

Universidad Nacional de Moreno

Unidad de Auditoria Interna

Proyecto de Auditoría: Tecnología de la información

Informe N°: 7-2012

Tabla de Contenidos

Informe Ejecutivo

I – Jurisdicción u Organismo	4
II – Síntesis - Conclusión	4
III – Lugar y fecha, firma y sello	5

Informe Analítico

I – Objeto de la Auditoría	7
II - Alcance	7
III – Limitaciones al Alcance	7
IV – Tarea realizada	7
V – Marco de referencia	8
VI – Circuito, tema o aspectos auditados	8
VII – Observaciones	8
VIII – Recomendaciones	8
IX – Opinión del Sector Auditado	8
X – Conclusión	9
XI – Lugar y fecha, firma y sello	9
Anexo I	10

Informe Ejecutivo

I – Jurisdicción u Organismo y Título

Universidad Nacional de Moreno.

Proyecto de auditoría: Tecnología de la Información – Resolución N° 48/05 SGN.

Informe N° 7-2012.

II – Síntesis - Conclusión

El presente Informe da cumplimiento al Plan de Auditoría 2012.

Su objetivo es evaluar el estado de situación del control interno de la tecnología informática de la Universidad, en base a los aspectos contemplados en la Resolución N° 48/05 SGN.

Las tareas fueron desarrolladas, a partir de un programa de trabajo específico emitido por la SIGEN enfocado en los siguientes temas: Organización Informática, Plan Estratégico Informático, Políticas y Procedimientos Informáticos, Seguridad Informática y Auditoría Interna-auditor de sistemas.

Las actividades de campo se llevaron a cabo entre el **20 de Agosto** y el **11 de Septiembre de 2012** en dependencias de la Universidad Nacional de Moreno.

El presente informe se encuentra referido a las observaciones y conclusiones sobre el objeto de la tarea por el período precedentemente indicado y no contempla la eventual ocurrencia de hechos posteriores que puedan modificar su contenido.

De la aplicación de procedimientos de auditoría, surgen las siguientes observaciones:

1. Respecto a la Organización Informática, no se da cumplimiento a los ítems 1.5 a 1.8.1, 1.9 y 1.10 del Instructivo de Trabajo N° 2/2012 GNyT - Circular N° 2/2012, detallados en Anexo I.
2. Respecto a las Políticas y Procedimientos, no se da cumplimiento en todos los casos al sub-ítem referido a Sanciones por Incumplimientos Especificadas y al ítem referido a Gestión y protección de bases de datos y archivos de datos, a Registro de incidentes sobre seguridad y a Gestión de sitios de internet / extranet / intranet.
3. No se ha creado aún, el Comité de Seguridad de la Información D.A. N° 669/04.

En razón de la observación planteada, se propone la siguiente recomendación.

1. Elaborar a la brevedad posible, un Manual de Organización que contemple la descripción de los distintos puestos de trabajo, con la asignación de sus deberes y su responsabilidad.
2. Elaborar a la brevedad posible, un Manual de Procedimientos Administrativos que contemple todos los procedimientos relativos al área de Tecnología Informática.
3. Conformar a la brevedad posible, el Comité de Seguridad de la Información.

En opinión del auditado, se informa que:

Respecto de la existencia de una descripción de la autoridad y responsabilidad de los puestos de trabajo que conforman la unidad de TI en la Universidad, es menester aclarar que no se dispone de un documento con el detalle de lo mencionado. Aun así, debe reconocerse que los empleados que ocupan formalmente dichos puestos tienen el conocimiento necesario para llevar sus tareas asignadas y las responsabilidades que el puesto le demande.

La unidad de TI ha comenzado a formular un proyecto para capacitar al usuario en la explotación de los informes que surgen de los sistemas de gestión para poder, en un mediano y largo plazo, comenzar a utilizar herramientas que permitan realizar análisis más complejos de dicha información resultante (lo que se conoce como minería de datos).

En cuanto a las Políticas y Procedimientos, dado que la Universidad transita en su segundo año de vida, faltan aún documentar algunos procedimientos y políticas del área, las que serán desarrolladas a lo largo de los años venideros.

