579

Ministerio de Educación, Ciencia y Tecnología
Secretaría de Ciencia, Tecnología e Innovación Productiva
Consejo Nacional de Investigaciones Científicas y Técnicas

BUENOS AIRES, 23 MAR 2007

VISTO el Expediente N° 4330/06 del Registro de este Consejo Nacional, y

CONSIDERANDO:

Que la Decisión Administrativa de la Jefatura de Gabinete de Ministros N° 669/2004 establece que se debe dictar o bien adecuar las políticas de seguridad de la información conforme a la Política de Seguridad Modelo.

Que se debe conformar un Comité de Seguridad de la Información integrado por representantes de las Direcciones Nacionales o Generales o equivalentes del Organismo, designado por sus máximas autoridades.

Que la Oficina Nacional de Tecnología de Información aprobó el Modelo de Política de Seguridad de la Información para Organismos de la Administración Pública Nacional en su Disposición 6/2005.

Que el objetivo de las Políticas de Seguridad de la Información es proteger los recursos de información del Organismo y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Que es necesario establecer las Políticas de Seguridad de la Información del Organismo.

Ministerio de Educación, Ciencia y Tecnología
Secretaría de Ciencia, Tecnología e Innovación Productiva
Consejo Nacional de Investigaciones Científicas y Técnicas

Que es necesario conformar el Comité de Seguridad de la Información y designar al Responsable de Seguridad de la Información.

Que la Dirección de Asuntos Jurídicos y la Asesoría Legal han tomado la intervención correspondiente.

Que la presente medida fue acordada en la reunión de Directorio de fecha 13 y 14 de marzo de 2007.

Que el dictado de la presente se realiza en uso de las atribuciones conferidas por los Decretos N° 1661/96, N° 1256/03, N° 563/04 y N° 1427/05 y R.D. N° 346/02 y N° 671/04.

Por ello,

EL DIRECTORIO DEL
CONSEJO NACIONAL DE INVESTIGACIONES CIENTIFICAS Y TECNICAS
RESUELVE:

ARTICULO 1°.- Apruébanse las Políticas de Seguridad de la Información que obran en el Anexo I, las que serán de cumplimiento obligatorio en el ámbito de este Consejo Nacional.

ARTICULO 2°.- Desígnanse los integrantes del Comité de Seguridad de la Información y al Responsable de Seguridad de la Información según la nómina que figura en el Anexo II.

ARTICULO 3°.- Regístrese, comuníquese a las Gerencias de Desarrollo Científico y Tecnológico, de Gestión Operativa, de Evaluación y Acreditación, a la Asesoría Legal y a la Unidad de Auditoría Interna, cumplido archívese.

RESOLUCION D N° 579

Dr. EDUARDO H. CHARREAU
PRESIDENTE
CONICET

Ministerio de Educación, Ciencia y Tecnología
Secretaría de Ciencia, Tecnología e Innovación Productiva
Consejo Nacional de Investigaciones Científicas y Técnicas

ANEXO I

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. OBJETIVOS GENERALES

La información utilizada en la generación de la producción científico tecnológica, el control de gestión y el desarrollo de la actividad administrativa es considerada como activo intangible de valor. El Directorio fija como objetivos en relación a la misma:

1.- Mejorar su calidad, a fin de que sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones del Organismo.

2.- Utilizarla dentro de un adecuado entorno de seguridad.

En relación con los objetivos enunciados se especifican:

a.- El alcance (punto 2).

b.- Las pautas o principios generales vinculados con la calidad de la información (punto 3).

c.- Las pautas o principios generales vinculados con la seguridad de la información (punto 4).

d.- La forma cómo se organizará la seguridad de la información (punto 5).

2. ALCANCE

2.1 La información utilizada en el CONICET cualquiera sea su representación, ubicación, medio empleado para soportarla y plataforma utilizada para procesarla deberá ser confiable. Debe ser convenientemente protegida de acuerdo a su nivel de sensibilidad y criticidad a fin de garantizar su confidencialidad, integridad y disponibilidad, como así también su autenticidad, auditabilidad y legalidad. Se impedirá su duplicación no autorizada y se evitará el repudio de su autoría.

2.2 Esta Política debe ser conocida y cumplida por todos los agentes del Organismo, tanto se trate de funcionarios políticos como técnicos, miembros de las carreras del personal científico y tecnológico, becarios, administrativos y resto del personal sea cual fuere su nivel jerárquico, su situación y sede de revista, así como por cualquier otra persona o institución que acceda a información del CONICET.

