Universidad Nacional de Córdoba

República Argentina

Exp. 46-00-41399 y
agreg.: 76-05-00736

VISTO:

Las recientes actuaciones del Poder Ejecutivo Nacional en materia de seguridad de sistemas de información a través de la Decisión Administrativa 669/2004;

Que la Universidad Nacional de Córdoba posee sistemas de información que operan bajo tecnologías de información y comunicaciones para la gestión informatizada de diversas áreas específicas; y

CONSIDERANDO:

La creciente importancia que ostentan los sistemas de información que dependen de las tecnologías referidas en los Vistos;

Que, los sistemas referidos constituyen herramientas de misión crítica, y que poseen crucial importancia en el desarrollo de algunas actividades administrativas o académicas en esta Casa;

Que, la misma evolución de tales tecnologías implica el surgimiento de escenarios de complejidad en cuanto a las actividades de administración operativa necesaria para el correcto desempeño de los sistemas;

Que, para tales tareas de administración se requiere de un conjunto de profesionales especializados según distintos perfiles, para las diversas funciones en juego, a saber: desarrollo, personalización, testeo, instalación, puesta a punto, operación cotidiana y mantenimiento de los sistemas de información;

Que, la coordinación de las antedichas funciones requieren de instancias de coordinación que garanticen el correcto desempeño de los sistemas;

Que, para facilitar las tareas de coordinación se requiere del establecimiento de una normativa clara y adecuada que delimite las operaciones aceptables;

Que, es recomendable en esa normativa la inclusión de procedimientos a los que deberán ajustarse los actores involucrados en la administración de la información y de los sistemas;

Que, esta Universidad no posee aún una política completa al respecto;

Que, es conveniente introducir a la brevedad un conjunto mínimo de procedimientos en resguardo de la información y de los sistemas que la soportan;

Por ello y teniendo en cuenta lo informado a fojas 12 por la Secretaría de Ciencia y Tecnología, por la Comisión creada por Resolución Rectoral N° 302/00 y lo dictaminado por la Dirección de Asuntos Jurídicos a fs. 26 bajo el nro. 33775 cuyos términos se comparten y lo aconsejado por la Comisión de Vigilancia y Reglamento,

Universidad Nacional de Córdoba

República Argentina

Exp. 46-00-41399 y
agreg.: 76-05-00736

EL H. CONSEJO SUPERIOR
DE LA UNIVERSIDAD NACIONAL DE CÓRDOBA

R E S U E L V E :

ARTÍCULO 1°.- Disponer que el personal estable, con contrato temporario o profesional independiente bajo modalidad de locación de servicios, que cumple funciones de administración de los sistemas de información que obran en la Universidad, sea en el ámbito del Área Central, o en las distintas Unidades Académicas y que operen total o parcialmente bajo la jurisdicción de Secretarías o Subsecretarías del Área Central deberá dar cumplimiento a lo establecido en el ANEXO "Condiciones Mínimas de Seguridad de los Sistemas de Información" que forma parte de la presente.

ARTÍCULO 2°.- Adoptar los principios rectores en materia de seguridad de la información establecidos y descriptos en la Norma Argentina IRAM/ISO 17799, la que será aplicada a la manera de marco referencial para la solución de problemas y generación de políticas en materia de seguridad de la información en la Universidad.

ARTÍCULO 3°.- Declarar que dicha norma deberá ser de conocimiento obligatorio por parte del personal que cumple funciones en los sistemas de información en esta Universidad.

ARTÍCULO 4°.- Establecer que la normativa contenida en el ANEXO deberá formar parte de los contratos de locación de servicios de los profesionales que cumplen funciones en los sistemas de información dependiente del Área Central.

ARTÍCULO 5°.- Instruir a las Unidades Académicas de esta Casa a adherir a la presente Resolución.

ARTÍCULO 6°.- Comuníquese y pase para su conocimiento y efectos a la Subsecretaría de Informática.

DADA EN LA SALA DE SESIONES DEL H. CONSEJO SUPERIOR A VEINTIÚN DÍAS DEL MES DE MARZO DE DOS MIL SEIS.

