Política General de Seguridad de la Información

COMISIÓN NACIONAL DE INVESTIGACIÓN CIENTÍFICA Y TECNOLÓGICA

Documento PO-PRE-27000-2011-001

Información del Documento

HISTORIA DEL DOCUMENTO			
Nombre del Documento	Política General de Seguridad de la Información		
Preparado por	Marcelo Iribarren – Carmen Gorroño – Elena Hernández		
Responsable del Documento	Elena Hernández	Fecha de Creación	29/06/2011
Aprobado por	Comité de Seguridad de la Información	Fecha de Aprobación	

CONTROL DE VERSIONES			
Versión	Fecha de Creación	Preparada por	Descripción
1.0	31-Mar-2011	E. Hernandez	Creación y primera versión del documento.
1.1	17-Jun-2011	M. Iribarren	Revisión crítica de la 1ra versión. Todas las secciones.
1.2	21-Jun-2011	Carmen Gorroño	Cambio de dominios de la seguridad según la norma ISO 27001.
2.0	21-Jun-2011	M. Iribarren: E. Hernandez	Cambio de formato a SANS-compatible. Inclusión de secciones faltantes. Cambio de la sección 4.0 a nueva política de organización de la seguridad (*).
2.1	07/07/2011	Paula Arismendi y Elena Hernández	Responsable del Dcto.
2.1	14/07/2011	Comité Operativo	Revisión final y aprobación por el Comité Operativo

(*) La presente versión substituye completamente a todas las precedentes, de manera que éste sea el único documento válido de entre todos los de la serie.

Tabla de Contenido

1. Introducción

La Comisión Nacional de Ciencia y Tecnología (CONICYT), creado en 1967 como organismo asesor de la Presidencia de la República, es un servicio público descentralizado con personalidad jurídica y patrimonio propio, que se relaciona con el poder ejecutivo a través del Ministerio de Educación.

CONICYT tiene por objeto asesorar a la Presidencia de la República en materias de desarrollo científico y está orientada por dos pilares estratégicos: el fomento de la formación de capital humano y el fortalecimiento de la base científica y tecnológica del país.

Como tal, CONICYT reconoce la importancia y el valor de la información con respecto al funcionamiento eficiente y efectivo de la organización. La información no es sólo crítica para el éxito de la organización, sino estratégica para su supervivencia a largo plazo.

Por esta razón, se establece la siguiente política que regula el manejo de la información en CONICYT, orientada a definir las medidas que resguarden la confidencialidad, integridad y disponibilidad de la información propia de la organización, el acceso a la información en conformidad con la constitución, las leyes, y demás normas jurídicas, así como asegurar la continuidad de los servicios que le son propios.

Es por ello que la Dirección 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 para todos los activos de información institucional considerados relevantes, de manera tal 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, el entorno y las tecnologías.

Es imprescindible contar con un marco general en el cual encuadrar todos los subprocesos asociados a la Gestión de la Seguridad, comenzando por definir sus objetivos, el alcance o amplitud, los roles y responsabilidades y el marco general para elaboración y revisión de las políticas de seguridad específicas para la información de CONICYT.

Esta política general, las políticas específicas y procedimientos de seguridad asociados utilizarán como marco de referencia los requerimientos del D.S. N° 83/2004, del Ministerio Secretaría General de la Presidencia (Seguridad y Confiabilidad de documentos electrónicos) y las buenas prácticas definidas en la norma ISO 27001-2005, la que adicionalmente deberá constituir el marco rector de todas las iniciativas de seguridad adoptadas por CONICYT.

2. Objetivos

Esta política general de seguridad de la información cubre los siguientes objetivos:

- Establecer las expectativas de la Dirección con respecto al correcto uso que el personal haga de los recursos de información de CONICYT, así como de las medidas que se deben adoptar para la protección de los mismos.
- Establecer para todo el personal de la organización la necesidad de la seguridad de la información y promover la comprensión de sus responsabilidades individuales.
- Determinar las medidas esenciales de seguridad de la información que CONICYT debe adoptar, para protegerse apropiadamente contra amenazas que podrían afectar en alguna medida 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 estratégico y coordinador de las políticas de fomento del desarrollo científico y tecnológico del país.
    - Interrupción total o parcial de los procesos que soportan el negocio.
- Proporcionar a todo el personal de CONICYT una herramienta que facilite la toma de decisiones apropiada, en situaciones relacionadas con la preservación de la seguridad de la información.

