Universidad Nacional de Moreno

Unidad de Auditoria Interna

Proyecto de Auditoría: Seguridad Informática
Sistemas del Consorcio SIU

Informe Nº: 6-2016

Tabla de Contenidos

Informe Ejecutivo

I – Jurisdicción u Organismo 4

II – Síntesis - Conclusión 4

III – Lugar y fecha, firma y sello 6

Informe Analítico

I – Objeto de la Auditoria 8

II - Alcance 8

III – Limitaciones al Alcance 8

IV – Tarea realizada 8

V – Marco de referencia 9

VI – Circuito, tema o aspectos auditados 9

VII – Observaciones 11

VIII – Recomendaciones 12

IX – Opinión del Sector Auditado 13

X – Conclusión 15

XI – Lugar y fecha, firma y sello 15

Informe Ejecutivo

I – Jurisdicción u Organismo y Titulo

Universidad Nacional de Moreno.

Proyecto de auditoría: Seguridad Informática. Sistemas del Consorcio SIU.

Informe Nº 6-2016.

II – Síntesis - Conclusión

El presente Informe da cumplimiento al Plan de Auditoria 2016.

Su objetivo es evaluar las políticas, normas y procedimientos de control, de los Sistemas Informáticos del Consorcio SIU, utilizados por la Universidad Nacional de Moreno.

Las tareas fueron desarrolladas, conforme las Normas de Auditoría Interna Gubernamental (Resolución N°152/02) y del Manual de Control Interno Gubernamental (Resolución N°03/11).

Las actividades de campo se llevaron a cabo entre el **2 de mayo** y el **29 de julio de 2016** 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 auditoria, surgen las siguientes observaciones:

1. Las contraseñas de los usuarios de los Sistemas Siu Mapuche y Siu Guaraní no caducan. Ello conlleva como riesgo, mantener una misma contraseña para un usuario, aumentando la probabilidad de accesos indebidos a los sistemas, como, por ejemplo, a través de suplantación de identidad. (alta)
2. Existe un número importante de Usuarios privilegiados (usuarios con permisos para alterar datos) en los Sistemas Siu Mapuche y Siu Guaraní. Asimismo, el acceso a información sensible o confidencial, podría verse afectado por la gran cantidad de usuarios para leer y/o modificar datos o por usuarios cuya naturaleza de trabajo no requiere acceder a determinada información. (alta)
3. No hay procesos y/o procedimientos formalizados para las actividades que se ejecutan, o requerimientos que se reciben. La carencia de documentación sobre las actividades que realizan o cómo se administra el sistema, es un potencial riesgo en caso que la persona se ausente o se desvincule de la Universidad. (media)

4. Existen requerimientos de usuarios que son gestionados y resueltos de manera informal. No contar con un procedimiento definido y formalizado para cada tipo de requerimiento aumenta la probabilidad de error humano al otorgar accesos indebidos o no validados por los responsables de la información, afectando la confidencialidad e integridad de la información. (media)
5. Existen 4 usuarios del sistema Siu Mapuche activos al 31 de mayo de 2016, que no figuran en la nómina de empleados de la Universidad (la fecha corresponde a la baja procesada por el área de Recursos Humanos). Dichos usuarios continúan teniendo acceso a la información del Sistema según su perfil definido. El riesgo que ello conlleva, podría ser mayor si el usuario también estuviese activo en la red y/o tuviese permisos para alterar información en el sistema. (baja)
6. El personal del área de Sistemas, utiliza un usuario privilegiado con permisos de Administración total del sistema (usuario toba). Existen además dos usuarios genéricos (Reporte y prueba) que no están asociados a un empleado en el sistema. La práctica de usuarios genéricos y/o compartidos no permite individualizar qué persona física ejecutó acciones sobre el sistema. El usuario toba cuenta con permisos de administración total, por lo que el riesgo es mayor, ya que podría alterar cualquier valor del sistema (incluso Actas de alumnos) sin la debida identificación. (alta)
7. Existen 5 usuarios en sistema Siu Guaraní que al 31 de Mayo de 2016 no figuran en la nómina de empleados de la Universidad (la fecha corresponde a la baja procesada por el área de Recursos Humanos). Dichos usuarios continúan teniendo acceso a la información del Sistema según su perfil definido. Asimismo, el 30% de los usuarios activos en el sistema no accedió a la aplicación en lo que va del año 2016. (baja)

