquetes de software externo, estableciendo que tales aplicaciones deberán operar sin modificaciones, aplicando control a los posibles riesgos a la integridad de la(s) plataforma(s) y el impacto a riesgos que deben ser definidos y tratados[71].
- Los sistemas de información, tanto de desarrollo interno como los paquetes de software desarrollados externamente se deben revisar regularmente para verificar su cumplimiento con las políticas y normas de seguridad de la información establecidas en la institución (cumplimiento técnico)[72].

---

[69] ISO 27002:2013 A.14.2.1
[70] ISO 27002:2013 A.14.2.3
[71] ISO 27002:2013 A.14.2.4
[72] ISO 27002:2013 A.18.2.3

- Posterior a la implementación se debe revisar y auditar la existencia de controles de seguridad definidos en la etapa de diseño.

Programas Fuentes

Generación de código fuente

Se deben diseñar procesos para el desarrollo y mantención de software que cumplan con una metodología definida que garantice la integridad e inviolabilidad del código fuente desarrollado. Para ello, los procedimientos deben definir medidas de seguridad tales como:

- Operar dentro de un ambiente de desarrollo con acceso restringido y sin acceso al ambiente de producción.
- Separación de ambientes de desarrollo, testing y producción.
- Definición y separación de las funciones del personal involucrado en el desarrollo y mantención de sistemas, del personal del Área Operaciones y Redes cuando los sistemas están en operación[73].
- La metodología de desarrollo de sistemas debe contemplar un procedimiento para realizar el control de cambios en los requerimientos[74].
- La metodología debe establecer requisitos de seguridad, documentar, mantener y aplicar principios para la ingeniería de desarrollo de sistemas seguros, en cualquier punto del desarrollo o implementación de sistemas de información, tanto de los nuevos desarrollos, como de las mejoras a sistemas existentes[75].
- En los contratos con terceros externos para el desarrollo de software específico, se deberán incorporar aspectos relacionados con el licenciamiento, calidad del software, seguridad y propiedad de fuentes desarrollado según contratos[76].

Mantención y resguardo de código fuente

- Se debe mantener un control de versiones de los códigos fuente y su correspondiente ejecutable, como también de sus respaldos.
- El procedimiento de mantención de software debe definir claramente a las personas usuarias que tendrán la atribución de solicitar cambios, mantenciones correctivas y evolutivas, los que deben ser evaluados en su impacto a nivel institucional y eventualmente aprobados por el Comité de Seguridad.
- Las mantenciones a paquetes de software serán evaluadas por el Área de Informática y su ejecución deberá ser autorizada y justificada por las jefaturas de las distintas áreas de la institución y sólo si responden a motivos de fuerza mayor.

Protección de datos

- Dependiendo de la naturaleza de los datos y los requerimientos de seguridad de los usuarios, se deben considerar medidas de seguridad adecuadas y específicas para cada proyecto informático (desarrollo o mantención), considerando siempre la protección de datos sensibles y datos reservados como parte del mismo, independiente que esta materia no sea parte de los requerimientos definidos.
- Durante las etapas de análisis y diseño, se deberán identificar, documentar y aprobar los requerimientos de seguridad que se otorgarán a los datos y/o mensajes que el sistema remita e incorporarlos en las etapas de desarrollo e implementación.
- Se deberán diseñar e implementar procedimientos de validación de datos y accesos de acuerdo a perfiles de usuarios.
- El equipo de trabajo encargado del proyecto, deberá, en la etapa de recepción y análisis de requerimientos, definir la pertinencia de incorporación de datos sensibles y datos reservados, y los distintos perfiles de acceso de usuarios, además de nominar a quienes inicialmente puedan acceder a esta información y las restricciones de acceso.
- Cada sistema desarrollado debe contar con un usuario administrador funcional en la etapa de operación normal, que tenga privilegios de administración de parámetros y perfiles de usuarios propios del sistema, que será responsable de la coherencia de los parámetros entre sí y de la compatibilidad de éstos a nivel institucional.
- Se deberán diseñar e implementar las herramientas de software necesarias para que el usuario administrador del sistema monitoree la operación de éste por parte

[73] ISO 27002:2013 A.9.4.5 / A.14.2.6
[74] ISO 27002:2013 A.14.2.2
[75] ISO 27002:2013 A.14.1.1 / A.14.2.5
[76] ISO 27002:2013 A.14.2.7

de los usuarios finales y permita identificar fallas en la operación que podrían redundar en una mala calidad de la información que provee el sistema.