Para cumplir con estos objetivos el SGSI se basa en la identificación de los activos de información involucrados en los procesos de negocios y en los procesos de soporte de la institución, lo cual implica llevar a cabo junto a los responsables de los diferentes procesos de negocio de la institución las siguientes actividades esenciales:

1 Identificar, para todos los procesos de negocio, los activos de información involucrados, catalogados como información física, información digital, personas e infraestructura, clasificándolos según lo establezca la ley de información sensible.

2 Para cada activo de información identificar un responsable que vele por su disponibilidad, confidencialidad e integridad.

3 Analizar el riesgo al cual están expuestos, con la ayuda de la metodología CAIGG y el encargado de riesgos.

4 Difundir en forma planificada entre todo el personal de la institución el objetivo corporativo de preservación de la información, sus características y las responsabilidades individuales para lograrlo, inserto esto en los planes de capacitación anual de la institución como actividades permanentes y en el proceso de inducción del nuevo personal.

3. Alcance

Esta política se aplica a todo el personal de CONICYT, planta, contrata y honorarios, y también al personal externo que preste o prestare servicios, remunerados o no, a CONICYT ya sean integrantes de las diferentes comisiones o comités que tienen acceso privilegiado a la información.

También es aplicable a 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.

La política cubre toda la información, entre otros, la impresa o escrita en papel, almacenada electrónicamente, trasmitida por correo o usando medios electrónicos, mostrada en películas o hablada en una conversación.

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 a todos los procesos de negocio de la organización, iniciándose con los procesos propios del Programa FONDECYT y avanzando paulatinamente a las otras unidades de negocio de la institución.

Así también, como apoyo a esta política general, cada dominio especificado por el estándar ISO 27001 tendrá una política específica, que complementará la presente y normará las particularidades de cada dominio.

Cada Política deberá contar con procedimientos asociados, mecanismos de control y sanciones asociadas al no cumplimiento.

4. Definiciones

Información: la información es la interpretación que se da a un conjunto de datos, pudiendo residir esta en medios electromagnéticos, físicos o en el conocimiento de las personas. En el caso de la presente política, se entenderá como información a toda forma proveniente de datos relacionados con los procesos de negocio de la Comisión Nacional de Investigación Científica y Tecnológica, así como antecedentes proporcionados tanto por los usuarios internos como los externos, siempre que sea dentro del contexto del ejercicio de sus funciones y del cumplimiento de sus obligaciones.

Información Pública: toda aquella información no catalogada como secreta o reservada, tal como lo establece el ordenamiento jurídico vigente.

Información reservada (conocimiento reservado) : son aquellos documentos cuyo conocimiento está circunscrito al ámbito de la respectiva unidad del órgano a que sean remitidos, en virtud de una ley o de una norma administrativa dictada en conformidad a ella, que les confiere tal carácter, cuando la naturaleza misma de la información requiera ser tratada de manera reservada.

La información secreta (solamente a quien le atañe la información debe conocerlo): son aquellos documentos cuyo conocimiento está circunscrito a las autoridades o personas a las que vayan dirigidos y a quienes deban intervenir en su estudio y resolución, en virtud de una ley o de una norma administrativa dictada en conformidad a ella, que les confiere tal carácter. Una norma que establece restricciones claras es la ley de datos personales.

Seguridad de la Información: es el nivel de confianza que la organización desea tener de su capacidad para preservar la confidencialidad, integridad y disponibilidad de la información. Tiene como objetivo proteger el recurso información de una amplia gama de amenazas, con el fin de asegurar la continuidad del negocio, minimizar el daño y, cumplir su misión y objetivos estratégicos.

Confidencialidad: es asegurar que la información es accesible sólo para las personas autorizadas para ello.

Integridad: es salvaguardar la exactitud y totalidad de la información en su procesamiento, transmisión y almacenamiento.

Disponibilidad: es asegurar que los usuarios autorizados tengan acceso a la información y los activos asociados cuando estos sean requeridos.

Buen uso: se entiende por “buen uso” de los activos de información de la organización, a las expectativas que CONICYT tiene con respecto al cuidado que su personal debe tener con los activos que la organización les entregue para el desempeño de sus funciones.

Personal: es toda persona a la cual se le concede autorización para acceder a la información y a los sistemas de CONICYT. El personal puede ser interno o externo a la organización.

Supervisor: es toda persona encargada de un grupo de personas, área, división, programa o departamento en CONICYT.

Tercero: se refiere a empresas prestadoras de servicios, las empresas contratistas, sub-contratistas y cualquiera que, por cuenta propia o de terceros, desarrolle trabajos para o por cuenta de CONICYT.