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

1. Definir y formalizar una política general sobre Contraseñas y aplicarla a cada usuario de los sistemas según corresponda.
2. Revisar los usuarios privilegiados en los sistemas para definir si el privilegio es requerido o no; además, implementar controles sobre los usuarios privilegiados con determinada frecuencia. Adicionalmente, trabajar con los responsables de la información de cada sistema para acordar un mecanismo de autorización de privilegios.
3. Definir los tipos de requerimientos que pueden recibir por parte de los usuarios y documentar un procedimiento sobre cómo resolverlos en los sistemas.
4. Establecer un mecanismo de gestión de requerimientos para atender cada tipo de solicitud que pueden generar los usuarios, permitiendo la trazabilidad y asegurando los niveles de aprobación necesarios según corresponda. Definir con las áreas responsables de la información, un

mecanismo de aprobación de usuarios y/o privilegios según el rol del usuario.

5. Eliminar a los usuarios que no pertenecen más a la Universidad, del sistema Siu Mapuche y revisar que no estén activos en los demás sistemas de la Universidad. Si bien el Manual de "*Seguridad de la Información*" define claramente que la responsabilidad de solicitar la baja de usuarios corresponde al área usuaria, se recomienda que el área de Sistemas establezca un mecanismo de revisión periódica de usuarios y privilegios.
6. Eliminar o minimizar el uso del usuario toba. En caso que no pueda ser eliminado, asignar un responsable por las acciones de dicho usuario y modificar su contraseña. Todos aquellos administradores que utilicen dicho usuario debieran solicitar usuarios con perfil administrador según el proceso correspondiente. Con respecto a los usuarios reporte y prueba, revisar el uso y necesidad de dichos usuarios e identificar responsables en caso que no sean dados de baja.
7. Eliminar a los usuarios que no pertenecen más a la Universidad, del Sistema Siu Guaraní y revisar que no permanezcan activos en los demás sistemas de la Universidad.

Sobre la base de la tarea realizada, se concluye:

Las políticas, normas y procedimientos de control aplicados sobre los sistemas informáticos Siu Mapuche y Siu Guaraní utilizados por la Universidad Nacional de Moreno resultan satisfactorios, excepto por lo informado en el apartado Observaciones.

III – Lugar y fecha, firma y sello

Buenos Aires, 29 de julio de 2016.

Informe Analítico

Universidad Nacional de Moreno

Proyecto de Auditoría: Seguridad Informática.

Sistemas del Consorcio SIU
Informe Nº 6-2016

Informe Analítico

I - Objeto

El presente Informe da cumplimiento al Plan de Auditoria 2016.

Su objetivo es evaluar las políticas, normas y procedimientos de control, de los Sistemas Informáticos del Consorcio SIU, utilizados por la Universidad Nacional de Moreno.

II - Alcance

Las tareas fueron desarrolladas, conforme las Normas de Auditoría Interna Gubernamental (Resolución N°152/02) y del Manual de Control Interno Gubernamental (Resolución N°03/11).

Las actividades de campo se llevaron a cabo entre el **2 de mayo** y el **29 de julio de 2016** en dependencias de la Universidad Nacional de Moreno.

III – Limitaciones al Alcance

No existen limitaciones al alcance.

IV – Tarea realizada

A los fines de evaluar la gestión, políticas, normas y procedimientos de control, de los Sistemas Informáticos del Consorcio SIU, utilizados por la Universidad Nacional de Moreno, se aplicaron los siguientes procedimientos:

1. Entrevistas a responsables y usuarios del sistema informático.
2. Revisión y análisis de procedimientos, métodos y técnicas, aplicables a la seguridad y confiabilidad de los sistemas informáticos.
3. Verificación de documentación y análisis de la integridad de la información que surge de los sistemas informáticos.

V – Marco de Referencia

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

- Mejores prácticas de Información Tecnológica.