- En los contratos con terceros externos para el desarrollo de software específico, se deberán incorporar aspectos relacionados con la seguridad y la confidencialidad de la información, así como también las sanciones por incumplimiento[77].
- Todo desarrollo externo debe ser supervisado y monitoreado por la Institución, mediante metodología definida de común acuerdo entre ambas partes. El monitoreo debe considerar al menos:
  - Niveles de desempeño del servicio y acuerdos formales ante posibles incidentes de seguridad por la actividad de terceros externos;
  - Aseguramiento de capacidad de servicio suficiente que garanticen niveles de continuidad ante fallas;
  - Cambios a la provisión de servicios (SLA) y/o cambios producidos por el desarrollo de nuevas aplicaciones[78].
- Todo sistema desarrollado debe incluir un plan de respaldo periódico y recuperación de datos que, en régimen de operación normal y debe ser ejecutado por el Área Operaciones y Redes.
- Al utilizar Firma Electrónica Avanzada, se debe considerar la legislación vigente que describe las condiciones bajo las cuales una firma digital es legalmente válida.
- Las pruebas, tanto de desarrollo como de usuarios, se deben realizar en un ambiente aislado del ambiente de producción, privilegiando el uso de datos ficticios; para el caso de información sensible y/o reservada, si así lo requiere el tipo de prueba, se establecerán procedimientos de control de responsabilidad de uso, en la utilización de la información real para estos tipos de datos[79].
- Las aplicaciones desarrolladas para ambiente web y telefonía móvil deben considerar las medidas de seguridad que ofrece el mercado y desarrollar las que sean necesarias para proteger los datos y software de ataques maliciosos.
- La modificación, actualización o eliminación de datos del ambiente de producción, sólo podrán ser realizados a través de sistemas de información y de acuerdo al esquema de control de accesos implementado.
- Los casos en los que no fuera posible aplicar la precedente norma, se deben considerar excepciones, y será el Encargado de Seguridad quien definirá las coordinaciones para la gestión de dichas excepciones, los cuales deberán establecer claramente el responsable de la solicitud y el ejecutor de las mismas.

Control de acceso

- Cada proyecto informático, en su proceso de desarrollo, debe considerar la definición de perfiles de usuarios autorizados a acceder a los datos, operar el sistema, mantener parámetros, utilizar firma electrónica avanzada y controlar el acceso a funcionalidades.
- Cuando se trabaje con datos sensibles, se deberán definir los perfiles de usuarios que tendrán acceso a ellos y bajo qué condiciones. Se deberán diseñar e implementar restricciones y controles necesarios para resguardar la confidencialidad de estos datos, utilizando métodos de encriptación, si son requeridos.
- La documentación debe incluir las pautas para mantener la consistencia en el acceso y/o restricciones a las funcionalidades en cuanto a la incorporación o desvinculación de nuevos usuarios.
- Cada sistema debe generar una bitácora de acciones relevantes, las que serán registradas con fecha y firma electrónica simple.
- Se deberá asegurar que la información involucrada en desarrollos de aplicaciones que pasen a través de redes públicas, serán protegidas de actividad fraudulenta, acceso y/o modificación no autorizada mediante autenticación, requisitos de protección de información confidencial y protección para evitar pérdida o duplicación de la información transaccional. También se deberá considerar protección que evite la transmisión incompleta, enrutamiento incorrecto mediante técnicas tecnológicas, entre otras, firma electrónica, autenticación punto a punto, protocolos de comunicación protegidos y/o certificados digitales de confianza[80].

[77] ISO 27002:2013 A.14.2.7
[78] ISO 27002:2013 A.15.2.1 / A.15.2.2
[79] ISO 27002:2013 A.14.2.8 / A.14.2.9 / A.14.3.1
[80] ISO 27002:2013 A.14.1.2 / A.14.1.3

Norma N° 13: Auditoría Automática de los Sistemas de Información

Objetivo

Asegurar una adecuada identificación y seguimiento de los eventos que requieren de seguridad al interior de los sistemas de información.

Alcance de esta norma interna

Esta norma aplica a los procedimientos sobre los registros de seguridad que deben tener los sistemas de información, su implementación y acceso.

Responsables del cumplimiento

Todo el personal del área de Desarrollo, usuarios administradores de sistemas y quienes participen en los equipos de trabajo en fase de desarrollo y personal del Área Operaciones y Redes en la implementación de pautas de seguridad de la información.

Incumplimientos

Las medidas disciplinarias están descritas en el Anexo Sanciones por incumplimientos que forma parte del conjunto de medidas disciplinarias de la institución.

Disposiciones de la norma

Requerimientos de registro de eventos de seguridad

- Serán formalmente acordados y convenidos en la etapa de levantamiento y toma de requerimientos durante el proceso de desarrollo de sistemas. El acuerdo debe ser convenido en el grupo de trabajo y ratificado con el Área Operaciones y Redes.
- Exclusivamente los usuarios administradores sistemas de información específicos, podrán solicitar al Encargado de Seguridad Institucional registrar eventos adicionales de seguridad.
- Para situaciones de excepción, a través de las jefaturas pertinentes, se podrá solicitar el registro de eventos de algún usuario.

Implementación de registro de eventos de seguridad[81]

El Área Operaciones y Redes es responsable de implementar los eventos de seguridad de los sistemas de información desarrollados internamente en los servidores que los soporten.

- Para una mejor implementación, se contará con el apoyo del área de Desarrollo, quienes, en la etapa de requerimientos y análisis de desarrollo, conocerán de los requerimientos de seguridad de cada sistema de información en particular.
- Se registrarán todos los eventos relacionados con las configuraciones de seguridad de los sistemas de información.
- Todo software desarrollado debe permitir el registro automático de la información de los eventos de seguridad.

Acceso a los registros

Exclusivamente el Encargado de Seguridad, el personal del Área Operaciones y Redes, Auditoría Interna y funcionarios autorizados, pueden acceder a los registros de eventos de seguridad en la medida que lo permitan los sistemas.