Ministerio de Educación, Ciencia y Tecnología
Secretaría de Ciencia, Tecnología e Innovación Productiva
Consejo Nacional de Investigaciones Científicas y Técnicas

3.- PAUTAS O PRINCIPIOS GENERALES VINCULADOS CON LA CALIDAD DE LA INFORMACIÓN

La información disponible en el Organismo debe permitir a sus agentes cumplir con sus obligaciones y responsabilidades. Procedimientos y metodologías de trabajo adecuados deben ser utilizados para identificar los datos, captarlos, registrarlos, estructurarlos en información y comunicarlos en tiempo y forma.

El proceso de clasificación de la información (punto 4.2) originará, de corresponder, planes de acción específicos para mejorar su calidad.
Los planes de mejoramiento de calidad de la información abarcarán las distintas etapas del ciclo de vida de los datos:

- Métodos o información por los cuales se originan y son recogidos.
- Procedimientos de conversión en formatos aptos para su procesamiento.
- Medios utilizados para el transporte y su recepción.
- Metodología de procesamiento.
- Procedimientos de almacenamiento y comunicación a los usuarios.

4. PAUTAS O PRINCIPIOS GENERALES VINCULADOS CON LA SEGURIDAD DE LA INFORMACIÓN

Se consideran aspectos específicos vinculados con la Seguridad de la Información:

- La existencia de Políticas de Administración de Personal que induzcan al mejor cumplimiento de la Política de Seguridad de la Información.
- La Clasificación de la Información.
- Los criterios y métodos utilizados en la Administración de Accesos.
- La Seguridad Física y Ambiental.
- La Gestión de Comunicaciones.
- La Gestión de Centros de Procesamiento referida al desarrollo, mantenimiento, soporte técnico y operación de los sistemas informáticos.
- La existencia de planes de contingencia.

4.1 Existencia de Políticas de Administración de Personal que induzcan al mejor cumplimiento de la Política de Seguridad de la Información

El recurso diferencial del CONICET lo constituyen las personas que lo conforman, por encima de los recursos tecnológicos ó económicos; es por ello que Recursos Humanos fomentará la motivación, el desarrollo y el adiestramiento de los agentes en materia de calidad y seguridad de la Información.
Se implementarán mecanismos de acción que contribuyan a evitar errores humanos, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de datos.
El Comité de Seguridad de la Información determinará la conveniencia y oportunidad de que los agentes del CONICET suscriban un compromiso de Confidencialidad o No-Divulgación.

4.2 Clasificación de la Información

La Información se clasificará en función de su sensibilidad a fin de definir niveles de protección y medidas de tratamiento especial, acordes a su nivel de criticidad. La clasificación efectuada será revisada periódicamente para detectar aquellos casos en los cuales por el transcurso del tiempo se ha convertido en "Información Pública" o "Información Obsoleta".
La destrucción de información obsoleta debe asegurar la confidencialidad de la misma hasta el momento de su eliminación definitiva.
Los Propietarios de la Información -en colaboración con el Responsable de Seguridad de la Información -son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, y de definir las áreas o usuarios específicos que deberán tener permisos de acceso. A fin de establecer el plazo de conservación -guarda- de la información se trabajará con el asesoramiento y colaboración del personal técnico de archivo dependiente de la Dirección de Despacho.

4.3 Administración de Accesos

Accederán a la información aquellas personas autorizadas. Los permisos se otorgarán en función de "la necesidad de hacer": los usuarios tendrán acceso a la información que precisan conocer, para poder cumplir con las tareas que les fueron asignadas.
Los derechos de acceso a los sistemas de información, bases de datos y servicios de procesamiento serán administrados prioritariamente utilizando técnicas de autenticación y autorización. Son de aplicación obligatoria para todos los

usuarios finales y para el personal técnico que define, instala, administra y mantiene el software de base y los programas aplicativos. Cuando por circunstancias especiales sea necesario recurrir a métodos alternativos, se requerirá formalmente la correspondiente autorización.
Los Propietarios de la Información determinarán quiénes están autorizados para ver, incorporar, modificar, ó eliminar datos. Para aquellos casos en los cuales los Propietarios de la Información definan las autorizaciones de acceso por áreas, serán los responsables de dichas áreas los que deberán indicar y mantener actualizado el nombre y apellido de los empleados que tendrán los accesos asignados. Estos procedimientos estarán documentados.