VI – Circuito, tema o aspectos auditados

La tarea de auditoria se llevó a cabo sobre una muestra de Sistemas Informáticos, representativos de la actividad que desarrolla la Universidad. Se trabajó sobre los Sistemas Siu Mapuche y Siu Guaraní.

Cabe señalar, que el conocimiento y habilidad del personal que ha sido entrevistado durante el trabajo de auditoria, es destacado (Sistemas, Secretaría Académica y RRHH), convirtiéndose en un activo muy valioso para la Universidad. Asimismo, se destaca, la actitud proactiva y de apoyo continuo en el desarrollo del trabajo realizado.

También se destaca, la elaboración y puesta en marcha, del Manual de Seguridad de la Información.

De la aplicación de los procedimientos descriptos en el apartado Tarea Realizada, se numeran aquellos aspectos destacados, clasificándose los mismos en tres categorías: General, SIU Mapuche y SIU Guaraní. La categoría General manifiesta aspectos que alcanzan a la totalidad de los sistemas verificados. Las categorías Siu Mapuche y Siu Guaraní corresponden a los aspectos propios de cada sistema.

Categoría	ALTA	MEDIA	BAJA
General	2	2	0
SIU Mapuche	0	0	1
SIU Guaraní	1	0	1

1. Aspectos que alcanzan a la totalidad de los sistemas relevados

1.1 Modificaciones de Usuarios

Se evidencia en los sistemas, que las contraseñas de sus usuarios no caducan. Ello conlleva como riesgo, mantener una misma contraseña para un usuario, aumentando la probabilidad de accesos indebidos a los sistemas, como, por ejemplo, a través de suplantación de identidad.

1.2 Usuarios Privilegiados

Existe un gran número de Usuarios privilegiados (usuarios con permisos para alterar datos).
En la revisión se observó lo siguiente:

- El mecanismo para asignar privilegios no es claro o no está formalizado.
- Existen privilegios asociados a usuarios cuyos roles han cambiado y podrían no ser necesarios.

Lo antedicho, refleja como riesgo, que el acceso a información sensible o confidencial, podría verse afectado por la gran cantidad de usuarios para leer y/ o modificar datos o por usuarios cuya naturaleza de trabajo no requiere acceder a determinada información.

1.3 Documentación

Ausencia de procesos y/o procedimientos formalizados para las actividades que se ejecutan o requerimientos que se reciben.
Si bien los responsables de los sistemas demuestran habilidad para administrar los sistemas, la carencia de documentación sobre las actividades que realizan o cómo se administra el sistema, es un potencial riesgo en caso que la persona se ausente o se desvincule de la Universidad.

1.4 Gestión de requerimientos

Durante la revisión se observó lo siguiente:

- Existen requerimientos de usuarios que son gestionados y resueltos de manera informal.
- El proceso de aprobación del Formulario "***Solicitud de Usuario***" no está claro para los usuarios.

No contar con un procedimiento definido y formalizado para cada tipo de requerimiento aumenta la probabilidad de error humano al otorgar accesos indebidos o no validados por los responsables de la información, afectando la confidencialidad e integridad de la información. Ejemplos de esto son:

- Reseteo de contraseñas de manera telefónica sin ningún tipo de validación al usuario
- Pedidos de modificación de datos no contemplados por los flujos de información normales de los sistemas (modificar actas, calificaciones, etc.)

2. Aspectos que alcanzan al Sistema Siu Mapuche

2. 1 Altas, Bajas y Modificaciones de usuarios

Se evidencian 4 usuarios del sistema Siu Mapuche, activos en sistema al 31 de mayo de 2016, que no aparecen en la nómina de empleados de la Universidad (la fecha corresponde a la baja procesada por el Depto de Recursos Humanos).
Dichos usuarios continúan teniendo acceso a la información del Sistema según su perfil definido. El riesgo que ello conlleva, podría ser mayor si el usuario también estuviese activo en la red y/o tuviese permisos para alterar información en el sistema.
Si bien el Manual de "***Seguridad de la Información***" define claramente que la responsabilidad de solicitar la baja de usuarios corresponde al área usuaria, resulta necesario establecer un mecanismo de revisión periódica de usuarios y privilegios.