Si bien por el momento no se ha constituido en el ámbito de la Universidad un Comité de Seguridad de la Información, se ha comenzado a transitar el camino de la construcción del área, tratando de ajustar y acomodar todo lo relativo a seguridad de la información, basándose en la normativa aplicable y vigente para dicha tarea.

Sobre la base de la tarea realizada, se concluye:

En función al objetivo planteado, al alcance y a la tarea realizada, la Universidad Nacional de Moreno, ha dado cumplimiento a la normativa detallada en el punto V del Informe Analítico, con las salvedades expuestas en el apartado Observaciones.

III – Lugar y fecha, firma y sello

Buenos Aires, 14 de Septiembre de 2012.

Informe Analítico

Universidad Nacional de Moreno
Proyecto de Auditoría: Tecnología de la Información –
Resolución N° 48/05 SGN
Informe N° 7

Informe Analítico

I - Objeto

El presente Informe da cumplimiento al Plan de Auditoría 2012.

Su objetivo es evaluar el estado de situación del control interno de la tecnología informática de la Universidad, en base a los aspectos contemplados en la Resolución N° 48/05 SGN.

II - Alcance

Las tareas fueron desarrolladas, a partir de un programa de trabajo específico emitido por la SIGEN enfocado en los siguientes temas: Organización Informática, Plan Estratégico Informático, Políticas y Procedimientos Informáticos, Seguridad Informática y Auditoría Interna-auditor de sistemas.

Las actividades de campo se llevaron a cabo entre el **20 de Agosto** y el **11 de Septiembre de 2012** en dependencias de la Universidad Nacional de Moreno.

III – Limitaciones al Alcance

No existen limitaciones al alcance.

IV – Tarea realizada

A los fines de verificar, la Organización Informática, el Plan Estratégico Informático, las Políticas y Procedimientos Informáticos, la Seguridad Informática y la Auditoría Interna-auditor de sistemas, se aplicaron los siguientes procedimientos:

1. Relevar los puntos de control conforme el Instructivo de Trabajo N°2/2012 – GNyT.

V – Marco de Referencia

Para el cumplimiento de los objetivos de auditoría, se aplicaron las siguientes normativas:

- Resolución N° 48/2005 SIGEN.
- Instructivo de Trabajo N° 2/2012 GNyT - Circular N° 2/2012.

-

VI – Circuito, tema o aspectos auditados

Ver anexo I.

VII – Observaciones

1. Respecto a la organización Informática, no se da cumplimiento a los ítems 1.5 a 1.8.1, 1.9 y 1.10 del Instructivo de Trabajo N° 2/2012 GNyT - Circular N° 2/2012, detallados en Anexo I.
2. Respecto a las Políticas y Procedimientos, no se da cumplimiento en todos los casos al sub-ítem referido a Sanciones por Incumplimientos Especificadas y al ítem referido a Gestión y protección de bases de datos y archivos de datos, a Registro de incidentes sobre seguridad y a Gestión de sitios de internet / extranet / intranet.
3. No se ha creado aún, el Comité de Seguridad de la Información D.A. N° 669/04.

VIII – Recomendaciones

1. Elaborar a la brevedad posible, un Manual de Organización que contemple la descripción de los distintos puestos de trabajo, con la asignación de sus deberes y su responsabilidad.
2. Elaborar a la brevedad posible, un Manual de Procedimientos Administrativos que contemple todos los procedimientos relativos al área de Tecnología Informática.
3. Conformar a la brevedad posible, el Comité de Seguridad de la Información.

IX – Opinión del sector auditado

Respecto de la existencia de una descripción de la autoridad y responsabilidad de los puestos de trabajo que conforman la unidad de TI en la Universidad, es menester aclarar que no se dispone de un documento con el detalle de lo mencionado. Aun así, debe reconocerse que los empleados que ocupan formalmente dichos puestos tienen el conocimiento necesario para llevar sus tareas asignadas y las responsabilidades que el puesto le demande.