/mae

Prof. Ing. FÉLIX R. ROCA
SECRETARIO GENERAL
UNIVERSIDAD NACIONAL DE CÓRDOBA

PROF. ING. JORGE H. GONZALEZ
RECTOR
UNIVERSIDAD NACIONAL DE CORDOBA

RESOLUCIÓN

120

Académicas y que operen total o parcialmente bajo la jurisdicción de Secretarías o Subsecretarías del Area Central deberá dar cumplimiento a lo establecido en el ANEXO "Condiciones Mínimas de Seguridad de los Sistemas de Información" que forma parte de la presente;

Artículo 2do:
Adoptar los principios rectores en materia de seguridad de la información establecidos y descriptos en la Norma Argentina IRAM/ISO 17799, la que será aplicada a la manera de marco referencial para la solución de problemas y generación de políticas en materia de seguridad de la información en la Universidad;

Artículo 3ro:
Declarar que dicha norma deberá ser de conocimiento obligatorio por parte del personal que cumple funciones en los sistemas de información en esta Universidad;

Artículo 4to.:
Que la normativa contenida en el ANEXO deberá formar parte de los contratos de locación de servicios de los profesionales que cumplen funciones en los sistemas de información dependientes del Area Central;

Artículo 5to.:
Invitase a las Unidades Académicas de esta Casa a adherir a la presente resolución;

ANEXO
Condiciones de Seguridad de los Sistemas de Información
Aplicable para Personal y Profesionales de Informática
en la Universidad Nacional de Córdoba

El presente Anexo expresa las condiciones de seguridad lógica y física requeridas por la Universidad ser aplicadas a sus sistemas de información, y que deberán ser cumplidas obligatoriamente por el Personal alcanzado.-

Primero: EL Personal que administre las diferentes funciones en los sistemas de información deberá colaborar activamente en el resguardo de la seguridad (lógica y física) de los sistemas de información de la UNC a los cuales tenga acceso en cumplimiento de sus funciones, estando obligado a:

1) Brindar protección a los datos de LA UNIVERSIDAD procurando que, por medio de sus servicios y de la aplicación eficaz de los recursos disponibles de equipamiento y programas

informáticos, la información contenida en los sistemas de LA UNIVERSIDAD cuenten con el mejor nivel posible de seguridad lógica y física.-

2) Mantener la integridad y disponibilidad de la información en los sistemas de LA UNIVERSIDAD, evitando acciones que puedan vulnerar, modificar sin autorización , eliminar o corromper los contenidos de tales sistemas.-
3) Registrar y comunicar a la Dependencia titular de los sistemas, de modo fehaciente y en plazos no superiores a las 24 horas, sobre los incidentes de seguridad que EL PROFESIONAL detectare en los sistemas de información de LA UNIVERSIDAD.-
4) Suministrar a la Dependencia titular de los sistemas, las claves de acceso, los programas fuente, la documentación o cualquier otro recurso o componente que corresponda a los sistemas de información, en la oportunidad y modalidad en que les sean solicitados por la Subsecretaría de Informática.-
5) Mantener la confidencialidad sobre los datos y sistemas, evitando copiarlos o darlos a conocimiento a personal o terceros no autorizados, entendiéndose que se trata de material reservado, excepto en aquellos casos en que la Dependencia titular de los sistemas disponga lo contrario. Esta condición de privacidad y confidencialidad mantendrá su vigencia tanto en horarios laborables como en no-laborables, y regirá aún despues de extinguida la presente relación contractual.-
6) No ceder a terceros las claves de acceso a los sistemas de información de la Universidad, en términos y modalidades similares a los expresados en el párrafo anterior.-
7) Ejercer tareas de control sobre los accesos lógicos o físicos a los sistemas de información de la Universidad cuya administración le haya sido asignada por el funcionario a cargo de la Dependencia titular de los sistemas .-
8) Evitar y suprimir los accesos lógicos remotos que apliquen procedimientos no encriptados o transmisión en "texto claro" de las claves de acceso a los sistemas antes referidos.-
9) Presentar informes periódicos sobre las tareas que desarrolla a los fines de permitir una adecuada supervisión o control que, en defensa de la seguridad e integridad de los sistemas, disponga la Subsecretaría de Informática, la Unidad de Auditoría Interna, la Secretaría de Administración o cualquier otro organismo de la Universidad al que le sean otorgadas funciones de contralor sobre los sistemas de información.-
10) Mantener el almacenamiento de los archivos de registro de sistemas (archivos de "logs") por el tiempo y bajo la modalidad que la Universidad determine, y facilitar el acceso de la Subsecretaría de Informática o de la Unidad de Auditoría Interna a tales archivos que sean generados por los sistemas de información. A los fines del ejercicio de acciones de monitoreo por parte de la Universidad, tales archivos de registro no podrán ser alterados o modificados, sea en sus contenidos o en los parámetros que permitan determinar sus fechas o tiempos de generación.-
11) Llevar un registro de las modificaciones solicitadas por las Unidades Académicas y demás Dependencias de la Universidad, preferentemente en libros de registro (formato de libros de actas) sobre soporte papel, asentando el tipo de modificación producida, organismo solicitante, fecha y hora de producción, y cualquier otro detalle que facilite el posterior monitoreo de los cambios producidos.-