Responsable de la Información: es el usuario a cargo de la información y de los procesos que la manipulan sean estos manuales, mecánicos o electrónicos.

Encargado de Seguridad: es la persona que la autoridad máxima del servicio designa para la definición, diseño, implementación y supervisión de las medidas de seguridad de la información.

Comité de Seguridad: es el equipo conformado por supervisores que representan a las áreas de la organización, responsable de la toma de decisiones en temas de la seguridad de la información.

Activo de Información: Todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución.

Podemos distinguir 3 tipos de activos:

a) La Información propiamente tal, en sus múltiples formatos (papel o digital, texto, imagen, audio, video, etc.).

b) Los Equipos/Sistemas que la soportan.

c) Las Personas que la utilizan.

Los activos poseen valor para la organización, y necesitan por tanto ser protegidos adecuadamente, para que el "negocio" no se vea perjudicado (implica detectar vulnerabilidades y establecer controles).

5. Responsabilidades y Cumplimiento

5.1. Responsabilidades

Director(a) Ejecutivo de CONICYT: en su calidad de tal, responde ante el Presidente de la Comisión por la existencia y cumplimiento de las medidas que mantengan un nivel de seguridad de la información acorde con el rol de la organización y los recursos disponibles.

Encargado de Seguridad: es el principal responsable en la definición de los criterios de seguridad de la información en CONICYT, para lo cual deberá analizar periódicamente el nivel de riesgo existente, proponiendo soluciones. Una vez autorizada la implementación de las medidas, deberá coordinar con quienes corresponda su materialización oportuna y correcta.

Comité de Seguridad: tiene por responsabilidad asesorar al Director(a) Ejecutivo de CONICYT, en temas de seguridad de la información, en coordinación con el Encargado de Seguridad.

Responsable del Documento: tiene que mantener la aplicabilidad de este documento acorde a las prácticas operacionales de CONICYT, por lo que es responsable de generar las modificaciones necesarias para que esté siempre actualizado. Además es responsable de publicar y dar a conocer nuevas versiones del documento.

Personal de CONICYT: tiene la responsabilidad de cumplir con lo formalizado en este documento y aplicarlo en su entorno laboral. Además, tiene la obligación de alertar de manera oportuna y adecuada, según lo determine la política de manejo de incidentes, cualquier incidente que atente contra la seguridad de la información.

5.2. Cumplimiento

La presente Política General de Seguridad de la Información entra en vigencia una vez oficializada por el o la Directora(a) Ejecutivo (a) de CONICYT y, las jefaturas de los distintos Programas, Departamentos y Unidades de CONICYT serán responsables de ponerlas en conocimiento de su personal subordinado.

Para el caso del personal que se contrate con posterioridad a la fecha de publicación, se le deberá entregar una copia del presente documento y hacer firmar una declaración de toma de conocimiento y aceptación de la misma.

La presente política está alineada con las directrices de las leyes y regulaciones existentes. Cualquier conflicto con estas regulaciones debe ser informado inmediatamente al responsable de este documento.

6. Política

6.1. De la Información Interna

- La información es un activo vital y todos sus accesos, usos y procesamiento, deberán ser consistentes con las políticas y estándares emitidos por CONICYT en cada ámbito en particular.
- 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 en las recomendaciones dadas por el responsable designado de dicha información. Para ello, la Dirección de CONICYT deberá proveer los recursos que permitan implementar los controles necesarios para otorgar el nivel de protección correspondiente al valor de los activos.
- 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.
- CONICYT proveerá los mecanismos para que la información sea accedida y utilizada por el personal que de acuerdo a sus funciones así lo requiera. Sin embargo, se reserva el derecho de revocar al personal, el privilegio de acceso a la información y tecnologías que la soportan, si la situación y las condiciones lo ameriten.

6.2. De la Información de los Usuarios Externos

- Si la institución procesa y mantiene información de usuarios externos que sean datos personales y/o sensibles de acuerdo a la normativa vigente , la organización se compromete a asegurar que esta información no será divulgada sin previa autorización y estará protegida de igual manera que la información interna.
- En el caso que la información de usuarios externos que se procese y mantenga y que no tenga las características anteriormente mencionadas, esta podrá ser divulgada sin previa autorización.

- Si se requiere compartir información de los usuarios externos de CONICYT con instituciones externas, con motivo de externalizar servicios, a éstas se le exigirá la firma de un contrato de confidencialidad y no divulgación previo a la entrega de la información.