La unidad de TI ha comenzado a formular un proyecto para capacitar al usuario en la explotación de los informes que surgen de los sistemas de gestión para poder, en un mediano y largo plazo, comenzar a utilizar herramientas que permitan realizar análisis más complejos de dicha información resultante (lo que se conoce como minería de datos).

En cuanto a las Políticas y Procedimientos, dado que la Universidad transita en su segundo año de vida, faltan aún documentar algunos procedimientos y políticas del área, las que serán desarrolladas a lo largo de los años venideros.

Si bien por el momento no se ha constituido en el ámbito de la universidad un Comité de Seguridad de la Información, se ha comenzado a transitar el camino de la construcción del área, tratando de ajustar y acomodar todo lo relativo a seguridad de la información, basándose en la normativa aplicable y vigente para dicha tarea.

X – Conclusión

En función al objetivo planteado, al alcance y a la tarea realizada, la Universidad Nacional de Moreno, ha dado cumplimiento a la normativa detallada en el punto V del Informe Analítico, con las salvedades expuestas en el apartado Observaciones.

XI – Lugar y fecha, firma y sello

Buenos Aires, 14 de Septiembre de 2012.

Anexo I. Instructivo de Trabajo N° 2/2012 GNyT - Circular N° 2/2012 - SINDICATURA GENERAL DE LA NACIÓN

Tecnología Informática (TI). Aspectos Organizacionales

ORGANISMO / ENTIDAD:	UNIVERSIDAD NACIONAL DE MORENO (UNM)
-----------------------------	--------------------------------------

1. ORGANIZACIÓN INFORMÁTICA

ASPECTO A EVALUAR	CUMPLE			COMENTARIOS / REF. A PAPELES DE TRABAJO
	SI	NO	PARCIAL	
1.1. ¿Se ha asignado la	X			Funciones STIC / Organigrama.

responsabilidad por las actividades de Tecnología de la Información (TI) de la organización a una única unidad? En caso afirmativo indicar Nombre completo del área y si la misma figura en el organigrama aprobado. Si existiera más de un área responsable, detallar Nombre de cada una y si figuran en el organigrama.				
1.2. ¿Se observa homogeneidad y unicidad de criterios y objetivos en materia de TI?	X			Plan de Gestión 2012.
1.2.1. ¿Todo el personal que desarrolla tareas informáticas depende del área responsable de TI? (es decir, no existen informáticos en otras áreas)	X			
1.2.2. ¿Todas las compras o contrataciones informáticas se tramitan con la intervención del área de TI? En caso negativo, indique los casos y su justificación.	X			
1.3. La unidad de TI ¿se encuentra ubicada dentro de la estructura orgánica de modo de poseer independencia respecto de las áreas usuarias?	X			
1.4. La unidad de TI ¿presta servicios a todos los sectores de la organización?	X			
1.5. ¿Se posee una descripción documentada y aprobada de los puestos de trabajo que conforman la unidad de TI?		X		
1.6. La mencionada descripción, ¿contempla tanto la autoridad como la responsabilidad de los puestos de trabajo?		X		
1.7. ¿Se encuentra todo el personal de TI notificado de sus deberes y responsabilidades?		X		
1.8. La asignación de responsabilidades efectuada ¿presenta una adecuada separación de funciones fomentando el control por oposición de intereses?		X		
1.8.1. Las funciones de Desarrollo y Mantenimiento de		X		

Sistemas ¿Se encuentran asignadas a personas que NO cumplen funciones en el ámbito de producción (procesamiento, administración de la plataforma, operaciones, etc.)?				
1.8.2. Considerando el tamaño del área informática, el resto de las funciones informáticas ¿se encuentran suficientemente separadas? (es decir aparte de la separación mínima entre Desarrollo y Producción aludida en el punto anterior)	X			
1.9. ¿Existe un procedimiento para identificar y documentar las necesidades de capacitación de todo el personal que utiliza los servicios informáticos?		X		
1.10. ¿Existe un plan de capacitación informático que abarque a usuarios finales y técnicos?		X		