12) Aplicar las modificaciones mencionadas sólo en tanto y cuanto éstas cuenten con el visto bueno del Subsecretario de Informática o del titular de la dependencia propietaria de los correspondientes sistemas.-
13) Ejecutar las políticas de respaldo de la información y sistemas, de acuerdo a lo normado por el Subsecretaría de Informática, o por la Autoridad Universitaria competente.-

Segundo: Todo el Personal alcanzado por el artículo 1ro. de la presente, suscribirá una declaración aceptando explícitamente que corresponde a la Universidad la plena potestad y derecho para aplicar políticas y procedimientos de supervisión, control o monitoreo sobre la actividad que desarrolla el referido personal, en resguardo de la seguridad de los sistemas de información que pertenezcan a la Universidad. A tales fines LA UNIVERSIDAD queda facultada a:

1) Auditar o contratar auditorías por terceros sobre la gestión de sus sistemas de información.-
2) Aplicar periódicamente, perfeccionar o disponer acciones y procedimientos de control para la protección física y lógica de los sistemas de información y de los recursos informáticos de su propiedad.-
3) Monitorear la actividad que EL PROFESIONAL desarrolle como consecuencia del presente vínculo contractual.-
4) Solicitar, a los fines de esclarecimiento en caso de incidentes de seguridad, el apartamiento temporario de las funciones de EL PROFESIONAL, si LA UNIVERSIDAD lo considerase de conveniencia.-
5) Incluir programas periódicos de entrenamiento y capacitación del personal en cuestiones relativas a la seguridad y operación segura de los sistemas de información, quedando EL PROFESIONAL obligado a colaborar con su experiencia y conocimientos en tales acciones, o bien a perfeccionarse a través de los mismos. Tales programas se llevarán a cabo bajo la supervisión exclusiva de la Subsecretaría de Informática.-

Tercero: EL PROFESIONAL se obliga a aceptar y respetar que:

1. Corresponde al Subsecretario de Informática o al Secretario de Administración según corresponda, la gestión y gerenciamiento de los sistemas de información de LA UNIVERSIDAD que operen bajo su respectiva jurisdicción. A tales efectos, en materia de seguridad informática, serán de aplicación los principios rectores, recomendaciones y terminología contenidos en la Norma Argentina IRAM-ISO/IEC 17799 que EL PROFESIONAL declara conocer.-
2. El desarrollo y verificación (testeo) de sistemas operativos, bases de datos y aplicaciones, o de las actualizaciones o cambio de versiones de los mismos, deberán contar con la aprobación previa del Subsecretario de Informática y, en los casos que correspondiere, de la Facultad, Instituto o Escuela propietaria de los recursos de información afectados. A tales efectos, y salvo el caso de circunstancias excepcionales debidamente justificadas, para tales iniciativas EL PROFESIONAL deberá solicitar por medios fehacientes la correspondiente

autorización y aprobación con al menos treinta (30) días de antelación al inicio de las actividades o acciones pertinentes, incluyendo en el pedido un análisis de los factores de riesgo ante fallas eventuales de los productos a aplicar o instalar.-