3. Aspectos que alcanzan al Sistema Siu Guaraní

3.1 Usuarios genéricos y/o compartidos

Durante la revisión del sistema y de Actas académicas con modificaciones al 31 de mayo de 2016, se observó lo siguiente:

- El personal del área de Sistemas, utiliza un usuario privilegiado con permisos de Administración total del sistema (usuario toba).
- Existen además dos usuarios genéricos (Reporte y prueba) que no están asociados a un empleado en el sistema.

La práctica de usuarios genéricos y/o compartidos no permite individualizar qué persona física ejecutó acciones sobre el sistema. El usuario toba cuenta con permisos de administración total, por lo que el riesgo es mayor, ya que podría alterar cualquier valor del sistema (incluso Actas) sin la debida identificación.

3. 2 Altas, Bajas y Modificaciones de usuarios

Se evidencian 5 usuarios en sistema al 31 de mayo de 2016 que no aparecen en la nómina de empleados de la Universidad (la fecha corresponde a la baja procesada por el Depto de Recursos Humanos).
Se reitera que el riesgo ocasionado, podría ser mayor si el usuario también estuviese activo en la red y/o tuviese permisos para alterar información en el sistema.
Adicionalmente, se observa que el 30% de los usuarios activos en el sistema no accedió a la aplicación en lo que va del año 2016.

VII – Observaciones

1. Las contraseñas de los usuarios de los Sistemas Siu Mapuche y Siu Guaraní no caducan. Ello conlleva como riesgo, mantener una misma contraseña para un usuario, aumentando la probabilidad de accesos indebidos a los sistemas, como, por ejemplo, a través de suplantación de identidad. (alta)
2. Existe un número importante de Usuarios privilegiados (usuarios con permisos para alterar datos) en los Sistemas Siu Mapuche y Siu Guaraní. Asimismo, el acceso a información sensible o confidencial, podría verse afectado por la gran cantidad de usuarios para leer y/o modificar datos o por usuarios cuya naturaleza de trabajo no requiere acceder a determinada información. (alta)
3. No hay procesos y/o procedimientos formalizados para las actividades que se ejecutan, o requerimientos que se reciben. La carencia de documentación sobre las actividades que realizan o cómo se administra el sistema, es un potencial riesgo en caso que la persona se ausente o se desvincule de la Universidad. (media)
4. Existen requerimientos de usuarios que son gestionados y resueltos de manera informal. No contar con un procedimiento definido y formalizado para cada tipo de requerimiento aumenta la probabilidad de error humano al otorgar accesos indebidos o no validados por los

responsables de la información, afectando la confidencialidad e integridad de la información. (media)

5. Existen 4 usuarios del sistema Siu Mapuche activos al 31 de mayo de 2016, que no figuran en la nómina de empleados de la Universidad (la fecha corresponde a la baja procesada por el área de Recursos Humanos). Dichos usuarios continúan teniendo acceso a la información del Sistema según su perfil definido. El riesgo que ello conlleva, podría ser mayor si el usuario también estuviese activo en la red y/o tuviese permisos para alterar información en el sistema. (baja)
6. El personal del área de Sistemas, utiliza un usuario privilegiado con permisos de Administración total del sistema (usuario toba). Existen además dos usuarios genéricos (Reporte y prueba) que no están asociados a un empleado en el sistema. La práctica de usuarios genéricos y/o compartidos no permite individualizar qué persona física ejecutó acciones sobre el sistema. El usuario toba cuenta con permisos de administración total, por lo que el riesgo es mayor, ya que podría alterar cualquier valor del sistema (incluso Actas de alumnos) sin la debida identificación. (alta)
7. Existen 5 usuarios en sistema Siu Guaraní que al 31 de Mayo de 2016 no figuran en la nómina de empleados de la Universidad (la fecha corresponde a la baja procesada por el área de Recursos Humanos). Dichos usuarios continúan teniendo acceso a la información del Sistema según su perfil definido. Asimismo, el 30% de los usuarios activos en el sistema no accedió a la aplicación en lo que va del año 2016. (baja)