2. PLAN ESTRATÉGICO DE TI

ASPECTO A EVALUAR	CUMPLE			COMENTARIOS / REF. A PAPELES DE TRABAJO
	SI	NO	PARCIAL	
2.1. ¿Se ha elaborado e implementado un plan informático estratégico?	X			
2.2. El plan estratégico de TI ¿se encuentra alineado con el plan estratégico y el presupuesto de la organización?	X			
2.3. Para la elaboración de dicho plan ¿se han considerado, evaluado y priorizado los requerimientos de todas las áreas de la organización?	X			
2.4. ¿Se han incluido en el plan informático, consideraciones respecto de la evolución de la infraestructura tecnológica, contemplando un esquema de actualización orientado a evitar la obsolescencia tecnológica?	X			
2.5. El plan informático de la organización ¿se encuentra aprobado por la máxima autoridad de la organización?	X			

2.6. El plan informático ¿describe para cada uno de los proyectos, los plazos, los beneficios a obtener así como los recursos necesarios?	X			
2.7. ¿Se realiza una revisión sistemática orientada a mantener la actualización del plan informático?	X			
2.8. ¿Se encuentra elaborado el presupuesto asociado a la ejecución del plan informático?	X			
2.9. El presupuesto ¿ha sido evaluado y aprobado?	X			
2.10. ¿Se encuentra incorporado al presupuesto anual de la organización?	X			
2.11. La dirección de la organización ¿supervisa en forma periódica el grado de avance del plan informático?	X			
2.12. Las adquisiciones de hardware, software u otros servicios informáticos ¿responden a los proyectos incluidos en el plan informático de la organización?	X			
2.13. ¿Todos los proyectos informáticos que se llevan a cabo, se encuentran contemplados en el Plan?	X			
2.14. En caso de existir situaciones de excepción sobre los puntos 2.12 y 2.13, ¿están estas situaciones autorizadas por la dirección de la organización y auditadas por la Unidad de Auditoría Interna?	X			

3. POLÍTICAS Y PROCEDIMIENTOS

ASPECTO A EVALUAR	CUMPLE			COMENTARIOS / REF. A PAPELES DE TRABAJO
	SI	NO	PARCIAL	
3.1. La unidad de TI ¿ha desarrollado, documentado y comunicado las políticas y procedimientos respecto de las actividades relacionadas con TI?			X	

3.2. Desarrollo de Sistemas / Modificaciones

ASPECTO A EVALUAR	CUMPLE	N/A
-------------------	--------	-----

	SI	NO
3.2.1. Documentado	X	
3.2.2. Aprobado	X	
3.2.3. Actualizado	X	
3.2.4. Tareas/Controles Definidos	X	
3.2.5. Responsables Identificados	X	
3.2.6. Sanciones por Incumplimientos Especificadas		X

3.3. Pasaje a producción sistemas

ASPECTO A EVALUAR	CUMPLE		N/A
	SI	NO	
3.3.1. Documentado	X		
3.3.2. Aprobado	X		
3.3.3. Actualizado	X		
3.3.4. Tareas/Controles Definidos	X		
3.3.5. Responsables Identificados	X		
3.3.6. Sanciones por Incumplimientos Especificadas		X	

3.4. Cambio de emergencia sobre sistemas o datos

ASPECTO A EVALUAR	CUMPLE		N/A
	SI	NO	
3.4.1. Documentado			X
3.4.2. Aprobado			X
3.4.3. Actualizado			X
3.4.4. Tareas/Controles Definidos			X
3.4.5. Responsables Identificados			X
3.4.6. Sanciones por Incumplimientos Especificadas			X

3.5. Documentación de sistemas

ASPECTO A EVALUAR	CUMPLE		N/A
	SI	NO	
3.5.1. Documentado			X
3.5.2. Aprobado			X
3.5.3. Actualizado			X
3.5.4. Tareas/Controles Definidos			X
3.5.5. Responsables Identificados			X
3.5.6. Sanciones por Incumplimientos Especificadas			X