Eventos generales a registrar para todos sistemas de información

- Accesos fallidos de ingreso de usuarios
- Alta, baja o modificación de usuarios y grupos
- Cambios en la configuración de la seguridad
- Procesos de depuración de información no automatizados
- Cambios de perfil para usuario que tengan permisos temporales
- Accesos de usuarios que accedan a información clasificada como sensible
- Accesos de los usuarios del área de Desarrollo de Sistemas cuando acceden al ambiente de Producción.

Acciones ante situaciones de anormalidad

- El Área Operaciones y Redes debe analizar los eventos de seguridad e informar al Encargado de Seguridad Institucional ante incidentes observados.
- El Encargado de Seguridad informará al Dueño de Datos si corresponde y al Jefe del área de Recursos Humanos y de Auditoría Interna cuando la situación lo amerite.
- El Área Operaciones y Redes conservará los respaldos de soportes de seguridad y eventualmente comunicará al Encargado de Seguridad la necesidad de conservación por períodos mayores a los definidos en las políticas de respaldo.

[81] ISO 27002:2013 A.12.4.1 / A.12.4.2

Norma N° 14: Tercerización de Servicios Tecnológicos e Informáticos

Objetivo

Definir las actividades y las acciones que permitan guiar, formalizar y administrar los procesos de entregar a terceros la responsabilidad por la ejecución de tareas de la institución, uso y aplicación de tecnologías de la información (Outsourcing).

Por Outsourcing se entiende la acción de delegar de manera regular en especialistas externos la responsabilidad en la ejecución de determinadas funciones y tareas de sistemas y administración de infraestructura de TI, de modo tal que la organización pueda concentrarse en sus negocios específicos. Estas acciones no se refieren a contrataciones cortas y puntuales, sino a la prestación de un servicio establecido con acuerdos firmados y con una duración prolongada.

Alcance de esta norma interna

Esta norma aplica a los procedimientos sobre asociados a la gestión de TI, los equipos informáticos de la Organización, y equipos externos que eventualmente deban conectarse a la red de la Entidad y sus unidades dependientes donde sea implementado este procedimiento, como las aplicaciones y programas que se utilizan para el procesamiento de datos e información.

Responsables del cumplimiento

Todos los usuarios, Administradores de Seguridad, Custodio de las Datos, las Unidades de Informática, Jefaturas de División, Jefaturas de Departamento, Jefaturas de Servicio, y la Unidad de Gestión de Personas son responsables del cumplimiento de este procedimiento.

Registros de Control

Todos los usuarios, Administradores de Seguridad, Custodio de las Datos, las Unidades de Informática, Jefaturas de División, Jefaturas de Departamento, Jefaturas de Servicio, y la Unidad de Gestión de Personas son responsables del cumplimiento de este procedimiento.

Incumplimientos

Las medidas disciplinarias están descritas en el Anexo Sanciones por incumplimientos que forma parte del conjunto de medidas disciplinarias de la institución.

Disposiciones de la norma

Para una adecuada administración de los riesgos relacionados con la delegación de funciones a empresas y/o personal externo a la institución, es necesario establecer un adecuado método de enfrentar los procesos de tercerización y definir sus principales modalidades con su respectiva metodología de ejecución.

Servicios de TI sujetos a tercerización

- Infraestructura de tecnologías de la información, que comprende dotar a la Superintendencia de todo el Hardware de base, las redes de comunicaciones, los sistemas de almacenamiento, los servidores u otra capacidad de procesamiento de la información y el software relacionado.
- Desarrollo y mantenimiento de software, que incluye el análisis, el diseño y el desarrollo de aplicaciones personalizadas.
- Gestión de aplicaciones y sistemas, que comprende la conducción de la operación diaria de programas aplicativos y sistemas de aplicaciones incluidos mantenimiento, monitoreo, soporte de usuarios, soporte de performance (desempeño) y básico.
- Provisión de soluciones de Aplicaciones (ASP), que engloba a la prestación y entrega de una oferta de servicio contractual que permite la puesta en marcha, el hospedaje, la gestión y el acceso, así como el recibir directamente en la ubicación de la institución, el producto de la ejecución de soluciones ubicadas y administradas en forma remota y sin que estas sean de propiedad de la institución.
- Servicios de punta a punta, que involucra la entrega de toda la gama de prestaciones asociadas a la utilización de Tecnologías de la información a la institución, desde la gestión del funcionamiento diario, a través de la infraestructura básica, hasta la operación y entrega de resultados de aplicaciones y servicios de todo nivel.

- Otros, que comprende prestaciones específicas y generalmente de alto nivel de experticia tales como la ingeniería de sistemas o comunicaciones, la puesta en marcha o migraciones de aplicaciones complejas, la evaluación y mitigación de riesgos, o la integración e investigación de aplicaciones y utilización de nuevos dispositivos tecnológicos.

Tratamiento para procesos de evaluación y asignación de servicios a un tercero

La externalización de servicios debe realizarse cumpliendo con lineamientos precisos, usando una metodología estructurada y cuidando de evaluar no sólo las oportunidades que conlleva, sino también los riegos que el cambio paradigmático involucra.