3. La información, claves de acceso, protocolos y procedimientos que residen en los sistemas de LA UNIVERSIDAD poseen el carácter de reservados y confidenciales, salvo disposición en contrario expresa de la Autoridad Universitaria.-
4. Los desarrollos de programas, aplicaciones o sistemas, que en todo o en parte realice EL PROFESIONAL como consecuencia de la presente relación contractual, constituyen propiedad exclusiva de LA UNIVERSIDAD, y que en consecuencia, le corresponde a la misma el acceso y posesión de la totalidad de la documentación, programas fuente, programas ejecutables, claves de acceso, reportes y archivos de registro ("logs").-

(Fin del Documento).----------

[1]POLITICA DE SEGURIDAD DE LA INFORMACION
Decisión Administrativa 669/2004
Establécese que los organismos del Sector Público Nacional comprendidos en los incisos a) y c) del artículo 8º de la Ley Nº 24.156 y sus modificatorias deberán dictar o adecuar sus políticas de seguridad. Conformación de Comités de Seguridad en la Información. Funciones de los mismos y responsabilidades en relación con la seguridad.
Bs. As., 20/12/2004
VISTO los Decretos N° 103 de fecha 25 de enero de 2001 y N° 624 de fecha 21 de agosto de 2003 y
CONSIDERANDO:
Que por la norma citada en primer término, se aprobó el Plan Nacional de Modernización de la Administración Pública Nacional orientado a un funcionamiento eficiente de la Administración Pública Nacional y a introducir en la gestión de las organizaciones públicas el cumplimiento de resultados mensurables y cuantificables.
Que la ADMINISTRACION PUBLICA NACIONAL no puede permanecer ajena a los avances y a la aplicación de las nuevas tecnologías de gestión, información y comunicación, ya que las mismas contribuyen al incremento de la productividad de los organismos y a optimizar el manejo de la información, reduciendo los costos asociados a su traslado y archivo.
Que este proceso sigue la tendencia, internacional de los países más adelantados, quienes han encarado proyectos de Gobierno Electrónico, con el fin de lograr la prestación de servicios más eficientes a los administrados y al mismo tiempo mejorar su gestión interna, mediante, la incorporación de modernas tecnologías informáticas.
Que dichos servicios deben ofrecerse con las máximas garantías de seguridad para satisfacer apropiadamente las demandas de la población y para evitar la comisión de ilícitos.
Que el uso de las tecnologías informáticas permite a la ADMINISTRACION PUBLICA NACIONAL manejar y procesar gran cantidad de información imprescindible para su normal funcionamiento.
Que la información puede ser objeto de una amplia gama de usos indebidos, debiéndose preservar su confidencialidad, integridad y disponibilidad, a fin de garantizar la prestación continua e ininterrumpida de los diversos servicios prestados por el Sector Público Nacional.
Que en este marco, se torna necesario que cada organismo del Sector Público Nacional sea capaz de prevenir que sus sistemas de información se vean afectados, implementando a tal fin políticas de seguridad, procedimientos internos y sistemas de prevención.
Que a los efectos de facilitar la elaboración y ejecución de las políticas mencionadas y elevar los niveles de seguridad de los sistemas de información de los organismos públicos, deviene necesario establecer una Política de Seguridad Modelo y dictar las normas aclaratorias y complementarias correspondientes.
Que es facultad de la SUBSECRETARIA DE LA GESTION PUBLICA de la JEFATURA DE GABINETE DE MINISTROS entender en la definición, de estrategias sobre tecnologías de información, comunicaciones asociadas y otros sistemas electrónicos de tratamiento de información en la ADMINISTRACION PUBLICA.
Que ha tomado intervención el Servicio Jurídico competente.