VIII – Recomendaciones

1. Definir y formalizar una política general sobre Contraseñas y aplicarla a cada usuario de los sistemas según corresponda.
2. Revisar los usuarios privilegiados en los sistemas para definir si el privilegio es requerido o no; además, implementar controles sobre los usuarios privilegiados con determinada frecuencia. Adicionalmente, trabajar con los responsables de la información de cada sistema para acordar un mecanismo de autorización de privilegios.
3. Definir los tipos de requerimientos que pueden recibir por parte de los usuarios y documentar un procedimiento sobre cómo resolverlos en los sistemas.
4. Establecer un mecanismo de gestión de requerimientos para atender cada tipo de solicitud que pueden generar los usuarios, permitiendo la trazabilidad y asegurando los niveles de aprobación necesarios según corresponda. Definir con las áreas responsables de la información, un mecanismo de aprobación de usuarios y/o privilegios según el rol del usuario.
5. Eliminar a los usuarios que no pertenecen más a la Universidad, del sistema Siu Mapuche y revisar que no estén activos en los demás

sistemas de la Universidad. Si bien el Manual de "*Seguridad de la Información*" define claramente que la responsabilidad de solicitar la baja de usuarios corresponde al área usuaria, se recomienda que el área de Sistemas establezca un mecanismo de revisión periódica de usuarios y privilegios.

6. Eliminar o minimizar el uso del usuario toba. En caso que no pueda ser eliminado, asignar un responsable por las acciones de dicho usuario y modificar su contraseña. Todos aquellos administradores que utilicen dicho usuario debieran solicitar usuarios con perfil administrador según el proceso correspondiente. Con respecto a los usuarios reporte y prueba, revisar el uso y necesidad de dichos usuarios e identificar responsables en caso que no sean dados de baja.
7. Eliminar a los usuarios que no pertenecen más a la Universidad, del Sistema Siu Guaraní y revisar que no permanezcan activos en los demás sistemas de la Universidad.

IX – Opinión del sector auditado

1. La STIC tiene como tarea programada la implementación de caducidad de las contraseñas cada noventa días en los sistemas Mapuche, Guaraní, Pilagá y Diaguita.
   Se está trabajando actualmente sobre el sistema Mapuche. Esta implementación será concluida en el trascurso del mes de septiembre. Se estima para el mes de octubre la implementacion sobre Guaraní y durante el mes de noviembre en el resto de los sistemas.
2. La STIC sólo otorga sobre los sistemas y recursos de red los permisos autorizados mediante el Formulario "***Solicitud de Usuario***", herramienta implementada en la Universidad desde el año 2013. Dicho formulario, disponible en la Intranet, debe ser enviado por los responsables de cada área de la Universidad, a nivel de Secretario/Subsecretario, para autorizar los permisos, permitiendo detallar qué nivel de acceso es requerido en cada caso. Esta misma herramienta deben utilizar para quitar los permisos o dar de baja un usuario. Con el objetivo de formalizar estos aspectos, en Mayo de 2014 el Consejo Superior de la UNM aprobó el **Manual de Seguridad de la Información** que, respecto a este punto observado en la auditoría detalla: *"**Control de Acceso a la Información: ADMINISTRACIÓN DE USUARIOS** Todo personal de la UNM que necesite disponer de herramientas o servicios informáticos, debe ser inicialmente autorizado por medio del FORMULARIO aprobado a tal fin, el cual, deberá estar firmado por la máxima autoridad del área (con rango no menor a SECRETARIO o la máxima autoridad de nivel equivalente). Este FORMULARIO deberá ser entregado a la STIC, que asignará los elementos (hardware, usuario de red, mail institucional y accesos a los sistemas de información de la UNIVERSIDAD), según lo determine dicho responsable. Si se necesitara posteriormente modificar*