Modelo de ejecución de un proceso de tercerización

La tercerización mejora la flexibilidad institucional, además de incrementar la capacidad para acomodarse a las cambiantes situaciones y oportunidades de aumentar eficiencia/eficacia, pero su adopción debe planificarse, ya que el proceso ineludiblemente enfrentará una serie de riesgos asociados. Para minimizarlos es necesario cubrir los siguientes ámbitos de acción:

Estrategia de tercerización

- Se requiere un período de análisis evaluación y discusión para decidir la factibilidad y conveniencia del proyecto y fijar los objetivos.
- Se debe identificar y establecer el alcance de los procesos potencialmente a externalizar, los criterios y factores necesarios para tomar la decisión y el examen de los beneficios estratégicos.
- Se debe contrastar la prestación de los servicios en cuestión con los medios internos de que dispone la institución y contrastarlos con la entrega de ellos desde fuera de la organización.
- Se deben determinar las ventajas que se obtendrán mediante la contratación de los servicios.
- Se debe definir la administración del proyecto y analizar cuál será el impacto del cambio.
- Se deben definir los criterios de selección de los proveedores y establecer una evaluación preliminar del mercado de los proveedores.

Evaluación de proveedores y llamado a licitación

- Se realiza la exploración del mercado público para asegurar la disponibilidad de proveedores que ofrezcan los servicios requeridos y se fijan los criterios y requisitos para el llamado y evaluación de las propuestas, los servicios a licitar y las estrategias de negociación.
- Se debe emitir un llamado a propuesta (RFP) en un formato que garantice la entrega y recepción de información en forma imparcial, no sesgada y homologable. El llamado a propuesta debe incluir detalle descriptivo de los productos y servicios solicitados, su nivel de servicios esperados y, de ser necesario, alternativas de solución a ser estudiadas y presentadas por los eventuales proveedores. Se deja claramente establecido que toda licitación deberá cumplir con todos los estándares definidos por la administración pública para tal efecto.
- Las propuestas deberán ser evaluadas siguiendo algún modelo de benchmarking que las torne homogéneas.

Adjudicación

- Evaluadas las ofertas y aprobado el pliego de condiciones se adjudica el servicio a un proveedor principal y, como mínimo, se selecciona un proveedor alternativo de contingencia.
- Se debe planificar y acordar la transferencia del servicio, ajustando el alcance y los detalles del servicio de acuerdo a los resultados de la evaluación (financiero-contable-técnico) del proveedor, se establecen los modelos para fijar los precios, las condiciones de borde (como pueden ser adiciones o disminuciones en las prestaciones de servicios, la periodicidad y duración de los acuerdos tarifarios) y los límites de dichos acuerdos.
- Se redactan y firman los contratos principales y anexos, los acuerdos de nivel de servicios (Service Level Agreements-SLA's), y las cláusulas de penalidad o multas.

Implementación y administración

- Se elabora y sigue un plan de implementación donde se transfieren, de acuerdo a la concepción del proceso, las responsabilidades, los recursos humanos y los activos según lo firmado, respetando un calendario y un cuidadoso plan de comunicaciones. En estos procesos siempre hay un período de traslape, en el cual coexisten los esquemas de trabajo pre-tercerización con los del proveedor contratado, hasta que éste se hace cargo por completo del servicio.
- Se debe exigir al proveedor un plan detallado de conducción del cambio que considere en detalle las situaciones que la migración tanto física como de servicios acarreará a la organización.
- El servicio tercerizado se somete a evaluación y control por parte de la Superintendencia, nombrándose a un coordinador entre el proveedor y la institución. El coordinador controla que la prestación del servicio sea satisfactoria, incluyendo el seguimiento y control del proceso a nivel estratégico, así como operativo, o sea cómo se presta el servicio en la práctica, la calidad de los procesos y el esquema metodológico adoptado, la respuesta ante requerimientos, el cumplimiento de acciones de soporte y de reparación, así como el cumplimiento de los procedimientos de escalamiento.

Roles y Atribuciones de Administración de Proyecto de Externalización de TI

Se deben considerar diferentes roles, para su desarrollo y concreción:

- Jefe de Proyecto: Corresponde a la jefatura de la Unidad de Tecnología. Debe establecer los objetivos, definir los indicadores para evaluar el avance del proyecto, asignar el equipo de trabajo, negociar el servicio y sus SLA, adjudicar e implementar el servicio.
- Equipo de Trabajo: Corresponde al conjunto de profesionales que participan en el proyecto de externalización del área de informática u otras áreas de la institución. Realizan el trabajo detallado, recopilan y estructuran la información relevante para definir el servicio y sus SLA (Niveles de Servicio), estructurar los antecedentes provistos por los proponentes, ponderan la información y presentan las alternativas de decisión.
- Administrador de Contrato: funcionario de la Unidad TI al cual se le asigna el rol de administrar el contrato adjudicado al proveedor, con el objeto de asegurar la prestación de los servicios y SLA contratados, así como administrar los cambios al contrato de externalización que van ocurriendo con el servicio.

Norma N° 15: Gestión de la Ciberseguridad

Objetivo

La Política Nacional de Ciberseguridad tiene por objetivo el diseño, implementación y puesta en marcha de medidas que permitan proteger la seguridad y la libertad de los usuarios del ciberespacio, reafirmando el compromiso nacional de promover un ciberespacio libre, abierto, democrático y seguro.