3.6. Administración de proyectos informáticos

ASPECTO A EVALUAR	CUMPLE		N/A
	SI	NO	
3.6.1. Documentado	X		
3.6.2. Aprobado	X		
3.6.3. Actualizado	X		
3.6.4. Tareas/Controles Definidos	X		
3.6.5. Responsables Identificados	X		
3.6.6. Sanciones por Incumplimientos Especificadas		X	

3.7. Clasificación de activos informáticos (y de la información)

ASPECTO A EVALUAR	CUMPLE		N/A
	SI	NO	
3.7.1. Documentado			X
3.7.2. Aprobado			X
3.7.3. Actualizado			X
3.7.4. Tareas/Controles Definidos			X
3.7.5. Responsables Identificados			X
3.7.6. Sanciones por Incumplimientos Especificadas			X

3.8. Identificación y gestión de riesgos informáticos

ASPECTO A EVALUAR	CUMPLE		N/A
	SI	NO	
3.8.1. Documentado			X
3.8.2. Aprobado			X
3.8.3. Actualizado			X
3.8.4. Tareas/Controles Definidos			X
3.8.5. Responsables Identificados			X
3.8.6. Sanciones por Incumplimientos Especificadas			X

3.9. Generación y resguardo de backups

ASPECTO A EVALUAR	CUMPLE		N/A
	SI	NO	
3.9.1. Documentado	X		
3.9.2. Aprobado	X		
3.9.3. Actualizado	X		
3.9.4. Tareas/Controles Definidos	X		

3.9.5. Responsables Identificados	X		
3.9.6. Sanciones por Incumplimientos Especificadas		X	

3.10. Plan de recuperación ante interrupciones o contingencias

ASPECTO A EVALUAR	CUMPLE		N/A
	SI	NO	
3.10.1. Documentado	X		
3.10.2. Aprobado	X		
3.10.3. Actualizado	X		
3.10.4. Tareas/Controles Definidos	X		
3.10.5. Responsables Identificados	X		
3.10.6. Sanciones por Incumplimientos Especificadas		X	

3.11. Prueba del plan de contingencias

ASPECTO A EVALUAR	CUMPLE		N/A
	SI	NO	
3.11.1. Documentado	X		
3.11.2. Aprobado	X		
3.11.3. Actualizado	X		
3.11.4. Tareas/Controles Definidos	X		
3.11.5. Responsables Identificados	X		
3.11.6. Sanciones por Incumplimientos Especificadas		X	

3.12. Restricciones de acceso físico a los recursos informáticos críticos

ASPECTO A EVALUAR	CUMPLE		N/A
	SI	NO	
3.12.1. Documentado	X		
3.12.2. Aprobado	X		
3.12.3. Actualizado	X		
3.12.4. Tareas/Controles Definidos	X		
3.12.5. Responsables Identificados	X		
3.12.6. Sanciones por Incumplimientos Especificadas		X	

3.13. Registro de incidentes sobre seguridad

ASPECTO A EVALUAR	CUMPLE		N/A
	SI	NO	
3.13.1. Documentado		X	

3.13.2. Aprobado		X	
3.13.3. Actualizado		X	
3.13.4. Tareas/Controles Definidos		X	
3.13.5. Responsables Identificados		X	
3.13.6. Sanciones por Incumplimientos Especificadas		X	

3.14. Administración de permisos de acceso

ASPECTO A EVALUAR	CUMPLE		N/A
	SI	NO	
3.14.1. Documentado	X		
3.14.2. Aprobado	X		
3.14.3. Actualizado	X		
3.14.4. Tareas/Controles Definidos	X		
3.14.5. Responsables Identificados	X		
3.14.6. Sanciones por Incumplimientos Especificadas		X	

3.15. Gestión de contraseñas

ASPECTO A EVALUAR	CUMPLE		N/A
	SI	NO	
3.15.1. Documentado	X		
3.15.2. Aprobado	X		
3.15.3. Actualizado	X		
3.15.4. Tareas/Controles Definidos	X		
3.15.5. Responsables Identificados	X		
3.15.6. Sanciones por Incumplimientos Especificadas		X	