4.4 Seguridad Física y Ambiental

La seguridad física y ambiental constituyen elementos importantes a ser considerados para minimizar los riesgos de daños e interferencias a la información, y a las operaciones normales del Organismo.
El equipamiento destinado al procesamiento de la información del CONICET será protegido por medidas de seguridad física y controles de acceso de acuerdo a su nivel de criticidad.
La información se ubicará en áreas protegidas y resguardadas por perímetros de seguridad definidos, según el grado de sensibilidad de la misma.

4.5 Gestión de Comunicaciones

Los distintos canales de comunicación que permitan el intercambio de información con Organismos Externos y entre las distintas dependencias del CONICET, contemplarán la inclusión de medidas orientadas a proteger la vulnerabilidad de los datos enviados y/o recibidos.
Se tomarán recaudos especiales para la protección de la integridad de la información publicada electrónicamente, a fin de prevenir la modificación no autorizada que podría dañar la reputación del CONICET.

4.6 Gestión de Centros de Procesamiento de Datos

El desarrollo, mantenimiento y operación de las aplicaciones informáticas constituyen puntos críticos de seguridad. La seguridad de los sistemas de información deberá ser planificada desde el desarrollo de las aplicaciones y gestionada durante su mantenimiento.

Los sistemas informáticos que soporten los datos del Organismo -desarrollados por personal propio y/o terceros-, incluirán controles de seguridad y validación. Se dará prioridad a la implementación de controles automatizados preventivos por sobre cualquier otra metodología de control.
Principios de control interno tales como: segregación de tareas, controles cruzados y la existencia de rastros de auditoria, deberán ser tenidos en cuenta en la confección de todo esquema de manipulación de datos.
Los ambientes de operaciones, desarrollo, mantenimiento y prueba de los sistemas, estarán separados a fin de minimizar los riesgos de incidentes producidos por la utilización de información operativa, y a fin de garantizar la calidad de los procesos que se implementan.
Todo software instalado debe ser previamente autorizado y provenir de fuentes confiables.

4.7 Existencia de Planes de Contingencia

El desarrollo e implementación de Planes de Contingencia deberá asegurar la oportuna reanudación de las operaciones indispensables, protegiendo los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación. Deberán minimizarse los efectos de las posibles interrupciones provocadas por fallas en el equipamiento, accidentes y/o acciones deliberadas.

5. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

A fin de asegurar una adecuada Administración de la Seguridad de la Información se define la siguiente estructura organizativa, así como los roles y funciones asociadas.
Se crean:

1. El Comité de Seguridad de la información.
2. El Rol de Responsable de Seguridad de la Información.
3. La Figura de Propietario de la Información.

5.1 Comité de Seguridad de la Información

Está formado por un miembro del Directorio, representantes de las Gerencias, de la Unidad de Auditoría Interna y personal designado por el Directorio. Sus miembros elegirán un coordinador a los efectos de impulsar la concreción de los objetivos planteados. El Comité de Seguridad tiene entre sus funciones:

- Revisar y proponer a la máxima autoridad del CONICET para su aprobación, la Política y las funciones generales en materia de seguridad de la información.
- Asignar la propiedad de la información a las diversas áreas, en relación con sus funciones y competencias.
- Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes graves relativos a la seguridad.
- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área.
- Promover que la seguridad sea parte del proceso de planificación de la información.
- Promover la difusión y apoyo a la seguridad de la información dentro del CONICET.

5.2 Responsable de Seguridad de la Información

Cumplirá funciones relativas a la seguridad de los sistemas de información del CONICET, lo cual incluye la supervisión de los aspectos inherentes a los temas tratados en la presente Política.

Tiene entre sus funciones:

- Colaborar con los Propietarios de la Información en la clasificación y elaboración de las normas y procedimientos relacionados a la Seguridad de la Información.
- Asistir al personal en materia de seguridad de la información, y coordinar la interacción con Organismos especializados.
- Colaborar con el personal técnico especializado en la definición, control e implementación de medidas de seguridad lógica, física y ambiental para los controles de acceso, el procesamiento y el resguardo de datos.
- Efectuar el seguimiento, documentación y análisis de los incidentes de seguridad reportados.