Para poner en práctica esta política, el Ministerio del Interior estableció dentro de su institución un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información, denominado CSIRT (Computer Security Incident Response Team, Equipo de Respuesta ante Incidencias de Seguridad Informáticas).

La Superintendencia de Salud estableció, a través del Comité de Seguridad de la Información, la Norma de Gestión de Incidentes de Seguridad, que aborda los procedimientos y protocolos orientados a la mitigación y corrección de vulnerabilidades y amenazas que pudieran afectar la seguridad de su información institucional, o la continuidad operacional de sus servicios estratégicos.

Los objetivos específicos buscan:

- Establecer responsabilidades de las distintas Unidades con relación a la seguridad de los datos institucionales (integridad, disponibilidad y confidencialidad), ya sea se encuentren en la plataforma informática como en su manipulación a cargo de los funcionarios en general.
- Responder en forma rápida, eficaz y ordenada ante la ocurrencia de incidentes de seguridad que afecten los activos de información institucionales.
- Asegurar un enfoque consistente y eficaz sobre la gestión de los incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

Alcance de esta norma interna

Esta norma aplica a los procedimientos sobre los registros de seguridad que se realizan en el ciberespacio, sus transacciones, almacenamiento y acceso.

Responsables del cumplimiento

Todos los usuarios, Administradores de Seguridad, Custodio de las Datos, las Unidades de Informática, Superintendente, Jefaturas de Intendencias, Jefes de Departamento y Gestión de Personas son responsables del cumplimiento de este procedimiento.

Incumplimientos

Las medidas disciplinarias están descritas en el Anexo Sanciones por incumplimientos que forma parte del conjunto de medidas disciplinarias de la institución.

Disposiciones de la norma

Para una adecuada administración de los riesgos inherentes al procesamiento y almacenamiento de la información en el ciberespacio se deberá llevar un control minucioso de los activos de información que se utilizan en esta plataforma y mantener un registro detallado de incidentes de Ciberseguridad en una Base de Datos que permita el análisis de información para corregir y evitar efectos adversos en la continuidad operacional[82].

Gestión de la Infraestructura Crítica de Ciberseguridad

La gestión de infraestructura en materias de Ciberseguridad requiere una adecuada administración de riesgos, establecer niveles de tolerancia, definir roles y responsabilidades de los participantes y aplicar metodologías para llevar a cabo las mejores prácticas de negocio. Por ello es fundamental definir la infraestructura crítica de Ciberseguridad de modo que sea posible mantener la continuidad de los sistemas de información y junto con ello, la continuidad operacional de la institución.

Para esto se deben considerar los siguientes elementos:

- Identificar la infraestructura crítica en términos de Ciberseguridad, esto es, aquellos activos de información lógicos que son considerados críticos para el funcionamiento del negocio. Asimismo, identificar la infraestructura física, hardware y sistemas tecnológicos que almacenan, administran y soportan estos

[82] Recopilación actualizada de normas Superintendencia de Bancos

activos y que, de no operar adecuadamente, exponen a la institución a riesgos de integridad, disponibilidad y confidencialidad de la información.

- Mantener una hoja de ruta que considere un listado de funciones básicas, metodologías y mejores prácticas como resultado de la definición de criticidad de su infraestructura.
- Desarrollar e implementar los resguardos necesarios para proteger la infraestructura definida como crítica. El Área de Informática debe establecer las medidas de seguridad adecuadas para prever, detectar y gestionar oportunamente los eventos e incidencias que puedan afectar la Ciberseguridad de la infraestructura crítica.
- Revisar regularmente las políticas y procedimientos para prever la adopción oportuna de medidas ante escenarios de amenazas de Ciberseguridad.
- Disponer de planes de recuperación de operaciones o procesos críticos, en forma oportuna y eficiente.
- Promover una cultura de riesgos en materia de Ciberseguridad, a través de procesos formales de difusión, capacitación y concientización de todos los funcionarios y del personal de empresas externas que interactúan con la información de la institución.

Base de Incidentes de Ciberseguridad

Condiciones mínimas para el desarrollo y mantención de una Base de Incidentes

A continuación, se detalla algunos elementos que permitirían identificar, registrar, evaluar, controlar, mitigar, monitorear y reportar incidentes operacionales relacionados con la Ciberseguridad:

- Mantener una base de incidentes de Ciberseguridad donde se registren los eventos no planificados por la institución, que ponen en riesgo la seguridad de los activos de información presentes en el ciberespacio e identificando de manera individual cada uno de estos incidentes.
- Gestionar los incidentes de Ciberseguridad, con el fin de detectar, investigar y generar acciones de mitigación del impacto de estos eventos, resguardando la confidencialidad, disponibilidad e integridad de sus activos de información.
- El Área de Informática debe reportar al Comité de Seguridad y al Oficial de Seguridad los incidentes acontecidos al menos una vez al año, con el fin de mejorar su gestión y prevención.
- Poner a disposición de las autoridades de la Superintendencia y de Auditoría Interna la base completa de incidentes.
- Realizar regularmente pruebas para detectar las amenazas y vulnerabilidades que pudieran existir en la infraestructura crítica de Ciberseguridad, que permitan evaluar su nivel de exposición y riesgo en plataformas web, redes y sistemas (pentesting) y/o jaqueo ético para evidenciar los niveles de vulnerabilidad de la institución.