(ampliar o reducir) los accesos ya otorgados, se utilizará el mismo procedimiento de alta de usuario: confección del FORMULARIO, autorización por parte de un superior y entrega a la SUBSECRETARÍA. En caso de retiro de un funcionario, es responsabilidad de las autoridades informar a la STIC sobre la anulación y cancelación de los derechos otorgados como usuario informático de la UNM." Sin embargo, dado que esta Subsecretaría reconoce que no es informada sobre la baja de accesos, se trabaja en forma contínua, concientizando a las distintas áreas de la UNM, en la importancia de actualizar la información de usuarios y accesos a sistemas y recursos de red. Cabe mencionar a su vez que dentro del plan de actividades, se encuentra programado para este segundo semestre trabajar en la revisión, modificación y creación de perfiles de acceso a las aplicaciones y los datos de cada uno de los sistemas, dado que a medida que se fue incorporando personal a las áreas de la Universidad se fueron complejizando los diferentes requierimientos de accesos respecto a lo definido al momento de la instalación inicial de los sistemas. Esta tarea, que se realizará de manera conjunta con el referente funcional de cada una de las áreas, se ha iniciado en el corriente mes comenzando con el sistema Diaguita.

3. Se implementó durante el mes de agosto/2016, el registro interno de los distintos requerimientos que se reciben de las áreas, por parte del personal de la STIC, con la finalidad de organizar los pedidos y la distribución del trabajo, y de realizar el seguimiento de lo que se encuentra pendiente de resolución. No se está documentando en esta planilla la forma de resolución de los pedidos. Se tomará en cuenta la recomendación recibida, en los casos en que sea últil registrarlo para resolver rápidamente un requerimiento posterior similar.
4. Respecto a este punto, fue remitido a las áreas usuarias de sistemas de información, desde la Secretaría General un memo. Mediante este mecanismo se les solicita que formalicen el representante funcional de cada sistema, quien será el encargado de hacer llegar, mediante el formulario que se adjunta, las modificaciones que se requieran sobre las aplicaciones (si corresponde) o sus bases de datos. Este mecanismo ya se encuentra en funcionamiento.
5. El formulario "Solicitud de Usuario", mencionado en el apartado "**A.2 Usuarios Privilegiados",** es la herramienta que debe ser usada por los responsables de áreas para informar la necesidad de dar de baja los usuarios sobre los sistemas. Esto puede suceder cuando el personal es traspasado a otra dependencia dentro de la UNM o es dado de baja de la Institución. Al respecto, el **Manual de Seguridad de la Información** ya citado, detalla específicamente: *"En caso de retiro de un funcionario, es responsabilidad de las autoridades informar a la STIC sobre la anulación y cancelación de los derechos otorgados como usuario informático de la UNM."* Cabe destacar que, normalmente, la STIC no es informada de estos cambios, motivo por el cual se han detectado las anormalidades que detalla el informe de auditoría. Para resolver los casos de bajas definitivas de la planta de personal de la UNM se implementó en un mecanismo periódico de comunicación entre el

Departamento de Recursos Humanos y la STIC, mediante el cual se informan las bajas mensuales. Sin embargo, sigue quedando pendiente resolver los casos en los cuales un agente cambia de área dentro de la UNM y el área que deja no pide a la STIC la baja en los sistemas a los cuales tenía acceso.

6. Respecto a los usuarios "**toba**", con permisos de administración total sobre el sistema, y "**prueba**", generado para tener una visión particular de la aplicación sobre el ambiente de producción para la resolución de emergencias, solo lo utilizan la persona responsable del Departamento de Sistemas y el programador de desarrollos personalizados sobre Guaraní. En cuanto al usuario "**reporte**", igualmente, el conocimiento de la contraseña y su uso corresponde a la persona Responsable del Departamento y al desarrollador de reportes personalizados de Guaraní. No hay más técnicos ni funcionarios que hagan uso de estos usuarios o conozcan sus contraseñas, por lo cual no se ha justificado la generación de usuarios administradores personalizados. No obstante lo cual, se considerará la recomendación realizada.
7. Esta observación queda respondida en la observacion referente al sistema Mapuche.

X – Conclusión

Las políticas, normas y procedimientos de control aplicados sobre los sistemas informáticos Siu Mapuche y Siu Guaraní utilizados por la Universidad Nacional de Moreno resultan satisfactorios, excepto por lo informado en el apartado Observaciones.

XI – Lugar y fecha, firma y sello

Buenos Aires, 29 de julio de 2016.