Comunicarlos al Comité de Seguridad de la Información, a los Propietarios de la Información y al ArCERT - Coordinación de Emergencias en Redes Teleinformáticas-.

- Participar en la definición de estándares de seguridad a implementar en el ambiente informático, y validarlos periódicamente.
- Participar en la definición, documentación, prueba y actualización de los planes de contingencia.
- Participar en la elaboración y divulgación de los programas de capacitación referidos a la seguridad.

5.3 Propietario de la Información

Es el responsable de clasificar la información de acuerdo con el grado de sensibilidad y criticidad de la misma, y de definir qué usuarios deberán tener permisos de acceso de acuerdo a las tareas asignadas.
En todos los casos existe un área dentro del CONICET para la cual la Información sometida a análisis tiene un rol protagónico, en razón de su existencia como área funcional. El Comité de Seguridad de la Información asignará la Propiedad de la Información a las diversas Gerencias, en relación con sus funciones y competencias. Los niveles gerenciales se responsabilizarán por el cumplimiento de la política general, normas, procedimientos y estándares de seguridad de la información relativos a sus áreas. El concepto "Propietario de la Información" debe ser entendido desde su acepción técnica, no jurídica.

Ministerio de Educación, Ciencia y Tecnología
Secretaría de Ciencia, Tecnología e Innovación Productiva
Consejo Nacional de Investigaciones Científicas y Técnicas

GLOSARIO DE TERMINOS Y DEFINICIONES

Autenticidad	Asegura la validez de la información en tiempo, forma y distribución. Garantiza el origen de la información, validando al emisor a fin de evitar suplantación de identidades.
Confiabilidad	La información generada es adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
Confidencialidad	Garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
Dato	Representación formalizada de hechos, conceptos ó instrucciones adecuada para la comunicación, interpretación y procesamiento por medios humanos ó sistematizados.
Disponibilidad	Garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.
Estándar	Conjunto de parámetros lógicos o físicos determinados y específicos para cada ambiente, de forma de garantizar un marco de seguridad adecuado a las normas y procedimientos establecidos.
Información	Significado que se asigna a un dato soportado en cualquier medio. Es una salida del procesamiento de datos desde el punto de vista informático.
Integridad	Salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
Legalidad	Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el CONICET.
No Repudio	Evita que una entidad o persona que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

Ministerio de Educación, Ciencia y Tecnología
Secretaría de Ciencia, Tecnología e Innovación Productiva
Consejo Nacional de Investigaciones Científicas y Técnicas

Normas	Reglas concretas que definen cursos de acción precisos para las distintas tareas que se desarrollan dentro del CONICET; éstas deben regir a los procedimientos de Seguridad de la Información.
Política	Principios básicos que sirven de medio para alcanzar los objetivos del CONICET y sobre los cuales deben asentarse las normas y procedimientos.
Procedimientos	Detalle y ordenamiento de tareas tendientes a ejecutar y controlar las funciones administrativas u operativas del CONICET en línea con las normas de Seguridad de la Información.
Protección a la duplicación	Impide que se grabe una transacción para luego reproducirla con el objeto de simular múltiples peticiones del mismo remitente original. Asegura que una transacción sólo se realiza una vez, a menos que se especifique lo contrario.
Sistema de Información	Conjunto de recursos manuales y/o automatizados organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos.
Tecnología de la Información	Hardware y software operados por el CONICET o por terceros que procesen información en su nombre, para llevar a cabo funciones propias del Organismo.

2007 - "Año de la Seguridad Vial"

Ministerio de Educación, Ciencia y Tecnología
Secretaría de Ciencia, Tecnología e Innovación Productiva
Consejo Nacional de Investigaciones Científicas y Técnicas

ANEXO II

Integrantes del Comité de Seguridad de la Información en representación de cada una de las áreas:

Directorio de CONICET:	Dr. Mario Lattuada
Presidencia:	Ing. Alberto Arleo
Gerencia de Desarrollo Científico y Tecnológico:	Dr. Jorge Tezón
Gerencia de Gestión Operativa:	CPN. Jorge Figari
	Lic. Eduardo Wagener
Gerencia de Evaluación y Acreditación:	Lic. Jorge Atrio
Asesoría Legal:	Dr. Juan Poli
Unidad de Auditoria Interna:	CC. Ricardo Renyi

Responsable de Seguridad de la Información: CPN. Alberto Collia.