Variables mínimas que debe contener la Base de Incidentes de Ciberseguridad

- Identificación única del incidente.
- Fecha y hora de inicio del incidente.
- Fecha y hora en la que el incidente es detectado.
- Tipo de amenaza o vulnerabilidad del incidente que coloca en riesgo a los activos de información virtuales, de acuerdo a la clasificación presentada a continuación:
    - Falla producida en la estructura física que soporta el activo de información.
    - Falla en los accesos producto de una inadecuada definición, control o vulneración.
    - Acción de fuerzas de la naturaleza como incendios, terremotos, tormentas electromagnéticas, entre otros.
    - Terrorismo.
    - Fallas en los procesos, definición, control o vulneración.
    - Falla en los proveedores.
    - Inadecuada arquitectura tecnológica, definición, control o vulneración.
    - Prácticas inadecuadas de los usuarios internos de la organización.
    - Prácticas inadecuadas de los usuarios externos de la organización.
    - Falla en las redes de comunicaciones.

- Fuente de la amenaza o vulnerabilidad, estableciendo si se trata de una causa externa o interna de la organización.
- Descripción del incidente que permita entender las causas especificando el tipo de ataque (ciberespionaje, phishing, malware, denegación de servicio, entre otros) y especifique el tipo de amenaza o vulnerabilidad que lo produce.
- Activos involucrados, distinguiendo aquellos efectivamente vulnerados de los potencialmente en riesgo.
- Tipo de productos o servicios involucrados cuando corresponda aquellos productos o servicios prestados por la institución que fueron afectados por el incidente, ya sea en su disponibilidad o funcionamiento.
- Número de usuarios afectados cuando corresponda.
- Identificación de los proveedores cuando corresponda.
- Tiempo de resolución del incidente, medido en horas y minutos.
- Costos de incidentes, entendidos como el valor de las pérdidas potenciales o reales.
- Costos de mitigación y reparación asociados al incidente, sea que este se haya o no materializado.
- Descripción de las acciones realizadas y áreas responsables de su implementación, cuando corresponda.
- Estado del incidente, indicando para cada evento si los planes de acción para su corrección definitiva se encuentran implementados.
- Fecha y hora de Cierre del incidente

Norma N° 16: Gestión de Incidentes de Seguridad de la Información

La Superintendencia de Salud, a través de su Comité de Seguridad de la Información, establece la Norma de Gestión de Incidentes de Seguridad, orientada a la mitigación y corrección de vulnerabilidades y amenazas que pudieran afectar la seguridad de la información institucional, gubernamental o la continuidad operacional de los servicios estratégicos del País.

Objetivos

- Establecer responsabilidades de las distintas Unidades con relación a la seguridad de los datos institucionales (integridad, disponibilidad y confidencialidad), ya sea se encuentren en la plataforma informática como en su manipulación a cargo de los funcionarios en general.
- Responder en forma rápida, eficaz y ordenada ante la ocurrencia de incidentes de seguridad que afecten los activos de información institucionales.
- Asegurar un enfoque consistente y eficaz sobre la gestión de los incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

Responsables del cumplimiento

Todo el personal de la Superintendencia y terceros que interactúan de manera habitual u ocasional con los sistemas de información y que accedan a información sensible y/o a los recursos informáticos en el desarrollo de sus tareas habituales.

Disposiciones de la norma

Responsabilidades

En general, el área de seguridad de la información adoptará un rol activo como responsable técnico de establecer procedimientos ante el Comité, que permitan garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad relacionados con la plataforma tecnológica. Por otra parte, las Unidades dueñas de los datos a que pertenecen los usuarios de los sistemas, son responsables del manejo que den a los datos institucionales, lo que deberá ser supervisado por las jefaturas correspondientes.

Unidades responsables

Las siguientes Unidades deberán establecer directrices respecto a sus competencias en relación con la protección de los datos y garantizar la continuidad operativa de los servicios prestados por el Ministerio del Interior, con la debida difusión y control de cumplimiento a cargo de las respectivas jefaturas.

- Encargado de Ciberseguridad: De acuerdo al Instructivo Presidencial N°8 publicado con fecha 23 de octubre de 2018, será responsable de la seguridad informática de su servicio y velar por las medidas de seguridad establecidas en dicho instructivo.
- Unidad de Tecnologías de Información: En lo que se refiere a la plataforma tecnológica, comprendiendo a sus unidades internas.
- Unidades Dueñas de los datos: En lo que se refiere al uso, manipulación y protección de acceso a datos institucionales de modo de garantizar su integridad, disponibilidad y confidencialidad.
- Departamento de Administración y Finanzas: Para resguardar y dar seguridad a las zonas de trabajo, de accesos no autorizados y protección ambientales de seguridad.
- Funcionarios: En lo que se refiere al uso, manipulación y protección de acceso a datos institucionales de modo de garantizar su integridad, disponibilidad y confidencialidad, asociados a los procesos y sistemas institucionales.