3.16. Atención y soporte a usuarios

ASPECTO A EVALUAR	CUMPLE		N/A
	SI	NO	
3.16.1. Documentado	X		
3.16.2. Aprobado	X		
3.16.3. Actualizado	X		
3.16.4. Tareas/Controles Definidos	X		
3.16.5. Responsables Identificados	X		
3.16.6. Sanciones por Incumplimientos Especificadas		X	

3.17. Operaciones, procesamiento y/o administración de la plataforma de procesamiento

	SI	NO	
3.17.1. Documentado			X
3.17.2. Aprobado			X
3.17.3. Actualizado			X
3.17.4. Tareas/Controles Definidos			X
3.17.5. Responsables Identificados			X
3.17.6. Sanciones por Incumplimientos Especificadas			X

3.18. Gestión de cambios a las operaciones y/o configuración de la plataforma

ASPECTO A EVALUAR	CUMPLE		N/A
	SI	NO	
3.18.1. Documentado			X
3.18.2. Aprobado			X
3.18.3. Actualizado			X
3.18.4. Tareas/Controles Definidos			X
3.18.5. Responsables Identificados			X
3.18.6. Sanciones por Incumplimientos Especificadas			X

3.19. Implementación y revisión de registros de transacciones o logs

ASPECTO A EVALUAR	CUMPLE		N/A
	SI	NO	
3.19.1. Documentado	X		
3.19.2. Aprobado	X		
3.19.3. Actualizado	X		
3.19.4. Tareas/Controles Definidos	X		
3.19.5. Responsables Identificados	X		
3.19.6. Sanciones por Incumplimientos Especificadas		X	

3.20. Gestión de licencias de software

ASPECTO A EVALUAR	CUMPLE		N/A
	SI	NO	
3.20.1. Documentado			X
3.20.2. Aprobado			X
3.20.3. Actualizado			X
3.20.4. Tareas/Controles Definidos			X
3.20.5. Responsables Identificados			X

3.20.6. Sanciones por Incumplimientos Especificadas			X
---	--	--	---

3.21. Mantenimiento preventivo de recursos informáticos

ASPECTO A EVALUAR	CUMPLE		N/A
	SI	NO	
3.21.1. Documentado			X
3.21.2. Aprobado			X
3.21.3. Actualizado			X
3.21.4. Tareas/Controles Definidos			X
3.21.5. Responsables Identificados			X
3.21.6. Sanciones por Incumplimientos Especificadas			X

3.22. Inventario de recursos informáticos

ASPECTO A EVALUAR	CUMPLE		N/A
	SI	NO	
3.22.1. Documentado	X		
3.22.2. Aprobado	X		
3.22.3. Actualizado	X		
3.22.4. Tareas/Controles Definidos	X		
3.22.5. Responsables Identificados	X		
3.22.6. Sanciones por Incumplimientos Especificadas		X	

3.23. Control y monitoreo de servicios informáticos prestados por terceros

ASPECTO A EVALUAR	CUMPLE		N/A
	SI	NO	
3.23.1. Documentado			X
3.23.2. Aprobado			X
3.23.3. Actualizado			X
3.23.4. Tareas/Controles Definidos			X
3.23.5. Responsables Identificados			X
3.23.6. Sanciones por Incumplimientos Especificadas			X

3.24. Gestión de sitios de internet / extranet / intranet

ASPECTO A EVALUAR	CUMPLE		N/A
	SI	NO	
3.24.1. Documentado		X	
3.24.2. Aprobado		X	

3.24.3. Actualizado		X	
3.24.4. Tareas/Controles Definidos		X	
3.24.5. Responsables Identificados		X	
3.24.6. Sanciones por Incumplimientos Especificadas		X	

3.25. Asignación de equipos o elementos informáticos a usuarios / Desplazamiento de equipos

ASPECTO A EVALUAR	CUMPLE		N/A
	SI	NO	
3.25.1. Documentado	X		
3.25.2. Aprobado	X		
3.25.3. Actualizado	X		
3.25.4. Tareas/Controles Definidos	X		
3.25.5. Responsables Identificados	X		
3.25.6. Sanciones por Incumplimientos Especificadas		X	