6.3. De las Auditorías

- Con el fin de velar por el correcto uso de los activos de información de su propiedad, CONICYT se reserva el derecho de auditar en todo momento y sin previo aviso, el cumplimiento de las políticas vigentes y que dicen relación con el acceso y uso que los usuarios hacen de los activos de información.
- CONICYT se reserva el derecho de tomar medidas administrativas en contra del personal que no dé cumplimiento a lo dispuesto en la presente política, las políticas específicas que se deriven y en su documentación de referencia, acciones que pueden ser solicitadas por el responsable de Recursos Humanos o el Encargado de Seguridad.

6.4. Del Compromiso de la Dirección del Servicio

- La Dirección del Servicio velará por la existencia de un plan formal de difusión de está política y las políticas específicas que la sustenten.
- La Dirección del Servicio, mediante la estructura que se defina en la política específica “Aspectos Organizativos de la Seguridad de la Información”, procurará que todo el personal reciba un entrenamiento suficiente en materia de seguridad, consistente con sus necesidades y su rol dentro de CONICYT.
- 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.

6.5. Deberes del Personal

- La información y las tecnologías de información deben ser usadas sólo para propósitos relacionados con el servicio y autorizados por los supervisores, debiéndose aplicar criterios de buen uso en su utilización.
- Las claves de acceso a la información y a las tecnologías de información son individuales, intransferibles y de responsabilidad única de su propietario.
- 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.
- Está absolutamente prohibido al personal de la organización divulgar cualquier información que según el ordenamiento jurídico esté catalogada como “Reservada” o “Secreta”, Organización y Mantención de las Políticas

Con el objetivo de garantizar el cumplimiento de la Política General de Seguridad de la Información y las políticas específicas que se definan posteriormente, CONICYT ha establecido una estructura organizacional de seguridad que contempla la definición de

funciones específicas en el ámbito de seguridad, las cuales serán ejecutadas por un Comité de Seguridad y un Responsable de Seguridad.

Las características de esta instancia organizacional y roles se detallan en el documento Política Específica - Aspectos Organizativos de la Seguridad de la Información.

6.6. Difusión de la Política

Resulta clave para que la presente política se integre en la cultura organizacional, la existencia de un plan formal de difusión, capacitación y sensibilización en torno a la seguridad de la información.

El Director Ejecutivo de CONICYT será el responsable de la existencia permanente y el cumplimiento de un plan formal de difusión, capacitación y sensibilización de la seguridad de la información.

El Encargado de Seguridad de la información es el responsable de la ejecución del plan y el cumplimiento de sus objetivos, así como la existencia de un plan comunicacional que lo complemente.

7. Formato y Mantención de las Políticas

7.1. Formato de las Políticas

Toda política debe contener las siguientes secciones:

1. Introducción
2. Propósito
3. Alcance
4. Definiciones
5. La política en si
6. Aplicación de la política y responsabilidades
7. Historial de revisión

Asociada a cada política se deben emitir los mecanismos de control y las sanciones cuando se viola la política respectiva.

7.2. Mantención de la Política

- La mantención de la presente política será realizada por el Encargado de Seguridad de la Información y sus cambios aprobados por el Comité de Seguridad de la Información y el o la Directora(a) Ejecutivo(a) de CONICYT.
- Las políticas específicas asociadas a la presente política general deberán ser aprobadas por el Comité de Seguridad y firmadas por el o la Directora(a) Ejecutivo (a) de CONICYT. Los procedimientos asociados serán aprobados por el el Director Ejecutivo mediante resolución exenta.
- El presente documento debe ser revisado a lo menos 1 vez al año y actualizado cada vez que se realicen cambios relevantes en CONICYT 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.
- El Comité Operativo de Seguridad solicitará al área de comunicaciones interna que difunda la política dependiendo del alcance de la misma y su importancia para el negocio.

7.3. Documentación de Referencia

El presente documento constituye una política de alto nivel, destinada a normar los aspectos más relevantes de la gestión de seguridad de la información, con una vigencia de largo plazo, por lo cual la Dirección promulgará documentos adicionales que explicitan en mayor detalle las medidas de seguridad de alto nivel dispuestas en el presente documento.

Dichos documentos deberían estar asociados a los dominios definidos en la ISO/IEC 27001-2005, los cuales son:

- Organización de la Seguridad de la Información.
- Gestión de Activos.
- Seguridad de los Recursos Humanos.
- Seguridad Física y del Ambiente.
- Gestión de las Operaciones y de las Comunicaciones.
- Control de Acceso.
- Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
- Gestión de Incidentes de la Seguridad de la Información.
- Gestión de Continuidad de Negocios.
- Cumplimiento.

***** Fin del Documento *****