Informe de las debilidades de la seguridad de la información

Se exigirá a todos los funcionarios y contratistas, que utilizan los sistemas y servicios de información de la organización, informar sobre cualquier debilidad de seguridad de la información de los sistemas o servicios. Esta función es importante para la institución, pues en la medida que los funcionarios están alertas a estos detalles se maximiza la vigilancia y resguardo de los activos institucionales.

En este sentido todos los funcionarios deberán siempre estar alertas tanto a los temas de respeto a las políticas de seguridad de la información como a señales que

parezcan extrañas o poco habituales, teniendo en consideración que cada uno de ellos puede ser blanco u objetivo de un ataque cibernético mediante el cual se puede acceder a información personal o institucional relevante, entre la que destaca en primera instancia:

- Credenciales o contraseñas.
- Direcciones de correo electrónico.
- Perfiles de usuario o gustos personales de compras y/o navegación web.
- Información confidencial (documentos sensibles institucionales, tarjetas de crédito, entre otros).
- Recursos del sistema (CPU, RAM y disco duro), para almacenar malware o utilizar equipos institucionales sin autorización.

Canalización de incidentes de Ciberseguridad

- Los funcionarios deberán reportar sus dudas, alertas o fallas de seguridad al Oficial de Seguridad que determinará el tipo de incidente y su escalamiento en caso que se determine que corresponde a un incidente mayor.
- De igual forma la Unidad de Tecnologías de Información debe reportar al Oficial de Seguridad las anomalías de seguridad que se detecten en el funcionamiento de la red, servidores, estaciones de trabajo u otras que afecten los activos de información.
- Por su parte el Oficial de Seguridad, que también es el Encargado de Ciberseguridad, canalizará los incidentes de Ciberseguridad a la Plataforma CSIRT Gubernamental a través de los mecanismos dispuestos por esta entidad. En este caso, el Encargado de Ciberseguridad deberá mantener informado de la evolución de estos incidentes al Comité de Seguridad de la Información y, se determina, a todos los funcionarios de la Institución.

Norma N° 17: Transferencia de Archivos

Objetivo

Establecer mecanismos de transferencia de archivos electrónicos de manera segura, con la finalidad de resguardar su contenido evitando que terceros puedan acceder total o parcialmente a sus datos.

Responsables del cumplimiento

Todo el personal de la institución y terceros que interactúan de manera habitual u ocasional, que envíen o reciban archivos con información sensible y/o reservada.

Incumplimientos

Las medidas disciplinarias están descritas en el Anexo de Sanciones por incumplimientos que forma parte del conjunto de medidas disciplinarias de la Superintendencia.

Registros de Control

La Unidad de Tecnologías de la Información en conjunto con la Unidad de Generación de Estadísticas y Datos son responsables de construir los procedimientos de transferencia de archivos con información sensible y/o reservada identificando los responsables de envío y recepción de cada transacción que se realice. Además, deberán llevar un registro de las transacciones realizadas por quienes envían y/o reciben archivos de datos.

Disposiciones de la Norma

En norma de la institución:

Mecanismos de transferencia de archivos

- La transferencia o recepción de archivos de datos con información sensible y/o reservada debe ser realizada exclusivamente desde una plataforma tecnológica segura. Para estos efectos la Unidad de Tecnologías de Información proveerá los sistemas o herramientas computacionales que garanticen transferencias seguras.
- No está permitido realizar transferencia o recepción de archivos con información sensible y/o reservada a través de correo electrónico institucional o personal, así como cualquier otro mecanismo que permita su recepción o envío.
- No está permitido usar espacios virtuales de almacenamiento, ofrecidos por empresas de tecnología, para guardar, recibir o enviar archivos con información sensible y/o reservada.
- En caso de falla de los medios tecnológicos de recepción o envío de archivos provistos por la Superintendencia, la Unidad de Tecnologías de Información deberá indicar la forma de proceder para operar frente a situaciones de emergencia.

Responsabilidades y recomendaciones

- Frente a un envío de información sensible y/o reservada desde una entidad externa a través de medios prohibidos, los funcionarios y funcionarias deberán responder que no se da por recibida dicha información y orientar la forma en que se debe realizar.
- Los correos electrónicos que lleguen a casillas electrónicas institucionales o personales con información sensible, deben ser borrados de las casillas de recepción además de notificar al Subdpto de Tecnologías de Información, la Unidad de Gestión de Datos y Estadísticas como se señala en el punto anterior.

Norma N° 18: Anexo Sanciones por incumplimiento

Objetivos

Establecer las responsabilidades y atribuciones que tienen las funcionarias y funcionarios en el acceso y uso de la información atendidas las responsabilidades de su cargo.

Establecer las sanciones infracciones y violaciones de las obligaciones establecidas por leyes, estatutos, reglamentos y contratos y de los efectos u incidentes significativos que conlleva infringir la Política de Seguridad de la Información.

El incumplimiento por parte de los usuarios de las instrucciones contempladas en la presente norma, parte integrante de la Política de Seguridad de la Información, quedará sujeto a los precedentes contemplados en el Estatuto Administrativo para investigar y sancionar las posibles responsabilidades, incluyendo el Código del Trabajo, Contrato de Trabajo a honorarios y las leyes que rigen la gestión de los Servicios Públicos.

Responsables del cumplimiento

Todo el personal de la Superintendencia y terceros que interactúan de manera habitual u ocasional con los sistemas de información y que accedan a información sensible y/o a los recursos informáticos en el desarrollo de sus tareas habituales.