3.26. Desafectación de equipos o elementos informáticos

ASPECTO A EVALUAR	CUMPLE		N/A
	SI	NO	
3.26.1. Documentado	X		
3.26.2. Aprobado	X		
3.26.3. Actualizado	X		
3.26.4. Tareas/Controles Definidos	X		
3.26.5. Responsables Identificados	X		
3.26.6. Sanciones por Incumplimientos Especificadas		X	

3.27. Uso de firma digital

ASPECTO A EVALUAR	CUMPLE		N/A
	SI	NO	
3.27.1. Documentado	X		
3.27.2. Aprobado	X		
3.27.3. Actualizado	X		
3.27.4. Tareas/Controles Definidos	X		
3.27.5. Responsables Identificados	X		
3.27.6. Sanciones por Incumplimientos Especificadas		X	

3.28. Gestión de comunicaciones interorganizacionales, conexiones remotas, etc.

ASPECTO A EVALUAR	CUMPLE	N/A
-------------------	--------	-----

	SI	NO	
3.28.1. Documentado			X
3.28.2. Aprobado			X
3.28.3. Actualizado			X
3.28.4. Tareas/Controles Definidos			X
3.28.5. Responsables Identificados			X
3.28.6. Sanciones por Incumplimientos Especificadas			X

3.29. Teletrabajo

ASPECTO A EVALUAR	CUMPLE		N/A
	SI	NO	
3.29.1. Documentado			X
3.29.2. Aprobado			X
3.29.3. Actualizado			X
3.29.4. Tareas/Controles Definidos			X
3.29.5. Responsables Identificados			X
3.29.6. Sanciones por Incumplimientos Especificadas			X

3.30. Gestión y protección de bases de datos y archivos de datos

ASPECTO A EVALUAR	CUMPLE		N/A
	SI	NO	
3.30.1. Documentado		X	
3.30.2. Aprobado		X	
3.30.3. Actualizado		X	
3.30.4. Tareas/Controles Definidos		X	
3.30.5. Responsables Identificados		X	
3.30.6. Sanciones por Incumplimientos Especificadas		X	

4. SEGURIDAD

ASPECTO A EVALUAR	CUMPLE			COMENTARIOS / REF. A PAPELES DE TRABAJO
	SI	NO	PARCIAL	
4.1. ¿Se posee una política de seguridad de la información acorde con la normativa aplicable (D.A. Nº 669/04, Disp. ONTI Nº 06/05) y las prácticas recomendadas? (Nota: Si bien la normativa está dirigida a organismos de la Administración	X			

Central y Descentralizados, se requiere respuesta también del resto del SPN, dado que se trata de una práctica recomendada para incrementar el control interno y la seguridad informática).				
4.1.1. ¿Dicha política de seguridad, se encuentra aprobada?	X			
4.2. ¿Se ha constituido un Comité de Seguridad de la Información (según lo establecido en la D.A. N° 669/04)? (Nota: Si bien la normativa está dirigida a organismos de la Administración Central y Descentralizados, se requiere respuesta también del resto del SPN, dado que se trata de una práctica recomendada para incrementar el control interno y la seguridad informática).		X		
4.2.1. En caso afirmativo, ¿dicho Comité se reúne periódicamente?		X		
4.2.2. ¿Se documentan los temas tratados en las reuniones y decisiones adoptadas?		X		

5. AUDITORÍA INTERNA DE SISTEMAS

ASPECTO A EVALUAR	CUMPLE			COMENTARIOS / REF. A PAPELES DE TRABAJO
	SI	NO	PARCIAL	
5.1. ¿Se ejecutan auditorías internas de sistemas?	X			Cabe mencionar que el año 2012 se aprobó el primer Plan de Auditoría de la Universidad Nacional de Moreno, el que contempla el presente informe.
5.2. ¿Los responsables de llevar a cabo auditoría de sistemas, reúnen los requisitos de competencia técnica, independencia y autoridad para efectuar revisiones objetivas de los controles informáticos y preparar informes sobre sus hallazgos y recomendaciones?	X			El presente informe se realizó con la colaboración de personal idóneo y competente en Sistemas Informáticos.