Que la presente medida se dicta en ejercicio de las facultades conferidas por el artículo 100, inciso 2 de la CONSTITUCION NACIONAL.
Por ello,
EL JEFE DE GABINETE DE MINISTROS
DECIDE:
Artículo 1° — POLITICA DE SEGURIDAD DE LA INFORMACION Establécese que los organismos del Sector Público Nacional comprendidos en el artículo 7° de la presente medida, deberán dictar o bien adecuar sus políticas de seguridad de la información conforme a la Política de Seguridad Modelo a dictarse de conformidad con el artículo 8°, dentro del plazo de CIENTO OCHENTA (180) días de aprobada dicha Política de Seguridad Modelo.
Art. 2° — COMITE DE SEGURIDAD DE LA INFORMACION las máximas autoridades de los organismos comprendidos en el artículo 7° de la presente medida, deberán conformar en sus ámbitos un Comité de Seguridad de la Información integrado por representantes de las Direcciones Nacionales o Generales o equivalentes del organismo.
Art. 3° —COORDINACION DEL COMITE DE SEGURIDAD DE LA INFORMACION. El Comité de Seguridad dé la Información citado en el artículo precedente, será coordinado por el Subsecretario o su equivalente en cada área Ministerial o Secretaría de la Presidencia de la Nación o por el funcionario designado por las máximas autoridades de cada organismo descentralizado, que tenga a su cargo las áreas de apoyo.
Art. 4° —FUNCIONES DEL COMITE DE SEGURIDAD DE LA INFORMACION. Serán funciones del Comité de Seguridad de la Información:
1. Revisar y proponer a la máxima autoridad del organismo para su aprobación, la Politica y las responsabilidades generales en materia de seguridad de la información.
2. Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
3. Tomar conocimiento y supervisar la investigación y el monitoreo de los incidentes relativos a la seguridad.
4. Aprobar las principales iniciativas para incrementar la seguridad de la información.
5. Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.
6. Garantizar que la seguridad sea parte del proceso de planificación de la información.
7. Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
8. Promover la difusión y apoyo, a la seguridad de la información dentro del Organismo.
9. Coordinar el proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información del Organismo frente a interrupciones imprevistas.
Art. 5° — RESPONSABILIDADES SOBRE LA SEGURIDAD DE LOS SISTEMAS DE INFORMACION. Las máximas autoridades de los organismos comprendidos en el artículo 7° del presente, deberán asignar las funciones relativas a la seguridad de sus sistemas de información a un funcionario de su planta dentro del plazo de CIENTO OCHENTA (180) días de aprobada la Política de Seguridad Modelo.

Art. 6° — La asignación de funciones relativas a la seguridad informática y la integración del Comité de Seguridad de la Información, establecidas en los artículos 5° y 2° de la presente medida, respectivamente, no deberá implicar erogaciones presupuestarias adicionales.

Art. 7° — ALCANCE. La presente Decisión Administrativa será de aplicación a los organismos comprendidos en los incisos a) y c) del artículo 8° de la Ley N° 24.156 y sus modificatorias.

Art. 8° — POLITICA DE SEGURIDAD MODELO - NORMAS ACLARATORIAS Y COMPLEMENTARIAS. Facúltase al señor SUBSECRETARIO DE LA GESTION PUBLICA de la JEFATURA DE GABINETE DE MINISTROS a aprobar la Política de Seguridad Modelo y dictar las normas aclaratorias y complementarias de la presente medida. El SUBSECRETARIO DE LA GESTION PUBLICA de la JEFATURA DE GABINETE DE MINISTROS podrá delegar en el DIRECTOR NACIONAL DE LA OFICINA NACIONAL DE TECNOLOGIAS DE INFORMACION dichas facultades.

Art. 9° — INVITACION. Invitase a los Gobiernos Provinciales, Municipales, al Gobierno de la Ciudad Autónoma de Buenos Aires y a los Poderes Legislativo y Judicial de la Nación a adherir a la presente.

Art. 10. — Comuníquese, publíquese, dése a la Dirección Nacional del Registro Oficial y archívese. — Alberto A. Fernández. — Aníbal D. Fernández.