Generalidades

La Superintendencia de Salud considera que la seguridad de la información es responsabilidad de todos los miembros de su equipo. Cada persona que maneja información o utiliza los sistemas de información de la Superintendencia de Salud debe conocer las políticas y procedimientos de seguridad de la misma, para dar cumplimiento estricto a los resguardos allí contemplados.

Las normas específicas y sus procedimientos para cada uno de los ámbitos de la seguridad de la información se realizan a partir del Comité de Seguridad de la Superintendencia de Salud en documentos que hacen operativa la presente política.

Disposiciones de la norma

Realizar un procedimiento de selección adecuado que permite una verificación de antecedentes de los candidatos de acuerdo a los requerimientos y necesidades institucionales, selección que se encuentra acorde con las leyes, regulaciones y normas éticas relevantes y en proporción a los requisitos del negocio[83].

Realizar las actividades destinadas a asegurar la preservación de la confidencialidad, integridad y disponibilidad de la información, las que se planificarán y ejecutarán a partir del diagnóstico de la situación de la Institución en cada uno de sus procesos y de la evaluación de los riesgos asociados a seguridad de la información, los que serán priorizados en función de su severidad y probabilidad[84]. La efectividad de estas actividades deberá ser controlada por los encargados de cada proceso y ejecutada por cada uno de los funcionarios y funcionarias a fin de verificar que se cumplan los requerimientos de seguridad de la información.

A fin de resguardar la calidad en la implementación de las medidas de seguridad comprendidas en la política, la Superintendencia de Salud determinará los conocimientos necesarios para las personas que cumplan funciones que afectan a la seguridad de la información y proporcionará la capacitación y/o acciones pertinentes para alcanzar o mantener los niveles adecuados de conocimientos y competencias[85].

El incumplimiento de la política de seguridad de la información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y características del aspecto no cumplido. Tales sanciones, se encuentran establecidas en el Estatuto Administrativo, en el DFL 29/2004 y en las leyes que rigen la gestión de los Servicios Públicos.

Toda infracción que se denuncie dando origen a una investigación sumaria o a un sumario administrativo, se realizará conforme a la ***"Guía Práctica para Tramitación de Sumario Administrativo e Investigación Sumaria"***, conforme a la Ley N° 18.834, sobre Estatuto Administrativo, a fin de determinar las responsabilidades

[83] ISO 27002:2013 A.7.1.1
[84] ISO 27002:2013 A.7.2.1
[85] ISO 27002:2013 A.7.2.2

asociadas y se aplicarán las medidas de sanciones disciplinarias que de tal proceso se determinen[86].

La categorización de las faltas relacionadas con seguridad de la información, dependerá de la consecuencia del proceso investigativo llevado a cabo, la que puede implicar una anotación de demérito, censura, multa o destitución, o suspensión privada o total del empleo.

Todas las funcionarias y funcionarios deben suscribir un documento expreso a modo de compromiso, denominado ***"Obligaciones y Responsabilidades en el resguardo en la Disponibilidad y Seguridad de la Información"***, el cual es firmado al momento de ingresar a la Institución, con el fin de tomar conocimiento de las atribuciones y obligaciones que en atención a su cargo le serán concedidas, formato que será parte integrante del Manual de Higiene y Seguridad y del proceso de inducción y que está referido a:

- Protección, uso correcto y resguardo del equipamiento tecnológico puesto a su disposición (programas, hardware, software), como también aquellos de su entorno (impresoras, escáner, CD, DVDs, pendrives, etc.)[87].
- Resguardar y proteger la información que por las condiciones y atribuciones de su cargo tiene acceso, correspondiente al manejo de datos, sistemas y procesos informáticos.
- Resguardar las claves de acceso atendiendo su carácter de personal e intransferible debiendo actuar conforme a las instrucciones emanadas de la Política de Seguridad de la Información
- Manejo de los equipos informáticos asignados de acuerdo a la disposición que la Institución determine.
- Denunciar toda irregularidad que el funcionario(a) observe o tome conocimiento respecto al resguardo y seguridad de la información.
- Las referencias anteriores deben ser de cumplimiento permanente en cualquier cargo y/o puesto de trabajo que el funcionario este sirviendo en la institución.
- Ante una situación de cese de funciones, la institución seguirá el procedimiento correspondiente para la recepción de todos los activos asignados y/o de responsabilidad del funcionario que se desvincula[88].

[86] ISO 27002:2013 A.7.2.3
[87] ISO 27002:2013 A.7.1.2
[88] ISO 27002:2013 A.7.1.2

2. **Difúndanse** los contenidos de la Política de Seguridad 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° 537 del 31 de julio de 2019, que aprobó la anterior Política de Seguridad Institucional de la Información.

ANÓTESE, COMUNÍQUESE Y PUBLÍQUESE EN EL PORTAL WEB

PATRICIO FERNÁNDEZ PÉREZ
SUPERINTENDENTE DE SALUD

CVA/CMB/SAQ/MJC/RSC/EHD/LRG/RCL/RDM/TNA

Distribución

- Superintendente
- Fiscalía
- Intendencias
- Agencias Regionales
- Departamentos y Unidades
- Oficina de Partes